DIE ONTWIKKELING VAN 'N KATEGORISERINGSMEGANISME VIR BEHEERMAATREëLS IN DIE VELD VAN REKENAARSEKERHEID EN DIE KOPPELING DAARVAN MET STANDAARDE VIR BEHEERMAATREëLS.

C.J. BOSCH

87/1893/4

DIE ONTWIKKELING VAN 'N KATEGORISERINGSMEGANISME VIR BEHEERMAATREëLS IN DIE VELD VAN REKENAARSEKERHEID EN DIE KOPPELING DAARVAN MET STANDAARDE VIR BEHEERMAATREëLS

deur

CHRISTIAAN JOHANNES BOSCH

VERHANDELING

voorgelê ter vervulling van die vereistes
vir die graad

MAGISTER IN DIE EKONOMIESE EN BESTUURSWETENSKAPPE

in

INFORMATIKA

in die

FAKULTEIT EKONOMIESE EN BESTUURSWETENSKAPPE

aan die

RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER : Prof. J.H.P. Eloff

Mei 1992

Opgedra aan my ouers

met onuitspreeklike dank vir 24 jaar se liefde, onderskraging en leiding.

Aan Kobie - dankie vir soveel om sin aan alles te gee.

'n Opregte woord van dank aan my studieleier, prof. J.H.P. Eloff, vir sy bekwame leiding en aanmoediging met die studie gedoen vir hierdie verhandeling, asook vir sy geduld met my nie-akademiese bedrywighede. Dit was vir my 'n voorreg om saam met 'n akademikus en mens van hierdie gehalte te werk.

SOLI DEO GLORIA

SUMMARY

TITLE	:	The development of a mechanism for categorizing countermeasures in the field of computer security and linking it to countermeasure standards.
AUTHOR	:	Christiaan J. Bosch
SUPERVISOR	:	Prof. J.H.P. Eloff
DEGREE	:	M.Com.
DEPARTMENT	:	Computer Science
LANGUAGE	:	Afrikaans

SUMMARY

Although much research has been done on countermeasures in the field of information security, and an almost equal amount of work on defining standards for security countermeasures, there still seems to be an absence in literature regarding a clear linkage between countermeasures and standards, especially from a management point of view.

The identification and selection of countermeasures form part of most risk analysis approaches. Risk analysis packages compete for obtaining a maximum or at least comprehensive knowledge base of countermeasures. Identifying and selecting countermeasures from an organization specific rather than from a product point of view in this sea of alternatives present a problem. A holistic approach is required which will not only improve management's conceptual understanding of the issue, but will also enable a linkage of countermeasures to specific standards.

This dissertation proposes a framework for categorizing countermeasures and matching international and in-house standards with these countermeasures. The resulting set of specifications can then be compared with security facilities provided by available IT products in order to select a product which matches the organization's needs.

The study is management-orientated in the sense that IT products and countermeasures are considered from a cost-effective point of view. An informal, high level, non-technical approach is followed in the discussion of subjects, with the emphasis on completeness rather than detailed descriptions.

The following is a synopsis of the chapters presented in this study:

Chapter one serves as an introduction to the study by defining and discussing the concepts of computer security and risk analysis. The chapter concludes with a discussion of the goals of this study.

In chapter two the author discusses the two most important international security standards, which are the TCSEC (Orange Book) and the ITSEC (White Book). A summary of the specific requirements of each of these standards is presented in appendices A and B at the end of the study.

In chapter three the author presents a hierarchical framework for categorizing countermeasures to assist in the identification and selection of countermeasures. The different categories of countermeasures are then discussed in detail.

In chapter four the different categories of countermeasures defined in chapter three are linked to specific requirements. For every type of countermeasure a minimum level of proficiency to which the countermeasure must adhere, is defined. Where applicable, these requirements are defined with specific reference to the TCSEC and ITSEC standards.

In chapter five the results of the previous chapters are combined to define a methodology which can be used to compare the security requirements set by an organization for an IT product with the actual security facilities provided by a specific IT product.

The dissertation concludes with a brief discussion of the results of the study, as well as ideas initiated during this research project, which can form the basis of further research.

INHOUDSOPGAWE

DOELSTELLINGS EN OORSIG 1

HOOFSTUK 1 'N OORSIGTELIKE BESKOUING VAN REKENAARSEKERHEID EN RISIKO-ANALISE 3

1. REKENAARSEKERHEID 4
   1.1 Definisie 4
   1.2 'n Metodologie vir Rekenaarsekerheid 5

2. RISIKO-ANALISE 7
   2.1 Definisie 7
   2.2 Take in die Risiko-analise fase 9
   2.3 Risiko-analise tegnieke 10
   2.4 Kwantifisering van risiko 11
   2.5 Koste/voordele analise 14

3. PROBLEEMSTELLING 16

HOOFSTUK 2 HUIDIGE STANDAARDE VIR BEHEERMAATREëLS 18

1. INLEIDING 19

2. DIE ORANJE BOEK 20
   2.1 Sekerheidsvereistes 22
   2.2 Sekerheidsklasse 31
   2.3 Voorstellingsmeganisme 33
   2.4 Kritiek teen die Oranje Boek 39
   2.5 Die Rooi Boek 41

3. DIE WIT BOEK 43
   3.1 Funksionaliteit en Versekering 44
   3.2 Evalueringsklasse en -vlakke 45

3.3 Sekerheidsvereistes 48
3.4 Voorstellingsmeganisme 56

4. VERGELYKING VAN ORANJE BOEK EN WIT BOEK 62

HOOFSTUK 3 'N KATEGORISERINGSMEGANISME VIR BEHEERMAATREëLS .. 65

1. TOEPASSINGSEKERHEID MAATREëLS 70
1.1 Toepassing ontwikkelingskontroles 70
1.2 Toepassing sekerheidsmeganismes 73

2. LOGIESE SEKERHEID MAATREëLS 78
2.1 Stelselprogrammatuur 78
2.2 Apparatuur 88
2.3 Databasisse 91
2.4 Mikrorekenaars 101

3. VERSPREIDE STELSELS SEKERHEID MAATREëLS 106
3.1 Vertroulikheidsmaatreëls 107
3.2 Integriteitsmaatreëls 110
3.3 Nie-repudiëring 112
3.4 Sekerheidsbuitelyne 113
3.5 Toegangsbeheer 115
3.6 Verkeersvloei vertroulikheid 116
3.7 Identifikasie en verifikasie 117

4. FISIESE SEKERHEID MAATREëLS 118
4.1 Ligging 119
4.2 Konstruksie 119
4.3 Fisiese toegangsbeheer 120
4.4 Kragvoorsiening 122
4.5 Lugversorging 124
4.6 Brandbeskerming 124
4.7 Waterbeskerming 127
4.8 Veilige berging 127
4.9 Rugsteunaanlegte 128
4.10 Kommunikasielyn beskerming 130
4.11 Uitstralingsbeskerming 131

5. ADMINISTRATIEWE SEKERHEIDSMAATREëLS 132
5.1 Personeelbeleid 132
5.2 Sekerheidsbeleid 139
5.3 Organisatoriese verantwoordelikhede 140
5.4 Rampherstelbeplanning 143
5.5 Assuransie 146
5.6 Dokumentasie 147

6. GEVOLGTREKKING 150

HOOFSTUK 4 DEFINIëRING VAN 'N RAAMWERK WAARBINNE FUNKSIONALITEIT GEKOPPEL WORD MET STANDAARDE VIR BEHEERMAATREëLS 152

1. TOEPASSINGSEKERHEID MAATREëLS 161
1.1 Toepassing ontwikkelingskontroles 161
1.2 Toepassing sekerheidsmeganismes 162

2. LOGIESE SEKERHEID MAATREëLS 165
2.1 Stelselprogrammatuur 165
2.2 Apparatuur 168
2.3 Databasisse 171
2.4 Mikrorekenaars 174

3. VERSPREIDE STELSELS SEKERHEID MAATREëLS 175
3.1 Vertroulikheidsmaatreëls 175
3.2 Integriteitsmaatreëls 177
3.3 Nie-repudiëring 177
3.4 Sekerheidsbuitelyne 178
3.5 Toegangsbeheer 178
3.6 Verkeersvloei vertroulikheid 179
3.7 Identifikasie en verifikasie 179

4. FISIESE SEKERHEID MAATREëLS 180
4.1 Ligging 180
4.2 Konstruksie 180
4.3 Fisiese toegangsbeheer 181
4.4 Kragvoorsiening 181

4.5 Lugversorging 182
4.6 Brandbeskerming 182
4.7 Waterbeskerming 182
4.8 Veilige berging 183
4.9 Rugsteunaanlegte 183
4.10 Kommunikasielyn beskerming 184
4.11 Uitstralingsbeskerming 184

5. ADMINISTRATIEWE SEKERHEIDSMAATREëLS 185
5.1 Personeelbeleid 185
5.2 Sekerheidsbeleid 189
5.3 Organisatoriese verantwoordelikhede 190
5.4 Rampherstelbeplanning 192
5.5 Assuransie 193
5.6 Dokumentasie 194

6. GEVOLGTREKKING 196

HOOFSTUK 5 'N METODOLOGIE VIR DIE VERGELYKING VAN DIE SEKERHEIDSEIENSKAPPE VAN 'N IT PRODUK MET 'N ORGANISASIE SE VEREISTES 197

1. METODOLOGIE 198
1.1 Fase 1 : Bepaling van vereistes vir beheermaatreëls 200
1.2 Fase 2 : Bepaling van fasiliteite van IT produk 201
1.3 Fase 3 : Vergelyking van roosdiagramme 202

2. GEVOLGTREKKING 209

HOOFSTUK 6 SAMEVATTING 211

BYLAE A TCSEC 214

BYLAE B ITSEC 223

BYLAE C ARTIKEL 233

BIBLIOGRAFIE 249

LYS VAN FIGURE

Figuur 1.1 : Die verwantskap tussen verliese en die koste van beheermaatreëls 15

Figuur 2.1 : TCSEC Klasse 36

Figuur 2.2 : TCSEC Vereistes 36

Figuur 2.3 : Evaluering van produk A volgens TCSEC vereistes (deursigtig) 37

Figuur 2.4 : Evaluering van produk A volgens TCSEC vereistes. 38

Figuur 2.5 : Evaluering van produk A (opsommend) 38

Figuur 2.6 : ITSEC Klasse 59

Figuur 2.7 : ITSEC Vereistes 59

Figuur 2.8 : Evaluering van produk B volgens ITSEC vereistes (deursigtig) 60

Figuur 2.9 : Evaluering van produk B volgens ITSEC vereistes. 61

Figuur 3.1 : 'n Kategoriseringsmeganisme vir beheermaatreëls. 68

Figuur 3.2 : Toepassing ontwikkelingskontroles 70

Figuur 3.3 : Toepassing sekerheidsmeganismes 73

Figuur 3.4 : Stelselprogrammatuur 79

Figuur 3.5 : Apparatuur 88

Figuur 3.6 : Databasisse 92

Figuur 3.7 : Mikrorekenaars 102

Figuur 3.8 : Vertroulikheidsmaatreëls 107

Figuur 3.9 : Integriteitsmaatreëls 111

Figuur 3.10 : Nie-repudiëring 113

Figuur 3.11 : Sekerheidsbuitelyne 114

Figuur 3.12 : OSI-vlakke en sekerheidsbuitelyne 115

Figuur 3.13 : Toegangsbeheer 115

Figuur 3.14 : Verkeersvloei vertroulikheid 117

Figuur 3.15 : Identifikasie en verifikasie 118

Figuur 3.16 : Fisiese sekerheid maatreëls 118

Figuur 3.17 : Personeelbeleid 132

Figuur 3.18 : Sekerheidsbeleid 139

Figuur 3.19 : Organisatoriese verantwoordelikhede 141

Figuur 3.20 : Rampherstelbeplanning 143

Figuur 3.21 : Assuransie 146

Figuur 3.22 : Dokumentasie 148

Figuur 4.1 : Objek hergebruik binne die kategoriserings-meganisme 155

Figuur 4.2 : Formaat vir beskrywing van beheermaatreëls en vereistes 157

Figuur 4.3 : Koppeling van beheermaatreëls met internasionale en algemene standaarde 160

Figuur 5.1 : Metodologie vir vergelyking van organisasie-vereistes met fasiliteite van IT produk 199

Figuur 5.2 : Koppeling van ITSEC/TCSEC met beheermaatreëls .. 203

Figuur 5.3 : Koppeling van beheermaatreëls met TCSEC vereistes 204

Figuur 5.4 : Subversamelings 206

Figuur 5.5 : Raamwerk van roosdiagram met vereistes/fasiliteite 206

Figuur 5.6 : Roosdiagram A - Vereistes vir beheermaatreëls met sekerheidsklasse (deursigtig) 207

Figuur 5.7 : Roosdiagram B - IT produk fasiliteite met sekerheidsklasse (deursigtig) 207

Figuur 5.8 : Roosdiagram A - Vereistes vir beheermaatreëls met sekerheidsklasse 208

Figuur 5.9 : Roosdiagram B - IT produk fasiliteite met sekerheidsklasse 208

LYS VAN TABELLE

Tabel 2.1 : Evaluering van produk A 35

Tabel 2.2 : Evaluering van produk B - Funksionaliteit (Hiërargies) 57

Tabel 2.3 : Evaluering van produk B - Funksionaliteit (Nie-hiërargies) 57

Tabel 2.4 : Evaluering van produk B - Versekering 58

Tabel 3.1 : Eienskappe van beheermaatreëls 69

Tabel 3.2 : Sekerheidsaktiwiteite tydens die SDLC 74

Tabel 3.3 : Fasiliteite van 'n UPS stelsel 123

Tabel 3.4 : Opsomming van rugsteunalternatiewe 130

Tabel 4.1 : Wit Boek vereistes (Objek hergebruik) 156

Tabel 4.2 : Oranje Boek vereistes (Objek hergebruik) 157

Tabel 5.1 : Evaluering van produk volgens TCSEC vereistes .. 205

DOELSTELLINGS EN OORSIG

Hierdie studie word onderneem binne die veld van rekenaarsekerheid en fokus spesifiek op die identifisering en selektering van beheermaatreëls, met inagneming van internasionale standaarde, as deel van die risiko-analise fase in die implementering van rekenaarsekerheid binne 'n organisasie.

Die studie is bestuursgeoriënteerd in die sin dat IT produkte en beheermaatreëls vanuit 'n koste-effektiewe oogpunt beskou word. 'n Hoëvlak, informele, nie-tegniese benadering word gevolg in die hantering van onderwerpe, met die klem op volledigheid eerder as gedetailleerde beskrywings.

Die doelstellings van hierdie studie kan opsommend soos volg gestel word:

- Die bespreking en konseptuele voorstelling van die belangrikste internasionale standaarde wat gebruik word in die evaluering van rekenaarstelsels met die oog op sekerheid.

- Die ontwikkeling van 'n kategoriseringsmeganisme waarvolgens beheermaatreëls wat gebruik word om die graad van rekenaarsekerheid te verhoog, geïdentifiseer en geselekteer kan word.

- Die koppeling van die internasionale evalueringstandaarde met die kategoriseringsmeganisme ten einde 'n stel spesifikasies daar te stel waarmee beskikbare IT produkte vergelyk kan word aan die hand van die sekerheidsfasiliteite wat dit bied.

Die uiteensetting van die verhandeling is soos volg:

In hoofstuk 1 word die agtergrond van die studie geskets deur die konsepte rekenaarsekerheid en risiko-analise te definieer en kortliks te bespreek. Daarna word die fokus van hierdie studie in die vorm van 'n probleemstelling beskryf.

In hoofstuk 2 bespreek die skrywer die belangrikste twee internasionale sekerheidstandaarde, naamlik TCSEC (die Oranje Boek) en ITSEC (die Wit Boek) volledig. 'n Opsomming van die spesifieke vereistes van elk van hierdie standaarde word in bylaes A en B aan die einde van die studie gegee.

In hoofstuk 3 stel die skrywer 'n hiërargiese kategoriseringsmeganisme vir beheermaatreëls voor ten einde die identifisering en selektering van beheermaatreëls te vergemaklik. Die verskillende kategorieë beheermaatreëls word dan in detail bespreek.

In hoofstuk 4 word die verskillende kategorieë beheermaatreëls wat in hoofstuk 3 geïdentifiseer is, gekoppel met spesifieke vereistes. Vir elke beheermaatreël word daar 'n minimum vlak van werkverrigting gedefinieer waaraan die maatreël moet voldoen. Waar van toepassing, word hierdie vereistes gedefinieer met spesifieke verwysing na die ITSEC en TCSEC standaarde.

In hoofstuk 5 word die resultate van die vorige hoofstukke gekombineer deur 'n metodologie te beskryf wat gebruik kan word om die sekerheidsvereistes wat 'n organisasie vir 'n bepaalde inligtingstegnologie (IT) produk stel, te vergelyk met die sekerheidsfasiliteite wat die produk bied.

Die verhandeling word in hoofstuk 6 afgesluit met 'n opsomming van die resultate van die studie, en 'n bespreking van idees wat deur die skrywer in hierdie studie geïnisieer is wat as basis vir verdere studie kan dien.

HOOFSTUK 1

'N OORSIGTELIKE BESKOUING VAN REKENAARSEKERHEID EN RISIKO-ANALISE

Hierdie hoofstuk dien as inleiding tot die studie en skets die raamwerk waarbinne verdere hoofstukke geïnterpreteer moet word. Ten eerste word die konsep rekenaarsekerheid gedefinieer met spesifieke verwysing na 'n metodologie waarvolgens 'n organisasie rekenaarsekerheid behoort te implementeer. Tweedens word die risiko-analise fase, wat deel vorm van so 'n tipiese metodologie, bespreek.

Die hoofstuk word afgesluit met 'n probleemstelling waarin die fokus van die studie, naamlik die kategorisering van beheermaatreëls en die koppeling daarvan met internasionale standaarde, uiteengesit word.

1. REKENAARSEKERHEID

1.1 Definisie

Badenhorst [6] definieer **rekenaarsekerheid** as "die beskerming van 'n organisasie se rekenaarbates en die doeltreffendheid van die installasie om sodoende 'n betroubare en akkurate diens van hoë gehalte te lewer."

Rekenaarsekerheid verseker die vertroulikheid, integriteit en beskikbaarheid van die komponente van 'n rekenaarstelsel.[74]

- **Vertroulikheid** beteken dat 'n stelsel of spesifieke dele daarvan slegs vir gemagtigde partye toeganklik is.

- **Integriteit** beteken dat die stelselkomponente slegs deur gemagtigde partye gewysig kan word, en dus as akkuraat en volledig aanvaar kan word.

- **Beskikbaarheid** beteken dat die stelsel en sy komponente wel vir gemagtigde partye beskikbaar is wanneer hul dit benodig en in soverre dit deur die organisasie se behoeftes vereis word.

Die oorkoepelende begrip rekenaarsekerheid kan in twee kategorieë verdeel word, [6] nl.

- **Tegnologiese rekenaarsekerheid** - Bestaan uit **fisiese** rekenaarsekerheid wat die fisiese beskadiging van rekenaarstelselkomponente voorkom, en **logiese** rekenaarsekerheid wat gerig is op die beskerming van data en programme wat in die stelsel geberg of versend word.

- **Toepassingsrekenaarsekerheid** - Gerig op aspekte rakende die ontwikkeling en onderhoud van toepassingstelsels, met die doel om betroubare, maklik-onderhoubare programme daar te stel, met die nodige interne kontroles wat beheer uitoefen oor die gebruik daarvan.

Die hoofkomponente van rekenaarstelsels is **apparatuur, programmatuur, data** en **mense** [74]. Daar is hoofsaaklik vier tipes bedreigings vir die sekerheid van hierdie komponente van rekenaarstelsels, nl.

- **onderbreking** - 'n bate (stelsel of deel van 'n stelsel) raak verlore, onbeskikbaar of onbruikbaar;

- **onderskepping** - 'n ongemagtigde party verkry toegang tot 'n deel van 'n stelsel;

- **modifikasie** - 'n ongemagtigde party verkry nie net toegang tot 'n stelsel nie, maar verander ook die inhoud daarvan; en

- **fabrikasie** - objekte word deur 'n ongemagtigde party geskep en toegevoeg tot die stelsel.

Ten einde die impak van hierdie bedreigings op 'n organisasie se inligtingsbates te verminder, is dit noodsaaklik dat daar 'n stel **beheermaatreëls** geïmplementeer sal word. Hierdie beheermaatreëls moet dus op elkeen van die hoofkomponente van rekenaarstelsels (apparatuur, programmatuur, data en mense) toegepas word om ongemagtigde onderbreking, onderskepping, modifikasie of fabrikasie van enige deel van die inligtingstelsels te voorkom.

Bogenoemde beheermaatreëls kan deur die organisasie self ontwikkel word, of in die vorm van fisiese toerusting of as deel van programmatuurpakkette aangekoop word.

1.2 'n Metodologie vir Rekenaarsekerheid

Baie organisasies implementeer verskillende aspekte van rekenaarsekerheid op 'n stuksgewyse basis sonder dat dit deel van 'n breër strategie vorm. Badenhorst et al. [8] definieer 'n omvattende metodologie, naamlik die **RS-metodologie**, wat chronologiese fases en take in die lewenssiklus van rekenaar-

sekerheid in 'n organisasie stipuleer. Die voordeel van so 'n metodologie is dat dit die hele spektrum van rekenaarsekerheid dek, insluitende tegnologiese en toepassingsekerheid. Dit verskaf verder 'n meer gestruktureerde bestuurskema vir die beheer van kostes en skedules, en dit dra by tot effektiewe kommunikasie tussen gebruikers, ouditeure, topbestuur en rekenaarpersoneel.

Die metodologie bestaan uit **vyf fases**, nl.

- **Inisiëring** - 'n Spesiale taakgroep wat uit sleutelpersone in die organisasie bestaan, moet aangewys word. Hierdie groep het die verantwoordelikheid om die sekerheidsplan deur al die fases te bestuur. Topbestuur se bewustheid van en verbintenis tot rekenaarsekerheid moet in hierdie fase verseker word.

- **Rekenaarsekerheidsbeleid** - Topbestuur moet 'n korporatiewe sekerheidsbeleid, gebaseer op die organisasie se missie en doelstellings, ontwikkel wat die basis sal vorm vir toepaslike rekenaarsekerheidsmaatreëls.

- **Risiko-analise en projekdefinisie** - Rekenaarsekerheidsrisiko's en potensiële verliese moet gekwantifiseer word en koste-effektiewe beheermaatreëls moet geselekteer word.

- **Installering** - Hierdie fase dek alle tegnologiese aspekte van rekenaarsekerheid soos fisiese en logiese toegang en die installering van ander toepaslike beheermaatreëls.

- **Instandhouding** - Die ontwikkeling van beheermaatreëls in rekenaartoepassings moet geskied parallel met instandhoudingsprosedures soos oudit-funksies, opleiding en hersiening van die sekerheidsplan.

2. RISIKO-ANALISE

Die derde fase van die RS-metodologie, naamlik risiko-analise en projekdefinisie, vorm die agtergrond waarteen hierdie studie onderneem word.

2.1 Definisie

Bauknecht en Strauss [10] definieer risiko as "die moontlikheid van 'n negatiewe afwyking van die realiteit van die plan, die gevaar dat 'n beplande prestasie nie behaal kan word nie". Risiko spruit voort uit die kombinasie van die intrinsieke waarde van 'n bate en die effek wat die realisering van enige van 'n aantal bedreigings wat op die bate van toepassing is, kan hê [39]. Risiko verskil van **onsekerheid** in die sin dat die voorkoms van 'n gebeurtenis in die toekoms deur objektiewe of statistiese waarskynlikhede voorspel kan word, terwyl dit nie moontlik is met onsekerhede nie.

In risiko-analise raamwerke vir inligtingstelsels word dit algemeen erken dat risiko's veroorsaak word deur die impak van **bedreigings**, d.i. potensieel skadelike gebeurtenisse, op **bates**, d.i. die eienskappe van die inligtingstelsels self [39]. Fordyce [36] definieer 'n bate as 'n objek wat bydra tot die doelwitte van die organisasie en dus van waarde is vir die organisasie. Bates sluit in tasbare sowel as nietasbare items. Ten einde hierdie bates te beskerm teen bedreigings, is dit nodig om 'n stel **beheermaatreëls en -toestelle** daar te stel. Die hoofdoelwit van risiko-analise is dan ook om 'n voorlopige projekplan vir die implementering van sodanige beheermaatreëls op te stel [7].

Dit is noodsaaklik dat senior bestuur sal begryp dat data, inligting, stelsel- en toepassingsprogrammatuur, en rekenaarapparatuur krities belangrike bates van die organisasie is. Senior bestuur moet in staat wees om die finansiële implikasies wat enige verlies aan sekerheid op die organisasie kan hê, te besef ten einde die sekerheidsmaatreëls te ondersteun (finansieel en andersins). Dit is derhalwe noodsaaklik dat

die risiko erken en gekwantifiseer moet word en beheer kan word.

Risiko-analise bestaan hoofsaaklik uit twee onderafdelings, naamlik risikobepaling en risikobestuur [47]. **Risikobepaling** is die proses waardeur die blootstelling van 'n rekenaarstelsel aan verliese beraam word. Dit behels die identifikasie van bates wat beskerm moet word, bedreigings van toepassing op die bates, en inherente kwesbaarhede van die rekenaarstelsel. Deur **risikobestuur** word 'n stel beheermaatreëls geselekteer om die blootstelling van rekenaarstelsels te minimaliseer met inagneming van beskikbare hulpbronne en ander beperkings.

Boehm [12] beskryf vier moontlike maniere waarop risiko hanteer kan word. **Risiko-vermyding** fokus op die vermindering van risiko deur 'n afskaling of hersiening van die doelwitte wat nagestreef word. Deur **risiko-oordrag** word bronne van risiko oorgedra van een deel van 'n stelsel na 'n ander. 'n Derde opsie is **risiko-beheer**, wat behels dat die teenwoordigheid van 'n spesifieke risiko aanvaar word, en dat daar planne voorberei word om dit so goed moontlik te hanteer, asook gebeurlikheidsplanne sou die risiko realiseer. 'n Laaste algemene metode om risiko te verminder is deur soveel moontlik **inligting** oor beplande nuwe stelsels te genereer voor die stelsels aangekoop of geïmplementeer word. Hierdie laaste opsie kan ook voorafgaande tot die ander opsies uitgevoer word.

Voordele van 'n deeglike risiko-analise sluit in [74]:

- Dit verhoog die **bewustheid** van rekenaarsekerheid onder alle vlakke van bestuur, deurdat personeel betrek word by die proses.

- 'n Sistematiese ontleding stel die organisasie in staat om **inligtingbates** en geassosieerde **kwesbaarhede** tesame met

toepaslike **beheermaatreëls** te identifiseer.

- Dit verbeter die **basis van besluitneming** ten einde oortollige beheermaatreëls uit te skakel maar terselfdertyd effektiewe maatreëls vir ernstige bedreigings daar te stel.

- Dit bied 'n basis om uitgawes aan sekerheidsmaatreëls te regverdig teenoor **topbestuur**.

2.2 Take in die Risiko-analise fase

Binne die breër raamwerk van risiko-bepaling en risiko-bestuur kan 'n aantal spesifieke **take** in die risiko-analise fase geïdentifiseer word. Badenhorst et al. [7] beskryf hierdie take soos volg:

- Bepaal die **huidige rekenaaromgewing** in terme van apparatuur, programmatuur, data en mense.

- Identifiseer die **inligtingsbates** van die organisasie.

- Bepaal die **huidige vlak** of status van rekenaarsekerheid in die organisasie.

- Bepaal die potensiële **finansiële verliese** wat die organisasie kan ly as gevolg van 'n verlies van rekenaarsekerheid.

- Doen 'n **voorlopige risiko-analise** deur 'n realistiese evaluering van potensiële risiko's en geassosieerde beheermaatreëls ten einde die koste-effektiewe toepassing van beheermaatreëls te verseker.

- Bepaal **versekeringsalternatiewe** en identifiseer risiko's wat aanvaarbaar is vir die organisasie, met die goedkeuring van topbestuur.

- Herevalueer die **organisasie-spesifieke RS-metodologie** om te verseker dat alle relevante aspekte daarin aangespreek word.

- Doen 'n **koste-ontleding** van die implementering van beheermaatreëls, insluitende direkte en indirekte koste.

- Berei **bestuursinligting** voor ten einde goedkeuring van topbestuur te verkry om die sekerheidsplan te implementeer.

2.3 Risiko-analise tegnieke

In die literatuur word daar onderskei tussen kwantitatiewe en kwalitatiewe benaderings tot risiko-analise.

'n **Kwantitatiewe** risiko-analise druk risiko uit as numeries kwantifiseerbare parameters. Dit verskaf 'n raamwerk waarbinne ontleders die omvang van stelselrisiko's kan bepaal, die effektiwiteit van beheermaatreëls kan evalueer en uitgawes aan die rampherstelprogram kan regverdig en daarvoor begroot. Direkte geldelike verliese, die onvermoë van die stelsel om sy missie te vervul, 'n verlies van die vertroulikheid, beskikbaarheid of integriteit van data en 'n onderbreking in rekenaardiens moet o.a. ondersoek word. Elke spesifieke aanbeveling moet die produk wees van 'n noukeurige ontleding van die gekwantifiseerde risiko en die koste van beskerming teenoor die verwagte voordele [14]. In die bepaling van waarskynlikhede is dit wel soms nodig om subjektiewe "grade van geloof" te gebruik. Dit is egter onvermydelik en indien dit goed gemotiveer word en realisties is, aanvaarbaar vir risiko-analise. [39] [37]

'n **Kwalitatiewe** risiko-analise daarenteen, verwys na benaderde beoordelingskemas met verbale kwalifiseerders soos "hoog", "medium" of "laag". Hoewel dit eenvoudiger is, kan dit terselfdertyd misleidend en onvoldoende wees aangesien die kwalifiseerders hoogs subjektief en relatief tot die waarne-

mer se verwysingsraamwerk is [39]. Indien die risiko-analise kwalitatief gedoen word, moet kwalifiseerders of beskrywers aan objektiewe skale gekoppel kan word ten einde 'n voldoende basis aan senior bestuur te bied om die impak van risiko's te evalueer in die korporatiewe omgewing.

'n Ander belangrike verskil tussen die twee algemene benaderings is die hoeveelheid **tyd en koste** wat benodig word om die analise te doen. Die kwantitatiewe benadering vereis dat die stelsel of organisasie deeglik bestudeer word ten einde bedreigings en kwesbaarhede te identifiseer, waarskynlikhede te bereken en kostes te bepaal. In baie gevalle gaan dit gepaard met uitgebreide opnames onder 'n verskeidenheid van mense in die organisasie. Die kwalitatiewe benadering, daarenteen, benodig aansienlik minder mense en tyd. [37]

2.4 Kwantifisering van risiko

Boyer [14] identifiseer twee verwante stelle ekonomiese aangeleenthede wat deur die risiko-analise aangespreek moet word. Die eerste stel, wat primêr deur die **inligtingstelselsafdeling** aangespreek moet word, handel hoofsaaklik oor die koste om rekenaarvermoë te vervang en die integriteit, sekerheid of beskikbaarheid van die stelsel te herstel. Die tweede stel ekonomiese aangeleenthede is meer vaag en betrek die **inligtingstelselsgebruikers** - dit gaan oor die koste verbonde aan die nie-beskikbaarheid van die rekenaardiens. Basiese gegewens kan egter verkry word deur die werklike inkomste wat verloor sal word te spesifiseer, of 'n koste af te lei wat gebaseer is op die verlies van operasionele beheer.

Boyer wys ook op 'n **derde stel**, meer abstrakte, ekonomiese aangeleenthede wat verreikende gevolge kan hê en wat nie binne die uitsluitlike domein van die inligtingstelselsafdeling of die gebruikers val nie. Die eerste is 'n onderbreking in 'n **groot aantal prosesse** a.g.v. die geïntegreerdheid van en die interafhanklikheid tussen rekenaartoepassings en ander

stelsels in die organisasie. Die tweede is 'n verlies van **markaandeel** a.g.v. onvermoë om effektiewe diens aan klante te lewer. Derdens is die verlies van **data en programmatuur**, iets wat nie as bates op 'n organisasie se balansstaat aangedui word nie, maar wat tog noodsaaklik is vir die realisering van inkomste. Hierdie drie aangeleenthede word dikwels oor die hoof gesien juis a.g.v. die moeilike kwantifiseerbaarheid daarvan, terwyl dit 'n wesenlike deel van die totale verlies kan uitmaak.

Benewens die kwantifisering van die impak van 'n ramp op die organisasie, moet die Randwaarde van potensiële voordele ook in die voorlegging ingesluit word. Die risiko-analise moet telkens vir elke objek of besigheidsfunksie aandui wat die **koste van beskerming** is vergeleke met die **potensiële verlies** in die afwesigheid van beskermende maatreëls.

'n Algemene metode om risiko te kwantifiseer is om die **waarskynlikheid** van elk van die potensiële bedreigings op die rekenaaromgewing te beraam en elke waarskynlikheid dan te kombineer met die **potensiële verlies** wat dit in elke departement van die organisasie op tasbare en nie-tasbare bates tot gevolg sal hê om 'n kwantitatiewe maatstaf van die jaarlikse risiko in geldterme te verskaf.

Fordyce [36] onderskei tussen twee begrippe, naamlik "Annual Frequency Estimate" (AFE) en "Annual Loss Expectancy" (ALE). **AFE** word bereken deur te bepaal hoeveel keer per jaar 'n verlies waarskynlik sal voorkom, en deur watter bedreiging. Vir elke geïdentifiseerde bedreiging/kwesbaarheid paar moet daar 'n AFE bereken word. **ALE** stel die bedrag van verlies in die waarde van 'n bate voor indien daardie verlies oor 'n aantal jaar geamortiseer word. Sodoende kan verliese wat ongereeld behoort voor te kom vergelyk word met algemene verliese, en kan koste-effektiewe beheermaatreëls ontwikkel word. [43]

Boehm [12] beskryf twee konsepte wat onderliggend is aan kwantitatiewe risiko-analise, naamlik risiko-impak en die risiko-vermindering hefboom.

Risiko-impak word voorgestel deur die formule

$$RI = W(OR) * V(OR)$$

waar W(OR) die waarskynlikheid van 'n onbevredigende resultaat is, en
V(OR) die verlies in die geval van 'n onbevredigende resultaat.

Deur die risiko-impak syfer met W(OR) as die waarskynlikheid van die realisering van 'n spesifieke risiko per jaar te bereken, stel RI die ALE ("Annual Loss Expectancy") voor.

Die **Risiko-vermindering hefboom** word voorgestel deur die formule

$$RVH = (RI1 - RI2)/RVK$$

waar RI1 die risiko voor die risikoverminderingspoging is;
RI2 die risiko na die risikoverminderingspoging is; en
RVK die koste verbonde aan risikovermindering is.

RVH is dus 'n maatstaf van die relatiewe koste-voordeel van verskillende risikoverminderingsaktiwiteite.

Deur van die risiko-impak waarde gebruik te maak, kan risiko's in **prioriteitsvolgorde** verdeel word. Deur verder die risiko-vermindering hefboom te gebruik, kan 'n aanduiding verkry word welke van die risiko-verminderingsopsies in paragraaf 3.1 bespreek, die mees wenslike is.

2.5 Koste/voordele analise

'n Koste/voordele analise binne die konteks van risiko-analise behels die vergelyking van die **gekwantifiseerde risiko** (of ALE) met die **koste van beheermaatreëls** om die risiko te verminder, oor te dra of te vermy.

'n Eenvoudige koste/voordele analise kan deur die volgende voorbeeld geïllustreer word.

Gestel 'n klerevervaardiger maak gebruik van 'n debiteure-stelsel om klante te faktureer. 'n Verlies in die integriteit van die data op die stelsel kan potensieel lei tot 'n geraamde verlies van R500 000 per jaar. Daar is 'n 0.5% waarskynlikheid dat die data-integriteit op 'n kwaadwillige wyse aangetas kan word.

Die AFE is dus 0.005, en die ALE word bereken op

R500 000 * 0.005 = R2 500

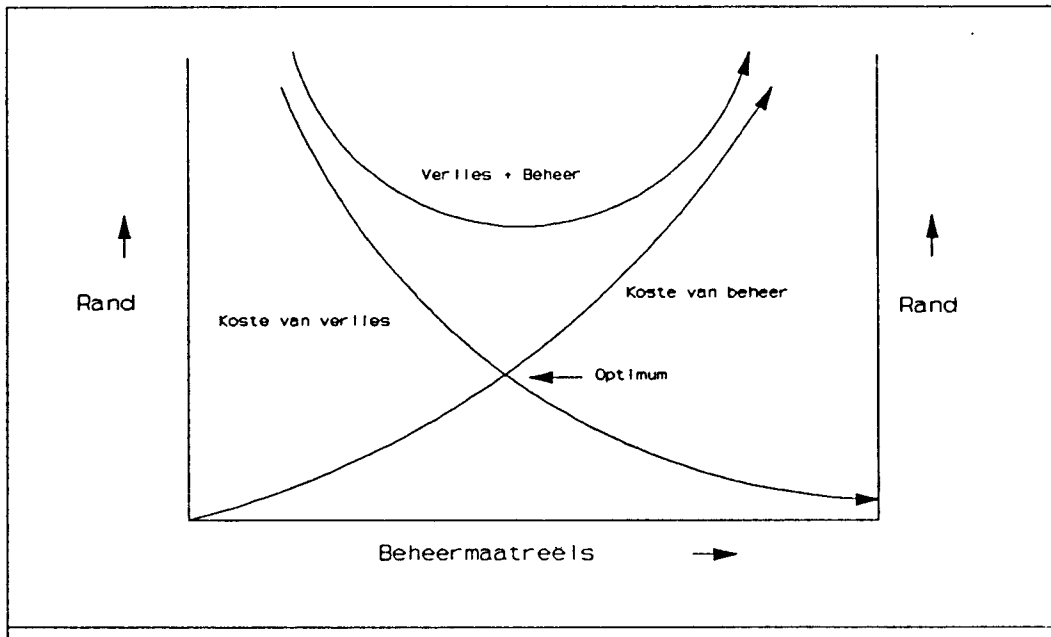
Gestel verder dat die koste van beheermaatreëls om die bedreiging te verminder R1 000 is en dat sodanige beheermaat-reëls 80% effektief is. Indien die beheermaatreëls geïmple-menteer word, sal dit 'n afname in verlies meebring van

R2 500 * 0.8 = R2 000

Die netto besparing wat teweeggebring word, is dus R1 000 (R2 000 - R1 000), en die beheermaatreëls sal dus koste-effektief wees.

Bogenoemde voorbeeld is eenvoudig in die sin dat dit aanvaar dat daar vir 'n elke spesifieke bedreiging een beheermaatreël is, en dat die koste-impak van beide maklik kwantifiseerbaar is. In die praktyk is dit egter nie die geval nie, en is die totale **sekerheidskostekurwe** die kombinasie van die koste van sekerheid, verliese, versekering en verwante koste. [97]

Fig. 1.1 beskryf die verwantskap tussen verliese en goedgeselekteerde beheermaatreëls. Indien die mees effektiewe beheermaatreëls eerste geïmplementeer word, sal die verliese wat daardeur verplaas word baie groter wees as die koste van die beheermaatreëls. Soos wat meerdere beheermaatreëls egter toegepas word, vernou die gaping tussen die koste van beheermaatreëls en die verliese, totdat 'n punt bereik word waar die som van beheerkostes en verliese 'n minimum is. Anders gestel, die punt op die horisontale as waar die koste van beheermaatreëls gelyk is aan die koste van verliese, verteenwoordig die optimum punt vir die **graad van rekenaarsekerheid.** [6] [25]



Figuur 1.1 Die verwantskap tussen verliese en die koste van beheermaatreëls

In werklikheid is die kurwe nie so glad as wat deur die figuur voorgestel word nie, maar die belangrike punt is dat beheermaatreëls **interafhanklik** is. Een beheermaatreël kan in sommige gevalle die afname in meerdere bedreigings tot gevolg hê, terwyl 'n beheermaatreël in ander gevalle ook nutteloos kan wees in die afwesigheid van ander spesifieke beheermaatreëls.

3. PROBLEEMSTELLING

Soos blyk uit die take in die risiko-analise fase soos deur Badenhorst beskryf, vorm die identifikasie en seleksie van beheermaatreëls 'n integrale komponent van die risiko-analise proses.

Bestaande risiko-analise pakkette fokus egter daarop om 'n maksimum hoeveelheid beheermaatreëls in 'n kennisbasis te versamel, met 'n gemiddeld van ongeveer 1000 maatreëls per benadering (bv. die CRAMM risiko-analise pakket [21] [20]). Die identifikasie van beheermaatreëls word hierdeur bemoeilik, aangesien die verband tussen al die verskillende beheermaatreëls meestal nie konseptueel voorgestel word nie. Ten einde hierdie identifikasieproses te vergemaklik, is dit noodsaaklik om oor 'n meganisme te beskik waardeur beheermaatreëls gekategoriseer kan word volgens die funksionaliteit daarvan. So 'n meganisme moet alle beskikbare beheermaatreëls op verskillende vlakke van detail voorstel, sodat beide bestuur en stelselspersoneel nut daaruit kan put.

'n Belangrike aspek wat in ag geneem moet word by die seleksie van beheermaatreëls, is die effektiwiteit daarvan. Hierdie effektiwiteit word gemeet aan hoofsaaklik twee faktore, naamlik die koste van beheermaatreëls en die vlak van werkverrigting wat dit bied. Ten einde die vlak van werkverrigting te bepaal, moet die beheermaatreëls aan sekere standaarde gemeet word.

Verskillende internasionale standaarde is reeds vir hierdie doel gedefinieer. Die belangrikste hiervan is die Trusted Computer Security Evaluation Criteria (TCSEC) en die gepaardgaande dokumente in die "Rainbow Series" [70] [78], die Information Technology Security Evaluation Criteria (ITSEC) [51], en die sekerheidsaddendum tot die Open Systems Interconnection (OSI) Netwerk Argitektuur [16]. Benewens internasionale standaarde, kan interne organisasie-spesifieke standaarde gedefinieer word om 'n bepaalde organisasie se

behoeftes te beskryf.

Alhoewel 'n paar IT produkte ontwerp en getoets is met die oog op hierdie internasionale standaarde, was daar baie min pogings om hierdie standaarde direk aan spesifieke beheermaatreëls te koppel. Die algemene benadering wat gevolg word, is een waar verskaffers produkte ontwikkel met beheermaatreëls wat bepaalde fasiliteite bied. Die produkte in geheel word dan geëvalueer volgens hierdie standaarde.

Wat egter nodig is, is 'n benadering waar individuele beheermaatreëls geïdentifiseer en geselekteer word volgens 'n organisasie se spesifieke behoeftes en met inagneming van internasionale en/of organisasie-spesifieke standaarde. Sodoende kan die organisasie 'n stel spesifikasies saamstel waaraan alle produkte wat oorweeg word, gemeet kan word ten einde te bepaal of die produkte effektief binne die organisasie geïmplementeer kan word.

Hierdie studie benader dié probleem deur die volgende aspekte te bespreek:

- 'n Skema waarvolgens die sekerheidsfasiliteite wat 'n IT produk bied, konseptueel voorgestel kan word (Hoofstuk 2).

- 'n Kategoriseringsmeganisme waarvolgens 'n organisasie beheermaatreëls kan identifiseer en selekteer om aan sy spesifieke behoeftes te voldoen (Hoofstuk 3).

- 'n Meganisme waardeur spesifieke vereistes met hierdie beheermaatreëls gekoppel kan word deur gebruikmaking van internasionale en/of organisasie-spesifieke standaarde (Hoofstuk 4).

- 'n Metodologie waardeur 'n spesifieke IT produk visueel vergelyk kan word met die vereistes wat 'n bepaalde organisasie vir 'n bepaalde produk stel (Hoofstuk 5).

HOOFSTUK 2

HUIDIGE STANDAARDE VIR BEHEERMAATREëLS

In hierdie hoofstuk word daar breedvoerig gekyk na die twee belangrikste kriteriastelle, oftewel standaarde, wat tans vereistes vir beheermaatreëls in veilige stelsels spesifiseer. Vir elkeen van hierdie standaarde stel die skrywer 'n voorstellingsmeganisme voor wat gebruik kan word om die evaluering van 'n produk volgens die betrokke standaard konseptueel voor te stel.

Ten eerste word 'n paar belangrike konsepte wat van toepassing is op hierdie gebied, bespreek. Daarna word die sg. Oranje Boek bespreek met 'n ontleding van die verskillende vereistes en klasse. 'n Soortgelyke ontleding van die vereistes en klasse van die sg. Wit Boek word ook gemaak. Die hoofstuk word afgesluit met 'n vergelyking van die twee standaarde.

1. INLEIDING

Ten einde 'n rekenaarstelsel as 'n veilige ("secure") stelsel te kan evalueer, is dit noodsaaklik dat vaste, universeel-toepasbare kriteria daargestel word. Die sukses van sodanige kriteria kan gemeet word aan die mate waarin dit sekerheids-eienskappe volledig beskryf en waarin die eienskappe geëvalu-eer kan word relatief tot die kriteria.

Die meeste evalueringskriteria kan in twee kategorieë onderverdeel word, naamlik funksionaliteit en versekering. **Funksionaliteit** verwys na die fasiliteite en reëls waardeur sekerheidsdienste aan gebruikers verskaf word. Funksionali-teit is relatief maklik meetbaar en verskille in funksionali-teit is maklik sigbaar aangesien dit manifesteer in meganis-mes wat die gebruiker se aksies kontroleer, en waarmee die gebruiker op direkte of indirekte wyse in aanraking is. [70] [78]

Versekering is die vertroue wat in 'n stelsel geplaas kan word, en die betroubaarheid waarmee die stelsel ontwikkel, getoets, gedokumenteer, onderhou en afgelewer word. 'n Punt wat die graad van versekering beskryf is dus 'n uitdrukking van die evalueerder se mate van vertroue in die effektiwiteit waarmee die sekerheidsfunksionaliteit geïmplementeer is. Versekering word nie deur enige sigbare meganismes voorgestel nie, en kan dus moeiliker wees om te evalueer. [70] [78]

Daar is in werklikheid twee fases in versekeringsevaluering, naamlik evaluering van die ontwerp en evaluering van imple-mentering. **Ontwerp evaluering** is gerig daarop om te verseker dat 'n gegewe stelselontwerp werklik die funksionaliteit bied wat dit veronderstel is om te doen, en dat dit nie bloot voorkom asof die stelsel hierdie veronderstelde funksionali-teit bied nie. Deur ontwerp evaluering word ook gepoog om te verseker dat 'n fundamentele ontwerpsfout nie die stelsel se effektiwiteit in 'n latere stadium kan belemmer nie. In die ontwerp evaluering word daar dus gefokus op die **korrektheid**

van die stelsel uit die oogpunt van die konstruksie daarvan. [70] [51]

Implementering evaluering is gerig daarop om te bepaal of die sekerheidsfunksies en meganismes wat deur die stelsel verskaf word, werklik aan die sekerheidsbehoeftes van 'n spesifieke omgewing voldoen. Hierdie proses kan voor of na die installering van die stelsel uitgevoer word. Implementering evaluering fokus dus op die **effektiwiteit** van die stelsel. [70] [51]

Vir die doeleindes van hierdie studie word 'n **standaard** gedefinieer as die versameling **vereistes** wat 'n minimum vlak van werkverrigting beskryf waaraan die beheermaatreëls wat 'n IT produk bied, moet voldoen.

Die twee vernaamste internasionale standaarde wat tans vir die evaluering van die sekerheidseienskappe van stelsels gebruik word, is die Oranje Boek in die V.S.A. en die Wit Boek in Europa.

2. DIE ORANJE BOEK

Die Department of Defense Computer Security Center (CSC) is in 1981 in die V.S.A. gestig met o.a. die volgende doelwitte [78]:

- Om die algemene beskikbaarheid van veilige rekenaarstelsels aan te moedig.

- Om die tegniese sekerheidseienskappe van stelsels in die industrie en regeringsafdelings te evalueer.

- Om tegniese sekerheidskriteria vir die evaluering van rekenaarstelsels te ontwikkel.

- Om navorsing in rekenaar- en netwerksekerheidstegnologie te doen en te borg.

Voortspruitend uit hierdie doelwitte het die CSC die Department of Defense **Trusted Computer System Evaluation Criteria (TCSEC)** in Augustus 1983 gepubliseer. TCSEC het algemeen bekend geraak as die "Oranje Boek" vanweë die kleur van die boek se omslag. Die verantwoordelikhede van die CSC is in 1985 uitgebrei om alle federale agentskappe in te sluit en die sentrum is herdoop tot die National Computer Security Center (NCSC). Terselfdertyd is die Oranje Boek hersien en heruitgereik. [78]

Die Oranje Boek beskryf evalueringskriteria wat gebruik word om die mate van vertroue wat in 'n spesifieke rekenaarstelsel geplaas kan word, te bepaal. Dit stel die koper of gebruiker van 'n produk in staat om die presiese vlak van sekerheid nodig vir 'n spesifieke stelsel, toepassing of omgewing te bepaal en 'n gegewe produk daarteen te vergelyk. Die Oranje Boek definieer vier breë hiërargiese afdelings of vlakke van beskerming - D, C, B en A, in volgorde van verhoogde sekerheid. Binne elke afdeling definieer die Oranje Boek een of meer klasse, wat elk deur spesifieke vereistes beskryf word waaraan 'n stelsel moet voldoen om 'n gradering in daardie klas te verkry. Sommige afdelings het slegs 'n enkele klas, terwyl ander twee of meer het.

Deur die Oranje Boek se kriteria te gebruik, evalueer die NCSC produkte wat deur verskaffers ingedien word om op 'n sekere vlak van vertroue gesertifiseer te word. Produkte wat suksesvol geëvalueer word deur die NCSC se Trusted Products Evaluation Program (TPEP) word op die **Evaluated Products List (EPL)** geplaas. [70] [78]

Die NCSC het 'n aantal boeke gepubliseer bykomend tot die Oranje Boek ten einde gespesialiseerde, ingewikkelde areas aan te spreek. Hierdie publikasies staan gesamentlik bekend as die **Reënboog Reeks** ("Rainbow Series"), aangesien elke boek 'n ander omslagkleur het.

Die belangrikste van hierdie addisionele publikasies is sekerlik die **Trusted Network Interface (TNI)** oftewel die "Rooi Boek", wat die kriteria wat in die Oranje Boek vir netwerke en netwerkkomponente beskryf word, interpreteer. Hierdie boek identifiseer sekerheidseienskappe wat nie in die Oranje Boek genoem word nie maar wat wel op netwerke van toepassing is, en dit beskryf hoe hierdie eienskappe in die gegradeerde klassifikasie van stelsels in die Oranje Boek inpas. [78]

'n Ander belangrike publikasie in die Reënboog Reeks is die Trusted Database Management System Interpretation (TDI) wat die Oranje Boek se vereistes vir Database Management Systems (DBMS) produkte interpreteer. [78]

2.1 Sekerheidsvereistes

Twee konsepte wat deur die Oranje Boek gebruik word en wat verduideliking verdien, is 'n "Trusted system" en 'n "Trusted Computing Base". 'n "**Trusted system**" word gedefinieer as:

> "...a system that employs sufficient hardware and software integrity measures to allow its use to simultaneously process a range of sensitive unclassified or classified information for a diverse set of users without violating access privileges." Alhoewel 'n "trusted system" tegnies verskil van 'n "secure system", sal die vertaling "**veilige stelsel**" vir die res van die bespreking gebruik word.

'n "**Trusted Computing Base**" (TCB) verwys na die meganismes wat sekerheid in 'n stelsel toepas. Die Oranje Boek beskryf die TCB as:

> "The totality of protection mechanisms within a computer system - including hardware, firmware, and software - the combination of which is responsible for enforcing a security policy."

Die Oranje Boek definieer vier breë hiërargiese afdelings van sekerheidsbeskerming. Die afdelings, in stygende volgorde van vertroue, is:

D Minimum sekerheid
C Diskresionêre beskerming
B Verpligte beskerming
A Geverifieerde beskerming

Elke afdeling bestaan uit een of meer genommerde klasse, met groter nommers wat 'n hoër graad van sekerheid aandui. Elke klas word gedefinieer deur 'n spesifieke stel kriteria waaraan 'n stelsel moet voldoen om 'n gradering in daardie klas te verkry. Die kriteria val in vier algemene kategorieë, naamlik **sekerheidsbeleid, aanspreeklikheid, versekering** en **dokumentasie**. Hierdie vier kategorieë word volledig in [78] bespreek. Die volgende is slegs 'n opsomming daarvan:

2.1.1 Sekerheidsbeleid Vereistes

'n Sekerheidsbeleid is die stel reëls en gebruike wat bepaal hoe 'n organisasie sensitiewe inligting bestuur, beskerm en versprei. Die Oranje Boek beskryf die volgende vereistes vir 'n sekerheidsbeleid:

Diskresionêre Toegangsbeheer
Diskresionêre toegangsbeheer is 'n metode om toegang tot lêers en ander stelselobjekte te beperk gebaseer op die identiteit van gebruikers en/of die groepe waartoe hulle behoort. Deur diskresionêre toegangsbeheer kan die gebruiker self sy lêers beskerm deur te spesifiseer wie toegang daartoe mag verkry.

Objek Hergebruik
Objek hergebruik vereistes beskerm lêers, geheue, en ander objekte in 'n veilige stelsel teen onwillekeurige toegang deur gebruikers wat nie gemagtig is om toegang daartoe te verkry nie. 'n Stelsel se gewone toegangsbeheereienskappe

bepaal wie toegang tot spesifieke objekte het. Objek hergebruik vereistes bepaal wat met hierdie objekte gebeur wanneer dit hertoegeken word.

Etikette

Die Oranje Boek vereis dat elke subjek en stoorobjek 'n geassosieerde sensitiwiteitsetiket het. 'n Gebruiker se sensitiwiteitsetiket spesifiseer die vlak van vertroue wat met die gebruiker geassosieer word, terwyl 'n lêer se sensitiwiteitsetiket die vlak van vertroue wat 'n gebruiker moet hê om toegang tot die lêer te verkry, spesifiseer.

Etiketintegriteit

Hierdie vereiste verseker dat die sensitiwiteitsetikette wat met subjekte en objekte geassosieer word, akkurate voorstellings is van die sekerheidsvlakke van hierdie subjekte en objekte.

Uitvoer van geëtiketteerde inligting

'n Veilige stelsel moet verseker dat wanneer inligting deur die stelsel geskryf word, die inligting steeds deur beskermingsmeganismes beveilig word. Die Oranje Boek onderskei tussen twee tipes uitvoertoestelle, nl. multivlak en enkelvlak. 'n **Multivlak** uitvoertoestel of kommunikasiekanaal is een waarheen inligting op verskillende vlakke van sensitiwiteit geskryf kan word, bv. magnetiese skywe. Wanneer inligting na so 'n toestel toe geskryf word, moet die stelsel 'n manier hê om 'n sekerheidsvlak daarmee te assosieer. 'n **Enkelvlak** uitvoertoestel of kommunikasiekanaal is een waarheen inligting slegs op een spesifieke sensitiwiteitsvlak geskryf kan word, bv. drukkers en terminale. Die spesifieke sensitiwiteitsvlak is gewoonlik afhanklik van die fisiese ligging van die toestel, en uitvoer na enkelvlak toestelle hoef nie geëtiketteer te word met die sekerheidsvlak van die inligting nie. Die Oranje Boek vereistes vir **menslik-leesbare** uitvoer sluit in menslik-leesbare sensitiwiteitsetikette aan die begin en einde van elke uitvoerstuk.

Subjek Sensitiwiteitsetikette
Die doel van subjek sensitiwiteitsetikette is dat die gebruiker altyd sal weet op welke sekerheidsvlak hy werk. Veilige stelsels vertoon tipies die gebruiker se klaring as hy aanteken, en hervertoon dit wanneer die sekerheidsvlak verander.

Toestel Etikette
Toestel etikette word gebruik om die laagste en hoogste vlak van inligting wat aan 'n toestel gestuur kan word, te spesifiseer ten einde beperkings van die fisiese omgewing waar die toestel geleë is, in ag te neem.

Verpligte Toegangsbeheer
Verpligte toegangsbeheer plaas alle besluite oor toegang tot objekte onder beheer van die stelsel, in teenstelling met diskresionêre toegangsbeheer waar die gebruiker hierdie besluite moet neem.

2.1.2 Aanspreeklikheidsvereistes

Aanspreeklikheid beteken dat die stelsel in staat is om alle gebruikers te identifiseer, te bepaal of gebruikers gemagtigde toegang tot inligting verkry en rekord te hou van alle sekerheidsverwante aksies wat gebruikers in die stelsel neem. Die spesifieke aanspreeklikheidsvereistes van die Oranje Boek is:

Identifikasie en Verifikasie
Hierdie proses vereis dat 'n gebruiker homself moet identifiseer alvorens hy enige werk verrig wat interaksie met die TCB vereis. Die identifikasie geskied tipies deur 'n identifiseerder met 'n geassosieerde wagwoord in te sleutel.

Veilige Pad
'n Veilige pad verskaf 'n onfeilbare weg waardeur 'n gebruiker direk met die TCB kan kommunikeer sonder dat dit nodig is om deur onveilige toepassings en vlakke in die bedryfstelsels

te werk. 'n Veilige pad is die ander sy van die identifikasie en verifikasie vereiste, aangesien dit aan die gebruiker die versekering gee dat hy met 'n veilige stelsel werk.

Oudit

Oudit behels die vaslegging, ondersoek en hersien van sekerheidsverwante aktiwiteite in 'n veilige stelsel. 'n Sekerheidsverwante aktiwiteit verwys na enige aktiwiteit wat verband hou met 'n subjek se toegang tot 'n objek. Die Oranje Boek vereis selektiewe versameling en reduksie hulpmiddels vir oudit wat die stelseladministrateur in staat stel om bv. slegs een gebruiker se aktiwiteite te monitor op 'n spesifieke deel van die stelsel.

2.1.3 Versekeringsvereistes

Versekering is 'n waarborg dat die sekerheidsbeleid van 'n veilige stelsel korrek geïmplementeer is en dat die stelsel se sekerheidseienskappe die sekerheidsbeleid korrek uitvoer. Die Oranje Boek onderskei tussen **operasionele versekering** en **lewenssiklus versekering**.

(i) Operasionele Versekering

Operasionele versekering is gerig daarop om te verseker dat die argitektuur van 'n veilige stelsel en die spesifieke implementering daarvan die stelselsekerheidsbeleid toepas. Die volgende operasionele versekering vereistes word deur die Oranje Boek gespesifiseer:

Stelselargitektuur

Die stelselargitektuur vereiste handel oor die manier waarop die stelsel ontwerp is om sekerheid moontlik, en selfs onvermybaar, te maak. Alhoewel alle stelsels nie noodwendig met die oog op sekerheid ontwerp word nie, moet hulle suiwer beginsels van apparatuur en bedryfstelsel ontwerp ondersteun, en ook die vermoë hê om spesifieke sekerheidseienskappe wat later tot die stelsel bygevoeg kan word, te kan ondersteun.

In die VAX/VMS bedryfstelsel onderhou die TCB byvoorbeeld 'n domein vir sy eie uitvoering wat hom beskerm teen inmenging. Die geheue bestuurstelsel beskerm die bladsye van die stelselgeheue teen hergebruik. Bykomend daartoe word die ouditspoor in 'n beskermde area onderhou met alarms wat pogings om die inhoud daarvan te wysig of uit te wis, opspoor. [19]

Stelselintegriteit

Die Oranje Boek vereis dat apparatuur en programmatuur eienskappe verskaf moet word om periodiek die korrekte werking van die apparatuur en firmatuur elemente van die TCB te toets. Tipies kan integriteitstoetse vir apparatuur en firmatuur komponente (bv. sentrale verwerkingseenheid, geheue en kontroleerders) gedoen word elke keer wanneer die stelsel aangeskakel word. Slegs indien al die toetse suksesvol is, word die stelsel in bedryf gestel. [78]

Koverte Kanaal Ontleding

'n Koverte kanaal is 'n inligtingspad wat nie normaalweg deur die stelsel gebruik word nie en daarom nie deur die stelsel se normale sekerheidsmeganismes beskerm word nie. Benewens identifikasie van koverte kanale, vereis die Oranje Boek ook dat die omvang van inligting wat hierdie kanale dra, bepaal moet word. Die Oranje Boek gebruik die konsep "bandwydte" om koverte kanale te kwantifiseer, d.i. die tempo waarteen 'n koverte kanaal inligting kan oordra. Daar is twee tipes koverte kanale, naamlik stoorkanale en tydskanale.

Koverte stoorkanale dra inligting oor deur klein veranderings in data of selfs die teenwoordigheid van die data self. 'n Programmeerder kan byvoorbeeld 'n roetine in 'n personeel-stelsel plaas wat, indien die salaris van 'n werknemer 'n bepaalde bedrag oorskry, 'n punt agter sy naam plaas. In netwerke kan 'n inluisteraar byvoorbeeld agterkom watter nodes dikwels met mekaar kommunikeer deur die hoeveelheid boodskappe wat tussen die nodes gestuur word, te monitor.

Koverte tydskanale dra inligting oor deur die tyd te meet wat dit vir 'n bepaalde prosedure of gebeurtenis neem om te voltooi, die persentasie SVE tyd bestee, of die tyd wat verloop tussen gebeurtenisse.

Veilige Fasiliteit Bestuur

Veilige fasiliteit bestuur ("trusted facility management") is die aanwysing van 'n spesifieke individu of individue om die sekerheidsverwante funksies van die stelsel te administreer. Twee konsepte wat sentraal is in veilige fasiliteit bestuur, is die volgende:

- Minste voorreg ("least privilege") wat beteken dat die gebruikers van die stelsel die mins moontlike aantal voorregte vir die kortste moontlike tyd moet hê wat nodig is om hul werk te doen. Selfs al het 'n bestuurder bv. "hoogs geheim" sekerheidsklaring vir strategiese projekte, beteken dit nie hy mag toegang hê tot alle "hoogs geheime" data, bv. salarisse van ander bestuurders nie.

- Verdeling van pligte, ("seperation of duties") wat daarop gerig is om sekerheidsverwante take eerder aan verskillende individue toe te wys as om al die beheer in een persoon te sentreer. In hoogs veilige stelsels is daar tot drie afsonderlike administratiewe funksies wat verantwoordelik is vir die dag-tot-dag bedryf van die stelsel, nl. die stelseladministrateur, die sekerheidsadministrateur en 'n operateur.

Veilige Herstel

Veilige herstel ("trusted recovery") verseker dat daar nie 'n breuk in sekerheid is wanneer die stelsel ineenstort of faal nie. Dit behels beide die voorbereiding vir stelselfaling en die herstel van die stelsel.

(ii) Lewenssiklus Versekering

Lewenssiklus versekering verseker dat 'n veilige stelsel ontwerp, ontwikkel en onderhou word met formele en streng gekontroleerde standaarde. Die volgende vereistes, wat veral fokus op menslike administratiewe beheermaatreëls, word deur die Oranje Boek beskryf:

Sekerheidstoetsing

Die stelselontwikkelaar moet alle sekerheidseienskappe toets en verseker dat die stelsel werk soos wat in die dokumentasie beskryf word, en die resultate van hierdie toetse dokumenteer. Daar word onderskei tussen meganisme toetsing, d.w.s. toetsing van sekerheidsmeganismes soos identifikasie en verifikasie, en koppelvlak toetsing, d.w.s. toetsing van alle gebruikersroetines wat sekerheidsfunksies oproep.

Ontwerp Spesifikasie en Verifikasie

Hierdie vereiste behels 'n formele wiskundige en geoutomatiseerde bewys dat die ontwerpsbeskrywing vir 'n stelsel ooreenkom met die stelsel se sekerheidsbeleid. 'n **Formele** bewys is 'n volledige en oortuigende argument dat 'n stelsel veilig is, of ten minste dat die stelselontwerp en implementering die sekerheidsbeleid van die stelsel uitvoer. Die ontwerpspesifikasie word weergegee in 'n **beskrywende hoëvlak spesifikasie** bekend as **DTLS** ("descriptive top-level specification") in informele taal, of 'n **formele hoëvlak spesifikasie** bekend as **FTLS** ("formal top-level specification") in wiskundige, presiese vorm.

Konfigurasie Bestuur

Konfigurasie bestuur beskerm 'n veilige stelsel terwyl dit ontwerp, ontwikkel en onderhou word. Dit behels die identifikasie, beheer en verslagdoening van alle veranderings wat aan die oorspronklike TCB gemaak word, insluitende apparatuur, firmatuur en programmatuur.

Veilige Verspreiding

Veilige verspreiding ("trusted distribution") beskerm 'n veilige stelsel terwyl dit na die kliënt vervoer word. Dit behels eerstens dat die verspreider verseker dat die stelsel wat by die kliënt arriveer, die presiese stelsel is wat deur hom versend word. Tweedens moet die kliënt met ontvangs van die stelsel die geldigheid daarvan toets om te verseker dat dit die oorspronklike stelsel is.

2.1.4 Dokumentasie Vereistes

Die Oranje Boek vereis vier spesifieke dokumente wat 'n veilige stelsel moet vergesel. Die dokumentasie vereistes is die volgende:

Sekerheidseienskappe Gebruikershandleiding

Hierdie gebruikershandleiding is gerig op gewone gebruikers sonder spesiale voorregte, en bespreek onderwerpe soos hoe om aan te teken op die stelsel en lêers en ander inligting te beskerm.

Veilige Fasiliteit Handleiding

Hierdie handleiding is gerig op stelseladministrateurs en/of sekerheidsadministrateurs en behandel onderwerpe soos hoe om die stelsel op te stel ten einde te verseker dat dit veilig is, die toepassing van stelselsekerheid en die optimale benutting van die stelsel.

Toetsdokumentasie

'n Veilige stelsel word as sodanig beskou hoofsaaklik op grond van die resultate van toetse wat bepaal of die sekerheidsmeganismes doeltreffend is. Dit is derhalwe noodsaaklik dat die dokumentasie onder andere 'n toetsplan, aannames oor die toetsomgewing, toetsprosedures, verwagte resultate en werklike resultate bevat.

Ontwerpsdokumentasie

Ontwerpsdokumentasie behels die dokumentasie van die interne eienskappe van die apparatuur, firmatuur en programmatuur. 'n Sleutelaspek hiervan is om die grense van die stelsel te definieer en te onderskei tussen die dele daarvan wat sekerheidsrelevant is en die wat nie is nie. Die twee hoofdoelwitte van ontwerpsdokumentasie is eerstens om aan die evalueringspan te bewys dat die stelsel aan die evalueringskriteria voldoen, en tweedens om die ontwerps- en ontwikkelingspan te help om die stelsel se sekerheidsbeleid te definieer en te bepaal hoe goed die sekerheidsbeleid in die implementering van die stelsel weerspieël word.

2.2 Sekerheidsklasse

'n Volledige uiteensetting van die sekerheidsvereistes vir elke klas word in Bylae A aan die einde van die studie gegee. Let daarop dat die klasse hiërargies op mekaar volg, en dat, in die bylae, vir elke klas slegs die addisionele vereistes vir die betrokke sekerheidseienskap gegee word. Die skrywer bied hier slegs 'n opsomming van die klasse.

D Stelsels : Minimum sekerheid

Die Oranje Boek spesifiseer geen vereistes vir afdeling D nie, aangesien hierdie afdeling slegs dien om stelsels te beskryf wat aan geen van die vereistes van die hoër klasse voldoen nie. Daar is in werklikheid geen geëvalueerde stelsels in hierdie klas nie, aangesien 'n verskaffer nie die moeite sal doen om 'n stelsel te laat evalueer as dit nie 'n redelike mate van sekerheidsfasiliteite bied nie.

C1 Stelsels : Diskresionêre Sekerheidsbeskerming

C1 stelsels verskaf redelik beperkte sekerheidsfasiliteite wat daarop gerig is om gebruikers te verhoed om toevallige foute te maak wat die sekerheid van die stelsel kan benadeel. Die belangrikste eienskappe van die C1 klas is wagwoorde (identifikasie en verifikasie) en diskresionêre beskerming van lêers en ander objekte.

C2 Stelsels : Gekontroleerde Toegangsbeskerming
Bykomend tot die eienskappe van C1 stelsels, bied C2 stelsels die volgende fasiliteite:

- Aanspreeklikheid van individuele gebruikers deur wagwoord kontroles en ouditteg nieke.

- Meer gedetailleerde diskresionêre beheermaatreëls tot die granulariteit van 'n enkele gebruiker.

- Objek hergebruik, wat verhoed dat data wat in die geheue of op 'n stoormedium agterbly nie beskikbaar gestel word aan 'n ander gebruiker nie.

B1 Stelsels : Etiket Sekerheidsbeskerming
B1 en hoër stelsels ondersteun verpligte toegangsbeheer, waar elke lêer en ander hoofobjekte in die stelsel geëtiketteer word. Die stelsel gebruik hierdie sensitiwiteitsetikette om met die sekerheidsvlakke van gebruikers te vergelyk ten einde die sekerheidsbeleid toe te pas.

B2 Stelsels : Gestruktureerde beskerming
B2 en hoër stelsels voeg nie baie meer sigbare sekerheids-eienskappe by die stel wat reeds in B1 stelsels vereis word nie. Hulle brei eerder die bestaande eienskappe uit en vereis bykomende versekering dat die eienskappe korrek ontwerp is en werk. In die B2 klas word etikette uitgebrei om toestelle in te sluit, 'n veilige pad eienskap word bygevoeg, asook die konsep van minste voorreg.

B3 Stelsels : Sekerheidsdomeine
Daar is geen sigbare bykomende vereistes vir B3 stelsels nie, maar die stelselontwerp en versekering eienskappe is baie strenger. Veilige fasiliteit bestuur, veilige herstel, en die vermoë om die administrateur onmiddellik in kennis te stel van 'n breuk in sekerheid, word onder andere vereis. B3 stelsels is nie baie algemeen nie aangesien 'n verskaffer net

sowel kan aangaan om 'n A1 gradering vir 'n stelsel te verkry as daar reeds aan B3 vereistes voldoen word.

A1 Stelsels : Geverifieerde Ontwerp
A1 stelsels is tans bo aan die sekerheidsleer, alhoewel die moontlikheid ondersoek word om vereistes te definieer wat A1 stelsels oortref in die areas van stelselargitektuur, toetsing en formele verifiëring. Die enigste bykomende eienskappe van A1 stelsels bo dié van B3 stelsels is veilige verspreiding en bykomende versekering deur formele ontleding en wiskundige bewys dat die stelselontwerp ooreenkom met die stelsel se sekerheidsbeleid en ontwerpspesifikasies.

2.3 Voorstellingsmeganisme

Die konseptuele voorstelling van die mate waarin 'n spesifieke produk aan die vereistes van die Oranje Boek voldoen, geniet bykans geen aandag in die literatuur nie. In die volgende voorbeeld maak die skrywer van sogenaamde **roos-diagramme** gebruik om die evaluering van 'n produk konseptueel voor te stel. Die voordeel van hierdie voorstellingsmeganisme is dat twee verskillende produkte met een oogopslag vergelyk kan word volgens die kriteria van die Oranje Boek.

Die roos-diagram bestaan eerstens uit **konsentriese sirkels** wat die verskillende sekerheidsklasse van die kriteria (C1, C2, B1, B2, B3 en A1) voorstel (figuur 2.1). Elke sirkel word verdeel in 27 **segmente**, wat elk 'n spesifieke vereiste (soos gedefinieer in die TCSEC, bylae A) voorstel, bv. identifikasie en verifikasie, stelselargitektuur ens. (figuur 2.2).

Die produk wat geëvalueer word, kan nou aan elke vereiste gemeet word om te bepaal in welke sekerheidsklas die produk val vir die spesifieke vereiste (m.a.w. die mate waaraan die produk aan 'n spesifieke vereiste voldoen). Vir elke segment (vereiste) word daar dus 'n punt bepaal wat op die buiterand van 'n konsentriese sirkel (sekerheidsklas) tussen die segmentgrense aangeteken word. Al die punte word dan met

mekaar verbind en die ingeslote area van die veelhoek word ingekleur. Hierdie ingeslote area stel dus voor in watter mate voldoen die produk aan die verskillende sekerheids-vereistes individueel en bied terselfdertyd 'n duidelike beeld van die mate waaraan die produk aan die kriteria van die Oranje Boek as geheel voldoen.

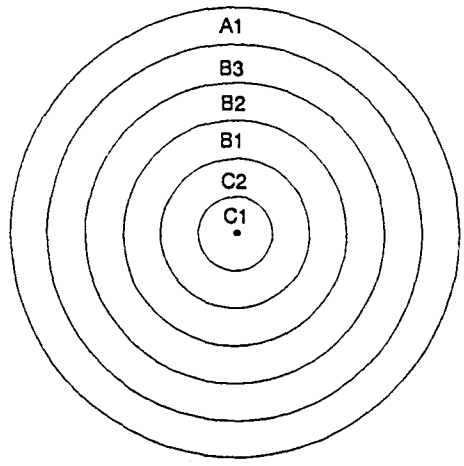
Let daarop dat hierdie voorstellingsmeganisme geen wiskundige gronde het nie, m.a.w. die ingeslote oppervlak van die veelhoek dui nie noodwendig die mate aan waaraan 'n produk aan die kriteria voldoen nie. Die meganisme het slegs konseptuele voorstelling ten doel.

Vir die doeleindes van die voorbeeld word 'n denkbeeldige produk A gekies. Die sekerheidsvereistes en die klasse waaraan die produk voldoen, word in tabel 2.1 uiteengesit (sien bylae A vir 'n opsomming van die vereistes).

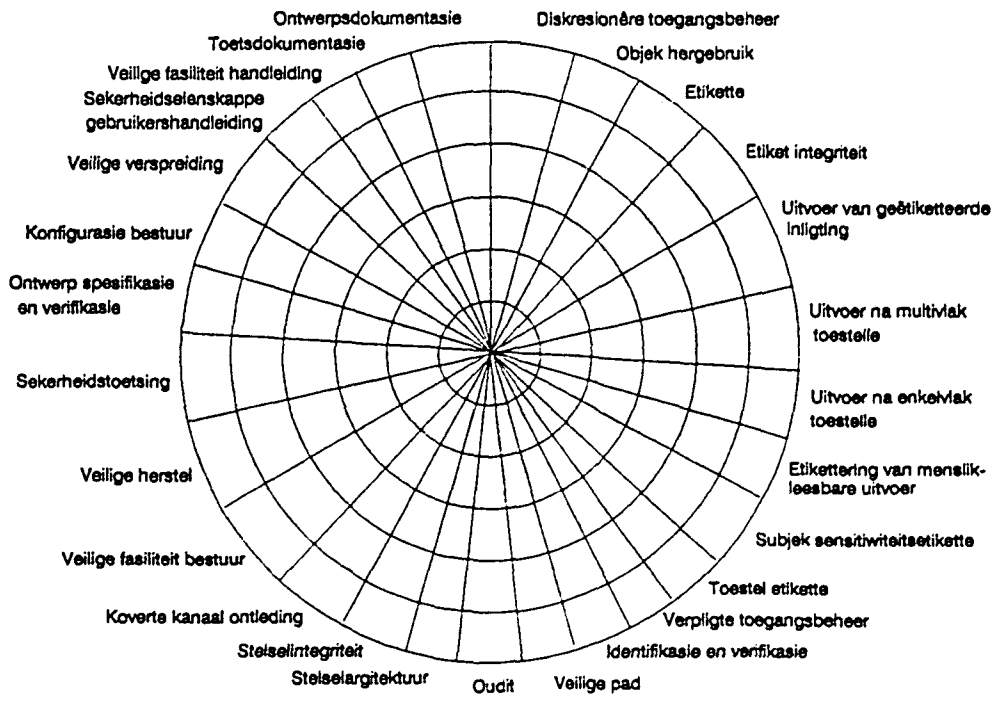
Figuur 2.3 toon 'n deursigtige roosdiagram vir produk A t.o.v. die 27 sekerheidsvereistes van die Oranje Boek om te illustreer hoe die punte van die "roos" met mekaar verbind word. Figuur 2.4 toon die ingekleurde roosdiagram vir produk A, terwyl figuur 2.5 opsommenderwys die roosdiagram vir produk A toon t.o.v. die vier basiese kategorieë van seker-heidsvereistes van die Oranje Boek.

Sekerheidsvereiste	Sekerheids-klas
Diskresionêre toegangsbeheer	B2
Objek hergebruik	A1
Etikette	A1
Etiket integriteit	A1
Uitvoer van geëtiketteerde inligting	A1
Uitvoer na multivlak toestelle	A1
Uitvoer na enkelvlak toestelle	A1
Etikettering van menslik-leesbare uit-voer	A1
Subjek sensitiwiteitsetikette	B1
Toestel etikette	B1
Verpligte toegangsbeheer	C2
Identifikasie en verifikasie	A1
Veilige pad	B1
Oudit	B1
Stelselargitektuur	B2
Stelselintegriteit	A1
Koverte kanaal ontleding	B1
Veilige fasiliteit bestuur	B2
Veilige herstel	A1
Sekerheidstoetsing	B1
Ontwerp spesifikasie en verifikasie	B1
Konfigurasie bestuur	B3
Veilige verspreiding	A1
Sekerheidseienskappe gebruikershandlei-ding	A1
Veilige fasiliteit handleiding	B1
Toetsdokumentasie	B1
Ontwerpsdokumentasie	B1

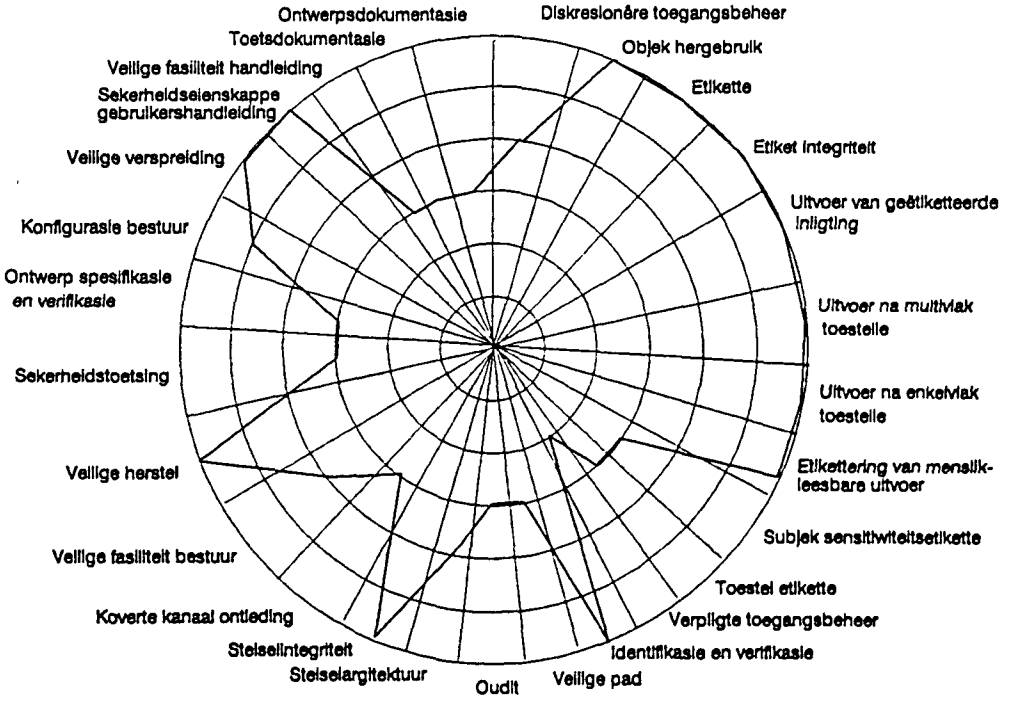
TABEL 2.1 EVALUERING VAN PRODUK A



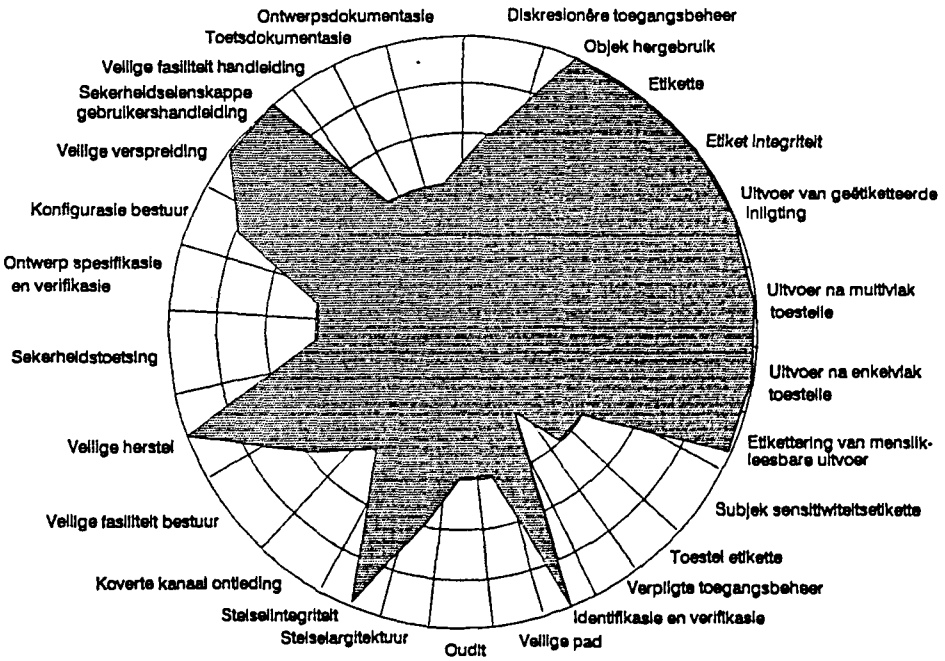
Figuur 2.1 TCSEC Klasse



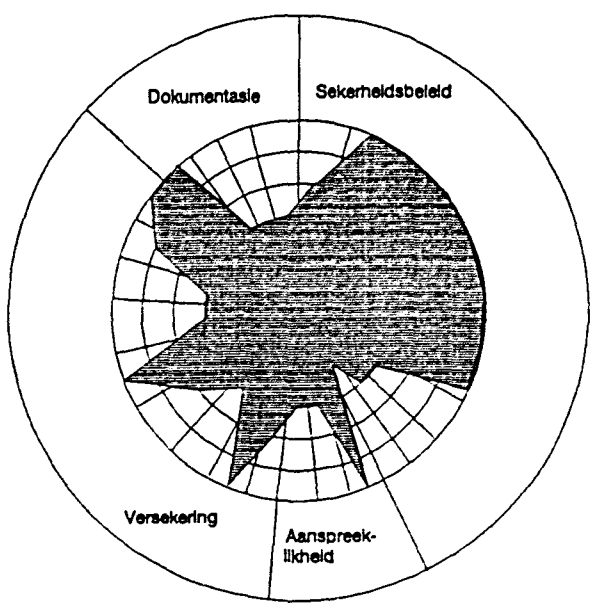
Figuur 2.2 TCSEC Vereistes



Figuur 2.3 Evaluering van produk A volgens TCSEC vereistes (deursigtig)



Figuur 2.4 Evaluering van produk A volgens TCSEC vereistes



Figuur 2.5 Evaluering van produk A (opsommend)

toegangsbeheer soos in die Oranje Boek gedefinieer, gebruik te maak. In hierdie verband het 'n gesamentlike studiegroep van SRI International en Gemini Computers in 1988 'n model ontwikkel wat beskryf hoe dit moontlik is om sienings te gebruik vir diskresionêre toegangsbeheer, etikettering van nuwe data en afleidingsreëls in 'n multivlak databasis stelsel wat aan die vereistes vir verpligte toegangsbeheer voldoen. [59]

Binding van kriteria

Die binding van funksionaliteit en versekering in 'n enkele dubbelletter klas is te beperkend. Dit bied nie 'n sinvolle evalueringsmeganisme vir byvoorbeeld 'n geval waar 'n stelsel hoë versekering maar beperkte funksionaliteit verskaf nie. [15]

Onbuigbaarheid

Die Oranje Boek kombineer gepubliseerde stelselkriteria met stelselevaluering en -gradering relatief tot die kriteria. Hierdie proses verskaf geen aanmoediging of beloning vir stelsels wat verder gaan as, of nie letterlik voldoen aan, die Oranje Boek se spesifieke vereistes nie. [70]

Evalueringsprogram

Die volgende drie punte van kritiek wat deur Winters [92] geïdentifiseer word, is eerder gerig op die evalueringsprogram wat deur NCSC uitgevoer word, as wat dit op die Oranje Boek self gerig is.

Eerstens neem die proses om 'n EPL gradering te verkry tans ten minste twee tot drie jaar. Beide verskaffers en gebruikers is besorg oor die impak wat hierdie uitgerekte evalueringsproses op hul vermoë om nuwe tegnologie te bemark en te gebruik, kan hê.

Tweedens word die NCSC se versekeringsvereistes in sommige kringe as ietwat subjektief en dinamies beskou, met 'n gebrek

aan spesifieke vaste kriteria. 'n Rede hiervoor is waarskynlik dat dit die verskaffer se verantwoordelikheid is om aan die NCSC te demonstreer dat die stelseleienskappe oor voldoende versekering beskik.

Derdens aanvaar die NCSC nie produkte deur verskaffers buite die V.S.A. vir evaluering nie. Hierdie beperking hou die gevaar in dat die Oranje Boek as internasionale standaard geïsoleer sal word terwyl ander tegnologies gevorderde lande hul eie standaarde ontwikkel. [70]

2.5 Die Rooi Boek

Alhoewel baie van die konsepte en meganismes wat in die Oranje Boek beskryf word van toepassing is op netwerkomgewings, is daar veral twee tekortkominge in die Oranje Boek met betrekking tot netwerke. Eerstens is die Oranje Boek gerig op enkel-stelsel sekuriteit, en tweedens laat die Oranje Boek na om vereistes vir beskikbaarheid en waarmerking ("authentication") te stel, twee aspekte wat baie belangrik is in netwerksekerheidsbestuur.

Ten einde hierdie en ander tekortkominge van die Oranje Boek te ondervang, het die NCSC 'n stel standaard kriteria ontwikkel vir die evaluering van die vlak van vertroue wat in 'n netwerk gestel kan word. In 1987 is die **Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria** (TNI) gepubliseer. Beter bekend as die "Rooi Boek", beskryf hierdie publikasie die wyse waarop spesifieke sekerheidseienskappe, die versekeringsvereistes en die graderingstruktuur van die TCSEC uitgebrei word tot netwerke wat strek vanaf geïsoleerde lokale area netwerke tot wye area internetwerk stelsels. Die Rooi Boek bespreek die eienskappe en vereistes in twee kategorieë, naamlik TCSEC vereistes en ander sekerheidsdienste. [70] [78]

2.5.1 TCSEC Vereistes

In Deel I beskryf die Rooi Boek die vereistes vir elke klas wat in die Oranje Boek bespreek word, en toon dan aan hoe die NTCB ("Network Trusted Computing Base") van 'n spesifieke netwerkproduk aan die vereistes van daardie klas sal voldoen. Die graderings wat toegeken word is dieselfde klasse as dié van die Oranje Boek.

2.5.2 Ander Sekerheidsdienste

In Deel II beskryf die Rooi Boek addisionele netwerk sekerheidsdienste wat beskikbaar kan wees in spesifieke netwerke. Die graderingstelsel vir hierdie dienste is kwalitatief, nl. geen, minimum, redelik, en goed. Die dienste word in drie kategorieë verdeel : kommunikasie-integriteit, diensweiering en blootstellingsbeskerming.

Kommunikasie-integriteit

Hierdie dienste verseker dat netwerkboodskappe akkuraat versend word en nie vervals is, tydens versending gewysig is, of gerepudieer is deur die ontvanger of sender van die boodskap nie. Die spesifieke dienste is:

- **Waarmerking** - Bewys die identiteit van die gebruiker en die stelsel wat die boodskap versend.

- **Kommunikasieveld-integriteit** - Beskerm die akkuraatheid en integriteit van die boodskap.

- **Nie-repudiëring** - Bewys dat 'n boodskap versend en ontvang is.

Diensweiering

Hierdie dienste verseker dat die netwerk te alle tye aanhou werk en dat alle dienste wat deur gebruikers benodig word ten volle beskikbaar is. Die volgende dienste word gedefinieer:

- **Kontinuïteit van bedryf** - Laat die netwerk doeltreffend

werk selfs as komponente daarvan faal.

- **Protokol-gebaseerde beskerming** - Spoor netwerkprobleme op deur die gebruik van bestaande protokoldienste, soos bv. die meting van die versendingstempo tussen stelsels.

- **Netwerkbestuur** - Monitor die algehele netwerkprestasie om aanvalle op die netwerk, falings of ongelykhede op te spoor.

Blootstellingsbeskerming

Dienste in hierdie kategorie is gerig daarop om die inligting wat oor 'n netwerk versend word, vertroulik te hou. Die volgende dienste word gedefinieer:

- **Data-vertroulikheid** - Beskerm data teen onderskepping deur ongemagtigde gebruikers tydens versending.

- **Verkeersvloei vertroulikheid** - Beskerm eienskappe van die versende data, soos boodskaplengte, teen ontleding deur 'n indringer.

- **Selektiewe roetering** - Vermy bedreigings deur boodskappe só te roeteer dat verdagte netwerke of stelsels vermy word.

3. DIE WIT BOEK

In Europa is daar ook oor die afgelope paar jaar werk gemaak van die definiëring van standaarde vir beheermaatreëls. In die Verenigde Koninkryk, Duitsland, Frankryk en Nederland is aanvanklik afsonderlike kriteria ontwikkel vir spesifieke aspekte van veilige stelsels. In 1990 het afgevaardigdes van die industrie en akademie in hierdie lande egter bymekaargekom onder die beskerming van die German Information Security Agency (GISA) ten einde 'n gemeenskaplike standaard vir inligtingsekerheid uit te werk. Die resultaat hiervan was die publikasie van die Europese ekwivalent van die TCSEC, die

Information Technology Security Evaluation Criteria (ITSEC) of "Wit Boek". Die kriteria is die eerste stap in die daarstelling van 'n enkele, internasionale (of ten minste Europese) sekerheidstandaard. [78]

In ITSEC word drie redes gegee vir die harmonisering van verskillende standaarde [51]:

- Die ondervinding van verskillende lande kan saamgevoeg word sodat almal daarby kan baat.

- Die industrie wil nie verskillende standaarde in verskillende lande hê nie.

- Die basiese konsepte en benaderings is dieselfde in verskillende lande hetsy dit in kommersiële, regerings- of verdedigingstoepassings is.

Die ITSEC kriteria is hoofsaaklik gerig op die evaluering van inligtingstegnologie-produkte en -stelsels. In die Wit Boek word 'n **produk** gedefinieer as 'n apparatuur/programmatuur pakket wat van die rak af gekoop kan word en in 'n verskeidenheid van bedryfsomgewings gebruik kan word. 'n **Stelsel** daarenteen, word ontwerp en ontwikkel volgens die behoeftes van 'n spesifieke gebruiker in 'n unieke bedryfsomgewing. [51]

3.1 Funksionaliteit en Versekering

In die Wit Boek word daar 'n duidelike onderskeid getref tussen funksionaliteitsvereistes en versekeringsvereistes van 'n stelsel of produk wat geëvalueer word (die sogenaamde "**Target of Evaluation**" of TOE), en daar bestaan ook afsonderlike klasse vir die vereistes in hierdie twee kategorieë. [51]

Die **funksionaliteit** van 'n TOE bestaan uit al die aktiewe funksies van die TOE wat bydra tot sekerheid. Funksionaliteit

word op drie vlakke van abstraksie beskou. Die mees abstrakte vlak is **sekerheidsdoelwitte**, dit is die bydrae wat 'n TOE tot sekerheid wil maak. Hieruit volg **sekerheidsfunksies**, d.i. die eienskappe van die TOE wat bydra tot die sekerheidsdoelwitte. Die sekerheidsfunksies word verrig deur spesifieke **sekerheidsmeganismes**, d.i. die logika of algoritme wat 'n spesifieke funksie implementeer. Die dokument of dokumente wat hierdie aspekte van funksionaliteit beskryf, staan bekend as die **sekerheidsmikpunt** ("security target").

Soos vroeër gemeld, behels **versekering** die vertroue dat die geselekteerde sekerheidsfunksies wel die sekerheidsdoelwitte bereik. Die Wit Boek onderskei spesifiek tussen vertroue in die **korrektheid** en vertroue in die **effektiwiteit** van die sekerheidsfunksies en meganismes van die TOE.

Slegs wanneer 'n TOE suksesvol geëvalueer word in terme van die korrektheid daarvan, word die effektiwiteit van die TOE geëvalueer. [51]

3.2 Evalueringsklasse en -vlakke

Funksionaliteitsvereistes word geklassifiseer in klasse F1 tot F10. Klasse F1 tot F5 volg hiërargies op mekaar en stem in 'n groot mate ooreen met die funksionaliteit van die TCSEC evalueringsklasse C1, C2, B1, B2, en B3/A1, onderskeidelik. Die oorblywende klasse is nie-hiërargies en word gebruik vir die gradering van data- en programintegriteit (F6), stelselbeskikbaarheid (F7), data-integriteit tydens kommunikasie (F8), data-vertroulikheid tydens kommunikasie (F9), en netwerksekerheid, insluitende vertroulikheid en integriteit (F10). Klasse F6 tot F10 kan aanvullend tot mekaar en tot die gekose basisvlak (F1, F2, F3, F4, of F5) geëvalueer word. [70]

Die evalueringsvlakke m.b.t. **versekering** word gedefinieer binne die konteks van die korrektheidskriteria. Die vereistes vir effektiwiteit verander nie volgens vlak nie, maar bou

eerder op die vereistes vir korrektheid. Indien 'n TOE nie voldoen aan die evaluering van hetsy korrektheid of effektiwiteit nie, word 'n gradering van **E0** daaraan toegeken. Die volgende opsommende beskrywings van die verskillende vlakke word deur die Wit Boek gegee [51]. Let daarop dat elke vlak se vereistes addisioneel tot die vorige vlak s'n is, en die vorige vlak se vereistes dus per definisie insluit.

Vlak E1 : Daar is 'n sekerheidsdoelwit en 'n informele beskrywing van die sekerheidsargitektuur van die TOE. Toetsing dui aan dat die TOE die sekerheidsmikpunt bereik.

Vlak E2 : Daar is 'n informele beskrywing van die gedetailleerde ontwerp. Bewys van toetsing word gegee. Daar is konfigurasiebeheer en beheer oor die verspreidingsproses.

Vlak E3 : Die gedetailleerde ontwerp en die bronkode van die sekerheidsfunksies word verskaf.

Vlak E4 : Daar is 'n formele model van die sekerheidsbeleid. Die argitekturele en gedetailleerde ontwerp word deeglik genoteer. Ontleding vir kwesbaarhede word op hierdie deeglike benadering gebaseer.

Vlak E5 : Daar is 'n noue ooreenkoms tussen die gedetailleerde ontwerp en die bronkode. 'n Ontleding van kwesbaarhede word gedoen deur die bronkode te gebruik.

Vlak E6 : 'n Formele beskrywing van die sekerheidsargitektuur van die TOE, wat ooreenstem met die formele model van die sekerheidsbeleid, word gegee.

Omskakeling van graderings

ITSEC is bedoel as 'n superstel van TCSEC, en die hiërargiese ITSEC graderings kan derhalwe rofweg omgeskakel word na TCSEC graderings. Die omskakeling is soos volg [51]:

ITSEC		TCSEC
E0	-->	D
F1,E2	-->	C1
F2,E2	-->	C2
F3,E3	-->	B1
F4,E4	-->	B2
F5,E5	-->	B3
F5,E6	-->	A1

Dit is egter belangrik om daarop te let dat hierdie omskakeling nie presies is nie, d.w.s. 'n stelsel wat as F3,E3 gegradeer word, voldoen nie noodwendig aan al die vereistes vir 'n B1 stelsel nie (of omgekeerd). 'n Internasionale studiegroep [15] het byvoorbeeld die Oranje Boek se vereistes vir B3 vergelyk met die Wit Boek se vereistes vir F5/E5 en die volgende gevolgtrekkings gemaak:

- 'n F5/E5 stelsel moet aan addisionele vereistes voldoen vir stelselargitektuur, veilige pad, etikette op gedrukte uitvoer en objek hergebruik, ten einde as 'n B3 stelsel geklassifiseer te word.

- 'n B3 stelsel moet aan addisionele vereistes voldoen vir ontwerpspesifikasies, konfigurasiebestuur, toetsprosedures, veilige verspreiding en onderhoudskontroles, ten einde as 'n F5/E5 stelsel geklassifiseer te word.

'n Verdere faktor wat in gedagte gehou moet word met die omskakeling van graderings, is dat die subjektiewe aard van die graderingsproses dit moeilik maak om konsistentheid te verseker tussen evaluerings wat by verskillende fasiliteite, deur verskillende evalueerders en in verskillende lande

gedoen is, veral in ag genome die verskil in die standaarde self. [70]

In die volgende paragrawe word die funksionaliteits- en versekeringsvereistes van die Wit Boek opgesom. Die bron wat gebruik is, is weergawe 1 van die ITSEC kriteria wat in Mei 1990 gepubliseer is. [51]

3.3 Sekerheidsvereistes

3.3.1 Funksionaliteit

(i) Generiese klasse

Die sekerheidsfunksies in ITSEC word in die sekerheidsmikpunt onder agt generiese opskrifte beskryf. Daar is egter geen beperking op die spesifieke funksionaliteit wat deur 'n TOE bereik kan word nie, en derhalwe kan enige verdere kategorieë in die sekerheidsmikpunt beskryf word deur die beskikbare spesifikasieformaat te gebruik. Die spesifieke vereistes vir die hiërargiese klasse F1 tot F5 en die vereistes vir die nie-hiërargiese klasse F6 tot F10 word in Bylae B aan die einde van hierdie studie opgesom. Die agt bestaande kategorieë is:

Identifikasie en Verifikasie

Hierdie afdeling sluit in funksies soos die verifiëring van die identiteit van 'n gebruiker, asook funksies om nuwe gebruikersidentiteite by te voeg en oues te verwyder.

Toegangsbeheer

Enige funksies wat gerig is op die beheer van die vloei van inligting tussen, en die gebruik van hulpbronne deur, gebruikers, prosesse en objekte. Dit sluit in die administrasie en verifikasie van regte, en die opstelling en onderhoud van lyste of reëls vir verskillende tipes toegang deur verskillende gebruikers.

Aanspreeklikheid
Funksies wat gerig is op die versameling, beskerming en ontleding van inligting m.b.t. die uitoefening van regte om sekerheidsrelevante aksies te verrig.

Oudit
Funksies gerig daarop om gebeurtenisse wat 'n bedreiging vir sekerheid inhou, op te spoor en te ondersoek. Sommige funksies mag voldoen aan die eienskappe van beide aanspreeklikheid en oudit.

Objek Hergebruik
Funksies wat die hergebruik van geheue en skyfspasie moontlik maak sonder om die ongewenste vloei van inligting toe te laat.

Akkuraatheid
Funksies wat poog om die korrektheid en konsistentheid van sekerheidsrelevante inligting te verseker. Dit behels bv. dat spesifieke verwantskappe tussen verskillende dele data korrek onderhou word, en dat inligting tussen prosesse oorgedra word sonder wysiging.

Betroubaarheid van diens
Funksies gerig daarop om konsistentheid en beskikbaarheid van diens te verseker. Dit sluit in funksies om te verseker dat tyd-kritiese take stiptelik uitgevoer word, en dat toegang tot hulpbronne beskikbaar is wanneer dit nodig is. Verder behels dit ook foutopsporings- en foutherstelfunksies gerig op die minimalisering van diensonderbreking.

Data-uitruiling
Funksies wat die sekerheid van data verseker tydens versending oor kommunikasiekanale. Waar moontlik moet die kommunikasie-sekerheidsfunksies beskryf word in die terminologie van die OSI-sekerheidsargitektuur.

(ii) Spesifikasiestyle

Daar word onderskei tussen drie benaderings tot die styl waarin die funksionaliteit van 'n TOE gespesifiseer word, naamlik informele, semi-formele en formele spesifikasie.

Informele spesifikasie word nie geskryf in 'n notasie wat spesiale beperkings of konvensies vereis nie. Daar word eerder van 'n natuurlike taal (d.i. Engels, Duits ens.) gebruik gemaak. Die spesifikasie is derhalwe eenvoudig maar leen hom tot onduidelikhede en dubbelsinnighede.

Semi-formele spesifikasie vereis die gebruik van 'n tipe beperkte notasie in ooreenstemming met 'n spesifieke stel konvensies. Hierdeur word die omvang van dubbelsinnighede of onduidelikhede in die spesifikasies verminder. Alhoewel spesiale opleiding gewoonlik nodig is om hierdie tipe spesifikasies te skryf, is opleiding gewoonlik nie nodig om dit te lees nie. Voorbeelde hiervan is die Claims taal, gestruktureerde diagramme en informele sekerheidsbeleid modelle. [51]

Formele spesifikasie word geskryf in 'n wiskundige notasie gebaseer op gevestigde wiskundige konsepte. Die spesifikasie kan ondubbelsinnig wees en kan bewys word om konsistent en korrek te wees m.b.t. 'n stel aksiome. Spesiale opleiding word gewoonlik vereis om hierdie tipe spesifikasies te lees of te skryf. Voorbeelde hiervan is formele spesifikasietale en formele sekerheidsbeleid modelle soos Bell en La Padula. [51]

3.3.2 Versekering - Korrektheid

Die evalueringskriteria vir die bepaling van korrektheid onderskei tussen kriteria m.b.t. die wyse waarop die stelsel ontwikkel is (**konstruksie**) en kriteria m.b.t. die wyse waarop die stelsel gebruik sal word (**bedryf**). Kriteria vir konstruksie en bedryf word verder verdeel in verskillende fases of aspekte. Die vereistes vir elke fase of aspek verander dan

volgens die verskillende evalueringsvlakke. Die spesifieke vereistes vir elke evalueringsvlak word in Bylae B aan die einde van hierdie studie opgesom. Let daarop dat vlakke hiërargies op mekaar volg en dat vir elke vlak, slegs die addisionele vereistes vir die betrokke kriteriaklas gegee word.

(i) Konstruksie

Die kriteria vir konstruksie word verdeel in twee kategorieë, naamlik die **ontwikkelingsproses** en die **ontwikkelingsomgewing**.

Ontwikkelingsproses

Die belangrikste bron van vertroue in die korrektheid van die sekerheidsaspekte van 'n TOE is 'n begrip van die wyse waarop die stelsel ontwikkel is. Hierdie ontwikkelingsproses bestaan uit 'n aantal fases waarvoor kriteria beskryf word wat faktore identifiseer wat bydra tot hierdie vertroue.

Fase 1 : Vereistes

Hierdie fase dek die identifikasie en beskrywing van die sekerheidsmikpunt van die stelsel, wat die basislyn van evaluering vorm. Dit sluit in die mikpunt vir die evalueringsvlak wat bereik moet word.

Fase 2 : Argitekturele Ontwerp

Hierdie fase dek die algehele hoëvlak definisie en ontwerp van die TOE. Dit neem die vorm aan van 'n beskrywende hoëvlak spesifikasie wat die basiese struktuur van die TOE identifiseer, asook die eksterne koppelvlakke en die verdeling in apparatuur en programmatuur komponente.

Fase 3 : Gedetailleerde Ontwerp

Hierdie fase dek die verfyning van die argitekturele ontwerp van die TOE tot 'n vlak van detail wat gebruik kan word as 'n basis vir programmering en/of apparatuur konstruksie, d.w.s. alle vlakke van ontwerp en spesifikasie onder die aanvanklike hoëvlak spesifikasie. Komponente

op die laagste vlak van spesifikasie word genoem basiese komponente; dit is vanaf hierdie komponente wat die werklike kode en/of apparatuur geproduseer sal word.

Fase 4 : Implementering
Dié fase dek die implementering van die gedetailleerde TOE ontwerp as apparatuur en/of programmatuur. Elke basiese komponent sal eers geprogrammeer of gebou word vanaf die basiese komponent spesifikasies en dan getoets word teen hierdie spesifikasies. Die doel is dat die hele TOE dan uiteindelik teenoor die sekerheidsmikpunt getoets kan word.

Ontwikkelingsomgewing
Die ontwikkelingsomgewing behels die maatreëls, prosedures en standaarde wat deur die ontwikkelaar toegepas word tydens die ontwikkeling, produksie en onderhoud van die meesterkopie van die TOE.

Aspek 1 : Konfigurasiebeheer
Dié aspek dek die kontroles wat deur die ontwikkelaar op sy ontwikkelings-, produksie- en onderhoudsprosesse toegepas word, sodat elke verandering aan ontwerp of implementering op 'n gekontroleerde wyse geskied. Die bepaling van konfigurasiebeheer sluit in 'n begrip van die ontwikkelaar se kwaliteitsbestuur kontroles.

Aspek 2 : Ontwikkelaarsekerheid
Ontwikkelaarsekerheid dek die fisiese, prosedure-, tegniese en personeelmaatreëls wat in die ontwikkelingsomgewing toegepas word. Die doel hiervan is om die ontwikkeling te beskerm teen aanvalle en om die vertroulikheid van inligting toepaslik te beskerm.

(ii) Bedryf

Die kriteria vir die bedryf van die stelsel word ook in twee kategorieë verdeel, naamlik die **bedryfsdokumentasie** en die **bedryfsomgewing**.

Bedryfsdokumentasie

Bedryfsdokumentasie is die belangrikste wyse waarop die ontwikkelaar van 'n TOE en sy kliënte kommunikeer. Die verstaanbaarheid, dekking en korrektheid daarvan is derhalwe belangrike faktore in die veilige bedryf van die TOE.

Aspek 1 : Gebruikersdokumentasie

Hierdie dokumentasie bevat die inligting oor die TOE wat deur die ontwikkelaar aan die eindgebruikers verskaf word, en behoort die eindgebruiker in staat te stel om die sekerheidsvermoë van die TOE te begryp, asook die bydrae wat hy moet maak om sekerheid tydens gebruik te verseker.

Aspek 2 : Administrasie Dokumentasie

Hierdie dokumentasie bevat die inligting oor die TOE wat deur die ontwikkelaar verskaf word vir gebruik deur diegene wat die gebruik en bedryf van die TOE administreer. Die inligting behoort die kliënt se tegniese, administratiewe en bedryfspersoneel te help om die TOE op 'n veilige wyse op te stel en te bedryf.

Bedryfsomgewing

Die bedryfsomgewing behels die maatreëls, prosedures en standaarde m.b.t. die veilige aflewering, installering en bedryf van die TOE. In die geval van 'n stelsel wat reeds in gebruik is, is dit moontlik om die werklike bedryfsprosedures te evalueer, andersins is dit slegs moontlik om die voorgestelde prosedures te evalueer.

Aspek 1 : Aflewering en Konfigurasie

Hierdie aspek dek die prosedures wat gebruik word om sekerheid te behou tydens die oordrag van die stelsel of

die komponente daarvan na die gebruiker, hetsy by die aanvanklike aflewering of as deel van daaropvolgende wysigings aan die stelsel. Dit sluit in enige spesiale prosedures wat nodig is om die TOE te konfigureer tydens installering, of om die oorspronklikheid daarvan aan die kliënt te demonstreer.

Aspek 2 : Aanskakeling en Bedryf
Hierdie aspek dek die prosedures wat deur die operateurs en/of eind-gebruikers gebruik word om die TOE op 'n veilige wyse op 'n daaglikse basis te gebruik. Dit sluit in dag-tot-dag bedryf asook ander roetine-aktiwiteite soos rugsteuning en buitengewone aktiwiteite soos aanskakeling en herstel ná 'n stelselfaling.

3.3.3 Versekering - Effektiwiteit

Evaluering van effektiwiteit bepaal of die vlak van vertroue wat deur die evaluering van die TOE se korrektheid bepaal is, geldig bly vir die kombinasie van korrektheid en effektiwiteit wanneer die voorgestelde gebruik van die TOE binne die konteks van die omgewing waarin dit gebruik sal word, beoordeel word.

Die bepaling van die effektiwiteit van die TOE word slegs gedoen nadat die vlak van vertroue in die korrektheid daarvan bepaal is deur gebruik te maak van die dokumentasie en resultate van laasgenoemde evaluering. Die vertroue wat geplaas kan word in die effektiwiteit van die TOE word derhalwe beperk tot die evalueringsvlak wat vir die korrektheid bepaal is. Indien die TOE aan enige van die vereistes vir effektiwiteit tekortskiet, sal 'n algehele gradering van vlak E0 daaraan toegeken word, aangesien dit ongeskik is om te gebruik soos voorgestel in die sekerheidsmikpunt.

Indien die vlak van vertroue in die korrektheid van die TOE vlak E0 is, is dit uiteraard nie nodig om die vertroue in die effektiwiteit te evalueer nie.

In die evaluering van die effektiwiteit van 'n TOE word daar eweneens onderskei tussen die **konstruksie** en die **bedryf** daarvan.

Konstruksie

Aspek 1 : Toepaslikheid van Funksionaliteit

Die sekerheidsmikpunt word gebruik as 'n basis om te bepaal of die sekerheidsfunksies en -meganismes in werklikheid die geïdentifiseerde bedreigings vir die sekerheid van die TOE sal teenwerk.

Aspek 2 : Binding van Funksionaliteit

Hierdie aspek behels 'n ondersoek na die vermoë van die sekerheidsfunksies en meganismes van die TOE om saam te bind op 'n wyse wat onderling ondersteunend is en 'n geïntegreerde en effektiewe geheel bied.

Aspek 3 : Bepaling van Kwesbaarheid : Konstruksie

Die kwesbaarhede wat tydens die bepaling van die korrektheid van die konstruksie van die TOE geïdentifiseer is, word ondersoek om te bepaal of hulle in werklikheid die sekerheid van die TOE soos gespesifiseer in die sekerheidsmikpunt, negatief kan beïnvloed.

Aspek 4 : Sterkte van Meganismes

Hierdie aspek vereis oorweging van die vlak van hulpbronne wat nodig is ten einde 'n suksesvolle direkte aanslag op die stelsel te maak. Ten einde die **minimum sterkte** gradering vir 'n TOE te bepaal (d.i. basies, medium of hoog), moet daar verseker word dat daar geen kritiese meganismes van 'n laer sterkte is as die betrokke gradering nie. 'n Kritiese meganisme is een wat nie deur ander meganismes beskerm word nie en waarvan die faling 'n kwesbaarheid skep.

Bedryf

Aspek 1 : Gemak van Gebruik

Ten einde die effektiwiteit van die sekerheidsmeganismes te verseker, is dit nodig dat dit in die praktiese bedryfsomgewing geïmplementeer en beheer word, en dat die gebruik daarvan geoudit word.

Aspek 2 : Bepaling van Kwesbaarheid : Bedryf

Enige kwesbaarhede wat tydens die bepaling van die korrektheid van die bedryf van die TOE geïdentifiseer is, word ondersoek om te bepaal of dit in die praktyk die veilige bedryf van die TOE kan benadeel.

3.4 Voorstellingsmeganisme

Soos wat die geval met die kriteria vir die Oranje Boek is, bestaan daar nie 'n duidelike konseptuele voorstellingsmeganisme vir die evaluering van 'n produk volgens die Wit Boek se kriteria nie. Die meganisme wat deur die skrywer voorgestel word, is eweneens 'n roosdiagram wat op dieselfde beginsel as die voorstellingsmeganisme vir die Oranje Boek berus (sien paragraaf 2.3).

Die voorstellingsmeganisme verskil egter in die volgende opsigte van die een wat vir die Oranje Boek gebruik is :

- Aangesien daar 'n duidelike onderskeid gemaak word tussen die vereistes vir funksionaliteit en versekering in die Wit Boek, word twee afsonderlike roosdiagramme gebruik om die onderskeie vereistes (soos gedefinieer in die ITSEC, bylae B) voor te stel.

- Die vyf nie-hiërargiese klasse van die Wit Boek (F6 - F10) kan nie logies in die vorm van konsentriese sirkels voorgestel word nie. Hierdie klasse word derhalwe deur 'n **een-dimensionele matriks** met vyf blokke (een vir elke klas) voorgestel (figuur 2.6). Indien die produk aan die vereistes vir 'n spesifieke klas voldoen, word die ooreen-

stemmende blok ingekleur.

- Die **funksionaliteitsdiagram** bestaan uit vyf konsentriese sirkels (klasse F1 - F5) en vyf segmente, terwyl die **versekeringsdiagram** uit ses konsentriese sirkels (E1 - E6) en tien segmente bestaan (figuur 2.6 en figuur 2.7).

Vir die doeleindes van die voorbeeld word 'n denkbeeldige produk B gekies. Die sekerheidsvereistes en die klasse waaraan die produk voldoen, word in tabel 2.2, tabel 2.3 en tabel 2.4 uiteengesit (sien bylae B vir 'n opsomming van die vereistes). Figuur 2.8 toon die deursigtige roosdiagramme en een-dimensionele matriks vir produk B t.o.v. die sekerheids-vereistes van die Wit Boek, terwyl figuur 2.9 die ingekleurde roosdiagramme en matriks toon.

Sekerheidsvereiste	**Sekerheids-klas**
Identifikasie en verifikasie	B2
Toegangsbeheer	A1
Aanspreeklikheid	A1
Oudit	A1
Objek hergebruik	A1

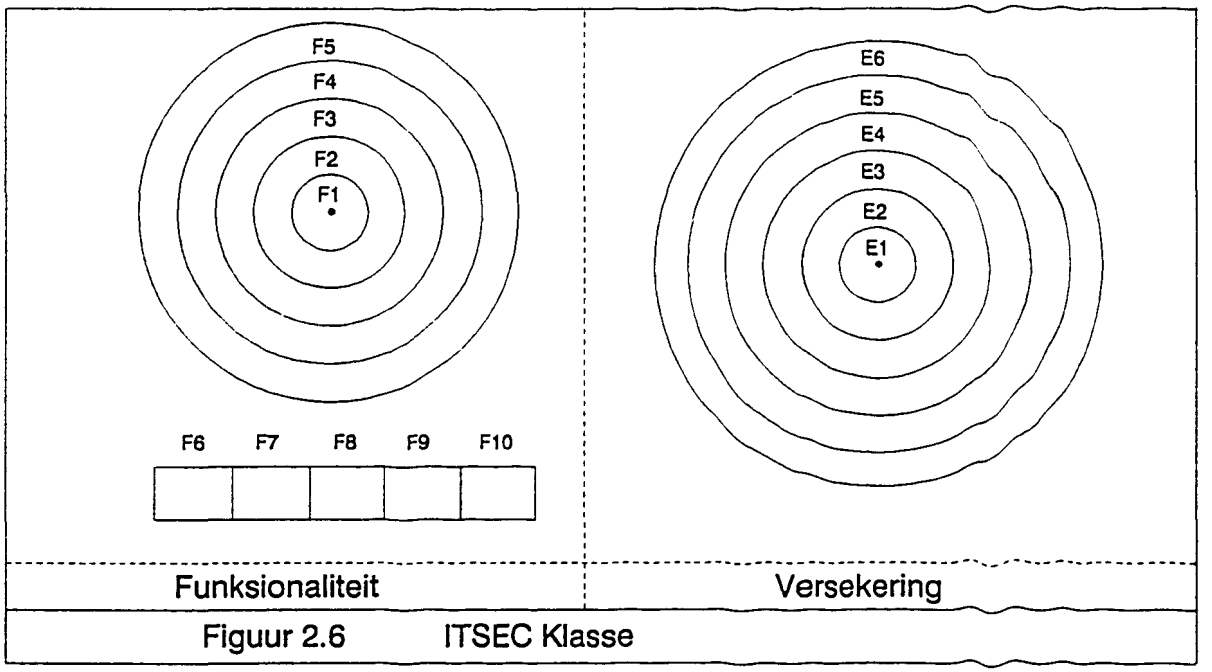
TABEL 2.2 EVALUERING VAN PRODUK B - FUNKSIONALITEIT (Hiërargies)

Sekerheidsklas	**Voldoen (Ja/Nee)**
F6	Nee
F7	Nee
F8	Ja
F9	Ja
F10	Ja

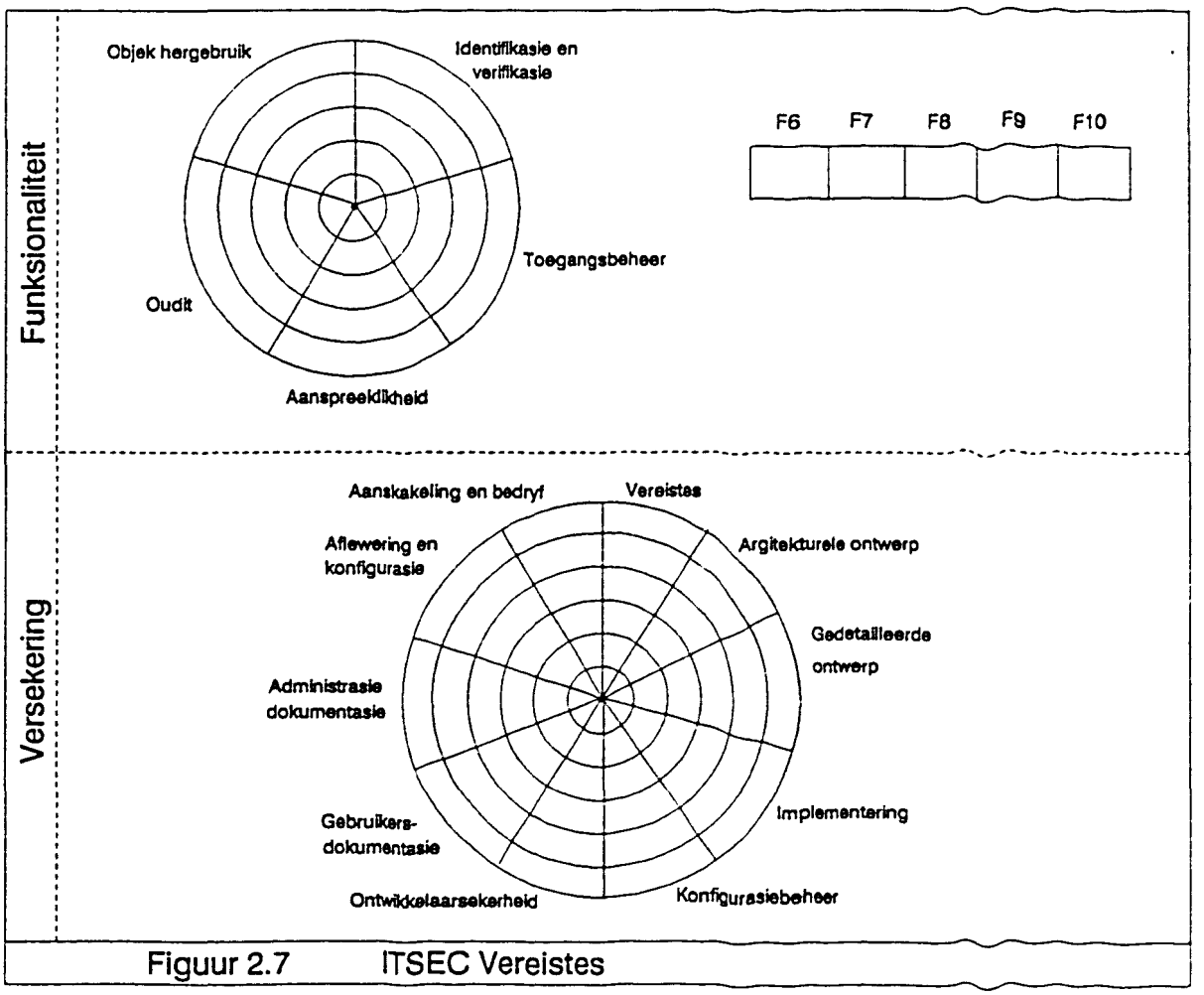
TABEL 2.3 EVALUERING VAN PRODUK B - FUNKSIONALITEIT (Nie-Hiërargies)

Sekerheidsvereiste	Sekerheids-klas
Vereistes	E3
Argitekturele ontwerp	E3
Gedetailleerde ontwerp	E3
Implementering	E4
Konfigurasiebeheer	E3
Ontwikkelaarsekerheid	E6
Gebruikersdokumentasie	E4
Administrasie dokumentasie	E6
Aflewering en konfigurasie	E4
Aanskakeling en bedryf	E6

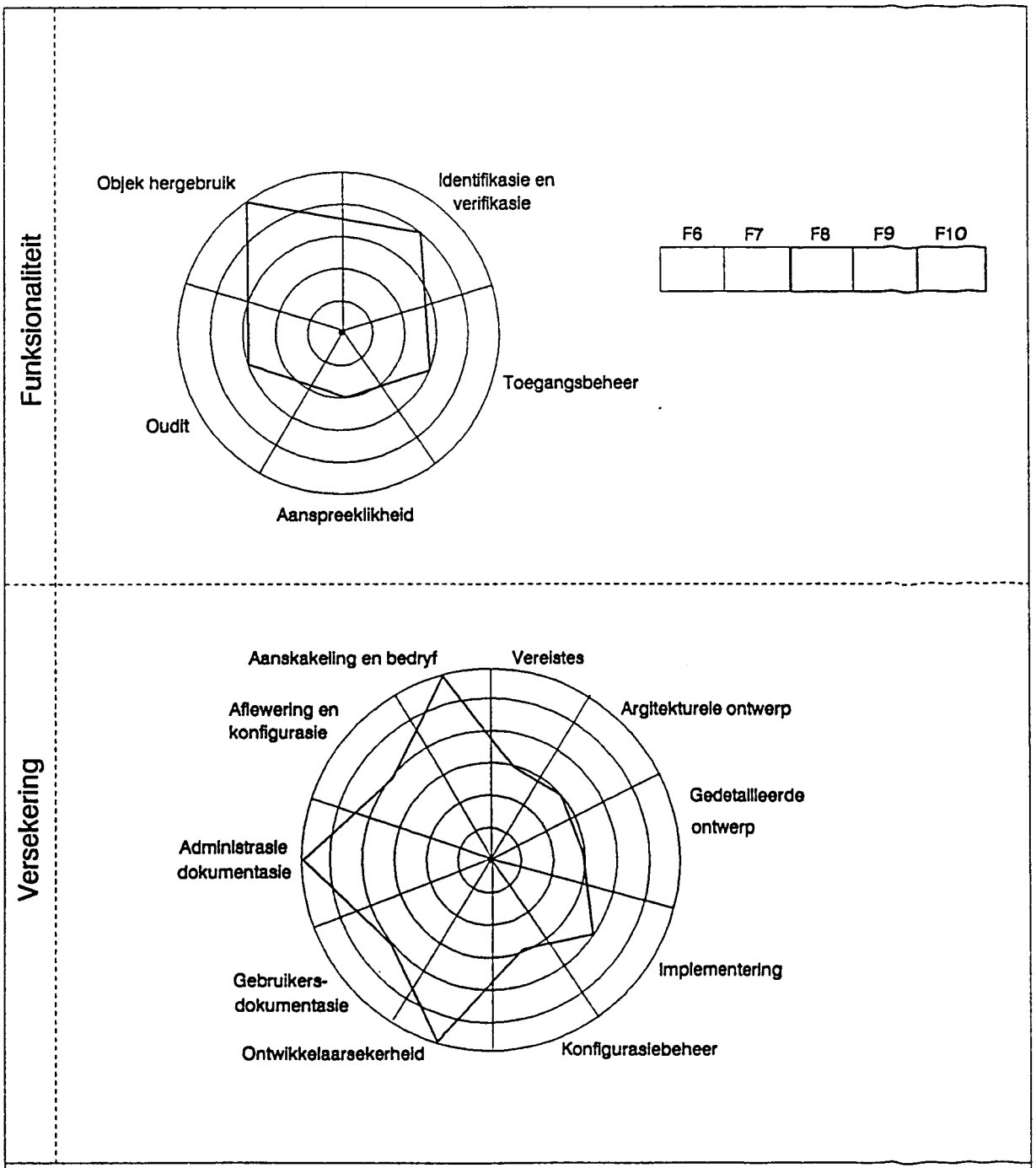
TABEL 2.4 EVALUERING VAN PRODUK B - VERSEKERING (Hiërargies)



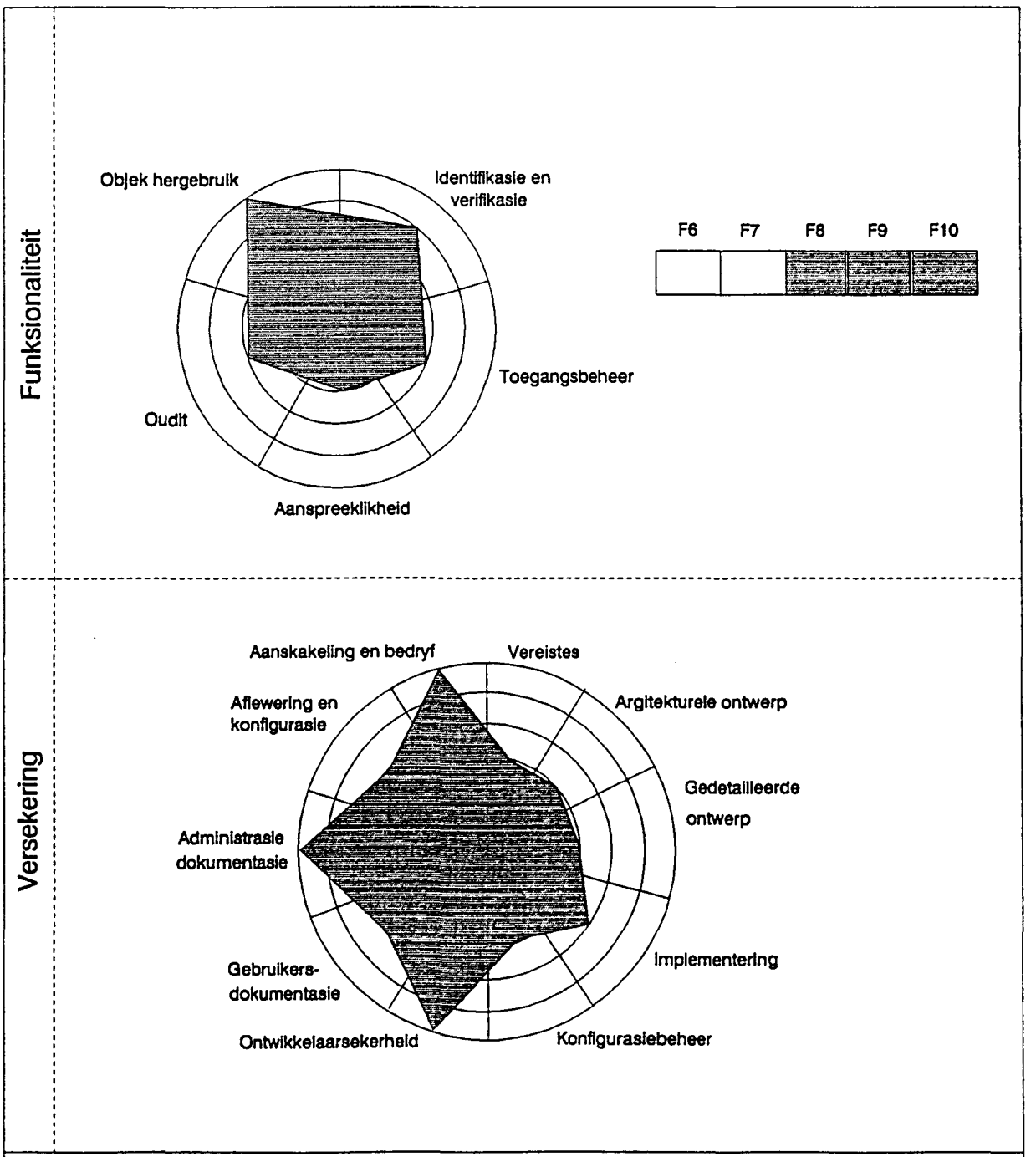
Figuur 2.6 ITSEC Klasse



Figuur 2.7 ITSEC Vereistes



Figuur 2.8 Evaluering van produk B volgens ITSEC vereistes (deursigtig)



Figuur 2.9 Evaluering van produk B volgens ITSEC vereistes

4. VERGELYKING VAN ORANJE BOEK EN WIT BOEK

'n Duitse studiegroep, die VDMA/ZVEI werksgroep, het op aanbeveling van die EUROBIT Industriële Beleid groep begin met 'n projek om die TCSEC en ITSEC kriteria te vergelyk met die doel om een universele standaard daar te stel [5]. Die metode wat gebruik is, is om die funksionaliteits- en versekeringsaspekte vir elke standaard te modulariseer (d.w.s. in basiese komponente op te breek), hierdie basiese komponente te vergelyk en dan saam te voeg in een superstel.

Alhoewel die vergelyking net vir spesifieke funksionaliteits- en versekeringsvereistes gedoen is, blyk die metode wat gevolg word suksesvol te wees, en is die aanbeveling van die werksgroep dat 'n internasionale groep voltyds die taak moet aanpak om die twee standaarde saam te voeg. [5]

Daar is egter 'n paar fundamentele verskille tussen die Oranje Boek en die Wit Boek, wat vervolgens opgesom word.

In die Oranje Boek word beide die funksionaliteitseienskappe en die versekeringsattribute beliggaam in die vereistes vir elke afdeling en klas. Dit verteenwoordig 'n hoogs **gebondelde benadering** tot die kriteria aangesien die een klas tegelykertyd funksionaliteit en versekering voorstel. In hierdie opsig is die kriteria wat in die Wit Boek vervat word, meer ongebondeld in dié sin dat funksionaliteitsvereistes in klasse F1 tot F10 verdeel word, en versekeringsvereistes in vlakke E0 tot E6. In die geval van die Wit Boek kan daar dus meer definitief gespesifiseer word in watter mate die betrokke TOE aan die verskillende vereistes voldoen. [15] [70]

'n Tweede belangrike verskil is dat die Oranje Boek, soos vroeër in paragraaf 2.3 bespreek, min aandag gee aan die beginsels van **integriteit** en **beskikbaarheid**. Daarteenoor konsentreer die nie-hiërargiese klasse F6 tot F10 van die Wit Boek juis op die beginsels van integriteit en beskikbaarheid,

hetsy binne 'n stelsel of tydens data-uitruiling tussen stelsels.

'n Derde verskil is dat waar die Oranje Boek pertinent 'n **beskermde domein** in die stelselargitektuur vereis vir die uitvoering van sekerheidsrelevante funksies, die Wit Boek geen modulariteit m.b.t. die stelselargitektuur vereis nie. Laasgenoemde vereis dus nie dat die sekerheidsrelevante dele van die stelsel in 'n TCB geïsoleer word nie. [70]

Vierdens plaas die Wit Boek geen beperking op die **funksionaliteit** van 'n stelsel wat geëvalueer word nie, en kan enige geskikte **spesifikasiestyl** ook gebruik word [51]. Hierteenoor is die Oranje Boek se vereistes baie nougeset in die funksies wat aangespreek word, en kan 'n stelsel waarvan die funksionaliteit verder as die Oranje Boek se dekking strek, nie sinvol geëvalueer word nie [70]. Waar die Oranje Boek te beperkend in die vereistes is wat gestel word, loop die Wit Boek die gevaar om te algemeen te wees in die spesifikasie van vereistes. [15]

'n Vyfde belangrike verskil is dat die Oranje Boek primêr fokus op **bedryfstelsels**, terwyl die Wit Boek fokus op produkte en stelsels. [5] [92]

Die klaarblyklike voordele van die Wit Boek bo die Oranje Boek is die volgende:

- Die Wit Boek dek al drie komponente van rekenaarsekerheid, naamlik vertroulikheid, integriteit en beskikbaarheid.

- Die Oranje Boek en die ander boeke in die Reënboog Reeks is gerig op die behoeftes van regerings- en verdedigingsstelsels, terwyl die Wit Boek wyer toepasbaar is en sowel 'n geklassifiseerde regeringsomgewing as 'n ongeklassifiseerde kommersiële omgewing dek. [11]

- Die Wit Boek onderskei pertinent tussen funksionaliteits- en versekeringsvereistes, wat waarskynlik van groter nut sal wees vir die ontwikkeling van 'n model.

- Die Wit Boek bied meer buigbaarheid in die sin dat die vereistes uitgebrei en aangepas kan word na gelang van spesifieke omstandighede.

- Aangesien die Wit Boek se kriteria ontwerp is met spesifieke inagneming van die Oranje Boek en die klasse D tot A1 op die Wit Boek se klasse en vlakke afgebeeld kan word, blyk dit dat die Wit Boek se kriteria meer omvattend is.

Die skrywer volstaan met hierdie bespreking van die TCSEC en die ITSEC. In die volgende hoofstuk word 'n kategoriseringsmeganisme vir beheermaatreëls voorgestel en bespreek met die oog op die koppeling daarvan met standaarde in die daaropvolgende hoofstukke.

HOOFSTUK 3

'N KATEGORISERINGSMEGANISME VIR BEHEERMAATREëLS

In hoofstuk 2 is standaarde vir beheermaatreëls bespreek met spesifieke verwysing na die Oranje Boek en die Wit Boek. Die doel van hierdie hoofstuk is om die belangrikste beheermaatreëls wat vir die handhawing van rekenaarsekerheid gebruik word, te identifiseer, te kategoriseer en kortliks te beskryf. In hoofstuk 4 sal standaarde vir beheermaatreëls gekombineer word met die verskillende kategorieë beheermaatreëls wat in hierdie hoofstuk geïdentifiseer word.

Die kategoriseringsmeganisme wat gebruik word ter indeling van hierdie hoofstuk is deur die skrywer ontwikkel. In die ondersoek na beheermaatreëls het die skrywer gevind dat daar 'n definitiewe leemte in die literatuur bestaan betreffende 'n duidelike en volledige kategorisering van beheermaatreëls.

Die kategoriseringsmeganisme word in figuur 3.1 uiteengesit. Die meganisme bestaan uit vyf kategorieë en drie hiërargiese vlakke van beheermaatreëls.

Vir die doeleindes van hierdie studie definieer die skrywer **beheermaatreëls** binne die konteks van rekenaarsekerheid as:

> **Die versameling prosedures en standaarde wat ten doel het om die vertroulikheid, integriteit, en beskikbaarheid van 'n organisasie se inligtingsbates te beskerm.**

Prosedures verwys na alle tegnieke, hetsy administratiewe reëlings, logiese programmatuur- of apparatuurfunksies, of fisiese toestelle wat binne die raamwerk van rekenaarseker-

heid gebruik word.

Standaarde verwys na vereistes, reëls en regulasies wat van toepassing is op 'n organisasie se fisiese bates, inligtingsbates en personeel.

Inligtingsbates is alle data, programmatuur en apparatuur wat die totale inligtingstelselsfunksie van 'n organisasie vorm.

Vertroulikheid, integriteit en beskikbaarheid is reeds in hoofstuk 1 par. 1.1 gedefinieer.

Die **vyf kategorieë** waarin beheermaatreëls verdeel word, is die volgende:

- Toepassingsekerheid maatreëls
- Logiese sekerheid maatreëls
- Verspreide stelsels sekerheid maatreëls
- Fisiese sekerheid maatreëls
- Administratiewe maatreëls

Die definisie van hierdie kategorieë sluit aan by Badenhorst [6] se definisie van rekenaarsekerheid. (Sien ook hoofstuk 1 par. 1.1).

Toepassingsekerheid maatreëls is beheermaatreëls wat gerig is op aspekte rakende die ontwikkeling en onderhoud van toepassingstelsels, met die doel om betroubare, maklik-onderhoubare programme daar te stel, met die nodige interne kontroles wat beheer uitoefen oor die gebruik daarvan.

Logiese sekerheid maatreëls is beheermaatreëls wat gerig is op die beskerming van data en programme wat in die rekenaarstelsel geberg word.

Verspreide stelsels sekerheid maatreëls is beheermaatreëls wat toegepas word om data te beskerm tydens data-uitruiling tussen verskillende stelsels, substelsels of stelselkompo-

nente.

Fisiese sekerheid maatreëls is beheermaatreëls wat ten doel het om die fisiese beskadiging van of toegang tot rekenaarstelselkomponente te voorkom.

Administratiewe maatreëls is beheermaatreëls wat gerig is op die suksesvolle implementering van toepassing-, logiese, verspreide stelsels en fisiese sekerheid, en wat toegepas word deur organisatoriese konvensies, reëls en regulasies.

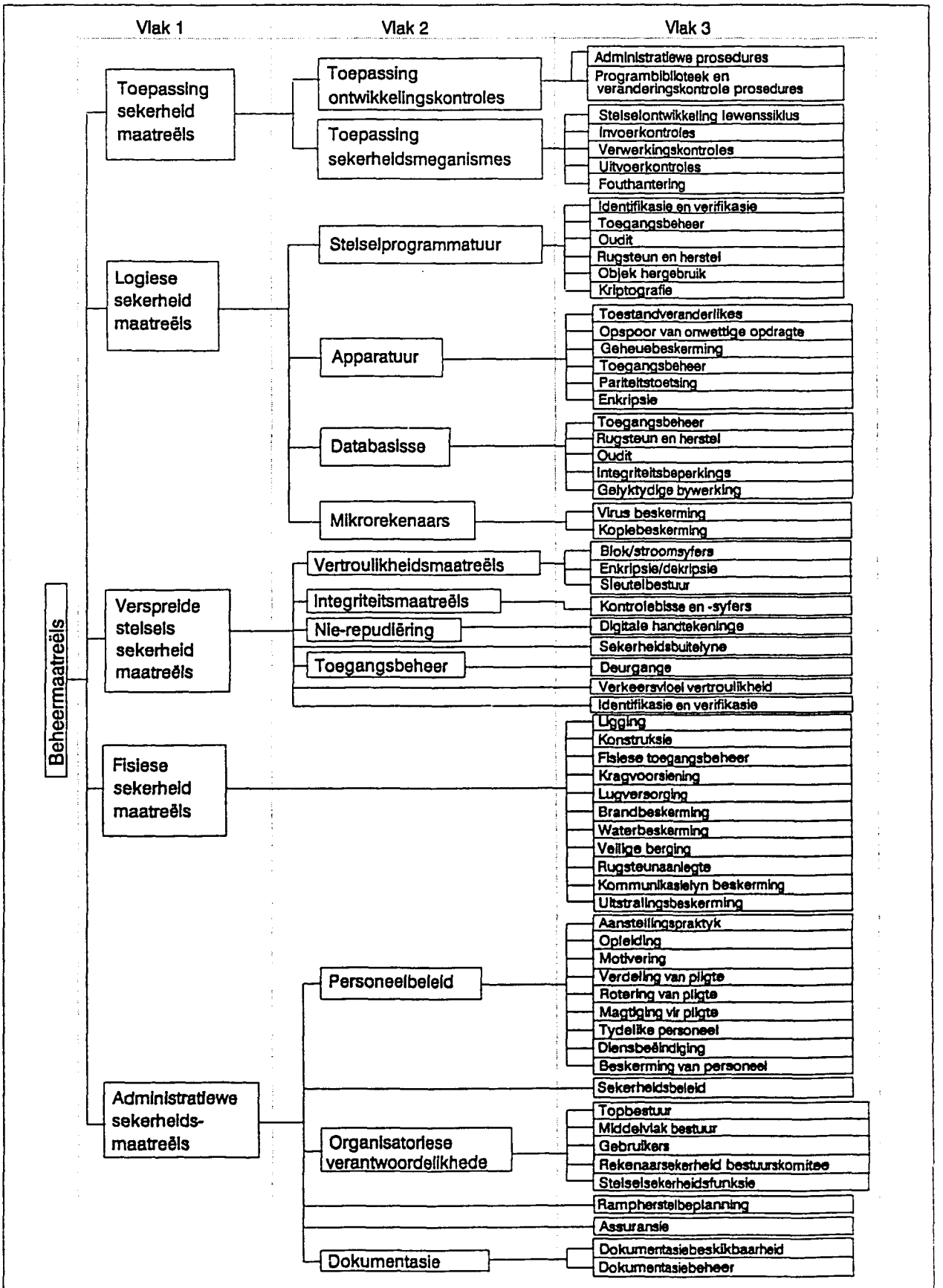
Elke kategorie word soos volg in **drie vlakke** verdeel:

- **Vlak 1** beskryf elke kategorie op die hoogste vlak. Op hierdie vlak word daar slegs 'n onderskeid getref tussen die vyf basiese kategorieë soos wat dit hierbo uiteengesit is.

- **Vlak 2** beskryf elke kategorie in meer detail deur van subkategorieë gebruik te maak. Hierdie subkategorieë dien slegs as verdere verfyning van die basiese kategorie, en verteenwoordig nie die werklike beheermaatreëls nie.

- **Vlak 3** definieer die beheermaatreëls soos wat dit binne elke kategorie en/of subkategorie voorkom.

Tompkins et al. [86] en Wood [99] identifiseer 'n aantal eienskappe waaraan beheermaatreëls moet voldoen. Hierdie eienskappe is van toepassing op al vyf bogenoemde kategorieë, en word in gekonsolideerde vorm in tabel 3.1 opgesom.



Figuur 3.1 'n Kategoriseringsmeganisme vir beheermaatreëls

Korrektheid	'n Beheermaatreël moet aan die spesifikasies en doelwitte wat daarvoor gestel is, voldoen.
Betroubaarheid	'n Beheermaatreël moet die betrokke funksie met die vereiste presisie uitvoer.
Doeltreffendheid	Die minimum hoeveelheid rekenaarhulpbronne en kode moet deur die beheermaatreël benodig word om sy funksie uit te voer.
Integriteit	Wysiging van 'n beheermaatreël deur ongemagtigde persone moet verhoed word.
Bruikbaarheid	Die minimum tyd en moeite moet benodig word om die beheermaatreël te leer, te hanteer, invoer voor te berei en die uitvoer daarvan te interpreteer.
Onderhoubaarheid	Die minimum tyd en moeite moet benodig word om 'n fout in die beheermaatreël op te spoor en reg te stel, of om die impak van ander stelselveranderings daarop te bepaal.
Toetsbaarheid	'n Beheermaatreël moet relatief maklik getoets en geoudit kan word ten einde te verseker dat dit die korrekte funksie verrig.
Buigsaamheid	Die werking van 'n beheermaatreël moet met relatief min moeite aangepas kan word by veranderde omstandighede.
Integreerbaarheid	'n Beheermaatreël moet maklik met die bestaande stelsels geïntegreer kan word.
Koste-effektiwiteit	'n Beheermaatreël se koste moet minder wees as die gevolglike afname in die verwagte verlies.
Eenvoud	Hoe eenvoudiger 'n beheermaatreël is, hoe minder tyd sal aan die ontwerp, implementering, bedryf en instandhouding daarvan bestee word.
Minste voorreg ("Least Privelege")	Beheermaatreëls moet gebaseer word op die beginsel dat die minimum fasiliteite of inligting wat nodig is aan die betrokke partye besikbaar gestel word.
Onafhanklikheid van beheer en subjek	Die persoon wat verantwoordelik is vir die ontwerp, implementering en/of bedryf van die beheermaatreël moet nie dieselfde persoon wees wat daardeur beheer moet word nie.
Universele toepasbaarheid	'n Beheermaatreël moet konsistent en omvattend toegepas word oor die spektrum van omgewings, stelsels en persone wat beheer moet word.
Aanvaarding van beheer deur subjekte	Gebruikers en ander persone wat aan 'n beheermaatreël onderwerp word, moet die maatreël aanvaar as positiewe beheer.
Ouditeerbaarheid	Beheermaatreëls moet genoegsame bewys versamel om aan te toon dat dit korrek werk en enige pogings om dit te omseil, opspoor en aanteken.
Diepte van verdediging	Veelvoudige, oorvleuelende beheermaatreëls wat een bate beskerm, verskaf groter sekerheid.
Isolering en kompartementering	Bates word verdeel in verskillende groepe, elk met sy eie beheermaatreëls, sodat omseiling of faling van een beheermaatreël nie alle bates kompromitteer nie.
Randbeheer	'n Groter mate van sekerheid word verkry deur indringing op te spoor en te voorkom by die buiterand van die stelsel.
Versuim na weiering	Wanneer 'n beheermaatreël faal, moet toegang aan gebruikers wat die diens benodig, geweier word.
Parameter-gebaseerdheid	Beheermaatreëls is meer effektief en aanpasbaar indien veranderlikes in plaas van konstantes gebruik word in die ontwerp daarvan.
Vyandige omgewing	Beheermaatreëls moet ontwerp word met die oog op 'n omgewing waar die mees ongunstige scenario van toepassing is in terme van o.a. die eerlikheid en vermoë van gebruikers.

TABEL 3.1 EIENSKAPPE VAN BEHEERMAATREëLS

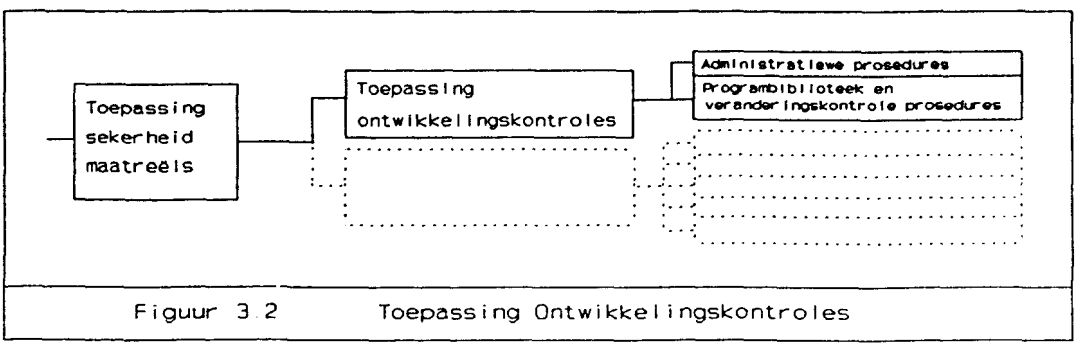
1. TOEPASSINGSEKERHEID MAATREëLS

Die sekerheid van toepassings kan op twee wyses verhoog word. Eerstens moet toepassings op 'n veilige wyse ontwikkel en in stand gehou word om te verseker dat die moontlikheid van opsetlike of onopsetlike foute in die toepassings geminimaliseer word, en dat daar geen prosedures in toepassings ingesluit word wat die vertroulikheid, integriteit of beskikbaarheid daarvan kan kompromitteer nie. Die maatreëls waardeur dit verseker word, staan bekend as **toepassing ontwikkelingskontroles.**

Tweedens moet toepaslike sekerheidsmeganismes ontwikkel en in die toepassings ingesluit word. Na hierdie meganismes word verwys as **toepassing sekerheidsmeganismes.**

1.1 Toepassing Ontwikkelingskontroles

Toepassing ontwikkelingskontroles verwys na **prosedures en standaarde** wat toegepas word in die ontleding, ontwerp, implementering, toetsing en instandhouding van nuwe stelsels en programme. Die skrywer onderskei tussen administratiewe prosedures en programbiblioteek en veranderingskontrole prosedures.



Figuur 3.2 Toepassing Ontwikkelingskontroles

1.1.1 Administratiewe Prosedures

Administratiewe prosedures verwys na organisatoriese reëls en regulasies wat toegepas word tydens die ontwikkeling van toepassings. Die belangrikste beheermaatreëls is die volgende [74] [56] [22]:

- **Betrokkenheid** van die gebruikersafdeling en interne oudit afdeling tydens goedkeuring van stelselontwikkelingsprojekte, opstel van stelselspesifikasies en ontwikkeling van die stelsel.

- **Standaarde** van ontwikkeling, d.w.s. ontwerp, dokumentasie, styl, taal, programmering, toetsing en konfigurasiebestuur moet ontwikkel en toegepas word.

- **Verdeling** van die taak tussen 'n aantal programmeerders.

- Gesamentlike **evaluering** van die totale bronkode deur die groep programmeerders.

- **Modulariteit** - skryf die program in modules wat elk 'n afsonderlike, redelik onafhanklike funksie verrig.

- **Enkapsulering** - afbakening van die grense van elke module en definiëring van duidelike koppelvlakke.

- **Inligtingverberging** - ander programmeerders moet slegs weet wat 'n module doen, en nie hoe dit gedoen word nie.

- **Onafhanklike toetsing**, m.a.w. toetsing deur ander persone as dié wat die toepassing geskryf het, veral gebruikers en interne ouditeure.

- **Konfigurasiebestuur** - Enige veranderings aan programme of roetines moet deeglik goedgekeur, getoets, geïmplementeer en gedokumenteer word.

- Program/stelsel veranderings moet bestuur word deur 'n **veranderingskontrole komitee**.

- Veranderings moet gedoen word volgens voorafbepaalde **prosedures** en deur **gemagtigde persone**.

- 'n **Logboek** met relevante inligting oor alle veranderings aan die stelsel/program moet gehou word.

- Daar moet verseker word dat alle toepassings aan vasgestelde standaarde voldoen deur gebruik te maak van **sekerheidsoudits**.

1.1.2 Programbiblioteek en Veranderingskontrole Prosedures

'n Programbiblioteek en veranderingskontrole prosedures kan gebruik word as hulpmiddel om toepassing ontwikkelingskontroles te implementeer.

'n **Programbiblioteek** is 'n programmatuurpakket wat programweergawes outomaties katalogiseer en beheer ten einde te verseker dat die korrekte weergawe gebruik word vir produksielopies. Slegs programme wat deeglik gedokumenteer, hersien, getoets en goedgekeur is, behoort in die produksiebiblioteek opgeneem te word.

Veranderingskontrole prosedures word gebruik om die eienskappe van die pakket te implementeer vir sekerheidsdoeleindes. Die pakket bied funksies soos die volgende [86] [56]:

- Stoor en toetsing van programme wat ontwikkel word of gewysig word, sonder om produksieprogramme te versteur.

- Verbied verwerking van lewendige data deur programme en stelsels wat nie in die produksiebiblioteek aangehou word nie.

- Onderhou 'n op-datum voorraadlys van alle produksieprogramme en -stelsels.

- Onderhou 'n logboek van alle verandering aan die produksiebiblioteke.

- Stel en onderhou program/stelsel benamingskonvensies en 'n weergawe-nommerstelsel.

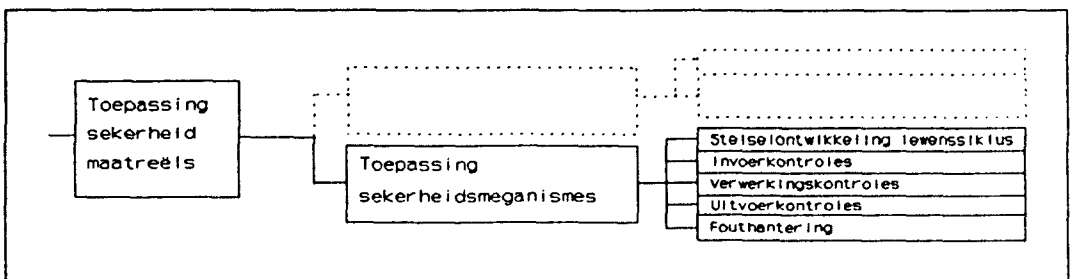
- Vereis spesiale magtiging om produksieweergawes van programme te verander.

- Geënkripteerde berging van produksieweergawes van programme.

1.2 Toepassing sekerheidsmeganismes

Toepassing sekerheidsmeganismes verwys na **prosedures en funksies** wat in toepassings ingesluit word, en waarvan die uitvoering bydra om die vertroulikheid, integriteit en/of beskikbaarheid van die toepassing en die data wat dit verwerk, te verseker.

Daar word eerstens gekyk na die ontwikkeling van sodanige meganismes, waarna die belangrikste meganismes bespreek word.



Figuur 3.3 Toepassing sekerheidsmeganismes

1.2.1 Stelselontwikkeling Lewenssiklus

Die **stelselontwikkeling lewenssiklus** ("System Development Life Cycle - (SDLC)") verskaf 'n struktuur om te verseker dat sekerheidsmeganismes beplan, ontwerp, ontwikkel en getoets word op 'n wyse wat ooreenstem met die sensitiwiteit van die toepassing en/of data. Tompkins et al. [86] identifiseer 'n aantal sekerheidsaktiwiteite wat tydens die SDLC gedoen moet word (sien tabel 3.2).

Die **programmatuur kwaliteitsversekering proses** verskaf die evaluerings- en ouditte*gnieke om te verseker dat die aktiwiteite wat tydens die SDLC uitgevoer word, operasioneel effektiewe veiligheidsmaatreëls lewer. Die sekerheidsaktiwiteite wat tydens die programmatuur kwaliteitsversekering proses gedoen moet word, bestaan uit die hersiening en evaluering van die sekerheidvereistes, ontwerp, spesifikasies, en toetsgereedheid, asook 'n oorsig oor die sekerheidstoets en evalueringsproses. [86]

1.	Bepaal die sensitiwiteit van die data of toepassing
2.	Bepaal die sekerheidsdoelwitte van die stelsel
3.	Identifiseer die sekerheidsrisiko's
4.	Doen 'n sekerheidsuitvoerbaarheid studie
5.	Definieer die sekerheidsvereistes
6.	Ontwikkel die sekerheidstoetsplan
7.	Ontwerp sekerheidspesifikasies
8.	Integreer sekerheidspesifikasies met toepassingspesifikasies
9.	Ontwikkel die sekerheidstoetsprosedures
10.	Skryf sekerheidsrelevante kode
11.	Dokumenteer die sekerheidsmeganismes
12.	Doen sekerheidstoetsing en -evaluering
13.	Skryf die sekerheid toetsontledingsverslag
14.	Berei die sekerheidsertifikasieverslag voor

TABEL 3.2 SEKERHEIDSAKTIWITEITE TYDENS DIE SDLC

1.2.2 Invoerkontroles

Die doel van invoerkontroles is om die volledigheid, akkuraatheid en integriteit van die invoertransaksies vanaf brondokumente na rekenaar-leesbare vorm te verseker. Hierdie kontroles moet ook die voorkoming, opsporing en korreksie van foute tydens die invoerproses verseker. Invoerkontroles kan hoofsaaklik verdeel word in brondokument kontroles en data-omskakeling en invoer.

Brondokument kontroles sluit die volgende in [56] [30]:

- Gebruik spesiaal ontwerpte vorms met voorafgedrukte inligting en sekwensiële dokumentnommers.

- Hou streng beheer oor alle invoervorms, veral dié wat sensitiewe inligting bevat, en vernietig dit na die voorafbepaalde tyd.

- Onderhou logboeke van vorms wat gebruik word.

Data-omskakeling- en invoerkontroles sluit die prosesse en funksies in waardeur die invoer transaksie-inligting na rekenaar-leesbare formaat omgeskakel word [86] [30] [95]. Voorbeelde hiervan is:

- Kontroletotale om te verseker dat die data volledig en akkuraat ingevoer is.

- Rekordtellings wat bv. die aantal rekords ingevoer vergelyk met die aantal oorspronklike rekords.

- Kontrolevelde in rekords om die integriteit van die rekords te verseker.

- Waardebeperkings wat op die data wat in sekere velde gehou kan word, geplaas word.

1.2.3 Verwerkingskontroles

Verwerkingskontroles is gerig op validering (d.i. die toetsing vir geldigheid) van die invoertransaksies en lêers, validering van die verwerking van die inligting, en die verskaffing van die nodige verslae en lyste. Die belangrikste beheermaatreëls is bondelbalansering, dataredigering, datavalidering en verslae en lyste. [56]

In die geval van bondelverwerking word **bondelbalansering** gedoen ten einde die integriteit van die invoerinligting te verifieer, deur o.a. van kontroletotale gebruik te maak.

Dataredigering behels die toetsing van karakters, velde en transaksies vir geldigheid en aanvaarbaarheid, en die redigering van foutiewe data.

Datavalidering word deur die toepassingsprogram gedoen om te verseker dat verwerking met die korrekte lêers gedoen word en dat sodanige verwerking volledig en behoorlik gedoen word.

Alle foute en probleme wat tydens die verwerkingsproses opgespoor word, word in **verslae en lyste** opgesom met die oog op latere ontleding en regstelling. Voorbeelde van sulke verslae is 'n ouditspoor van alle transaksies ingedien vir verwerking, aanvaarde transaksies, verwerpte transaksies, veranderings aan die meesterlêer, en sensitiewe transaksies.

1.2.4 Uitvoerkontroles

Die doel van uitvoerkontroles is om die akkuraatheid en integriteit van die verwerkte inligting te verifieer en om te verseker dat uitvoer slegs na die toepaslike gemagtigde personeel versprei word. Die belangrikste beheermaatreëls is uitvoerverspreiding, uitvoerrekonsiliasie, en behoud van uitvoer. [56]

Uitvoerverspreiding beheermaatreëls is gerig daarop om te verseker dat slegs gemagtigde personeel uitvoer ontvang, dat

sodanige uitvoer akkuraat en volledig is, en dat dit tydig ontvang word.

Uitvoerrekonsiliasie het ten doel om te verifieer dat die integriteit van invoertransaksies nie verlore gegaan het tydens verwerking nie, dat verwerking akkuraat en volledig gedoen is en dat hierdie akkuraatheid in die uitvoer weerspieël word.

Behoud van uitvoer behels eerstens dat die periodes vir die behoud van uitvoerverslae, lyste en kopieë van uitvoerdokumente duidelik gedefinieer en gedokumenteer word. Hierdie periodes word beïnvloed deur wetlike vereistes, maatskappybeleid en vereistes vir effektiewe bedryf. Na afloop van die bepaalde periode moet die uitvoer vernietig word deur bv. versnippering of verbranding.

1.2.5 Fouthantering

Fouthanteringsprosedures is prosedures waardeur data wat vroeër foutief ingevoer is, gekorrigeer word in die data- en meesterlêers. Die belangrikste beheermaatreëls is foutopsporing, foutregstelling en foutontleding. [17] [56]

Foutopsporing word gedoen met behulp van prosesverslae wat as gevolg van foute en probleme tydens verwerking geproduseer word.

Foutregstelling behels die regstelling van alle geïdentifiseerde foute en is onderhewig aan al die beheermaatreëls wat geld vir data-invoer. 'n Foutkontrole logboek en regstellingskontrole logboek bevat al die relevante inligting aangaande foute en regstellende aksies.

Deur **foutontleding** word die bronne, aard, frekwensie en tyd van spesifieke soorte foute ontleed ten einde probleme in die stelsel of moedswillige aanvalle op die stelsel op te spoor.

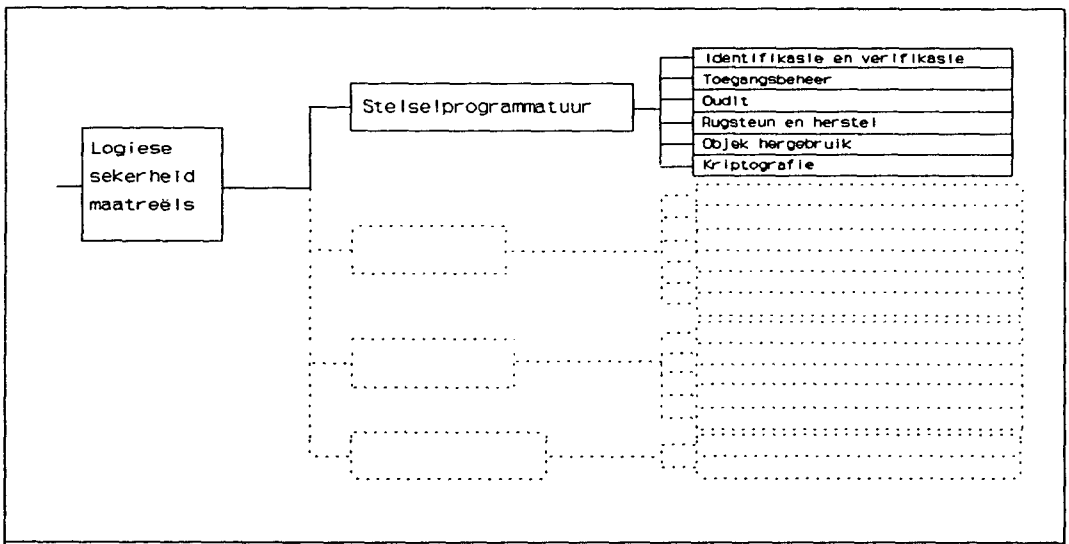
2. LOGIESE SEKERHEID MAATREëLS

Beheermaatreëls vir logiese sekerheid het ten doel om die sekerheid van data en programme wat in 'n rekenaarstelsel geberg word, te verseker. Logiese sekerheid maatreëls word op hoofsaaklik vier vlakke geïmplementeer, nl. stelselprogrammatuur, apparatuur, databasisse en mikrorekenaars. Alhoewel sommige beheermaatreëls op meer as een kategorie van toepassing is, word maatreëls in die kategorie geplaas waarop dit in die grootste mate van toepassing is.

2.1 Stelselprogrammatuur

Stelselprogrammatuur beheermaatreëls kan gedefinieer word as sekerheidsdienste wat deur die **bedryfstelsel** en **geassosieerde nutsroetines** verskaf word. Die beheermaatreëls kan deur die vervaardiger as deel van die bedryfstelsel verskaf word, of dit kan by die basiese bedryfstelsel gevoeg word in die vorm van 'n sekerheidspakket. [17] [101]

Die voordeel daarvan om sekerheidsfasiliteite in die stelselprogrammatuur in te sluit, is dat dit nie nodig sal wees vir alle toepassings om self sekerheidsdienste te verskaf nie. Sodoende word die TCB klein en onderhoubaar, met uniforme toepassing van sekerheidsreëls. Dit is verder moeiliker vir stelselgebruikers en programmeerders om beheermaatreëls op die vlak van stelselprogrammatuur te omseil. [70] [101]



Figuur 3.4 Stelselprogrammatuur

2.1.1 Identifikasie en Verifikasie

Identifikasie en verifikasie is een van die mees basiese vereistes vir 'n veilige stelsel. Die doel daarvan is dat twee verskillende entiteite, bv. 'n gebruiker en 'n stelsel of twee verskillende nodes in 'n netwerk, mekaar sonder enige twyfel uniek kan identifiseer as gemagtigde entiteite met wie daar op 'n bepaalde vlak van sekerheid gekommunikeer kan word. Daar word onderskei tussen gebruikeridentifikasie en -verifikasie en stelselidentifikasie en -verifikasie.

Gebruikeridentifikasie en -verifikasie

Die proses bestaan uit twee stappe. Ten eerste moet die gebruiker homself identifiseer deur 'n unieke eienskap. Tweedens moet die gebruiker aan die stelsel bewys dat hy wel is wie hy sê hy is, m.a.w. die stelsel moet sy identiteit kan verifieer. Verifikasiemeganismes val in drie kategorieë, nl. [74] [56] [42] [33] [45]:

- **Iets wat die gebruiker weet,** byvoorbeeld 'n wagwoord of enkripsiesleutel. 'n Voorbeeld van die gebruik van wagwoorde in netwerk- of hoofraamomgewings is **terugskakel-stelsels.** 'n Gebruiker identifiseer homself aan die

terugskakelstelsel, gewoonlik deur 'n wagwoord. Die stelsel verbreek dan die kommunikasielyn met die gebruiker, herwin die gebruiker se telefoonnommer of terminaaladres en skakel hom terug of inisieer weer die verbinding met die gebruiker.

- **Iets wat die gebruiker besit,** byvoorbeeld 'n geënkodeerde kaart soos 'n slimkaart ("smartcard") wat vir finansiële transaksies gebruik word. Die gebruiker plaas die kaart in 'n kaartleser wat aan 'n sentrale verwerker gekoppel is. Die verwerker verkry die gebruiker se rekeningnommer vanaf die kaart en versoek hom dan om 'n wagwoord in te sleutel wat met die rekeningnommer vergelyk word om die gebruiker se identiteit te verifieer.

- **Iets aangaande die gebruiker,** soos sy stem of handtekening. 'n Produk wat dinamiese handtekening verifikasie doen, is die Sign/On eenheid van Signify, Inc. Deur die eenheid met 'n sentrale databasis te koppel kan 'n onbeperkte aantal gebruikers geverifieer word deur fisies hul handtekening op die eenheid se blad aan te bring.

Stelselidentifikasie en -verifikasie

Die ander kant van gebruikersidentifikasie en verifikasie is stelselidentifikasie en verifikasie, en hoewel dit nie so dikwels gebruik word nie, is dit ewe belangrik. Daar word onderskei tussen stelsel-gebruiker en stelsel-stelsel meganismes. [74] [70]

- **Stelsel-gebruiker :** Net soos wat die gebruiker homself aan die stelsel as betroubaar moet bewys, moet die stelsel homself aan die gebruiker as betroubaar bewys, ten einde te verhoed dat die gebruiker vertroulike inligting aan 'n nagebootste stelsel bekend maak. Een stelselidentifikasiemetode is byvoorbeeld dat die stelsel persoonlike data aan die gebruiker vertoon soos sy vorige aanteken- en afteken-tye.

- **Stelsel-stelsel** : Wanneer twee stelsels of prosesse in verskillende veilige domeine met mekaar kommunikeer, is dit eweneens noodsaaklik dat die stelsels/prosesse mekaar kan identifiseer en verifieer. 'n Algemene meganisme wat gebruik word, is **vraag-antwoord** ("challenge-response") stelsels. Dit behels kortliks dat stelsel A byvoorbeeld 'n geënkripteerde identifikasie aan stelsel B stuur. Stelsel B dekripteer die boodskap met die gemeenskaplike enkripsiesleutel en indien stelsel A se identiteit duidelik blyk, stuur stelsel B 'n geënkripteerde identifikasie met 'n wagwoord aan A, waarna A stelsel B se identiteit kan verifieer. Die kernaspek van hierdie stelsel is dus die gemeenskaplike enkripsiesleutel waaroor beide A en B beskik.

2.1.2 Toegangsbeheer

Nadat 'n gebruiker toegang tot 'n stelsel verkry het, is dit steeds nodig om te bepaal of hy die reg het om sekere aksies uit te voer op objekte in die stelsel. Hierdie proses staan bekend as **toegangsbeheer** of magtiging, en is veral belangrik waar 'n aantal verskillende gebruikers toegang het tot gesentraliseerde data. Dit behels ook die prosedure waardeur 'n stelsel bepaal of sekere prosedures en programme gemagtig is om toegang tot ander programme en data te verkry. Dit sluit dus in die beheer van toegang deur alle **subjekte** tot alle **objekte** in die stelsel. Daar kan onderskei word tussen diskresionêre toegangsbeheer en verpligte toegangsbeheer as basiese metodes van logiese toegangsbeheer.

Diskresionêre toegangsbeheer stel die gebruiker in staat om toegang tot sy lêers en ander stelselobjekte te beperk volgens sy eie diskresie gebaseer op die identiteit van gebruikers en/of die groepe waaraan hulle behoort. Die spesifieke tipe toegang van elke subjek tot elke objek kan ook gespesifiseer word, waarvan die mees algemene tipes lees, skryf en uitvoer is. Daar bestaan verskillende meganismes waardeur diskresionêre toegangsbeheer toegepas word. Die

belangrikste daarvan is [74] [56] [54] [58]:

- **Self/Groep/Publieke** kontroles waardeur gebruikers in drie kategorieë verdeel word, naamlik die eienaar van 'n objek, spesifieke groepe wat toegang daartoe het, en ander gebruikers. Aan elke kategorie word daar dan spesifieke toegangsregte toegeken. Daar kan ook gespesifiseer word aan watter groepe of individue toegang tot spesifieke objekte geweier word.

- 'n **Gids** ("directory") wat vir elke subjek 'n lys van objekte spesifiseer waartoe die subjek toegang het, met die spesifieke toegangsregte tot elke objek.

- 'n **Toegangsbeheerlys** ("access control list") wat vir elke objek 'n lys van subjekte spesifiseer wat tot die objek toegang het, met elke subjek se spesifieke toegangsregte.

- 'n **Toegangsbeheermatriks** wat 'n kombinasie van die vorige twee meganismes is - 'n tabel waarin elke ry 'n subjek voorstel, elke kolom 'n objek en elke inskrywing die stel toegangsregte vir die subjek tot die objek.

- 'n **Vermoë** ("capability"), d.i. 'n nie-vervalsbare kenteken wat aan die houer daarvan sekere regte tot 'n objek gee, en wat oorgedra kan word aan 'n ander subjek.

- **Prosedure-georiënteerde toegangsbeheer** wat 'n prosedure implementeer wat toegang tot objekte beheer bo en behalwe die basiese toegangsbeheer wat deur die bedryfstelsel toegepas word.

Verpligte toegangsbeheer of nie-diskresionêre toegangsbeheer word veral deur stelsels toegepas wat uiters sensitiewe data verwerk. Hiervolgens word sensitiwiteitsetikette aan alle subjekte en alle objekte in die stelsel toegeken en alle besluite oor toegang word deur die stelsel geneem. 'n Subjek

(bv. gebruiker) se sensitiwiteitsetiket spesifiseer die vlak van vertroue wat met die subjek geassosieer word, terwyl 'n objek (bv. 'n lêer) se sensitiwiteitsetiket die vlak van vertroue wat 'n subjek moet hê om toegang daartoe te verkry, spesifiseer. Sensitiwiteitsetikette bestaan uit twee dele, nl. [74] [78]

- 'n **Hiërargiese klassifikasie** of rang, byvoorbeeld ongeklassifiseerd, vertroulik, geheim, of uiters geheim; en

- 'n **Nie-hiërargiese kategorie** of kompartement (bv. verkope), wat 'n projek of groep aandui waarvoor die betrokke data toeganklik is.

Verpligte toegangsbeheer prosedures word gebaseer op die Bell en LaPadula roostermodel wat die Basic Security Theorem genoem word. Die model pas twee belangrike toegangsreëls op 'n "need-to-know" basis toe. Die reëls is [74] [78]:

- Die **"Simple Security Property"**, wat bepaal dat :
  'n Subjek s mag slegs lees-toegang na 'n Objek o verkry as S(o) <= S(s), waar S(o) die sensitiwiteitsvlak van die objek o en S(s) die sensitiwiteitsvlak van die subjek s voorstel.

- Die **"*-Property"** of "star-property", wat bepaal dat :
  'n Subjek s wat lees-toegang tot 'n Objek o het, mag skryf-toegang tot 'n objek p verkry slegs as S(o) <= S(p), waar S(o) die sensitiwiteitsvlak van objek o en S(p) die sensitiwiteitsvlak van objek p voorstel.

2.1.3 Oudit

Oudit is die vaslegging, ondersoek en hersien van sekerheidsverwante aktiwiteite. Waar identifikasie, verifikasie en toegangsbeheer daarop gerig is om ongemagtigde toegang en aksies te voorkom, is oudit daarop gerig om ongemagtigde

aksies na die tyd op te spoor en korrektiewe stappe te neem.

Oudit het twee belangrike doelwitte, naamlik monitering en rekonstruksie [78]. Deur **monitering** word gebruikersaksies gemonitor met die oog daarop om 'n breuk in sekerheid te voorkom of te identifiseer. **Rekonstruksie** is die vermoë om, in die geval van 'n breuk in sekerheid, 'n verslag saam te stel van wat gebeur het, wat herstel moet word, en wie aanspreeklik vir die breuk in sekerheid is.

'n **Sleutelelement** in die ouditproses is die hou van 'n **ouditspoor**, d.i. 'n lêer waarin alle sekerheidsverwante aktiwiteite vasgelê word. Die volgende aktiwiteite behoort tipies in 'n ouditspoor vasgelê te word [17] [56] [66] [63]:

- Alle pogings, geldig of ongeldig, om toegang tot die stelsel te verkry.

- Alle versoeke, gemagtig of ongemagtig, vir toegang tot beskermde objekte, d.i. programme, data en transaksies.

- Alle wysigings van sensitiewe data en programme.

- Alle veranderings in voorregte of sekerheidsattribute.

- Alle aanteken en afteken transaksies, hetsy suksesvol of onsuksesvol.

Vir elke gebeurtenis wat aangeteken word, moet die relevante data wat daarop betrekking het ook aangeteken word. Tipiese inligting is:

- Datum en tyd van gebeurtenis.
- Identifikasie van gebruiker wat gebeurtenis geïnisieer het.
- Tipe gebeurtenis.
- Suksesvol of onsuksesvol.

- Oorsprong van die versoek (bv. terminaal-ID).
- Naam van betrokke objek.

Dit is duidelik dat die volume sekerheidsverwante aktiwiteite wat aangeteken word, ontsettend groot kan word. 'n Goeie oudit hulpmiddel behoort funksies te verskaf wat hierdie aangetekende aktiwiteite selektief kan versamel en reduseer om die belangrikste gegewens aan die stelseladministrateur te verskaf.

Kritiese aspekte van stelselsekerheid kan ook intyds gemonitor word sodat, in die geval van 'n buitengewone breuk in sekerheid, daar onmiddellik tot korrektiewe maatreëls oorgegaan kan word. 'n Voorbeeld hiervan is wanneer 'n gebruiker 'n onaanvaarbare aantal kere die verkeerde identifikasie en/of wagwoord insleutel. [17]

2.1.4 Rugsteun en Herstel

Rugsteun en herstel is van kardinale belang om te verseker dat, in die geval van 'n stelselfaling, ramptoestand of ander fout die minimum data verlore gaan, en dat die stelsel herstel kan word na die toestand wat gegeld het op 'n tydstip so na as moontlik voor die oomblik van faling.

Die stelselprogrammatuur moet fasiliteite verskaf om beide die rugsteun- en herstelprosedures te vergemaklik en so volledig moontlik te maak. Afhangende van die tipe stelsel en die vereistes vir beskikbaarheid, moet rugsteun op 'n daaglikse of selfs intydse basis plaasvind.

Aangesien hierdie funksie egter 'n integrale deel van enige databasis beheerstelsel behoort te wees, word dit volledig onder die subkategorie databasisse bespreek (sien par. 2.3.2).

2.1.5 Objek hergebruik

Objek hergebruik fasiliteite verskaf sekerheid deur te verseker dat wanneer 'n objek, bv. 'n lêer of aanteken ID, toegeken of hertoegeken word, daardie objek nie data bevat wat oorgebly het van vorige gebruik daarvan nie. Dit geskied byvoorbeeld deur data uit te vee deur dit fisies te oorskryf met niksseggende getalle, of deur te verhoed dat 'n spesifieke ID hertoegeken kan word. [87]

Algemene **objek hergebruik** fasiliteite is [78]:

- Skoonmaak van geheue blokke voor dit aan 'n program of data toegeken word.

- Skoonmaak van blokke op skyf wanneer 'n lêer geskrap word of wanneer die blokke hertoegeken word aan 'n lêer.

- Demagnetisering van magnetiese bande wanneer dit nie meer gebruik word nie.

- Uitwissing van wagwoord buffers na enkriptering.

- Waar data in plaaslike geheue (bv. buffers) van drukkers of terminale geberg word, word die plaaslike geheue skoongemaak wanneer die gebruiker afteken of wanneer 'n taak voltooi is.

2.1.6 Kriptografie

Kriptografie verwys na die tegnieke om data om te skakel vanaf gewone, leesbare teks na 'n geheime, onleesbare vorm, asook die terugskakeling daarvan weer na leesbare vorm.

Die geheime of geënkodeerde teks staan bekend as syferteks, die omskakelingsproses na syferteks as enkripsie en die terugskakelingsproses as dekripsie. Die enkripsieproses word gedoen deur 'n enkripsie-algoritme wat 'n bewerking op teks doen deur gebruik te maak van 'n kriptografiese sleutel.

Die drie belangrikste tegnieke waardeur enkripsie gedoen word, is die volgende [27] [76]:

- **Substitusie** behels die vervanging van bisse, karakters of blokke karakters deur substituut-bisse of -karakters.

- **Transposisie** is 'n tipe substitusie waarin bisse, karakters of blokke karakters herrangskik word volgens 'n permutasie.

- **Verberging** is 'n tegniek waardeur oortollige bisse, karakters of blokke karakters by die oorspronklike data gevoeg word.

Kriptografiese stelsels (ook syferstelsels genoem) val in twee algemene kategorieë, naamlik **vertroulikheidstelsels**, wat daarop gerig is om die inhoud van die boodskap geheim te hou, en **verifikasiestelsels**, wat daarop gerig is om die oorspronklikheid van die boodskapinhoud en/of die afsender se adres te verifieer. Binne elk van hierdie klasse kan daar onderskei word tussen twee tipe stelsels op grond van die sleutelverspreiding, naamlik private sleutel en publieke sleutel stelsels. [70] [17] [76] [73]

- **Private sleutel** (simmetriese) stelsels gebruik 'n enkele sleutel vir beide die enkripsie- en dekripsieproses. 'n Afsonderlike sleutel is nodig vir elke paar gebruikers wat kommunikeer, en beide kante van die kommunikasieproses moet die sleutel geheim hou. 'n Voorbeeld hiervan is die **Data Encryption Standard** (DES), 'n hoogs-gesofistikeerde enkripsie-algoritme wat d.m.v. apparatuur toestelle of programmatuur geïmplementeer word en wat die Amerikaanse standaard vir enkripsie-algoritmes vorm.

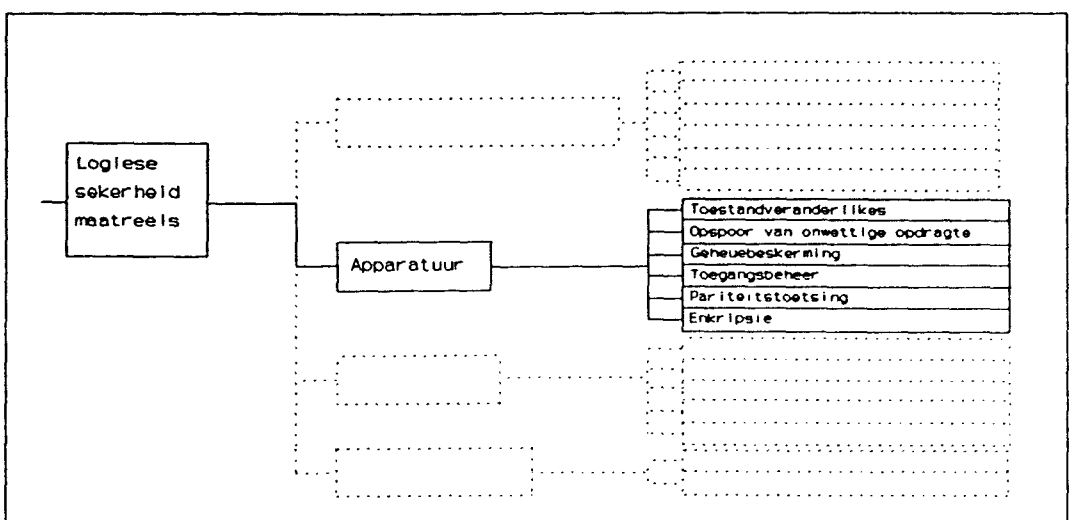
- **Publieke sleutel** (asimmetriese) stelsels gebruik twee sleutels : 'n publieke sleutel wat algemeen bekend is en gebruik word om die boodskap te enkripteer, en 'n private

sleutel wat verwant is aan die publieke sleutel, maar wat slegs aan die ontvanger van die boodskap bekend is en gebruik word om die boodskap te dekripteer. Die bekendste voorbeeld hiervan is die Rivest-Shamir-Adleman (RSA) enkripsie-algoritme.

Benewens die wye toepasbaarheid van kriptografie in netwerke (wat in par. 4. bespreek word), kan kriptografie byvoorbeeld ook deur die bedryfstelsel gebruik word om toegangsbeheerlyste te beskerm teen verandering, of om wagwoord tabelle te beskerm met die oog op vertroulikheid.

2.2 Apparatuur

Apparatuur beheermaatreëls vorm deel van beheermaatreëls vir logiese sekerheid en verwys na die basiese argitektuureienskappe van die rekenaartoerusting wat deur die stelselprogrammatuur gebruik kan word om beheermaatreëls te implementeer. Die vermoë van apparatuur om ondersteuning aan stelselfunksies soos geheuebestuur te verskaf, verminder die hoeveelheid stelselprogrammatuur wat nodig is vir 'n veilige stelsel. [79]



Figuur 3.5 Apparatuur

2.2.1 Toestandveranderlikes

Apparatuur toestandveranderlikes verwys na 'n argitekturele ontwerp wat die stelsel in staat stel om in spesiale veilige verwerkingstoestande bedryf te word, en wat die uitvoering van sensitiewe bewerkings of kernbeheeropdragte tot hierdie toestande beperk. Die apparatuur ondersteun tipies twee of meer verskillende bedryfstoestande, nl. een of meer bevoorregte toestande en 'n nie-bevoorregte toestand. [17] [70] [56]

In die **bevoorregte toestand** (opsigterstoestand) word slegs die bedryfstelsel onder beheer van die stelseladministrateur toegelaat om opdragte uit te voer. Hierdie bevoorregte opdragte word gebruik om stelselhulpbronne aan toepassingsprogramme toe te ken, invoer/uitvoer bewerkings te doen en om reëls vir toegangsbeheer te bepaal. 'n Program in hierdie toestand het dus toegang tot alle dele van die geheue.

In die **nie-bevoorregte toestand** (gebruikerstoestand) mag toepassingsprogramme wat deur gewone gebruikers gebruik word, opdragte uitvoer. Hierdie programme het dus slegs toegang tot gewone opdragte en beperkte dele van die geheue, en moet staatmaak op die stelseladministrateur en bedryfstelsel om bevoorregte opdragte uit te voer.

Die 80286 verwerker onderskei byvoorbeeld tussen vier vlakke van voorregte (0 die meeste betroubaar en 3 die minste betroubaar), en elke segment in geheue word gemerk met die toepaslike voorreg vlak. [28]

2.2.2 Opspoor van onwettige opdragte

Apparatuur kan gebruik word om alle onwettige transakies te onderskep en/of te kanselleer, bv. ongeldige operateurskodes. 'n Voorbeeld hiervan is die **faal-stop bewerking** van die VIPER mikroverwerker : apparatuur staak uitvoering van alle prosesse wanneer 'n apparatuurfout of onwettige opdragkodes opgespoor word. [70] [17]

2.2.3 Geheuebeskerming

Apparatuur kan so ontwerp word dat dit beskerming aan data en prosesse verleen op grond van die fisiese plasing daarvan binne die stelsel. Verskillende gebruikers en prosesse se data word geskei deur verwante kode fisies saam te groepeer in geheueblokke. Aan elke geheueblok word geassosieerde apparatuurregisters, nl. bo- en onderregisters ("base/bounds registers") toegeken, wat die fisiese adresse van die begin en einde van die blok bevat. [78] [17] [56]

Bo- en onderregisters word deur twee verskillende tegnieke ondersteun, afhangende van die argitekturele ontwerp van die geheue [55] [74] [28]:

- **Segmentering** verdeel die geheue in blokke sodat alle logies-verwante data in een blok gestoor kan word. Die blokke se grootte wissel na gelang van die hoeveelheid data wat saam gegroepeer word. Die segmentadresse en -groottes word in 'n segmentregister in geheue gestoor. Die 80286 verwerker maak gebruik van segmentering om apparatuur-geheuebeskerming toe te pas.

- **Paginering** verdeel die fisiese adresruimte in vaste-grootte blokke wat bladsye genoem word. Die bladsy-adresse en die verplasing ("offset") van spesifieke data binne elke bladsy word in 'n bladsy-gids in geheue gestoor, wat gebruik word om virtuele geheue adresse om te skakel na werklike fisiese geheue adresse. Die 80386 verwerker verskaf apparatuur-ondersteuning vir paginering.

2.2.4 Toegangsbeheer

Die wyse waarop die bedryfstelsel toegangsbeheer toepas, is in hierdie geval afhanklik van die ontwerp van geheue in die apparatuur [70] [56] [74]:

- **Sleutels en slotte** : Apparatuurregisters wat met geheue-blokke van objekte geassosieer word, dien as "slotte" wat

die sensitiwiteitsetikette van die blokke bevat. Slegs subjekte waarvan die apparatuurregisters ooreenstemmende etikette ("sleutels") bevat, het toegang tot die data of prosesse in die geheueblokke. 'n Voorbeeld van so 'n apparatuur-gebaseerde meganisme is die SIDEARM verwysings-monitor wat in die LOCK projek gebruik word.

- **Etiket-argitektuur** ("tagged architecture") : Hiervolgens het elke woord in masjiengeheue een of meer ekstra bisse wat die toegangsregte tot daardie woord identifiseer. Die geheue-ontwerp maak voorsiening vir die implementering van hierdie meganisme.

2.2.5 Pariteitstoetsing

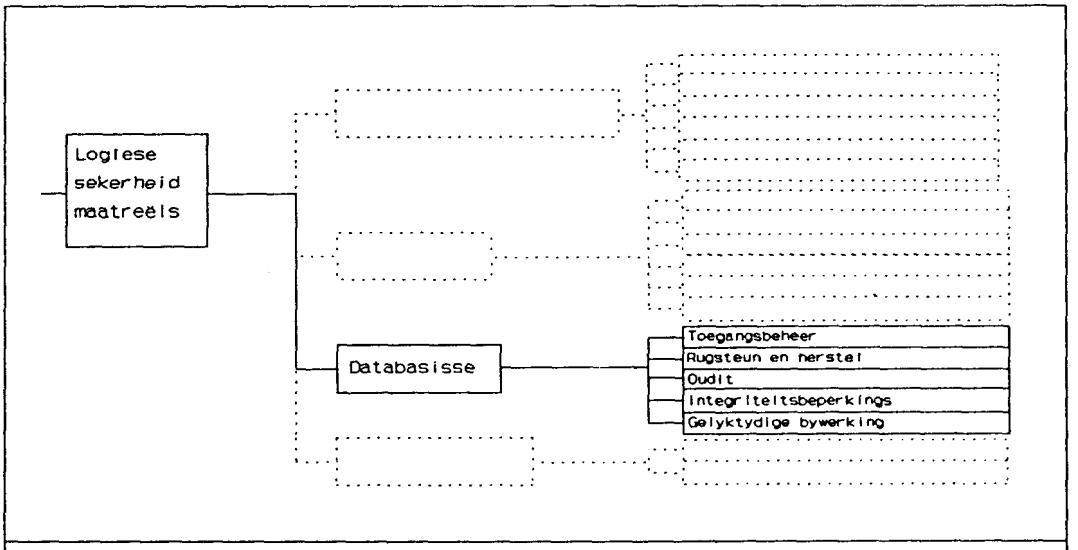
Outomatiese pariteitstoetsing kan deur apparatuur gedoen word. Die voordeel daarvan is dat dit baie vinniger is as pariteitstoetsing deur programmatuur. [55]

2.2.6 Enkripsie

Die veiligste manier om enkripsie-algoritmes te implementeer, is deur middel van apparatuurtoestelle. DES is byvoorbeeld aanvanklik in FIPS Publikasie 46 gespesifiseer "vir gebruik deur apparatuurtegnologie". Hierdie vereiste vir DES het egter later verval met die publikasie van ANSI X3.92-1981. [27]

2.3 Databasisse

Die feit dat databasisse toelaat dat data deur 'n groot aantal gebruikers gedeel kan word, het uiteraard sekerheids-implikasies wat toegangsbeheer, rugsteun en herstel, oudit, integriteitsbeperkings en hantering van gelyktydige bywerking noodsaak. Beheermaatreëls in databasisse word deur die databasis beheerstelsel ("Database Management System (DBMS)"), of die bedryfstelsel self toegepas.



Figuur 3.6 Databasisse

2.3.1 Toegangsbeheer

Alhoewel toegangsbeheermaatreëls in databasisse soortgelyk aan dié in stelselprogrammatuur is, beskik databasisse oor twee eienskappe wat spesiale toegangsbeheermaatreëls noodsaak.

Eerstens staan objekte in 'n bepaalde verwantskap met mekaar in 'n databasis. Indringers kan dus afleidings oor sensitiewe data-elemente maak deur toegang tot verwante nie-sensitiewe data te verkry. Hierdie verskynsel staan bekend as die **afleidingsprobleem.** [1] [18] [93]

Die belangrikste tegnieke om die afleidingsprobleem te hanteer, is die volgende [1] [74]:

- **Beperkte respons suppressie** : Lae-frekwensie elemente word uitgesluit uit die uitvoer ten einde inligting oor individuele rekords van gebruikers te weerhou.

- **Kombinering van resultate** : In plaas van individuele waardes, word waardes as deel van reekse voorgestel, bv. hoeveel werknemers ontvang 'n salaris in die reeks R1 000

tot R2 000.

- **Ewekansige steekproef** : 'n Resultaat word afgelei deur 'n steekproef van die databasis te maak; vir elke steekproef word die populasie-elemente ewekansig gekies.

- **Opsetlike foute** : Antwoorde word met 'n geringe faktor versteur sodat dit min of meer akkuraat is, maar nie presiese inligting kan openbaar nie.

- **Navraag-ontleding** : Elke navraag wat deur 'n spesifieke gebruiker gedoen word, word ontleed teen die agtergrond van vorige navrae om te bepaal watter afleidings hy kan maak. Die afleidings wat deur die rig van verskillende navrae gemaak kan word, kan geïdentifiseer en geëlimineer word met behulp van 'n ekspertstelsel. So 'n model om hierdie ontleding te outomatiseer, die sg. Database Inference Controller, word deur Buczkowski [18] beskryf.

Tweedens is die **granulariteit** van beskerming in 'n databasis fyner as in die geval van stelselprogrammatuur, aangesien nie net objekte soos lêers nie, maar selfs data-entiteite se sensitiwiteitsvlakke verskil. Voortvloeiend hieruit is die konsep van **multivlak sekerheid** in databasisse, wat behels dat twee of meer vlakke van sekerheid nodig is vir beide data-entiteite en gebruikers van een databasis. [60] [74]

Toegangsbeheer in 'n databasis is afhanklik van twee faktore, naamlik die ontwerp van die databasis en meganismes om ongemagtigde toegang te voorkom.

Die belangrikste **databasisontwerp** style is die volgende [49] [60] [74] [38]:

- **Partisionering** : Die databasis word in verskillende databasisse verdeel, elk met sy eie vlak van sekerheid. In verspreide databasisse word hierdie tegniek toegepas deur

per vlak ontwerp ("perlevel design"), d.i. elke databasis bevat data slegs op een sekerheidsvlak, of deur **afbeelding ontwerp** ("replicated design"), waar elke databasis alle data tot op 'n gegewe vlak van sekerheid bevat.

- **Integriteitslot** ("integrity lock") : Hierdie ontwerp verskaf verpligte ("mandatory") sekerheid in 'n DBMS. 'n Veilige filter word in 'n onveilige DBMS geplaas om data te etiketteer en hierdie sensitiwiteitsetikette te kontroleer om toegangsbeheer toe te pas. Wanneer 'n data-element geskep word, word die data en die sensitiwiteits-etiket "geseël" met 'n kriptografiese kontroletotaal. Sodoende kan toegang beperk word tot gemagtigde gebruikers en kan daar verseker word dat daar nie met die data of die sensitiwiteitsetiket gepeuter is nie.

- **Hinke-Schaefer ontwerp** : 'n Onveilige DBMS word op 'n veilige bedryfstelsel gebruik. Die bedryfstelsel skei die data in duidelik gedefinieerde segmente volgens die sekerheidsvlak daarvan. Die TCB van die bedryfstelsel beheer alle toegang tot die databasis. 'n Gesofistikeerde uitbreiding op hierdie ontwerp is die SEAVIEWS argitek-tuur.

- **Veilige voorkant** ("trusted front-end") : Enige versoeke word deur 'n veilige voorkant proses geverifieer, na die onveilige databasis beheerstelsel gestuur vir verwerking, en die respons word eweneens geverifieer om te verseker dat dit akkuraat en op die regte sensitiwiteitsvlak is.

Gebaseer op een van hierdie ontwerpstyle, kan die volgende meganismes gebruik word om toegangsbeheer in 'n multivlak databasis toe te pas [75] [26] [94] [93]:

- **Magtigingsreëls** : Toegang tot die data word beperk op grond van magtigingsreëls wat uit vier dele bestaan, nl. 'n subjek, 'n objek, 'n aksie en 'n beperking, bv.

gebruiker A mag die salarisveld in die personeelrelasie lees of wysig, mits die nuwe salaris minder as R10 000 is. Hierdie tegniek is soortgelyk aan toegangsbeheerlyste met die addisionele fasiliteit dat toegang beperk kan word op grond van die inhoud van 'n veld.

- **Enkripsie** : Data-elemente word in geënkripteerde vorm gestoor en gedekripteer wanneer 'n gemagtigde gebruiker 'n navraag daarop doen. Die hele kriptografiese proses is deursigtig vir die gebruiker.

- **Subskemas** ("Views") : 'n Subskema is 'n subversameling van 'n databasis wat attribute, rekords en elemente filtreer sodat die gebruiker slegs die data sien waartoe hy gemagtig is. So 'n subskema kan dien as 'n enkele gebruiker se eie databasis waarheen alle navrae gerig word.

- **Gebruiker-gedefinieerde prosedures** : Die gebruikers of databasisadministrateur skryf prosedures wat onder bepaalde omstandighede deur die DBMS opgeroep word. Die prosedure word gebruik om gebruikersaksies te beheer of te beperk op grond van sekere voorwaardes waarvan die geldigheid getoets word.

- **Poli-instansiëring** ("Polyinstantiation") : Deur hierdie tegniek kan elke relasie meer as een rekord hê wat met 'n bepaalde sleutelveld geassosieer word, nl. een rekord vir elke sekerheidsklas. Die doel hiervan is dat 'n laer-vlak gebruiker nie kan afleidings maak oor 'n rekord deur agter te kom dat die rekord se sekerheidsvlak verander het nie. Die nadeel hiervan is egter dat die integriteit van die databasis verlore gaan, aangesien daar twee verskillende weergawes van dieselfde rekord is.

2.3.2 Rugsteun en herstel

Die rugsteun- en herstelproses is gerig daarop om te verseker dat die korrekte data te alle tye beskikbaar is, d.w.s. integriteit en beskikbaarheid is hier ter sprake. Die proses kan in drie stappe verdeel word, naamlik rugsteuning, joernalisering en herstel.

Rugsteun

Rugsteun is die maak van kopieë van hele lêers of dele daarvan, met die doel om die lêers in 'n latere stadium te herstel na die status en met die inhoud wat gegeld het tydens rugsteuning.

Die frekwensie waarmee rugsteunkopieë gemaak moet word, hang onder andere af van die aantal gebruikers in die stelsel en die volume werk wat daagliks gedoen word. Daar word onderskei tussen 'n **volledige** rugsteun en 'n **inkrementele** rugsteun. In eersgenoemde geval word alle lêers in die stelsel gekopieer, terwyl in laasgenoemde geval slegs die lêers wat verander is of geskep is sedert die vorige volledige rugsteun, gekopieer word. [26]

Die volgende riglyne vir die rugsteunproses word in [78] geïdentifiseer:

- Enkripteer rugsteunlêers wat sensitiewe data bevat.

- Berg ekstra rugsteunlêers by 'n buite-aanleg in 'n geslote, brandvaste kluis.

- Verifieer rugsteunkopieë gereeld om te verseker dat die kopieë korrek gemaak is en nie beskadig is nie.

- Vernietig die inhoud van rugsteunkopieë voor die medium (d.i. skyf of band) hergebruik word vir ander doeleindes.

- Maak 'n rugsteunkopie van die rugsteun voordat dit in 'n herstelaksie gebruik word.

Joernalisering

Joernalisering behels die hou van 'n joernaal of logboek van alle aktiwiteite wat data in die stelsel verander, tipies die verandering van rekords in 'n databasis. Outomatiese joernalisering is deursigtig vir die gebruiker en vir toepassingsprogramme wat veranderings aan rekords en lêers maak.

Die inligting wat tydens joernalisering vasgelê word, bevat [75] [30] [26]:

- Die identifikasie van die taak wat die bywerking, skrapping of byvoeging uitgevoer het, d.i. die transaksie ID.

- Die tyd en datum waarop die transaksie uitgevoer is.

- Die identifikasie van die subjek (gebruiker) en die objek (lêer of rekord).

- 'n Rekord van hoe die data in die databasis gelyk het voor die transaksie, d.i. die begin-beeld ("before image"), en 'n rekord van hoe die data gelyk het na die transaksie, d.i. die eind-beeld ("after image").

Dit is belangrik dat die joernaal geskryf word voordat die transaksie gedoen word, sodat daar reeds 'n rekord in die transaksiejoernaal is in geval die stelsel faal tydens die skryf van die transaksie.

Herstel

Die herstelproses behels die herstel van die stelsel na 'n korrekte toestand vanuit 'n foutiewe toestand deur gebruik te maak van rugsteunkopieë, en met die minimum verlies van inligting. Die stelsel moet in staat wees om 'n falingsituasie op te spoor of te herken, die herstelprosedure te inisieer en gebruikers in kennis te stel van probleme in die stelsel. Die stelsel moet ook in staat wees om te bepaal of daar 'n verlies van data was en indien wel, wat die presiese

omvang daarvan is. [30]

Daar word hoofsaaklik onderskei tussen voorwaartse herstel en terugwaartse herstel van 'n databasis. [75] [26]

- **Voorwaartse herstel** word gedoen in die geval van bv. 'n mediafaling (bv. van die skyfkontroleerder) waar die databasis in geheel of gedeeltelik vernietig is. Dit word gedoen deur die mees onlangse kopie van die volledige databasis te laai en aan te vul met die mees onlangse inkrementele rugsteunkopieë. Waar 'n transaksiejoernaal beskikbaar is, word die eind-beelde van die transaksies laastens op die rekords in die databasis toegepas.

- **Terugwaartse herstel** word gedoen in die geval van bv. 'n stelselfaling. Die databasis self word nie fisies beskadig nie, maar alle transaksies wat besig is om uitgevoer te word, word onderbreek. Die integriteit van die databasis kan herstel word deur die transaksiejoernaal terugwaarts te verwerk tot by die mees onlangse korrekte toestand, deur gebruik te maak van die begin-beelde van transaksies. Daar word van kontrolepunte gebruik gemaak om te bepaal waar die mees onlangs korrekte toestand was.

2.3.3 Oudit

'n Databasis beheerstelsel behoort fasiliteite te verskaf om oudit van stelselgebruikers se aksies moontlik te maak. In die geval van 'n databasis is dit belangrik om alle toegange op 'n rekord-, veld- en elementvlak in die ouditspoor in te sluit.

Jajodia et al. [53] wys op die belangrikheid daarvan dat 'n databasis twee tydsdimensies moet hê vir die doeleindes van oudit. Die eerste dimensie, **transaksietyd**, gee die tyd weer waarop die oorspronklike inligting in die databasis gestoor is, en die tweede dimensie, **geldige tyd**, gee die tyd weer waarop die huidige inligting geldig geword het. Op hierdie

wyse weerspieël die databasis historiese sowel as huidige data, en kan alle aksies wat op die data gedoen is, gerekonstrueer word.

Die ouditfunksie vir databasisse stem grootliks ooreen met dié van stelselprogrammatuur, en word dus nie weer hier bespreek nie. Vir verdere inligting verwys na par. 2.1.3.

2.3.4 Integriteitsbeperkings

Integriteitsbeperkings kan gedefinieer word as voorwaardes waaraan die data in spesifieke velde moet voldoen, of voorwaardes wat van toepassing is op enige verwerking van die waardes in die databasis.

Integriteitsbeperkings kan gegrond word op die volgende vereistes [75] [56] [26]:

- **Geldigheid**, bv. is die data in die attribuut BEDRAG numeries?

- **Redelikheid**, bv. 'n werknemer se maandelikse salaris kan nie meer as R10 000 wees nie.

- **Reeksbeperkings**, bv. rentekoerse moet tussen .05 en .25 wees.

- **Waardebeperkings**, bv. kredietlimiete moet R500, R1 000 of R1 500 wees.

- **Formaatbeperkings**, bv. 'n identiteitsnommer moet 13 syfers hê.

- **Toestandsbeperkings** beskryf die toestand waarin die hele databasis moet verkeer om korrek te wees. 'n Voorbeeld hiervan is dat elke kliënt bv. 'n unieke nommer moet hê.

- **Oorgangsbeperkings** beskryf die toestande wat moet geld voordat veranderings aan die databasis aangebring kan word, bv. dat geen rekening geskrap mag word indien daar nog 'n uitstaande balans is nie.

Die eenheid van die DBMS wat integriteitsbeperkings toepas en dus verantwoordelik is vir die strukturele integriteit van die databasis, staan bekend as 'n **integriteitsmonitor.** [74]

2.3.5 Gelyktydige Bywerking

Gelyktydige bywerking verwys na 'n geval waar twee of meer gebruikers gelyktydig besig is om bywerkings tot die databasis te maak. Die DBMS moet 'n meganisme verskaf wat verseker dat die databasis in so geval korrek bygewerk word. Dit is egter belangrik dat hierdie meganisme nie die beskikbaarheid of integriteit van data kompromitteer nie. Daar is hoofsaaklik drie meganismes waardeur gelyktydige bywerking hanteer kan word [75] [26]:

Transaksiejoernaal

Gelyktydige bywerking kan vermy word deur gebruikers slegs toe te laat om rekords in die databasis te lees. Enige bywerkingsaksies word in 'n afsonderlike transaksiejoernaal gestoor. Periodiek word hierdie transaksiejoernaal dan uitgevoer en die veranderings word sekwensieel aan die databasis aangebring. Die nadeel hiervan is egter dat die data in die databasis verouderd is totdat die transaksiejoernaal uitgevoer word.

Eenvoudige Rekordsluiting

Eenvoudige rekordsluiting behels dat wanneer 'n gebruiker 'n rekord lees met die doel om 'n bywerking te doen, die rekord gesluit word vir ander gebruikers en hulle geen toegang daartoe kan verkry nie. Eers wanneer die bywerkingstransaksie op 'n spesifieke rekord afgehandel is, word die rekord ontsluit. Benewens rekords, kan 'n individuele veld, lêer of die hele databasis ook gesluit word.

'n Probleem met eenvoudige rekordsluiting ontstaan egter in die geval waar 'n logiese transaksie uit 'n paar fisiese transaksies bestaan, en die logiese transaksie om een of ander rede opgeskort word. Indien 'n rekord wat as deel van die logiese transaksie bygewerk is, intussen deur 'n ander gebruiker met nuwe data bygewerk is, word hierdie laaste bywerking ongedaan gemaak deur die herstelproses.

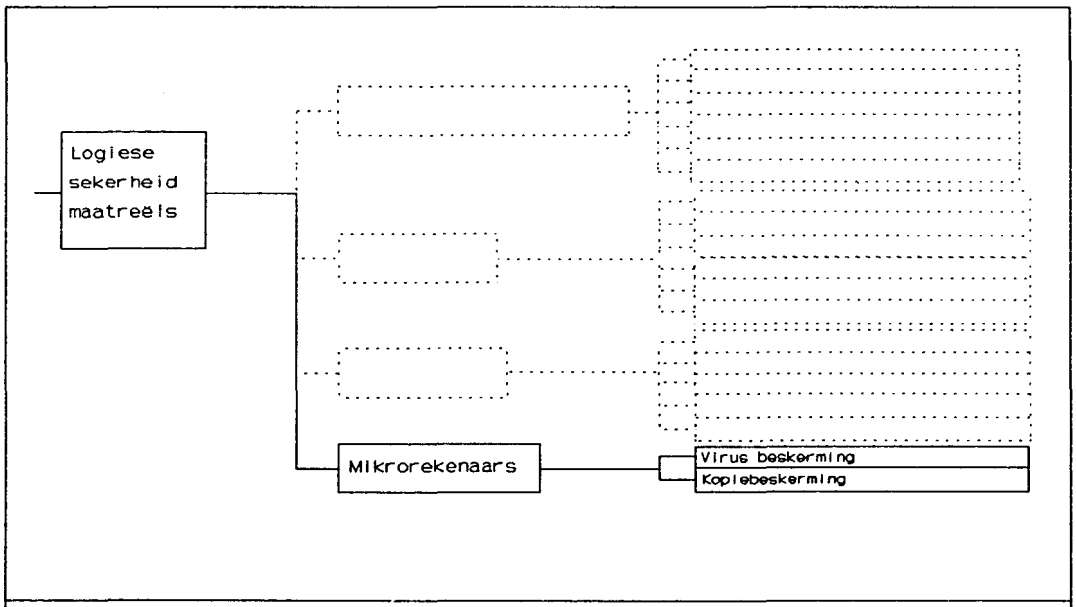
Twee-fase rekordsluiting

Deur twee-fase rekordsluiting word die probleem van eenvoudige rekordsluiting opgelos deurdat 'n gebruiker sy slotte op al die rekords wat deur 'n logiese transaksie beïnvloed word, hou totdat die volledige transaksie afgehandel is. Daar is dus 'n groei-fase waarin meer en meer rekords gesluit word, en 'n inkrimpingsfase waarin alle rekords ontsluit word.

Waar hierdie meganisme geïmplementeer word, moet spesiale aandag aan die probleem van **verstarring** ("deadlock") gegee word. Hierdie probleem ontstaan deurdat twee verskillende gebruikers elkeen 'n slot op 'n rekord hou wat deur die ander een benodig word om sy transaksie te voltooi. 'n Voorkomende benadering wat gevolg kan word, is dat 'n gebruiker eers moet seker maak dat alle rekords wat hy in 'n logiese transaksie gaan sluit, wel beskikbaar is (d.w.s. nie reeds gesluit is nie). Indien 'n verstarring egter ontstaan, moet die databasis beheerstelsel in staat wees om dit op te spoor en een van gebruikers se transaksies te kanselleer.

2.4 Mikrorekenaars

Benewens die beheermaatreëls wat deur stelselprogrammatuur toegepas word en wat in paragraaf 2.1 bespreek is, is virus beskerming en kopie beskerming belangrike beheermaatreëls met betrekking tot die mikrorekenaar omgewing.



Figuur 3.7 Mikrorekenaars

2.4.1 Virus Beskerming

'n Virus is 'n parasitiese vorm van rekenaarkode wat programme aantas deur 'n kopie van homself in die program te versteek. 'n Virus word uitgevoer elke keer wanneer die program wat hom bevat, uitgevoer word. Sodoende versprei 'n virus deur 'n stelsel terwyl hy die integriteit van programme en data aantas met die moontlike gevolg van 'n stelselfaling.

Mikrorekenaars van alle soorte is uiters kwesbaar vir virusaanvalle, aangesien enige nuwe program deur 'n gebruiker met behulp van 'n sagteskyf op die stelsel gelaai kan word. Mikrorekenaars wat in 'n netwerk verbind is, is uiteraard ook baie kwesbaar, veral omdat die virus in hierdie geval baie vinniger na ander gebruikers versprei. **Hoofraamrekenaars** daarenteen, blyk die beste beskermd te wees teen virusaanvalle, aangesien die hoofraam se bedryfstelsels kompleks is en interne beheermaatreëls verhoed dat virusaanvalle maklik kan plaasvind. Fisiese en logiese toegang tot die stelsel kan ook beter beperk word. [32] [103] [2]

Alhoewel die oorgrote meerderheid van aangetekende virus-

aanvalle op mikrorekenaars voorgekom het, kan die bedreiging vir hoofraamrekenaars egter nie buite rekening gelaat word nie. Die Cornell virus het byvoorbeeld in minder as een dag duisende hoofraamrekenaars dwarsdeur die wêreld aangetas. [103]

Maatreëls vir die hantering van virusaanvalle is gerig op die voorkoming, inperking en regstelling van virusse.

- **Administratiewe prosedures** : Hierdie prosedures verwys na reëls en gebruike wat in die organisasie toegepas kan word om virusse te voorkom. Voorbeelde hiervan is 'n verbod op die gebruik van onbekende of ongemagtigde programmatuur (insluitende speletjies) en 'n bewusmaking van gebruikers oor die gevare wat virusse inhou. [82] [46]

- **Inenting** ("vaccination") : Inentingsprosedures is 'n vorm van 'n virus filter en is daarop gerig om virusse wat reeds in die stelsel is, te identifiseer, dit te elimineer en om reproduksie te voorkom. Die prosedures bied egter nie beskerming teen alle virusse nie, slegs teen sommige virusse wat reeds bekend is. Een tegniek wat gebruik word, is dat die vertaler verdedigingsprosedures genereer en dit insluit by alle programme wat vertaal word vanaf bronkode na uitvoerbare kode. 'n Program kan dan bv. homself ondersoek vir interne foute en dit regstel. 'n Voorbeeld van so 'n hulpmiddel is Antigen van Digital Dispatch, Inc. [2] [24] [44] [103]

- **Enkripsie** : Alle uitvoerbare programme in 'n stelsel word geënkripteer. Indien 'n virus nie die uitvoerbare kode kan aantas voordat dit geënkripteer word nie, kan die virus nooit uitgevoer word nie. Selfs al word die uitvoerbare kode aangetas voor enkripsie, sal die virus nie in staat wees om homself te reproduseer na 'n ander (geënkripteerde) uitvoerbare program nie. Hierdie tegniek plaas egter 'n groot las op die stelsel en behoort net in uiters

kritiese stelsels gebruik te word. [2]

- **Kriptografiese kontroletotale** : 'n Kontroletotaal word vir elke beskermde program of proses bereken op grond van die uitvoerbare kode en 'n tydstempel, en hierdie totaal word geënkripteer. Voor die uitvoering van die program of proses word die kontroletotaal gedekripteer en herbereken om te verseker dat die uitvoerbare kode nie aangetas is nie. 'n Program wat hierdie tegniek gebruik, is Cryptographic Checksum deur dr. Fred Cohen. [32] [44]

- **Toegangsbeheer programmatuur** : Alhoewel toegangsbeheer programmatuur vir 'n verskeidenheid van redes toegepas word, kan dit virusvoorkoming as 'n byvoordeel bied. Aangesien toegang tot kritiese objekte beperk word, kan 'n virus nie programme wysig tensy dit reeds by 'n hoëvlak proses aangeheg is nie. [2]

- **Toets-na-produksie beheer** : Hierdie maatreëls beheer die instelling van nuwe programmatuur in die produksie-omgewing. Dit sluit in programmatuur toetsing, verifikasie, kwaliteitsversekering en skriftelike magtiging voor implementering. Produksieprogramme word slegs vanaf streng gekontroleerde biblioteke uitgevoer, en daar is duidelike skeiding tussen die produksie- en ontwikkelingsomgewings. Hierdie prosedures is van toepassing op nuwe programmatuur asook op veranderings aan bestaande programmatuur. (Sien ook par. 1.1.1) [2] [32]

- **Kompartementering** : Deur kompartementering word data en programme in eksklusiewe groepe verdeel, sodat elke program slegs toegang het tot data en programme in sy eie groep. Sodoende word virusse beperk tot die bepaalde kompartement waarin dit voorgekom het, en word die hele stelsel nie aangetas nie. 'n Voorbeeld hiervan is aparte biblioteke met aparte magtigings. [74] [32]

- **Rugsteun en Herstel** : Indien 'n virus opgespoor is en daar is geen betroubare manier om dit uit te wis nie, is die enigste oplossing gewoonlik om die oorspronklike weergawe van die program of data te herlaai. Die prosedures vir rugsteun en herstel is soortgelyk aan dié wat in par. 2.3.2 bespreek is. [2] [32]

2.4.2 Kopiebeskerming

Aangesien alleenstaande mikrorekenaars vereis dat elke gebruiker oor sy eie kopie van die programmatuur op die mikrorekenaar beskik, is dit noodsaaklik dat programmatuur wel kopieerbaar moet wees. Terselfdertyd moet gebruikers egter verhoed word om ongemagtigde kopieë van programmatuur vir persoonlike gebruik te maak. Pfleeger [74] identifiseer drie basiese metodes om programmatuur teen ongemagtigde kopiëring te beskerm, naamlik deur die gebruik van programmatuurtegnieke, programmatuur/apparatuur kombinasies, en apparatuurtegnieke.

Programmatuurtegnieke

Die mees algemene programmatuurtegniek word deur pakkette soos Everlock toegepas wat die programmatuur beskerm en toelaat dat slegs 'n voorafgespesifiseerde aantal kopieë met 'n spesiale installeringsprogram gemaak word.

Beskerming op hierdie vlak word ook gedoen deur die oorspronklike kopie van die programmatuur op een of ander wyse te "beskadig" sodat dit nie deur die kopiëringsprogrammatuur gelees kan word nie. Twee tegnieke wat gebruik word, is die volgende:

- **Ongeldige formaat** : Die oorspronklike sagteskyf word voorsien van een of meer slegte sektore, of daar word bane op plekke geskryf waar daar nie bane behoort te wees nie.

- **Falingsbisse** : Die magnetiese stoormedium word beskadig deur bv. baie klein krapmerke op een deel van die oppervlak te maak wat nie as 'n 0 of 1 gelees kan word nie.

Programmatuur/Apparatuur Kombinasies

Hierdie tegniek berus op die feit dat apparatuur nie so maklik gereproduseer kan word as programmatuur nie, daarom word die oorspronklike programmatuurkopie vergesel van 'n apparatuurtoestel. Programmatuur en apparatuur word dan gekombineer deur bv. 'n programmatuurtoets te doen op die apparatuurtoestel. Hierdie toestel dien as 'n elektroniese "sleutel" wat in een van die poorte ingedruk word. Wanneer 'n beskermde program geloop word, stuur dit eers 'n sein na die poort. Indien die sleutel aanwesig is, stuur dit 'n herkenbare sein terug.

Apparatuurtegnieke

Hierdie tegnieke behels dat 'n program vir 'n spesifieke rekenaar geskryf of geïnisieer word. Twee tegnieke wat gebruik word, is:

- **Unieke serienommer** : Die rekenaar waarop die program geloop word, word van 'n unieke serienommer in geheue voorsien. Die program toets dan vir die spesifieke nommer voordat dit uitgevoer word.

- **Kriptografiese verwerker** : Die verwerker bevat 'n dekripsiesleutel en -proses. Die program word geënkripteer met die gebruiker se unieke sleutel, en tydens uitvoering kan slegs die gemagtigde rekenaar dus die program dekripteer en uitvoer.

3. VERSPREIDE STELSELS SEKERHEID MAATREëLS

Verspreide stelsels verwys na stelsels waar die invoer, verwerking, stoor en uitvoer van data nie by een fisiese plek geskied nie. Beheermaatreëls vir hierdie tipe stelsels is spesifiek gerig op die beskerming van die vertroulikheid, integriteit en beskikbaarheid van data tydens data-uitruiling (kommunikasie). Voorbeelde van sulke stelsels is Lokale Area Netwerke, Wye Area Netwerke, Globale Area Netwerke en hoofraamstelsels.

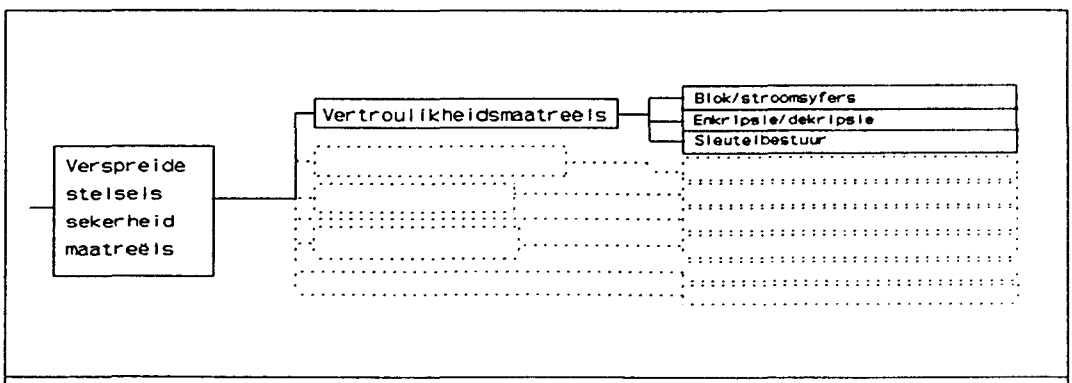
Die International Standards Organisation (ISO) se Open

Systems Interconnection (OSI) netwerkargitektuur bied 'n raamwerk waarbinne sekerheidsdienste vir verspreide stelsels gedefinieer kan word. Die belangrikste sekerheidsdienste wat in die sekerheidsaddendum tot die OSI argitektuur gedefinieer word, word as raamwerk vir die volgende bespreking van beheermaatreëls in verspreide stelsels gebruik.

Hierdie beheermaatreëls is vertroulikheidsmaatreëls, integriteitsmaatreëls, identifikasie en verifikasie, toegangsbeheer, nie-repudiëring, verkeersvloei-vertroulikheid en sekerheidsbuitelyne. [16] [71]

3.1 Vertroulikheidsmaatreëls

Vertroulikheidsmaatreëls het ten doel om sensitiewe data te beskerm teen ongemagtigde blootstelling tydens kommunikasie tussen verskillende verspreide stelsels of nodes [71]. Die belangrikste maatreëls konsentreer op kriptografiese tegnieke, naamlik blok- en stroomsyfers, skakelenkripsie, end-tot-end enkripsie en sleutelbestuur.



Figuur 3.8 Vertroulikheidsmaatreëls

3.1.1 Blok/Stroomsyfers

Die tipe syferstelsel wat in 'n kommunikasiestelsel gebruik word, hang daarvan af of karakters in 'n stroom of in blokke versend word. [27] [91]

- 'n **Stroomsyfer** word gebruik in gevalle waar die kommunika-

siestelsel karakters een-vir-een in 'n stroom moet hanteer. Elke karakter wat deur die uitvoereenheid ontvang word, word geënkripteer en dan versend. 'n Voorbeeld van hierdie syferstelsel is die Vigenère syfer.

- 'n **Bloksyfer** hanteer teks in blokke deur 'n groep karakters as een blok te enkripteer. 'n Verfyning hiervan is syfer blok skakeling ("cipher block chaining") waarvolgens die uitvoer van een geënkripteerde blok in die invoer van die volgende blok se enkripsie gebruik word. 'n Voorbeeld van 'n bloksyfer is die DES, wat in vier verskillende operasionele modusse gebruik kan word.

Pfleeger [74] beskryf vier sekerheidsimplikasies van die verskillende tegnieke, nl:

- **Spoed van transformasie** : Stroomsyfer enkripteer elke karakter sodra dit beskikbaar word, en is vinniger as bloksyfer aangesien laasgenoemde moet wag vir 'n blok karakters voor dit die enkripsie kan doen.

- **Foutvoortplanting** : Aangesien elke karakter afsonderlik geënkriptreer word in die geval van stroomsyfer, word slegs een karakter deur 'n fout in die enkripsieproses beïnvloed, terwyl al die karakters in 'n blok beïnvloed word in die geval van bloksyfer.

- **Diffusie** : In die geval van bloksyfer word die oorspronklike teks versprei in 'n blok syferteks, wat ontleding van die syferteks moeiliker maak. Stroomsyfer kan makliker ontleed word aangesien syferteks 'n een-tot-een afbeelding van oorspronklike teks is.

- **Immuniteit teen byvoegings** : Stroomsyfer is meer vatbaar vir byvoegings in die teks deur 'n aanvaller, aangesien elke karakter onafhanklik geënkripteer word. Met bloksyfer is die grootte van 'n blok egter vasgestel en sal die byvoeging van 'n karakter 'n onreëlmatigheid in die blokgrootte veroorsaak.

3.1.2 Enkripsie/dekripsie

Enkripsie/dekripsie verwys na die kriptografiese proses soos in par. 2.1.6 bespreek. In 'n verspreide stelsels omgewing word daar hoofsaaklik onderskei tussen skakelenkripsie en end-tot-end enkripsie. [91] [79] [3]

- **Skakelenkripsie** verskaf beskerming aan 'n boodskap terwyl dit tussen twee nodes op 'n kommunikasielyn is. Die boodskap word geënkripteer net voor dit op die fisiese kommunikasieskakel tussen twee nodes geplaas word, gewoonlik op vlak 2 (die dataskakel vlak) van die OSI model. Dekripsie vind soortgelyk plaas sodra dit deur die volgende netwerkkommunikasienode gaan, en die proses word herhaal totdat die boodskap die bestemming bereik.

- **End-tot-end enkripsie** beskerm die boodskap vanaf die oorspronklike afsender tot by die uiteindelike ontvanger. Die enkripsie/dekripsie proses vind op die hoogste vlakke van die OSI model plaas, d.w.s. die toepassings- of presentasievlak. Die boodskap word nie gedekripteer voordat dit die eindbestemming bereik nie. Aangesien die afsender en ontvanger se identiteite egter in leesbare teks beskikbaar moet wees om nodes in staat te stel om die boodskap op die korrekte roete te stuur, is verkeersontleding moontlik.

3.1.3 Sleutelbestuur

Die sterkte en sekerheid van 'n kriptografiese stelsel is afhanklik van die sekerheid wat geld vir die generering, administrasie en verspreiding van die sleutels wat gebruik word in die enkripsie/dekripsie proses.

Die belangrikste oorweging wat geld tydens die **generering** van 'n enkripsie/dekripsie sleutel is dat die sleutel so ewekansig moontlik gekies word. Daar moet dus geen voorspelbare verwantskap tussen die bisse van die sleutel wees nie.

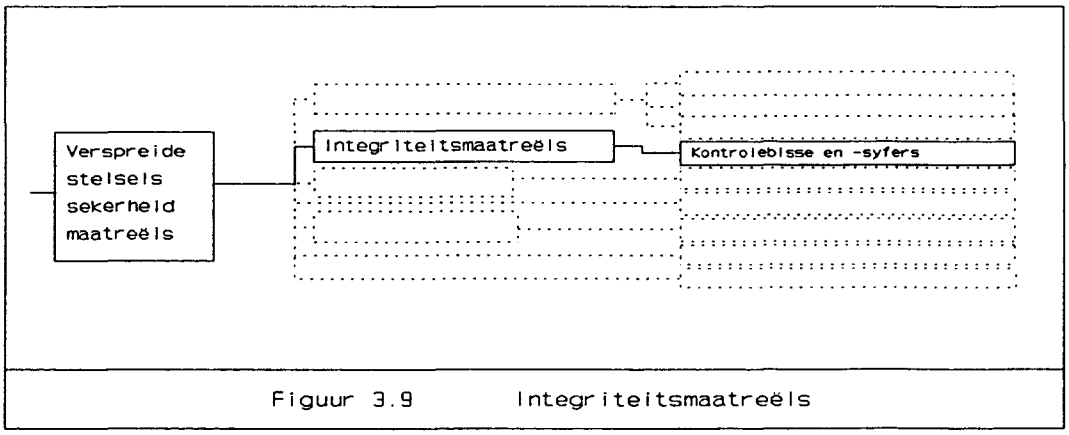
Sleutels kan outomaties gegenereer word deur die gebruik van programmatuur (bv. 'n pseudo-ewekansige getal generator), of deur ewekansige bis generators wat die fisiese geraas op kommunikasiekanale gebruik om sleutels te genereer. [56] [27]

Wat die **administrasie** van sleutels betref is dit noodsaaklik dat sleutels gereeld verander word. Die periode wat verloop tussen veranderings aan sleutels word gedeeltelik beïnvloed deur die tyd wat dit vir 'n indringer neem om die sleutel te ontsyfer. [91]

Sleutelverspreiding is die proses waardeur kriptografiese sleutels aan die gemagtigde nodes gestuur word. Dit is uiters noodsaaklik dat hierdie sleutels nie tydens verspreiding gekompromitteer word nie. Dit kan byvoorbeeld gedoen word deur die toepaslike sessiesleutel in geënkripteerde vorm aan die ontvanger te stuur voordat die boodskap 'n aanvang neem. Die enkripsie/dekripsie van die sessiesleutels word gedoen deur gebruik te maak van 'n voorafgereelde meestersleutel. [74]

3.2 Integriteitsmaatreëls

Die maatreëls waardeur die integriteit van 'n versende boodskap gekontroleer kan word, maak almal gebruik van een of ander vorm van **kontrolebisse en -syfers** wat by die boodskap gevoeg word. Hierdie maatreëls kan verdeel word in maatreëls teen toevallige foute en maatreëls teen aktiewe aanvalle.



Figuur 3.9 Integriteitsmaatreëls

Maatreëls teen **toevallige foute** spoor foute op wat veroorsaak word deur bv. steurnisse op die kommunikasielyn. Aangesien die tegnieke wat toegepas word algemene kennis is, is hierdie tegnieke nie geskik om aktiewe aanvalle op te spoor nie. Die belangrikste tegnieke is pariteitstoetsing en sikliese oortolligheidskontroles. [27] [76] [40]

- **Pariteitstoetsing** behels die byvoeging van 'n pariteitsbis by elke karakter wat versend word. Die ontvanger bereken op sy beurt die pariteitsbis vir elke karakter en vergelyk dit met die gestuurde een.

- 'n **Blokkontrolesom** is 'n uitbreiding van pariteitstoetsing deur die byvoeging van 'n karakter (d.i. 'n ekstra stel pariteitsbisse) aan die einde van 'n raam of blok karakters. Die tegniek staan ook bekend as longitudinale pariteit.

- Deur **sikliese oortolligheidskontroles** ("cyclic redundancy checks") word 'n wiskundige bewerking op 'n blok data gedoen. Die reswaarde wat oorbly word dan as 'n kontroleveld by die versende data gevoeg.

Maatreëls teen **aktiewe aanvalle** behels die gebruik van 'n kriptografiese sleutel wat slegs aan die afsender en ontvanger van die boodskap bekend is. Die belangrikste tegniek is die volgende [91] [77]:

- 'n **Boodskap-waarmerkingskode** ("Message Authentication Code" of MAC), ook genoem 'n kriptografiese kontroletotaal [27] is 'n waarde wat bereken word deur die hele boodskap of gedeeltes daarvan deur 'n syferstelsel te voer deur gebruik te maak van 'n private sleutel. Die afsender voeg die MAC dan by die boodskap voor dit versend word. Die ontvanger bereken sy eie MAC met ontvangs deur die gemeenskaplike private sleutel te gebruik, en vergelyk dit dan met die gestuurde MAC om te bepaal of die boodskap gewysig is tydens versending. Hierdie metode verseker dus die oorspronklikheid van die boodskap, maar laat die ontvanger steeds toe om 'n boodskap te vervals aangesien hy oor dieselfde private sleutel as die afsender beskik. 'n Voorbeeld van 'n boodskap-waarmerkingsalgoritme is DES in die syfer-blokskakel modus.

Twee eenvoudige beheermaatreëls wat vir beide toevallige foute en aktiewe aanvalle gebruik kan word, is transaksienummering en tydstempels. [23] [91]

- **Transaksienummering** behels die toekenning van sekwensiële nommers aan boodskappe of boodskapblokke ten einde te verseker dat boodskappe in die regte volgorde ontvang word.

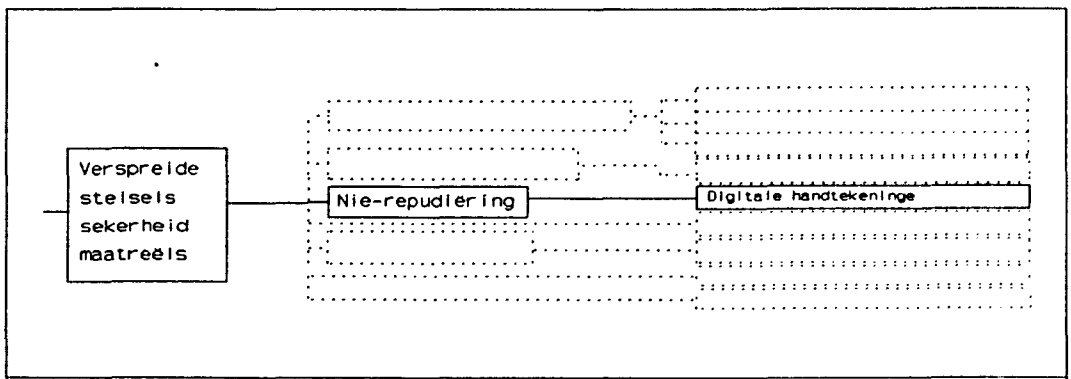
- **Tydstempels** : Deur elke boodskap of boodskapblok te merk met die datum en tyd van versending kan die ontvanger eweneens die volgorde van boodskappe kontroleer, asook dat die gaping tussen opeenvolgende boodskappe nie onreëlmatig klein of groot is nie.

3.3 Nie-repudiëring

Nie-repudiëringsmaatreëls verseker dat die afsender van 'n boodskap nie kan ontken dat hy 'n boodskap gestuur het nie, of die inhoud van die boodskap kan ontken nie. Dit verseker ook dat die ontvanger van die boodskap nie die ontvangs of die inhoud daarvan kan ontken nie. Die belangrikste beheer-

maatreël is digitale handtekeninge.

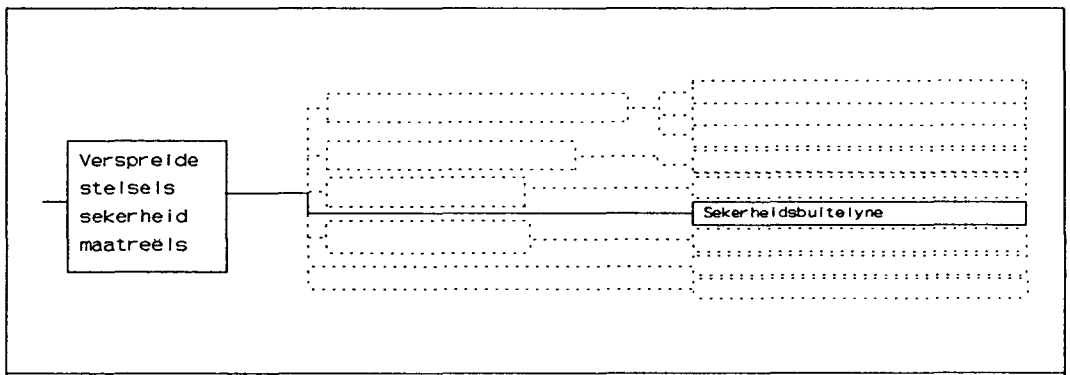
'n **Digitale handtekening** is 'n waarmerkingsmetode wat gebruik maak van 'n publieke sleutel stelsel. Die afsender gebruik sy private sleutel en pas 'n transformasie-algoritme op die boodskap toe (d.w.s. hy plaas sy unieke handtekening daarop). Die ontvanger transformeer die getekende boodskap terug na sy oorspronklike vorm deur die afsender se publieke sleutel te gebruik. Hierdie metode is die rekenaar-ekwivalent van 'n skriftelike handtekening, aangesien dit eerstens bewys dat die boodskap oorspronklik is (d.w.s. deur die ontvanger ontvang is in dieselfde vorm as wat die afsender dit gestuur het), en terselfdertyd verhoed dit ook die ontvanger om die boodskap te vervals. [27] [73] [70]



Figuur 3.10 Nie-repudiëring

3.4 Sekerheidsbuitelyne

'n Veilige netwerk of veilige deel van 'n netwerk kan beskou word asof dit binne 'n **sekerheidsbuitelyn** ("security perimeter") geleë is. Hierdie buitelyn vorm 'n logiese grens rondom 'n veilige area wat dit skei van die onveilige area daarbuite. Dit is derhalwe nie nodig om beheermaatreëls binne hierdie areas te implementeer nie aangesien sekerheid verseker word deur veilige personeel en toerusting. [71] [78]



Figuur 3.11 Sekerheidsbuitelyne

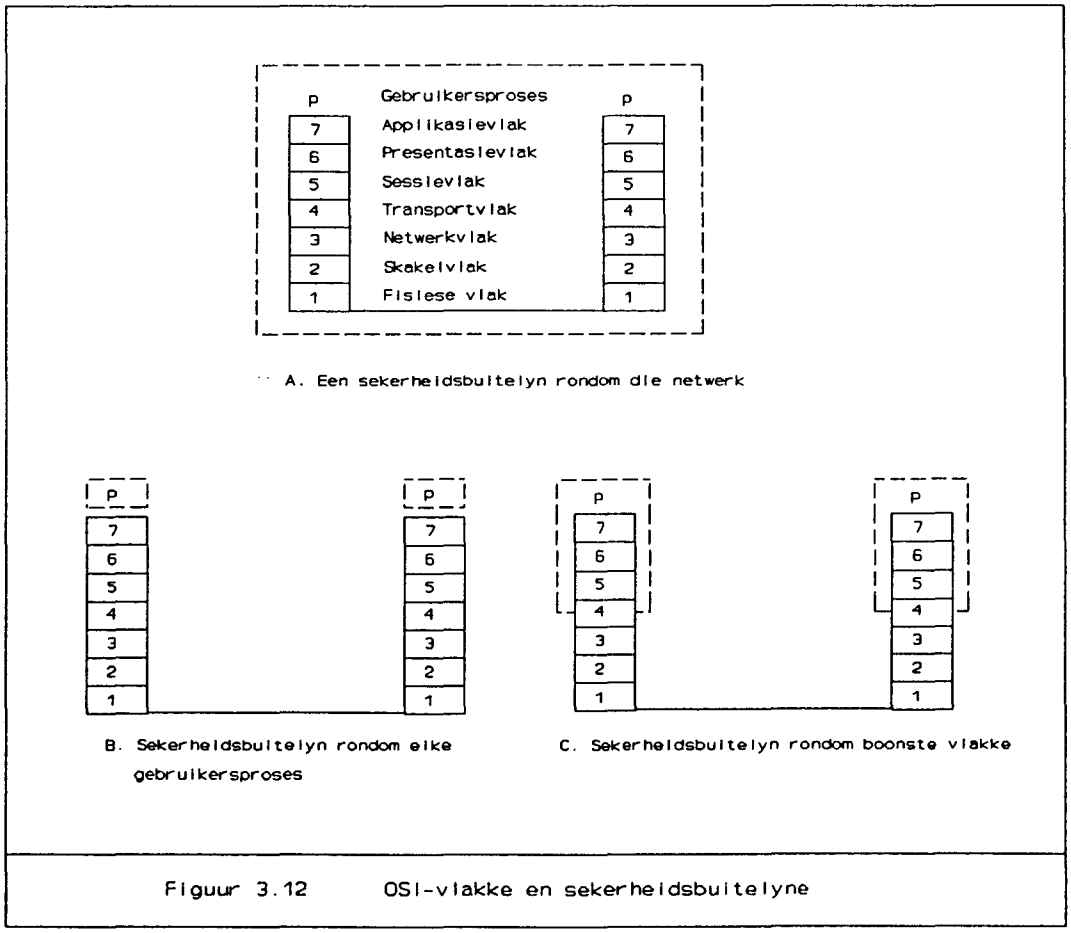
Sekerheidsbuitelyne kan op drie verskillende maniere gebruik word, nl. [16] [71]:

- **Buitelyn rondom die netwerk** : In hierdie geval kan die hele netwerk as veilig beskou word, en geen spesiale sekerheidsmaatreëls is nodig binne die netwerk nie. Sekerheidsmaatreëls word slegs op die buitenste vlak van die netwerk toegepas. (Fig. 3.12 A)

- **Buitelyn rondom elke gebruikersproses** : Elke proses word omring deur 'n sekerheidsbuitelyn, wat beteken dat elke proses sy eie sekerheidsdienste verskaf en niks binne die OSI argitektuur as veilig beskou hoef te word nie. (Fig. 3.12 B)

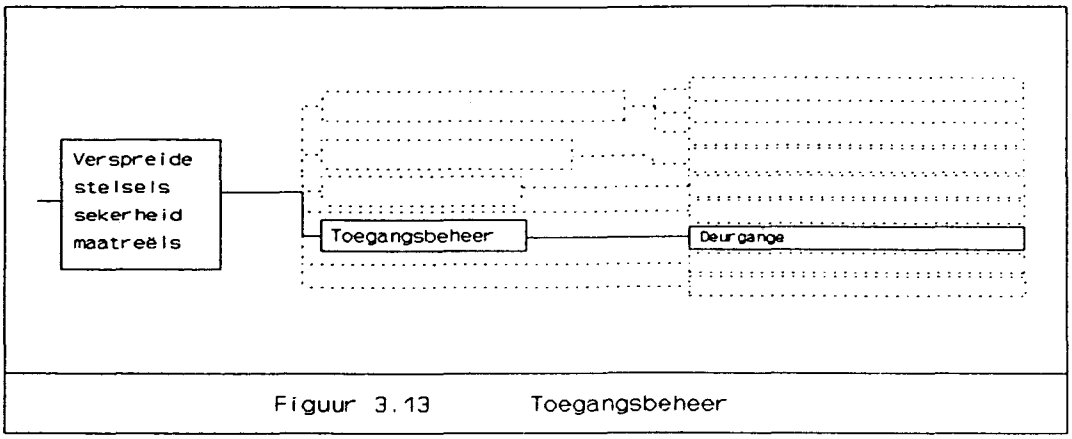
- **Buitelyn rondom boonste OSI-vlakke** : Hierdie opsie is 'n middeweg tussen die vorige twee alternatiewe. Die buitelyn word byvoorbeeld om die vierde (transport) vlak van die OSI argitektuur getrek. (Fig. 3.12 C)

Waar 'n hoë mate van sekerheid vereis word, kan verskillende sekerheidsbuitelyne op verskillende OSI-vlakke gebruik word.



Figuur 3.12 OSI-vlakke en sekerheidsbuitelyne

3.5 Toegangsbeheer



Figuur 3.13 Toegangsbeheer

Toegangsbeheer in 'n verspreide stelsels omgewing beskerm die stelsels teen ongemagtigde gebruik van hulpbronne wat toeganklik is deur 'n netwerk. Onveilige stelsels buite die sekerheidsbuitelyn kan slegs met die veilige stelsel kommunikeer d.m.v. 'n veilige **deurgang** ("gateway") wat toegangsbeheer toepas. Hierdie toegangsbeheer bepaal nie net wie toegang tot bepaalde lêerbedieners en nodes het nie, maar ook watter tipe toegang daardie stelsels of gebruikers het, bv. lees, skryf, byvoeg of skrap [42].

Toegangsbeheer op **internetwerk vlak** behels o.a. dat inkomende data volgens stelselprotokol geëtiketteer word en uitgaande data gefiltreer word sodat slegs data wat die onveilige stelsel mag verwerk, deurgelaat word. Sekerheidsbuitelyne en deurgange kan ook gebruik word om 'n groot stelsel in kleiner komponente te verdeel en die kommunikasie tussen hierdie komponente streng te beheer. [78] [70]

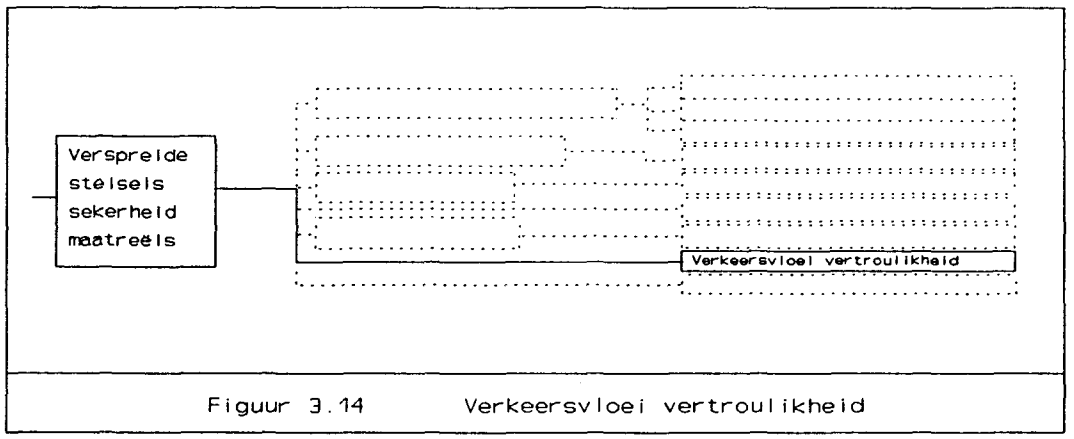
Deurgange kan geklassifiseer word as een van die volgende twee tipes [40] [70]:

- **Toepassingsdeurgange** doen omskakeling tussen verskillende protokol stelle, bv. tussen DECNET en SNA protokolle vir lêeroordrag.

- 'n **Roeteerder** ("router") beheer die roetes van pakkette tussen netwerke, bv. 'n LAN brug vir netwerke in dieselfde aanleg, of 'n internetwerk deurgang vir koppeling van netwerke deur 'n openbare datanetwerk.

3.6 Verkeersvloei vertroulikheid

Beheermaatreëls wat daarop gerig is om die vertroulikheid van verkeersvloei te verseker, verberg die frekwensie, lengte en oorsprong/bestemming patrone van die boodskapverkeer in 'n netwerk.



Figuur 3.14 Verkeersvloei vertroulikheid

Drie tegnieke wat gebruik kan word om die hoeveelheid inligting wat na 'n spesifieke node gaan, te verberg, is [79] [74]:

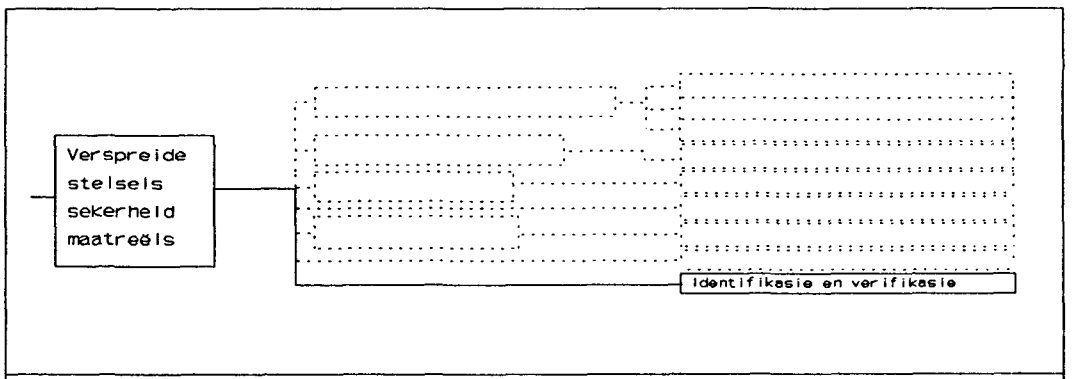
- **Verkeersopvulling** : Niksseggende boodskappe of geraas word op onaktiewe kommunikasieroetes geplaas om die indruk te wek dat daar wel kommunikasie plaasvind, met die gevolg dat roetes wat wel besig is, nie uitgesonder word nie.

- **Roetebeheer** : Boodskappe word via ander nodes na die bestemming gestuur, dus word 'n A-C boodskap bv. verberg deur twee boodskappe, A-B en B-C.

- **Skakelenkripsie** : Aangesien die adresse van die afsender en ontvanger deel is van die geënkripteerde boodskap, kan verkeersvloei nie ontleed word deur die oorsprong/bestemming adresse te monitor nie.

3.7 Identifikasie en verifikasie

Identifikasie en verifikasie in 'n verspreide stelsels omgewing het ten doel om die identiteit van die kommunikerende eweknie-entiteit en die oorsprong van ontvangde inligting te verifieer.

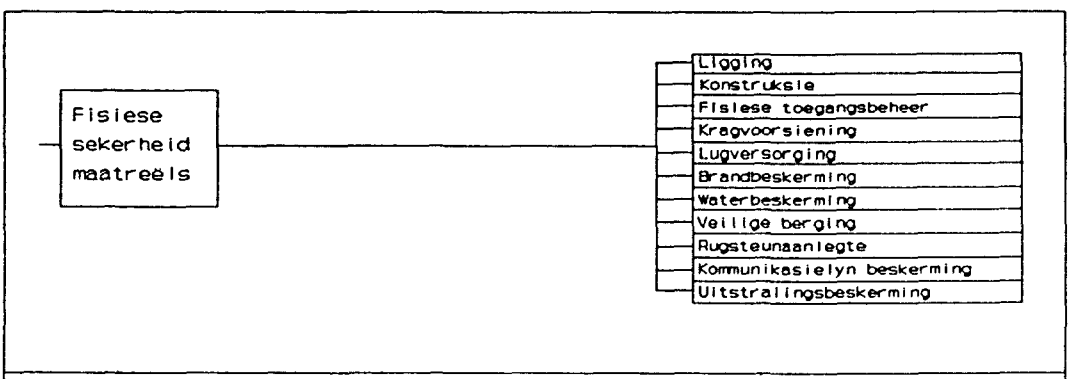


Figuur 3.15 Identifikasie en verifikasie

Die mees algemene metodes om identifikasie en verifikasie in 'n verspreide stelsels omgewing toe te pas, is **wagwoordstelsels** en **terugskakelstelsels** [42]. (sien par. 2.1.1).

4. FISIESE SEKERHEID MAATREëLS

Fisiese sekerheid maatreëls het ten doel om die sekerheid van inligtingstelsels te beskerm deur die fisiese beskadiging van of toegang tot rekenaarstelselkomponente te voorkom.



Figuur 3.16 Fisiese sekerheid maatreëls

4.1 Ligging

Die ligging van die aanleg waarin die rekenaarfasiliteit geleë is, speel 'n belangrike rol in die bepaling van die fisiese sekerheid van die rekenaarstelsel. Die aanleg moet in 'n risiko-vrye omgewing wees, d.w.s. daar moet gewaak word teen onder andere die volgende risiko-faktore in die nabyheid [102] [41] [101] [30] [62]:

- Aanlegte waar chemiese of ander plofbare of hoogs-ontvlambare stowwe verwerk of geberg word, bv. vulstasies.

- Kragtige radio- of radartoerusting wat steurings in die elektriese seine van rekenaartoerusting kan veroorsaak.

- Internasionale lughawens wat die risiko van vliegtuigongelukke vergroot.

- Riviere en die moontlikheid van vloede.

- Ondergrondse aktiwiteite soos myne.

4.2 Konstruksie

Daar is vele faktore wat in ag geneem moet word om die konstruksie van die rekenaaraanleg of die gebou waarin die aanleg is, so veilig moontlik te maak. Voorbeelde hiervan is [100] [30] [101] [62] [35]:

- Waar die rekenaarsentrum nie in 'n aparte gebou gehuisves word nie, moet die sentrum afgeskei word deur waterdigte en relatief brandvaste mure, deure, vloere en plafonne.

- Die gebou moet aan alle relevante bouregulasies voldoen en sterk genoeg ontwerp wees om omgewingstoestande soos wind, weerlig, aardbewings en vloede te weerstaan.

- Indien moontlik, moet die rekenaarsentrum weg van die kelder, grondvloer of boonste vloer van die gebou geplaas

word om die risiko van oorstromings en lekkasies uit te skakel.

4.3 Fisiese Toegangsbeheer

Die doel van fisiese toegangsbeheermaatreëls is om die hulpbronne van die inligtingstelselsafdeling, wat sensitiewe inligting en tasbare bates insluit, te beskerm deur fisiese toegang daartoe te beperk. Die toegangsbeheermeganisme moet verseker dat individue slegs toegelaat word tot die ruimte waarvoor toegang gereguleer word indien hul identiteit geverifieer is, wat aantoon dat hulle deur 'n verantwoordelike individu gemagtig is om toegang tot die area te verkry.

Daar is drie vlakke van toegangsbeheermaatreëls, naamlik toegangsbeheer tot die perseel, toegangsbeheer tot die inligtingstelselsafdeling en toegangsbeheer binne die inligtingstelselsafdeling. [56]

Toegangsbeheer tot die perseel is gerig op die voorkoming en opsporing van ongemagtigde toegang tot die gebou waarin die inligtingstelselsafdeling is. Tipies sal slegs werknemers van die betrokke organisasie toegelaat word, en sal besoekers slegs ná identifikasie en magtiging deur werknemers toegelaat word.

Toegangsbeheer tot die inligtingstelselsafdeling behels dat slegs diegene wat 'n geldige en noodsaaklike rede het om in die inligtingstelselafdeling te wees, daar toegelaat word. Hierdie area sluit alle invoer- en uitvoerareas, programmeerders- en stelselontledersareas, voorradekamer en rekenaarkamer in.

Toegangsbeheer binne die inligtingstelselsafdeling moet toegepas word sodat die mees kritiese areas net vir 'n beperkte aantal persone wat toegang daartoe moet hê, toeganklik is. Toegang tot die rekenaarkamer moet byvoorbeeld beperk word tot bedryfspersoneel wat onder andere verantwoordelik is

vir die aanskakeling van die stelsel en die installering van magnetiese bande en skyfpakke. Programmeerders en stelselontleders behoort slegs in spesiale omstandighede en onder toesig in die rekenaarkamer toegelaat te word. Net so moet toegang tot die biblioteek waarin programme, data en dokumentasie gestoor word, beperk word tot die operateurs of bibliotekarisse. [41]

Daar is hoofsaaklik vier tipes **toegangsbeheermaatreëls**. Die eerste beheermaatreël (visuele herkenning) is hoofsaaklik van toepassing op toegang tot die perseel, terwyl die ander drie beheermaatreëls op al drie bogenoemde gevalle van toepassing is, afhangende van die sekerheidsvereistes vir die spesifieke omgewing. Die vier maatreëls word vervolgens kortliks beskryf [64] [78] [74]:

- **Visuele herkenning** deur 'n wag of ontvangsdame by die punt waar ingang gereguleer word. Identiteitskaarte met die gebruiker se naam en foto kan gebruik word om die proses meer waterdig te maak. Hierdie beheermaatreël is hoofsaaklik van toepassing op toegangsbeheer tot die perseel.

- **Iets wat die gebruiker weet**, soos 'n wagwoord. 'n Tegniek wat algemeen gebruik word, is **kombinasieslotte**, wat uit 'n eenvoudige elektroniese slot bestaan wat deur die korrekte kombinasie van syfers oopgemaak word. Dit is egter nie baie veilig nie, aangesien een kode deur al die gebruikers gedeel word. Die kode moet derhalwe gereeld verander word en is dus slegs prakties in die geval waar 'n klein aantal gebruikers toegang tot 'n area het.

- **Iets wat die gebruiker besit** : 'n Voorbeeld hiervan is **vraag-antwoord** ("challenge-response") stelsels. Die gebruiker besit 'n klein elektroniese toestel wat 'n enkripsieprogram en -sleutel bevat. Die stelsel vertoon 'n ewekansige getal aan die gebruiker, en laasgenoemde voer dit in die toestel in wat dit enkripteer. Die gebruiker

voer dan weer die geënkripteerde getal in die stelsel in, waarna die stelsel dit kan verifieer met sy eie geënkripteerde getal. 'n Verdere voorbeeld is **kaarte** soortgelyk aan OTM kaarte of slimkaarte wat identifikasie-inligting aangaande die gebruiker bevat.

- **Iets aangaande die gebruiker,** byvoorbeeld **biometriese stelsels** wat gebruik maak van gebruikers se fisiese eienskappe om hul identiteit te verifieer. Stelsels wat vandag gebruik word, ondersoek bv. vingerafdrukke, palmafdrukke, retina-patrone, stempatrone en handtekeninge.

In die voorafgaande bespreking is daar as uitgangspunt geneem dat die inligtingstelselsafdeling in een bepaalde area gesentreerd is. Die toegangsbeheerproses vereis 'n veilige grens rondom so 'n area ten einde die toegang van individue tot die ruimte te reguleer. In die geval van netwerke en mikrorekenaars is dit egter nie noodwendig die geval nie, en kan die nodes en mikro's oor die hele gebou versprei wees. In só 'n geval kan die veilige area in kleiner areas verdeel word, elk met afsonderlike toegangsbeheermaatreëls.

Indien dit nie prakties uitvoerbaar is om toegangsbeheer tot elke rekenaar toe te pas nie, is dit noodsaaklik dat mikrorekenaars **vasgesluit** sal wees, en dat die rekenaarkas ook gesluit word sodat die hardeskyf byvoorbeeld nie verwyder kan word nie. Daarbenewens is dit noodsaaklik dat inligting op die hardeskyf beskerm word deur **logiese toegangsbeheermaatreëls.** (Sien par. 2.1.1 en par. 2.1.2) [95]

4.4 Kragvoorsiening

Een van die mees algemene oorsake van veral kortstondige rekenaaronderbrekings is 'n onderbreking in elektrisiteitsvoorsiening, hetsy beperk tot die gebou self of meer verspreid in die omgewing. Benewens 'n kragonderbreking moet daar ook voorsorg getref word teen onreëlmatige wisselinge in die kragstroom.

Die vier belangrikste tipes kragvoorsieningskontroles is die volgende [17] [105] [30] [50] [35] [101]:

- **Lynmonitors** wat kragprobleme identifiseer.

- **Stroomreguleerders** wat elektriese "geraas" kan beheer en stroomspanning reguleer, bv. "Constant Voltage Transformers" en "Spike Suppression Plugs".

- **Korttermyn Rugsteunkrag** wat die kragvoorsieningsfunksie outomaties oorneem sodat daar genoeg tyd is om die stelsels gekontroleerd af te sluit, bv. 'n nie-verbreekbare kragtoevoer-eenheid ("Uninterruptible Power Supply" (UPS) stelsel) (sien tabel 3.3).

- **Langtermyn Rugsteunkrag** wat krag verskaf vir solank as wat die alternatiewe energiebron beskikbaar is, bv. dieselgenerators of gasturbine stelle.

UPS bied beskerming teen die volgende bedreigings:
- Weerligstrale - Pieke in stroomspanning a.g.v. netwerkskakeling - Elektriese "geraas" veroorsaak deur masjiene, lugversorgers, kopieerders, ens. - Onderspanning en oorspanning - Frekwensie-variasies - Kragonderbrekings
TABEL 3.3 FASILITEITE VAN 'N UPS-STELSEL

4.5 Lugversorging

'n Spesiale lugversorgingstelsel behoort vir die rekenaarsentrum geïnstalleer te word waar dit prakties moontlik is. So 'n stelsel het hoofsaaklik drie funksies, naamlik [101] [30] [100]:

- **Regulering van temperatuur** om te waak teen oorverhitting van toerusting. 'n Tipiese normale temperatuurvlak is 21°C ± 2°C.

- **Regulering van humiditeit** om vogtigheidsneerslae of 'n te droë atmosfeer te voorkom. Vogtigheid lei tot korrosie en falings in stroombane, terwyl droë lug bydra tot die opbou van statiese ladings, en magnetiese bande kan laat krul. 'n Relatiewe humiditeitsvlak van 50% ± 5% is gewoonlik aanvaarbaar.

- **Onderhoud van 'n stof-vrye atmosfeer** deur slegs gesuiwerde lug in te laat, en die lugversorgde area teen 'n hoër druk as aangrensende areas te onderhou sodat enige lekkasies slegs skoon lug na buite deurlaat.

4.6 Brandbeskerming

Maatreëls wat die rekenaaromgewing teen brand beskerm, is gerig op die voorkoming, opsporing en beheer van brande.

Voorkoming

Prosedures en meganismes vir voorkoming van brande is gerig op die veilige ontwerp van die rekenaaromgewing en administratiewe maatreëls wat brand-risiko's kan verminder. Die belangrikste aspekte is die volgende [100] [101] [30] [62]:

- **Konstruksie** : Die mure van die rekenaarkamer moet strek van die ware vloer na die ware plafon, en mure, deure, vloere, plafonne en alle ander items wat in die konstruksie gebruik word, moet van relatief brandvaste materiaal gemaak word.

- **Administratiewe reëls** moet toegepas word wat die risiko van brand sal verminder. Voorbeelde hiervan is die verbied van rook in die rekenaarkamer en 'n verbod op die stoor van vlambare materiaal soos papier in die rekenaarkamer.

- Die **lugversorgingstelsel** moet temperatuur effektief beheer en afsonderlik van ander stelsels wees sodat hitte, rook en vuur nie vanaf 'n ander plek na die rekenaarkamer deurgevoer word nie. (Sien ook paragraaf 4.5)

- **Kragontkoppeling** : Die installasie moet 'n noodskakelaar hê wat in 'n noodgeval gebruik kan word om kragtoevoer na die rekenaar, lugversorging en hoof kragbron af te skakel.

Opsporing

Opsporing behels tipies die aktivering van 'n alarmstelsel en/of die inwerkstelling van rookverwydering of brandblus toerusting. Daar is drie vorms van outomatiese brandopsporingsmeganismes wat in die rekenaaromgewing gebruik kan word [41] [101]:

- **Hittesensors** reageer wanneer die temperatuur 'n sekere voorafbepaalde vlak bereik, of wanneer daar 'n onreëlmatig vinnige styging in die temperatuur is.

- **Rooksensors** verskaf 'n vroeë waarskuwing deur rook op te spoor selfs voordat enige stowwe ontvlam het. Afhangende van die betrokke omgewing, kan ioniseringsensors en/of optiese spreiding sensors gebruik word.

- **Uitstralingsensors** spoor infrarooi en ultraviolet strale op. Die meeste vlamme stuur beide hierdie tipe strale uit, terwyl baie materiale infrarooi strale uitstuur wanneer dit warm word.

Ongeag watter tipe sensormeganisme gebruik word, moet hierdie sensors geïnstalleer word in die rekenaarkamer, die kluis

waar bande en skywe gestoor word, die hoof lugversorgingstoevoer, en onder die geligte vloer. Die sensors moet gesoneer word sodat die oorsprong van die brand dadelik geïdentifiseer kan word. [30]

Brandbeheer

Maatreëls vir brandbeheer het ten doel om 'n brand so gou moontlik te blus of onder beheer te bring ten einde die skade aan bates tot die minimum te beperk. Daar is hoofsaaklik drie brandbeheer tegnieke wat in die rekenaaromgewing gebruik kan word [62] [87] [101] [61] [30] [100]:

- **Watersprinkelaars** is die mees algemene meganisme wat buite die rekenaarkamer gebruik word om brande te blus en die brandskade te beperk. Nadele van sprinkelaars is egter dat dit per ongeluk kan afgaan, die onbetroubaarheid van die aktiveringstemperatuur graderings en die omvangryke skade aan rekenaarapparatuur deur die groot hoeveelheid water. Sprinkelaars behoort dus slegs as 'n laaste alternatief gebruik te word om 'n algehele ramp te voorkom.

- **Gasoorstroming** is 'n tegniek waardeur gas wat suurstof uit die lug onttrek, in groot hoeveelhede in die rekenaarkamer ingepomp word. Die mees algemene stelsels gebruik koolstofdioksied en Halon 1301. Koolstofdioksied word aanbeveel vir gebruik in ruimtes onder die vloer of kluise waar daar nie personeel is nie, aangesien gekonsentreerde hoeveelhede daarvan skadelik vir die mens is. Halon 1301 is veral geskik vir gebruik in die rekenaarkamer aangesien dit kleurloos, reukloos, nie-geleidend, nie-lewensgevaarlik is en geen oorblyfsels laat na gebruik nie.

- **Hand-brandblussers** is veral nuttig in gevalle waar die brand buite die rekenaarkamer is en die omvang daarvan klein genoeg is dat die sprinkelaarstelsel nie geaktiveer word nie. Koolstofdioksied brandblussers wat vir elektriese brande gebruik kan word, behoort strategies deur die

gebou versprei te wees en alle personeel moet opgelei word in die gebruik daarvan. Water brandblussers moet ook beskikbaar wees vir nie-elektriese brande.

4.7 Waterbeskerming

Alhoewel waterskade gewoonlik geassosieer word met vloede en storms, is die grootste oorsake daarvan minder dramatiese gebeure soos lekkasies, verstoppings, kondensasie op toerusting of selfs die foutiewe aktivering van die sprinkelaarstelsel. Benewens die ligging en konstruksie van die rekenaarsentrum (sien par. 4.1 en 4.2) kan die volgende maatreëls aangewend word om waterskade te voorkom of te beperk [35] [80] [100]:

- **Vogtigheidsensors** : Daar is drie basiese tipes sensors wat gebruik kan word om vogtigheid op te spoor. Kabelsensors bied kontinue dekking oor 'n area, puntsensors monitor 'n bepaalde punt, en bandsensors monitor 'n bepaalde sone. Hierdie toestelle moet onder geligte vloere en naby lugversorgers, verkoelde watereenhede, bevogtigers en ontvogtigers geplaas word.

- **Insuleer** waterverkoelingspype en ander waterpype sodat water nie op toerusting drup of kondenseer nie.

- Voorsien **seile of plastiekbedekkings** om toerusting te bedek in geval van waterlekkasies of sprinkelaaraktivering.

- Installeer 'n **waterpomp** of hou 'n draagbare pomp byderhand om groot hoeveelhede water te verplaas.

4.8 Veilige Berging

Veilige berging behels dat alle dokumentasie en magnetiese media (rekords) beskerm word teen onopsetlike sowel as kwaadwillige beskadiging terwyl dit nie gebruik word nie. Die belangrikste prosedures is die volgende [41] [100]:

- Rekords wat binne die rekenaararea gehou word, moet in 'n veilige **brandkluis** geberg word en beperk word tot die minimum wat nodig is vir die doeltreffende bedryf van die rekenaarstelsel.

- **Buite-aanlegte** kan gebruik word om rekords wat min gebruik word en rugsteunkopieë te berg, mits dit eweneens in veilige brandkluise gestoor word.

- **Vervoer** van media tussen die rekenaarsentrum en bergingsareas moet slegs deur betroubare persone gedoen word.

4.9 Rugsteunaanlegte

Rugsteunaanlegte dien as alternatiewe fasiliteite waar die bedryf van kritiese stelsels voortgesit kan word wanneer 'n omvangryke ramp die beskikbaarheid van die bestaande rekenaarfasiliteit belemmer.

Daar is ses verskillende alternatiewe by die keuse van 'n rugsteunaanleg [83] [34] [67] [84] [90] [72] [69]:

- **Fasiliteite deur verskaffer voorsien** : Toets- en demonstrasiesentrums van die oorspronklike verskaffer van apparatuur en programmatuur kan op die korttermyn gebruik word.

- **Kommersiële diensburo's** is organisasies wat 'n rekenaarinstallasie in stand hou en dan die rekenaartyd aan gebruikers verhuur wat nie 'n eie installasie kan bekostig nie, of wat die fasiliteite vir 'n bepaalde tyd nodig het.

- 'n **Gedeelde rugsteunfasiliteit** behels dat een organisasie 'n rugsteunaanleg in stand hou en verskillende organisasies kan dan as intekenaars op hierdie diens inskryf teen 'n maandelikse of jaarlikse paaiement. Die hoofraam- en randapparatuur word só gekies dat dit aanpasbaar is met die rekenaartoerusting van die deelnemende organisasies.

- Deur **wedersydse ooreenkomste** gaan een organisasie 'n ooreenkoms met 'n ander organisasie aan wat 'n soortgelyke apparatuurkapasiteit en konfigurasie het om, in geval van 'n noodtoestand, die beskikbare fasiliteite met mekaar te deel.

- **Duplikaataanlegte** is fasiliteite soortgelyk aan maar geografies verwyderd van die oorspronklike fasiliteite. Daar word onderskei tussen 'n "**hot site**" en 'n "**warm site**". By eersgenoemde fasiliteit word duplikate van die apparatuur, randapparatuur, stelselprogrammatuur en ten minste die kritiese toepassings en data van 'n organisasie in stand gehou. Afhangende van die spesifieke organisasie word die duplikaatstelsel intyds, daagliks, weekliks of maandeliks bygewerk deur die programmatuur en data van die oorspronklike stelsel te rugsteun. Laasgenoemde fasiliteit verskil in dié opsig dat slegs duplikate van die apparatuur, randapparatuur en stelselprogrammatuur in stand gehou word.

- **'n Leë Dop** ("Cold Site") is 'n fasiliteit wat ten volle toegerus is om 'n rekenaarsentrum te huisves, maar dit bevat geen apparatuur voordat die noodsituasie ontstaan nie. Dit sluit in krag en bedrading, lugverkoeling, geligte vloere en telekommunikasietoerusting.

Tabel 3.4 vergelyk die verskillende alternatiewe aan die hand van relevante kriteria.

	Vers-kaffer	Diens-buro	Deelfasi-liteit	Wedersydse ooreenkoms	Duplikaat aanleg	Leë Dop
Koste	L	L - H	M	L	H	L
Gereedheid	M	L - M	H	M	H	L
Aanpasbaarheid	M	M	H	M - H	H	H
Administratiewe beheer	L	L	H	L	H	H
Toetsfasiliteite	L	L	H	L	H	L
Sekerheid	L	L	M - H	L	H	H
Eksklusiewe gebruik	L	L	M	L	H	H
Langtermyn	L	L	M - H	L	H	H
Betroubaarheid van diens	L	L	M - H	L - M	H	H

TABEL 3.4 OPSOMMING VAN RUGSTEUNALTERNATIEWE

L = Geen tot Laag / Nooit tot Selde	M = Gemiddeld / Soms	H = Hoog tot Ten Volle / Dikwels tot Altyd

4.10 Kommunikasielyn beskerming

Kommunikasielyne is blootgestel aan inluistering deurdat 'n aanvaller die sein onderskep tussen kommunikerende stelsels. Daar word onderskei tussen **passiewe** inluister waar die vertroulikheid van die boodskap verbreek word, en **aktiewe** inluister waar die vertroulikheid en integriteit van die boodskap verbreek word. Die tipe kommunikasiemedium wat gebruik word, het 'n invloed op kommunikasiesekerheid aangesien dit moeiliker is om op sommige media in te luister as op ander. Die mees algemene kommunikasiemedia is kabel, mikrogolf, satelliet en optiese vesel. [74]

Dit is bykans onmoontlik om openbare kommunikasielyne, mikrogolf- en satellietseine fisies te beveilig. Die volgende basiese veiligheidsmaatreëls kan egter as 'n eerste linie van beveiliging dien [56] [76]:

- **Toegangsbeheer** : Sluit die skakelbord kas waarin die verskillende kommunikasielyne verbind word en beperk toegang daartoe op uiters selektiewe basis.

- **Isolasie** : Kommunikasielyne wat binne die organisasie se beheer is, kan in metaalpype in sement vasgelê word om dit ontoeganklik vir 'n aanvaller te maak.

- **Inspeksie** : Kommunikasielyne moet periodiek geïnspekteer word om enige tapsnitte in die lyne op te spoor.

4.11 Uitstralingsbeskerming

Elektroniese toerusting, waaronder rekenaarapparatuur soos skerms, skyfaandrywers, verwerkers en kabels, straal elektromagnetiese seine uit. Hierdie seine kan op 'n afstand ontvang en gedekodeer word ten einde die data wat deur die apparatuur verwerk word, te rekonstrueer.

In die laat vyftigerjare het die Amerikaanse regering 'n program genaamd **TEMPEST** op die been gebring wat ten doel gehad het om die uitstralingsprobleem te hanteer. TEMPEST het sedertdien 'n oorkoepelende term geword vir die tegnologie wat seinuitstralings van elektroniese toerusting beperk, en die program word tans gebruik om te sertifiseer dat rekenaartoerusting nie opspoorbare seine uitstraal nie. [78]

Daar is hoofsaaklik twee benaderings wat gevolg kan word om aan die TEMPEST vereistes te voldoen [74] [50] [78]:

- Deur **afskerming** word 'n toestel met 'n geleidende omhulsel omsluit. Sodoende word die seine wat uitgestraal word, versprei in die geleier en kan geen inligting daaruit afgelei word as dit onderskep word nadat dit deur die geleier gegaan het nie. Voorbeelde hiervan is 'n koperomhulsel wat om 'n elektriese kabel geplaas word, of afskerming van 'n hele gebou deur 'n skerm in die mure en plafon in te bou.

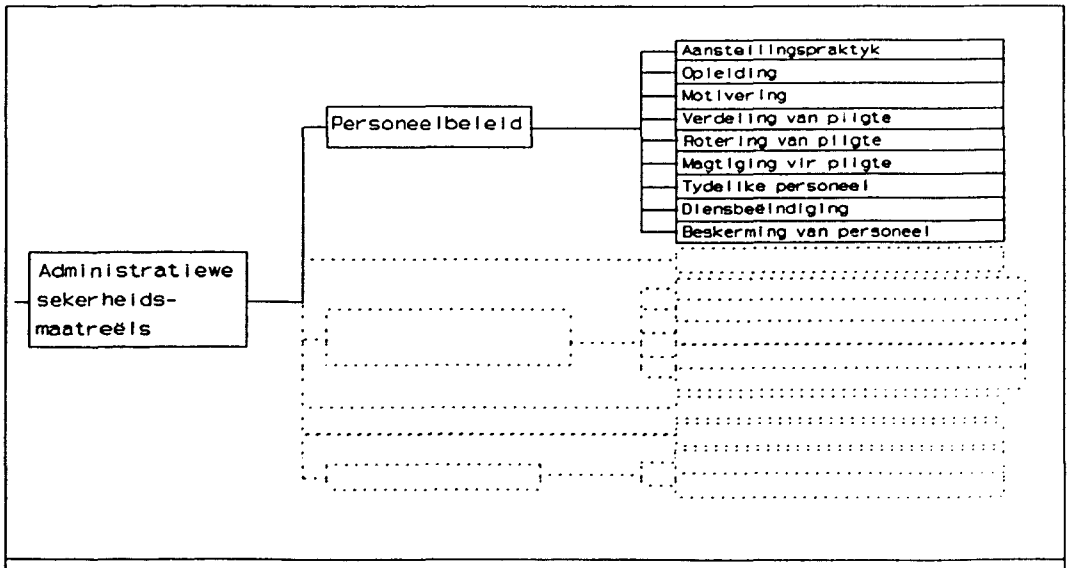
- **Uitstralingsmodifikasie** : Produkte word só ontwerp dat seine by die bron gewysig word deur die byvoeging van nagemaakte seine. Hierdie tegniek is egter tegnologies meer ingewikkeld as die afskermingsbenadering.

Die WNNR het in 1986 - 1988 ook bewys dat plasing van apparatuur verder as 200 meter vanaf die punt van ontvangs effektief is om die moontlikheid van ontvangs van apparatuurseine uit te skakel. Hierdie tegniek is egter nie altyd prakties uitvoerbaar nie.

5. ADMINISTRATIEWE SEKERHEIDSMAATREËLS

Administratiewe sekerheidsmaatreëls is beheermaatreëls wat gerig is op die suksesvolle implementering van toepassing-, fisiese en logiese sekerheid, en wat toegepas word deur organisatoriese konvensies, reëls en regulasies.

5.1 Personeelbeleid



Figuur 3.17 Personeelbeleid

5.1.1 Aanstellingspraktyk

Uit 'n sekerheidsoogpunt is dit noodsaaklik dat 'n nuwe werknemer nie 'n risiko vir die organisasie is nie. Die belangrikste maatreëls wat toegepas kan word om dit te voorkom, word vervolgens bespreek.

- **Interne werwing** behels dat 'n bestaande werknemer eerder vir 'n sensitiewe pos oorweeg word, aangesien hy reeds 'n veronderstelde lojaliteit teenoor die organisasie het. Dit is egter nie altyd prakties moontlik nie en waar 'n

eksterne applikant beter gekwalifiseerd is, behoort hy ná 'n deeglike sekerheidsklaring eerder aangestel te word. [30]

- **Onderhoude** met applikante waarin die tegniese- sowel as die sekerheidsgeskiktheid van die applikante getoets word. [41]

- **Verifiëring** van elke applikant se opvoedkundige kwalifikasies, vorige werksondervinding, mediese geskiedenis, besigheidsverwysings en persoonlike verwysings. [102]

- **Sielkundige- en persoonlikheidstoetse** waarin applikante se geskiktheid vir 'n pos getoets word tesame met die mate van integriteit en eerlikheid waaroor hulle beskik. [22]

- 'n **Vetroulikheidsooreenkoms** moet met elke nuwe werknemer gesluit word, waarin die werknemer se verantwoordelikheid om die organisasie se inligting te beskerm, uitgespel word. Benewens die sekerheidsbeskerming wat die ooreenkoms bied, verskaf dit ook aan die werkgewer wetlike ondersteuning om op te tree in 'n geval waar 'n werknemer verantwoordelik is vir 'n opsetlike breuk in sekerheid. [104] [65]

- **Periodieke herevaluering** van werknemers se verbintenis tot die organisasie se doelwitte en die nakoming van die vertroulikheidsooreenkoms moet gedoen word om probleemgevalle te identifiseer. [17]

5.1.2 Opleiding

Opleiding van werknemers behels dat hulle vertroud gemaak word met die werksomgewing ten einde nalatige en onopsetlike foute uit te skakel wat die vertroulikheid, integriteit of beskikbaarheid van stelsels kan kompromitteer. Opleiding kan in die volgende twee kategorieë verdeel word:

- **Sekerheidsopleiding** is gerig daarop om 'n algemene sekerheidsbewustheid by gebruikers te kweek deur hulle vertroud te maak met die risiko's wat gepaard gaan met 'n breuk in sekerheid, die doel van sekerheid, die toepassing van gesonde sekerheidsprosedures en die hantering van beheermaatreëls soos toegangsbeheer. [17]

- **Tegniese opleiding** het ten doel om die bedreiging wat a.g.v. onervare, swak opgeleide of nalatige werknemers ontstaan, sover moontlik uit te skakel. Werknemers moet vertroud gemaak word met alle relevante funksies en fasiliteite van stelsels wat hulle gebruik. Dit kan bv. gedoen word deur deeglike toesig oor en leiding aan onervare werknemers. [30] [22]

5.1.3 Motivering

Werknemers wat gefrustreerd is met hul werksomstandighede en 'n mindere mate van lojaliteit teenoor die organisasie het, bied 'n wesenlike bedreiging vir sekerheid. Aggressie wat kan lei tot 'n aanval op die bron van frustrasie (d.i. die organisasie of die rekenaarstelsel) is 'n erkende gevolg van 'n gebrek aan motivering in die werksituasie [52]. Dit is derhalwe noodsaaklik dat werknemers voortdurend gemotiveerd en gelukkig in hul werksituasie is.

Faktore wat bydra tot hierdie gemotiveerde houding, is o.a. die volgende [52] [22]:

- **Bevorderingsgeleenthede** en 'n voortdurende evaluering van 'n werknemer se prestasie wat lei tot bevordering.

- **Werkersdeelname** in bestuursbesluite wat werknemers op direkte of indirekte wyse raak.

- Toekenning van **verantwoordelikhede** aan werknemers.

- **Tegniese ondersteuning**, veral aan onervare werknemers.

- Gesonde **interpersoonlike verhoudings** met bestuurders en eweknie-kollega's.

- Voldoende **salarisse** en **werksekuriteit**.

- Erkenning van die belangrikheid van die **informele organisasie**.

- Prosedures en kanale waardeur **klagtes** en probleme opgelos kan word.

- 'n Gemaklike en gerieflike fisiese **werksomgewing**.

5.1.4 Verdeling van pligte

Hierdie tegniek berus op die beginsel dat dit moeiliker vir 'n individu is om 'n misdryf te pleeg wanneer hy die samewerking van ander werknemers daarvoor nodig het. Dit verhoed een persoon of 'n groep persone om een tipe transaksie of funksie so te domineer dat verlies aan sekerheid nie opgespoor word nie. Dit het die volgende implikasies [96] [101] [17] [87] [56]:

- Een taak word opgebreek in 'n aantal **verskillende take** wat deur verskillende individue verrig word.

- Die vermoë van een individu om beheer oor meer as een **funksionele area** uit te oefen, word beperk.

- **Individuele beheer** word beperk deurdat 'n sensitiewe taak, byvoorbeeld dié van 'n rekenaaroperateur, deur ten minste twee persone uitgevoer moet word.

- Hierdie beginsel sluit ook die **"need-to-know"** beginsel in, wat behels dat inligting wat aan werknemers gegee word, beperk word tot dít wat nodig is om hul werk doeltreffend uit te voer.

5.1.5 Rotering van pligte

Waar moontlik moet pligte tussen verskillende werknemers op 'n willekeurige basis periodiek geroteer word. Die tyd en detail van die rotering moet egter nie vooraf bekend gemaak word nie. Hierdie tegniek ontmoedig 'n aanvaller aangesien die waarskynlikheid dat 'n misdryf opgespoor sal word, vergroot wanneer sy pligte onverwags deur 'n ander persoon vervul word.

5.1.6 Magtiging vir pligte

Die magtigingsproses behels die evaluering van elke werknemer individueel om te bepaal tot welke vlakke van sensitiwiteit hy toegang mag hê vir verskillende take. Hierdie magtiging vorm die basis vir logiese en fisiese toegangsbeheer. (Sien par. 2.1.2 en par. 5.3)

5.1.7 Tydelike personeel

Kontrakprogrammeerders, konsultante, diensverteenwoordigers en ander tydelike personeel bied 'n sekerheidsrisiko aangesien hulle nie deur dieselfde mate van lojaliteit aan die organisasie verbind word as vaste werknemers nie, en hulle enige tyd vir 'n ander (moontlik kompeterende) organisasie kan gaan werk. Twee voorsorgmaatreëls wat getref kan word, is die volgende [65] [102]:

- Hierdie persone moet spesiale ondernemings soortgelyk aan die vertroulikheidsooreenkomste van vaste personeel teken, waarin hulle hulself verbind tot die handhawing van die organisasie se sekerheid.

- Die risiko van tydelike personeel kan in 'n mate verminder word deur slegs van geakkrediteerde tydelike personeel gebruik te maak (d.i. personeel wat bv. deur 'n hoog-aangeskrewe personeelagentskap aanbeveel word).

5.1.8 Diensbeëindiging

Waar 'n werknemer, veral 'n programmeerder of operateur, se diens beëindig word a.g.v. ontslag of bedanking, moet daar deeglike voorsorgmaatreëls getref word om te verhinder dat die werknemer - wat nou "niks het om te verloor" nie - 'n aanval op die sekerheid van die stelsel kan doen. Hierdie voorsorgmaatreëls sluit in [102] [101] [17]:

- Ernstige sekerheidsoortredings moet **onmiddellike ontslag** tot gevolg hê. Dit dien nie net as beskerming teen verdere aanvalle nie, maar dien ook as voorbeeld om die erns van sekerheid aan personeel te demonstreer.

- In die geval waar 'n werknemer **bedank**, moet die werkgewer d.m.v. 'n onderhoud met die werknemer bepaal wat die redes vir die bedanking is, ten einde vas te stel of die werknemer enige griewe het wat tot 'n aanval op sekerheid kan lei.

- Werknemers wat kennis van bedanking gee of om 'n ander nie-sekerheidsverwante rede afgedank word, moet so gou moontlik van **sensitiewe take** verwyder word.

- 'n **Formele kontrole** dat alle kopieë van handleidings, dokumentasie, programlyste ens., asook sleutels en toegangskaarte, wat in die werknemer se besit was, aan sy bestuurder oorhandig is.

- Vra die werknemer om 'n **verklaring** te teken dat hy geen vertroulike inligting wat hy in die uitvoering van sy pligte bekom het, sal oordra nie.

- Wagwoorde, identifiseerders en inskrywings in toegangsbeheerlyste wat met die werknemer geassosieer is, moet gekanselleer word.

5.1.9 Beskerming van personeel

Die vorige agt beheermaatreëls het gehandel oor die beskerming van die rekenaarstelsel teen personeel. Die ander sy van die munt van personeelbeleid, is die beskerming van die personeel teen die stelsel. Beheermaatreëls in hierdie kategorie is daarop gerig om die veiligheid van personeel te verseker in normale omstandighede sowel as in die geval van 'n ramp of noodsituasie. [101]

Voorbeelde hiervan is [100] [35]:

- 'n **Veilig ontwerpte gebou** wat aan al die bouregulasies voldoen met betrekking tot nooduitgange, brandbestrydingstoerusting, lugversorging ens.

- 'n Duidelik hoorbare **brandalarm** wat gereeld getoets word.

- 'n Vinnige en veilige prosedure om te verseker dat daar **verslag** gedoen kan word van alle persone, insluitende besoekers en tydelike werkers, tydens 'n noodgeval.

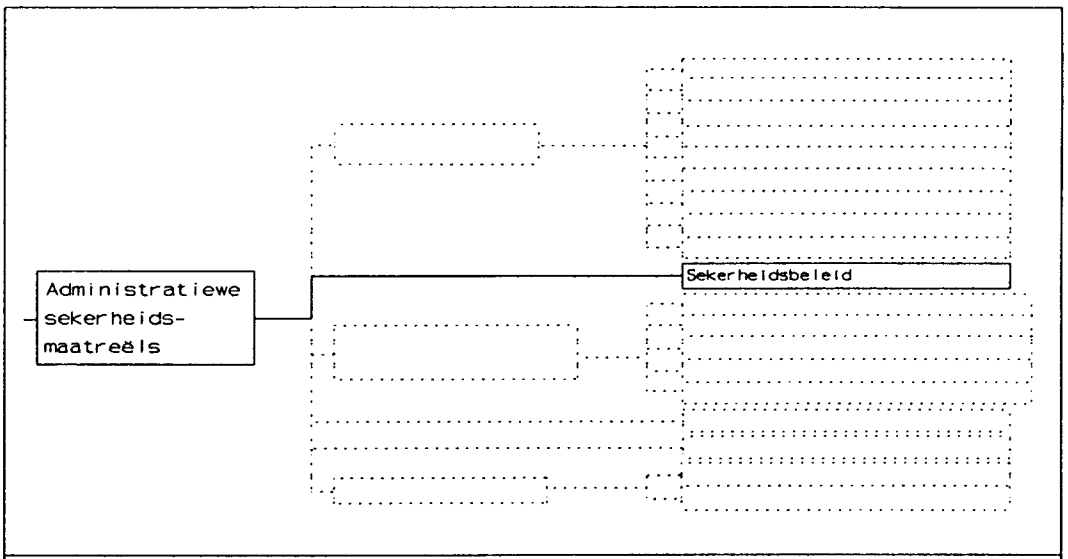
- 'n Op-datum **ontruimingsplan** wat gereeld geoefen word en wat verseker dat die gebou binne 'n aanvaarbare tyd ontruim kan word.

- 'n **Luidsprekerstelsel** wat in noodgevalle gebruik kan word om met personeel te kommunikeer.

- Kontroleer gereeld dat alle **nooduitgange** maklik van binne oopgemaak kan word en nie geblokkeer word nie.

- **Kommunikeer** alle noodprosedures aan personeel en toets die werking daarvan gereeld.

5.2 Sekerheidsbeleid



Figuur 3.18 Sekerheidsbeleid

Beheermaatreëls om sekerheid in 'n organisasie se inligtingstelsels toe te pas, moet gegrond wees op 'n korporatiewe rekenaarsekerheidsbeleid.

'n **Sekerheidsbeleid** kan beskryf word as 'n beleidsdokument wat opgestel word deur persone wat verantwoordelik is vir inligtingsekerheid binne 'n organisasie, en wat 'n uitdrukking is van die korporatiewe verbintenis tot die beskerming van die vertroulikheid, integriteit en beskikbaarheid van die organisasie se inligting.

Dit is noodsaaklik dat 'n sekerheidsbeleid deur die topbestuur van 'n organisasie uitgereik word. Eloff [29] stel dat 'n sekerheidsbeleid senior bestuur se betrokkenheid by die bekendstelling, implementering en onderhoud van 'n veilige rekenaarstelselsomgewing regdeur die organisasie, demonstreer. 'n Sekerheidsbeleid moet nie net die totale ondersteuning van topbestuur hê nie, maar topbestuur moet ook volle verantwoordelikheid neem vir die uitvoering van so 'n beleid. [89] [9]

Die volgende aspekte moet in 'n sekerheidsbeleid gedek word [29] [89] [81]:

- 'n Algemene raamwerk vir rekenaarsekerheid **terminologie** vir gebruik regdeur die organisasie.

- Die **doel en belangrikheid** van rekenaarsekerheid in terme van die organisasie se afhanklikheid daarvan.

- Die **omvang** van rekenaarsekerheid binne die spesifieke organisasie.

- Die **verantwoordelikheid en aanspreeklikheid** van alle lyn- en staffunksies t.o.v. rekenaarsekerheid in die organisasie.

- 'n Informele hoëvlak beskrywing van maatreëls vir die handhawing van **toepassingsekerheid**.

- 'n Informele hoëvlak beskrywing van maatreëls vir die handhawing van **fisiese rekenaarsekerheid**.

- 'n Informele hoëvlak beskrywing van maatreëls vir die handhawing van **logiese rekenaarsekerheid**.

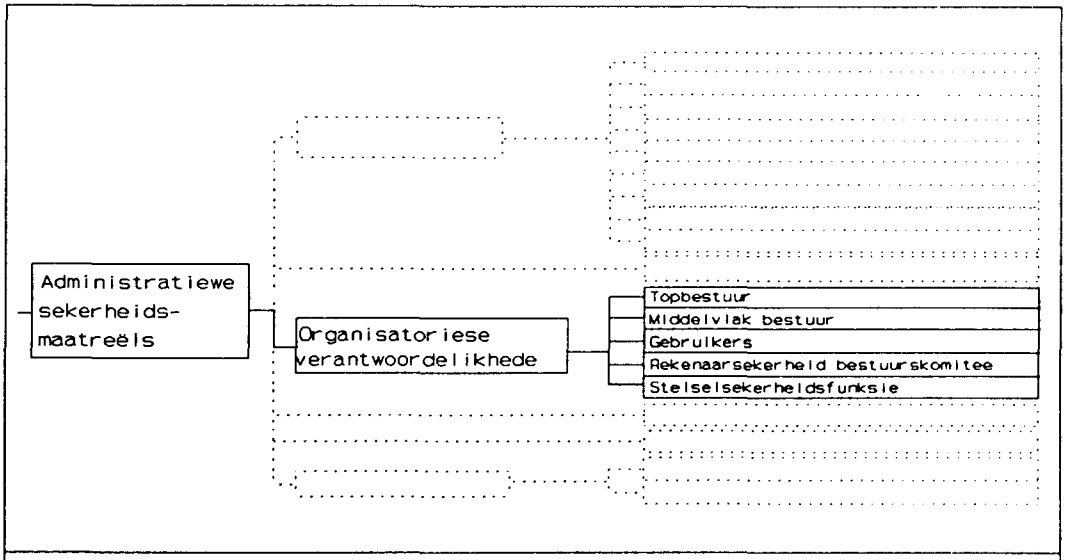
- 'n Informele hoëvlak beskrywing van maatreëls vir die handhawing van sekerheid in **verspreide rekenaarstelsels**.

- 'n Beskrywing van **administratiewe prosedures** en beginsels wat gevolg moet word vir die handhawing van sekerheid.

5.3 Organisatoriese Verantwoordelikhede

Die verantwoordelikheid om rekenaarsekerheid in 'n organisasie daar te stel en te onderhou, berus by verskillende vlakke in die organisasie, vanaf topbestuur tot by gebruikers. Dit is derhalwe noodsaaklik dat daar 'n toepaslike **organisasietruktuur** met lyn- en stafverhoudings bestaan wat die opstel

en implementering van die sekerheidsbeleid sal vergemaklik.



Figuur 3.19 Organisatoriese verantwoordelikhede

Die verantwoordelikhede van die verskillende vlakke kan soos volg opgesom word:

5.3.1 Topbestuur (Lynverhouding)

Topbestuur is uiteindelik aanspreeklik vir die doeltreffende nakoming van die organisasie se doelwitte. Aangesien inligtingstelsels en die sekerheid daarvan van deurslaggewende belang is in die bereiking van hierdie doelwitte, is dit duidelik dat topbestuur ook aanspreeklik is vir die rekenaarsekerheid van die organisasie.

Topbestuur is spesifiek verantwoordelik vir die volgende aspekte [30] [29] [98]:

- Die opstel van en 'n verbintenis tot 'n **korporatiewe inligtingsekerheidsbeleid**.

- Die toekenning van finansiële en ander **hulpbronne** om te voorsien in die inligtingsekerheidsbehoeftes van die organisasie.

- Die definiëring van 'n toepaslike **organisasiestruktuur** wat die implementering van rekenaarsekerheid op alle vlakke sal fasiliteer. Dit sluit in die aanwysing van 'n sekerheid bestuurskomitee.

- **Kommunikasie** van die sekerheidsbeleid aan alle personeel.

5.3.2 Middelvlak bestuur (Lynverhouding)
Hierdie vlak van bestuur bestaan uit **afdelingsbestuurders** van die verskillende besigheidsfunksies, bv. personeel, finansies, bemarking ens. Elke afdelingsbestuurder is verantwoordelik vir rekenaarsekerheid binne sy eie afdeling, asook vir die nakoming van die sekerheidsbeleid deur die werknemers in sy afdeling. Waar nodig, kan bestuurders hul verantwoordelikheid na die stelselsekerheidsfunksie delegeer. [29]

5.3.3 Gebruikers (Lynverhouding)
Gebruikers is verantwoordelik vir die nakoming van standaarde en prosedures in die gebruik van beheermaatreëls. Dit sluit bv. in die toekenning van regte aan ander gebruikers vir diskresionêre toegangsbeheer en die gereelde rugsteuning van data op mikrorekenaars. [30]

5.3.4 Rekenaarsekerheid Bestuurskomitee (Stafverhouding)
Hierdie komitee bestaan uit **bestuursvlak-verteenwoordigers** van alle gebruikersafdelings, rekenaarfasiliteite en inligtingstelselspersoneel. Die doel van die komitee is om die sekerheidsbeleid van die organisasie te koördineer en die doeltreffendheid daarvan te evalueer, en om beleidsbesluite te neem oor aspekte van stelselsekerheid, of om aanbevelings oor sulke besluite aan topbestuur te maak. [29] [30] [81]

5.3.5 Stelselsekerheidsfunksie (Stafverhouding)
Hierdie funksie bestaan uit 'n **gesentraliseerde groep spesialiste** wat verantwoordelik is vir die tegniese implementering van die sekerheidsbeleid, byvoorbeeld die databasisadministrateur, dataverwerkingsbestuurder, interne ouditeur,

stelselontleders en programmeerders. Die funksie staan in 'n stafverhouding tot alle ander funksies en rapporteer aan die rekenaarsekerheid bestuurskomitee.

Die funksie het onder meer die volgende verantwoordelikhede [29] [30] [81]:

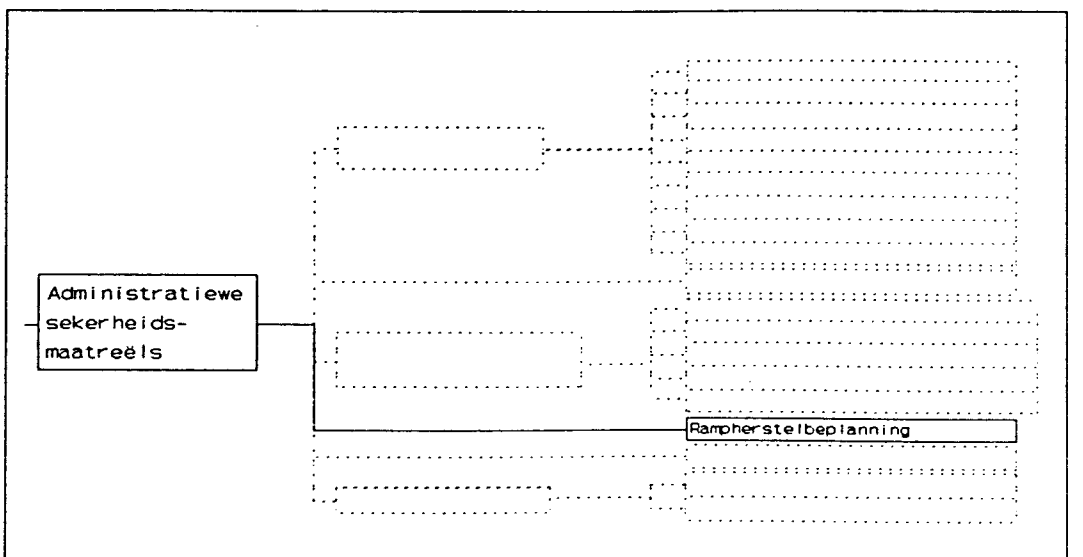
- Ontwerp en implementeer logiese sowel as fisiese beheermaatreëls binne die raamwerk van die sekerheidsbeleid.

- Ontwikkel standaarde en gedetailleerde prosedures vir die ontwerp, toetsing, implementering en evaluering van beheermaatreëls.

- Lei gebruikersgroepe op en staan hulle by in die gebruik van sekerheidsmeganismes.

- Monitor die status van rekenaarsekerheid en die nakoming van standaarde en prosedures deur stelselspersoneel en gebruikers.

5.4 Rampherstelbeplanning



Figuur 3.20 Rampherstelbeplanning

Rampherstelbeplanning is daarop gerig om die herstel van 'n organisasie se inligtingsverwerkingsvermoë te verseker in geval van 'n noodsituasie wat die beskikbaarheid van inligtingstelsels kompromitteer. 'n Kernelement van die rampherstelbeplanningsproses is die opstel van 'n rampherstelplan.

'n **Rampherstelplan** kan gedefinieer word as 'n voorafbepaalde, ten volle gekoördineerde en getoetste, logistieke plan om enige ramp te minimaliseer en te beperk, 'n vinnige en gladde oorgang na rugsteunmodus te verskaf en 'n snelle, effektiewe herstel van normale bedryf in die datasentrum te verseker. [14]

Die volgende fases in die rampherstelbeplanningsproses is reeds deur die skrywer in [13] volledig bespreek, en word hier slegs volledigheidshalwe herhaal:

- **Samestelling van 'n projekspan** : Die verantwoordelikheid vir die opstel van 'n rampherstelplan moet aan 'n groep sleutelpersone wat verteenwoordigend is van verskillende funksionele areas, opgedra word. [43] [34]

- **Risiko-analise** : Ten einde die implikasies wat 'n ramp op die organisasie kan hê, te bepaal, moet 'n kwantitatiewe of kwalitatiewe risiko-analise gedoen word. Die omvang van die risiko sal bepalend wees vir die omvang van die rampherstelplan. [39] [14]

- **Goedkeuring deur topbestuur** : Soos met alle ander aspekte van rekenaarsekerheid, is die volledige ondersteuning van topbestuur noodsaaklik vir die suksesvolle uitvoering van rampherstelbeplanning. Die resultate van die risiko-analise fase moet aan topbestuur voorgelê word sodat goedkeuring vir die opstel en implementering van 'n rampherstelplan verkry kan word. [72]

- **Identifiseer kritiese toepassings**, d.w.s. alle toepassings wat met spesifieke gereeldheid uitgevoer moet word om die organisasie te laat oorleef, en waarvan die uitvoering so gou moontlik hervat moet word na enige gebeurlikheid wat rekenaardiens onderbreek het. [83]

- **Identifiseer vereiste hulpbronne**, d.w.s. alle apparatuur, stelselprogrammatuur en personeel wat nodig is om kritiese toepassings te ondersteun. Aandag moet ook gegee word aan die vereistes vir sekerheid vir elke kritiese toepassing, en die maksimum toelaatbare "aftyd" vir elke toepassing. [83]

- **Evalueer rugsteunalternatiewe** : In hierdie fase moet 'n bepaalde rugsteunfasiliteit gekies word wat aan die betrokke organisasie se vereistes voldoen, soos wat dit in die vorige fases bepaal is. 'n Formele ooreenkoms moet ook met die verskaffer van die fasiliteit aangegaan word waarin die hoeveelheid tyd en kapasiteit wat by die fasiliteit beskikbaar is, asook elke party se verantwoordelikhede, gespesifiseer word. (Sien par. 5.9 vir 'n bespreking van rugsteunalternatiewe) [34]

- **Stel herstelspanne saam** : Alle personeel word in verskillende spanne ingedeel, en elke span is verantwoordelik vir die uitvoering van een of meer aktiwiteite van die rampherstelprogram, bv. fasiliteit voorbereidingspan, rekenaar bedryfspan, data-invoer en beheerspan, tegniese ondersteuningspan, en vervoerspan. [4]

- **Dokumentering van die plan** : Die volledige rampherstelplan moet in 'n modulêre struktuur gedokumenteer word. Die modules moet so ingedeel word dat die aard en omvang van die ramp sal bepaal welke modules uitgevoer moet word. Die dokumentasie sluit in 'n beskrywing van die plan in terme van beleid, doelwitte, aannames en beperkings, asook 'n volledige beskrywing van alle prosedures en take wat

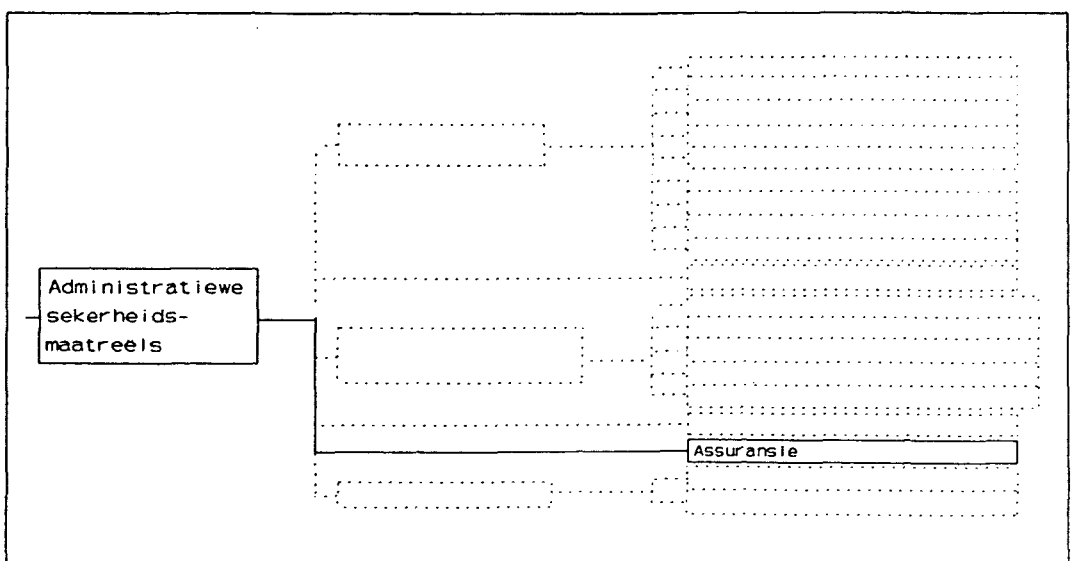
uitgevoer moet word met 'n lys van die persone wat daarvoor verantwoordelik is. [68]

- **Toetsing** : Na voltooiing van die rampherstelplan moet die plan gereeld getoets word. Dit kan die vorm aanneem van 'n stap-vir-stap deurgaan van die logika, of die fisiese uitvoering van die plan of dele daarvan in 'n nagebootste rampsituasie. [85]

- **Instandhouding** : Die inligtingstelselsomgewing van 'n organisasie is 'n dinamiese omgewing, derhalwe is dit noodsaaklik dat die rampherstelplan voortdurend bygewerk sal word om die veranderings in apparatuur, stelselprogrammatuur, toepassings en personeel te weerspieël. [57]

5.5 Assuransie

Alhoewel assuransie streng gesproke nie deur die definisie van beheermaatreëls vir rekenaarsekerheid ingesluit word nie (d.w.s. nie bydra tot die beskerming van die vertroulikheid, integriteit of beskikbaarheid van rekenaarstelsels nie), verdien dit tog vermelding in soverre dit 'n metode is om die finansiële verliese wat gepaard kan gaan met 'n breuk in rekenaarsekerheid, te verplaas.



Figuur 3.21 Assuransie

Assuransie in die konteks van inligtingstelsels word algemeen gebruik om drie breë kategorieë van verlies te dek, naamlik [101]:

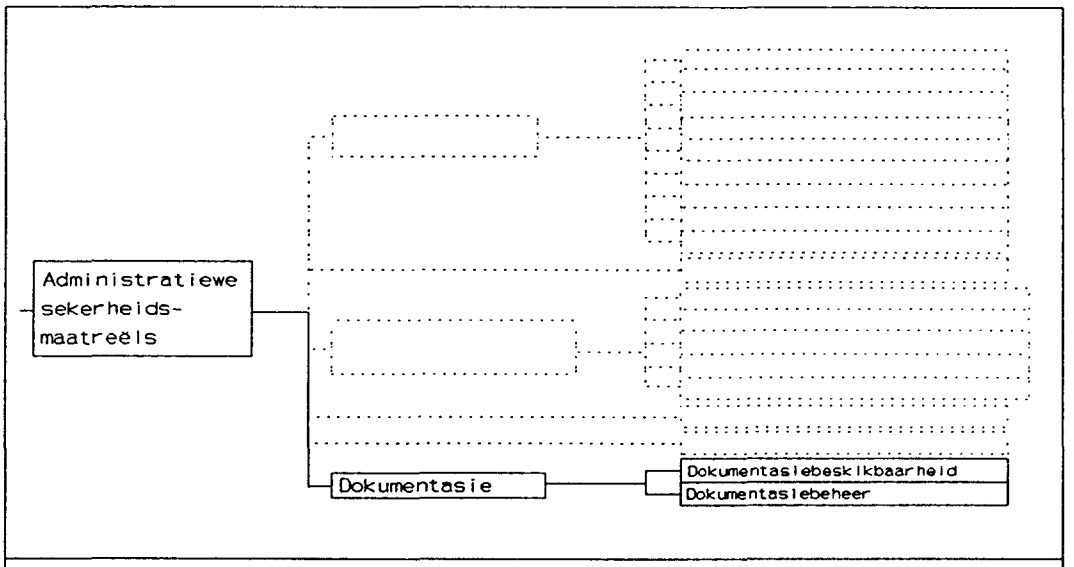
- **Materiële skade**, m.a.w. fisiese skade aan apparatuur of programmatuur wat die gevolg is van gebeurtenisse soos brand, oorstroming, diefstal, vandalisme ens.

- **Besigheidsonderbreking**, d.i. die verlies aan inkomste a.g.v. 'n onderbreking in die diens of produk wat die organisasie lewer.

- **Risiko aan en van personeel**, bv. die risiko van besering of bekendmaking van persoonlike inligting van personeel, en die risiko van oneerlike dade deur personeel of onopsetlike foute deur personeel.

5.6 Dokumentasie

Dokumentasie in die verband van rekenaarsekerheid kan gedefinieer word as **georganiseerde geskrewe inligting** wat met die ontwikkeling en bedryf van rekenaarstelsels geassosieer word. Twee oënskynlik teenstrydige aspekte is hier van belang, naamlik dokumentasiebeskikbaarheid en dokumentasiebeheer.



Figuur 3.22 Dokumentasie

5.6.1 Dokumentasiebeskikbaarheid

Voldoende dokumentasie het ten doel om stelselontleders, programmeerders, ouditeure, operateurs en gebruikers in staat te stel om die werking van die stelsel beter te verstaan. Die beskikbaarheid van hierdie dokumentasie kan stelselsekerheid verhoog deur programmeerders-, operateurs en gebruikersfoute te verminder. Dit dien ook om probleme en standaarde te kommunikeer en die stelsel oor die algemeen makliker te maak om te gebruik. [95]

Die belangrikste tipes dokumentasie is die volgende [22] [102]:

- **Probleemdefinisie dokumentasie** bestaan uit 'n geskrewe stelling van die aard en doelwitte van 'n projek en verseker dat die probleem akkuraat opgelos word.

- **Stelseldokumentasie** behels alle inligting wat nodig is om die beoogde stelsel te definieer sodat dit geprogrammeer, getoets en geïmplementeer kan word.

- **Programdokumentasie** verseker dat alle inligting wat nodig is vir 'n volledige begrip van die gedetailleerde logika van elke rekenaarprogram, voorberei word.

- **Bedryfsdokumentasie** verskaf instruksies aan bedryfspersoneel om die stelsel en die programme in die stelsel te loop.

- **Gebruikersdokumentasie** stel die gebruikers in staat om stelsels en die sekerheidsmeganismes daarvan te verstaan en dit te gebruik.

5.6.2 Dokumentasiebeheer

Elke dokumentasiekategorie moet met die toepaslike **sensitiwiteitsvlak** gemerk en daarvolgens beheer word. Slegs gemagtigde personeel behoort toegang te hê tot 'n spesifieke vlak of tipe dokumentasie op 'n "need-to-know" basis. So mag gebruikers of bedryfspersoneel byvoorbeeld nie toegang hê tot programmatuurdokumentasie nie. [22]

Rugsteunkopieë van alle belangrike dokumentasie soos bedryfsdokumentasie en gebruikersdokumentasie moet gemaak word, en sulke kopieë moet in veilige bewaring (in 'n brandkluis) gehou word by 'n buite-aanleg. [102] [22]

6. GEVOLGTREKKING

Met die skryf van hierdie hoofstuk het die skrywer 'n paar tendense geïdentifiseer.

Eerstens was dit duidelik dat, alhoewel die konsep van beheermaatreëls binne die veld van rekenaarsekerheid vanuit verskeie oogpunte (bv. toegangsbeheer, wagwoorde, biometriese stelsels, netwerksekerheid, brandbeskerming ens.) in die literatuur bespreek word, daar weinig aandag in die literatuur gegee word aan 'n oorsigtelike, bestuursgeoriënteerde beskouing van die totale komposisie van beheermaatreëls. Dit wil voorkom asof die algemene opvatting is dat die onderwerp van beheermaatreëls slegs relevant is vir rekenaarpersoneel en produkverskaffers. Die skrywer is van mening dat die kategoriseringsmeganisme wat in hierdie hoofstuk voorgestel word, 'n definitiewe bydrae kan lewer om die begrip wat 'n organisasie se bestuur van beheermaatreëls het, te verbeter. Dit is per slot van sake die bestuur wat die uiteindelike besluit moet neem of daar geïnvesteer moet word in spesifieke beheermaatreëls al dan nie.

Tweedens blyk dit dat risiko-analise pakkette meeding om 'n omvattende kennisbasis van beheermaatreëls te verkry. Die gemiddelde aantal beheermaatreëls wat sulke pakkette voorstel, is in die omgewing van 1000 (bv. die CRAMM risiko-analise pakket [21] [20]). Die identifikasie en seleksie van beheermaatreëls raak dus 'n geweldig ingewikkelde proses met hierdie magdom van alternatiewe. 'n Eenvoudige kategoriseringsmeganisme soos wat deur die skrywer voorgestel word, kan hierdie identifikasie- en seleksieproses baie vergemaklik deurdat elke beheermaatreël se posisie en funksie duideliker voorgestel kan word. Die organisasie kan dus eerstens besluit welke beheermaatreëls is nodig om in sy spesifieke behoeftes te voorsien, en dan verskillende produkte evalueer aan die hand van die beheermaatreëls wat dit bied.

Derdens is dit duidelik dat, wat die literatuur betref, die

klem in die rekenaarsekerheidsveld oor die afgelope 20 jaar verskuif het vanaf fisiese sekerheid na veral logiese sekerheid maatreëls en verspreide stelsels sekerheid maatreëls. 'n Area wat meer aandag begin geniet, is die van administratiewe maatreëls, veral personeelbeleid, sekerheidsbeleid en organisatoriese verantwoordelikhede, met 'n gepaardgaande klem op bestuursbetrokkenheid by die formulering en toepassing van sekerheidsbeleid. Hierdie area bied egter nog ruim geleentheid vir verdere navorsing.

Laastens moet daarop gelet word dat die kategoriseringsmeganisme soos in hierdie hoofstuk voorgestel, nie as 'n finale oplossing beskou moet word nie, maar bloot as 'n model wat uitgebrei en aangepas kan word na gelang van verskillende scenario's.

Die identifikasie van beheermaatreëls moet opgevolg word deur 'n keuse van 'n bepaalde stel maatreëls. Hierdie keuse moet deels gegrond word op die effektiwiteit van die verskillende maatreëls. Ten einde die effektiwiteit van 'n bepaalde maatreël te bepaal, is dit nodig om hierdie maatreël te meet aan spesifieke standaarde. In die volgende hoofstuk word die koppeling van verskillende internasionale en organisasiespesifieke standaarde met beheermaatreëls bespreek.

HOOFSTUK 4

DEFINIëRING VAN 'N RAAMWERK WAARBINNE FUNKSIONALITEIT GEKOPPEL WORD MET STANDAARDE VIR BEHEERMAATREëLS

In hoofstuk 4 word die inhoud van die vorige twee hoofstukke gekombineer ten einde 'n raamwerk daar te stel wat die beheermaatreëls wat in die vorige hoofstuk gedefinieer is, koppel met standaarde vir hierdie beheermaatreëls. Vir die doeleindes van hierdie hoofstuk word 'n **standaard** gedefinieer as die versameling vereistes wat 'n minimum vlak van werkverrigting beskryf waaraan beheermaatreëls vir rekenaarsekerheid moet voldoen.

Die **uitgangspunte** van hierdie raamwerk is soos volg :

- Dit moet omvattend en volledig wees ten einde die totale spektrum van beheermaatreëls soos in hoofstuk 3 bespreek, te dek.

- Dit moet informeel van aard wees, d.w.s. eenvoudig en verstaanbaar uit 'n bestuursoogpunt.

- Aansluiting by huidige standaarde is belangrik, maar nie ten koste van die vorige twee vereistes nie.

- Die vereistes wat gedefinieer word, moet direk gekoppel kan word aan spesifieke beheermaatreëls.

- Vereistes wat op meer as een beheermaatreël van toepassing is, word onder elke toepaslike beheermaatreël gedefinieer.

Die volgende moontlikhede is ondersoek om as vertrekpunt vir die beskrywing van vereistes te dien :

Die Oranje Boek
Die Oranje Boek beperk funksionaliteit hoofsaaklik tot vertroulikheidsaspekte, terwyl die funksionaliteit wat in hoofstuk 3 bespreek is, spesifiek ook integriteits- en beskikbaarheidsmaatreëls insluit. Die Oranje Boek beskryf ook nie vereistes vir netwerke of databasisse nie (let wel sonder inagneming van die ander boeke in die reënboogreeks).

Die Wit Boek
Alhoewel die Wit Boek vereistes vir vertroulikheid, integriteit en beskikbaarheid definieer, is die omvang daarvan beperk tot sogenaamde tegniese maatreëls, m.a.w. die logiese sekerheidsmaatreëls wat in hoofstuk 3 bespreek is. Die Wit Boek beskryf ook nie vereistes vir die argitektuur van 'n stelsel in die toepassing van sekerheid nie, terwyl die Oranje Boek dit wel doen.

'n Samevoeging van die Oranje Boek en die Wit Boek
Navorsing is reeds gedoen om 'n konsep te ontwikkel waarvolgens die Oranje Boek en Wit Boek se sekerheidsvereistes saamgevoeg kan word ten einde een universele internasionale standaard daar te stel. Hierdie werk is gedoen deur die VDMA/ZVEP werkgroep gebaseer op 'n voorstel van die Eurobit industriële beleidsgroep [31]. Die metode wat die groep gevolg het, het uit vier stappe bestaan :

- **Modularisering van TCSEC** : Die TCSEC kriteria vir beide funksionaliteit en versekering is gedeeltelik gemodulariseer tot op 'n vlak van granulariteit wat vergelyking met die ITSEC moontlik maak.

- **Modularisering van ITSEC** : Die ITSEC kriteria vir beide funksionaliteit en versekering is gedeeltelik gemodulariseer tot op 'n vlak van granulariteit wat vergelyking met

die TCSEC moontlik maak.

- **Vergelyking** : Die gemodulariseerde kriteria is met mekaar vergelyk om verskille in betekenis te bepaal.

- **Superstel** : Die gemodulariseerde kriteria is saamgevoeg om een superstel te bou.

Die resultaat van hierdie navorsing het getoon dat die afbeelding van kriteriastelle (standaarde) deur modularisering, vergelyking en saamvoeging wel uitvoerbaar is. Alhoewel die studie slegs op enkele aspekte van die kriteria gekonsentreer het om die uitvoerbaarheid van die metode te bepaal, het die werksgroep voorgestel dat verdere studie onderneem word om 'n superstel vir al die vereistes van die twee standaarde te bou.

Die saamvoeging van die Oranje Boek en die Wit Boek op hierdie vlak van detail is dus, hoewel prakties moontlik, 'n onderwerp vir verdere studie wat buite die oogmerk van hierdie hoofstuk val.

'n Uitbreiding van die Oranje Boek en die Wit boek
Die vierde alternatief, wat uiteindelik as uitgangspunt vir die beskrywing van vereistes in hierdie studie geneem is, is 'n uitbreiding op die vereistes van die Oranje Boek en die Wit Boek. Die implikasie hiervan is dat daar vir elke beheermaatreël wat in die funksionaliteitsraamwerk in die vorige hoofstuk gedefinieer is, 'n ooreenstemmende vereiste gedefinieer word wat die minimum vlak van werkverrigting beskryf waaraan die beheermaatreël moet voldoen. Waar moontlik word hierdie vereiste gedefinieer met spesifieke verwysing na die Oranje Boek en die Wit Boek.

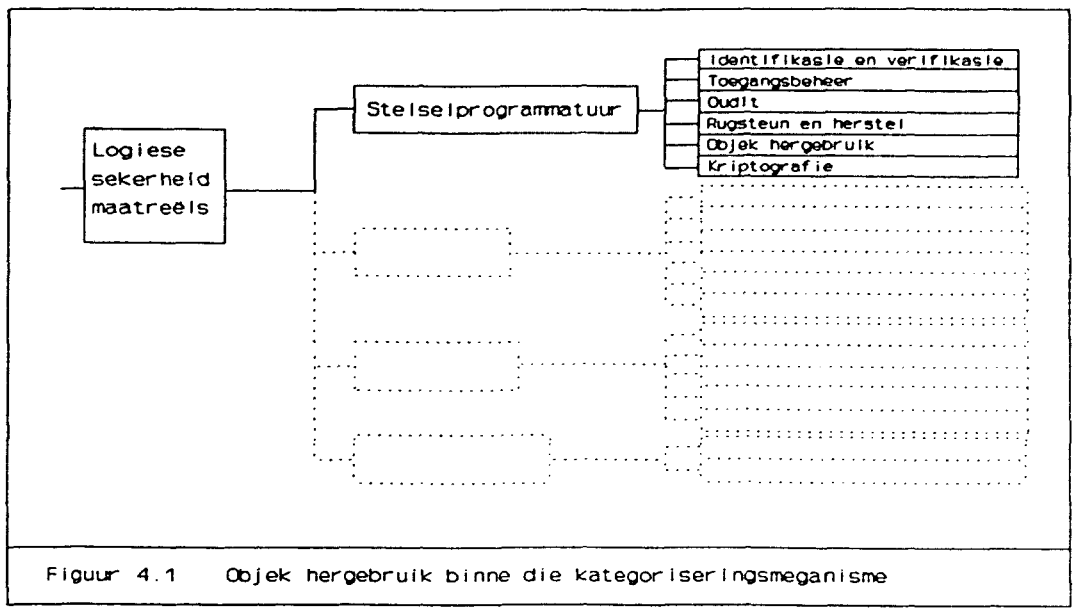
Die benadering verskil van die Eurobit benadering in die sin dat die vereistes van die Oranje Boek en die Wit Boek hier op 'n veel hoër vlak saamgevoeg word (waar moontlik) deur 'n algemene vereiste te definieer. Waar daar nie vereistes in een van die twee standaarde gedefinieer is vir 'n betrokke

beheermaatreël nie, definieer die skrywer sodanige vereiste op 'n hoë vlak.

Die resultaat van hierdie benadering is dat die vereistes wat deur die skrywer gedefinieer word, internasionale ontwikkelinge in ag neem sonder om streng daartoe gebind te wees. Hierdie benadering stel 'n organisasie in staat om vereistes te definieer volgens sy spesifieke behoeftes, met inagneming van internasionale standaarde waar dit van toepassing is.

Verduidelikende voorbeeld :
As vertrekpunt word die kategoriseringsmeganisme vir beheermaatreëls wat deur die skrywer in hoofstuk 3 gedefinieer is, gebruik. In die volgende voorbeeld word die beheermaatreël **objek hergebruik** en vereistes ten opsigte van objek hergebruik fasiliteite volledig uiteengesit soos in hoofstuk 3 en bylae A en B (sien figuur 4.1 en tabelle 4.1 en 4.2). Daarna word 'n verkorte formaat gedefinieer wat in die res van hierdie hoofstuk gebruik sal word om beheermaatreëls te koppel met standaarde.

Hoofstuk 3, par. 2.1.5 : Objek Hergebruik



Figuur 4.1 Objek hergebruik binne die kategoriseringsmeganisme

Objek hergebruik fasiliteite verskaf sekerheid deur te verseker dat wanneer 'n objek, bv. 'n lêer of aanteken ID, toegeken of hertoegeken word, daardie objek nie data bevat wat oorgebly het van vorige gebruik daarvan nie. Dit geskied byvoorbeeld deur data uit te vee deur dit fisies te oorskryf met niksseggende getalle, of deur te verhoed dat 'n spesifieke ID hertoegeken kan word. [78] [87]

Algemene objek hergebruik fasiliteite is [78]:

- Skoonmaak van geheue blokke voor dit aan 'n program of data toegeken word.

- Skoonmaak van blokke op skyf wanneer 'n lêer geskrap word of wanneer die blokke hertoegeken word aan 'n lêer.

- Demagnetisering van magnetiese bande wanneer dit nie meer gebruik word nie.

- Uitwissing van wagwoord buffers na enkriptering.

- Waar data in plaaslike geheue (bv. buffers) van drukkers of terminale geberg word, word die plaaslike geheue skoongemaak wanneer die gebruiker afteken of wanneer 'n taak voltooi is.

	Objek Hergebruik
F1	Geen vereistes
F2	Alle stoorobjekte wat terugkeer na die stelsel, word behandel voor dit hergebruik word deur ander subjekte, op so 'n wyse dat geen gevolgtrekkings gemaak kan word m.b.t. die vorige inhoud nie.
F3	Geen addisionele vereistes
F4	Geen addisionele vereistes
F5	Geen addisionele vereistes

TABEL 4.1 WIT BOEK VEREISTES (ITSEC - BYLAE B)

	Objek Hergebruik
C1	Geen vereistes
C2	Alle stoorobjekte wat terugkeer na die stelsel, word behandel voor dit hergebruik word deur ander subjekte, op so 'n wyse dat geen gevolg-trekkings gemaak kan word m.b.t. die vorige inhoud nie.
B1	Geen addisionele vereistes
B2	Geen addisionele vereistes
B3	Geen addisionele vereistes
A1	Geen addisionele vereistes

TABEL 4.2 ORANJE BOEK VEREISTES (TCSEC - BYLAE A)

Verkorte formaat

Die verkorte formaat wat in die res van hierdie hoofstuk gebruik sal word om beheermaatreëls en standaarde te koppel, word in figuur 4.2 aangedui. Die verskillende komponente van die formaat word daarna verduidelik aan die hand van die beheermaatreël Objek Hergebruik.

2.1.5 Objek hergebruik
Definisie :
Vereiste :
ITSEC :
TCSEC :
Meganismes :

Figuur 4.2 Formaat vir beskrywing van beheermaat-reëls en vereistes

2.1.5 Objek hergebruik	
Definisie :	Hierdie fasiliteite verseker dat wanneer 'n objek, bv. 'n lêer, toegeken of hertoegeken word, daardie objek nie data bevat wat oorgebly het van die vorige gebruik daarvan nie.

Die nommer van elke paragraaf (2.1.5 in die voorbeeld), stem presies ooreen met die nommer van die paragraaf waarin dieselfde beheermaatreël in hoofstuk 3 bespreek is. Sodoende word die verwysing na hoofstuk 3 vir verdere verduideliking van die beheermaatreël vergemaklik.

Die opskrif van elke paragraaf (**Objek hergebruik** in die voorbeeld) verwys na 'n spesifieke beheermaatreël op vlak 3 van die kategoriseringsmeganisme.

Die **definisie** wat na die opskrif volg, is 'n opsommende verduideliking van die funksie van die spesifieke beheermaatreël, soos dit in hoofstuk 3 volledig bespreek is. (Vir verdere verduideliking van elke beheermaatreël kan die ooreenstemmende paragraaf in hoofstuk 3 nageslaan word).

Vereiste :	Alle stoorobjekte wat terugkeer na die stelsel, word behandel voor dit hergebruik word deur ander subjekte, op so 'n wyse dat geen gevolgtrekkings gemaak kan word m.b.t. die vorige inhoud daarvan nie.

Die **vereiste** definieer die minimum funksionaliteit wat die spesifieke beheermaatreël moet bied om effektief te wees. Hierdie vereiste word in algemene terme gestel, aangesien die doel van die studie is om standaarde te koppel met beheermaatreëls en nie om 'n nuwe standaard as sodanig te definieer nie. Waar die vereiste ooreenstem met die Oranje Boek of die

Wit Boek se vereistes, word die mees basiese vereiste (d.w.s. die laagste klas bv. F1 of C1) vir die betrokke beheermaatreël beskryf. Vir verdere inligting oor die vereistes vir elke betrokke klas, verwys na bylae A (Opsomming van die Oranje Boek) en bylae B (Opsomming van die Wit Boek) aan die einde van hierdie studie.

ITSEC : Objek hergebruik (F2 - F5)

ITSEC verwys na die spesifieke vereistes en klasse van die Wit Boek wat op die beheermaatreël betrekking het. Hierdie vereistes word volledig in Bylae B uiteengesit.

TCSEC : Objek hergebruik (C2 en hoër)

TCSEC verwys na die spesifieke vereistes en klasse van die Oranje Boek wat op die beheermaatreël betrekking het. Hierdie vereistes word volledig in Bylae A uiteengesit.

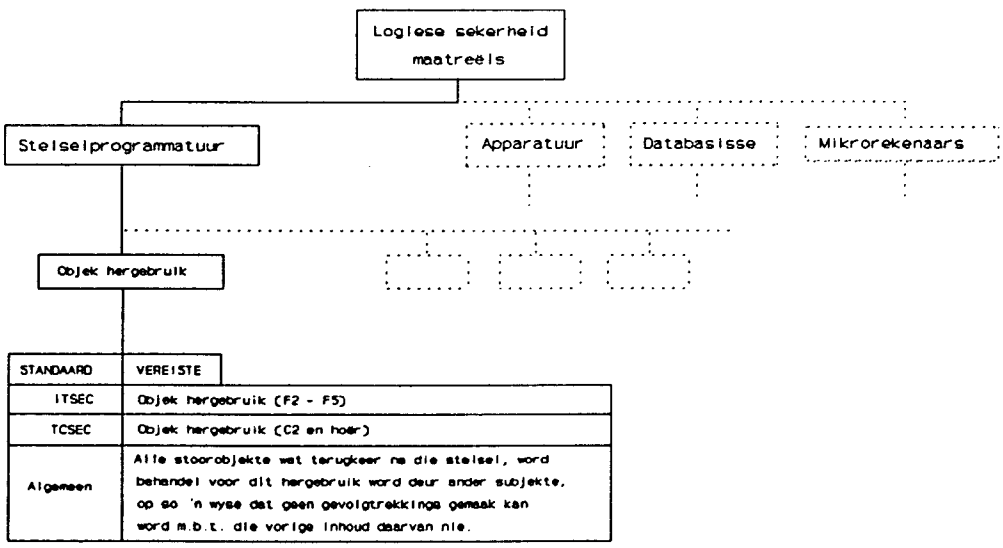
Meganismes : Uitwissing van buffers en geheueblokke, demagnetisering van bande.

Laastens word die **meganismes** wat gebruik kan word om die beheermaatreël te implementeer, gespesifiseer. Hierdie meganismes lê op vlak 4 van die kategoriseringsmeganisme en word eweneens in detail in die ooreenstemmende paragrawe in hoofstuk 3 bespreek.

Let daarop dat in die geval van TCSEC, slegs die Oranje Boek se vereistes in ag geneem is, en nie die Rooi Boek of ander boeke in die reënboogreeks nie.

Die koppeling van die beheermaatreël objek hergebruik met die toepaslike standaarde word in figuur 4.3 geïllustreer. Die algemene standaard verwys na die standaard wat die vereistes bevat wat in hierdie hoofstuk gedefinieer word, en wat 'n

uitbreiding op die TCSEC en ITSEC is.



Figuur 4.3 Koppeling van beheermaatreëls met internasionale en algemene standaarde.

1. TOEPASSINGSEKERHEID MAATREëLS

1.1 Toepassing ontwikkelingskontroles

1.1.1 Administratiewe prosedures

Definisie : Organisatoriese reëls en regulasies wat toegepas word tydens die ontwikkeling en instandhouding van toepassings.

Vereiste : Beheer oor die ontwikkeling van alle nuwe toepassings en die instandhouding van bestaande toepassings moet uitgeoefen word deur die toepassing van sekerheidsgerigte administratiewe prosedures en standaarde.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Konfigurasiebestuur, modulariteit, enkapsulering, inligtingverberging, sekerheidsoudits, onafhanklike toetsing.

1.1.2 Programbiblioteek en veranderingskontrole prosedures

Definisie : 'n Programmatuurpakket met prosedures wat programweergawes outomaties katalogiseer en beheer ten einde te verseker dat die korrekte weergawe gebruik word vir produksielopies.

Vereiste : Alle toepassings wat ontwikkel en onderhou word, moet beheer word binne die raamwerk van 'n programbiblioteek en alle veranderings aan toepassings moet aan streng kontroleprosedures onderwerp word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Programbiblioteek, veranderingskontrole prosedures.

1.2 Toepassing sekerheidsmeganismes

1.2.1 Stelselontwikkeling lewenssiklus

Definisie : Die proses waardeur sekerheidsmeganismes beplan, ontwerp, ontwikkel, getoets en in stand gehou word.

Vereiste : Ten einde te verseker dat sekerheidsmeganismes funksioneel korrek is, word die volgende onder meer vereis :

- Definiëring van sekerheidsvereistes
- Ontwerpspesifikasie en verifikasie
- Konfigurasiebestuur
- Implementering en toetsing van meganismes
- 'n Veilige ontwikkelingsomgewing
- Veilige verspreiding
- 'n Veilige bedryfsomgewing

ITSEC : Vereistes (E1 - E6)
Argitekturele ontwerp (E1 - E6)
Gedetailleerde ontwerp (E1 - E6)
Implementering (E1 - E6)
Konfigurasiebeheer (E2 - E6)
Ontwikkelaarsekerheid (E2 - E6)
Aflewering en konfigurasie (E1 - E6)
Aanskakeling en bedryf (E1 - E6)

TCSEC : Sekerheidstoetsing (C1 en hoër)
Ontwerp spesifikasie en verifikasie (B1 en hoër)
Konfigurasiebestuur (B2 en hoër)
Veilige verspreiding (A1)

Meganismes : Stelselontwikkeling lewenssiklus, programmatuur kwaliteitsversekering proses.

1.2.2 Invoerkontroles

Definisie : Beheermaatreëls wat die volledigheid en akkuraatheid van invoertransaksies vanaf brondokumente na rekenaar-leesbare vorm verseker.

Vereiste : Die stelsel moet invoerkontroles bevat wat opsetlike of onopsetlike foute tydens die invoerproses voorkom, opspoor en regstel.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Spesiaal ontwerpte vorms, logboeke, kontroletotale, kontrolevelde, waardebeperkings.

1.2.3 Verwerkingskontroles

Definisie : Beheermaatreëls wat verseker dat data korrek bygewerk word en verder verwerk word tot inligting.

Vereiste : Invoertransaksies en lêers moet getoets word vir geldigheid, verwerking van die inligting moet gevalideer word, en verslae oor die verwerkingsproses moet verskaf word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Bondelbalansering, dataredigering, datavalidering, verslae en lyste.

1.2.4 Uitvoerkontroles

Definisie : Beheermaatreëls wat die akkuraatheid en volledigheid van verwerkte inligting verifieer.

Vereiste : Uitvoer moet gekontroleer word teen invoer om die integriteit van die uitvoer te verseker, en maatreëls moet verseker dat slegs gemagtigde personeel uitvoer ontvang.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Uitvoerrekonsiliasie, veilige verspreiding.

1.2.5 Fouthantering

Definisie : Prosedures waardeur data wat vroeër foutief ingevoer is, gekorrigeer word in die data- en meesterlêers.

Vereiste : Prosedures moet voorsien word om data-foute op te spoor, dit reg te stel en die aard en frekwensie daarvan te ontleed.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Prosesverslae, foutkontrole logboek, regstellings logboek.

2. LOGIESE SEKERHEID MAATREëLS

2.1 Stelselprogrammatuur

2.1.1 Identifikasie en verifikasie

Definisie : Die proses waardeur twee verskillende entiteite, bv. 'n gebruiker en 'n stelsel, mekaar sonder enige twyfel uniek kan identifiseer as gemagtigde entiteite met wie daar op 'n bepaalde vlak van sekerheid gekommunikeer kan word.

Vereiste : Die stelsel identifiseer en verifieer gebruikers voor alle aksies tussen die stelsel en gebruikers.

ITSEC : Identifikasie en verifikasie (F1 - F5)

TCSEC : Identifikasie en verifikasie (C1 en hoër)
Veilige pad (B1 en hoër)

Meganismes : Wagwoorde, terugskakelstelsels, slimkaarte, handtekening verifikasie, vraag-antwoordstelsels.

2.1.2 Toegangsbeheer

Definisie : Die proses waardeur 'n gebruiker of stelseladministrateur toegangsregte aan verskillende subjekte toeken, en die beheer van toegang tot objekte gebaseer op die toegangsregte deur die stelselprogrammatuur.

Vereiste : Stelsel administreer en verifieer toegangsregte tussen elke gebruiker en/of gebruikersgroep en objekte onderhewig aan administrasie van regte. Aan alle stelselhulpbronne word geassosieerde sensitiwiteitsetikette toegeken.

ITSEC : Toegangsbeheer (F1 - F5)

TCSEC : Diskresionêre toegangsbeheer (C1 en hoër)
Sensitiwiteitsetikette (B1 en hoër)
Verpligte toegangsbeheer (B1 en hoër)

Meganismes : Self/groep/publieke kontroles, gidse, toegangsbeheerlyste, toegangsbeheermatrikse, vermoëns, prosedure-georiënteerde toegangsbeheer, verpligte toegangsbeheer.

2.1.3 Oudit

Definisie : Die vaslegging, ondersoek en hersien van sekerheidsverwante aktiwiteite met die doel om ongemagtigde aksies op te spoor en korrektiewe stappe te neem.

Vereiste : Die stelsel teken aksies soos toegang tot en wysiging van objekte aan en verskaf hulpmiddels vir die opsomming en ondersoek van hierdie aksies, sowel as vir selektiewe verslagdoening oor gebruikersaksies.

ITSEC : Aanspreeklikheid (F2 - F5, F6, F8, F10)
Oudit (F2 - F5, F6, F8, F10)

TCSEC : Oudit (C2 en hoër)

Meganismes : Ouditspoor, selektiewe verslae, intydse monitering.

2.1.4 Rugsteun en herstel

Definisie : Die proses waardeur kopieë van alle belangrike data en programmatuur op 'n gereelde basis veilig geberg word ten einde die stelsel ná 'n onderbreking te kan herstel na 'n toestand wat gegeld het op 'n tydstip so na as moontlik

voor die oomblik van faling.

Vereiste : Die stelsel kan herstel word ná 'n faling van individuele apparatuurkomponente, op so wyse dat alle konstant benodigde funksies deurlopend beskikbaar bly in die stelsel. Na die herstel en herintegrasie van die betrokke komponent sal die stelsel weer oor minstens die oorspronklike toleransie teen falings beskik.

ITSEC : Foutopsporing en herstel (F7)

TCSEC : Veilige herstel (B3 en hoër)

Meganismes : Rugsteun, joernalisering, herstelprosedures.

2.1.5 Objek hergebruik

Definisie : Hierdie fasiliteite verseker dat wanneer 'n objek, bv. 'n lêer, toegeken of hertoegeken word, daardie objek nie data bevat wat oorgebly het van die vorige gebruik daarvan nie.

Vereiste : Alle stoorobjekte wat terugkeer na die stelsel, word behandel voor dit hergebruik word deur ander subjekte, op so 'n wyse dat geen gevolgtrekkings gemaak kan word m.b.t. die vorige inhoud daarvan nie.

ITSEC : Objek hergebruik (F2 - F5)

TCSEC : Objek hergebruik (C2 en hoër)

Meganismes : Uitwissing van buffers en geheueblokke, demagnetisering van bande.

2.1.6 Kriptografie

Definisie : Die tegnieke waardeur data omgeskakel word vanaf gewone, leesbare teks na geheime, onleesbare vorm, asook die terugskakeling daarvan weer na leesbare vorm.

Vereiste : Die stelsel bied 'n fasiliteit om alle sensitiewe lêers, bv. wagwoordtabelle en toegangsbeheermatrikse, te enkripteer. Slegs die sekerheidsadministrateur het toegang tot hierdie fasiliteit.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Substitusie, transposisie, private sleutel stelsels (bv. DES), publieke sleutel stelsels (bv. RSA)

2.2 Apparatuur

2.2.1 Toestandveranderlikes

Definisie : 'n Argitekturele ontwerp wat die stelsel in staat stel om in spesiale veilige verwerkingstoestande bedryf te word, en wat die uitvoering van sensitiewe bewerkings of kernbeheeropdragte tot hierdie toestande beperk.

Vereiste : Die argitektuur verskaf 'n beskermde domein vir die uitvoering van sekerheidsverwante funksies, sodat gewone gebruikersprogramme nie met bevoorregte programme kan inmeng nie.

ITSEC : Geen klasse

TCSEC : Stelselargitektuur (C1 en hoër)

Meganismes : Ringgebaseerde argitektuur, bevoorregte en onbevoorregte toestande.

2.2.2 Opspoor van onwettige opdragte

Definisie : Apparatuur word gebruik om alle onwettige transaksies te onderskep en/of te kanselleer.

Vereiste : Wanneer 'n onwettige transaksie of stelselfout opgespoor word, staak apparatuur die uitvoering van alle prosesse of van die betrokke proses waarin die onwettige transaksie voorkom.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Faal-stop bewerking

2.2.3 Geheuebeskerming

Definisie : Die verdeling van geheue ten einde verskillende tipes data en prosesse van mekaar te skei en sensitiewe objekte sodoende te beskerm.

Vereiste : Verskillende prosesse word geïsoleer deur afsonderlike adresruimtes daaraan toe te ken.

ITSEC : Geen klasse

TCSEC : Stelselargitektuur (B1 en hoër)

Meganismes : Bo-en onderregisters, segmentering, paginering

2.2.4 Toegangsbeheer

Definisie : Die wyse waarop die bedryfstelsel toegangsbeheer toepas, is in hierdie geval afhanklik van die ontwerp van geheue in die apparatuur.

Vereiste : Apparatuurregisters bevat toegangsregte tot en wysers na objekte in geheue.

ITSEC : Geen klasse

TCSEC : Stelselargitektuur (C1 en hoër)

Meganismes : Sleutels en slotte, etiket-argitektuur

2.2.5 Pariteitstoetsing

Definisie : 'n Kontrolebis word bereken vir elke greep en aan die einde van die greep gevoeg ten einde die integriteit van die greep in 'n latere stadium te verifieer.

Vereiste : Pariteitsbisse word by data gevoeg en apparatuur identifiseer outomaties foute in die integriteit van die data.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Outomatiese pariteitstoetsing deur apparatuur

2.2.6 Enkripsie

Definisie : Leesbare teks word deur 'n enkripsie-algoritme omgeskakel in onleesbare teks en deur 'n dekripsie-algoritme weer teruggeskakel na leesbare teks.

Vereiste : Enkripsie- en dekripsie-algoritmes word deur middel van apparatuurtoestelle geïmplementeer.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : DES as apparatuur-gebaseerde algoritme.

2.3 Databasisse

2.3.1 Toegangsbeheer

Definisie : Die proses waardeur 'n gebruiker of stelsel-administrateur toegangsregte tot 'n databasis en entiteite daarin aan verskillende subjekte toeken, en die beheer van toegang tot objekte (entiteite) in die databasis gebaseer op die toegangsregte deur die databasis beheerstelsel.

Vereiste : Die stelsel identifiseer en verifieer gebruikers voor alle aksies tussen die gebruiker en die databasis. Die stelsel administreer en verifieer toegangsregte van gebruikers en prosesse tot spesifieke objekte of tipes objekte in die databasis.

ITSEC : Identifikasie en verifikasie (F6)
Toegangsbeheer (F6)

TCSEC : Geen klasse

Meganismes : Partisionering, integriteitslot, Hinke-Schaefer ontwerp, veilige voorkant, magtigingsreëls, enkripsie, subskemas, gebruiker-gedefinieerde prosedures, poli-instansiëring.

2.3.2 Rugsteun en herstel

Definisie : Die proses waardeur kopieë van alle belangrike data in die databasis op 'n gereelde basis veilig geberg word ten einde die databasis ná 'n onderbreking te kan herstel na 'n toestand wat gegeld het op 'n tydstip so na as moontlik voor die oomblik van faling.

Vereiste : Die databasis kan herstel word ná 'n faling van individuele apparatuurkomponente, op so wyse dat alle konstant benodigde funksies deurlopend beskikbaar bly in die stelsel. Na die herstel en herintegrasie van die betrokke komponent sal die databasis weer oor die oorspronklike toleransie teen falings beskik.

ITSEC : Foutopsporing en herstel (F7)

TCSEC : Veilige herstel (B3 en hoër)

Meganismes : Rugsteun, joernalisering, herstelprosedures

2.3.3 Oudit

Definisie : Die vaslegging, ondersoek en hersien van sekerheidsverwante aktiwiteite in 'n databasis met die doel om ongemagtigde aksies op te spoor en korrektiewe stappe te neem.

Vereiste : Die databasis beheerstelsel teken aksies soos toegang tot en wysiging van objekte aan en verskaf hulpmiddels vir die opsomming en ondersoek van hierdie aksies, asook vir selektiewe verslagdoening oor gebruikersaksies. Alle toegange op 'n rekord, veld en elementvlak moet in die ouditspoor ingesluit word.

ITSEC : Aanspreeklikheid (F6)

Oudit (F6)

TCSEC : Oudit (C2 en hoër)

Meganismes : Ouditspoor, selektiewe verslae, intydse monitering.

2.3.4 Integriteitsbeperkings

Definisie : Die voorwaardes waaraan die data in spesifieke velde in 'n databasis moet voldoen, of voorwaardes wat van toepassing is op enige verwerking van die waardes in 'n databasis.

Vereiste : Alle relevante velde in die databasis moet na wysigings getoets word ten einde te verseker dat dit aan integriteitsbeperkings voldoen.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Integriteitsmonitor

2.3.5 Gelyktydige bywerking

Definisie : Hierdie proses verwys na die hantering van 'n situasie waar twee of meer gebruikers gelyktydig besig is om bywerkings tot die databasis te maak.

Vereiste : Die databasis beheerstelsel moet 'n meganisme verskaf om te verseker dat die databasis in die geval van gelyktydige bywerking korrek bygewerk word, en dat die beskikbaarheid of integriteit van die data nie in die proses gekompromitteer word nie.

ITSEC : Kontinuïteit van diens (F7)

TCSEC : Geen klasse

Meganismes : Transaksiejoernaal, eenvoudige rekordsluiting, twee-fase rekordsluiting.

2.4 Mikrorekenaars

2.4.1 Virus beskerming

Definisie : Hierdie maatreëls is daarop gerig om die infeksie deur of voortplanting van virusse in 'n stelsel te voorkom.

Vereiste : Prosedures moet verskaf word wat virusse voorkom, virusse wat die stelsel wel infekteer verwyder of inperk, en laastens die skade wat deur virusse aangerig is, herstel.

ITSEC : Geen klasse

TCSEC : Stelselargitektuur (C1 en hoër) (Indirekte beskerming)

Meganismes : Antivuris pakkette, administratiewe prosedures, inenting, enkripsie, kriptografiese kontroletotale, toegangsbeheer programmatuur, toets-na-produksie-beheer, kompartementering, rugsteun en herstel.

2.4.2 Kopiebeskerming

Definisie : Beskerming van data en programmatuur teen ongemagtigde kopiëring met inagnemimg van die behoefte aan wettige kopieë.

Vereiste : Die stelsel moet prosedures verskaf om te verhoed dat gebruikers ongemagtigde kopieë van

data en programmatuur maak. Terselfdertyd moet gebruikers egter in staat wees om wettige kopieë te maak ten einde die beskikbaarheid van data en programme te verhoog.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Ongeldige formaat, falingsbisse, unieke serienommer, kriptografiese verwerker.

3. VERSPREIDE STELSELS SEKERHEID MAATREëLS

3.1 Vertroulikheidsmaatreëls

3.1.1 Blok/stroomsyfers

Definisie : Bloksyfer verwys na 'n enkripsie-algoritme wat op 'n blok teks toegepas word; stroomsyfer verwys na 'n enkripsie-algoritme wat op elke karakter individueel toegepas word.

Vereiste : In die geval van 'n bis-georiënteerde kommunikasieprotokol moet die boodskap d.m.v. 'n stroomsyfer geënkripteer word, in die geval van 'n blok-gerigte kommunikasieprotokol moet die boodskap d.m.v. 'n bloksyfer geënkripteer word.

ITSEC : Data-uitruiling (F9)

TCSEC : Geen klasse

Meganismes : Enkripsiesleutel, dekripsiesleutel, enkripsie-algoritme, dekripsie-algoritme.

3.1.2 Enkripsie/dekripsie

Definisie : Enkripsie verwys na die proses waardeur leesbare teks d.m.v. 'n sleutel en algoritme omgeskakel word na onleesbare teks; dekripsie verwys na die proses waardeur hierdie onleesbare teks weer teruggeskakel word na leesbare teks d.m.v. 'n verwante sleutel en algoritme.

Vereiste : Waar kommunikasie tussen verskillende nodes of tussen 'n terminaal en verwerkingseenheid plaasvind, moet die stelsel 'n fasiliteit hê om gebruikersinligting te enkripteer voor versending en dit outomaties te dekripteer aan die ontvangskant.

ITSEC : Data-uitruiling (F9, F10)

TCSEC : Geen klasse

Meganismes : Enkripsiesleutel, dekripsiesleutel, skakelenkripsie, end-tot-end enkripsie

3.1.3 Sleutelbestuur

Definisie : Die prosedures wat verseker dat 'n hoë mate van sekerheid geld vir die generering, administrasie en verspreiding van die sleutels wat gebruik word in die enkripsie/dekripsie proses.

Vereiste : Die enkripsie/dekripsie sleutels moet so ewekansig moontlik gekies word, sleutels moet gereeld verander word, en sleutels moet beskerm word teen ongemagtigde toegang tydens of na verspreiding.

ITSEC : Data-uitruiling (F9)

TCSEC : Geen klasse

Meganismes : Pseudo-ewekansige getal generator, ewekansige bis generator, administratiewe prosedures, enkripsie/dekripsie van sleutels.

3.2 Integriteitsmaatreëls

Definisie : Die maatreëls waardeur die akkuraatheid en volledigheid van die versende boodskap gekontroleer kan word.

Vereiste : Metodes vir foutopsporing en foutkorreksie word toegepas tydens data-uitruiling. Ongemagtigde manipulering van adresvelde, gebruikersdata en oudit-data kan betroubaar as foute geïdentifiseer word.

ITSEC : Data-uitruiling (F8, F10)

TCSEC : Geen klasse

Meganismes : Pariteitstoetsing, blokkontrolesom, sikliese oortolligheidskontrole,boodskap-waarmerkingskode, transaksienummering, tydstempels.

3.3 Nie-repudiëring

Definisie : Hierdie fasiliteit verseker dat die afsender of ontvanger van die boodskap nie kan ontken dat 'n boodskap gestuur is nie, of die inhoud van die boodskap kan ontken nie.

Vereiste : Die stelsel moet 'n meganisme verskaf om die versending, ontvangs en inhoud van 'n gestuurde boodskap onweerlegbaar te bewys.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Digitale handtekening

3.4 Sekerheidsbuitelyne

Definisie : 'n Logiese grens om 'n veilige netwerk of veilige deel van 'n netwerk wat dit skei van 'n onveilige area daarbuite.

Vereiste : 'n Sekerheidsbuitelyn moet vir die stelsel of verskillende dele daarvan gedefinieer word ten einde te bepaal welke dele daarvan is veilig en welke dele moet d.m.v. beheermaatreëls beskerm word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Sekerheidsbuitelyn om netwerk, elke gebruikersproses of boonste OSI-vlakke.

3.5 Toegangsbeheer

Definisie : Beskerming van verspreide stelsels teen ongemagtigde gebruik van hulpbronne wat toeganklik is deur 'n netwerk.

Vereiste : Stelsel administreer en verifieer toegang en toegangsregte tot alle lêerbedieners en nodes in die verspreide stelsel.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Toepassingsdeurgang, roeteerder.

3.6 Verkeersvloei vertroulikheid

Definisie : Beheermaatreëls wat gerig is daarop om die aard en omvang van verkeer in 'n netwerk verberg.

Vereiste : Die stelsel moet maatreëls verskaf wat die frekwensie, lengte en oorsprong/bestemming patrone van boodskapverkeer verberg.

ITSEC : Data-uitruiling (F10)

TCSEC : Geen klasse

Meganismes : Verkeersopvulling, roetebeheer, skakelenkripsie.

3.7 Identifikasie en verifikasie

Definisie : Die proses waardeur twee verskillende entiteite, bv. twee stelsels, mekaar sonder enige twyfel uniek kan identifiseer as gemagtigde entiteite met wie daar op 'n bepaalde vlak van sekerheid gekommunikeer kan word.

Vereiste : Voor die opstelling van die verbinding word die eweknie-entiteit geïdentifiseer en geverifieer. Met ontvangs van data is dit moontlik om die afsender van die data te identifiseer en te verifieer.

ITSEC : Identifikasie en verifikasie (F8, F10)

TCSEC : Geen klasse

Meganismes : Wagwoorde, terugskakelstelsels.

4. FISIESE SEKERHEID MAATREëLS

4.1 Ligging

Definisie : Beskerming van die rekenaarfasiliteit deur die plasing van die aanleg waarin die rekenaarfasiliteit geleë is binne 'n bepaalde omgewing.

Vereiste : Die omgewing waarin die rekenaaraanleg geleë is, moet so risiko-vry moontlik wees, hetsy van natuurlike risiko's of mensgemaakte risiko's.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Omgewingsondersoeke.

4.2 Konstruksie

Definisie : Beveiliging van die rekenaaraanleg deur die struktuur van die aanleg en die materiaal waarvan die mure, deure, vloere en plafonne vervaardig is.

Vereiste : Die konstruksie moet aan alle relevante bouregulasies voldoen, en die rekenaarsentrum moet deur waterdigte en brandvaste mure, deure, vloere en plafonne omring word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Waterdigte materiaal, bouregulasies.

4.3 Toegangsbeheer

Definisie : Beskerming van die hulpbronne van die inligtingstelselafdeling deur die beperking van fisiese toegang daartoe.

Vereiste : Toegang tot die rekenaarfasiliteit moet beperk word tot individue wie se identiteit geverifieer is en wat voldoende magtiging het.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Visuele herkenning, kombinasieslotte, vraag-antwoord stelsels, slimkaarte, biometriese stelsels.

4.4 Kragvoorsiening

Definisie : Versekering van die beskikbaarheid van die rekenaarfasiliteit deur kontinue elektriese krag te voorsien.

Vereiste : Rugsteunkrag moet beskikbaar wees in die geval van 'n kragonderbreking, en onreëlmatige wisselinge in die kragstroom moet uitgeskakel word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Lynmonitors, stroomreguleerders, UPS-stelsels, dieselgenerators.

4.5 Lugversorging

Definisie : Regulering van die atmosfeer in die rekenaar-omgewing om skade aan apparatuur en media te voorkom.

Vereiste : 'n Lugversorgingstelsel moet die temperatuur, humiditeit en stof-inhoud van die atmosfeer binne aanvaarbare vlakke reguleer om apparatuur en media te beskerm.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Lugversorgingstelsel.

4.6 Brandbeskerming

Definisie : Beskerming van die rekenaaraanleg teen brand- of rookskade.

Vereiste : Beheermaatreëls moet gerig wees op die voorkoming, opsporing en beheer van alle tipes brande wat realisties verwag kan word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Konstruksie, administratiewe reëls, lugversorgingstelsel, kragdiskonnektering, hitte-, rook- en uitstralingsensors, watersprinkelaars, gasoorstroming, hand-brandblussers.

4.7 Waterbeskerming

Definisie : Beskerming van die rekenaaraanleg teen waterskade a.g.v. oorstromings of lekkasies.

Vereiste : Beheermaatreëls moet waterskade voorkom, lekkasies opspoor en die omvang van waterskade beperk.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Vogtigheidsensors, insulering van pype, plastiekbedekkings, waterpomp.

4.8 Veilige berging

Definisie : Die beskerming van alle dokumentasie en magnetiese media teen ongemagtigde toegang, onopsetlike sowel as kwaadwillige beskadiging terwyl dit nie gebruik word nie.

Vereiste : Dokumentasie en media (hetsy oorspronklikes of duplikate) moet in 'n brandvaste, waterdigte plek geberg word en toegang daartoe moet beperk word tot gemagtigde persone.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Brandkluis, buite-aanleg, veilige vervoer.

4.9 Rugsteunaanlegte

Definisie : Alternatiewe fasiliteite waar die bedryf van kritiese stelsels voortgesit kan word wanneer 'n omvangryke ramp die beskikbaarheid van die bestaande rekenaarfasiliteit belemmer.

Vereiste : In geval waar die gewone rekenaarfasiliteit nie beskikbaar is nie, moet daar 'n rugsteunfasiliteit beskikbaar wees binne 'n aanvaar-

bare tyd. Die rugsteunalternatief wat gekies word, moet aan die organisasie se spesifieke behoeftes voldoen en verliese minimaliseer.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Verskaffer fasiliteite, kommersiële diensburo's, gedeelde rugsteunfasiliteit, wedersydse ooreenkomste, duplikaataanlegte, leë dop.

4.10 Kommunikasielyn beskerming

Definisie : Beskerming van kommunikasielyne tussen netwerknodes of terminale en hoofraamrekenaars teen inluistering of boodskap-modifikasie.

Vereiste : Toegang tot kommunikasielyne en koppelings moet beperk word tot gemagtigde persone. Sover prakties moontlik, moet kommunikasielyne geïsoleer word met metaalpype in sement, en alle oop lyne moet periodiek geïnspekteer word om tapsnitte op te spoor. Die sensitiwiteit van die data wat versend word moet in ag geneem word by die keuse van die tipe kommunikasiemedium.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Optiese vesel, inspeksie, isolasie, toegangsbeheer.

4.11 Uitstralingsbeskerming

Definisie : Voorkoming van inluistering deur die afgeleë ontvangs van elektromagnetiese seine wat deur

apparatuur uitgestraal word.

Vereiste : Toerusting wat gebruik word, moet aan TEMPEST standaarde voldoen, d.w.s. elektromagnetiese seine wat deur apparatuur uitgestraal word, moet afgeskerm of gewysig word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Afskerming deur geleidende omhulsels, uitstralingsmodifikasie deur die byvoeging van nagemaakte seine, afgeleë plasing van apparatuur.

5. ADMINISTRATIEWE SEKERHEIDSMAATREëLS

5.1 Personeelbeleid

5.1.1 Aanstellingspraktyk

Definisie : Die prosedures wat gevolg word by die indiensneming van nuwe personeel.

Vereiste : Nuwe werknemers moet getoets word vir sowel tegniese as sekerheidsgeskiktheid. By aanstelling moet hulle 'n vertroulikheidsooreenkoms onderteken, en hul verbintenis tot die organisasie se doelwitte moet periodiek herevalueer word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Interne werwing, onderhoude, opvoedkundige kwalifikasies, sielkundige toetse, vertroulikheidsooreenkoms.

5.1.2 Opleiding

Definisie : Die proses waardeur werknemers vertroud gemaak word met die werksomgewing ten einde nalatige en onopsetlike foute uit te skakel.

Vereiste : Werknemers moet vertroud gemaak word met sekerheidsbeginsels en -prosedures, en voldoende tegniese opleiding ontvang om foute wat 'n sekerheidsrisiko inhou, tot die minimum te beperk.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Sekerheidsopleiding, tegniese opleiding.

5.1.3 Motivering

Definisie : Die organisatoriese maatreëls wat ten doel het om 'n positiewe en ywerige houding by werknemers te kweek en te onderhou.

Vereiste : Daar moet na werknemers se belange omgesien word, 'n positiewe ingesteldheid moet gekweek word, en werknemers se houding en motivering moet voortdurend geëvalueer word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Bevorderingsgeleenthede, werkersdeelname, tegniese ondersteuning, gesonde interpersoonlike verhoudings, salarisse en werksekuriteit, klagtehantering, gerieflike werksomgewing.

5.1.4 Verdeling van pligte

Definisie : Die beginsel dat een taak onderverdeel word in 'n aantal take ten einde individuele beheer as sekerheidsrisiko uit te skakel.

Vereiste : Geen individu moet totale seggenskap oor sleuteltake of -aspekte in die rekenaaromgewing hê nie. Sensitiewe take moet tussen meerdere persone verdeel word en aan gesamentlike evaluering onderwerp word.

ITSEC : Geen klasse

TCSEC : Veilige fasiliteit bestuur (B2 en hoër)

Meganismes : Verdeling van take, "need-to-know" beginsel.

5.1.5 Rotering van pligte

Definisie : Vermindering van individuele beheer deur pligte periodiek tussen verskillende werknemers te roteer waar moontlik.

Vereiste : Pligte moet op 'n willekeurige basis tussen werknemers geroteer word. Die tyd en detail van die rotering moet nie vooraf bekend gemaak word nie.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Rotering van pligte.

5.1.6 Magtiging vir pligte

Definisie : Die proses waardeur 'n werknemer geëvalueer word om te bepaal tot welke vlakke van sensitiwiteit hy toegang mag hê vir verskillende

take.

Vereiste : Elke werknemer moet individueel geëvalueer word om sy sekerheidsklaring te bepaal, en vir elke taak wat hy moet verrig, moet 'n spesifieke magtiging aan hom toegeken word met bepaalde toegangsregte waar van toepassing.

ITSEC : Geen klasse

TCSEC : Veilige fasiliteit bestuur (B2 en hoër)

Meganismes : Sekerheidsklaring.

5.1.7 Tydelike personeel

Definisie : Die prosedures waardeur die sekerheidsrisiko wat tydelike personeel bied, verminder word.

Vereiste : Alle tydelike personeel moet getoets word vir sowel tegniese as sekerheidsgeskiktheid. By aanstelling moet hulle 'n spesiale vertroulikheidsooreenkoms onderteken, en hul verbintenis tot die organisasie se doelwitte moet periodiek herevalueer word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Vertroulikheidsooreenkoms, akkreditering van personeel.

5.1.8 Diensbeëindiging

Definisie : Die prosedures wat gevolg word wanneer 'n werknemer se diens beëindig word.

Vereiste : Waar 'n werknemer se diens beëindig word a.g.v. ontslag of bedanking, moet daar deeglike voorsorgmaatreëls getref word om te verhinder dat die werknemer 'n aanval op die sekerheid van die inligtingstelsels kan doen.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Onmiddellike ontslag, onderhoude, verwydering vanaf sensitiewe take, verklaring van geheimhouding, kansellasie van wagwoorde.

5.1.9 Beskerming van personeel

Definisie : Die maatreëls wat getref word om die veiligheid van personeel te verseker in normale omstandighede asook in die geval van 'n noodsituasie.

Vereiste : Die veiligheid van personeel moet te alle tye verseker word deur o.a. 'n veilig ontwerpte gebou en noodprosedures.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Brandalarm, ontruimingsprosedures, luidsprekerstelsel, nooduitgange, noodopleiding.

5.2 Sekerheidsbeleid

Definisie : 'n Beleidsdokument wat 'n uitdrukking is van die korporatiewe verbintenis tot die beskerming van die vertroulikheid, integriteit en beskikbaarheid van die organisasie se inligting.

Vereiste : Alle beheermaatreëls om sekerheid in 'n organisasie se inligtingstelsels toe te pas, moet gegrond wees op 'n korporatiewe sekerheidsbeleid. Hierdie beleid moet deur die topbestuur van die organisasie uitgereik word, en die topbestuur moet ook verantwoordelikheid vir die uitvoering daarvan aanvaar.

ITSEC : Vereistes (E1 - E6)

TCSEC : Geen klasse

Meganismes : Sekerheidsdoelwitte, sekerheidsterminologie, uiteensetting van verantwoordelikhede, beskrywing van beheermaatreëls.

5.3 Organisatoriese verantwoordelikhede

5.3.1 Topbestuur

Definisie : Die verantwoordelikheid van topbestuur om rekenaarsekerheid in 'n organisasie daar te stel en te onderhou.

Vereiste : Topbestuur moet 'n korporatiewe rekenaarsekerheidsbeleid opstel en uitvoer, finansiële en ander hulpbronne voorsien, 'n toepaslike organisasiestruktuur vir die implementering van rekenaarsekerheid definieer en die sekerheidsbeleid aan alle personeel kommunikeer.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Lyngesag.

5.3.2 Middelvlak bestuur

Definisie : Die verantwoordelikheid van middelvlak bestuur om rekenaarsekerheid in die verskillende afdelings binne die organisasie daar te stel en te onderhou.

Vereiste : Elke afdelingsbestuurder moet toesien dat die korporatiewe sekerheidsbeleid vir sy eie afdeling geïnterpreteer en toegepas word.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Lyngesag.

5.3.3 Gebruikers

Definisie : Die verantwoordelikheid van gebruikers om die sekerheidsbeleid toe te pas.

Vereiste : Gebruikers is verantwoordelik vir die nakoming van alle voorafgedefinieerde standaarde en prosedures in die gebruik van beheermaatreëls.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Opleiding, kommunikasie, oudit.

5.3.4 Rekenaarsekerheid Bestuurskomitee

Definisie : 'n Komitee bestaande uit bestuursvlak-verteenwoordigers van alle gebruikersafdelings, rekenaarfasiliteite en inligtingstelsels-personeel.

Vereiste : Die rekenaarsekerheid bestuurskomitee moet die

sekerheidsbeleid van die organisasie koördineer en die doeltreffendheid daarvan evalueer, beleidsbesluite neem oor aspekte van stelselsekerheid en aanbevelings oor sulke besluite aan topbestuur maak.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Stafgesag.

5.3.5 Stelselsekerheidsfunksie

Definisie : 'n Gesentraliseerde groep spesialiste wat verantwoordelik is vir die tegniese implementering van die sekerheidsbeleid.

Vereiste : Die stelselsekerheidsfunksie moet beheermaatreëls binne die raamwerk van die sekerheidsbeleid ontwerp, implementeer, toets en evalueer. Die funksie is ook verantwoordelik vir die opleiding van en bystand aan gebruikersgroepe, en om die nakoming van standaarde en prosedures te monitor.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Stafgesag.

5.4 Rampherstelbeplanning

Definisie : Die prosedures wat daarop gerig is om die herstel van 'n organisasie se inligtingsverwerkingsvermoë te verseker in geval van 'n noodsituasie wat die beskikbaarheid van inligtingstelsels kompromitteer.

Vereiste : Die organisasie moet oor 'n op-datum rampherstelplan beskik wat alle stappe en prosedures (tesame met die verantwoordelike persone) spesifiseer wat in die geval van 'n noodsituasie gevolg moet word, van die oomblik dat die noodsituasie ontstaan totdat volledige bedryf weer herstel is.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Projekspan, risiko-analise, identifikasie van kritiese toepassings en vereiste hulpbronne, rugsteunaanleg, herstelspanne, dokumentasie, toetsing, instandhouding.

5.5 <u>Assuransie</u>

Definisie : Verplasing van finansiële verliese deur die uitneem van versekering teen skade.

Vereiste : Waar assuransie 'n beter belegging blyk te wees om finansiële verliese te verplaas as die implementering van beheermaatreëls, moet voldoende assuransie uitgeneem word om sodanige verliese te dek.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Assuransie teen verliese a.g.v. materiële skade, besigheidsonderbreking en risiko's aan en van personeel.

5.6 Dokumentasie

5.6.1 Dokumentasiebeskikbaarheid

Definisie : Die beskikbaarheid van georganiseerde geskrewe inligting wat met die ontwikkeling en bedryf van rekenaarstelsels geassosieer word.

Vereiste : Voldoende dokumentasie moet beskikbaar wees om stelselontleders, programmeerders, ouditeure, operateurs en gebruikers in staat te stel om die werking van die stelsel beter te verstaan. Die dokumentasie sluit in die volledige sekerheidsbeleid en spesifikasie van beheermaatreëls.

ITSEC : Gebruikersdokumentasie (E1 - E6)
Administrasie dokumentasie (E1 - E6)

TCSEC : Sekerheidseienskappe gebruikershandleiding (C1 en hoër)
Veilige fasiliteit handleiding (C1 en hoër)
Toetsdokumentasie (C1 en hoër)
Ontwerpsdokumentasie (C1 en hoër)

Meganismes : Probleemdefinisie dokumentasie, stelseldokumentasie, programdokumentasie, bedryfsdokumentasie, gebruikersdokumentasie.

5.6.2 Dokumentasiebeheer

Definisie : Die beheer wat uitgeoefen word oor die verspreiding van en toegang tot dokumentasie.

Vereiste : Elke dokumentasiekategorie moet met die toepaslike sensitiwiteitsvlak gemerk en daarvolgens beheer word. Slegs gemagtigde personeel behoort toegang te hê tot 'n spesifieke vlak of tipe dokumentasie op 'n "need-to-know"

basis.

ITSEC : Geen klasse

TCSEC : Geen klasse

Meganismes : Sensitiwiteitsetikette, rugsteunkopieë, veilige bewaring.

6. GEVOLGTREKKING

Die koppeling van internasionale en organisasie-spesifieke standaarde met beheermaatreëls blyk dus wel uitvoerbaar te wees.

In die koppeling van internasionale standaarde met beheermaatreëls het die skrywer egter 'n groot leemte in die omvang van die standaarde geïdentifiseer. Internasionale standaarde konsentreer op veral aspekte van logiese sekerheid en (in 'n mindere mate) verspreide stelsels en administratiewe sekerheid, terwyl geen vereistes vir toepassingsekerheid en fisiese sekerheid gedefinieer word nie.

Verder is daar gevind dat baie min produkte reeds volgens TCSEC of ITSEC standaarde geëvalueer is. Hierdie verskynsel dui daarop dat leemtes wel bestaan in die algemene toepasbaarheid van die standaarde.

Dit was derhalwe vir die skrywer nodig om breë, algemene vereistes te definieer met die oog op die koppeling van standaarde met al die kategorieë van beheermaatreëls. Hierdie vereistes kan as vertrekpunt beskou word vir verdere studie ten einde 'n meer spesifieke, omvattende standaard daar te stel.

Die kategoriseringsmeganisme wat in hierdie studie voorgestel word en die koppeling van internasionale en/of organisasie-spesifieke standaarde met bepaalde maatreëls, behoort 'n organisasie in staat te stel om 'n goed-gedefinieerde stel spesifikasies vir beheermaatreëls daar te stel. Verskillende IT produkte kan dan aan die hand van hierdie spesifikasies geëvalueer word ten einde 'n produk te vind wat aan die organisasie se spesifieke behoeftes voldoen.

In die volgende hoofstuk word 'n metodologie voorgestel waarvolgens die sekerheidsfasiliteite wat 'n IT produk bied, op 'n eenvoudige wyse vergelyk kan word met die sekerheidsvereistes wat 'n organisasie vir 'n bepaalde produk stel.

HOOFSTUK 5

'N METODOLOGIE VIR DIE VERGELYKING VAN DIE SEKERHEIDSEIENSKAPPE VAN 'N IT PRODUK MET 'N ORGANISASIE SE VEREISTES

Soos in hoofstuk 1 gestel, blyk daar 'n behoefte te wees aan 'n struktuur waarvolgens IT produkte vergelyk kan word met 'n organisasie se behoeftes ten einde 'n produk te vind wat aan 'n organisasie se spesifieke vereistes voldoen. In die vorige hoofstukke van hierdie studie het die skrywer hierdie probleem stapsgewys benader deur die volgende aspekte te bespreek:

- 'n Skema waarvolgens die sekerheidsfasiliteite wat 'n IT produk bied, konseptueel voorgestel kan word (hoofstuk 2).

- 'n Kategoriseringsmeganisme waarvolgens 'n organisasie beheermaatreëls kan identifiseer en selekteer om aan sy spesifieke behoeftes te voldoen (hoofstuk 3).

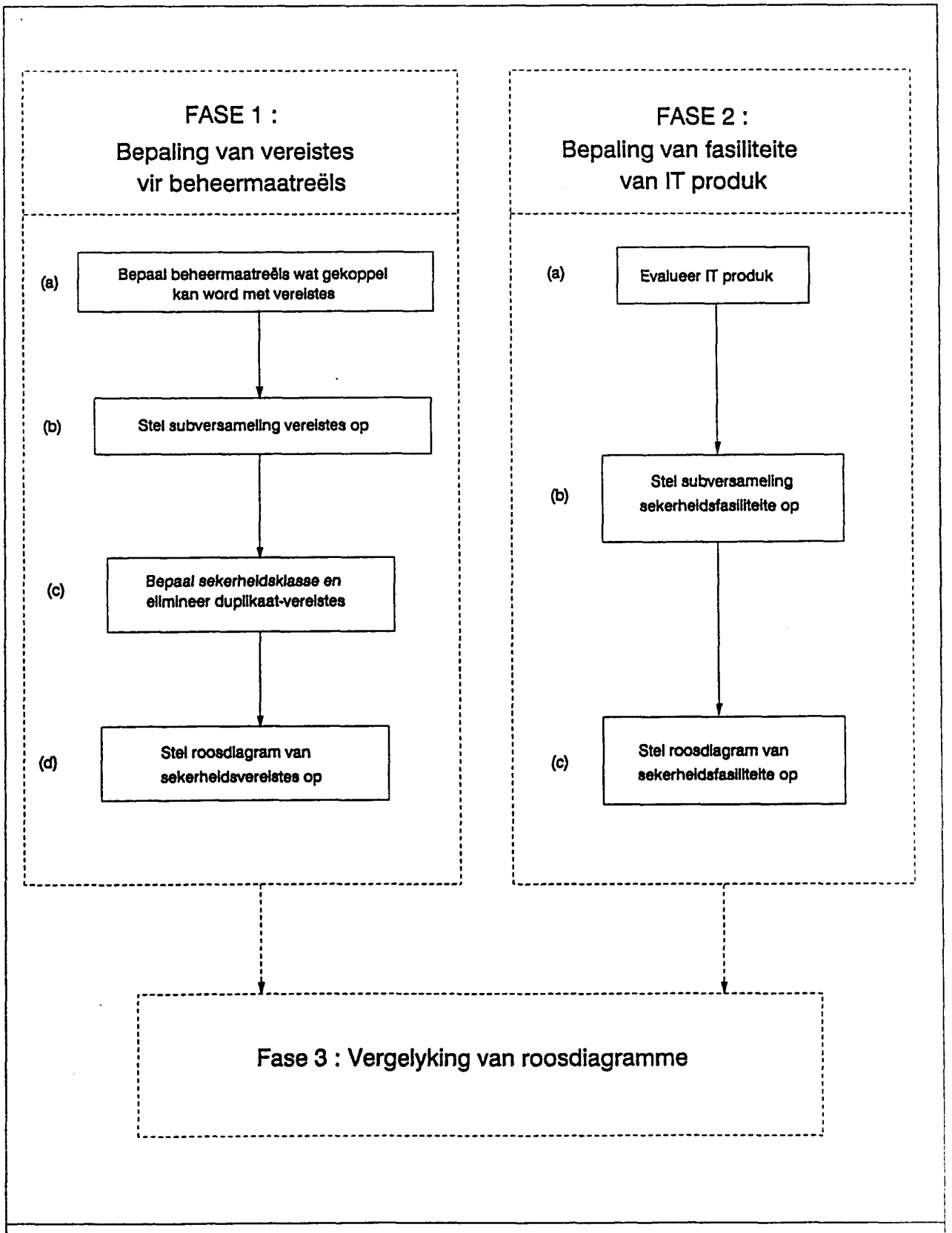
- 'n Meganisme waardeur spesifieke vereistes met hierdie beheermaatreëls gekoppel kan word deur gebruikmaking van internasionale en/of organisasie-spesifieke standaarde (hoofstuk 4).

In hierdie hoofstuk kombineer die skrywer die resultate van die vorige hoofstukke deur 'n metodologie voor te stel waardeur die sekerheidsfasiliteite wat 'n spesifieke IT produk bied, visueel vergelyk kan word met die vereistes wat 'n bepaalde organisasie vir 'n bepaalde produk stel.

1. METODOLOGIE

Die metodologie wat gebruik word, bestaan uit drie fases, naamlik die bepaling van vereistes vir beheermaatreëls, die bepaling van die sekerheidsfasiliteite van 'n IT produk en die vergelyking van die resultate van die eerste twee fases. Die eerste twee fases bestaan verder uit vier en drie take onderskeidelik. Vir die beskrywing van die metodologie is die TCSEC standaard as uitgangspunt geneem. Die metodologie kan egter maklik aangepas word om die ITSEC vereistes of organisasie-spesifieke vereistes te weerspieël.

Die verskillende take in elk van die fases soos in figuur 5.1 uiteengesit, word vervolgens bespreek.



Figuur 5.1 Metodologie vir vergelyking van organisasie-vereistes met fasiliteite van IT produk

1.1 Fase 1 : Bepaling van vereistes vir beheermaatreëls

Fase 1(a) : Bepaal beheermaatreëls wat gekoppel kan word met vereistes

Eerstens moet daar bepaal word vir welke tipe beheermaatreëls (soos in die kategoriseringsmeganisme in hoofstuk 3 bespreek) die Oranje Boek spesifieke vereistes beskryf.

Die meganisme wat in hoofstuk 4 uiteengesit is en waarvolgens al die beheermaatreëls in die kategoriseringsmeganisme gekoppel word met die toepaslike vereistes van die Oranje Boek en die Wit Boek, gee 'n aanduiding vir welke tipe beheermaatreëls daar toepaslike vereistes bestaan, en wat elkeen van hierdie vereistes is. Figuur 5.2 gee 'n uiteensetting van die beheermaatreëls en dui vir elke tipe beheermaatreël aan of die Oranje Boek (TCSEC) en die Wit Boek (ITSEC) spesifieke vereistes stel wat met die beheermaatreël gekoppel kan word.

Fase 1(b) - Stel subversameling vereistes op

Dit is duidelik dat, indien 'n mens na die totale kategoriseringsmeganisme kyk, nie die Oranje Boek of die Wit Boek vereistes vir al die tipes beheermaatreëls stel nie. Om 'n vergelyking tussen beheermaatreëls en die vereistes van die Oranje Boek dus sinvol te maak, is dit nodig om 'n subversameling van die Oranje Boek se vereistes op te stel wat slegs die vereistes bevat wat gekoppel kan word met spesifieke beheermaatreëls (sien figuur 5.3).

Fase 1(c) - Bepaal sekerheidsklasse en elimineer duplikaatvereistes

Vervolgens moet daar vir elke beheermaatreël bepaal word welke vlak van minimum werkverrigting deur die spesifieke organisasie benodig word, d.w.s. sekerheidsklas C1, C2, B1, B2, B3 of A1, soos in die TCSEC uiteengesit (sien bylae A). Vir die doeleindes van hierdie voorbeeld word die vereiste sekerheidsklasse arbitrêr gekies vir die behoeftes van 'n fiktiewe organisasie.

Om dubbelsinnigheid te voorkom, mag daar geen herhaling van enige element in die subversameling voorkom nie. In die geval waar een vereiste van toepassing is op twee of meer verskillende tipes beheermaatreëls (soos in die geval van stelselargitektuur, oudit en veilige herstel), is dit derhalwe nodig om vir elke sodanige vereiste een minimum sekerheidsklas te kies en die duplikaat-vereistes en sekerheidsklasse te elimineer. Die resultaat van hierdie stap word in figuur 5.4(a) voorgestel.

Fase 1(d) - Stel roosdiagram van sekerheidsvereistes op
Die laaste stap in hierdie fase is om die subversameling vereistes op 'n roosdiagram A af te beeld en punte wat die sekerheidsklas vir elke vereiste aandui, op die diagram aan te teken. Die tegniek wat gebruik word en die formaat van die roosdiagram is soortgelyk aan die een wat in hoofstuk 2, paragraaf 2.3 bespreek is, en word derhalwe nie weer hier bespreek nie.

Let daarop dat aangesien die subversameling van vereistes in hierdie geval slegs 18 elemente bevat, die roosdiagram eweneens slegs 18 segmente bevat. Die afbeelding van die vereistes op die diagram en die aantekening van die toepaslike punte word in figuur 5.5, 5.6 en 5.8 geïllustreer.

1.2 Fase 2 : Bepaling van fasiliteite van IT produk

Fase 2(a) - Evalueer IT produk
Die spesifieke IT produk wat ter sprake is, moet geëvalueer word aan die hand van die TCSEC. In die praktyk sal hierdie evaluering deur 'n onafhanklike liggaam gedoen word (sien hoofstuk 2, paragraaf 2) en sal 'n verslag aan die organisasie beskikbaar wees waarin die resultate van die evalueringsproses uiteengesit word.

Vir die doeleindes van hierdie bespreking word dieselfde fiktiewe produk gebruik wat in hoofstuk 2, paragraaf 2.3 gebruik is. Die vereistes en sekerheidsklasse wat op die produk van toepassing is, word volledigheidshalwe in tabel

5.1 uiteengesit.

Fase 2(b) - Stel subversameling sekerheidsfasiliteite op
'n Subversameling wat al die vereistes bevat soos in Fase 1(c) uiteengesit (d.w.s. na eliminering van duplikate), moet vervolgens opgestel word. Vir elke vereiste in die subversameling moet daar aangeteken word in welke mate voldoen die produk aan die vereiste, m.a.w. in watter sekerheidsklas val die produk vir die betrokke vereiste.

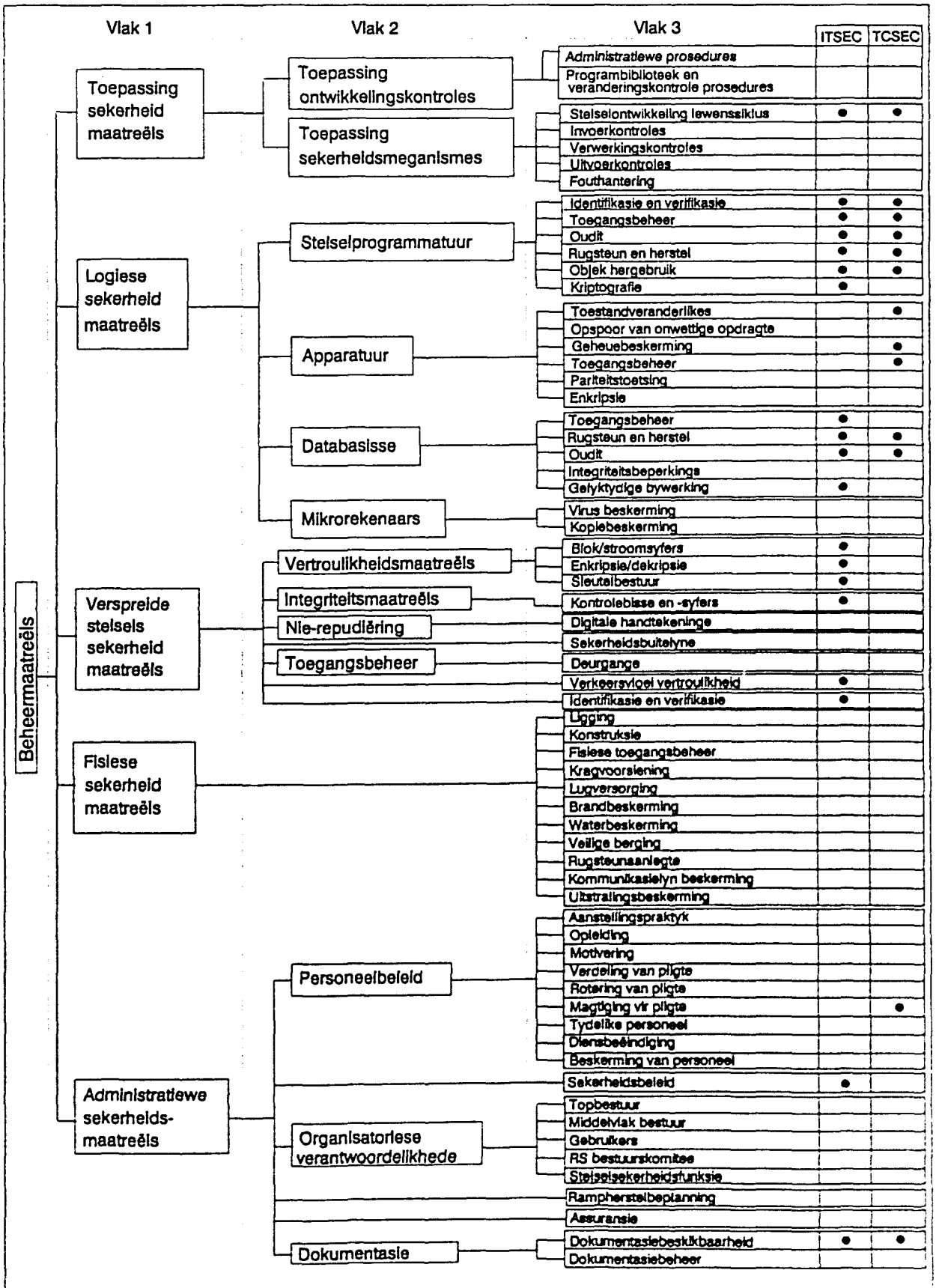
Aangesien die vereistes in hierdie geval egter verwys na 'n stel fasiliteite wat die produk bied, word die term fasiliteite vir die beskrywing van die subversameling vereistes gebruik. Die resultaat van hierdie stap word in figuur 5.4(b) voorgestel.

Fase 2(c) - Stel roosdiagram van sekerheidsfasiliteite op
Laastens moet 'n roosdiagram B opgestel word waarop die subversameling van fasiliteite afgebeeld word. Hierdie roosdiagram se raamwerk sal dus presies dieselfde lyk as roosdiagram A wat in Fase 1(d) opgestel is (sien figuur 5.5).

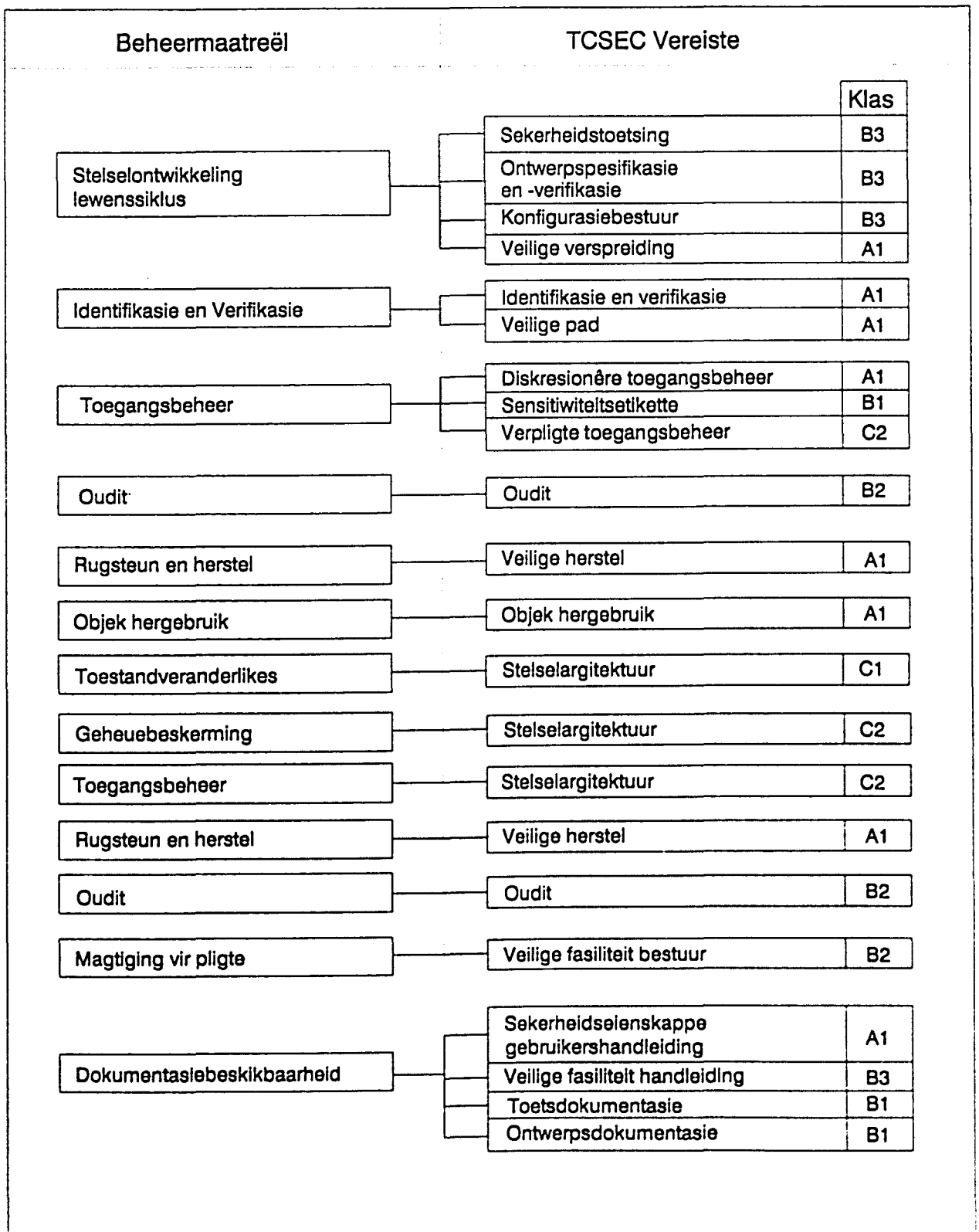
Die sekerheidsklas vir elke fasiliteit word dan op die diagram aangeteken en die punte word met mekaar verbind (sien figuur 5.7 en 5.9).

1.3 <u>Fase 3 : Vergelyking van roosdiagramme</u>

In die laaste fase word roosdiagram A en roosdiagram B wat in die vorige fases opgestel is, met mekaar vergelyk. Daar kan dus nou duidelik waargeneem word in hoe 'n mate 'n spesifieke produk voldoen aan die sekerheidsbehoeftes wat 'n bepaalde organisasie het. Die roosdiagram-tegniek stel 'n organisasie in staat om 'n produk in totaliteit te meet aan die volledige stel vereistes, en om terselfdertyd bepaalde fasiliteite van die produk te meet aan individuele vereistes wat die organisasie stel.



Figuur 5.2 Koppeling van ITSEC/TCSEC met beheermaatreëls



Figuur 5.3 Koppeling van beheermaatreëls met TCSEC vereistes

Sekerheidsvereiste	Sekerheids-klas
Diskresionêre toegangsbeheer	B2
Objek hergebruik	A1
Etikette	A1
Etiket integriteit	A1
Uitvoer van geëtiketteerde inligting	A1
Uitvoer na multivlak toestelle	A1
Uitvoer na enkelvlak toestelle	A1
Etikettering van menslik-leesbare uit-voer	A1
Subjek sensitiwiteitsetikette	B1
Toestel etikette	B1
Verpligte toegangsbeheer	C2
Identifikasie en verifikasie	A1
Veilige pad	B1
Oudit	B1
Stelselargitektuur	B2
Stelselintegriteit	A1
Koverte kanaal ontleding	B1
Veilige fasiliteit bestuur	B2
Veilige herstel	A1
Sekerheidstoetsing	B1
Ontwerp spesifikasie en verifikasie	B1
Konfigurasie bestuur	B3
Veilige verspreiding	A1
Sekerheidseienskappe gebruikershandlei-ding	A1
Veilige fasiliteit handleiding	B1
Toetsdokumentasie	B1
Ontwerpsdokumentasie	B1

TABEL 5.1 EVALUERING VAN PRODUK VOLGENS TCSEC VEREISTES

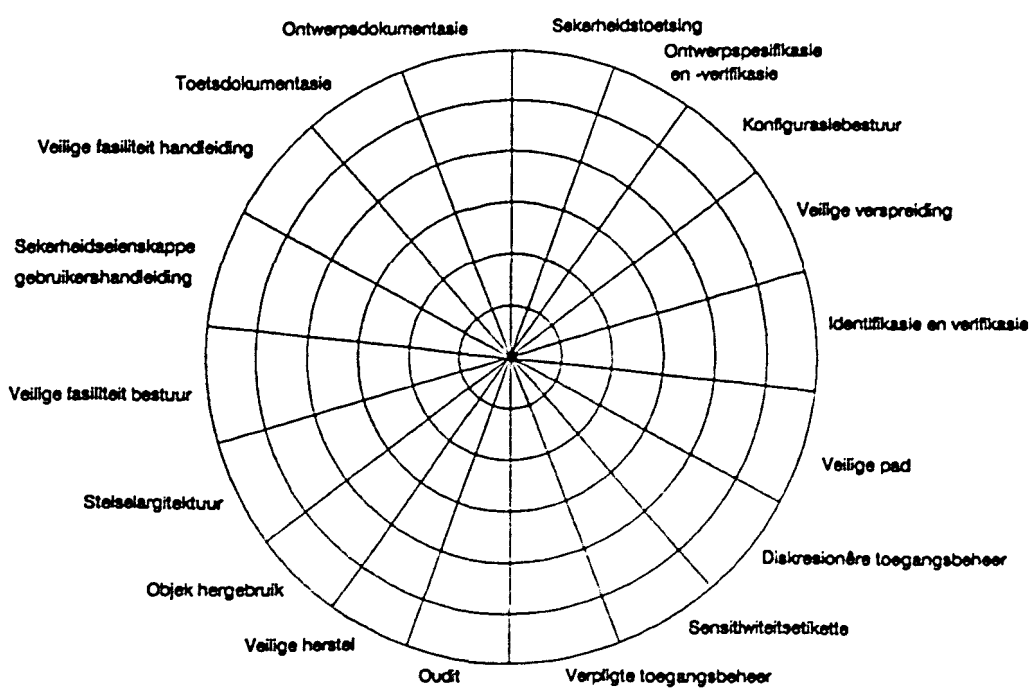
(a) Subversameling A

Vereistes vir beheermaatreëls	Klas
Sekerheidstoetsing	B3
Ontwerpspesifikasie en -verifikasie	B3
Konfigurasiebestuur	B3
Veilige verspreiding	A1
Identifikasie en verifikasie	A1
Veilige pad	A1
Diskresionêre toegangsbeheer	A1
Sensitiwiteitsetikette	B1
Verpligte toegangsbeheer	C2
Oudit	B2
Veilige herstel	A1
Objek hergebruik	A1
Stelselargitektuur	C2
Veilige fasiliteit bestuur	B2
Sekerheidselenskappe gebruikershandleiding	A1
Veilige fasiliteit handleiding	B3
Toetsdokumentasie	B1
Ontwerpsdokumentasie	B1

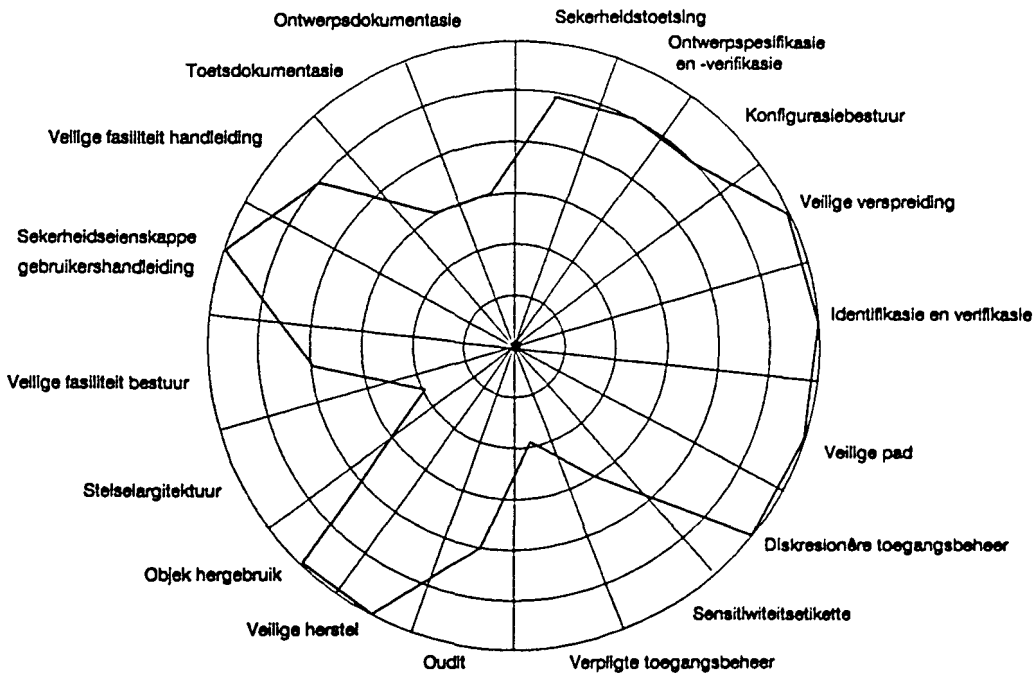
(b) Subversameling B

IT produk fasiliteite	Klas
Sekerheidstoetsing	B1
Ontwerpspesifikasie en -verifikasie	B1
Konfigurasiebestuur	B3
Veilige verspreiding	A1
Identifikasie en verifikasie	A1
Veilige pad	B1
Diskresionêre toegangsbeheer	B2
Sensitiwiteitsetikette	B1
Verpligte toegangsbeheer	C2
Oudit	B1
Veilige herstel	A1
Objek hergebruik	A1
Stelselargitektuur	B2
Veilige fasiliteit bestuur	B2
Sekerheidselenskappe gebruikershandleiding	A1
Veilige fasiliteit handleiding	B1
Toetsdokumentasie	B1
Ontwerpsdokumentasie	B1

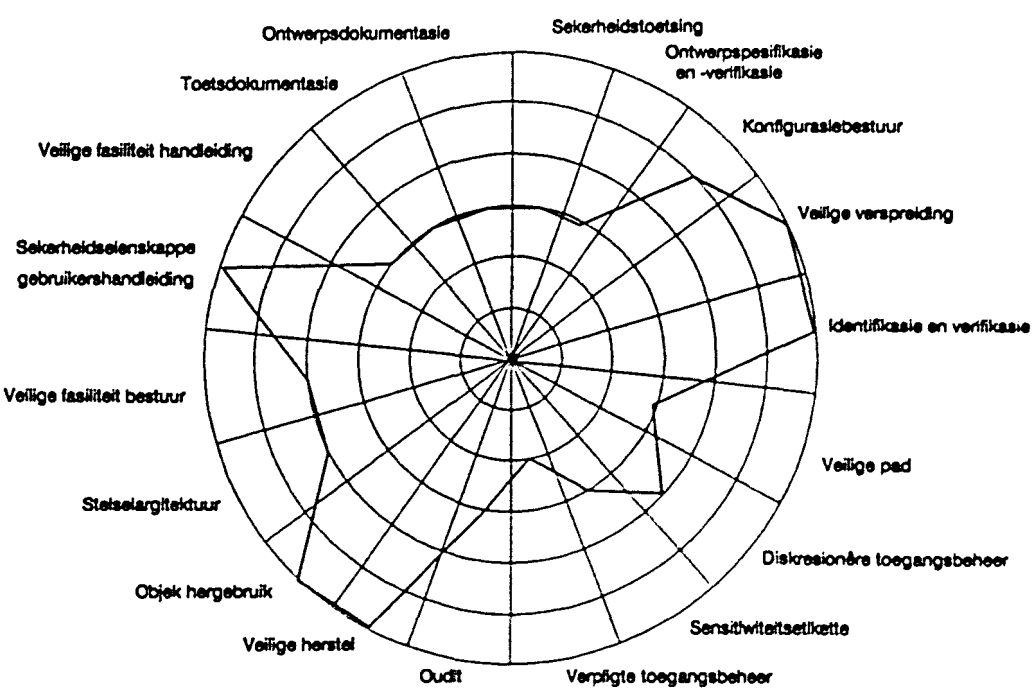
Figuur 5.4 Subversamelings



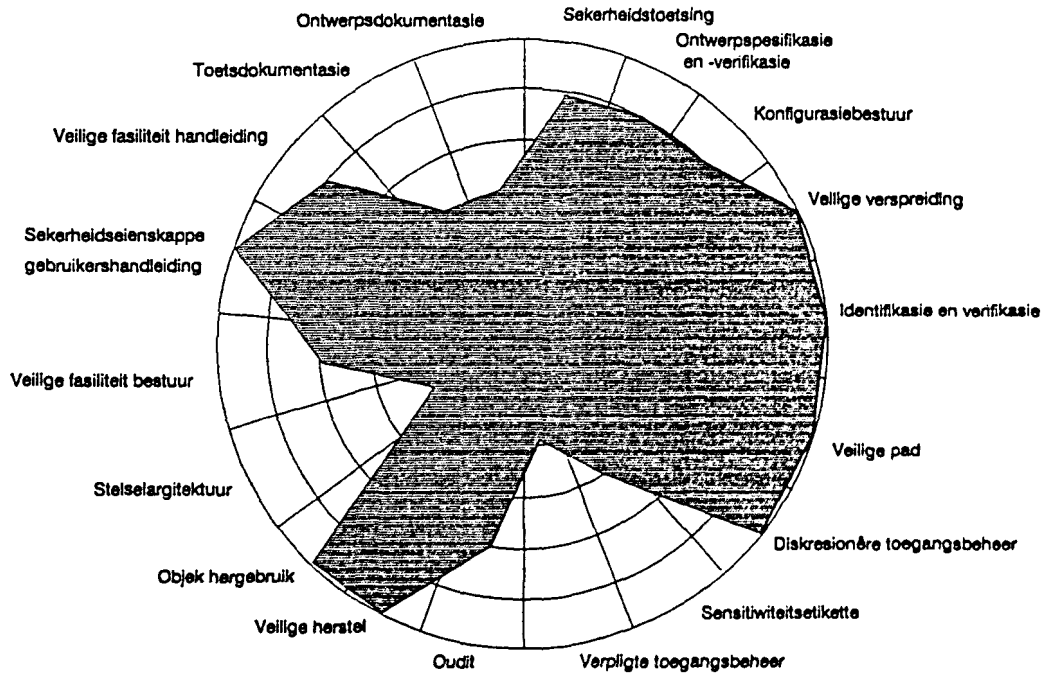
Figuur 5.5 Raamwerk van roosdiagram met vereistes/fasiliteite



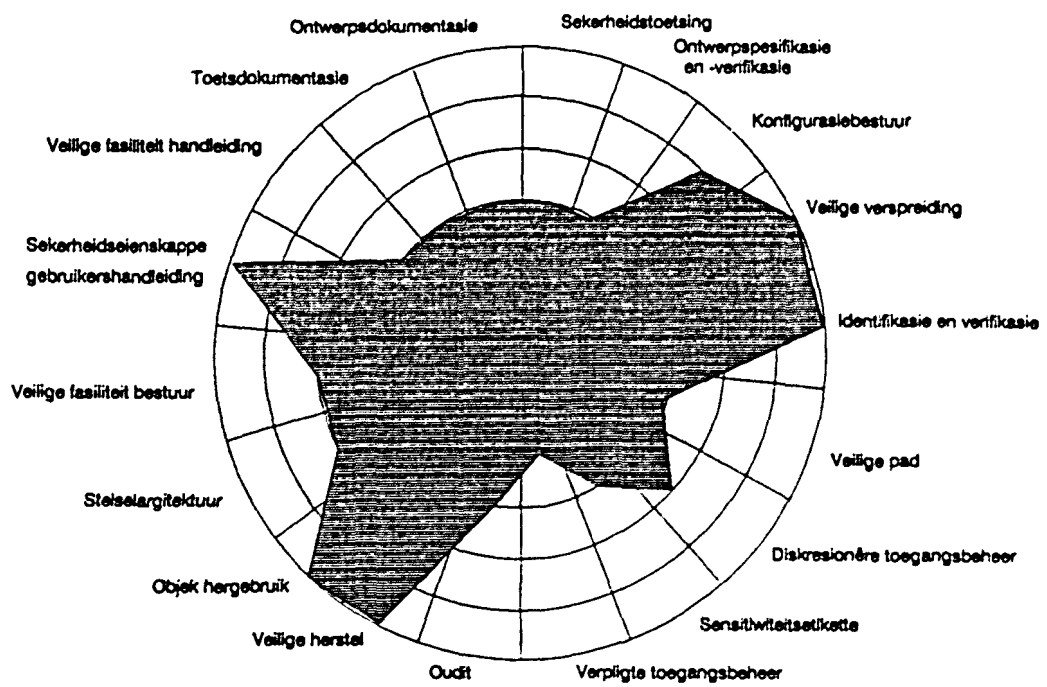
Figuur 5.6 Roosdiagram A - Vereistes vir beheermaatreëls met sekerheidsklasse (deursigtig)



Figuur 5.7 Roosdiagram B - IT produk fasiliteite met sekerheidsklasse (deursigtig)



Figuur 5.8 Roosdiagram A - Vereistes vir beheermaatreëls met sekerheidsklasse



Figuur 5.9 Roosdiagram B - IT produk fasiliteite met sekerheidsklasse

GEVOLGTREKKING

Uit die vergelyking van roosdiagramme A en B vir die spesifieke voorbeeld wat in hierdie hoofstuk gebruik is, kan die volgende gevolgtrekkings gemaak word:

- Die produk wat geëvalueer is, voldoen aan die behoeftes van die organisasie t.o.v. konfigurasiebestuur, veilige verspreiding, identifikasie en verifikasie, sensitiwiteitsetikette, verpligte toegangsbeheer, veilige herstel, objek hergebruik, veilige fasiliteit bestuur, sekerheidseienskappe gebruikershandleiding, toetsdokumentasie, en ontwerpsdokumentasie.

- Die produk bied nie voldoende fasiliteite om aan die organisasie se behoeftes t.o.v. sekerheidstoetsing, ontwerpspesifikasie en -verifikasie, veilige pad, diskresionêre toegangsbeheer, oudit, en veilige fasiliteit handleiding te voldoen nie.

- Die produk bied slegs vir een aspek meer fasiliteite as wat die organisasie vereis, naamlik stelselargitektuur.

- In geheel gesien, voldoen die produk in 'n redelike groot mate aan die organisasie se behoeftes. Die organisasie behoort egter te bepaal watter impak die tekortkominge in produk-fasiliteite (veral m.b.t. sleutelaspekte soos diskresionêre toegangsbeheer en veilige pad) op die vereiste vlak van rekenaarsekerheid sal hê.

Die metodologie wat in hierdie hoofstuk deur die skrywer voorgestel is, is daarop gerig om op bestuursvlak 'n eenvoudige, opsommende vergelyking tussen 'n organisasie se sekerheidsbehoeftes en beskikbare IT produkte moontlik te maak. Deur van hierdie metodologie gebruik te maak, kan die inligtingstelsels afdeling die nakoming van standaarde in die keuse van 'n bepaalde IT produk beklemtoon en verseker. Die verskillende alternatiewe produkte met die gepaardgaande implikasies t.o.v. effektiwiteit kan duidelik aan topbestuur voorgestel word.

Die metodologie moet daarom nie op 'n tegniese, detail-georiënteerde vlak beskou word nie. Die vernaamste tekortkoming van die metodologie is dat die uiteindelike roosdiagramme nie noodwendig alle vereistes van die organisasie met alle fasiliteite van die IT produk vergelyk nie. Die oorsake hiervan is die volgende:

- Die feit dat daar nie vir alle beheermaatreëls - soos in die kategoriseringsmeganisame gedefinieer - spesifieke vereistes in die TCSEC of ITSEC gedefinieer word nie, het tot gevolg dat die subversameling van produk-fasiliteite nie alle fasiliteite wat die produk bied, weerspieël nie.

- Die eliminering van duplikaat-vereistes (fase 1(c)) veroorsaak dat nie alle beheermaatreëls in die uiteindelike subversameling van vereistes direk verteenwoordig word nie.

'n Omvattende organisasie-spesifieke standaard waarin spesifieke vereistes vir alle beheermaatreëls gedefinieer word, behoort bogenoemde probleme te ondervang. In hierdie verband kan die vereistes wat in hoofstuk 4 vir alle tipes beheermaatreëls gedefinieer word, as vertrekpunt gebruik word.

In geheel gesien glo die skrywer egter dat die metodologie wat in hierdie hoofstuk voorgestel word, wel sinvol gebruik kan word met die oog op bestuursverslaggewing. In die volgende hoofstuk word die resultate van hierdie studie saamgevat ter afsluiting.

HOOFSTUK 6

SAMEVATTING

In hierdie studie het die skrywer gekonsentreer op hoofsaaklik twee aspekte binne die veld van rekenaarsekerheid en meer spesifiek risiko-analise, naamlik die identifisering en selektering van beheermaatreëls en die toepassing van bepaalde sekerheidstandaarde in die keuse van IT produkte.

In die evaluering van die twee belangrikste internasionale standaarde vir veilige stelsels, naamlik die Oranje Boek en die Wit Boek, het die skrywer gevind dat elkeen van hierdie standaarde bepaalde tekortkominge het (soos in hoofstuk 2 bespreek). Gesien in die lig van die feit dat relatief min produkte tot dusver volgens hierdie standaarde geëvalueer is, hang daar ook 'n vraagteken oor die algemene toepasbaarheid daarvan in die kommersiële gebied.

Juis hierdie feit beklemtoon die relevansie van dié studie. Die koppeling van beheermaatreëls wat aan 'n bepaalde organisasie se behoeftes voldoen met hierdie internasionale standaarde, behoort by te dra tot die toepasbaarheid van die standaarde in die kommersiële omgewing. Die voorstellingsmeganisme waardeur die mate waarin 'n produk aan die Oranje boek of Wit Boek se vereistes voldoen, konseptueel voorgestel kan word, kan eweneens bydra tot die aanvaarbaarheid van die standaarde in die IT mark.

As alternatief tot internasionale standaarde behoort die ontwikkeling van organisasie-spesifieke standaarde ernstige oorweging te geniet. Waar die internasionale standaarde voorsiening moet maak vir 'n ontsettend wye verskeidenheid van stelsels, kan 'n organisasie-spesifieke standaard gebou

word rondom die eienskappe en behoeftes van die bepaalde organisasie. Hierdie eienskap sal die moontlikheid van 'n suksesvolle implementering van 'n sekerheidstandaard aansienlik kan verbeter.

Die ontwikkeling van 'n tipiese organisasie-spesifieke standaard gebaseer op internasionale standaarde, is derhalwe 'n baie relevante onderwerp wat as fokuspunt vir verdere studie kan dien.

Die kategoriseringsmeganisme vir beheermaatreëls wat in hoofstuk 3 deur die skrywer voorgestel is, kan 'n definitiewe bydrae lewer om die proses van identifisering en selektering van beheermaatreëls wat vir 'n spesifieke organisasie van belang is, te vergemaklik. In die samestelling van die kategoriseringsmeganisme is 'n wye verskeidenheid van publikasies bestudeer. Alhoewel moeite gedoen is om die meganisme so volledig moontlik te maak, mag dit wees dat 'n bepaalde organisasie addisionele beheermaatreëls benodig wat nie deur die kategoriseringsmeganisme beskryf word nie. Die kategoriseringsmeganisme moet derhalwe as dinamies beskou word en kan aangepas word om 'n spesifieke organisasie se omgewing te weerspieël.

Dit was nie die skrywer se doel om in hierdie studie bepaalde produkte te ontleed aan die hand van die kategoriseringsmeganisme nie. Die klassifikasie van produkte wat op die Suid-Afrikaanse mark beskikbaar is volgens die kategoriseringsmeganisme, is 'n onderwerp waarop in verdere studie gekonsentreer behoort te word.

Dit is verder belangrik om daarop te let dat die vergelyking van 'n IT produk met 'n organisasie se vereistes slegs een deel van die besluitnemingsproses is. Die uiteindelike keuse van 'n spesifieke produk sal beïnvloed word deur 'n kombinasie van die fasiliteite wat verskaf word en die koste verbonde aan die verkryging en implementering van die produk. Slegs indien hierdie koste laer is as die finansiële verliese wat in die afwesigheid van 'n spesifieke produk verwag word,

behoort die produk oorweeg te word as 'n wenslike alternatief om risiko te vermy.

'n Onderwerp wat in hierdie verband verdere studie verdien, is koste-voordele ontleding as deel van die risiko-analise fase in rekenaarsekerheid. So 'n koste-voordele ontleding sal behels dat die risiko gekwantifiseer moet word, en dat hierdie potensiële verliese dan vergelyk moet word met die koste van beheermaatreëls wat nodig is om die risiko te neutraliseer.

Voordat die koste van beheermaatreëls bepaal kan word, moet die organisasie eers 'n stel vereistes saamstel waaraan beheermaatreëls moet voldoen, en beskikbare produkte moet dan gemeet word aan hierdie vereistes (die metodologie wat in hoofstuk 5 voorgestel is, kan toegepas word). Die koste van die produk of produkte wat aan die organisasie se behoeftes voldoen, sal dus uiteindelik opgeweeg word teen die gekwantifiseerde risiko in die afwesigheid van die produk of produkte.

Die skrywer is ten slotte van mening dat hierdie studie wel 'n bydrae lewer tot die veld van rekenaarsekerheid deur die bestuursbeginsel van koste-effektiwiteit in die identifisering en selektering van beheermaatreëls en die keuse van IT produkte toe te pas.

Die voorstellingsmeganismes vir standaarde, kategoriseringsmeganisme vir beheermaatreëls, koppeling van beheermaatreëls met standaarde en die metodologie vir die vergelyking van 'n organisasie se vereistes met IT produkte, is alles aspekte wat tot op datum nie in die literatuur behandel is nie. Teen hierdie agtergrond gesien is dit nie die skrywer se oogmerk om dit wat in hierdie studie gesê is, as onaantasbare waarhede te propageer nie, maar eerder om verdere navorsing in hierdie verband te stimuleer.

---ooOoo---

BYLAE A

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

(DIE ORANJE BOEK)

'N OPSOMMENDE VERWYSING

	C1	C2	B1	B2	B3	A1
1. SEKERHEIDSBELEID						
Diskresionêre toegangsbeheer	TCB onderskei watter groepe het toegang tot objek. Geen onderskeid tussen verskillende tipes toegang. Gebruiker hoef nie lêer te besit om dit te kan weggee. TCB beskerm nie self nuwe objekte nie.	TCB onderskei watter individuele gebruikers het toegang tot objek. Gebruiker moet reg tot lêer hê om dit weg te gee. TCB moet nuwe objekte beskerm.	Geen addisionele vereistes	Geen addisionele vereistes	Toegangsbeheerlyste spesifiseer vir elke objek 'n lys van individue met hul onderskeie modusse van toegang tot die objek. Spesifiseer ook watter gebruikers het nie toegang tot objek.	Geen addisionele vereistes
Objek hergebruik	Geen vereistes	Objek wat hertoegeken word mag geen data van vorige gebruik bevat.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Etikette	Geen vereistes	Geen vereistes	Elke subjek en stoorobjek het 'n geassosieerde sensitiwiteitsetiket.	Alle steiselhulpbronne het geassosieerde sensitiwiteitsetikette	Geen addisionele vereistes	Geen addisionele vereistes
Etiket integriteit	Geen vereistes	Geen vereistes	Sensitiwiteitsetikette is akkurate weerspieëlings van subjekte of objekte waarmee hulle geassosieer word.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Uitvoer van geëtiketteerde inligting	Geen vereistes	Geen vereistes	TCB bepaal vir elke kommunikasiekanaal of invoer/uitvoer toestel of dit enkelvlak of multivlak is.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Uitvoer na multivlak toestelle	Geen vereistes	Geen vereistes	Sensitiwiteitsetiket van objek word saam met objek uitgevoer na dieselfde fisiese medium en in dieselfde vorm as die objek.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes

	C1	C2	B1	B2	B3	A1
Uitvoer na enkelvlak toestelle	Geen vereistes	Geen vereistes	Sensitiwiteitsetiket van objek nie uitgevoer saam met objek. TCB voer slegs objekte met dieselfde of laer sensitiwiteitsetikette as die bepaalde toestel na die toestel uit.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Etikettering van menslik-leesbare uitvoer	Geen vereistes	Geen vereistes	TCB merk die begin en einde van alle menslik-leesbare uitvoer met die toepaslike menslik-leesbare sensitiwiteitsvlak, asook die begin en einde van elke bladsy met die sensitiwiteitsvlak van die bladsy.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Subjek sensitiwiteitsetikette	Geen vereistes	Geen vereistes	Geen vereistes	TCB stel 'n terminaal-gebruiker in kennis van enige verandering in die sensitiwiteitsvlak geassosieer met die gebruiker tydens 'n interaktiewe sessie.	Geen addisionele vereistes	Geen addisionele vereistes
Toestel etikette	Geen vereistes	Geen vereistes	Geen vereistes	TCB ondersteun die toekenning van minimum en maksimum sensitiwiteitsvlakke aan alle fisiese toestelle ten einde beperkings van die fisiese omgewing waar die toestelle geleë is, te oorkom.	Geen addisionele vereistes	Geen addisionele vereistes

BYLAE A TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (ORANJE BOEK) - VERVOLG

	C1	C2	B1	B2	B3	A1
Verpligte toegangsbeheer	Geen vereistes	Geen vereistes	TCB pas verpligte toegangs-beheer oor alle subjekte en stoorobjekte onder sy beheer toe. Aan alle subjekte en objekte word sensitiwiteits-etikette toegeken wat 'n kombinasie van hiërargiese klassifikasievlakke en nie-hiërargiese kategorieë is.	TCB pas verpligte toegangs-beheer toe oor alle hulpbronne, insluitende invoer/uitvoer toestelle, wat direk of indirek toeganklik is vir subjekte ekstern tot die stelsel.	Geen addisionele vereistes	Geen addisionele vereistes
2. AANSPREEKLIKHEID						
Identifikasie en verifikasie	Die TCB onderskei slegs tussen gemagtigde en ongemagtigde gebruikers. Gemagtigde gebruikers hoef nie individuele aanteken ID's te hê nie.	Elke gebruiker het 'n individuele ID wat uniek is. Hierdie ID word gebruik om toegang tot lêers te verifieer en die gebruiker se aksies te oudit.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Veilige pad	Geen vereistes	Geen vereistes	Geen vereistes	TCB ondersteun 'n veilige kommunikasieroete met die gebruiker vir aanvanklike aanteken en magtiging.	TCB ondersteun 'n veilige kommunikasieroete met die gebruiker wanneer 'n positiewe TCB-gebruiker konneksie benodig word, bv. om die gebruiker se sekerheidsvlak te verander.	Geen addisionele vereistes
Oudit	Geen vereistes	Die TCB oudit sekerheids-verwante aksies en beskerm oudit data. Die TCB kan selektief oudit per gebruiker.	TCB oudit enige veranderinge in sekerheidsvlakke, en kan selektief volgens sekerheidsvlak oudit.	TCB oudit aksies wat gebruik kan word om koverte kanale te misbruik.	TCB monitor die vermeerdering van sekerheidsaksies wat 'n moontlike oortreding van die sekerheidsbeleid mag aandui.	Geen addisionele vereistes

BYLAE A TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (ORANJE BOEK) - VERVOLG

	C1	C2	B1	B2	B3	A1
3. VERSEKERING						
3.1 Operasionele Versekering						
Stelselargitektuur	Die TCB onderhou 'n beskermde domein vir uitvoering van sekerheidsrelevante funksies wat dit beskerm teen eksterne inmenging.	Hulpbronne word beskerm sodat hulle onderworpe is aan toegangsbeheer en oudit.	Isolasie van prosesse deur afsonderlike adresruimtes.	Die TCB is intern gestruktureer in goed-gedefinieerde, grootliks onafhanklike, modules. Apparatuureienskappe soos segmentering word gebruik om logies afsonderlike stoorobjekte met verskillende attribute te ondersteun.	'n Presiese en eenvoudige beskermingsmeganisme waardeur funksies in verskillende vlakke gedefinieer en hiërargies gestruktureer word, en die vlakke met mekaar kommunikeer deur goed-gedefinieerde koppelvlakke.	Geen addisionele vereistes
Stelselintegriteit	Apparatuur en/of programmatuur fasiliteite word verskaf wat gebruik kan word om die korrekte werking van die apparatuur en firmatuur elemente van die TCB te verseker.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Koverte Kanaal Ontleding	Geen vereistes	Geen vereistes	Geen vereistes	Die stelsel bied beskerming teen koverte stoorkanale. Stelselontwikkelaars identifiseer alle koverte stoorkanale en bepaal die maksimum bandwydte vir elke geïdentifiseerde kanaal.	Die stelsel bied beskerming teen koverte stoorkanale en koverte tydskanale. Stelselontwikkelaars doen 'n koverte kanaal ontleding vir beide tipes kanale.	Formele metodes word gebruik in die ontleding.

BYLAE A TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (ORANJE BOEK) - VERVOLG

	C1	C2	B1	B2	B3	A1
Veilige Fasiliteit Bestuur	Geen vereistes	Geen vereistes	Geen vereistes	Die TCB ondersteun afsonderlike operateur en administrateur rolle en funksies.	Die stelsel moet duidelik onderskei tussen die rolle van stelseladministrateur en sekerheidsadministrateur. Enige sekerheidsadministrateur funksies deur ander persone moet deeglik geoudit word.	Geen addisionele vereistes
Veilige Herstel	Geen vereistes	Geen vereistes	Geen vereistes	Geen vereistes	Prosedures en meganismes word verskaf om te verseker dat nâ 'n stelselfaling of ineenstorting, herstel kan plaasvind sonder 'n verlies van sekerheid.	Geen addisionele vereistes
3.2 Lewenssiklus Versekering						
Sekerheidstoetsing	Die sekerheidsmeganismes van die stelsel word getoets om te bepaal of dit werk soos in die stelseldokumentasie beskryf, en dat daar geen ooglopende manier vir 'n ongemagtigde gebruiker is om hierdie meganismes te omseil nie.	Toetse word gedoen om gebreke op te spoor wat die isolering van hulpbronne kan belemmer of ongemagtigde toegang tot oudit en magtigingsdata kan verleen.	Toetse word gedoen om stelselgebreke op te spoor wat 'n ongemagtigde gebruiker sal toelaat om diskresionêre of verpligte toegangsbeheermaatreëls te omseil of wat die TCB in 'n toestand van geen respons kan plaas. Alle sodanige gebreke moet gekorrigeer of geneutraliseer word.	Alle gebreke moet gekorrigeer word, neutralisering is nie voldoende nie. Toetse moet toon dat die TCB ooreenstem met die beskrywende hoëvlak spesikasie. Die TCB moet "relatief beskermd wees teen indringing", volgens die Oranje Boek.	Geen ontwerpsgebreke en slegs 'n paar korrigeerbare implementeringsgebreke mag tydens toetsing gevind word en daar moet redelike sekerheid wees dat slegs 'n paar oorbly. Die TCB moet "beskerm wees teen indringing", volgens die Oranje Boek.	Toetse moet toon dat die TCB ooreenstem met die FTLS.

BYLAE A TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (ORANJE BOEK) - VERVOLG

	C1	C2	B1	B2	B3	A1
Ontwerp Spesifikasie en Verifikasie	Geen vereistes	Geen vereistes	Die ontwerpsdokumentasie sluit 'n formele of informele model van die sekerheids-beleid in.	Die ontwerpsdokumentasie bevat 'n formele model van die sekerheidsbeleid en 'n akkurate DTLS van die TCB.	Die ontwerpsdokumentasie toon 'n duidelike, een-tot-een afbeelding tussen die DTLS en die TCB, wat aantoon dat die DTLS ooreenstem met die formele model van die sekerheidsbeleid.	Die ontwerpsdokumentasie bevat 'n FTLS van die TCB, en toon 'n duidelike, een-tot-een afbeelding tussen die FTLS en die TCB, wat aantoon dat die FTLS ooreenstem met die formele model van die sekerheidsbeleid.
Konfigurasie Bestuur	Geen vereistes	Geen vereistes	Geen vereistes	Tydens ontwikkeling en onder-houd van die TCB kontrolleer 'n konfigurasie bestuur stelsel alle veranderings in die DTLS, ander ontwerpsdata, implementeringsdokumentasie, bronkode, die lopende weergawe van die objek kode, en toetshulpbronne en dokumentasie.	Geen addisionele vereistes	Tydens ontwerp, ontwikkeling en onderhoud van die TCB kontrolleer 'n konfigurasie bestuur stelsel alle veranderings aan items gelys vir B2 en B3 stelsels, sowel as sekerheidsrelevante apparatuur, firmatuur en programmatuur wat die formele model en FTLS wysig.
Veilige Verspreiding	Geen vereistes	Geen vereistes	Geen vereistes	Geen vereistes	Geen vereistes	Riglyne vir veilige verspreiding sluit in : Beskermende verpakking van apparatuur, programmatuur, firmatuur en dokumentasie; betroubare koeriers; geregistreerde pos; boodskap waarmerkingskodes; enkripsie van die hele stelsel; toetsing by die ontvangskant deur bv. "checksum" programme; en kommunikasie tussen die afsender en ontvanger.

BYLAE A TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (ORANJE BOEK) - VERVOLG

	C1	C2	B1	B2	B3	A1
4. DOKUMENTASIE						
Sekerheidseienskappe Gebruikershandleiding	'n Enkele opsomming, hoofstuk of handleiding beskryf die beskermingsmeganismes van die TCB, riglyne vir hul gebruik, en die wyse waarop hul ineenskakel.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes
Veilige Fasiliteit Handleiding	'n Handleiding aan die stelseladministrateur beskryf funksies en voorregte wat met versigtigheid hanteer moet word wanneer 'n veilige fasiliteit geloop word.	Die prosedures vir die ondersoek en onderhoud van die ouditlêers sowel as die gedetailleerde oudit-rekordstruktuur vir elke tipe ouditaksie word gegee.	Die handleiding beskryf die operateur- en administrateurs-funksies m.b.t. sekerheid, insluitende riglyne vir die effektiewe gebruik van die sekerheidsmeganismes van die stelsel en hoe hulle ineenskakel.	Die TCB modules wat die verwysing validasie meganisme bevat, word geidentifiseer. Die prosedures vir die veilige bedryf van 'n nuwe TCB nà wysiging van enige van die modules van die TCB, word beskryf.	Die handleiding bevat prosedures om te verseker dat die stelsel aanvanklik op 'n veilige wyse aangeskakel word, asook prosedures om die bedryf van die stelsel te hervat na 'n onderbreking.	Geen addisionele vereistes
Toetsdokumentasie	Die stelselontwikkelaar verskaf 'n toetsplan, toetsprosedures en resultate van die sekerheidsmeganismes se funksionele toetsing.	Geen addisionele vereistes	Geen addisionele vereistes	Toetsdokumentasie sluit in die resultate van toetse wat die effektiwiteit van metodes vir die verlaging van koverte kanale se bandwydtes, bepaal.	Geen addisionele vereistes	Die resultate van die afbeelding tussen die FTLS en die TCB bronkode word gegee.

BYLAE A TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (ORANJE BOEK) - VERVOLG

	C1	C2	B1	B2	B3	A1
Ontwerpsdokumentasie	Dokumentasie sluit in die vervaardiger se filosofie van beskerming en hoe hierdie filosofie in die TCB vergestalt word.	Geen addisionele vereistes	Dokumentasie bevat 'n informele of formele beskrywing van die sekerheidsbeleid model wat deur die TCB toegepas word, asook 'n beskrywing om te toon dat dit voldoende is om die sekerheidsbeleid toe te pas.	'n Formele beskrywing van die sekerheidsbeleid model en 'n bewys dat dit voldoende is om die sekerheidsbeleid toe te pas, word gegee. Dit sluit ook in 'n DTLS en 'n beskrywing van die wyse waarop die TCB die verwysingsmonitor-konsep implementeer. n Beskrywing word gegee van die wyse waarop die TCB gestruktureer is om toetsing te fasiliteer en die "minste voorreg" toe te pas. Alle ouditeerbare aksies wat gebruik kan word om koverte kanale te misbruik, word geïdentifiseer.	Informele tegnieke toon aan dat die TCB ooreenstem met die DTLS en 'n afbeelding tussen TCB en DTLS elemente word gegee.	Daar word informeel aangetoon dat die TCB implementering ooreenstem met die FTLS. Daar word met formele tegnieke getoon dat die FTLS elemente met die elemente van die TCB ooreenstem. 'n Beskrywing van apparatuur, firmatuur en programmatuur meganismes wat nie deur die FTLS beskryf word nie, maar intern tot die TCB is, word duidelik beskryf.

BYLAE B

INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA

(DIE WIT BOEK)

'N OPSOMMENDE VERWYSING

	F1	F2	F3	F4	F5
Identifikasie en Verifikasie	Stelsel identifiseer en verifieer gebruikers voor alle aksies tussen gebruiker en stelsel.	Stelsel identifiseer en verifieer gebruikers uniek voor alle aksies tussen stelsel en gebruiker. Vir elke interaksie kan stelsel identiteit van gebruiker bepaal.	Geen addisionele vereistes	Identifikasie en verifikasie hanteer deur 'n veilige pad tussen gebruiker en stelsel geinisieer deur gebruiker.	Identifikasie en verifikasie hanteer deur 'n veilige pad tussen gebruiker en stelsel geiniseer deur gebruiker of stelsel.
Toegangsbeheer	Stelsel administreer en verifieer toegangsregte tussen elke gebruiker en/of gebruikersgroep en objekte onderhewig aan administrasie van regte.	Stelsel kan gebruiker se toegang tot objek beperk tot aksies wat objek nie kan wysig. Toegangsregte kan toegeken word tot granulariteit van enkele gebruiker. Beheer oor voortplanting van toegangsregte.	Stelsel voorsien alle subjekte en stoorobjekte met attribute as basis vir verpligte toegangsregte. Verpligte toegangsbeheer word toegepas. Elke uitvoerkanaal word geidentifiseer en geadministreer as enkelvlak of multivlak. Menslik-leesbare uitvoer word toepaslik gemerk.	Toegangsregte kan gegroepeer word om verskillende rolle te ondersteun. Alle subjekte en objekte word van attribute voorsien. Vir multivlak uitvoerkanale kan die minimum en maksimum attribute vasgestel word.	Rolle van operateur, stelseladministrateur en stelselsekerheidsadministrateur word geskei. Vir elke objek onderhewig aan administrasie van regte kan lys van gebruikers en/of gebruikersgroepe voorsien word met geassosieerde toegangsregte tot objek.
Aanspreeklikheid	Geen vereistes	Stelsel teken die volgende gebeurtenisse met relevante data aan : * Gebruik van identifikasie en verifikasie meganisme * Gepoogde toegang tot objek onderhewig aan administrasie van regte * Skepping of skrapping van objek onderhewig aan administrasie van regte * Aksies deur gemagtigde gebruikers wat sekerheid van stelsel beinvloed.	Addisionele data word vir die verskillende aksies in F2 genoem, aangeteken.	Geen addisionele vereistes	Geen addisionele vereistes

BYLAE B INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (WIT BOEK) - KLASSE F1 - F5 - VERVOLG

	F1	F2	F3	F4	F5
Oudit	Geen vereistes	Hulpmiddels vir die ondersoek van die aanspreeklikheidsleers vir die doeleinde van oudit word verskaf. Aksies van een of meer gebruikers kan selektief geidentifiseer word.	Geen addisionele vereistes	Die stelsel is in staat om gebeurtenisse wat die misbruik van koverte kanale moontlik maak, te oudit.	'n Meganisme word verskaf om die voorkoms van spesifieke sekerheidsrelevante gebeurtenisse of potensiële bedreigings te monitor. Die meganisme is in staat om 'n spesifieke gebruiker of administrateur onmiddelik in kennis te stel van sodanige gebeurtenisse.
Objek Hergebruik	Geen vereistes	Alle stoorobjekte wat terugkeer na die stelsel, word behandel voor dit hergebruik word deur ander subjekte, op so 'n wyse dat geen gevolgtrekkings gemaak kan word m.b.t. die vorige inhoud nie.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes

F6	Identifikasie en Verifikasie	Toegangsbeheer	Aanspreeklikheid	Oudit
Vereistes vir stelsels met hoë integriteitsvereistes vir data en programme, bv. databasis stelsels.	Stelsel identifiseer en verifieer gebruikers voor alle aksies tussen gebruiker en stelsel. Vir elke interaksie kan stelsel identiteit van gebruiker bepaal.	Stelsel administreer en verifieer toegangsregte van gebruikers en prosesse tot spesifieke objekte. Toegang deur gebruikers tot objekte word beperk sodat dit slegs moontlik is deur spesiale prosesse. Objekte kan toegewys word aan 'n voorafgedefinieerde tipe. Vir elke tipe objek word gespesifiseer watter gebruikers of prosesse het sekere toegangsregte tot hierdie objekte. Alle kommunikasie tussen stelsel en gebruiker geskied deur veilige pad. Minimum toegangsregte wat bestaan : * Vir alle objekte : lees, skryf, byvoeg, skrap, hernoem * Vir uitvoerbare objekte : uitvoer, skrap, hernoem * Vir objekte van 'n spesifieke tipe : skep, skrap	Stelsel teken die volgende gebeurtenisse met relevante data aan : * Gebruik van identifikasie en verifikasie meganisme * Gepoogde toegang tot objek onderhewig aan administrasie van regte * Skepping of skrapping van objek onderhewig aan administrasie van regte * Aksies deur gemagtigde gebruikers wat sekerheid van stelsel beïnvloed. * Definisie of skrapping van tipes * Toekenning van tipe aan objek * Toestaan of terugtrek van toegangsregte tot objek of objektipe	Hulpmiddels om aanspreeklikheidsleërs te ondersoek vir ouditdoeleindes word verskaf en gedokumenteer. Aksies van een of meer gebruikers kan selektief geïdentifiseer word.

F7	Betroubaarheid van Diens	
Vereistes vir die beskikbaarheid van 'n volledige stelsel of spesiale funksies van 'n stelsel.	Foutopsporing en Foutherstel : Stelsel kan herstel ná faling van individuele apparatuurkomponente, op so wyse dat alle konstant benodigde funksies deurlopend beskikbaar bly in die stelsel. Na herstel en herintegrasie van betrokke komponent sal die stelsel weer oor die oorspronklike toleransie teen falings beskik.	Kontinuïteit van Diens : Ongeag die las op die stelsel moet 'n maksimum responstyd vir sekere aksies gewaarborg word. Vir sekere aksies moet gewaarborg word dat die stelsel nie onderhewig aan vergrendeling ("deadlock") is nie.

F8	Identifikasie en Verifikasie	Data-uitruiling	Aanspreeklikheid	Oudit
Vereistes m.b.t. die beskerming van data-integriteit tydens data-uitruiling.	Stelsel identifiseer en verifieer gebruikers voor alle aksies tussen gebruiker en stelsel. Vir elke interaksie kan stelsel identiteit van gebruiker bepaal. Voor die opstelling van 'n verbinding word die eweknie-entiteit geïdentifiseer en geverifieer. Met ontvangs van data is dit moontlik om die sender van die data te identifiseer en te verifieer.	Metodes vir foutopsporing en foutkorreksie word toegepas tydens data-uitruiling. Opsetlike manipulering van adresvelde en gebruikersdata kan geïdentifiseer word. Spesiale addisionele kennis wat beskerm word en slegs vir enkele gemagtigde gebruikers toeganklik is, is nodig om bg. data te manipuleer.	Stelsel teken die volgende gebeurtenisse met relevante data aan : * Gebruik van die identifikasie en verifikasie meganisme * Geïdentifiseerde foute in die data-uitruiling * Data-uitruiling	Hulpmiddels om aanspreeklikheidslêers te ondersoek vir ouditdoeleindes word verskaf en gedokumenteer. Aksies van een of meer gebruikers kan selektief geïdentifiseer word.

F9	Data-uitruiling
Vereistes vir stelsels met hoë eise vir vertroulikheid van data tydens data-uitruiling.	Stelsel het fasiliteit om gebruikers-inligting te enkripteer voor uitruiling en om dit outomaties te dekripteer aan die ontvangskant. Die sleutels vir dekripsie word beskerm teen ongemagtigde toegang.

F10	Identifikasie en Verifikasie	Data-uitruiling	Aanspreeklikheid	Oudit
Vereistes vir netwerke met hoë eise vir die vertroulikheid en integriteit van inligting wat uitgeruil word.	Stelsel identifiseer en verifieer gebruikers voor alle aksies tussen gebruiker en stelsel. Vir elke interaksie kan stelsel identiteit van gebruiker bepaal. Voor die opstelling van 'n verbinding word die eweknie-entiteit geïdentifiseer en geverifieer. Met ontvangs van data is dit moontlik om die sender van die data te identifiseer en te verifieer.	Die stelsel bied die moontlikheid van end-tot-end enkripsie. Vertroulike verkeersvloei word gewaarborg op spesifieke kommunikasielyne. Ongemagtigde manipulering van gebruikersdata en aanspreeklikheidsdata word betroubaar as foute geïdentifiseer.	Stelsel teken die volgende gebeurtenisse met relevante data aan : * Gebruik van die identifikasie en verifikasie meganisme * Geïdentifiseerde foute in die data-uitruiling * Opstelling van verbinding * Spesiale data-uitruiling transaksies	Hulpmiddels om aanspreeklikheidslêers te ondersoek vir ouditdoeleindes word verskaf en gedokumenteer. Aksies van een of meer gebruikers kan selektief geïdentifiseer word.

BYLAE B INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (WIT BOEK) - KLASSE E1 - E6

	E1	E2	E3	E4	E5	E6
1. ONTWIKKELINGSPROSES						
Vereistes	Die sekerheidsmikpunt definieer die sekerheidsvereistes van die TOE. 'n Informele of semiformele benadering word gebruik om die sekerheidsfunksies te definieer. Die sekerheidsbeleid identifiseer die sekerheidsdoelwitte en bedreigings vir die stelsel.	Geen addisionele vereistes	Geen addisionele vereistes	'n Semiformele benadering word gebruik om die sekerheidsfunksies te definieer. 'n Formele beskrywing van die sekerheidsmodel en geassosieerde bewys van konsistentheid van sleutel sekerheidsfunksies word verskaf.	Geen addisionele vereistes	Geen addisionele vereistes
Argitekturele Ontwerp	Informele beskrywing van die argitektuur van die TOE beskryf hoe die sekerheidsmikpunt bereik sal word.	Die ontbinding van die TOE in sekerheidsrelevante komponente en ander komponente word beskryf.	Geen addisionele vereistes	Gestruktureerde beskrywing van die argitektuur van die TOE beskryf hoe die sekerheidsmikpunt bereik sal word.	Geen addisionele vereistes	'n Formele beskrywing van die argitektuur van die TOE definieer alle sekerheidsrelevante komponente en die skeiding van komponente wat nie formeel beskryf word nie. Die konsistentheid van die argitekturele beskrywing met die formele sekerheidsmodel word wiskundig bewys.

BYLAE B INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (WIT BOEK) - KLASSE E1 - E6 - VERVOLG

	E1	E2	E3	E4	E5	E6
Gedetailleerde Ontwerp	Waar sekerheidsmeganismes gegradeer moet word vir minimum sterkte, word spesifikasies vir die betrokke meganismes verskaf wat geskik is vir die ontleding van die onderlinge verband tussen die meganismes.	'n Informele beskrywing van die gedetailleerde ontwerp beskryf die realisering van alle sekerheidsfunksies en identifiseer alle sekerheids-meganismes. Alle koppelvlakke tussen sekerheidsrelevante komponente en ander komponente word gedokumenteer met elk se doel en parameters.	Geen addisionele vereistes	'n Gestruktureerde beskrywing van die gedetailleerde ontwerp spesifiseer alle basiese komponente en beskryf die realisering van alle seker-heidsfunksies deur alle vlakke van die ontwerpshiërargie, en identifiseer alle sekerheids-meganismes. 'n Ontleding van die ontwerp-kwesbaarheid bepaal wyses waarop dit moontlik is vir 'n gebruiker om die sekerheidsmeganismes van die TOE te deaktiveer of te omseil. Koverte kanale word geïdentifiseer en die misbruik daarvan kan geoudit word.	Geen addisionele vereistes	Formele metodes word gebruik in die ontleding van ontwerp-kwesbaarheid.
Implementering	Toetsing dui aan dat die TOE die sekerheidsmikpunt bereik.	Toetsdokumentasie word verskaf wat die plan, doel, prosedures en resultate van die toetse bevat, en wat aandui dat die TOE die sekerheidsmikpunt bereik.	Die bronkode van alle basiese komponente word verskaf en toetse word gebaseer op inligting van alle hiërargiese ontwerpsvlakke tot by die bronkode.	Toetsdokumentasie beskryf omvang van toetsdekking, en 'n regverdiging hoekom die dekking voldoende is. Toetse word ook gebaseer op resultate van ontleding van ontwerp-kwesbaarheid.	Bronkode word gestruktureer in klein, verstaanbare funksionele eenhede en daar word aangedui hoe dit ooreen-stem met funksionele eenhede van die gedetailleerde ontwerp. 'n Ontleding van die implementering-kwesbaarheid bepaal wyses waarop dit moontlik is vir 'n gebruiker om die sekerheidsmeganismes van die TOE te deaktiveer of te omseil, gebaseer op die bronkode. Koverte kanale word geïdentifiseer.	Die ooreenstemming tussen die mnemoniese voorstelling van die objekkode en die bronkode word d.m.v. steekproewe getoets.

	E1	E2	E3	E4	E5	E6
2. ONTWIKKELINGSOMGEWING						
Konfigurasiebeheer	Geen vereistes	Die ontwikkelingsproses word ondersteun deur 'n konfigurasiebeheerstelsel. 'n Konfigurasielys word verskaf wat alle basiese komponente van die TOE opsom.	Die ontwikkelingsproses word ondersteun deur 'n konfigurasiebeheerstelsel en 'n aanvaardingsprosedure. Die programmeringstale wat in die implementering gebruik word, is streng gedefinieer.	Die konfigurasiebeheerstelsel is hulpmiddel-gebaseerd. Hierdie hulpmiddels is in staat om veranderings aan verskillende weergawes van objekte te beheer en te oudit.	Alle objekte wat gedurende die ontwikkelingsproses geskep word, is onderhewig aan konfigurasiebeheer. Die skep en hantering van veranderlike verwantskappe tussen objekte word ondersteun deur 'n integrasieprosedure.	Alle hulpmiddels wat gedurende die ontwikkelingsproses gebruik word, is onderhewig aa konfigurasiebeheer. Die rolle wat deur die konfigurasiebeheerstelsel ondersteun word, word gedefinieer met hul take en verantwoordelikhede.
Ontwikkelaarsekerheid	Geen Vereistes	'n Dokument oor die sekerheid van die ontwikkelingsomgewing beskryf die fisiese, prosedure-, personeel- en ander maatreëls om die integriteit van die TOE en die vertroulikheid van die geassosieerde dokumentasie te beskerm.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes

	E1	E2	E3	E4	E5	E6
3. BEDRYFSDOKUMENTASIE						
Gebruikersdokumentasie	Sekerheidsrelevante funksies en hul doel word beskryf, met riglyne vir veilige gebruik. Verwysingshandleidings en gebruikershandleidings is gestruktureerd, intern konsistent en konsistent met ander dokumente wat op hierdie vlak verskaf word.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Sekerheidsrelevante funksies en hul doel word verduidelik.	Geen addisionele vereistes
Administrasie Dokumentasie	Die dokumentasie onderskei tussen funksies wat die administrateur toelaat om sekerheidsparameters te beheer, en funksies wat hom slegs toelaat om inligting te verkry. Dit bevat ook definisies van sekerheidsparameters, detail oor prosedures vir sekerheidsadministrasie, inligting oor administratief sekerheidsrelevante gebeurtenisse, riglyne vir die konsistente en effektiewe gebruik van die sekerheidsfunksies en die interaksie tussen die funksies, asook instruksies vir die installering en konfigurasie van die TOE.	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes	Geen addisionele vereistes

	E1	E2	E3	E4	E5	E6
4. BEDRYFSOMGEWING						
Aflewering en Konfigurasie	Die impak van verskillende moontlike konfigurasies op sekerheid word beskryf. Die prosedure vir aflewering en stelselgenerering word beskryf.	'n Goedgekeurde stelselgenerering prosedure vir hierdie vlak van versekering word gevolg ten einde die oorspronklikheid van die afgelewerde TOE te verseker. Die genereringsproses word so geoudit dat dit moontlik is om lateraan te rekonstrueer hoe en wanneer die TOE gegenereer is.	Geen addisionele vereistes	Geen addisionele vereistes	Die impak van verskillende moontlike konfigurasies op sekerheid word verduidelik. Die prosedure vir aflewering en stelselgenerering word verduidelik.	Die effekte van verskillende konfigurasies word gedefinieer binne die formele sekerheids-beleid model.
Aanskakeling en Bedryf	Die prosedures vir veilige aanskakeling en bedryf word beskryf.	Onaktiewe sekerheidsfunksies word gedokumenteer in die handleiding vir die sekerheidsadministrateur. Indien die TOE sekerheidsrelevante apparatuurkomponente bevat, bestaan daar selftoetsings-prosedures vir die komponente. Alle veranderings aan die TOE tydens aanskakeling en bedryf word geoudit.	Geen addisionele vereistes	Prosedures bestaan wat die TOE na 'n veilige toestand kan herstel nâ 'n stelsel-faling of fout.	Die prosedures vir veilige aanskakeling en bedryf word verduidelik. Geen onderhoud is moontlik sonder die instemming van die administrateur nie.	Geen addisionele vereistes

BYLAE C

ARTIKEL

VOORGELÊ VIR PUBLIKASIE

TER NAKOMING VAN DIE VEREISTES VIR DIE GRAAD

MAGISTER IN EKONOMIESE EN BESTUURSWETENSKAPPE

CATEGORIZING COUNTERMEASURES FOR INTERNATIONAL STANDARDS

C.J. Bosch
J.H.P. Eloff

Rand Afrikaans University
P.O. Box 524
Auckland Park
2000
South Africa

ABSTRACT

Although much research has been done on countermeasures in the field of information security, and an almost equal amount of work on defining standards for countermeasures, there still seems to be an absence in literature regarding a clear linkage between countermeasures and standards, especially from a management point of view.

The identification and selection of countermeasures form part of most risk analysis approaches. Risk analysis packages compete for obtaining a maximum or at least comprehensive knowledge base of countermeasures. Identifying and selecting countermeasures from an organization specific rather than from a product point of view in this sea of alternatives present a problem. A holistic approach is required which will not only improve management's conceptual understanding of the issue, but will also enable a linkage of countermeasures with specific standards.

This paper proposes a framework for categorizing countermeasures and matching international and in-house standards with these countermeasures. Countermeasures are divided into five categories using a four-level hierarchical approach. Matching standards with countermeasures requires a study of existing international and in-house standards and mapping these standards onto the different types of countermeasures. Only after countermeasures and appropriate requirements have been identified is it possible to establish a set of specifications which can be compared with available IT products.

Keywords : Information security, Risk analysis, Countermeasures, Standards.

1. Introduction

The identification, selection and implementation of countermeasures form an integral part of an overall strategy to achieve information security in an organization. Although the subject of countermeasures has widely been researched and discussed, management still seems to be reluctant to accept the importance of having a comprehensive system of countermeasures in place to maintain information confidentiality, integrity and availability.

This phenomenon may partly be attributed to the perception that the concept of countermeasures is one only relevant to and understood by computer staff and product vendors. This perception is fuelled by the fact that the majority of published articles on the subject focus on specific countermeasures without placing these countermeasures within a larger conceptual framework understood by non-systems staff. Such a framework will not only assist in the understanding of countermeasures, but will also serve as a guide in the identification of appropriate countermeasures.

Another issue with regard to safeguarding information assets is the determination of the effectiveness of countermeasures. Management evaluates various investment projects by comparing costs against benefits, always keeping in mind adherence to predefined standards. The same principle applies to information security. The cost of countermeasures must be lower than the risk replaced by it, and the countermeasures selected must adhere to certain standards.

Various such international standards have been defined, of which the most important ones are the Trusted Computer Security Evaluation Criteria (TCSEC), also known as the Orange Book [1] [2], the Information Technology Security Evaluation Criteria (ITSEC), also known as the White Book [3], and the security addendum to the Open Systems Interconnection (OSI) network architecture [4]. Another possible standard which can be used in the evaluation of countermeasures is an in-house standard defined by an organization to meet its particular needs.

Although various IT products have been designed for and tested against international standards, there has been very little effort to match these standards with specific countermeasures. The general approach taken is one of vendors developing products matching certain standards. What is needed, is an approach where individual countermeasures are selected and developed according to an organization's specific needs and matching existing international or in-house standards.

As mentioned earlier, the selection of countermeasures should be part of a comprehensive information security strategy. Such a strategy, called the RS-methodology, has been defined by Badenhorst and Eloff [5].

The methodology consists of five phases, namely initiation, computer security policy, risk analysis and project definition, installation and maintenance. The identification and selection of countermeasures form part of phase 3 of the methodology, namely risk analysis and project maintenance.

The objectives of this paper are the following :

- To present a framework for categorizing countermeasures from a management point of view.
- To illustrate a method for matching existing international standards with these categories of countermeasures.
- The framework also enables the organisation to match existing in-house standards for IT products with categories of countermeasures.

The remainder of the paper is structured as follow :

2. A framework for categorizing countermeasures
3. Matching countermeasures with standards

2. A Framework for Categorizing Countermeasures

For the purpose of this paper the authors define countermeasures within the context of information security as:

> **"The collection of procedures and standards which are aimed at safeguarding the confidentiality, integrity and availability of an organization's information assets."** [6] [7]

The framework for categorizing countermeasures is aimed at creating a conceptual model which will enable management to see the total composition of countermeasures in more clarity. It should also enable management to create an organization specific framework by identifying and selecting those countermeasures which are applicable to the organization's particular needs. Lastly it will help management understand more clearly its own role in developing and enforcing an information security policy.

The framework uses a hierarchical approach, made up of five categories and four levels.

The five categories are the following :

- **Application security countermeasures**, which are aimed at aspects regarding the development and maintenance of application systems, with the goal of achieving reliable, ease-of-maintenance systems with the necessary internal controls that control the use of these applications.

- **Logical security countermeasures**, which include all the measures used to safeguard the data and software that are stored in the computer system.

- **Distributed systems security countermeasures**, which are aimed at safeguarding data during data exchange between different systems, sub-systems or system components.

- **Physical security countermeasures**, which are aimed at protecting the security of information systems by preventing physical damage or unauthorised access to computer systems components.

- **Administrative countermeasures**, which are aimed at the successful implementation of application, logical, distributed systems and physical security, and are applied by organizational conventions and regulations.

Each of the above categories is divided into four levels as follows :

- **Level 1** describes each category on the highest level. On this level a distinction is made only between the five basic categories, e.g. logical security countermeasures.

- **Level 2** describes each category in further detail by making use of sub-categories. These sub-categories serve only to refine the basic categories, and do not represent the actual countermeasures, e.g. systems software.

- **Level 3** defines the actual countermeasures within each category and/or sub-category, e.g. identification and authentication.

- **Level 4** describes mechanisms which can be used to implement the different countermeasures, e.g. passwords, call-back systems, challenge-response systems, smartcards and biometric systems.

The framework for categorizing countermeasures is presented in figure 1. Due to space limitations, only the three higher levels are displayed. The columns ITSEC and TCSEC at the right of the framework are explained under section 3.

In the following section the category logical security countermeasures is explained in more detail to illustrate the use of the categorising framework.

It should be noted that mechanisms identified on level 4 serve only as examples and are not the only ones applicable to each category of countermeasures.

Figure 1.

2.1 Logical security countermeasures

Logical security countermeasures is one of the five main categories defined on level one of the categorizing framework. This category includes all the logical technological measures used to protect the confidentiality, integrity and availability of the data and software that are stored in the computer system. These measures are implemented on mainly four levels, namely systems software, hardware, databases and micro computers (see figure 2), each of which is discussed below.

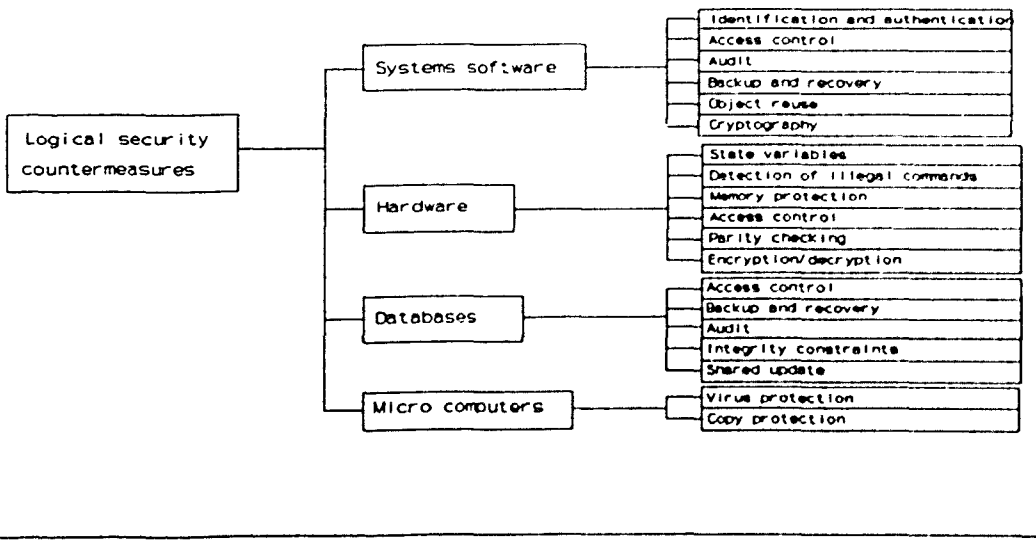


Figure 2 Logical Security Countermeasures

2.1.1 Systems software

Systems software countermeasures are defined by the authors as security services provided by the operating system and associated utilities. These countermeasures can be supplied by the vendor as part of the operating system or it can be added to the basic operating system in the form of a security package. Countermeasures in this sub-category includes :

- **Identification and authentication**, that is the process whereby two different entities, such as a user and a system or two systems, identify each other uniquely as authorised entities with whom there can be communicated on a certain level of trust. A distinction is made between user identification and authentication where the user must prove its identity to the system, and system identification and authentication where the system must prove its identity to the user. Mechanisms to implement this countermeasure include passwords, call-back systems, smartcards, biometric systems and challenge-response systems. [2] [6] [8]

- **Access control** refers to the control of access of subjects (e.g. users) to objects (e.g. files) in the system, as well as the differentiation between different types of access (e.g. read, write, execute) for different subjects to different objects. A distinction is made between discretionary access control where the user can limit access to objects under his control according to his own discretion, and mandatory access control where the system controls access of all subjects to all objects based on their respective sensitivity labels. Mechanisms include self/group/public controls, directories, access control lists, access control matrices, capabilities and sensitivity labels. [6] [9] [10]

- **Audit** is the recording, analysis and examination of security related events in the system. Where identification, authorization and access control are aimed at prohibiting unauthorised access and actions, audit is aimed at identifying unauthorised actions after the fact and taking corrective measures. Key elements in the process is an audit trail and selective reporting. [11] [12]

- **Backup and recovery** are of cardinal importance to ensure that, in the event of a system failure, disaster or other system error, the minimum data are lost, and that the system can be restored to the state that it was in as close as possible to the moment of failing. Periodic backups must be done of all software and data components. This type of countermeasure is of special importance in databases (see the sub-category databases below).

- **Object reuse** provides security by ensuring that when an object is assigned or reassigned, it does not contain data that are left over from previous use of the object. This facility includes clearing files, buffers and memory blocks and degaussing magnetic tapes after use. [1]

- **Cryptography** (also known as encryption/decryption) refers to the techniques of transforming data from normal, readable text to a secret, illegible form, as well as the reverse process of transforming the data back to a readable form. These systems fall into two basic categories, namely confidentiality systems aimed at keeping data secret, and verification systems aimed at verifying the authenticity and accuracy of data. Apart from its wide use in networks, cryptography can also be used by the operating system to protect sensitive files such as access control lists or password tables against tampering or viewing. The mechanisms used are encryption/-decryption algorithms, and public and private keys. [13] [14]

2.1.2 Hardware

Hardware countermeasures are part of logical security and refer to the basic architectural characteristics of the computer equipment used by the systems software to implement countermeasures. The ability of hardware to support system functions such as memory management reduces the amount of systems software required for a trusted system.

- **State variables** refer to an architectural design that allows the system to be operated in special trusted processing states, and that

limits the execution of sensitive operations to these states, e.g. ring-based architecture, privileged and non-privileged conditions. [15]

- **Detection of illegal commands** : Hardware can be used to intercept and/or cancel illegal transactions, e.g. fail-stop operations whereby hardware abort the execution of all processes when a hardware error or illegal command code is detected. [2] [15]

- **Memory protection** : Hardware can be designed to protect data and processes on the basis of their physical location within the system. Different users and processes are separated by physically grouping related code in memory blocks. Mechanisms used include base/bound registers, segmentation and paging. [16] [17]

- **Access control** in this context refers to a hardware memory design that forms the basis of operating system access control. Two mechanisms used are keys and locks, and tagged architecture. [2] [6]

- **Automatic parity checking** can be done by hardware as a quick way of ensuring integrity. [16]

- **Encryption/decryption** by hardware devices provide a very secure way of handling cryptographic algorithms and keys. [13]

2.1.3 Databases

The advantages that databases present in terms of sharing of resources have obvious security implications. Countermeasures in databases are enforced by the database management system (DBMS) or the operating system itself.

- **Access control** in databases differ from that in systems software because of the inference problem (users can gain information about sensitive data entities by gaining access to related data entities), and the high granularity of protection in databases (sensitivity differs up to element level). The specific mechanism used for enforcing access control depends on the database design. The most important database design styles are partitioning, integrity lock, Hinke-Schaefer design and trusted front-end. Based on one of these designs, the following mechanisms can be used to enforce access control in a multi-level database : authorization rules, encryption, views, user-defined procedures and polyinstantiation. [18] [19]

- **Backup and recovery** are similar to that discussed for systems software. All data and software are periodically backed up doing either an incremental or complete backup. Between backups information about all transactions are written to a transaction log, including so-called before and after images of the records. When a system failure occurs or the database is damaged in any way, the system can be restored by doing a forward or backward recovery. [19] [20]

- **Audit** of all the actions taken by database users should be possible. The principles are the same as those for systems software.

- **Integrity constraints** can be defined as conditions which must be satisfied by data in specific fields, or conditions which are applicable to any processing of the values in the database, e.g. range constraints, state constraints, format constraints and validity. Integrity constraints are enforced by a unit of the DBMS called an integrity monitor. [6] [19]

- **Shared update** refers to a situation where two or more users are updating specific records at the same time. Such a situation could compromise the integrity or availability of the record. Mechanisms used to handle this situation include transaction journals, simple record locking and two-phase locking. A DBMS must also provide a mechanism to handle the problem of deadlock associated with locking. [19] [20]

2.1.4 Micro computers

Apart from the countermeasures enforced by systems software, the following are important measures with regard to the stand-alone micro computer environment :

- **Virus protection** is aimed at the prevention and restriction of and the recovery from viruses. Although viruses are not limited to the micro environment, it is in this area where the majority of virus attacks have taken place. Measures taken are mainly administrative procedures, vaccination, encryption, cryptographic checksums, access control software, test-to-production control, compartmentisation and backup and recovery. [21] [22]

- **Copy protection** measures address the problem of prohibiting unauthorised duplication of software whilst ensuring the maximum availability of software. Measures include organizational regulations, software techniques such as illegal format or fail bits, hardware techniques such as unique serial numbers or a cryptographic processor, and a combination of hardware and software techniques. [6]

3. Matching Countermeasures with Standards

For the purpose of this paper a standard is defined as a set of requirements which describe a minimum proficiency level with which information security countermeasures must comply.

The approach taken by the authors in matching standards with countermeasures, is to take the framework defined in the previous section as starting point. Each type of countermeasure is then matched with an applicable requirement of a specific standard. Three possible standards can be used as source for these requirements, namely the White Book (ITSEC), the Orange Book (TCSEC) and an in-house standard.

The in-house standard describes a set of organization specific requirements that can be based on an international standard or developed independently according to the organization's particular needs.

The columns on the right of Figure 1 indicate for which countermeasures

does the White Book or Orange Book contain applicable requirements. (Note: Only the Orange Book, and not the other books in the so-called Rainbow series, was taken into consideration.)

Due to space limitations, only two examples of matching standards with countermeasures are presented here. Using these examples as a guideline, it should be possible to match other types of countermeasures with either of the three possible standards.

The first example refers to a case where applicable requirements exist in all three standards (i.e. White Book, Orange Book and in-house). The type of countermeasure selected for this example is identification and authentication in the sub-category systems software under logical security countermeasures.

The requirements presented by international standards matching this type of countermeasure are summarised in table 1 (ITSEC) and tables 2 and 3 (TCSEC). The identification and authentication requirement assures the system of the user's trustworthiness, while the trusted path requirement assures the user of the system's trustworthiness. (See [1] [2] and [3] for more information on the requirements). It should be noted that requirements are incremental according to classes, i.e. each class adds a requirement to the previous class.

Class	Requirement
F1	System identifies and authenticates users prior to all actions between the user and system.
F2	System uniquely identifies and authenticates users prior to all actions between the user and system. For every interaction the system can determine the user's identity.
F3	No additional requirements.
F4	Identification and authentication are handled via a trusted path between the user and system initialised by the user.
F5	Identification and authentication are handled by a trusted path between the user and system initialised by the user or system.

Table 1 ITSEC Requirements for Identification and Authentication

Class	Requirement
C1	Users identify themselves prior to all actions with the system and the system authenticates a user's identity.
C2	The system enforces individual accountability by uniquely identifying each individual user. This identity is associated with all audible actions taken by the individual.
B1	The system maintains authentication data that includes information for verifying the identity of individual users as well as information for detection of the clearance and authorizations of individual users.
B2	No additional requirements.
B3	No additional requirements.
A1	No additional requirements.

Table 2 TCSEC Requirements for Identification and Authentication

Class	Requirement
C1	No requirements.
C2	No requirements.
B1	No requirements.
B2	The system supports a trusted communication path between itself and users for initial login and authentication.
B3	The system supports a trusted communication path between itself and users for use when a positive system-to-user connection is required (e.g. login, change subject sensitivity level.)
A1	No additional requirements.

Table 3 TCSEC Requirements for Trusted Path

Figure 3 illustrates the matching of the White Book, Orange Book and in-house standard with the countermeasure Identification and Authentication.

The second example concerns a case where neither of the two international standards contains applicable requirements for the particular type of countermeasure. In this case an in-house standard is used to describe the requirement. The type of countermeasure used in the example is appointment practice in the sub-category staff policy under administrative countermeasures.

Figure 4 illustrates the matching of appointment practice with an in-house standard. (See [23] and [24] for more information on staff policy issues.)

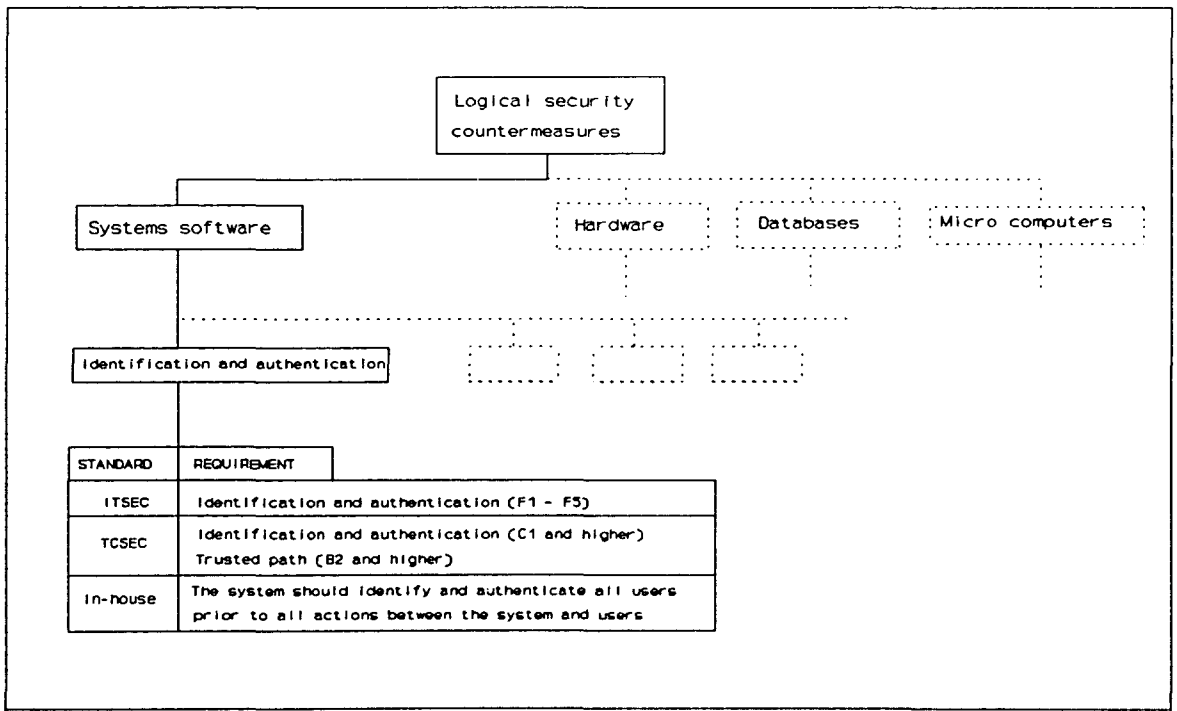


Figure 3 Matching Countermeasures with International and In-house Standards

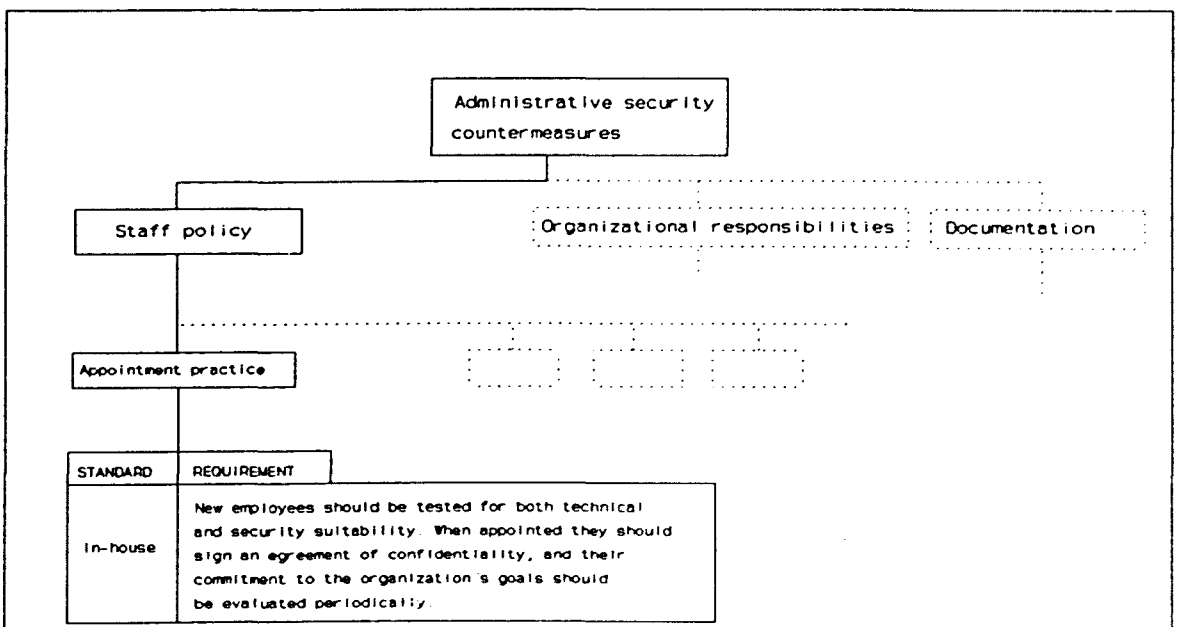


Figure 4 Matching Countermeasures with In-house Standards

4. Conclusion

Categorizing information security countermeasures provides a conceptual framework that can be used by both managers and systems staff not only to understand the broader picture, but also to identify and select countermeasures in accordance with organization specific needs and in coherence with IT developments. The framework presented in this paper should in no way be seen as a fixed solution, but rather as a model to which enhancements can be made for each different scenario.

For each type of countermeasure, international standards like the White Book and Orange Book should be examined to determine any requirements applicable to the countermeasure. Such requirements should be evaluated and adapted to meet the organization's needs. In the case where no requirements for a specific type of countermeasure exists, it is necessary to define an in-house requirement to ensure adherence to information security standards.

After examining different alternatives for countermeasures and determining appropriate requirements for each type of countermeasure, the organization will have a well defined set of specifications for measures needed to counter the threat against information security. Different IT products can then be evaluated against these specifications to find a product which will suit the organization's specific needs. The eventual choice of a particular product will be influenced by a combination of facilities provided and the cost of acquiring and implementing the product. Only if this cost is lower than the financial losses envisaged in its absence, should a particular product be considered a viable option.

References

[1] Russel D. and Gangemi G.T. Sr., Computer Security Basics, O'Reilly and Associates, Inc., July 1991

[2] National Research Council, Computers at Risk, National Academy Press, April 1991

[3] Information Technology Security Evaluation Criteria (ITSEC), Version 1, 2 May 1990

[4] Branstad D.K., "Considerations for Security in the OSI Architecture", IEEE Network Magazine Vol. 1 No. 2, April 1987, pp. 34 - 39

[5] Badenhorst K.P. and Eloff J.H.P., "Framework of a Methodology for the Life Cycle of Computer Security in an Organization", Computers & Security 8, 1989, pp. 433 - 442

[6] Pfleeger C.P., Security in Computing, Prentice-Hall, 1989

[7] Krauss L.I. and MacGahan A., Computer Fraud and Countermeasures, Prentice-Hall Inc., 1979

[8] Harper R.M., "Internal Controls in Local Area Networks : an Accountant's Perspective", Computers & Security 5, 1986, pp. 28 - 35

[9] Lunt T.F., "Access Control Policies : Some Unanswered Questions", Computers & Security 8, 1989, pp. 43 - 54

[10] Karger P.A., "Authentication and Discretionary Access Control in Computer Networks", Computers Networks and ISDN Systems 10, 1985, pp. 27 - 37

[11] Mercer L.C.J., "Tailor-made Auditing of Information Systems for the Detection of Fraud", Computers & Security 9, 1990, pp. 59 - 66

[12] Menkus B., "Maintaining Information Integrity", Computers & Security 9, 1990, pp. 111 - 115

[13] Davies D.W. and Price W.L., Security for Computer Networks, John Wiley & Sons, 1984

[14] Pritchard J.A.T., Security in On-Line Systems, The National Computing Centre, 1979

[15] Buck E.R., Introduction to Data Security and Controls, Q.E.D. Information Sciences Inc., 1982

[16] Keller L.S., Operating Systems : Communicating with and Controlling the Computer, Prentice Hall, 1988

[17] Ducklin P., "Chip Generations : Adressing Memory on the IBM-PC", BIT Magazine, April 1990, pp. 14 - 17

[18] **McHugh J. and Thuraisingham B.M.**, "Multilevel Security Issues in Distributed Database Management Systems", Computers & Security 7, 1988, pp. 387 - 396

[19] **Pratt P.J. and Adamski J.J.**, Database Systems : Management and Design, Boyd & Fraser, 1987

[20] **Date C.J.**, An Introduction to Database Systems, Volume 1, Fifth Edition, Addison-Wesley, 1990

[21] **Fåk V.**, "Are We Vulnerable to a Virus Attack?", Computers & Security 7, 1988, pp. 151 - 155

[22] **Zajac B.P.**, "Computer Viruses : Can they be Prevented?", Computers & Security 9, 1990, pp. 25 - 31

[23] **Zajac B.P.**, "Personnel : The Other Half of Data Security", Computers & Security 7, 1988, pp. 131 - 132

[24] **Menkus B.**, "The Employee's Role in Protecting Information Assets", Computers & Security 8, 1989, pp. 487 - 492

BIBLIOGRAFIE

IN ALFABETIESE VOLGORDE

[1] **Ahituv N.**
Lapid Y.
Neumann S.
"Protecting Statistical Databases Against Retrieval of Private Information",
Computers & Security 7, 1988, pp. 59 - 63

[2] **Al-Dossary G.M.**
"Computer Virus Prevention and Containment on Mainframes",
Computers & Security 9, 1990, pp. 131 - 137

[3] **Amsel E.**
"Network Security and Access Controls",
Computers & Security 7, 1988, pp. 53 - 57

[4] **Andrews W.C.**
"Executing a Disaster Plan",
Contingency Journal, July - Sept 1990, pp. 28 - 31

[5] **Arnold A.**
Persy C.
Sedlak G.
"Towards Mutual Recognition of Security Evaluations",
Proceedings : 14th National Computer Security Conference, NIST/NCSC, Oct. 1 - 4, 1991, pp. 669 - 672

[6] **Badenhorst K.P.**
"'n Metodologie vir die Implementering van Rekenaarsekerheid in 'n Groot Organisasie",
M.Sc verhandeling, RAU, Mei 1989

[7] **Badenhorst K.P.**
Eloff J.H.P.
"Computer Security Methodology : Risk Analysis and Project Definition",
Computers & Security 9, 1990, pp. 339 - 346

[8] **Badenhorst K.P.**
Eloff J.H.P.
"Framework of a Methodology for the Life Cycle of Computer Security in an Organization",
Computers & Security 8, 1989, pp. 433 - 442

[9] **Banks S.**
"Security Policy",
Computers & Security 9, 1990, pp. 605 - 610

[10] **Bauknecht K.**
Strauss C.
"Portfolio Techniques to Support Risk Management and Security"

[11] **Blatchford C.**
"European Initiative in Computer Security Standards", Proceedings : COMPSEC International 1991, Elsevier Advanced Technology, 1991, pp. 319 - 331

[12] **Boehm B.W.**
Software Risk Management, IEEE Computer Society Press, 1989, pp. 246 - 282

[13] **Bosch C.J.**
"'n Oorsigtelike Beskouing van Rampherstelbeplanning as deel van die Rekenaarsekerheid in 'n Organisasie", B.Com. Honneurs Skripsie, RAU, Januarie 1991

[14] **Boyer T.J.**
"Contingency Planning : An Opportunity for DP Management", Computer Security Journal, Winter 1982, pp. 7A1 - 7A9

[15] **Branstad M.A.**
Brewer D.
Jahl C.
Kurth H.
Pfleeger C.P.
"Apparent Differences between the U.S. TCSEC and the European ITSEC", Proceedings : 14th National Computer Security Conference, NIST/NCSC, Oct. 1 - 4, 1991, pp. 45 - 58

[16] **Branstad D.K.**
"Considerations for Security in the OSI Architecture", IEEE Network Magazine Vol. 1 No. 2, April 1987, pp. 34 - 39

[17] **Buck E.R.**
Introduction to Data Security and Controls, Q.E.D. Information Sciences Inc., 1982

[18] **Buczkowski L.J.**
"Database Inference Controller", Database Security, III : Status and Prospects, Elsevier Science Publishers, 1990, pp. 311 - 322

[19] **Candia T.** "How VMS Keeps Out Intruders", Computers & Security 9, 1990, pp. 499 - 502

[20] **CCTA** "A Guide to CRAMM for Management", Information Technology Security, 1988

[21] **CCTA** "CRAMM - For Secure IT Systems", Information Technology Security, 1988

[22] **Cerullo M.J.** "General Controls in Computer Systems", Computers & Security 4, 1985, pp. 33 - 45

[23] **Christoffersson P.** "Message Authentication and Encryption Combined", Computers & Security 7, 1988, pp. 65 - 71

[24] **Cohen F.** "On the Implications of Computer Viruses and Methods of Defense", Computers & Security 7, 1988, pp. 167 - 184

[25] **Courtney R.H. Jr.** "A Systematic Approach to Data Security", Computers & Security 1, 1982, pp. 99 - 112

[26] **Date C.J.** An Introduction to Database Systems, Volume 1, Fifth Edition, Addison-Wesley, 1990

[27] **Davies D.W.** **Price W.L.** Security for Computer Networks, John Wiley & Sons, 1984

[28] **Ducklin P.** "Chip Generations : Adressing Memory on the IBM-PC", BIT Magazine, April 1990, pp. 14 - 17

[29] **Eloff J.H.P.** "Computer Security Policy : Important Issues", Computers & Security 7, 1988, pp. 559 - 562

[30] **Enger N.L.**
Howerton P.W.
Computer Security : A Management Audit Approach, AMACOM, 1980

[31] **EUROBIT**
Towards Mutual Recognition of Security Evaluations, A study elaborated by VDMA/ZVEI Working Group on IT security, EUROBIT, October 1991

[32] **Fåk V.**
"Are We Vulnerable to a Virus Attack?", Computers & Security 7, 1988, pp. 151 - 155

[33] **Fifield K.J.**
"Smartcards Outsmart Computer Crime", Computers & Security 8, 1989, pp. 247 - 255

[34] **Fish T.B.**
Bressman L.H.
"Basics of Contingency Planning", Computer Security Handbook, pp. 7B1 - 7B21

[35] **Fitzgerald J.**
Designing Controls into Computerized Systems, 1981, pp. 48 - 51

[36] **Fordyce S.**
"Computer Security : A Current Assessment", Computers & Security 1, 1982, pp 9 - 16

[37] **Gardner P.E.**
"Evaluation of Five Risk Assessment Programs", Computers & Security 8, 1989, pp. 479 - 485

[38] **Graubart R.**
"A Comparison of Three Secure DBMS Architectures", Database Security, III : Status and Prospects, Elsevier Science Publishers, 1990, pp. 167 - 190

[39] **Guarro S.B.**
"Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management", Computers & Security 6, 1987, pp. 493 - 504

[40] **Halsall F.**
Data Communications, Computer Networks and OSI, Addison-Wesley, 1988

[41] **Hamilton P.** Computer Security,
Cassel/Associated Business Programmes Ltd, 1972

[42] **Harper R.M.** "Internal Controls in Local Area Networks : an Accountant's Perspective",
Computers & Security 5, 1986, pp. 28 - 35

[43] **Hiatt C.**
Motz A. "Disaster Recovery Planning : What it Should be, What it Is, How to Improve it",
Edpacs Vol. XVII no. 9, March 1990, pp. 1 - 9

[44] **Highland H.J.** "An Overview of 18 Virus Protection Products",
Computers & Security 7, 1988, pp. 157 - 161

[45] **Highland H.J.** "Product Reviews",
Computers & Security 7, 1988, pp. 13 - 18

[46] **Highland H.J.** "Virus Defense Alert",
Computers & Security 7, 1988, pp. 156 - 158

[47] **Hoffman L.J.** "Smoking Out the Bad Actors : Risk Analysis in the Age of the Microcomputer",
Computers & Security 8, 1989, pp. 299 - 302

[48] **Homer S.** "Setting Standards in Europe",
Computers & Security 9, 1990, pp. 295 - 300

[49] **Hosmer H.H.** "Handling Security Violations within an Integrity Lock DBMS",
Database Security, III : Status and Prospects, Elsevier Science Publishers, 1990, pp. 283 - 292

[50] **Hruska J.**
Jackson K. Computer Security Solutions,
Blackwell Scientific Publications, 1990

[51] **ITSEC**
Information Technology Security Evaluation Criteria (ITSEC) Version 1, 2 May 1990

[52] **Ivancevich J.M.**
Donelly J.H.
Gibson J.L.
Management Principles and Functions,
Irwin, 1989

[53] **Jajodia S.**
Gadia S.
Bhargava G.
Sibley E.H.
"Audit Trail Organization in Relational Databases",
Database Security, III : Status and Prospects, Elsevier Science Publishers, 1990, pp. 269 - 281

[54] **Karger P.A.**
"Authentication and Discretionary Access Control in Computer Networks",
Computers Networks and ISDN Systems 10, 1985, pp. 27 - 37

[55] **Keller L.S.**
Operating Systems : Communicating with and Controlling the Computer,
Prentice Hall, 1988

[56] **Krauss L.I.**
MacGahan A.
Computer Fraud and Countermeasures,
Prentice-Hall Inc., 1979

[57] **Kuong J.F.**
"A Framework for Auditing EDP Contingency and Recovery Plans",
Edpacs, January 1987, pp. 2 - 13

[58] **Lunt T.F.**
"Access Control Policies : Some Unanswered Questions",
Computers & Security 8, 1989, pp. 43 - 54

[59] **Lunt T.F.**
Denning D.E.
Shell R.R.
Heckman M.
Shockley W.R.
"Element-Level Classification with A1 Assurance",
Computers & Security 7, 1988, pp. 73 - 82

[60] **McHugh J.**
Thuraisingham B.M.
"Multilevel Security Issues in Distributed Database Management Systems",
Computers & Security 7, 1988, pp. 387 - 396

[61] **Menkus B.**
"Computer-Related Fire Problems Revisited",
Computers & Security 8, 1989, pp. 581 - 585

[62] **Menkus B.**
"It's Time to Rethink Data Processing Fire Protection",
Computers & Security 8, 1989, pp. 389 - 394

[63] **Menkus B.**
"Maintaining Information Integrity",
Computers & Security 9, 1990, pp. 111 - 115

[64] **Menkus B.**
"Physical Security : Selecting an Access Control System",
Computers & Security 8, 1989, pp. 201 - 205

[65] **Menkus B.**
"The Employee's Role in Protecting Information Assets",
Computers & Security 8, 1989, pp. 487 - 492

[66] **Mercer L.C.J.**
"Tailor-made Auditing of Information Systems for the Detection of Fraud",
Computers & Security 9, 1990, pp. 59 - 66

[67] **Michels J-P.**
"Contingency Planning for Data Processing",
Data Time Consultants Ltd., pp. 1 - 15

[68] **Michels J-P.**
Disaster Recovery Manual, Data Time Consultants

[69] **Montgomery G.** "Disaster Recovery Planning - A Way of Life", Corporate Computing Today, August 1989, pp. 8 - 9

[70] **National Research Council** Computers at Risk, National Academy Press, April 1991

[71] **Nel A.J.** **Eloff J.H.P.** "A Methodology for Network Security"

[72] **Pardo O.R.** **McDuffie C.** "A Fast Track Approach to Computer Contingency Planning", Edpacs Vol. XVI No. 5, November 1988, pp. 1 - 6

[73] **Pfitzmann B.** "Fail-stop Signatures; Principles and Applications", Proceedings : COMPSEC International 1991, Elsevier Advanced Technology, 1991, pp. 125 - 134

[74] **Pfleeger C.P.** Security in Computing, Prentice-Hall, 1989

[75] **Pratt P.J.** **Adamski J.J.** Database Systems : Management and Design, Boyd & Fraser, 1987

[76] **Pritchard J.A.T.** Security in On-Line Systems, The National Computing Centre, 1979

[77] **Ramaswamy R.** "Placement of Data Integrity Security Services in Open Systems Interconnection Architecture", Computers & Security 8, 1989, pp. 507 - 516

[78] **Russel D.** **Gangemi G.T. Sr.** Computer Security Basics, O'Reilly and Associates, Inc., July 1991

[79] **Rutledge L.S.** **Hoffman L.J.** "A Survey of Issues in Computer Network Security", Computers & Security 5, 1986, pp. 296 - 308

[80] **Schreider T.** "Leak-Sensing Devices", Mainframe Journal, September/October 1988, p.114

[81] **Shepherd S.J.** **Sanders P.W.** **Patel A.** "A Comprehensive Security System - the Concepts, Agents and Protocols", Computers & Security 9, 1990, pp. 631 - 643

[82] **Silltow J.** "A Computer Virus Contingency Plan", Proceedings : COMPSEC International 1991, Elsevier Advanced Technology, 1991, pp. 73 - 83

[83] **Silverman M.E.** "Contingency Planning : The Backup Site Decision", Computer Security Journal, Spring 1983, pp. 7A3 - 7A10

[84] **Stamps D.** "Disaster Recovery : Who's Worried?", Datamation, February 1 1987, pp. 60 - 64

[85] **Thurling G.** "Firms Unwilling to Hold Disaster Recovery Runs", Computing S.A., 29 January 1990

[86] **Tompkins F.** **Rice R.** "Integrating Security Activities into the Software Development Life Cycle and the Software Quality Assurance Process", Computers & Security 5, 1986, pp. 218 - 242

[87] **Van Tassel D.** Computer Security Management, Prentice-Hall, 1972

[88] **Von Solms S.H.** "Computer Security : Prevention Measures", Lesing tydens konferensie : "Computers : Crime, Security & the Law", aangebied deur Whitehead Morris - International Management Consultants

[89] **Von Solms S.H.** "Computer Security : Prevention Measures"

[90] **Walker D.D.** General Electric - An Approach to Disaster Recovery, IFIP Proceedings, Elsevier Science Publishers, 1984

[91] **Weber R.** "Controls in Electronic Funds Transfer Systems : A Survey and Synthesis", Computers & Security 8, 1989, pp. 123 - 137

[92] **Winters P.** "Secure Systems Design - An Evolving National Strategy", Computers & Security 9, 1990, pp. 379 - 389

[93] **Wiseman S.R.** "Control of Confidentiality in Databases", Computers & Security 9, 1990, pp. 529 - 537

[94] **Wiseman S.R.** "On the Problem of Security in Databases", Database Security, III : Status and Prospects, Elsevier Science Publishers, 1990, pp. 301 - 310

[95] **Wolfe C.** **Wiggins C.E.** "Internal Control in the Microcomputer Environment", The Internal Auditor, December 1986, pp. 54 - 60

[96] **Wong K.** "Computer Crime - Risk Management and Computer Security", Computers & Security 4, 1985, pp. 287 - 295

[97] **Wood C.C.** "A Context for Information Systems Security Planning", Computers & Security 7, 1988, pp. 455 - 465

[98] **Wood C.C.** "Information Systems Security : Management Success Factors", Computers & Security 6, 1987, pp. 314 - 320

[99] **Wood C.C.** "Principles of Secure Information Systems Design", Computers & Security 9, 1990, pp. 13 - 24

[100] **Wood M.B.** Guidelines for Physical Computer Security, NCC Publications, 1986

[101] **Wood M.B.** Introducing Computer Security, NCC Publications, 1982

[102] **Wooldridge S.** **Corder C.** **Johnson C.** Security Standards for Data Processing, Macmillan Press, 1973

[103] **Zajac B.P.** "Computer Viruses : Can they be Prevented?", Computers & Security 9, 1990, pp. 25 - 31

[104] **Zajac B.P.** "Personnel : The Other Half of Data Security", Computers & Security 7, 1988, pp. 131 - 132

[105] "UPS - The Best Computer Insurance Policy?", Corporate Computing Today, April 1990, pp. 9 - 10