Informatiebeveiliging op een hoger niveau

Onderzoek naar een methode voor het systematisch opstellen van informatiebeveiligingsbeleid

E.J. Stofbergen

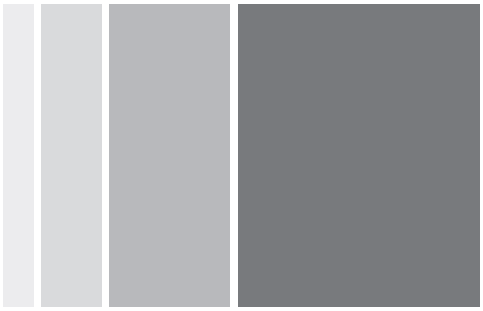
Informatiebeveiliging op een hoger niveau

Onderzoek naar een methode voor het systematisch opstellen van informatiebeveiligingsbeleid

Doctoraalscriptie

Auteur:	E.J. Stofbergen
Datum:	15 november 2004
Studie:	Econometrie
Afstudeervariant:	Bestuurlijke Informatica
Instelling:	Erasmus Universiteit Rotterdam Faculteit der Economische Wetenschappen Capaciteitsgroep Informatica
Begeleiding:	dr. ir. J. van den Berg (Erasmus Universiteit Rotterdam)

Voorwoord



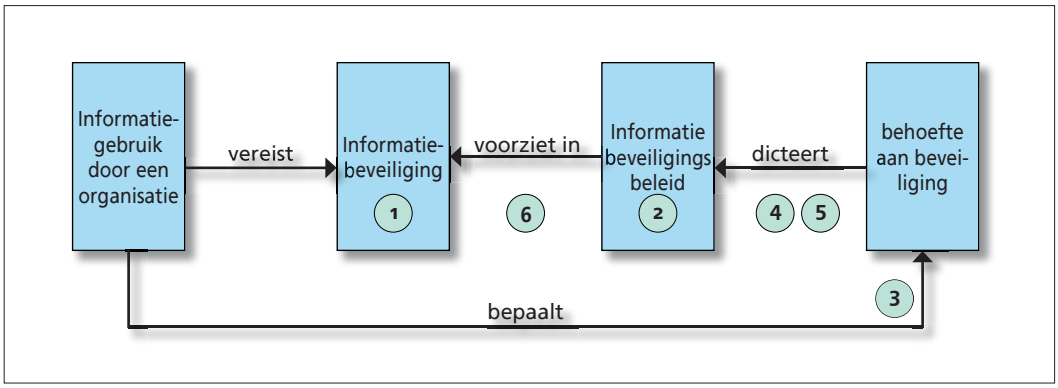
Na het schrijven van een doctoraalscriptie van deze omvang in een lange en soms roerige periode ontkom ik niet aan het schrijven van een voorwoord. De ontstaansgeschiedenis van deze scriptie zou zelfs een zeer uitgebreid voorwoord kunnen rechtvaardigen. Ik hou het echter kort. Diegenen die erbij betrokken zijn geweest kennen de feiten en kunnen deze op waarde schatten en voor anderen zijn die feiten eigenlijk niet relevant.

Mijn overheersende gevoel is dat het een zeer grote inspanning is geweest, maar dat het eind–resultaat zeer tot tevredenheid stemt. Hierbij wil ik mijn ouders, (schoon)familie en vrienden bedanken voor hun betrokkenheid in de verschillende fasen van de totstandkoming. Maar bovenal wil ik mijn vriendin bedanken die als enige alles van dichtbij heeft meegemaakt en evenveel energie in het proces heeft gestopt als ik.

Bijzondere dank wil ik nog uitspreken aan Jan voor de betrokken en prikkelende begeleiding, aan Tom voor het vertrouwen en aan Adwo voor het altijd constructieve en vaak humoristi–sche commentaar.

Samenvatting

Deze scriptie is het verslag van mijn onderzoek naar een methode voor het gestructureerd opstellen van informatiebeveiligingsbeleid op basis van de (informatie)behoeften van een organisatie. Het onderzoek is uitgewerkt door allereerst te onderzoeken wat informatie–beveiliging en informatiebeveiligingsbeleid zijn. Aansluitend is gezocht naar een relatie tussen de (informatie)behoeften van organisaties en de vereiste inhoud van het infor–matiebeveiligingsbeleid. Op basis van deze relatie is beschreven hoe het opstellen van informatiebeveiligingsbeleid dient plaats te vinden. Dit alles is uitgewerkt in zes onderzoeks–delen (kernvragen). Onderstaand is dit geheel schematisch weergegeven:



Informatiebeveiliging

Organisaties maken heden ten dage zeer intensief gebruik van informatietechnologie en passen veelal zelfs hun bedrijfsprocessen hierop aan. De kwaliteit van informatiesystemen en de daarin bevatte informatie is daardoor voor organisaties (in meer of mindere mate) van belang. Om de kwaliteit te waarborgen is vereist dat organisaties informatiebeveiliging onderdeel maken van hun bedrijfsvoering.

Informatiebeveiliging is gericht op het beschermen van de betrouwbaarheid (bestaande uit beschikbaarheid, integriteit en vertrouwelijkheid) van informatie. Voorwaarde hiervoor is wel dat alle maatregelen die in dit kader worden getroffen controleerbaar zijn. Hierbij gelden de kwaliteitsaspecten doeltreffendheid en doelmatigheid als randvoorwaarden voor de richtlijnen en maatregelen die ten behoeve van informatiebeveiliging worden gesteld en ingericht.

Informatiebeveiliging vormt een cyclisch proces waarin vier fasen kunnen worden onderkend: inventariseren, ontwerpen, implementeren en beheersen. In de fase van het ontwerpen wordt het informatiebeveiligingsbeleid opgesteld.

Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is het organisatiebrede beleid dat, middels strategische richtlijnen en procedures, sturing geeft aan de uitvoering van de informatiebeveiliging teneinde inbreuken op de betrouwbaarheid van de informatievoorziening te voorkomen en de gevolgen van eventuele inbreuken te beheersen.

Het beveiligingsbeleid is essentieel voor een goede werking van het informatiebeveiligingsproces. Het beleid dient diverse belangen, waaronder vorm en richting geven aan de informatiebeveiliging, betrokkenheid van het management verkrijgen en betuigen, het stellen van verantwoordelijkheden binnen de informatiebeveiliging en het voldoen aan wettelijke, maatschappelijke en commerciële eisen. Het beveiligingsbeleid hangt primair samen met het informatiebeleid, maar ook met het facilitair beleid, het personeelsbeleid en het financieel beleid.

Op basis van literatuur en diverse voorbeelden van beveiligingsbeleid is geïnventariseerd uit welke onderdelen beveiligingsbeleid bestaat. Naar aanleiding daarvan is vastgesteld dat

beveiligingsbeleid van verschillende organisaties globale overeenkomsten vertoont in vorm, reikwijdte en structuur. Beveiligingsbeleid verschilt tussen organisaties in de hoeveelheid beveiligingsrichtlijnen en de mate waarin deze stringent zijn.

De onderzochte voorbeelden suggereren dat een relatie bestaat tussen de hoeveelheid en stringentheid van de richtlijnen en het 'karakter' van een organisatie. De hypothese is dat het beveiligingsbeleid op basis van zo'n relatie kan worden gestandaardiseerd. Daarbij dient een balans te worden gevonden tussen maatwerk en confectie, teneinde het opstellen beveiligingsbeleid efficiënt en effectief te laten verlopen, waarbij het beleid wel voldoende moet worden afgestemd op de behoeften van een organisatie. Deze balans kan worden bereikt door het beveiligingsbeleid af te stemmen op de mate waarin een organisatie afhankelijk is van de betrouwbaarheid van de informatievoorziening.

Betrouwbaarheidsbehoefte

Naar aanleiding van de geconstateerde verschillen en overeenkomsten in beveiligingsbeleid is gezocht naar factoren die de invulling van het beveiligingsbeleid bepalen. Daarbij is aangegeven dat de invulling van beveiligingsbeleid in essentie wordt bepaald door de mate waarin organisaties behoefte hebben aan waarborging van de betrouwbaarheid van de informatievoorziening. Dit is gedefinieerd als de betrouwbaarheidsbehoefte.

De betrouwbaarheid van de informatievoorziening kent twee dimensies, te weten de afhankelijkheid en de kwetsbaarheid van de informatievoorziening. De afhankelijkheid geeft aan in welke mate de betrouwbaarheid van de informatievoorziening moet worden gewaarborgd op basis van de behoeften van een organisatie. Die behoeften komen voort uit de wijze waarop een organisatie gebruik maakt van informatievoorziening. De kwetsbaarheid wordt bepaald door de bedreigingen waaraan de informatievoorzieningen bloot staat. Dit is inherent aan het gebruik van informatie maar wordt daarentegen niet bepaald door het gebruik de informatievoorziening zelf maar door externe bedreigingen. De kwetsbaarheid is een indicatie van de mate waarin een organisatie nog niet voldoet aan de betrouwbaarheidseisen die volgen uit de afhankelijkheid, doordat kwetsbaarheden nog niet zijn afgedekt.

In essentie bepaalt de afhankelijkheid de mate waarin beveiliging vereist is en geeft de kwetsbaarheid aan op welke wijze moet worden gehandeld om (alsnog) aan dat vereiste niveau te voldoen. Daarmee is de afhankelijkheid de bepalende factor voor de betrouwbaarheidsbe-

hoefte, omdat het beveiligingsbeleid aangeeft welke niveau van beveiliging vereist is op basis van de behoeften van de organisatie. De kwetsbaarheid komt in beeld wanneer uitvoering wordt gegeven aan het beveiligingsbeleid.

Teneinde de betrouwbaarheidsbehoefte te bepalen is gezocht naar makkelijk vast te stellen ('oppervlakkige') organisatie kenmerken welke de afhankelijkheid van de informatievoorziening bepalen. Hierbij zijn de typologie en de attitude van een organisatie geëvalueerd. Naar aanleiding hiervan is beschreven dat noch de typologie, noch de attitude, noch enige andere oppervlakkige organisatie–eigenschap doorslaggevend is voor de afhankelijkheid van de informatievoorziening en dat een combinatie van dergelijk eigenschappen praktisch gezien zeer moeilijk is te bepalen. Derhalve dient te worden onderzocht hoe de betrouwbaarheidsbehoefte zelf rechtstreeks kan worden bepaald.

Mogelijke waarden van de betrouwbaarheidsbehoefte

Om efficiënt en effectief uitvoering te kunnen geven aan de relatie tussen de betrouwbaarheidsbehoefte en de invulling van het beveiligingsbeleid dient de betrouwbaarheidsbehoefte kwantificeerbaar te zijn. Alleen dan wordt de betrouwbaarheidsbehoefte meetbaar, waarbij aan specifieke waarden van de betrouwbaarheidsbehoefte een specifieke invulling van het beveiligingsbeleid kan worden gekoppeld.

Het vaststellen ('meten') van de betrouwbaarheidsbehoefte vereist dat het aantal mogelijk waarden klein genoeg is om de uitvoering niet te complex te maken, en tegelijkertijd voldoende verschillende waarden om verschillen tussen de betrouwbaarheidsbehoefte van organisaties met voldoende detail te kunnen representeren. Binnen dit onderzoek heb ik ervoor gekozen om de deel aspecten van de betrouwbaarheidsbehoefte (beschikbaarheid, integriteit en vertrouwelijkheid) ieder drie verschillende waarden aan te laten nemen. Dit betekent dat de betrouwbaarheidsbehoefte in totaal 27 verschillende waarden kan aannemen.

Gezien de algemene en strategische aard van het beveiligingsbeleid is het onwenselijk de gekwantificeerde betrouwbaarheidsbehoefte weer te geven met getallen, omdat dit een valse indruk van exactheid wekt. Ieder deelaspect van de betrouwbaarheidsbehoefte zal daarom worden gerepresenteerd in de zogenaamde linguïstische waarden L (laag), M (middelmatig) en H (hoog). Deze drie waarden dekken gezamenlijk het gehele behoeftenspectrum af, met uitzondering van de extremen, zijnde geen behoefte en maximale behoefte. Beide extremen kunnen niet door het beveiligingsbeleid worden afgedekt.

Waardebepaling van de betrouwbaarheidsbehoefte

Om de waarde van betrouwbaarheidsbehoefte – de triple (B,I,V) – vast te kunnen stellen is allereerst het gebruik van reguliere risicoanalyses onderzocht. Daarbij is aangegeven dat deze niet goed passen in de behoefte om de betrouwbaarheidsbehoefte efficiënt en effectief vast te stellen, omdat uitvoering gericht is op individuele informatiesystemen. Dit zal (met name voor organisaties met veel informatiesystemen) veel tijd en inzet vergen, waarbij het combineren van alle resultaten tot één betrouwbaarheidsbehoefte een complexiteit op zichzelf vormt.

Als alternatief is het begrip 'macrorisicoanalyse' uitgewerkt, gericht op het analyseren van de risico's waarvoor een organisatie zich geplaatst ziet op het hoogste niveau. Als concrete uitwerking van een macrorisicoanalyse is de SPRINT methode van het International Security Forum (ISF) beschreven. Deze methode is gericht op het snel en eenvoudig op hoofdlijnen bepalen van de afhankelijkheid en kwetsbaarheid van informatiesystemen. Aangezien eerder is bepaald dat de betrouwbaarheidsbehoefte, die bepalend is voor de invulling van het beveiligingsbeleid, in essentie bestaat uit de afhankelijkheid van de informatievoorziening, is alleen het deel 'afhankelijkheidsanalyse' van de SPRINT methode van belang.

De SPRINT methode is business georiënteerd, waarbij in samenwerking met managers de afhankelijkheid van informatiesystemen op hoofdlijnen worden bepaald. De SPRINT methode sluit nauw aan bij de doelen van dit onderzoek, zijnde de behoefte aan efficiëntie en effectiviteit. Omdat SPRINT gericht is op informatiesystemen, terwijl de betrouwbaarheidsbehoefte voor een organisatie als geheel geldt, is de SPRINT methode aangepast om bij dit laatste aan te sluiten.

De bruikbaarheid van de SPRINT methode als macro–risicoanalyse voor het opstellen van beveiligingsbeleid is op basis van een casus getoetst aan expert knowledge. Met drie experts is een proefanalyse uitgevoerd op een geschetste fictieve casus. Uit de proefanalyse komt naar voren dat de SPRINT methode geschikt is om te gebruiken binnen de te ontwikkelen methode voor het systematisch opstellen van informatiebeveiligingsbeleid. De methode biedt voldoende stabiliteit, gezien de gelijkheid in uitvoering door de experts.

Voorzichtigheid dient wel te worden betracht in geval van zeer grote of complexe organisaties, bijvoorbeeld met meerdere divisies of landenlocaties. In dat geval wordt de methode niet geschikt geacht om de betrouwbaarheidsbehoefte voor de organisatie als geheel te bepalen. In dat geval is de methode wel geschikt om te gebruiken per divisie of land. De experts benadrukken dat bij gebruik van de methode expert knowledge vereist is. De uitvoering en

uitkomst van de methode moet altijd een wisselwerking zijn tussen het de methode en de expert. Een expert dient de uitkomsten en toepasbaarheid van de methode te toetsen aan het beeld dat hij/zij heeft bij een organisatie. De methode kan worden gehanteerd als leidraad om het proces te structureren en leiden, maar kan niet worden gebruikt als geïsoleerd instrument zonder expert knowledge.

Van betrouwbaarheidsbehoefte naar beveiligingsbeleid

Op basis van de ontwikkelde methode om de betrouwbaarheidsbehoefte van een organisatie te bepalen is onderzocht hoe het beveiligingsbeleid kan worden ingevuld op basis van de gekwantificeerde betrouwbaarheidsbehoefte. Daarbij is aangegeven dat dit mogelijk wordt middels de standaardisatie van de mogelijke onderdelen van beveiligingsbeleid, te weten beschrijvende teksten en beveiligingsrichtlijnen.

Standaardisatie van beschrijvende teksten kan niet volledig plaatsvinden, omdat deze het karakter van het bedrijf weerspiegelen in het beveiligingsbeleid en beleid 'eigen' maken voor een organisatie. Wel is het mogelijk een standaard raamwerk te gebruiken als uitgangspunt voor de beschrijvende teksten. Dit raamwerk biedt een voorbeeldstructuur en teksten die op basis van de analyse van beveiligingsbeleid in hoofdstuk drie als standaard onderdelen zijn geïdentificeerd. In de appendices zo'n raamwerk opgenomen. De standaardisatie van beveiligingsrichtlijnen kan concreter worden uitgevoerd. Om standaardisatie van beveiligingsrichtlijnen mogelijk te maken is allereerst een verzameling van alle mogelijke richtlijnen vereist: het universum van beveiligingsrichtlijnen. Dit universum van mogelijke richtlijnen vormt de basis voor maken van de selectie van beveiligingsrichtlijnen die in het beveiligingsbeleid moeten worden opgenomen.

Omdat is bepaald dat de invulling van beveiligingsbeleid wordt bepaald door de betrouwbaarheidsbehoefte, is gekozen om de keuze van beveiligingsrichtlijnen daarop aan te sluiten. Daartoe moeten alle beveiligingsrichtlijnen in het universum worden geclassificeerd volgens dezelfde indeling als de betrouwbaarheidsbehoefte via een classificatie $R_{(B,I,V)}$. Deze classificatie geeft aan bij welke betrouwbaarheidsbehoefte een richtlijn van toepassing is. Aansluitend kan door koppeling van de voor een organisatie vastgestelde betrouwbaarheidsbehoefte aan de richtlijnen met een overeenkomstige classificatie het beveiligingsbeleid worden opgebouwd.

Teneinde inzicht te verkrijgen in de toepasbaarheid van deze werkwijze is met materie-experts een praktijktoets uitgevoerd op zowel het classificeren van richtlijnen als het op basis

van de classificatie samenstellen van beveiligingsbeleid. Hieruit is gebleken dat de voorgestelde methode praktisch bruikbaar is. Daarbij is echter wel aangegeven dat de toegekende classificatie op basis van de beperkte testgroep en de fictieve casus door gebruik in de praktijk verder geoptimaliseerd kan worden.

Naar aanleiding van de toetsing van het proefbeleid is geëvalueerd of het efficiënter en/of effectiever zou zijn om de stap van het bepalen van de betrouwbaarheidsbehoefte over te slaan en direct per mogelijke beveiligingsrichtlijn te evalueren of deze gewenst (vereist) is voor een organisatie. In dat geval zou echter het nut worden geëlimineerd van de eerste grove selectie op basis van de betrouwbaarheidsbehoefte. Dan zou namelijk iedere richtlijn door de expert opnieuw moeten worden beoordeeld op relevantie voor de betrokken organisatie. Zowel de (impliciete) inschatting van de beveiligingsbehoefte van de organisatie als (ongestructureerde) keuze van de richtlijnen zouden telkens opnieuw moeten worden uitgevonden.

Het belangrijke voordeel van de classificatie van richtlijnen is dat in de classificatie van de richtlijnen expert–kennis besloten ligt uitvoerende experts ondersteunt bij hun werkzaamheden. Een expert hoeft daardoor niet telkens zelf op basis van alleen zijn eigen kennis en ervaring een inschatting maken van de toepasbaarheid van een richtlijn. Daarbij is wel aangegeven dat de selectie van beveiligingsrichtlijnen op basis van de classificaties en de betrouwbaarheidsbehoefte niet 100% bindend hoeft te zijn. In de praktijk kunnen zich situaties voordoen waarin de standaard classificatie niet gepast is. Derhalve moet de geselecteerde richtlijnen altijd globaal worden beoordeeld op wenselijkheid, op basis van *professional judgement* van de betrokken expert(s).

Conclusies en aanbevelingen

Deze doelstelling om een methode te ontwikkelen voor het gestructureerd opstellen van informatiebeveiligingsbeleid is gerealiseerd door kwantificering van de betrouwbaarheidsbehoefte en classificatie van de standaard onderdelen van beveiligingsbeleid in de praktijk te brengen. Door deze twee aspecten te koppelen kan het beveiligingsbeleid worden opgesteld. Uit toetsing van deze methodiek op basis van een fictieve casus is gebleken dat de voorgestelde methode praktisch bruikbaar is. Daarbij is echter wel gebleken dat de toegekende classificatie door gebruik in de praktijk verder geoptimaliseerd kan worden. Tevens is aangegeven dat na selectie van beveiligingsrichtlijnen op basis van de classificaties en de betrouwbaarheidsbehoefte niet 100% bindend hoeft te zijn.

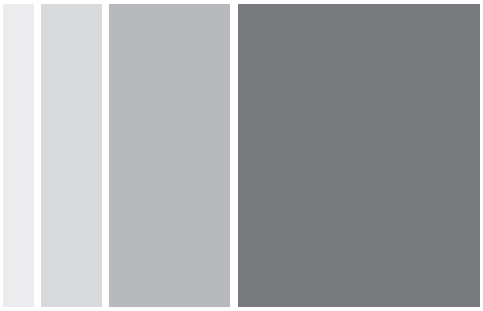
Tijdens het onderzoek is gebleken dat deze methode een duidelijk toegevoegde waarde heeft ten opzicht van het 'handmatig' opstellen van beveiligingsbeleid. Het gebruik van de methode voorkomt dat een expert bij het opstellen van beveiligingsbeleid iedere mogelijke beveiligingsrichtlijn alleen op basis van eigen kennis en ervaring telkens opnieuw moet worden beoordeeld op relevantie voor de betrokken organisatie. In de classificatie van de richtlijnen ligt zeer waardevolle bevatte expert–knowledge besloten waarop experts bij de uitvoering kunnen steunen. Dit levert een grote bijdrage aan de efficiëntie en de effectiviteit van het opstellen van informatiebeveiligingsbeleid.

Desondanks is ook aangegeven dat nog steeds de betrokkenheid van deskundigen vereist is. De methode is namelijk in geen geval een black box is waar je de betrouwbaarheidsbehoefte in stop en waar vervolgens een kant en klaar beveiligingsbeleid uit komt. De methode biedt een grove aanzet die vervolgens op basis van ervaring, deskundigheid en professional judgement moet worden vervolmaakt.

Mogelijkheden tot verdere verbetering van de methode liggen vooral in de verfijning van de kwantificering van de betrouwbaarheidsbehoefte en in optimalisatie van het universum van beveiligingsrichtlijnen. Het eerste betreft het inbouwen van een verder verfijning van de mogelijke waarden van de betrouwbaarheidsbehoefte. Het tweede betreft het volledig maken van het universum van mogelijke beveiligingsrichtlijnen en het verder verbeteren van de classificatie van de richtlijnen, vooral door meer expert–kennis bij de classificatie te betrekken. Hoe meer expert–kennis in de classificatie is bevat, hoe betrouwbaarder deze mag worden geacht.

Gezien de conclusie van het onderzoek dat het gebruik van een gestructureerde methode de efficiëntie en effectiviteit van het opstellen van beveiligingsbeleid verhoogt acht ik de completering van het universum en classificatie daarvan met meer experts zeer wenselijk. In mijn ogen bestaat er behoefte aan een volledig gereedschap voor het opstellen van beveiligingsbeleid in de vorm van een beschrijving van de methode en het bijbehorende volledige universum van geclassificeerde beveiligingsrichtlijnen waarin alle expert–kennis op dit gebied gebundeld is. Zo'n gereedschap zou analoog aan de code voor informatiebeveiliging een **'Code voor Informatiebeveiligingsbeleid'** moeten zijn die organisaties als de ultieme best practice voor beveiligingsbeleid kunnen hanteren.

Inhoudsopgave



1 Inleiding **16**

1.1 Informatie, automatisering en de noodzaak tot beveiliging 17
1.2 Sturing van informatiebeveiliging 18
1.3. Probleemformulering 19
1.4 Methodiek 22
1.5 Structuur van de tekst 23

2 Informatiebeveiliging **24**

2.1 Automatisering van de informatievoorziening 26
2.2 Kwaliteit van informatievoorziening 29
2.2.1 Kwaliteitsaspecten van informatievoorziening 29
2.2.2 Kwaliteitsaspecten verengd tot betrouwbaarheid 30
2.3 Het informatiebeveiligingsproces 31
2.4 Informatiebeveiligingsorganisatie 34
2.4.1 Rollen binnen de beveiligingsorganisatie 35
2.4.2 Beveiligingstaken en -verantwoordelijkheden 35
2.5 Theorieën, formele modellen en best practices 37
2.5 Conclusie 38

3 Informatie-beveiligingsbeleid 39
3.1. Wat is informatiebeveiligingsbeleid 40
3.2 De plaats van het beveiligingsbeleid binnen het informatiebeveiligingsproces 42
3.3 Het belang van informatiebeveiligingsbeleid 43
3.3.1 Vorm en richting geven aan de informatiebeveiliging 43
3.3.2 Betrokkenheid van het management verkrijgen en betuigen 44
3.3.3 Basis voor disciplinaire acties 45
3.3.4 Veranderen van de houding ten opzichte van informatiebeveiliging 45
3.3.5 Stellen van verantwoordelijkheden 46
3.3.6 Het uitsluiten van hoofdelijke aansprakelijkheid 46
3.3.7 Voldoen aan wettelijke, maatschappelijke en commerciële eisen 46
3.4 De context van informatiebeveiligingsbeleid 47
3.4.1 Relatie met andere beleidsgebieden 47
3.4.2 Reikwijdte van het informatiebeveiligingsbeleid 48
3.4.3 Invloedssfeer van het informatiebeveiligingsbeleid 48
3.5 Onderdelen van het informatie–beveiligingsbeleid 49
3.6 Voorbeelden van beveiligingsbeleid vergeleken 50
3.7 Balans tussen maatwerk en confectie 52
3.8 Conclusie 53

4 Betrouwbaarheidsbehoefte 55
4.1 Behoefte aan betrouwbaarheid 56
4.2 Afhankelijkheid en kwetsbaarheid van de informatievoorziening 57
4.3 De invloed van de betrouwbaarheidsbehoefte op het beveiligingsbeleid 60
4.4 Indicatieve factoren 60
4.4.1 Administratief organisatorische typologieën 61
4.4.2 Attitude 62
4.4.3 Andere organisatie eigenschappen 64
4.5 Conclusie 64

5 Mogelijke waarden van de betrouwbaarheidsbehoefte 66
5.1 Kwantificeren van de betrouwbaarheidsbehoefte 68
5.2 Randvoorwaarden voor kwantificering 69
5.3 Mogelijke waarden van de betrouwbaarheidsbehoefte 70
5.3.1 Gebruik van linguïstische waarden 70

5.3.2 Afdekking van het behoeftenspectrum *71*
5.4 Uitwerking van de mogelijke waarden van de betrouwbaarheidsbehoefte 72
5.4.1 Beschikbaarheid *72*
5.4.2 Integriteit *73*
5.4.3 Vertrouwelijkheid *74*
5.5 Conclusie 75

6 Kwantificering van de betrouwbaarheidsbehoefte 76
6.1 Gebruik van reguliere risicoanalyses 77
6.2 De 'macro' risicoanalyse 79
6.3 Evaluatie van de SPRINT methode voor het bepalen van de betrouwbaarheidsbehoefte 79
6.3.1 Kenmerken van de SPRINT methode *80*
6.3.2 Gebruik van de SPRINT afhankelijkheidsanalyse in het kader van dit onderzoek *81*
6.4 Gebruik van de SPRINT methode 82
6.4.1 Uitvoeren van de afhankelijkheidsanalyse *82*
6.4.2 Bepalen van de overall afhankelijkheid per betrouwbaarheidsaspect *83*
6.5 Proefanalyse met behulp van de aangepaste SPRINT methode 85
6.6 Conclusie 87

7 Van betrouwbaarheidsbehoefte naar beveiligingsbeleid 89
7.1 Invulling van beveiligingsbeleid op basis van de betrouwbaarheidsbehoefte 91
7.2 Standaardisatie van teksten 91
7.3 Standaardisatie van beveiligingsrichtlijnen 93
7.3.1 Samenstellen van een universum van informatiebeveiligingsrichtlijnen *94*
7.3.2 Classificeren van de richtlijnen in het universum *94*
7.3.3 Volledigheid van het universum *95*
7.4 Verkennend onderzoek naar het samenstellen van het universum van richtlijnen 97
7.4.1 Verzamelen van beveiligingsrichtlijnen *98*
7.4.2 Classificeren van beschikbare richtlijnen *98*
7.5 Proefinvulling van het beveiligingsbeleid op basis van de betrouwbaarheidsbehoefte 99
7.5.2 Selectie van richtlijnen voor de casusorganisatie *99*
7.5.2 Kwaliteit van de gemaakte richtlijnenselectie *100*

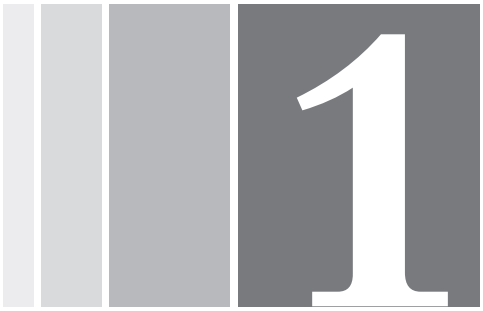
7.5.3 Efficiëntie van de gevolgde selectiemethode *102*
7.5 Conclusie 103

8 Conclusies en aanbevelingen 105
8.1 Conclusie 105
8.1.1 Beantwoording van de probleemstelling *106*
8.1.2 Realisatie van de doelstelling *107*
8.2 Aanbevelingen 109
8.2.1 Verfijning van de kwantificering van de betrouwbaarheidsbehoefte *109*
8.2.2 Optimalisatie van het universum van beveiligingsrichtlijnen *110*
8.2.3 Onderzoeksuitkomsten als toetsingskader voor beveiligingsbeleid *111*

Literatuuropgave 112

A Vergelijking voorbeeldenvan beveiligingsbeleid 116
B Raamwerk informatiebeveiligingsbeleid 127
C Vragenlijsten bepalingbetrouwbaarheidsbehoefte 138
D Verkennend onderzoek naar de bruikbaarheid van de SPRINT methode 142
E Universum vanbeveiligingsrichtlijnen 153

Inleiding



"De moderne bedrijfsvoering wordt dankzij de technologische ontwikkelingen steeds opener, waardoor de grenzen tussen uw organisatie en de buitenwereld vervagen. Dat geeft ongenode bezoekers ook meer manieren om binnen te dringen. U moet uw informatiesystemen dus beschermen tegen de mogelijkheid van een elektronische inbraak door een 'hacker'. [...] In veel gevallen is informatiebeveiliging zelfs geen keuze, maar een wettelijke verplichting."

Nederland gaat digitaal, netjes volgens het boekje
Ministerie van Economische Zaken, 2002

Deze scriptie is het verslag van het door mij binnen de studie Bestuurlijke Informatica uitgevoerde afstudeeronderzoek, zoals voorgeschreven door de Faculteit der Economische Wetenschappen. In dit inleidende hoofdstuk schetst ik om te beginnen de aanleiding voor het onderzoek, uitmondend in de doel- en probleemstelling. Aansluitend beschrijf ik op welke wijze ik het onderzoek heb uitgevoerd en hoe de resultaten van het onderzoek zijn beschreven in deze scriptie.

1.1 Informatie, automatisering en de noodzaak tot beveiliging

"Hoe langer hoe meer groeien computersystemen uit tot de zenuwcentra van het moderne bedrijfsleven." –Dit had een citaat kunnen zijn uit een willekeurig zeer recent boek over bedrijfsautomatisering. Deze zin is echter het begin van een uitgave van het Nederlands Genootschap voor Informatica (NGI) uit 1979 [NGI1979], waarin een overzicht wordt gegeven van de belangrijkste aspecten van computerbeveiliging. Ruim twintig jaar geleden bestond dus al een bewustzijn van de mate waarin organisaties afhankelijk zijn geworden van informatietechnologie (IT). Gezien de ontwikkelingen in de twintig jaar die achter ons liggen is deze afhankelijkheid alleen maar groter geworden. En er is geen enkele aanwijzing om te verwachten dat die ontwikkeling zich in de nabije toekomst niet door zal zetten.

Informatie is uitgegroeid tot de smeerolie die processen binnen organisaties soepel laat verlopen. Betrouwbare verwerking van informatie is een vereiste geworden voor de werking van bedrijfsprocessen. Voor tal van organisaties is het verwerken van informatie zelfs het belangrijkste proces. Steeds vaker wordt informatie daarom na arbeid, natuur en kapitaal benoemd tot vierde productiefactor. [OVER2000] Om de verwerking van informatie te optimaliseren maakten en maken organisaties steeds gretiger gebruik van de mogelijkheden die automatisering biedt. De toepassing van automatisering heeft een stormachtige ontwikkeling doorgemaakt en inmiddels is automatisering volledig verweven in bedrijfsprocessen.

De enorme toename in toepassing van IT heeft echter niet alleen zegeningen gebracht, maar heeft ook risico's geïntroduceerd. Het gemak waarmee IT binnen een organisatie informatie beschikbaar maakt, heeft als nadeel dat diegenen die dat willen (en daartoe in staat zijn) diezelfde IT kunnen gebruiken om op ongeautoriseerde wijze de informatie te ge/misbruiken. Om zeker te stellen dat de in gebruik zijnde informatie en informatieverwerkende systemen beschermd zijn tegen bedreigingen, dienen daarom maatregelen te worden getroffen, die specifiek toegespitst zijn op de automatisering van de informatieverzorging.

De ontwikkeling en toepassing van kennis op dit vlak is uitgegroeid tot een expertise die de laatste jaren (in positieve en negatieve zin) een grote schare aanhangers heeft vergaard, genaamd informatiebeveiliging (in internationaal verband aangeduid als *Information Security*). Informatiebeveiliging is een verzamelnaam voor het geheel van processen en maatregelen

om informatie en informatieverwerkende systemen te beschermen tegen bedreigingen, zoals bijvoorbeeld diefstal of beschadiging. In hoofdstuk twee wordt informatiebeveiliging verder uitgediept, waarbij de belangrijkste begrippen formeel worden gedefinieerd.

In de militaire wereld is altijd veel aandacht geweest voor beveiliging van (de communicatie van) informatie. Dit is logisch gezien enerzijds de aard en het belang van gebruikte informatie en anderzijds het vooruitstrevende gebruik van automatisering. Binnen niet–militaire publieke organisaties heeft beveiliging echter lange tijd geen hoge prioriteit gehad, mede door de latere intrede van automatisering.

Beveiliging van informatie vond binnen niet–militaire organisaties weliswaar ook al plaats in de tijd dat er nog geen computertechnieken werden ingezet om informatie te verwerken. In het pre–computertijdperk was het beveiligingsvraagstuk voor organisaties echter beperkt in complexiteit. De essentie van het vraagstuk was weliswaar ook destijds 'we beschikken over informatie die vitaal is voor onze organisatie en daar mag alleen op geautoriseerde wijze gebruik van worden gemaakt', maar de uitwerking daarvan was relatief eenvoudig. Alle informatie was namelijk vastgelegd op fysieke media (papier, microfiche, et cetera) en in de hoofden van mensen. Dit laatste was vroeger, maar ook met de huidige technieken, lastig te beveiligen. Maar de beveiliging van op fysieke media opgeslagen informatie was – simpel gezegd – een kwestie van een betrouwbare archivaris en een fysiek goed beveiligd archief.

Sinds de introductie van IT in de informatieverzorging zijn bestaande bedreigingen veranderd en nieuwe bedreigingen ontstaan. Informatie is op vele wijzen toegankelijk en de technieken waarmee de informatie wordt verwerkt, wordt door kwaadwillenden vaak beter begrepen dan door de geautoriseerde gebruikers. Door deze ontwikkelingen is de kern van het vakgebied informatiebeveiliging compleet veranderd. Als gevolg van de door automatisering geïntroduceerde diversiteit aan bedreigingen en beveiligingsmogelijkheden is informatiebeveiliging een zeer complexe zaak geworden. Organisaties dienen daarom de beveiliging van hun informatie systematisch in te richten en uit te voeren, niet alleen rekening houdend met, maar vooral uitgaand van de automatisering.

1.2 Sturing van informatiebeveiliging

De media doen regelmatig verslag van gevallen van falende informatiebeveiliging (fraude, uitgelekte creditcardnummers, 'bekladde' websites). Dit zijn vaak de directe gevolgen van bij–

voorbeeld configuratiefouten of software die niet *up-to-date* is. Organisaties die geconfronteerd worden met dergelijke beveiligingsincidenten, trachten uiteraard zo snel mogelijk de 'lekken' te dichten. Daarbij bestaat de neiging om de aandacht alleen te richten op het incident en hiertegen ad–hoc maatregelen te treffen. Om te voorkomen dat informatiebeveiliging alleen op deze wijze wordt aangepakt is een structurele oplossing vereist [COUM1998].

Informatiebeveiliging is namelijk, ondanks de onlosmakelijke verbinding met automatisering, niet slechts een kwestie van het beveiligen van operationele informatietechnologie. Goede informatiebeveiliging vereist een bewustzijn van de gevaren die IT met zich meebrengt en een organisatiebrede aanpak van die gevaren. Daartoe dienen organisaties een proces in te richten waarin —op basis van de afhankelijkheid van de informatievoorzien en de bedreigingen waaraan de organisatie blootstaat— maatregelen worden getroffen en onderhouden om de betrouwbaarheid van de informatievoorziening te waarborgen.

Daarbij is informatiebeveiliging het meest effectief wanneer sprake is van centrale coördinatie. De hoogste leiding van een organisatie dient in dat kader sturing te geven aan de doelstellingen en de uitvoering van de beveiligingsprocessen [ROOS1998]. Om op operationeel niveau (de maatregelen met betrekking tot) de informatiebeveiliging eenduidig te implementeren dienen daarom op managementniveau richtlijnen uitgevaardigd te worden, waarin het management het belang van informatiebeveiliging aanduidt en waarmee richting wordt gegeven aan de implementatie, invoering en operationalisering van informatiebeveiliging. Dit gebeurt middels het opstellen van een informatiebeveiligingsbeleid [ROOS1998], [OVER2000].

Het informatiebeveiligingsbeleid bevat uitgangspunten op hoog niveau die zijn gebaseerd op aanvaarde standaarden en wetgeving waaraan de organisatie onderhevig is. In het beveiligingsbeleid formuleert het management van een organisatie de doelen die zullen worden nagestreefd op het gebied van informatiebeveiliging en de wijze waarop die doelen gerealiseerd dienen te worden[1].

1.3. Probleemformulering

Het opzetten van beveiligingsbeleid is niet het uit de kast trekken van een standaard document, om vervolgens de naam van de betreffende organisatie op de juiste plek in te vullen. Geen twee organisaties zijn immers gelijk. Verschillen tussen organisaties strekken zich uit

van de mate van automatisering tot de branche waarin de organisatie opereert. Deze verschillen hebben tot gevolg dat aan de informatiebeveiliging (en daarmee het beveiligingsbeleid) per organisatie andere eisen kunnen worden gesteld. Tegenover deze gedifferentieerde eisen staat de veelgehoorde wens om het opstellen van beveiligingsbeleid te optimaliseren door het gebruik van standaard teksten en checklists [COUM1998].

Om aan deze (op het oog) tegengestelde wensen te voldoen – en daarmee het opstellen van beveiligingsbeleid zo efficiënt en effectief mogelijk te laten verlopen – dient een evenwicht te worden gevonden tussen het gebruik van standaard elementen en systematieken enerzijds en het toespitsen van beveiligingsbeleid op specifieke wensen en eigenschappen van een organisatie anderzijds. Vanuit de praktijk bestaat de behoefte aan een methode voor het bepalen van en benutten van dat evenwicht. Vooral organisaties met expertise in informatiebeveiliging (denk aan EDP Auditors of IT consultants) die zeer diverse cliënten adviseren bij het opstellen van beveiligingsbeleid kunnen hiervan profiteren[2].

In de praktijk en de literatuur is kennis voorhanden voor het bepalen van de afhankelijkheid van informatie(systemen) of mogelijke onderdelen van het beveiligingsbeleid. Tevens stellen diverse adviesorganisaties voorbeelden van beveiligingsbeleid beschikbaar. Een integrale methode voor het systematisch opstellen van informatiebeveiligingsbeleid, op basis van de genoemde behoefte aan efficiëntie en effectiviteit, de mogelijkheden van maatwerk en confectie combinerend, is echter niet beschikbaar. Naar aanleiding hiervan heb ik de doelstelling van mijn onderzoek als volgt geformuleerd:

Doelstelling

> *Het ontwikkelen van een algemene methode voor het opstellen van informatiebeveiligingsbeleid, waarmee op basis van de (informatie)behoeften van een organisatie het informatiebeveiligingsbeleid voor de organisatie efficiënt en effectief kan worden opgesteld.*

De doelstelling verdient een korte toelichting. Het moge evident zijn dat het genereren van een perfect uitgewerkt beveiligingsbeleid eisen aan de te ontwikkelen methode stelt die niet te bevredigen zijn. Dit is te wijten aan het feit dat in dat geval elke stap en elke keuze in een dergelijke traject tot in detail uitgewerkt zouden moeten zijn. (Al zou eventueel kunnen worden gedacht aan een intelligent systeem dat bijvoorbeeld via fuzzy logic kan redeneren op basis van beleidsprototypen, maar dat is een geheel andere insteek die hier buiten beschouwing wordt gelaten.) Dit onderzoek streeft ernaar, binnen de scope van een afstudeerscriptie,

een methode te ontwikkelen die in grote lijnen het proces van het opstellen van informatie–beveiligingsbeleid ondersteunt. Dat betekent dat het eindproduct meer een leidraad zal zijn dan een 'geautomatiseerde informatiebeveiligingsbeleidgenerator'.

Teneinde de geformuleerde doelstelling te realiseren, heb ik een probleemstelling geformu–leerd. In de probleemstelling komt de centrale vraag tot uitdrukking, die ik in mijn onderzoek zal beantwoorden. Middels het beantwoorden van deze vraag zal het behalen van de doelstel–ling worden nagestreefd.

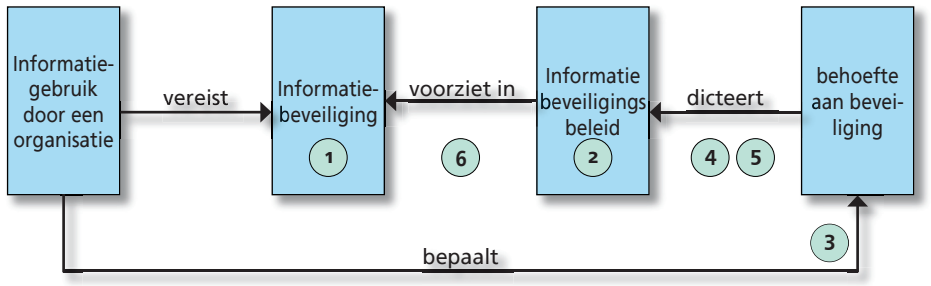
Probleemstelling

Welke factoren zijn voor een organisatie bepalend voor de invulling van het informatiebeveili-gingsbeleid, in welke mate zijn deze factoren bepalend en op welke wijze is het mogelijk het informatiebeveiligingsbeleid voor een organisatie systematisch van deze factoren af te leiden?

Teneinde de vraag uit de probleemstelling te beantwoorden, en daarmee de onderzoeksdoel–stelling te kunnen bereiken, heb ik de volgende te beantwoorden subvragen geformuleerd:

1. Wat wordt verstaan onder informatiebeveiliging en welke rol neemt het in binnen organisaties?
2. Wat wordt verstaan onder informatiebeveiligingsbeleid, in hoeverre verschilt infor–matiebeveiligingsbeleid tussen organisaties en welke mogelijkheden zijn er om informatiebeveiligingsbeleid te standaardiseren?
3. Welke factoren zijn bepalend voor de inhoud van het informatiebeveiligingsbeleid en wat is de invloed van deze factoren?
4. Aan welke voorwaarden dienen de beveiligingsbeleid bepalende factoren te voldoen om de inhoud van het beveiligingsbeleid op basis daarvan te kunnen bepalen?
5. Hoe kunnen de waarden van de beveiligingsbeleid bepalende factoren efficiënt en effectief worden vastgesteld zodat op basis daarvan het beveiligingsbeleid systematisch kan worden opgesteld?
6. Op welke wijze kan de inhoud van het informatiebeveiligingsbeleid efficiënt en effec–tief worden afgeleid van de gekwantificeerde beveiligingsbeleid bepalende factoren zodat het beleid voorziet in de voor een organisatie benodigde informatiebeveiliging?

In de rest van de tekst zullen deze vragen worden aangeduid als 'kernvragen', omdat de beantwoording ervan de kern van het onderzoek vormt. In figuur twee is de samenhang tus–sen de kernvragen schematisch weergegeven.



Figuur 2: De samenhang tussen de kernvragen schematisch weergegeven

1.4 Methodiek

Het verrichte onderzoek naar de antwoorden op de hierboven gestelde vragen heeft deels een descriptief, deels een normatief karakter en deels een toetsend karakter. Het descriptieve karakter ligt in de beantwoording van vraag één en twee. Daarbij wordt op basis van literatuurstudie en analyse van praktijkmateriaal[3] een overzicht geschetst van de algemeen geldende en geaccepteerde uitgangspunten en concepten van de informatiebeveiliging en de rol die beveiligingsbeleid hierin heeft. Dit betreft een definitiestudie, waarmee de basisconcepten voor de rest van het onderzoek wordt uiteengezet. Tevens wordt onderzocht in welke opzichten het informatiebeveiligingsbeleid van organisaties kan verschillen. Op basis van de verschillen (en overeenkomsten) wordt uitgewerkt in hoeverre beveiligingsbeleid kan worden gestandaardiseerd.

Vervolgens wordt, naar aanleiding van vraag drie, op basis van de onderzochte literatuur en praktijkvoorbeelden onderzocht welke factoren bepalend zijn voor de invulling van het informatiebeveiligingsbeleid. Hierop wordt in de literatuur beperkt ingegaan en de beschreven bevindingen komen daarom ook voort uit bestudering van praktijkvoorbeelden van informatiebeveiligingsbeleid en logische redenatie vanuit de in de beantwoording van vraag één en twee vastgestelde uitgangspunten. Daarmee heeft de beantwoording van vraag drie met name een normatief karakter.

De beantwoording van de vragen vier, vijf en zes en zeven is normatief van aard. Op basis van de antwoorden op de eerste drie vragen wordt een model ontwikkeld voor het kwantificeren van de voor het informatiebeveiligingsbeleid bepalende factoren. Aansluitend wordt een methode ontwikkeld om op basis van de gekwantificeerde factoren het beveiligingsbeleid op

te stellen. Onderdeel van deze laatste activiteit is het inventariseren van de mogelijke bouwstenen (met name beveiligingsrichtlijnen) van informatiebeveiligingsbeleid. In figuur 2 komt het onderscheid tussen de descriptieve onderdelen en de normatieve onderdelen tot uiting doordat de descriptieve delen één en twee concepten beschrijven (de blokken) en de normatieve delen drie tot en met zes relaties beschrijven (de pijlen).

De beantwoording van vragen vijf en zes kent naast een normatief karakter ook een toetsend karakter, omdat de kwaliteit van de ontwikkelde methodologie wordt getoetst op basis van kennis van materie-experts. De bij de toetsing gehanteerde methodiek wordt expliciet beschreven in de betreffende hoofdstukken.

1.5 Structuur van de tekst

De structuur van de tekst is gebaseerd op de in paragraaf 1.2.2 geformuleerde vragen. Deze vragen worden één voor één behandeld in aparte hoofdstukken (twee tot en met zeven). Aansluitend worden in hoofdstuk acht de conclusies en aanbevelingen geformuleerd.

Noten

1 In hoofdstuk 3 zal het beveiligingsbeleid in al haar facetten worden uitgewerkt.

2 Dit onderzoek is uitgevoerd in opdracht en onder begeleiding van een EDP Audit organisatie. Het onderzoek is echter niet alleen van nut voor EDP Auditors, maar voor iedere partij die actief bezig is met informatiebeveiligingsbeleid.

3 Voor het onderzoek waren enkele praktijkvoorbeelden van beveiligingsbeleid beschikbaar.

Informatiebeveiliging 2

"Informatiebeveiliging is niet langer het domein van specialisten. Onder invloed van de toenemende integratie van informatietechnologie (IT) in onze bedrijfsprocessen wordt beveiliging steeds vaker verankerd in de taken en verantwoordelijkheden van de bestaande organisatie. Informatiesystemen zijn onmisbaar geworden voor het kunnen aanbieden van producten en diensten aan de markt. Ook buiten de informatie-industrie werkt vrijwel elke werknemer tegenwoordig met IT. Dit heeft consequenties voor de manier waarop het beveiligingsvraagstuk moet worden aangepakt"

dr. E.E.O. Roos Lindgreen RE in COMPACT [ROOS1998]

Het is in het dagelijks leven (zowel zakelijk als privé) overduidelijk dat informatie en automatisering een zeer grote rol spelen in bijna alles wat we doen. Daar komt nog bij dat we een deel van de informatisering en automatisering niet eens merken, omdat het zich vooral achter de schermen afspeelt. Informatie is verweven in ons werk en ons leven. Weliswaar doet de transportbranche ons geloven dat zonder transport alles stil staat, maar meer nog zou je kunnen zeggen "zonder informatie staat alles stil". Gezien het belang van informatie voor

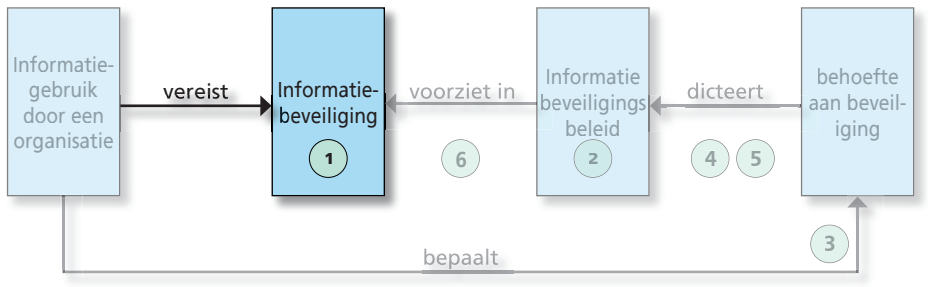
onze maatschappij en meer specifiek voor organisaties, moet op de kwaliteit ervan vertrouwd kunnen worden. Helaas staat de verwerking van informatie bloot aan vele bedreigingen en daarom moet werk worden gemaakt van de beveiliging, in de vorm van informatiebeveiliging [OVER2000, HART1995]. Teneinde, als basis voor de theorievorming omtrent beveiligingsbeleid, een duidelijk beeld te hebben van informatiebeveiliging, zal in dit hoofdstuk de volgende kernvraag worden beantwoord.

Kernvraag 1

Wat wordt verstaan onder informatiebeveiliging en welke rol neemt het in binnen organisaties?

In figuur 3 is nogmaals de samenhang tussen de kernvragen nogmaals weergegeven, waarbij ter verduidelijking de positie van dit hoofdstuk binnen het geheel is uitgelicht.

De kernvraag wordt uitgewerkt door allereerst in paragraaf 2.1 een indicatie te geven van de mate waarin de afhankelijkheid van informatievoorziening is gegroeid en hoezeer de automatisering ervan is toegenomen. In paragraaf 2.2 wordt vervolgens beschreven wat de kwaliteit van informatie bepaalt en op welke wijze deze kwaliteit wordt bedreigd. Aansluitend wordt in paragraaf 2.3 beschreven hoe de kwaliteit van informatie gewaarborgd wordt, in de vorm van informatiebeveiliging. Daarbij wordt voornamelijk ingegaan op de verschillende fasen die binnen informatiebeveiliging bestaan. Tot slot wordt in paragraaf 2.4 een overzicht geschetst van enkele algemeen geaccepteerde theorieën en modellen van informatiebeveiliging teneinde het begrip van informatiebeveiliging verder te vergroten.

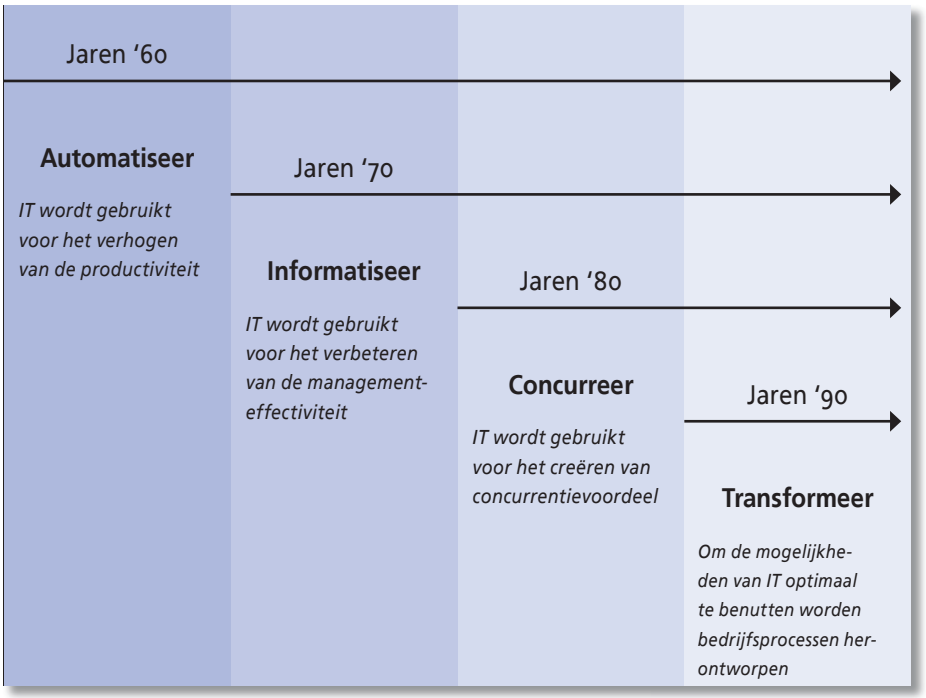


Figuur 3: De kernvraag van dit hoofdstuk is uitgelicht in het schema

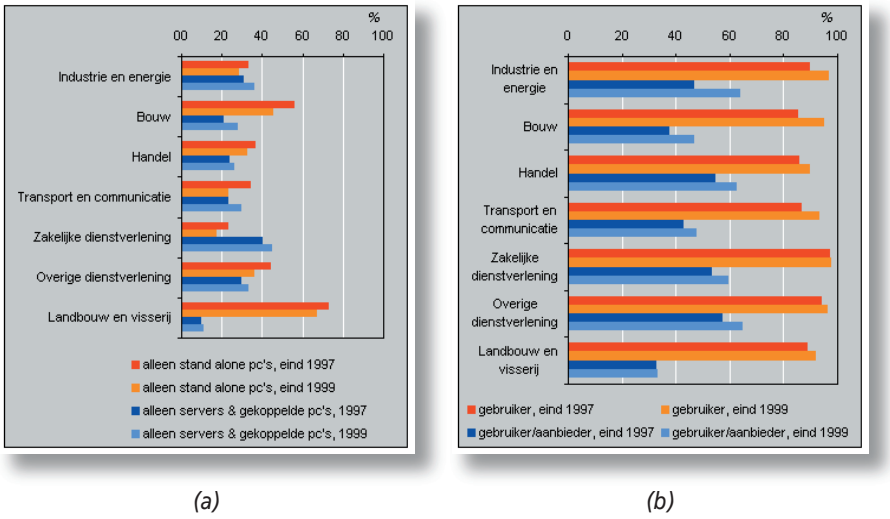
2.1 Automatisering van de informatievoorziening

Organisaties maken, zoals al beschreven in paragraaf 1.1, steeds intensiever gebruik van informatie om hun bedrijfsprocessen te sturen en te monitoren. Daarbij is het voor organisaties van belang om de vergaring, opslag, verwerking en verstrekking van informatie zo optimaal mogelijk te laten verlopen. Door optimaal gebruik te maken van informatievoorziening kunnen bedrijven sneller reageren op veranderende marktomstandigheden en kunnen belangrijke concurrentievoordelen worden behaald. Sinds de uitvinding van computertechnieken hebben organisaties dit mede getracht door het toepassen van automatisering. Dit uit zich vooral in twee ontwikkelingen in de toepassing van IT.

Ten eerste heeft de toepassing van computertechniek in de informatieverwerking van organisaties met de evolutie en revolutie van de techniek verschillende fasen doorlopen, zoals onder andere aangegeven door R. Pruijm [PRUI2000]. Deze fasen zijn weergegeven in figuur 3. Tijdens het doorlopen van deze fasen is informatietechnologie steeds meer verweven geraakt met de bedrijfsprocessen waardoor organisaties steeds afhankelijker zijn geworden van de



Figuur 3: Verschillende fasen in de toepassing van IT binnen organisaties



(a) *(b)*

Figuur 4: In afbeelding (a) worden de computerconfiguraties van geautomatiseerde bedrijven weergegeven. In afbeelding (b) is de mate van verbondenheid met internet aangegeven.

geautomatiseerde systemen. Met name in de laatste fase (*transformeer*) kiezen organisaties ervoor om bedrijfsprocessen te transformeren en herstructureren om de mogelijkheden van informatietechnologie ten volle te benutten. Hier bepalen de mogelijkheden van IT dus zelfs de inrichting van de bedrijfsprocessen. De bedrijfsprocessen zouden zonder deze IT niet o f nauwelijks kunnen functioneren.

Ten tweede kan geconstateerd worden dat de toepassing van IT (vooral) in de jaren negentig is verschoven van 'computation' naar 'communication'. De technieken die de mens in eer– ste instantie gebruikte om rekenkundige problemen op te lossen worden nu ingezet om 'de geïsoleerde mens' met anderen te verbinden [KELL1999]. Hierbij wordt IT ingezet om com– municatie binnen een organisatie en tussen organisaties onderling te verbeteren. In eerste instantie vormde IT een aanvulling op bestaande communicatievormen maar met het ver– strijken van de tijd zijn meer en meer klassieke vormen van communicatie geautomatiseerd tot het punt dat de communicatie bijna geheel afhankelijk is geworden van IT.

Deze drang naar (geautomatiseerde) communicatie blijkt met name uit de mate waarin organisaties hun computersystemen met elkaar verbinden en de mate waarin organisaties verbonden zijn met internet. Internet heeft organisaties in staat gesteld om via een gestan– daardiseerd medium te communiceren. Vooral in de tweede helft van de jaren negentig is het aantal bedrijven met netwerk– en/of internetverbinding explosief gegroeid, zoals te zien

is in figuur 5. Zo waren eind 1997 bij geautomatiseerde bedrijven ruim 1,6 miljoen PC's in gebruik, waarvan 82% via een netwerk gekoppeld. Eind 1999 was dit zelfs al opgelopen tot meer van 2 miljoen PC's waarvan 87% gekoppeld. Bij de overheid daalde het aantal stand–alone[4] PC's tussen 1997 en 1999 met 34%. Van de bedrijven met automatisering was eind 1997 zo'n 33% verbonden met internet. In 1999 was dit inmiddels opgelopen tot ruim 50% [CBS1999].

Genoemde ontwikkelingen hebben tot gevolg gehad dat informatie en de personen en appa–ratuur die de informatie verwerken steeds verder zijn geïntegreerd. Die integratie is zover gevorderd dat de informatie, personen en apparatuur die een (of meerdere) bedrijfsprocessen ondersteunen zijn verworden tot een eenheid. Zo'n eenheid wordt aangeduid als een infor–matiesysteem. Een informatiesysteem wordt door Overbeek et al [OVER2000] als volgt gedefinieerd:

Definitie:

> *Een **informatiesysteem** is een samenhangende gegevensverwerkende functionaliteit die kan worden ingezet om één of meer bedrijfsprocessen te kennen, te ondersteunen of te besturen. Een informatiesysteem kan de volgende componenten bevatten: apparatuur, programmatuur, gegevens, procedures en mensen.*

Het geheel van informatiesystemen dat binnen een organisatie is ingericht wordt de infor–matievoorziening genoemd. Dit is de overkoepelende term waarmee de verwerking van informatie en de daarbij gebruikte automatisering in deze tekst zal worden aangeduid.

Definitie:

> *De **informatievoorziening** is het geheel van informatiesystemen dat tot doel heeft te voorzien in de informatiebehoefte van een organisatie.*

Gezien het reeds meerdere malen aangehaalde belang van informatie en daarmee de informa–tievoorziening voor organisaties is het van belang een begrip te hebben van de kwaliteit van informatie en de bedreigingen waaraan die kwaliteit bloot staat. Dit wordt beschreven in de volgende paragraaf.

2.2 Kwaliteit van informatievoorziening

2.2.1 Kwaliteitsaspecten van informatievoorziening

Aan het gebruik van informatiesystemen kleven bepaalde gevaren die schade op kunnen leveren voor een organisatie. Die schade wordt veroorzaakt doordat de kwaliteit van de informatievoorziening wordt aangetast. Om de beveiliging van informatiesystemen te kunnen inrichten is het van belang te specificeren uit welke aspecten de kwaliteit van de informatievoorziening bestaat. Zich baserend op NivRA geschriften en het handboek EDP Auditing, noemt Hartman in [HART1995] de volgende kwaliteitsaspecten van informatie:

1. **Beschikbaarheid**
   De mate van ongestoorde voortgang van de informatievoorziening.
2. **Exclusiviteit**
   De mate waarin de bevoegdheid en mogelijkheid tot muteren, (uit)lezen, kopiëren, of kennisnemen (van informatie en andere systeemcomponenten) is beperkt tot een gedefinieerde groep gerechtigden.
3. **Integriteit**
   De mate van overeenstemming van informatie met het afgebeelde deel van de realiteit en dat niets ten onrechte is achtergehouden of verdwenen.
4. **Controleerbaarheid**
   De mate waarin het mogelijk is vast te stellen hoe het informatiesysteem en zijn componenten zijn gestructureerd en of het proces van gegevensverwerking en informatievoorziening tot het beoogde resultaat heeft geleid.
5. **Doelmatigheid**
   De mate waarin gewenste informatie tijdig en tegen aanvaardbare kosten wordt opgeleverd.
6. **Doeltreffendheid**
   De mate waarin de informatievoorziening alsook de daaraan dienstige verwerkingsprocessen aansluiten bij de verwachtingen van de gebruikers.

Een alternatieve wijze om naar kwaliteit van informatie te kijken komt met name voort uit de hoek van netwerk en communicatiebeveiliging. Daarin worden *security services* erkend, die beveiliging van dataverwerkende systemen en informatietransport verbeteren. Deze services, zoals onder andere beschreven door Stallings [STAL2000], zijn vertrouwelijkheid, authenticatie, integriteit, nonrepudiatie, toegangscontrole en beschikbaarheid. De genoemde services

hebben primair betrekking op dataverkeer, terwijl dit onderzoek zich niet alleen op dataverkeer maar op informatiesystemen in z'n algemeenheid. De indeling van kwaliteit naar security services zal hier derhalve niet verder worden uitgewerkt.

2.2.2 Kwaliteitsaspecten verengd tot betrouwbaarheid

In het kader van informatiebeveiliging zijn niet alle genoemde kwaliteitsaspecten van gelijk belang. Zoals door De Bruin en Schönfeld in het Handboek EDP Auditing [BRUI2000] wordt aangegeven, is de bescherming van informatie primair gericht op de waarborging van beschikbaarheid, integriteit en exclusiviteit (ook wel aangeduid als vertrouwelijkheid). Deze drie aspecten worden ook wel gebundeld in de term 'betrouwbaarheid'. Ook andere publicaties, zoals [OVER2000] beperken betrouwbaarheid in het kader van informatiebeveiliging tot de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. In het vervolg van deze tekst zal de volgende, op [OVER2000] gebaseerde definitie van betrouwbaarheid worden gehanteerd:

Definitie:

> *De **betrouwbaarheid** van de informatievoorziening geeft de mate aan waarin een organisatie zich kan verlaten op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.*

De begrippen beschikbaarheid, integriteit en vertrouwelijkheid worden veelal afgekort tot BIV. In internationale context worden deze begrippen aangeduid als *confidentiality* (vertrouwelijkheid), *integrity* (integriteit) en *availability* (beschikbaarheid), afgekort als CIA.

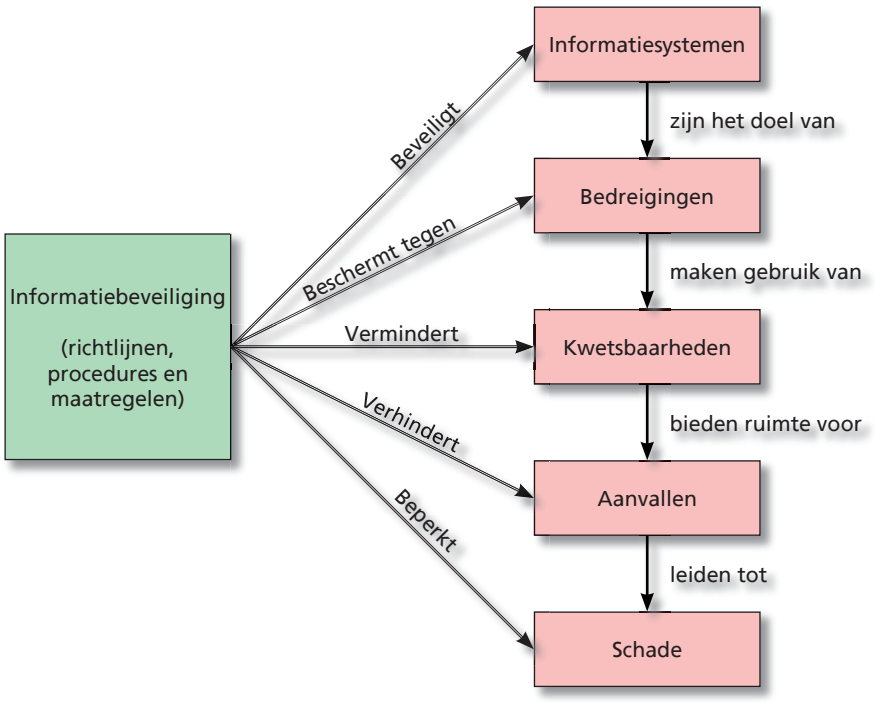
Ondanks dat controleerbaarheid geen onderdeel is van betrouwbaarheid, is het er wel nauw mee verbonden. Als namelijk "vastgesteld moet worden dat inderdaad in voldoende mate uitvoering is gegeven aan de aspecten integriteit, exclusiviteit en beschikbaarheid, dan is controleerbaarheid uiteraard van groot belang. Aan de andere kant kan erop gewezen worden dat ieder van de drie hierboven genoemde aspecten al een aspect van controleerbaarheid in zich draagt" [BRUI2000]. Hieruit kan worden geconcludeerd dat de haalbaarheid van de bescherming van beschikbaarheid, integriteit en exclusiviteit staat of valt met de controleerbaarheid ervan en dat controleerbaarheid in het kader van informatiebeveiliging derhalve als onderdeel van de andere drie aspecten kan worden beschouwd. Daarbij dient controleerbaarheid als vereiste te worden gesteld voor alle vormen van bescherming van informatie.

In het stuk van De Bruin en Schönfeld wordt tevens aangegeven dat de informatievoorziening naast 'veilig' vooral ook toereikend dient te zijn en dient te voorzien in de functionele wensen van de gebruikers. Deze kwaliteitsaspecten, door Hartman aangeduid als doeltreffendheid en doelmatigheid, dienen derhalve te worden gezien als randvoorwaarden voor de richtlijnen en maatregelen die ten behoeve van informatiebeveiliging worden ingesteld. Beveiliging kan immers leiden tot verminderde werkbaarheid en derhalve minder doeltreffende en doelmatige werking. Bij het inrichten van de informatiebeveiliging moet daarom een balans worden gevonden tussen de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van informatiebeveiliging enerzijds en de effectiviteit en efficiëntie ervan anderzijds.

2.3 Het informatiebeveiligingsproces

Om de in de vorige paragraaf besproken betrouwbaarheid van de informatievoorziening te waarborgen dienen inspanningen te worden geleverd. Deze inspanningen scharen we onder de noemer 'informatiebeveiliging'. Over de exacte invulling van dit begrip circuleren nogal wat verschillende meningen. De code voor informatiebeveiliging [NNI1994] definieert informatiebeveiliging als "het waarborgen dat de continuïteit van de bedrijfsvoering en het minimaliseren van de schade voor het bedrijf door het trachten te voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen".

Dit is in mijn ogen een wat beperkte definitie omdat alleen de continuïteit van de bedrijfsvoering wordt genoemd, in plaats van de eerder gedefinieerde betrouwbaarheid van de informatievoorziening, waarvan continuïteit een onderdeel is. In het Voorschrift Informatiebeveiliging Rijksoverheid (VIR) [BIZA1994] is een definitie te vinden die beter bij het begrip betrouwbaarheid aansluit: "informatiebeveiliging: het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van een informatiesysteem en daarmee van de informatie daarin". Deze definitie zal hierna als uitgangspunt worden aangehouden, waarbij de eerdere definities van informatievoorziening en betrouwbaarheid in de definitie zijn geïncorporeerd. Tevens is het begrip 'maatregelen' uitgebreid tot 'procedures, richtlijnen en maatregelen', omdat dit mijns inziens volledi ger is dan alleen maatregelen. De in de rest van deze scriptie gevolgde definitie luidt derhalve:



Figuur 5: De functies van informatiebeveiliging

Definitie:

> ***Informatiebeveiliging*** *is het implementeren en onderhouden van een samenhangend pakket van richtlijnen, procedures en maatregelen ter waarborging van de betrouwbaarheid van de informatievoorziening.*

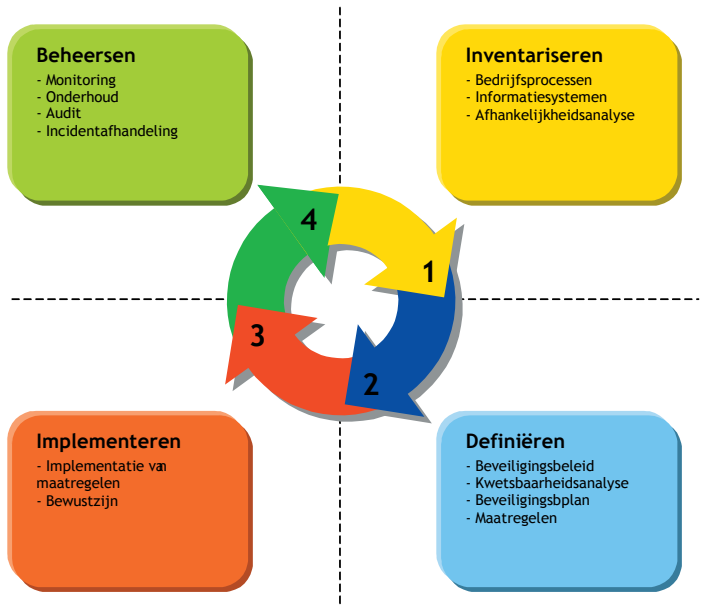
Zoals beschreven staat de betrouwbaarheid van informatiesystemen bloot aan bedreigingen. In het ergste geval kunnen die bedreigingen leiden tot afbreuk aan de betrouwbaarheid. Tussen bedreiging en schade zitten echter nog enkele stappen. Bedreigingen kunnen zich alleen manifesteren indien zich kwetsbaarheden voordoen. Eventuele kwetsbaarheden bieden ruimte voor aanvallen, welke uiteindelijk kunnen leiden tot schade. Informatiebeveiliging heeft een uitwerking op al deze aspecten. Dit is weergegeven in figuur 5.

De woorden "treffen en onderhouden" uit de definitie geven al aan dat informatiebeveiliging geen eenmalig iets is. Dit wordt onderbouwd door de literatuur ([OVER2000]; [NGI1995]; [INTER2001]), want daarin wordt informatiebeveiliging steevast beschreven als een cyclus of een proces[1]. De precieze uitwerking van dit proces (en de daarin genoemde stadia) verschilt

wel tussen de verschillende bronnen. Het voert binnen de reikwijdte van dit onderzoek echter te ver om een vergelijkend onderzoek van de verschillende uitwerkingen te doen. Dat is ook niet nodig, aangezien het beveiligingsproces alleen geschetst wordt teneinde de rol van beveiligingsbeleid daarin aan te kunnen duiden. Daarbij maakt het niet zozeer uit welke naam het stadium waarin beveiligingsbeleid zit heeft, maar waar het binnen het proces wordt geplaatst. Daarin komen de verschillende uitwerkingen namelijk in grote lijnen overeen.

In dat kader schets ik hier de grote lijn van het beveiligingsproces, zoals die is op te maken uit de beschikbare uitwerkingen. In essentie bestaat het informatiebeveiligingsproces uit de volgende vier fasen:

1. **Inventariseren** van het gebruik van informatie en de inzet van informatiesystemen binnen een organisatie. Hiermee ontstaat inzicht in de behoefte aan beveiliging van een organisatie.
2. **Ontwerpen** van het beveiligingsraamwerk, in de vorm van een beveiligingsorganisatie en een beveiligingsbeleid. In deze fase kan ook worden bepaald in hoeverre de organisatie voldoet aan het beleid en op welke gebieden verscherping van de beveiliging nodig is



Figuur 6: Het informatiebeveiligingsproces

3. **Implementeren** van beveiligingsmaatregelen op basis van het ontworpen beveiligingsraamwerk en de vastgestelde beveiliging nog tekortschiet..
4. **Beheersen** van de informatiebeveiliging middens evaluatie en (indien nodig) bijsturing van de werking van het beveiligingsraamwerk .

In het proces gaat fase vier weer over in fase één, waarbij de resultaten van de evaluatie meteen weer een inventarisatie vormen van het gebruik van informatiesystemen. In figuur 6 is het informatiebeveiligingsproces grafisch weergegeven.

2.4 Informatiebeveiligingsorganisatie

Om de informatiebeveiliging binnen een organisatie vorm te geven, dienen de hieraan verbonden verantwoordelijkheden en taken in de organisatie te worden ingebed. Hiertoe dient er een informatiebeveiligingsorganisatie te worden ingericht. De beveiligingsorganisatie wordt in diverse uitgaven nadere beschreven, waaronder in 'Organiseren van gegevensbeveiliging' [NGI1995] en in [ROOS1998].

In de literatuur heb ik geen concrete definitie kunnen vinden van de informatiebeveilig. Wel is duidelijk dat de beveiligingsorganisatie taken en verantwoordelijkheden beschrijft die zorgen voor het organiseren van de informatiebeveiliging. Op basis hiervan zal ik hierna de volgende definitie van de informatiebeveiligingsorganisatie hanteren.

Definitie

> *De **informatiebeveiligingsorganisatie** is het geheel van taken en verantwoordelijkheden die binnen een organisatie verantwoordelijk zijn voor de beheersing en sturing van de informatiebeveiliging teneinde de betrouwbaarheid van de informatievoorziening zoveel mogelijk te waarborgen.*

De taken en verantwoordelijkheden van de beveiligingsorganisatie vallen in de vier fasen van het informatiebeveiligingsproces zoals dat in de paragraaf hiervoor is beschreven.

2.4.1 Rollen binnen de beveiligingsorganisatie

Binnen de beveiligingsorganisatie kan een diversiteit aan rollen worden onderkend. Binnen de reikwijdte van deze scriptie voert het te ver een volledige analyse van de optimale beveiligingsorganisatie uit te voeren. Een uitgebreide opsomming van alle mogelijke functies, taken en verantwoordelijkheden binnen de informatiebeveiligingsorganisatie is te vinden in [NGI1995]. Ik beperk mij hier tot de meest essentiële en tevens meest voorkomende. Uit de genoemde literatuur en de beschikbare praktijkvoorbeelden van informatiebeveiligingsbeleid komen de volgende basale en meest voorkomende functies naar voren:

- Directie/Topmanagement;
- Lijnmanagement;
- Informatie–eigenaar;
- Security officer (ook wel Security coordinator of beveiligingscoördinator);
- Security administrator (ook wel beveiligingsbeheerder);
- (Externe) controleur.

Binnen de beveiligingsorganisaties kunnen meerdere rollen aan één persoon worden toegekend, zo lang daarmee een adequate functiescheiding niet wordt ondermijnd. Met name de functies van security officer en security administrator dienen te zijn gescheiden, omdat de eerste de tweede controleert.

2.4.2 Beveiligingstaken en -verantwoordelijkheden

Onderstaand worden de taken verantwoordelijkheden geschetst van de hiervoor opgesomde functies. Deze zijn gebaseerd op de beschrijvingen in de beschikbare praktijkvoorbeelden van informatiebeveiligingsbeleid en de literatuur op dit vlak ([NGI1995], [ROOS1998], [OVER2000]).

Directie/Topmanagement

- Bepalen van het vereiste niveau van informatiebeveiliging, gerelateerd aan de bedrijfsdoelstellingen;
- Opstellen van het informatiebeveiligingsbeleid;
- Aanmoedigen en ondersteunen van de naleving van het beveiligingsbeleid en de eraan gerelateerde richtlijnen en procedures.

Lijnmanagement

- Opstellen van informatiebeveiligingsplannen;
- Verantwoording dragen voor het implementeren van de uitgangspunten uit het informatiebeveiligingsbeleid in de organisatorische eenheden en systemen waarvoor lijnmanagers verantwoordelijk zijn;
- Het lijnmanagement dient periodiek de juiste implementatie van de informatiebeveiligingsmaatregelen te evalueren.

Eigenaren

- Inschatten van de beveiligingsrisico's ten opzichte van de data en de gevolgen van het verlies of manipulatie ervan op zowel korte als lange termijn;
- Het classificeren van informatiesystemen;
- Het bepalen van toegangsrechten tot de data, gebaseerd op het principe dat toegang tot data wordt afgeschermd, tenzij expliciete autorisatie is verleend;
- Het periodiek evalueren van de tot de data verleende toegangsrechten.

Beveiligingscoördinator (Security coordinator)

- lijnmanagers adviseren op het gebied van beveiligingszaken die zijn gerelateerd aan hun verantwoordelijkheden;
- ervoor zorgen dat nieuwe personeelsleden zich bewust zijn van hun rechten en plichten met betrekking tot beveiliging (awareness);

- het beveiligingsbeleid te onderhouden;
- het controleren van de naleving van het beveiligingsbeleid, richtlijnen en procedures
- beveiligingsincidenten rapporteren;
- De uitvoering van correctieve werkzaamheden te controleren;
- Uitvoeren van reguliere interne controle;
- Uitvoeren van ad–hoc evaluaties van de informatiebeveiliging(smaatregelen);
- Evalueren van externe controles.

Beveiligingsbeheerder (Security administrators)

- de aangevraagde autorisaties implementeren binnen de informatiesystemen;
- implementeren van technische beveiligingsmaatregelen voor IT–resources in overeenstemming met het Informatie Beveiligingsbeleid, richtlijnen en procedures;
- de aangevraagde autorisaties onderhouden binnen de informatiesystemen;

(Externe) EDP Audit

(Externe) EDP auditors zullen, gebaseerd op hun eigen risicoinschatting, periodiek (veelal jaarlijks) een onafhankelijk onderzoek uitvoeren naar de beveiliging binnen het bedrijf en zullen de resultaten rechtstreeks rapporteren aan de directie.

2.5 Theorieën, formele modellen en best practices

Het vakgebied van de informatiebeveiliging wordt al enkele decennia bestudeerd en in die tijd zijn diverse publicaties verschenen die worden beschouwd als de basis theorieën van het vakgebied. In deze paragraaf zal ik enkele hiervan kort bespreken omdat deze enerzijds de lezer een uitstekende verdieping van de theorie van informatiebeveiliging bieden en anderzijds omdat later in dit onderzoek nog aan sommigen ervan wordt gerefereerd.

Eén zijde van de belangrijkste publicaties betreft de gepubliceerde theorieën en formele modellen die in de loop der tijd, met name vanuit academische hoek, zijn gepubliceerd. De belangrijkste hiervan zijn het beveiligingsmodel van Bell en LaPadula [BELL1973] voor militaire omgevingen en het hierop geïnspireerde beveiligingsmodel van Clark en Wilson [CLARK1987] voor commerciële omgevingen. Door Landwehr is in aanvulling hierop een mooi overzichtsartikel [LAND1981] gepubliceerd waarin nog enkele basale formele beveiligingsmodellen worden beschreven. Deze modellen zijn vooral gericht op toegangsbeveiliging, maar bieden in het algemeen een mooie aanzet tot formalisatie van informatiebeveiliging.

Een tweede zijde van de belangrijkste publicaties betreft de veelal vanuit de (bedrijfs)praktijk geschreven *best business practices*. Dit zijn publicaties waarin op basis van ervaring wordt beschreven hoe bepaalde aspecten van informatiebeveiliging het beste kunnen worden aangepakt. De bekendste hiervan is Britse 'Code of practice for information security management', ook wel bekende onder standaardnummer BS7799 [BSI1999]. Een Nederlandse versie hiervan is (inmiddels in een tweede versie) gepubliceerd als de 'Code voor Informatiebeveiliging' [NNI2000]. Dit stuk "biedt een uitgebreide verzameling maatregelen voor een goede implementatie ('best practices') van informatiebeveiliging". De Code voor Informatiebeveiliging is in de loop der jaren uitgegroeid tot een breed geaccepteerde basis die tegenwoordig ook wordt gehanteerd als ijkpunt voor formele certificatie onder toezicht van de Raad voor Accreditatie [ECP2003].

2.5 Conclusie

In dit hoofdstuk is aangegeven dat organisaties heden ten dage zeer intensief gebruik maken van informatietechnologie en veelal zelfs hun bedrijfsprocessen hierop aanpassen. De kwaliteit van de informatiesystemen en de daarin bevatte informatie —gebundeld in de informatie–voorziening— is daarom voor organisaties (in meer of mindere mate) van belang. Om de kwaliteit van de informatievoorziening te waarborgen is vereist dat organisaties informatiebe–veiliging onderdeel maken van hun bedrijfsvoering.

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket van richtlijnen, procedures en maatregelen ter waarborging van de betrouwbaarheid van de informatievoorziening. De betrouwbaarheid van de informatievoorziening bestaat uit de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid. Voorwaarde hiervoor is wel dat alle maatregelen die in het kader van informatiebeveiliging worden getroffen con–troleerbaar zijn. Hierbij gelden de kwaliteitsaspecten doeltreffendheid en doelmatigheid als randvoorwaarden voor de richtlijnen en maatregelen die ten behoeve van informatiebeveili–ging worden ingesteld.

Informatiebeveiliging vormt een cyclisch proces waarin vier fasen kunnen worden onderkend: inventariseren, ontwerpen, implementeren en beheersen. In de fase van het ontwerpen wordt het informatiebeveiligingsbeleid opgesteld. Ten behoeve van de uitvoering van het infor–matiebeveiligingsproces dient een informatiebeveiligingsorganisatie te worden ingericht. De minimaal daarin voorkomende functies zijn directie, lijnmanagement, informatie–eigenaren, security coordinator, security administrator en de (externe) controlefunctie.

Noten

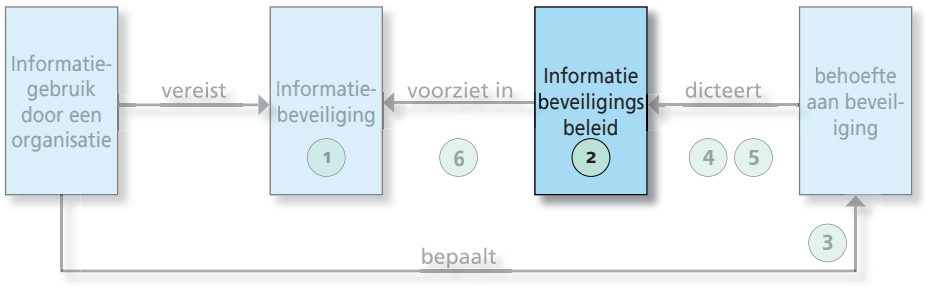
4 Stand–alone PC's zijn personal computers die niet verbonden zijn met een computernetwerk.

Informatie-beveiligingsbeleid

"Some people say information security is a people problem, while others say it is a technology problem. They are both right. But before anything can be done about information security, management must get involved. Therefore, information security is fundamentally a management problem. More specifically, the number one key to information security success is involvement of higher level management.

Information Security Policies made easy, Charles Cresson Wood [WOOD1994]

Hoofdstuk 2 heeft duidelijk gemaakt dat een structurele aanpak van informatiebeveiliging van groot belang is voor organisaties die waarde hechten aan de kwaliteit van hun informatie. Aangegeven is dat informatiebeveiliging bij zo'n structurele aanpak een cyclisch proces vormt. In de tweede fase van dit proces, de ontwerpfase, wordt het informatiebeveiligingsbeleid opgesteld. Aangezien informatiebeveiligingsbeleid de spil vormt waar dit onderzoek om draait is het nodig te bepalen wat verstaan wordt onder informatiebeveiligingsbeleid. Dit komt naar voren in de kernvraag van dit hoofdstuk:



Figuur 7: De kernvraag van dit hoofdstuk is uitgelicht in het schema

Kernvraag 2

> *Wat wordt verstaan onder informatiebeveiligingsbeleid, in hoeverre verschilt informatiebeveiligingsbeleid tussen organisaties en op welke mogelijkheden zijn er om informatiebeveiligingsbeleid te standaardiseren?*

Paragraaf 3.1 vangt de beantwoording van deze vraag aan met te beschrijven wat in de literatuur wordt verstaan onder beveiligingsbeleid. In 3.2 wordt aansluitend beschreven wat het belang is van beveiligingsbeleid voor een organisatie, waarna in 3.3 wordt ingegaan op de context van beveiligingsbeleid binnen een organisatie. Afrondend wordt in paragraaf 3.4 aangegeven welke onderwerpen in het beveiligingsbeleid dienen te worden beschreven ten einde het doel ervan te kunnen bereiken. In figuur 7 is uitgelicht wat de plaats is van dit hoofdtuk in het gehele onderzoek.

3.1. Wat is informatiebeveiligingsbeleid

Teneinde te komen tot een definitie van beveiligingsbeleid is het interessant in eerste instantie te inventariseren wat vanuit taalkundig oogpunt onder beveiligingsbeleid kan worden verstaan. Hiertoe beantwoord ik eerst de vraag wat beleid in het algemeen inhoudt. De 'dikke' Van Dale [DALE1999] omschrijft beleid als "het behandelen of wijze van behandelen van een zaak, bestuur m.betr.t. de gevolgde beginselen of gedraglijnen…". Simpeler gezegd gaat het bij beleid dus om een manier van handelen, betrekking hebbend op gedragslijnen (richt-

lijnen). Projecteren we deze definitie op informatiebeveiliging dan kan gezegd worden dat informatiebeveiligingsbeleid aangeeft hoe te handelen conform de richtlijnen voor informatiebeveiliging.

Het informatiebeveiligingsbeleid zal volgens de voorgaande taalkundige verklaring dus aangeven hoe om te gaan met beveiligingsrichtlijnen. Kijken we vervolgens naar de omschrijvingen van beveiligingsbeleid in de literatuur dan vinden we de volgende diversiteit aan beschrijvingen.

"Beveiligingsbeleid: het organisatiebeleid ter zake gegevensverwerking met al zijn elementen (apparatuur, programmatuur, gegevens)" [NGI1992]

"Doel van het beveiligingsbeleid is het bieden van richting en ondersteuning aan het management ten behoeve van informatiebeveiliging" [NGI1994]

"...Corporate Security Policy, which will specify the set of laws, rules and practices that regulate how assets are managed, protected and distributed within the organisation" [OECD2002]

"Het informatiebeveiligingsbeleid is een verzameling strategische uitgangspunten waarin het topmanagement [...] duidelijk maakt aan het tactisch en operationeel niveau welke gedragslijnen het [...] aanneemt om te komen tot een afgewogen stelsel van maatregelen." [HBR1995]

"Het beveiligingsbeleid is een essentieel instrument voor de aansturing en coördinatie van de verschillende beveiligingsprocessen binnen een organisatie. [...] Het beleid is derhalve primaire een communicatie instrument binnen de organisatie." [OVER2000]

"Het beveiligingsbeleid heeft tot doel om via een stelsel van maatregelen de gevolgen van inbreuken op de betrouwbaarheid van informatievoorziening te beheersen" [NGI1992]

De grote lijn die uit deze beschrijvingen kan worden gedestilleerd is dat informatiebeveiligingsbeleid de volgende eigenschappen heeft:

- bedrijfs- of organisatiebeleid;
- uitgedragen door het topmanagement;
- strategische doelstellingen, procedures en richtlijnen bevatten;
- gericht op de beveiliging van de gegevensverwerking (informatiebeveiliging)
- richting en ondersteuning gevend aan het lijnmanagement en bedrijfsprocessen;

- aanduidend hoe gereageerd dient te worden op inbreuken op de betrouwbaarheid van de informatievoorziening.

Dit alles evaluerend wordt in het vervolg van dit document onder informatiebeveiligingsbeleid het volgende verstaan:

Definitie:

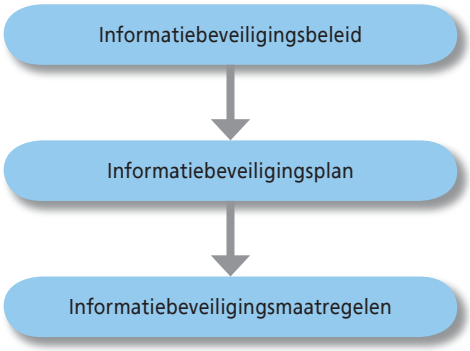
*Het **informatiebeveiligingsbeleid** is het organisatiebeleid dat –middels strategische doelstellingen, richtlijnen en procedures– richting en ondersteuning geeft aan informatiebeveiliging, teneinde de inbreuken op de betrouwbaarheid van de informatievoorziening zoveel mogelijk te voorkomen en de gevolgen van inbreuken te beheersen.*

In hoofdstuk 2 is reeds beschreven wat wordt verstaan onder betrouwbaarheid van de informatievoorziening.

3.2 De plaats van het beveiligingsbeleid binnen het informatiebeveiligingsproces

In het informatiebeveiligingsproces dat is beschreven in paragraaf 2.3, is het opstellen van het informatiebeveiligingsbeleid onderdeel van de 'definiëren' fase. In die fase wordt op basis van de in de voorgaande fase vastgestelde behoeften van de organisatie in het beveiligingsbeleid vastgelegd hoe informatiebeveiliging moet worden ingericht. Dit vormt de basis voor de uitvoering van informatiebeveiliging in de rest van het proces. In volgende cycli van het proces kan het beveiligingsbeleid eventueel worden bijgesteld op basis van eventueel gewijzigde behoeften.

Wanneer het beveiligingsbeleid is opgesteld wordt geïnventariseerd op welk niveau de beveiliging van de personen, computersystemen en processen die informatieverzorging voor hun rekening nemen zich bevindt. Vervolgens wordt op basis van die inventarisatie een beveiligingsplan opgesteld waarin wordt aangegeven wat er nog moet gebeuren om aan de door het beveiligingsbeleid gestelde richtlijnen te voldoen. Dit nog te verzetten werk wordt vervolgens vertaald in beveiligingsmaatregelen die ingericht dienen te worden om het vereiste niveau van informatiebeveiliging te bereiken. Dit traject is in essentie weergegeven in figuur 8.



Figuur 8: Sturing van informatiebeveiliging vanuit informatiebeveiligingsbeleid.

3.3 Het belang van informatiebeveiligingsbeleid

Alvorens deze het beveiligingsbeleid op te stellen is het belangrijk te bepalen waarom het opstellen ervan überhaupt zinvol is. Onderstaand worden daarom op basis van een literatuur–inventarisatie de belangen van beveiligingsbeleid uiteen gezet.

3.3.1 Vorm en richting geven aan de informatiebeveiliging

Het beveiligingsbeleid is een essentieel instrument voor de aansturing en coördinatie van het beveiligingsproces binnen een organisatie. [ROOS1998] Zonder de juiste sturing is het informatiebeveiligingsproces 'gebouwd op los zand'. Zoals [COU1998] aangeeft wordt vaak aandacht besteed "aan informatiebeveiliging na het optreden van een beveiligingsincident. Dan bestaat de neiging om de aandacht te richten op het incident en hiertegen ad–hoc maat–regelen te treffen." Uiteraard geldt bij incidenten dat eerst de hoogste nood geledigd moet worden, maar daarnaast moet worden gewerkt aan een structurele aanpak om te voorkomen dat een ongebalanceerde informatiebeveiliging ontstaat.

Zo denken veel organisaties bijvoorbeeld ten onrechte dat informatiebeveiliging afdoende verzorgd kan worden middels het aanschaffen van bepaalde beveiligingshard– en/of software. In de praktijk blijkt dat zelfs de beste soft– en/of hardware ten behoeve van informatiebe–veiliging nutteloos is wanneer er in de organisatie verder niets verandert. Het implementeren

van genoemde beveiligingstools behoort namelijk tot de operationele uitwerking van wat weldoordacht beleid dient te zijn. In [WOOD1994] wordt dit bevestigd. Wood schrijft hierin: "*Policies are the essence from which other elements of information security are derived.*"

Indien er geen centraal voorgeschreven beveiligingsbeleid is kunnen bijvoorbeeld verschillende activiteiten in het kader van informatiebeveiliging in tegenspraak met elkaar zijn. Of kan bijvoorbeeld het werk van één afdeling teniet worden gedaan door een andere afdeling die in het geheel geen aandacht besteed aan informatiebeveiliging. Een ketting is immers zo sterk als de zwakste schakel. Doordat beveiligingsbeleid een consistente aanpak bij het implementeren van beveiligingsmaatregelen bevordert, helpt het te voorzien in een adequaat en geschikt beveiligingsniveau om gevoelige en kritische informatie te beveiligen tegen ongeautoriseerde toegang en manipulatie.

3.3.2 Betrokkenheid van het management verkrijgen en betuigen

Informatiebeveiliging wordt door sommigen bestempeld als een technisch probleem en door anderen als een menselijk probleem [WOOD1994]. Beide stellingen zijn correct. Maar voordat op het technische of menselijke vlak iets aan informatiebeveiliging kan worden gedaan dient er betrokkenheid te zijn van het management. Steun van het hogere management is nodig om voldoende budget voor informatiebeveiliging te verkrijgen, het belang van informatiebeveiliging duidelijk te maken en beveiligingsmaatregelen in te stellen. Dit betekent dat managementtoeweiding een primaire voorwaarde is voor het slagen van informatiebeveiliging. Anders kan bij medewerkers gemakkelijk het idee ontstaan "als het management zich er niet druk om maakt, waarom zou ik het dan doen?"

In dit kader snijdt het mes van beveiligingsbeleid aan twee kanten. Aan de ene kant is het beveiligingsbeleid een ideaal startpunt om het management te betrekken bij informatiebeveiliging. Het beveiligingsbeleid is vaak zelfs de eerste keer dat het management met informatiebeveiliging wordt geconfronteerd [WOOD1994]. Middels het opzetten van beveiligingsbeleid is het management direct betrokken en tevens medeverantwoordelijk. Aan de andere kan toont het beveiligingsbeleid meteen de betrokkenheid van het management bij de informatiebeveiliging omdat het beveiligingsbeleid door het management zelf wordt uitge-

vaardigd. Het management spreekt zich persoonlijk uit over de manier waarop de organisatie met informatiebeveiliging om dient te gaan en dat het daaraan belang hecht en dit in de toekomst zal blijven doen.

3.3.3 Basis voor disciplinaire acties

Dit belang wordt in [WOOD1994] slechts kort genoemd, maar dient in de praktijk een groot belang. Zonder beleid is namelijk niet formeel beschreven wat wel en niet is toegestaan met betrekking tot de in de organisatie aanwezige informatiesystemen. Zonder beveiligingsbeleid is het derhalve ook niet helder wanneer betrokkenen op hun handelen kunnen worden aangesproken. Middels het beveiligingsbeleid wordt duidelijk aangegeven wat wel en niet mag. Daarmee is een maatstaf beschikbaar aan de hand waarvan het handelen van betrokken partijen kan worden beoordeeld en indien nodig een kapstok om disciplinaire acties aan op te hangen. In dit kader kan nog worden onderstreept dat het beveiligingsbeleid niet vrijblijvend is. Niet naleven van de richtlijnen dient dan ook niet zonder gevolgen te blijven. Idealiter dien het meegenomen te worden in beoordelingen.

3.3.4 Veranderen van de houding ten opzichte van informatiebeveiliging

In [WOOD1994] wordt een aantal belangen genoemd die allen betrekking hebben op het ten positieve veranderen van de houding ten opzichte van informatiebeveiliging. Dit overlapt enigszins met de eerdergenoemde behoefte aan managementondersteuning, maar is specifiek genoeg om hier nogmaals aan te stippen.

Over het algemeen heerst in organisaties een huiverige houding ten opzichte van automatisering. Wanneer informatiebeveiliging wordt uitgelicht blijkt dat dit vaak als belemmerend wordt gezien en daardoor met nog meer scepsis wordt benaderd. Door in het beveiligingsbeleid aan te geven wat het belang van informatie is voor de organisatie en welke risico's de organisatie loopt in het gebruik ervan. Daarmee kan een draagvlak worden gecreëerd voor de te stellen richtlijnen en te implementeren maatregelen. Daarbij komt dat het überhaupt opstellen van het beveiligingsbeleid, zoals beschreven in 3.2.2, helpt draagvlak te creëren.

3.3.5 Stellen van verantwoordelijkheden

Zoals in [ROOS1998] plastisch wordt beschreven, wordt informatiebeveiliging “gezien als een hete aardappel die zo snel mogelijk op het bordje van een ander geschoven dient te worden”. Het duidelijk stellen van taken, verantwoordelijkheden en bevoegdheden is daarom van het grootste belang. Dit dient derhalve opgenomen te worden in het informatiebeveiligingsbeleid.

3.3.6 Het uitsluiten van hoofdelijke aansprakelijkheid

In [WOOD1994] wordt beschreven hoe personen en dan vooral die uit het hogere management steeds vaker hoofdelijk aansprakelijk worden gesteld voor de kwalijke gevolgen van inbreuken op de betrouwbaarheid van de informatievoorziening. Hierbij wordt gesteld dat alleen al het opstellen van informatiebeveiligingsbeleid juridisch een voldoende signaal is dat het management het onderwerp informatiebeveiliging serieus heeft genomen en getracht heeft problemen te voorkomen. De Amerikaanse juridische situatie is zoals bekend wat spectaculairder dan de Europese, het argument houdt echter ook hier een kern van waarheid in zich.

3.3.7 Voldoen aan wettelijke, maatschappelijke en commerciële eisen

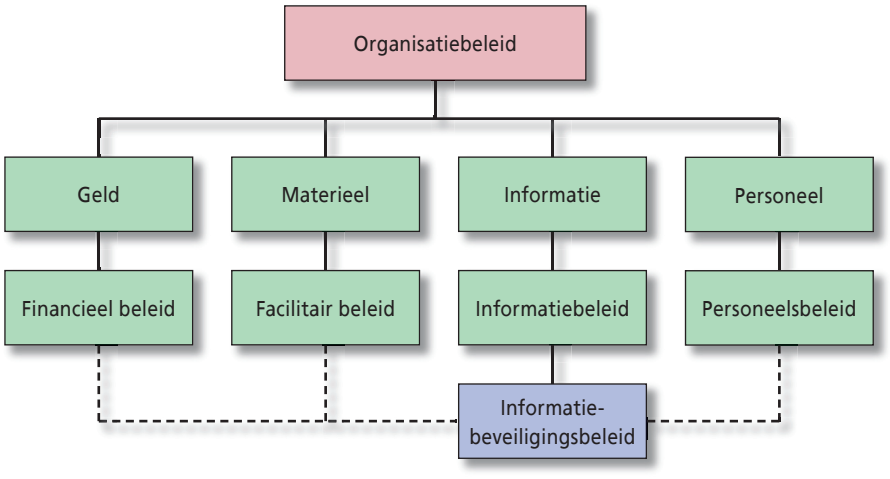
Het informatiebeveiligingsbeleid is een middel om te laten zien dat een organisatie voldoet aan de eisen die worden gesteld door diverse partijen in het maatschappelijk verkeer. Zo worden impliciet of expliciet eisen gesteld door aandeelhouders, fusiepartners, een brancheverenigingen, een beroepsorganisatie of toezichthouders [ROOS1998]. Zo stelt de wet expliciet eisen aan de beveiliging van informatiesysteem, zoals in de Wet Bescherming Persoonsgegevens [BEA2001] en de wet computercriminaliteit [BEA1993]. Daarnaast zijn rijksoverheden bijvoorbeeld vereist een beveiligingsbeleid op te stellen, zoals aangegeven in het voorschrift informatiebeveiliging rijksoverheid. [BIZA1994] Verder gelden voor Amerikaanse beursgenoteerde bedrijven na enkele grote boekhoudschandalen strenge eisen met betrekking tot interne beheersing, welke ook betrekking hebben op informatiebeveiliging en het daaraan ten grondslag liggende beleid [STUL2004].

3.4 De context van informatiebeveiligingsbeleid

Informatiebeveiliging kan geen geïsoleerde activiteit zijn. Het heeft relaties met vele werk-gebieden binnen organisaties. Dat betekent dat het beveiligingsbeleid ook relaties kent met andere beleidsgebieden. In deze paragraaf komt aan de orde welke relaties dit zijn en wat de reikwijdte is van het beveiligingsbeleid.

3.4.1 Relatie met andere beleidsgebieden

Het informatiebeveiligingsbeleid staat niet op zichzelf. Uiteraard heeft het om te beginnen een directe relatie met het informatiebeleid (de vierde productiefactor). Maar informatiebeveiliging is geen geïsoleerd proces en heeft derhalve ook gevolgen voor andere beleidsgebieden, te weten personeelsbeleid, financieel beleid en productiebeleid (de klassieke drie productiefactoren). [OVER2000] Dit betekent dat het beveiligingsbeleid en de overige beleidsgebieden elkaar beïnvloeden. Zo hebben bijvoorbeeld beveiligingseisen met betrekking tot personeel een directe relatie met het personeelsbeleid. Analoog heeft het facilitair beleid een relatie met het beveiligingsbeleid wanneer het bijvoorbeeld gaat om fysieke beveiliging. In figuur 9 zijn de relaties van beveiligingsbeleid met de andere beleidsgebieden grafisch weergegeven.



Figuur 9: De relatie van informatiebeveiligingsbeleid met andere beleidsgebieden

3.4.2 Reikwijdte van het informatiebeveiligingsbeleid

In de definitie van beveiligingsbeleid is aangegeven dat beveiligingbeleid bestaat uit richtlijnen. Tevens is aangegeven dat deze richtlijnen worden uitgewerkt in maatregelen. Het is belangrijk te bepalen waar richtlijnen ophouden en waar maatregelen beginnen. Dit onderscheid is niet met een scherpe snede te maken en kan in verschillende praktijksituaties anders worden gelegd. Feit is wel dat richtlijnen in het beleid algemeen geldend moeten zijn en richting en sturing bieden aan de implementatie van informatiebeveiliging. Maatregelen zijn over het algemeen praktischer en bijvoorbeeld gericht kunnen zijn op specifieke systemen of werkwijzen.

Het grensgebied tussen richtlijnen en maatregelen is een geleidelijke overgang. Om de grens tussen richtlijnen en maatregelen toch zo helder mogelijk te maken kan het onderscheid worden gezien als het onderscheid tussen het 'wat' en het 'hoe'. Richtlijnen zijn gericht op het wat moet worden beveiligd of wat het vereist niveau van beveiliging is. Maatregelen zijn gericht op hoe de beveiliging zo in te richten dat aan de gesteld richtlijnen te voldoen. Ter verder verduidelijking het volgende voorbeeld:

Richtlijn: *"Alleen geautoriseerde personen mogen de gebouwen van de organisatie betreden."*

Maatregel: *"Alle personeelsleden dienen gebruik te maken van toeganspasjes om de gebouwen van de organisatie te betreden."*

3.4.3 Invloedssfeer van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is in principe altijd geldig voor een gehele organisatie en alle informatiesystemen (apparatuur, programmatuur, gegevens, procedures en mensen). In voorkomende gevallen zal het beter passen om beveiligingsbeleid per bedrijfsonderdeel (bijvoorbeeld per werkmaatschappij) op te stellen. In die gevallen dient ten behoeve van eenheid in beleid en uitvoering toch centraal een beleidskader te worden opgesteld. [BRUI2000] Daarbij zal moet worden bepaald welke richtlijnen voor de gehele organisatie gelden en welke richtlijnen in het beleid van de afzonderlijke bedrijfsonderdelen moeten worden opgenomen.

Het opstellen van beleid voor de bedrijfsonderdelen kan worden gezien als het opstellen van het beveiligingsbeleid van een afzonderlijke organisatie, waarbij het centrale beleidskader een aanvullende invloedsfactor of randvoorwaarde vormt. Binnen dit onderzoek zal dit daarom niet als afzonderlijke situatie worden behandeld.

3.5 Onderdelen van het informatie-beveiligingsbeleid

In de artikelen en boeken die over beveiligingsbeleid zijn verschenen wordt in ruime mate aandacht besteed aan de verschillende onderwerpen die aan de orde dienen te komen. ([COUM1998], [ROOS1998], [BRUI2000], [BIZA1994], [NGI1992], [NNI2000]) Teneinde een volledig beeld te kunnen vormen van de onderwerpen die in beveiligingsbeleid kunnen of moeten worden opgenomen heb ik een inventarisatie gemaakt. Een methode voor het opstel–len van beveiligingsbeleid dient immers een volledig overzicht van mogelijke onderwerpen te bieden om te kunnen gebruiken als bouwstenen.

Uit de beschikbare literatuur komen de volgende mogelijke onderwerpen en onderdelen van beveiligingsbeleid naar voren.

- De doelstelling van informatiebeveiliging
- De doelstelling van het informatiebeveiligingsbeleid;
- De reikwijdte van het beveiligingsbeleid;
- De globale visie op informatiebeveiliging;
- Een expliciete verklaring van het (top)management waaruit hun betrokkenheid blijkt;
- Een beschrijving van (het belang van) de informatiesystemen binnen de organisatie;
- De uitgangspunten en randvoorwaarden van de informatiebeveiliging (geadopteerde standaarden, relevante wetgeving en dergelijke);
- De organisatie van de informatiebeveiliging;
- Voorschriften voor de classificatie van informatiesystemen;
- De wijze van toetsing en evaluatie van de informatiebeveiliging en het beleid;
- De melding en afhandeling van incidenten;
- Bewustwording /bewustmaking;
- Financiering
- Indeling in informatiesystemen en verantwoordelijkheidsgebieden;
- De eisen (richtlijnen) die gesteld worden aan de informatiebeveiliging.

In paragraaf 3.5 zal in aanvulling op deze theorie worden beoordeeld welke onderdelen voorkomen in praktijkvoorbeelden van informatiebeveiligingsbeleid.

3.6 Voorbeelden van beveiligingsbeleid vergeleken

Teneinde inzicht te verkrijgen in de mate waarin beveiligingsbeleid verschilt tussen organisaties en wat de redenen voor deze verschillen zijn, is het nuttig om allereerst een aantal in de praktijk gebruikte voorbeelden van informatiebeveiligingsbeleid te vergelijken. Voor dit onderzoek was een aantal praktijkvoorbeelden voorhanden, behorende bij de volgende organisaties:

- een zeer grote Nederlandse bank;
- een kleine Nederlandse bank;
- een grote Nederlande administratieve overheidsorganisatie;
- een Amerikaanse hotelketen;
- een middelgrote data- en telecomleveranciers;
- een middelgrote Nederlandse gemeente;
- een grote Nederlandse detailhandelsorganisatie;
- Een grote Nederlandse uitgeverij.

Deze voorbeelden zullen in dit onderzoek als 'trainingsset' worden gebruikt. Het uitgangspunt is daarbij dat de exemplaren van beveiligingsbeleid in de trainingsset adequaat zijn. Deze zijn immers in de praktijk in gebruik en aangenomen mag worden dat deze naar behoren werken, anders zouden ze wel worden aangepast. In bijlage A is een gedetailleerde uitwerking van deze vergelijking te vinden. In dit hoofdstuk wordt volstaan met de voor dit onderzoek belangrijkste conclusies.

Uit de vergelijking van de voorbeelden van informatiebeveiligingsbeleid blijkt dat de voorbeelden op hoofdlijnen overeenkomen. Blijkbaar verstaan bedrijven onder beveiligingsbeleid hetzelfde. De insteek van het beveiligingsbeleid (doel, niveau, plaats binnen de organisatie) sluit aan bij de theoretisch inzichten daaromtrent. Verder sluiten de voorbeelden voor wat betreft de voorkomende onderdelen redelijk tot goed aan bij de theorie. Behalve de doelstelling van informatiebeveiliging, de managementverklaring en de financiering komen alle beschreven onderdelen is de meeste exemplaren voor.

In essentie bestaan alle voorbeelden uit een prozaïsche beschrijving van de algemene setting en een verzameling beveiligingsrichtlijnen. Het algemene beeld is dat elke organisatie via het beleid richtlijnen stelt voor de informatiebeveiliging, toegelicht en ingebed in begeleidende en toelichtende teksten. Hoe 'stringent' de richtlijnen zijn verschilt per organisatie.

De invulling van deze twee elementen verschilt tussen de onderzochte exemplaren. De detaillering en mate van toelichting van de algemene setting varieert. Tevens verschillen de exemplaren in de hoeveelheid en mate van stringentie van de beveiligingsrichtlijnen; het ene voorbeeld bevat strengere richtlijnen dan het andere. Hierin komt het verschil in aansturing van de informatiebeveiliging naar voren. De ene organisatie stelt hogere eisen aan de informatiebeveiliging dan de andere en neemt in z'n beveiligingsbeleid dus andere (strengere) beveiligingsrichtlijnen op.

Wat opvalt aan de theoretische en praktische onderdelen, is dat de in theorie beschreven onderwerpen soms wat arbitrair zijn omdat ze net als veel andere onderwerpen onderdeel zijn van de richtlijnen. Het is de vraag wat rechtvaardigt dat onderwerpen apart worden vermeld, in plaats als deel van de richtlijnen. Waarom zou bijvoorbeeld de afhandeling van incidenten een apart onderwerp moeten zijn terwijl fysieke beveiliging niet expliciet wordt genoemd en gewoon onder de richtlijnen valt. Mijns inziens kunnen de onderdelen die gericht zijn op de werkelijke uitvoering van informatiebeveiliging het beste als richtlijnen worden opgenomen.

Verder valt op dat in alle onderzochte voorbeelden richtlijnen voor komen die op basis van het in paragraaf 3.4.2 gestelde onderscheid tussen richtlijnen en maatregelen eerder als maatregelen moeten worden aangemerkt. Bijvoorbeeld "na drie maal aanloggen met foutief wachtwoord dient een userid geblokkeerd te worden". Blijkbaar wordt bij het opstellen van beveiligingsbeleid niet altijd het zuivere standpunt gevolgd dat het beleid alleen richtlijnen op hoog niveau moet bevatten. Uit de onderzochte voorbeelden blijkt echter niet of dit een bewuste afwijking van de theorie is of niet. Bij het ontwikkelen van de verdere theorie zal dit aspect nog nader worden geëvalueerd.

In hoofdstuk zeven zal ik op basis van de theorie en de uitkomsten van de vergelijking van de praktijkvoorbeelden een aanzet doen voor een invulling van informatiebeveiligingsbeleid.

3.7 Balans tussen maatwerk en confectie

Wanneer gezocht wordt naar manieren om beveiligingsbeleid te standaardiseren, dan liggen deze ten eerste in het standaardiseren van de begeleidende teksten. Gezien de gevoelsmatige relatie tussen het belang van de informatievoorziening voor een organisatie en de inhoud van de beveiligingsrichtlijnen ligt het voor de hand dat daartussen een relatie bestaat. Indien die relatie inzichtelijk kan worden gemaakt, dan kan op basis daarvan worden getracht het opstellen van beveiligingsbeleid efficiënter en effectiever te laten verlopen. In het vervolg van dit onderzoek zal worden onderzocht welke relatie dit is en welke factoren daarbij bepalend zijn voor de invulling van de beveiligingsrichtlijnen.

Voordat onderzocht kan worden welke relatie bestaat tussen organisaties en hun beveiligingsbeleid om zodoende het opstellen te standaardiseren, dient eerst kritisch te worden geëvalueerd in hoeverre standaardisatie haalbaar is. Deze methode dient te zorgen dat het opstellen van beveiligingsbeleid zo efficiënt en effectief mogelijk verloopt.

Zoals in het inleidende hoofdstuk reeds kort is aangegeven dient, om dit te bereiken, getracht te worden beveiligingsbeleid te standaardiseren. Hierbij moet echter worden voorkomen dat een onvoldoende op een organisatie toegespitst, te algemeen stuk wordt gecreëerd. Daarom moet gezocht worden naar een balans tussen maatwerk en confectie. Dit is een evenwicht tussen enerzijds het gebruik van standaard teksten en anderzijds het telkens opnieuw volledig op maat schrijven van beveiligingsbeleid voor elke organisatie. Een dergelijk evenwicht kan ervoor zorgen dat het opstellen van beveiligingsbeleid zowel een optimale tijdsbesteding kent (efficiëntie), als een goed eindresultaat, afgestemd op een betreffende organisatie (effectiviteit).

Edo Roos Lindgreen raakt in [ROOS98] kort aan het mogelijke evenwicht tussen maatwerk en confectie. In een paragraaf die hij 'confectie op maat' geeft Roos Lindgreen aan dat er twee kampen zijn, namelijk de aanhangers van volledig maatwerk en de aanhangers van volledig confectie. In eerste instantie schetst hij alleen deze uiterste standpunten en stelt hij dat deze visies niet te verenigen zouden zijn. Hij schrijft hierover het volgende:

"Sommige deskundigen zijn van mening dat het intelligent gebruik van checklists als de Code voor informatiebeveiliging de toepassing van risicoanalyses geheel overbodig zal maken. Het is de vraag of het zo'n vaart zal lopen. Aan het gebruik van checklists kleeft een aantal bezwaren, waarvan de belangrijkste is samen te vatten onder de noemer '*one size does not fit all*'. De beveiligingsbehoeften van verschillende organisaties vertonenen onderling vaak

minder gelijkenis dan met op grond van andere overeenkomsten zou verwachten. Zelfs binnen één branche kunnen de bedrijfsprocessen van verschillende organisaties sterk uiteenlopen. Hetzelfde geldt voor de risico's die samenhangen met de automatisering van deze processen. Tenslotte is de toepasbaarheid van specifieke maatregelen mede afhankelijk van de omvang, de externe omgeving en de bedrijfscultuur van een organisatie. Zo kunnen maatregelen die zijn gebaseerd op verregaande controletechnische functiescheiding, niet worden gerealiseerd in kleine of onderbemande organisaties."

Aanvullende op dit sterke 'nee!' versoepelt hij zijn standpunt toch nog en laat hij ruimte voor een eventuele combinatie van maatwerk en confectie. "Ook bij intelligent gebruik van checklists moet altijd zorgvuldig worden afgewogen welke maatregelen wel en welke niet moeten worden getroffen, afhankelijk van het belang voor het te beschermen informatiesysteem voor de organisatie en de dreigingen waaraan dit systeem is blootgesteld. Een dergelijke afweging impliceert het uitvoeren van een risico–analyse. Het gebruik van checklists is daarom noodzakelijk maar niet voldoende; informatiebeveiliging is en blijft maatwerk, waarbij checklists buitengewoon nuttig kunnen zijn."

In deze laatste quote maakt Roos Lindgreen de stap naar specifieke informatiesystemen waar beveiligingsbeleid juist over een organisatie als geheel gaat. Maar aangezien beveiligingsbeleid overkoepeldend is voor alle informatiesystemen, geeft hij hier een nuttige aanwijzing voor dit onderzoek. Het punt dat hij maakt is namelijk dat moet worden afgewogen welke maatregelen (bij beleid betrekken we dit op richtlijnen) moeten worden getroffen, afhankelijk van het belang van een informatiesysteem en de bedreigingen waaraan het blootstaat. Wanneer ik dit projecteer op de informatievoorziening en het daar beveiligingsbeleid, dan hangen de te stellen richtlijnen samen met de mate waarin een organisatie afhankelijk is van haar informatiesystemen en de bedreigingen waaraan deze systemen bloot staan.

3.8 Conclusie

In dit hoofdstuk is gedefinieerd wat onder beveiligingsbeleid wordt verstaan. Daarbij is aangegeven dat het beveiligingsbeleid het organisatiebrede beleid is dat, middels strategische richtlijnen en procedures, sturing geeft aan de uitvoering van de informatiebeveiliging teneinde inbreuken op de betrouwbaarheid van de informatievoorziening te voorkomen en de gevolgen van inbreuken te beheersen.

Het beveiligingsbeleid is essentieel voor een goede werking van het informatiebeveiligings–proces. Daarbij dient het onder andere de volgende belangen:

- Vorm en richting geven aan de informatiebeveiliging;
- Betrokkenheid van het management verkrijgen en betuigen;
- Stellen van verantwoordelijkheden binnen de informatiebeveiliging;
- Vormen van een basis voor disciplinaire acties;
- Veranderen van de houding ten opzichte van informatiebeveiliging;
- Voldoen aan wettelijke, maatschappelijke en commerciële eisen.

Het beveiligingbeleid heeft een onderschikkende samenhang met het informatiebeleid (soms aangeduid als de vierde productiefactor). Daarnaast heeft het een wederzijdse invloed op het facilitair beleid, het personeelsbeleid en het financieel beleid (in essentie gericht op de drie productiefactoren grondstoffen, arbeid en kapitaal).

Op basis van literatuur en diverse voorbeelden van beveiligingsbeleid is geïnventariseerd uit welke onderdelen beveiligingsbeleid bestaat. Naar aanleiding daarvan is vastgesteld dat beveiligingsbeleid van verschillende organisaties globale overeenkomsten vertoont in vorm, reikwijdte en structuur. Beveiligingsbeleid verschilt tussen organisaties in de hoeveelheid beveiligingsrichtlijnen en de mate waarin deze stringent zijn.

De onderzochte voorbeelden suggereren dat een relatie bestaat tussen de hoeveelheid en stringentheid van de richtlijnen en het ‘karakter’ van een organisatie. Standaardisatie van het beveiligingsbeleid kan op basis van zo’n relatie worden gestandaardiseerd. Daarbij dient een balans te worden gevonden tussen maatwerk en confectie, teneinde het opstellen beveili–gingsbeleid efficiënt en effectief te laten verlopen, maar waarbij het beleid wel voldoende is afgestemd op de behoeften van een organisatie. Deze balans kan worden bereikt door het beveiligingsbeleid af te stemmen op de mate waarin een organisatie afhankelijk is van de informatievoorziening en de bedreigingen waaraan deze blootstaat. In het vervolg van dit onderzoek zal deze afhankelijkheid nader worden onderzocht, waarbij wordt uitgediept welke factoren bepalend zijn voor de invulling van het beveiligingsbeleid.

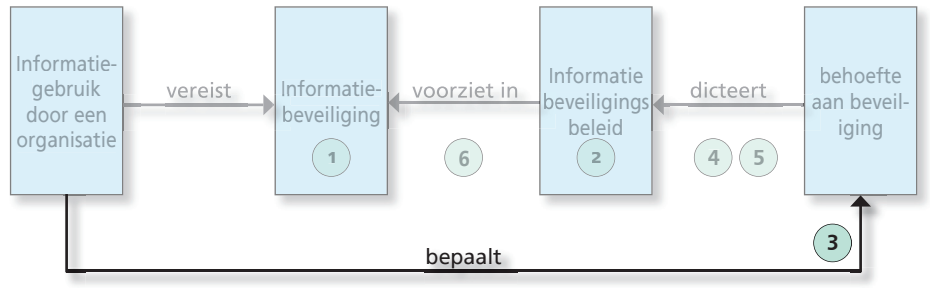
Betrouwbaarheids-behoefte

4

"De wijze waarop met bedreigingen wordt omgegaan zal van organisatie tot organisatie verschillen. Deze stelling gaat ook op indien organisaties eenzelfde typologie hebben. Verschillen ontstaan onder andere door verschillen in attitude van het management en de verschillen in cultuur tussen organisaties, die vaak historisch bepaald zijn. Bij het bepalen van de wijze waarop een organisatie zich tegen kwetsbaarheden teweer stelt, dient met deze beide facetten rekening te houden."

NGI uitgave 'Beveiligingsbeleid en beveiligingsplan' [NGI1992]

In hoofdstuk 3 is beschreven dat het opstellen van informatiebeveiligingsbeleid mogelijkheden biedt tot standaardisatie. Aangegeven is dat deze mogelijkheden liggen in het gebruik van standaard teksten en een systematische keuze van beveiligingsrichtlijnen. Om beveiligingsbeleid op te kunnen stellen op basis van dergelijke standaard elementen, is het nodig te bepalen wanneer welke elementen van toepassing zijn voor (en dus onderdeel moeten zijn van) het beveiligingsbeleid van een organisatie en welke factoren daarin bepalend zijn. In dit licht luidt de deelvraag die in dit hoofdstuk zal worden beantwoord als volgt:



Figuur 10: De kernvraag van dit hoofdstuk is uitgelicht in het schema

Kernvraag 3

> *Welke factoren zijn bepalend voor de inhoud van het informatiebeveiligingsbeleid en wat is de invloed van deze factoren?*

Allereerst wordt in paragraaf 4.1 beschreven dat het beveiligingsbeleid is gerelateerd aan de behoefte aan betrouwbaarheid van de informatievoorziening. Aansluitend wordt in 4.2 beschreven dat de betrouwbaarheid twee dimensies heeft, te weten afhankelijkheid en kwetsbaarheid, en wat de relatie van deze dimensies is met het beveiligingsbeleid. In 4.3 wordt uitgewerkt wat de relatie tussen de behoefte aan betrouwbaarheid en het beveiligingsbeleid inhoudelijk betekent. In 4.4 wordt tot slot ingegaan op de mogelijkheden om de behoefte aan betrouwbaarheid te bepalen aan de hand van 'oppervlakkige' organisatie–eigenschappen.

4.1 Behoefte aan betrouwbaarheid

Zoals aangegeven in de in hoofdstuk 2 gekozen definitie heeft het beveiligingsbeleid tot doel richting en ondersteuning te geven aan de informatiebeveiliging. En informatiebeveiliging heeft tot doel de betrouwbaarheid van informatievoorziening te waarborgen. Daarmee heeft informatiebeveiliging dus tot doel richting en ondersteuning te geven aan de waarborging van de betrouwbaarheid van de informatievoorziening.

Om te komen tot evenwichtige informatiebeveiliging dient deze richting aan te sluiten bij de behoefte van een organisatie om de betrouwbaarheid te waarborgen. Een organisatie zal immers altijd streven naar een inrichting van de informatiebeveiliging (die geld kost) die

voldoende bescherming biedt, maar niet onevenredig veel kost. Derhalve zal informatiebeveiligingsbeleid aan moet sluiten bij de behoefte aan (waarborging van) de betrouwbaarheid van de informatievoorziening.

In paragraaf 2.4 is beschreven hoe informatiebeveiligingsbeleid in de kern gericht is op de bescherming van de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid, die samen de betrouwbaarheid vormen. De behoefte aan betrouwbaarheid waar het beveiligingsbeleid bij aan dient te sluiten is analoog daaraan opgebouwd uit de behoefte aan beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening. Bij de verder beschrijving zal ik de term 'betrouwbaarheidsbehoefte' hanteren voor deze factor van invloed op het beveiligingsbeleid.

Definitie:

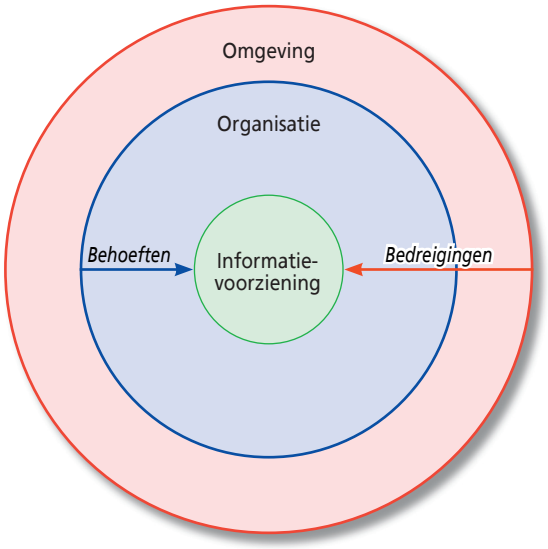
> *De **betrouwbaarheidsbehoefte** van een organisatie is de mate waarin een organisatie zich moet kunnen verlaten op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening en derhalve behoefte heeft aan bescherming van deze aspecten.*

Weten dat het beveiligingsbeleid afhangt van de betrouwbaarheidsbehoefte zegt echteronvoldoende, zolang niet duidelijk is wat deze betrouwbaarheidsbehoefte concreet inhoudt. In de volgende paragraaf wordt dit verder uitgewerkt.

4.2 Afhankelijkheid en kwetsbaarheid van de informatievoorziening

De betrouwbaarheid van de informatievoorziening kent voor organisaties twee invalshoeken. Enerzijds wordt de betrouwbaarheid van de informatievoorziening beïnvloed door de behoeften van de organisatie. Deze behoeften hebben betrekking op de eisen die een organisatie stelt aan de kwaliteit van de informatievoorziening op basis van de mate waarin de organisatie hiervan afhankelijk is. Hoe hoger de eisen van de organisatie aan de informatievoorziening, hoe beter de betrouwbaarheid moet worden gewaarborgd.

Anderzijds wordt de betrouwbaarheid van de informatievoorziening beïnvloed door bedreigingen, zowel vanuit de omgeving van de organisatie als vanuit de organisatie zelf. Deze



Figuur 11: De informatievoorziening wordt beïnvloedt door behoeften vanuit de organisatie (afhankelijkheid) en door de bedreigingen waaraan het bloot staat (kwetsbaarheid)

bedreigingen zijn van invloed op de mate waarin de betrouwbaarheid van de informatievoorziening kan worden aangetast. Bedreigingen kunnen ertoe leiden dat betrouwbaarheid van de informatievoorziening kwetsbaar is.

Deze twee invalshoeken worden in de theorie van informatiebeveiliging aangeduid als respectievelijk de afhankelijkheid en de kwetsbaarheid van de betrouwbaarheid van de informatievoorziening. In figuur 11 is schematisch het verschil weergegeven tussen deze invloedsfactoren. Beiden worden hierna formeel gedefinieerd op basis van Overbeek [OVER2000] en nader toegelicht.

Definitie:

> *De **afhankelijkheid van de informatievoorziening** is de mate waarin een organisatie afhankelijk is van de betrouwbaarheid van de informatievoorziening.*

De afhankelijkheid geeft aan hoe belangrijk de betrouwbaarheid van de informatievoorziening voor een organisatie is. Daarmee is de afhankelijkheid het uitgangspunt van de informatiebeveiliging en definieert het de beveiligingsdoelstellingen; op welke niveau dient de informatiebeveiliging te worden ingericht. In de accountingtheorie wordt dit ook wel aangeduid als de *soll*–positie. De afhankelijkheid van de informatievoorziening geeft daarmee

in essentie aan **in welke mate** de betrouwbaarheid moet worden beveiligd. De afhankelijkheid is een indicatie voor de mate waarin aantasting van de betrouwbaarheid van de informatievoorziening negatieve impact heeft op de bedrijfsvoering van een organisatie.

Definitie:

> *De **kwetsbaarheid van de informatievoorziening** is de mate waarin de informatievoorziening gevoelig is voor bedreigingen van de betrouwbaarheid van de informatievoorziening.*

De kwetsbaarheid is een indicatie van de bedreigingen die relevant zijn voor een organisatie en hoe kwetsbaar de organisatie is voor deze bedreigingen. De kwetsbaarheid heeft betrekking op de huidige staat, accountants noemen dit ook wel de *ist*–positie. De kwetsbaarheid van de informatiebeveiliging indiceert daarmee **op welke wijze** te handelen om te voldoen aan de beveiligingseisen die door de afhankelijkheid worden gedicteerd.

Het informatiebeveiligingsbeleid sluit direct aan bij de afhankelijkheid, omdat het de uitgangspositie van de informatiebeveiliging beschrijft. De kwetsbaarheid heeft geen directe invloed op het beveiligingsbeleid, omdat de kwetsbaarheid bepaald wordt door de wijze waarop de informatiebeveiliging werkelijk is ingericht, terwijl het beveiligingsbeleid beschrijft hoe de informatiebeveiliging ingericht zou moeten zijn. Kwetsbaarheid heeft wel een relatie met het informatiebeveiligingsplan (zie figuur 8 in paragraaf 3.2). Het informatiebeveiligingsplan is namelijk gericht op het treffen van maatregelen die de informatiebeveiliging van de *ist* naar de *soll*–positie brengen.

Hiermee is aangegeven dat de eerder gedefinieerde betrouwbaarheidsbehoefte in de kern staat voor de mate waarin een organisatie afhankelijkheid is van de informatievoorziening. De invulling van het informatiebeveiligingsbeleid wordt dus in de kern bepaald door de afhankelijkheid van de informatievoorziening. Op basis hiervan kan worden onderzocht wat de relatie is tussen de afhankelijkheid en het beveiligingsbeleid, hetgeen het onderwerp is van de volgende paragraaf.

Om verwarring te voorkomen met afhankelijkheid in de reguliere context van individuele informatiesystemen te voorkomen zal verder worden gesproken over 'betrouwbaarheidsbehoefte'. Deze term geeft beter aan dat het een eigenschap op hoger niveau betreft die de afhankelijkheid van de informatievoorziening voor een organisatie als geheel aanduidt.

4.3 De invloed van de betrouwbaarheids-behoefte op het beveiligingsbeleid

De invulling van het informatiebeveiligingsbeleid wordt primair bepaald door de afhankelijkheid van de informatievoorziening, breder aangeduid als de betrouwbaarheidsbehoefte. Maar wat houdt nu dat 'bepalen van de invulling' in. In hoofdstuk drie is al aangegeven dat het beveiligingsbeleid de uitgangspunten van de informatiebeveiliging schetst middels beveiligingsrichtlijnen, ingebed in prozaïsche beschrijvingen. De invloed van de afhankelijkheid zal dan ook moeten uitwerken op deze beveiligingsrichtlijnen en prozaïsche beschrijvingen.

De kern van de relatie is dat de betrouwbaarheidsbehoefte samenhangt met de stringentheid van het beveiligingsbeleid. Hoe groter de behoefte aan betrouwbaarheid van de informatievoorziening, hoe stringenter de richtlijnen die het beveiligingsbeleid moet stellen. Stringenter wil hierbij zeggen dat het beleid hogere eisen stelt aan de informatiebeveiliging. Wanneer de betrouwbaarheid van de informatievoorziening beter beschermd moet worden, worden dwingender richtlijnen gesteld. Derhalve bepaalt de betrouwbaarheidsbehoefte de stringentheid van de beveiligingsrechtlijnen en prozaïsche beschrijvingen. Immers, hoe meer behoefte er is aan de waarborging van de betrouwbaarheid van de informatievoorziening, hoe strenger de eisen die het beveiligingsbeleid moet stellen aan de informatiebeveiliging.

Om uitvoering te geven aan de invulling van het beveiligingsbeleid op basis van de betrouwbaarheidsbehoefte moet worden bepaald hoe de afhankelijkheid van de informatievoorziening kan worden bepaald. Hierop wordt ingegaan in de volgende paragraaf, waarbij wordt geëvalueerd of de afhankelijkheid van de informatievoorziening kan worden bepaald aan de hand van eenvoudig vast te stellen en veelal al bekende organisatiekenmerken.

4.4 Indicatieve factoren

In de vorige paragrafen is beschreven dat de afhankelijkheid van de informatiesystemen, gesplitst naar beschikbaarheid, integriteit en vertrouwelijkheid, primair bepalend is voor de invulling van het beveiligingsbeleid.

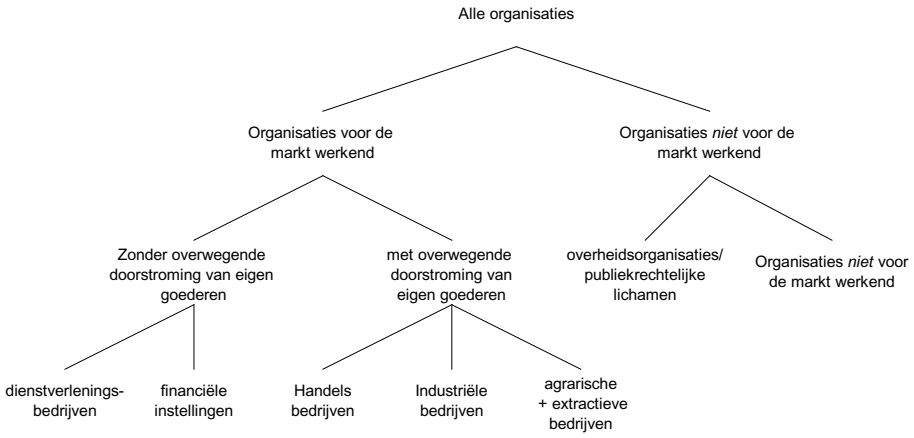
De afhankelijkheid van de informatievoorziening is geen organisatiekenmerk dat even op te zoeken is. Het staat niet op de gevel van een bedrijfspand, niet in jaarverslagen en het is niet

bekend bij de kamer van koophandel. Ook is het niet iets dat niet van 'de buitenkant' van een organisatie af te lezen: het is geen oppervlakkig organisatiekenmerk dat eenvoudig kan worden vastgesteld. Het is daarom interessant te evalueren of er andere factoren (organisatie–kenmerken) zijn die bepalend of indicatief zijn voor het beveiligingsbeleid, die wel eenvoudig van de buitenkant van een organisatie kunnen worden afgelezen.

4.4.1 Administratief organisatorische typologieën

Eén invalshoek van waaruit gezocht kan worden naar bepalende factoren is te denken vanuit de theorieën omtrent administratieve organisatie (AO). In de leer van de AO, zoals die door Starreveld is neergelegd, worden organisaties verdeeld in typologieën. [STAR1997]. Deze verdeling is schematisch weergegeven in figuur 12.

Het nut van deze typologieën zou kunnen liggen in het feit dat organisaties met een gelijke typologie een zelfde afhankelijkheid van hun informatiesystemen kennen. Starrevelds theo–rieën zijn echter primair gericht op administratieve systemen, terwijl organisatie veelal over meer dan alleen administratieve informatiesystemen beschikken. Dit heeft tot gevolg dat organisaties met identieke typologieën zeer verschillende eisen kunnen stellen aan informatie–beveiliging. [NGI1992] Zo valt onder 'dienstverlenende bedrijven' een enorm breed scala aan organisaties, variërend van de tweepersoons consultancy v.o.f. met beperkte automatisering



Figuur 12: De typologieën van Starreveld

tot de multinationale dienstverleners die hun volledige kennis in geautomatiseerde systemen hebben opgeslagen. Het moge duidelijk zijn dat deze twee (uiterste) organisaties zeer verschillende beveiligingsbehoeften hebben.

De typologie is dus niet echt geschikt als volledig bepalend uitgangspunt voor het beveiligingsbeleid. De typologie kan eventueel wel worden gebruikt als richtinggevende informatie. De grove scheiding in typologieën is namelijk wel een beperkte indicatie van de mate waarin organisatie afhankelijk zijn van de betrouwbaarheid van de informatievoorziening. Zo zullen financiële instellingen veelal een hoge afhankelijkheid van de informatievoorziening kennen, omdat deze beschikken over zeer privacy–gevoelige informatie met veelal directe financiële impact. Daar tegenover staan de agrarische en extractieve bedrijven die veelal minder afhankelijk zijn van de informatievoorziening, omdat de informatie over het algemeen minder gevoelig is en de beschikbaarheid van informatie niet de hoogte prioriteit heeft. Uiteraard bestaand op deze generalisatie ook uitzonderingen binnen beide typologieën.

De andere typologieën zijn minder indicatief voor de afhankelijkheid van de informatievoorziening. Voor de niet voor de markt werkende organisaties kan de afhankelijkheid variëren van laag (bijvoorbeeld een kleinschalige liefdadigheidsorganisatie) tot zeer hoog (bijvoorbeeld de belastingdienst). Veelal zal voor de afhankelijkheid voor handelsbedrijven, industriële bedrijven en dienstverlenende bedrijven gemiddeld zijn, maar zal sterk afhangen van het product of dienst waarmee zij werken.

Gezien het voorgaande kan de typologie van een organisatie een eerste indicatie vormen van de mate waarin een organisatie afhankelijk is van de informatievoorziening, maar ook niet meer dan dat. Typologieën kunnen dus niet worden gehanteerd als bepalende factor voor de afhankelijkheid van de informatievoorziening.

4.4.2 Attitude

Een ander punt waarop organisaties van elkaar verschillen is de bedrijfscultuur. Deze cultuur is historisch bepaald en wordt beïnvloed door vele factoren waaronder, de aard de kernactiviteiten, het scholingsniveau van het personeel en de houding van het management. In [NGI1992] wordt hierover het volgende geschreven: “een op de organisatie passend beleid voor de gegevensbescherming […] raakt alle onderdelen van een organisatie en is sterk afhankelijk van de in deze organisatie heersende cultuur, waarbij uiteraard ook de typologie van de organisatie en de complexiteit van de geïmplementeerde applicatiesystemen een rol spelen”.

In paragraaf 4.4.1 is reeds aangegeven dat de typologie van een organisatie in grote lijnen wel invloed heeft op het beveiligingsbeleid, maar dat deze invloed niet eenduidig is en erg lastig concreet aan te duiden is.

Het NGI [NGI1992] diept de attitude verder uit als factor die van invloed is op het beveiligingsbeleid. Zo wordt gesteld dat wat als een probleem of een kwetsbaarheid wordt gezien sterk afhangt van de voorstelling die bijvoorbeeld een manager zich van situaties kan maken of van de maatstaven die een manager aanlegt respectievelijk van hetgeen de manager zich kan permitteren. Hierbij worden de volgende mogelijke attitudes onderscheiden:

- **Risico-mijdend:** Het stelsel te nemen maatregelen is erop gebaseerd een zo gering mogelijk risico ongeregeld te laten. Relatief worden bij deze attitude veel kosten besteed aan preventieve beschermingsmaatregelen. De kwantificeerbare kosten zullen waarschijnlijk hoger uitkomen dan de kwantificeerbare baten;
- **Risico-neutraal:** de kosten voor beschermingsmaatregelen verbonden aan een dergelijke attitude zullen min of meer in evenwicht zijn met de baten. Maatregelen hebben veelal een signalerend en correctief karakter.
- **Risico-dragend:** De kosten verbonden aan deze attitude zullen laag zijn, omdat de attitude uitgaat van het maken van winst bij nemen van risico. Ten aanzien van de omvang van risico's en winst kan dit juist zijn. Het geldt echter niet voor de kans op het optreden van de risico's en de kans op winst.

[NGI1992] merkt hierbij op dat deze attitudes in zeker mate bepaald worden door hetgeen men zich maatschappelijk kan veroorloven. Banken, verzekeringsmaatschappijen, overheden, maar ook vele andere organisaties hebben een functie in onze samenleving, waarbij zorgvuldigheid in opereren een uitgangspunt is. Dit nog los van de verantwoordelijkheid die er is tegenover het eigen personeel, de klanten en de leveranciers.

Of de attitude een separate factor van invloed is valt echter te betwijfelen. Wat een organisatie zich maatschappelijk kan veroorloven heeft namelijk directe invloed op de mate waarin een organisatie afhankelijk is van de betrouwbaarheid van haar informatiesystemen. Hiermee doel ik op het feit dat de impact die een inbreuk op de beveiliging van een informatiesysteem ook de maatschappelijke factoren meeneemt. Een organisatie die een hoge afhankelijkheid van informatiesystemen kent zou automatisch een risico mijdende attitude moeten hebben. Ze kunnen zich immers (bijvoorbeeld door hun maatschappelijke verantwoordelijkheid) geen inbreuken op de informatiebeveiliging veroorloven.

Waar het de cultuur of het opleidingsniveau van een organisatie betreft gelden andere aspecten. De cultuur en het opleidingsniveau van een organisatie zijn namelijk inherent aan de mate waarin en de wijze waarop een organisatie om gaat met informatie en vice versa. Het is weliswaar zo dat het informatiebeveiligingsbeleid geldt voor alle werknemers, maar van diegenen die met de informatie omgaan mag een opleidingsniveau worden verwacht dat inherent is aan het belang van de informatie.

De conclusie is gezien dit alles dat de attitude van een organisatie weliswaar een factor van invloed is voor de informatiebeveiliging en daarmee het beveiligingsbeleid, maar dat deze factor volledig is bevat in de betrouwbaarheidsbehoefte.

4.4.3 Andere organisatie eigenschappen

Naast de beschreven typologieën en attitude zijn er nog diverse andere organisatie–eigenschappen waarvan de invloed op de afhankelijkheid van de informatievoorziening kan worden beoordeeld. Daarbij kan worden gedacht aan het aantal medewerkers, het aantal verschillende informatiesystemen, de omzet en/of winst, et cetera. Een vluchtige analyse van alleen typologieën en de attitude geeft echter al aan dat het moeilijk is grip te krijgen op de objectieve invloed van mogelijke oppervlakkige factoren.

Het probleem met de genoemde (min of meer) makkelijk in te schatten factoren is dat ze allemaal wel invloed hebben of kunnen hebben op de afhankelijkheid, maar dat niet eenvoudig is vast te stellen welke (combinatie van) factoren werkelijk bepalend zijn en in welke mate. Gezien deze complexiteit biedt het gebruik van objectieve oppervlakkige factoren geen praktische oplossing om de betrouwbaarheidsbehoefte van buitenaf vast te stellen. Als alternatief zal ik daarom de vaststelling van de betrouwbaarheidsbehoefte van binnenuit de organisatie benaderen, hetgeen nader wordt onderzocht in hoofstuk vijf.

4.5 Conclusie

Naar aanleiding van de in hoofdstuk drie geconstateerde verschillen en overeenkomsten in beveiligingsbeleid is gezocht naar factoren die de invulling van het beveiligingsbeleid bepalen. Daarbij is aangegeven dat de invulling van beveiligingsbeleid in essentie wordt bepaald door de mate waarin organisaties behoefte hebben aan waarborging van de betrouwbaarheid van de informatievoorziening.

De betrouwbaarheid van de informatievoorziening kent twee dimensies, te weten de afhankelijkheid en de kwetsbaarheid van de informatievoorziening. De afhankelijkheid geeft aan in welke mate een organisatie afhankelijk is van de informatievoorziening en derhalve in welke mate de betrouwbaarheid van de informatievoorziening moet worden gewaarborgd. De kwetsbaarheid geeft aan voor welke bedreigingen een organisatie kwetsbaar is en bepaalt op welke wijze de betrouwbaarheid van de informatievoorziening moet worden gehandhaafd; welke maatregelen moeten worden getroffen om de bedreigingen af te dekken en daarmee aan het vereiste niveau van beveiliging te voldoen.

Op basis hiervan is gesteld dat de invulling van het informatiebeveiligingsbeleid wordt bepaald door de afhankelijkheid van de informatievoorziening. Dit bepaalt namelijk in welke mate bescherming nodig is, hetgeen precies het doel van het beveiligingsbeleid is: aanduiden welk niveau van beveiliging moet worden ingericht. De kwetsbaarheid is gericht op de wijze waarop moet worden beveiligd om aan het door de afhankelijkheid vereiste beveiligingsniveau te voldoen. De kwetsbaarheid is hiermee niet bepalend voor het beveiligingsbeleid, omdat dit dus betrekking heeft op het bepalen welke acties moeten worden ondernomen om een organisatie te laten voldoen aan de (in het beveiligingsbeleid) gestelde beveiligingseisen.

In essentie is de afhankelijkheid gerelateerd aan (het gebruik van informatie door) de organisatie zelf en is de kwetsbaarheid gerelateerd aan de bedreigingen van buiten. Analoog hangt het beveiligingsbeleid alleen af van het gebruik van informatie door een organisatie en niet van de bedreigingen van buiten.

Teneinde de afhankelijkheid te bepalen is gezocht naar makkelijk vast te stellen ('oppervlakkige') organisatie kenmerken welke de afhankelijkheid van de informatievoorziening bepalen. Hierbij zijn in detail de typologie en de attitude van een organisatie geëvalueerd. Naar aanleiding hiervan is beschreven dat noch de typologie, noch de attitude, noch enige andere oppervlakkige organisatie–eigenschap doorslaggevend is voor de afhankelijkheid van de informatievoorziening. Derhalve dient te worden onderzocht hoe de afhankelijkheid van de informatievoorziening zelf rechtstreeks kan worden bepaald, hetgeen wordt beschreven in hoofdstuk vijf.

Mogelijke waarden van de betrouwbaarheidsbehoefte

5

"Het uitvoeren van een risicoanalyse heeft als groot voordeel dat de organisatie een goed inzicht krijgt in de afhankelijkheden en kwetsbaarheden van de IT. Risicoanalyses kennen ook nadelen: zij zijn niet alleen kostbaar, maar kunnen ook leiden tot een teveel aan informatie, waardoor het nemen van beslissingen niet makkelijker, maar juist moeilijker wordt."

Dr. E.E.O. Roos Lindgreen RE [ROOS1999]

In hoofdstuk vier is beschreven dat informatiebeveiliging —en de richting die daaraan wordt gegeven door het beveiligingsbeleid wordt bepaald door de betrouwbaarheidsbehoefte van een organisatie, welke in essentie afhangt van de afhankelijkheid van de informatievoorziening. Daarbij is geschetst dat de betrouwbaarheidsbehoefte gevolgen heeft voor de stringentie van het beveiligingsbeleid. Om voor een organisatie de stringentie van het beveiligingsbeleid te bepalen moet daarom de betrouwbaarheidsbehoefte van de organisatie worden vastgesteld.

De efficiëntie en effectiviteit van het opstellen van beveiligingsbeleid is erbij gebaat dat de invulling van het beveiligingsbeleid zo direct mogelijk wordt gerelateerd aan betrouw–

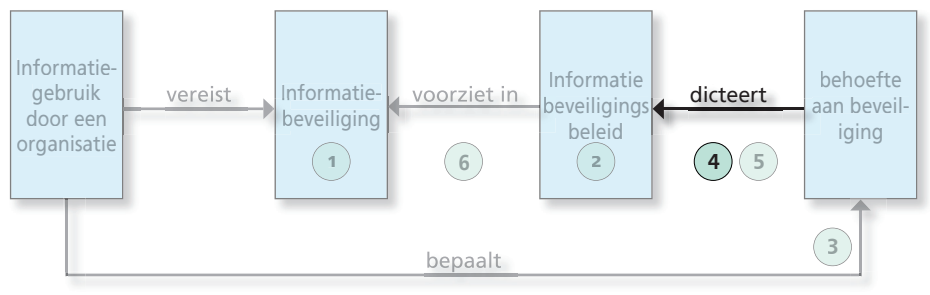
baarheidsbehoefte. Dat wil zeggen dat bij een bepaalde betrouwbaarheidsbehoefte zo direct mogelijk duidelijk moet zijn hoe stringent het beveiligingsbeleid moet zijn en wat derhalve de inhoud moet zijn. Bij voorkeur moet het mogelijk zijn om aan één bepaalde betrouwbaarheidsbehoefte direct één bepaalde invulling van het beveiligingsbeleid te koppelen.

Om op basis van deze relatie het beveiligingsbeleid op te stellen moet om te beginnen worden bepaald hoe de betrouwbaarheidsbehoefte efficiënt en effectief kan worden vastgesteld. Om dat te kunnen doen moet eerst meer duidelijkheid worden gecreëerd over de mogelijke waarden van het begrip betrouwbaarheidsbehoefte. Daarmee wordt de inputzijde van de te ontwikkelen methode vorm gegeven. Dit is verwoord in de kernvraag van dit hoofdstuk:

Kernvraag 4

Aan welke voorwaarden dienen de beveiligingsbeleid bepalende factoren te voldoen om de inhoud van het beveiligingsbeleid op basis daarvan te kunnen bepalen?

De beantwoording van de kernvraag zal ik in paragraaf 5.1 beginnen met het beschrijven van de nood om de betrouwbaarheidsbehoefte te kwantificeren om praktische uitvoering aan de relatie te kunnen geven. Aansluitend beschrijf ik in 5.2 de randvoorwaarden voor deze kwantificering. Paragraaf 5.3 behandelt vervolgens de mogelijke waarden die de betrouwbaarheidsbehoefte na kwantificering kan hebben. Tenslotte worden in paragraaf 5.4 de mogelijke waarden verder uitgewerkt door praktische typeringen aan de waarden te koppelen.



Figuur 13: De kernvraag van dit hoofdstuk is uitgelicht in het schema

De plaats van deze kernvraag binnen het gehele onderzoek is in figuur 13 uitgelicht. Het is het eerste deel van het uitdiepen van de te leggen relatie tussen de betrouwbaarheidsbehoefte en de invulling van het beveiligingsbeleid. Op het tweede deel hiervan wordt in hoofdstuk 6 verder ingegaan.

5.1 Kwantificeren van de betrouwbaarheidsbehoefte

Om de betrouwbaarheidsbehoefte van een organisatie direct te relateren aan de invulling van het beveiligingsbeleid moet duidelijk worden hoe de afhankelijkheid te 'meten' is. Wanneer de afhankelijkheid meetbaar is, wordt het namelijk mogelijk te onderzoeken hoe aan een betrouwbaarheidsbehoefte een bepaalde invulling van het beveiligingsbeleid kan worden gekoppeld. Om te kunnen meten moet eerst vaststaan met welke eenheid gemeten wordt: hoe moet de beschrijving (eenheid) van de betrouwbaarheidsbehoefte eruit zien.

Een mogelijke vorm is een *free form* beschrijving in de vorm van een prozaïsche verhandeling over de positie van de organisatie ten opzichte van haar informatiesystemen is. Een dergelijke invulling van de betrouwbaarheidsbehoefte maakt het echter niet mogelijk op systematische wijze de invulling van het beveiligingsbeleid te kiezen. Een vrije beschrijving biedt namelijk niet de mogelijkheid een directe relatie te leggen tussen de betrouwbaarheidsbehoefte en het beveiligingsbeleid. Een vrije beschrijving kan immers oneindig veel vormen aannemen en is moeilijk af te bakenen.

Een direct relatie leggen wordt eenvoudiger indien de mogelijke waarden van de betrouwbaarheidsbehoefte beperkt en afgebakend zijn. Om dat te bereiken is het gewenst de betrouwbaarheidsbehoefte kwantificeerbaar te maken. Daarmee wordt de betrouwbaarheidsbehoefte gemaakt tot een meetbare eenheid, wat het mogelijk maakt om aan de betrouwbaarheidsbehoefte een afgebakende waarde toe te kennen. Vervolgens kan getracht worden aan elke mogelijk waarde een invulling van beveiligingsbeleid te koppelen.

5.2 Randvoorwaarden voor kwantificering

Om het vaststellen van de betrouwbaarheidsbehoefte (de 'meting') een beperkt aantal mogelijke waarden te laten hebben moeten de drie deelaspecten van de betrouwbaarheidsbehoefte (beschikbaarheid, integriteit en vertrouwelijkheid) ook een beperkt aantal waarden aannemen. Hierbij dringt zich de vraag op bij hoeveel verschillende mogelijke waarden de kwantificering nog werkbaar is, waaronder ik de situatie versta waarin aan de volgende voorwaarden wordt voldaan:

- Het aantal mogelijke waarden is dermate beperkt dat de mogelijke waarden zo onderscheidend zijn dat het bepalen van de waarde geen ongewenst grote inspanning vergt;
- Het aantal mogelijke waarden is dermate groot dat de verschillen tussen de betrouwbaarheidsbehoeften van verschillende organisaties met voldoende precisie te representeren zijn.

Deze criteria zal ik nader toelichten. Alle mogelijk waarden van de betrouwbaarheidsbehoefte kunnen worden gezien als een spectrum van waarden. Het spectrum heeft als grenzen aan de ene kant een zo klein mogelijke (lees: geen) betrouwbaarheidsbehoefte en aan de andere kant een maximale betrouwbaarheidsbehoefte. Hoe meer waarden er mogelijk zijn, hoe kleiner het verschil is tussen de waarden, ervan uitgaande dat de afmetingen van het spectrum gelijk blijven. Hoe kleiner het verschil tussen de mogelijk waarden, hoe groter de vereiste inspanning zal zijn om de waarden te kunnen onderscheiden en daarmee de inspanning om een juiste keuze uit die waarden te kunnen maken.

Anderzijds dient het aantal mogelijke waarden echter niet te klein te zijn omdat er in dat geval te weinig keuzen zijn en de verschillen tussen organisaties niet met voldoende precisie door de verschillende waarden worden weergegeven. Er zal dus een evenwicht gekozen moeten worden tussen deze tegenstrijdige belangen, waarbij zowel de kosten (de vereiste inspanning) als de opbrengsten (het onderscheidend vermogen) acceptabel zijn.

Aangezien de betrouwbaarheidsbehoefte is opgebouwd uit drie deelaspecten wordt het vaststellen ervan snel complex wanneer de mogelijke waarden van de deelaspecten toenemen. Het uitbreiden van de mogelijke waarden van elk betrouwbaarheidsaspect leidt tot een toename van de orde n^3 (indien alledrie de factoren een gelijk aantal mogelijke waarden houden). In dit

onderzoek kies ik, gezien dit feit en de eis van werkbaarheid, voor drie mogelijke waarden per afhankelijkheidsaspect, hetgeen betekent dat de afhankelijkheid als geheel 3×3×3=27 mogelijke waarden aan kan nemen.

Minder mogelijke waarden is niet wenselijk omdat daarmee onvoldoende mogelijkheden bestaan om onderscheid aan te brengen in de afhankelijkheid van organisaties. Meer verschillende mogelijke waarden is vanuit het onderscheidsoogpunt wel wenselijk, maar leidt direct tot 64 of meer mogelijke waarden voor de betrouwbaarheidsbehoefte als geheel.

5.3 Mogelijke waarden van de betrouwbaarheidsbehoefte

5.3.1 Gebruik van linguïstische waarden

De deelaspecten van de betrouwbaarheidsbehoefte zijn uit te drukken in gradaties van hoeveelheid. Hierbij kan bijvoorbeeld gedacht worden aan '*nauwelijks*', '*enigszins*', '*zeer*', '*enorm*', et cetera. De waarde geeft aan in hoeverre een organisatie afhankelijk is van bijvoorbeeld de beschikbaarheid van de informatiesystemen en in hoeverre er derhalve behoefte is aan bescherming hiervan. Weliswaar kunnen de waarden ook door andere bewoordingen worden voorgesteld, zoals groen, geel, rood of de getallen 1, 2 en 3. Echter in alle gevallen representeren deze waarden de mate waarin er een beschermingsbehoefte bestaat.

Een representatie van de betrouwbaarheidsbehoefte in de vorm van getallen is minder wenselijk omdat dit de indruk kan wekken dat het hier om exact meetbare waarden gaat. Gezien de materie, het feit dat beveiligingsbeleid een strategische aard heeft, het over de gehele informatievoorziening gaat en ik de waarde snel efficiënt vast wil stellen zal de meting echter niet exact kunnen zijn. Daarom kies is ik voor het gebruik van woorden om de mogelijke waarden aan te duiden.

Voor de terminologie van de te hanteren mogelijke waarden baseer ik me op de theorie van de **fuzzy logic** ([NGUY1997], [PIJL2004]. Deze tak van de wiskunde houdt zich bezig met het berekenbaar maken van niet exacte waarden. Dit sluit nauw aan bij de behoefte om het niet exacte begrip betrouwbaarheidsbehoefte te kwantificeren. Op basis van fuzzy logic worden de aspecten beschikbaarheid, integriteit en vertrouwelijkheid aangeduid als zogenaamde

linguïstische variabelen. Deze variabelen kunnen *linguïstische waarden* aannemen, zoals 'enigszins', 'nauwelijks' en 'in grote mate'. In de context van fuzzy logic is de betrouwbaarheidsbehoefte een triple (B,I,V) van de linguïstische variabelen beschikbaarheid, integriteit en vertrouwelijkheid. In 5.2 is al aangegeven dat de deelaspecten van de betrouwbaarheidsbehoefte ieder drie waarden kunnen hebben, waardoor de triple (B,I,V) 27 waarden kan hebben.

5.3.2 Afdekking van het behoeftenspectrum

De mogelijke waarden per betrouwbaarheidsaspect dienen in theorie het volledige behoeftespectrum te beslaan. Er gelden echter bijzondere omstandigheden voor de extremen van het spectrum, zijnde geen behoefte aan bescherming van een deelaspect en maximale bescherming van een deelaspect. In het geval er geen behoefte is om een betrouwbaarheidsaspect te beschermen, hoeft het beveiligingsbeleid daarop ook niet in te gaan. De situatie van maximale behoefte aan bescherming bestaat alleen in theorie. In de praktijk is het niet mogelijk een betrouwbaarheidsaspect volledig te garanderen, omdat de kosten hiervan te hoog zijn. Dit betekent dat de extremen van het spectrum niet door de mogelijke waarden hoeven en kunnen worden afgedekt.

Ik kies ervoor om in het vervolg gebruik te maken van de termen 'laag' (L), middelmatig (M) en hoog (H) om de drie mogelijke waarden per betrouwbaarheidsaspect aan te duiden. Virtueel kunnen daar nog de waarden 'geen' (G) en 'volledig' (V) aan toe worden gevoegd die de extremen afdekken. Wanneer het gehele spectrum van betrouwbaarheidsbehoeften wordt gezien als een schaal van 0 tot 100%, dan kan deze waardenverdeling grofweg als de onderstaande verdeling van het spectrum worden gezien (zonder de evidente extremen G en V).

L: 10% tot 40%;
M: 40% tot 70%;
H: 70% tot 95%.

Uiteraard zijn deze waarden niet exact bepaald, maar vormen ze een globale verdeling op basis van de tekstuele beschrijving hiervoor. Bedoeld om het concept van de waarden meer inzichtelijk te maken. In hoofdstuk zes zal verder worden ingegaan op de verdeling van de waarden over het spectrum van betrouwbaarheidsbehoeften.

5.4 Uitwerking van de mogelijke waarden van de betrouwbaarheidsbehoefte

Om aan een organisatie een bepaalde betrouwbaarheidsbehoefte te kunnen toekennen, moet duidelijk zijn wat onder een bepaalde waarde wordt verstaan. In 5.3 is al beschreven dat ik uit ga van drie mogelijke waarden per betrouwbaarheidsaspect. In de volgende paragrafen zal ik de mogelijke waarden van de betrouwbaarheidsbehoefte per betrouwbaarheidsaspect verder uitwerken.

Uiteraard blijft gelden dat betrouwbaarheidsbehoefte van organisaties niet simpelweg kan worden gekarakteriseerd, zoals beschreven in hoofdstuk vier. Het is dan ook niet de bedoeling om een standaard organisaties of organisatieklassen te schetsen. De beschrijvingen die hieronder worden gegeven dienen ter illustratie om het mogelijk te maken een beeld te vormen bij de mogelijke waarden.

5.4.1 Beschikbaarheid

Lage beschikbaarheidsbehoefte

Dit is een organisatie die een lage behoefte heeft aan het op de juiste momenten beschikbaar zijn van informatie en essentiële diensten. Aantasting van de beschikbaarheid van de informatievoorziening heeft slechts kleine impact op de bedrijfsvoering. Het gaat hier dus om een organisatie met weinig tot geen tijdskritische systemen waarvan het niet beschikbaar zijn voor langere tijd geaccepteerd kan worden. De beschikbaarheid van de systemen is over het algemeen niet van primair belang voor de bedrijfsvoering. Denk hierbij aan het kleinbedrijf, middenstand, garagebedrijf en dergelijke.

Middelmatige beschikbaarheidsbehoefte

Het gaat hier om een organisatie die een middelmatige behoefte heeft aan het op de juiste momenten beschikbaar zijn van informatie en essentiële diensten. Aantasting van de beschikbaarheid heeft significante impact op de bedrijfsvoering. Het gaat hier dus om een organisatie met tijdskritische systemen waarvan het niet beschikbaar zijn slechts voor een beperkte tijdsduur geaccepteerd kan worden. De beschikbaarheid van de systemen is over het algemeen belangrijk voor de bedrijfsvoering. Voorbeelden zijn een postorderbedrijf, een middelgrote tot grote gemeente, accountantskantoor, een distributiebedrijf, transporteur en dergelijke.

Hoge beschikbaarheidsbehoefte

Dit is een organisatie die een hoge behoefte heeft aan het op de juiste momenten beschikbaar zijn van informatie en essentiële diensten. Aantasting van de beschikbaarheid van de informatievoorziening heeft ernstige impact op de bedrijfsvoering en kan zelfs het voortbestaan van de (deel)organisatie tot gevolg hebben. Het gaat hier dus om een organisatie met zeer tijdskritische systemen waarvan het niet beschikbaar zijn onacceptabel is. Systemen zijn dus van primair belang voor de bedrijfsvoering. Dit kan bijvoorbeeld een bank zijn, een verzekeraar of een grote industriële onderneming.

5.4.2 Integriteit

Lage integriteitsbehoefte

Het gaat hier om een organisatie die over het algemeen een lage behoefte heeft aan waarborging van de correctheid en volledigheid van informatie en computerprogrammatuur. Aantasting van de integriteit heeft beperkte impact op de bedrijfsvoering. Dit is dus een organisatie waarvoor de integriteit van haar informatie en programmatuur niet van primair belang is voor de bedrijfsvoering. Denk hierbij wederom aan het kleinbedrijf, middenstand, garagebedrijf en dergelijke.

Middelmatige integriteitsbehoefte:

Dit is een organisatie die een middelmatige behoefte heeft aan waarborging van de correctheid en volledigheid van de informatievoorziening. Aantasting van de integriteit heeft significante (merkbare) impact op de bedrijfsvoering. Dit is dus een organisatie waarvoor de integriteit van haar informatie en programmatuur over het algemeen belangrijk is voor de bedrijfsvoering. Denk hierbij aan een postorderbedrijf, middelgrote tot grote gemeente, accountantskantoor. Denk aan een distributiebedrijf, een transporteur en dergelijke.

Hoge integriteitsbehoefte

Hier gaat het om een organisatie die een hoge behoefte heeft aan waarborging van de correctheid en volledigheid van de informatievoorziening. Aantasting van de integriteit van de informatievoorziening heeft ernstige impact op de bedrijfsvoering en kan zelfs het voortbestaan van de (deel)organisatie in gevaar brengen. Het gaat hier dus om een organisatie

waarvoor de integriteit van haar informatie en programmatuur van primair belang is voor de bedrijfsvoering. Dit kan bijvoorbeeld een bank zijn, een verzekeraar, grote industrie, maar ook hightech bedrijven en eCommerce bedrijven.

5.4.3 Vertrouwelijkheid

Lage vertrouwelijkheidsbehoefte

Dit zal een organisatie zijn welke over het algemeen een lage behoefte heeft aan de bescherming van informatie tegen onbevoegde kennisname. Dit betekent dat de vertrouwelijkheid van informatie voor de organisatie niet van primair belang is voor de bedrijfsvoering en inbreuken op de vertrouwelijkheid slecht geringe schade zullen veroorzaken. Feit is wel dat praktisch elke organisatie vertrouwelijke gegevens heeft in de vorm van personeelsgegevens, welke ook als zodanig beschermd dienen te worden. Bij organisaties met een lage vertrouwelijkheidsbehoefte kan gedacht worden aan het kleinbedrijf, middenstand, kleine industrie.

Middelmatige vertrouwelijkheidsbehoefte

Dit is een organisatie die een medium behoefte heeft aan de bescherming van informatie tegen onbevoegde kennisname. Dit geeft aan dat de vertrouwelijkheid van haar informatie voor de organisatie over het algemeen belangrijk is voor de bedrijfsvoering en dat inbreuken op de vertrouwelijkheid substantiële (grote) schade kunnen veroorzaken. In de praktijk betreft het hier organisaties als een distributiebedrijf (klantgegevens), transporteur, industrie en dergelijke.

Hoge vertrouwelijkheidsbehoefte

Dit is een organisatie die een hoge behoefte heeft aan de bescherming van informatie tegen onbevoegde kennisname. Dit geeft aan dat de vertrouwelijkheid van haar informatie voor de organisatie over het algemeen van essentieel belang is voor de bedrijfsvoering en dat inbreuken op de vertrouwelijkheid zeer grote schade zullen veroorzaken. Het gaat hier veelal om organisaties die grote verzamelingen persoonsgegevens beheren of organisaties die met zeer gevoelige bedrijfsgegevens omgaan. Dit kan bijvoorbeeld een bank zijn, een verzekeraar, grote industrie, maar ook hier hightech bedrijven, eCommerce bedrijven, hightech bedrijven.

5.5 Conclusie

In dit hoofdstuk is een start gemaakt met het uitwerken van de inputkant van de methode voor het systematisch opstellen van informatiebeveiligingsbeleid. Daarbij is ingegaan op de randvoorwaarden die gelden ten aanzien van de waarden die de betrouwbaarheidsbehoefte kan hebben en welke mogelijke waarden deze binnen de methode kan aannemen.

Teneinde efficiënt en effectief uitvoering te kunnen geven aan de relatie tussen de betrouwbaarheidsbehoefte en de invulling van het beveiligingsbeleid dient de betrouwbaarheidsbehoefte kwantificeerbaar te zijn. Alleen dan wordt de betrouwbaarheidsbehoefte meetbaar, waarbij aan specifieke waarden van de betrouwbaarheidsbehoefte een specifieke invulling van het beveiligingsbeleid kan worden gekoppeld.

Het vaststellen ('meten') van de betrouwbaarheidsbehoefte vereist dat het aantal mogelijk waarden klein genoeg is om de uitvoering niet te complex te maken, en tegelijkertijd voldoende verschillende waarden om verschillen tussen de betrouwbaarheidsbehoefte van organisaties met voldoende detail te kunnen representeren. Binnen dit onderzoek kies ik ervoor de deel aspecten van de betrouwbaarheidsbehoefte (beschikbaarheid, integriteit en vertrouwelijkheid) ieder drie verschillende waarden aan te laten nemen. Dit betekent dat de betrouwbaarheidsbehoefte in totaal 27 verschillende waarden kan aannemen.

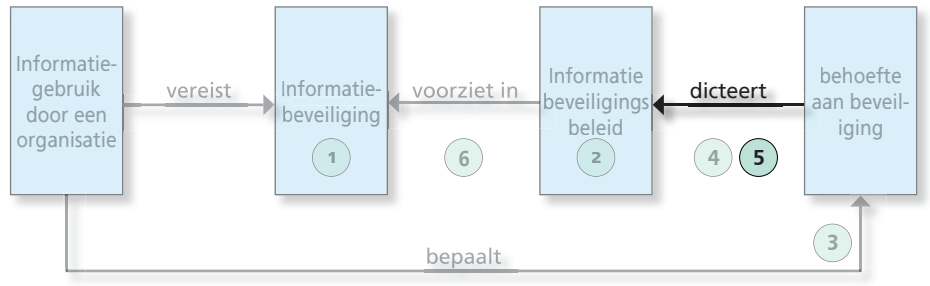
Gezien de algemene en strategische aard van het beveiligingsbeleid is het onwenselijk de gekwantificeerde betrouwbaarheidsbehoefte weer te geven met getallen, omdat dit een valse indruk van exactheid wekt. Tevens is het gezien de algemene en strategische aard van belang om qua terminologie aan te sluiten bij de denkwereld van managers (en natuurlijk materie–experts aangezien zij ermee moeten werken. Ieder deelaspect van de betrouwbaarheidsbehoefte zal daarom worden gerepresenteerd in de zogenaamde linguïstische waarden L (laag), M (middelmatig) en H (hoog). Deze drie waarden dekken gezamenlijk het gehele behoeftenspectrum af, met uitzondering van de extremen, zijnde geen behoefte en maximale behoefte. Beide extremen worden niet door het beveiligingsbeleid afgedekt.

Kwantificering van de betrouwbaar-heidsbehoefte

"Het begrip risicoanalyse wordt sterk door de situatie en de persoon bepaald. Subjectiviteit speelt een rol bij risico-analyse een belangrijke rol. Het wekt derhalve geen verwondering dat er met betrekking tot risicoanalyse een welhaast onoverkomelijke spraakverwarring bestaat."

NGI studierapport inzake toepassing van risicoanalyse
bij geautomatiseerde gegevensverwerking [NGI1991]

Na in hoofdstuk vijf vastgesteld te hebben hoeveel en welke verschillende waarden de betrouwbaarheidsbehoefte van een organisatie kan aannemen komt nu de complexe taak aan te geven hoe de waarde moet worden bepaald. Het beveiligingsbeleid is een zaak van het management, op strategisch en tactisch niveau richting gevend aan informatiebeveiliging. Rekening houdend met deze aspecten moet een methode worden ontwikkeld waarmee de betrouwbaarheidsbehoefte van een organisatie kan worden bepaald. Dit wordt uitgewerkt op basis van de volgende kernvraag:



Figuur 14: De kernvraag van dit hoofdstuk is uitgelicht in het schema

Kernvraag 5

Hoe kunnen de waarden van de beveiligingsbeleid bepalende factoren efficiënt en effectief worden vastgesteld zodat op basis daarvan het beveiligingsbeleid systematisch kan worden opgesteld?

In paragraaf 6.1 ga ik in op het gebruik van regulieren risicoanalyses als mogelijkheid om de betrouwbaarheidsbehoefte vast te stellen. In paragraaf 6.2 wordt dit verder gespecificeerd door in te gaan op het gebruik van een macrorisicoanalyse. In paragraaf 6.3 wordt aansluitend de SPRINT methode beschreven als mogelijke vorm van een macrorisicoanalyse. Daarbij wordt ook aangegeven welke aanpassingen in de SPRINT methode moeten worden doorgevoerd om deze toepasbaar te maken binnen de te ontwikkelen methode voor het systematisch opstellen van beveiligingsbeleid. Paragraaf 6.4 beschrijft vervolgens hoe vaststelling van de betrouwbaarheidsbehoefte met de SPRINT methode kan worden uitgevoerd. Tot slot wordt in paragraaf 6.5 beoordeeld in hoeverre de methode voldoet aan de wensen, door een proefanalyse uit te voeren met materie-experts.

De uitwerking van deze kernvraag vormt het tweede deel van het vormgeven van de relatie tussen de betrouwbaarheidsbehoefte en de invulling van het beveiligingsbeleid, zoals in figuur 14 is uitgelicht.

6.1 Gebruik van reguliere risicoanalyses

Een kwestie die zich opdringt is in hoeverre dit onderzoek moet trachten een methode te geven voor het bepalen van de betrouwbaarheidsbehoefte. Er zijn in de theorie en de prak-

tijk namelijk vele methoden ontworpen en in gebruik die zich richten op het bepalen van de vereiste bescherming van informatiesystemen. Deze methoden komen samen onder de noemer **risicoanalyse**. Voorbeelden zijn te vinden in onder andere [NGI1991], [NGI1992b] en [OVER2000].

De risicoanalyse wordt in [NGI1992b] gedefinieerd als "het inventariseren van de bedreigingen waaraan een proces onderworpen kan zijn, het inschatten van de mogelijke gevolgen van het blootstellen van het proces aan die bedreigingen en het doen van voorstellen om die gevolgen te minimaliseren op basis van de in het beveiligingsbeleid aangegeven uitgangspunten". Uit deze definitie blijkt dat een risicoanalyse allereerst gericht is op het bepalen van de bedreigingen (kwetsbaarheid) voor de informatievoorziening, terwijl voor het beveiligingsbeleid de afhankelijkheid van de informatievoorziening de bepalende factor is. De risicoanalyse zoals hier gedefinieerd legt daarmee de nadruk op het 'hoe' van de beveiliging en niet op het 'wat'.

Daarbij komt dat de risicoanalyse gericht is op het bepalen van de vereiste beveiliging van individuele informatiesystemen, terwijl het beveiligingsbeleid gericht is op de informatievoorziening als geheel. Het uitvoeren van een risicoanalyse op informatiesysteemniveau vereist veel tijd en inspanning. Wanneer per informatiesysteem een risicoanalyse dient te worden uitgevoerd om de betrouwbaarheidsbehoefte van een organisatie te bepalen zal dit bij een organisatie met veel informatiesystemen tot zeer tijdrovende onderzoeken leiden. Een dergelijke methode is in z'n algemeenheid een te kostbare aangelegenheid [NGI1992]. Weliswaar zou daarmee de betrouwbaarheidsbehoefte van een organisatie zeer precies in kaart kunnen worden gebracht, het sluit niet aan bij mijn behoefte aan een methode die met name is gericht op efficiëntie en effectiviteit. Tevens nemen veel risicoanalyses het begrip kwetsbaarheid mee in de analyse, hetgeen voor het beveiligingsbeleid niet bepalend is.

Naast de onevenredig grote inspanning van het uitvoeren van een systeemgerichte risicoanalyse komt als resultaat een zeer grote hoeveelheid, mogelijk sterk uiteenlopende, betrouwbaarheidsbehoeften van verschillende systemen beschikbaar. Het op basis daarvan afleiden van de betrouwbaarheidsbehoefte is dan al een complexiteit op zich. Daarbij komt dat veel risicoanalyses er vanuit gaan dat voorafgaand aan de risicoanalyse reeds een beveiligingsbeleid is geformuleerd [NGI1991], zoals ook blijkt uit de gegeven definitie. De eventuele sturing die het beveiligingsbeleid aan zo'n analyse geeft ontbreekt echter, wanneer de analyse juist bedoeld is om beveiligingsbeleid op te stellen.

Gezien deze aspecten is het moeilijk de betrouwbaarheidsbehoefte (afhankelijkheid van de informatievoorziening) van een organisatie te baseren op de uitkomsten van een reguliere risicoanalyse. De reguliere risicoanalyse is binnen de te ontwikkelen methode daarom niet de meest geschikte wijze om de betrouwbaarheidsbehoefte te bepalen.

6.2 De 'macro' risicoanalyse

De nadelen van de uitvoerige systeemgerichte risicoanalyses dwingen mij te zoeken naar een manier om de afhankelijkheid in kaart te brengen die meer gericht is op tactisch en strategisch niveau. In [NGI1992] wordt hiervoor een mogelijkheid geschetst in de vorm van een zoge–heten 'macro' risicoanalyse. Hierin beschrijft het NGI hoe het opzetten van beveiligingsbeleid voorafgegaan dient te worden door het uitvoeren van een risicoanalyse op macroniveau.

Deze 'macrorisicoanalyse' wordt gedefinieerd als "het analyseren van de risico's waarvoor een organisatie zich geplaatst ziet op het hoogste niveau".

Ter toelichting op de macrorisicoanalyse wordt verwezen naar het NGI rapport 'Risicoana–lyse en risicomanagement' [NGI1992b]. Daarin worden echter in onvoldoende mate 'handen en voeten' gegeven aan de uitvoering van deze macrorisicoanalyse. Het stuk gaat vooral zeer uitvoerig in op een procesbeschrijving van de risicoanalyse voor individuele informatiesy–stemen, het datamodel voor het verzamelen van de informatie uit de risicoanalyse en een zeer gedetailleerde systematiek om dit in uitvoering te brengen. Tevens wordt wederom onvol–doende geabstraheerd tot alleen de afhankelijkheid, waar het voor beveiligingsbeleid om gaat. Daardoor komt de uitwerking in het genoemde rapport niet uit de verf als handvat voor het uitvoeren van een macrorisicoanalyse.

6.3 Evaluatie van de SPRINT methode voor het bepalen van de betrouwbaarheidsbehoefte

Ondanks dat de specifieke uitwerking van [NGI1992b] niet voldoende aanknopingspunten biedt voor uitvoering, sluit het idee van de macrorisicoanalyse goed aan op de doelen die ik nastreef en daarom zoek ik alternatieve uitwerkingen. Een in het oog springende macrori–

sicoanalyse is de zogenaamde SPRINT methode [ISF1997] van het International Security Forum (ISF). SPRINT staat voor *Simplified Process for Risk Identification*. Hierna zal ik de bruikbaarheid van de SPRINT methode binnen de doelen van deze scriptie onderzoeken.

Voorafgaan is het essentieel te melden dat SPRINT gericht is op het verkrijgen van een score op basis van de kennis van managers over een organisatie en de afhankelijkheid van de informatievoorziening. Gevoelsmatig weet iedere manager waar in zijn organisatie(eenheid) de sterke en zwakke punten liggen, wat de kwetsbaarheden zijn. Hij kan derhalve in uitgangspunten een richting geven van de afhankelijkheid van de informatievoorziening. Op deze wijze kan snel sturing worden gegeven worden aan het proces dat moet leiden tot het inrichten van de informatiebeveiliging.

De SPRINT methode betreft dus geen klinische objectieve meting of berekening van waarden zoals die veelal plaatsvindt bij het gebruik van risicoanalyses. Daarmee wordt de vaststelling van de betrouwbaarheidsbehoefte gebaseerd op expert knowledge en niet op objectieve feiten. Dit heeft als voordeel dat het vaststellen van de betrouwbaarheidsbehoefte een stuk sneller en eenvoudiger kan zijn omdat het gebaseerd is op globale waarnemingen en inzichten. Dit betekent dat bewust wordt geaccepteerd dat de waarneming een subjectief karakter heeft. Door structurering van de methodiek zal de vaststelling zoveel mogelijk worden geobjectiveerd.

6.3.1 Kenmerken van de SPRINT methode

De gedachte achter de SPRINT methode is dat reguliere risicoanalyses zeer nuttig zijn voor het beveiligen van specifieke informatiesystemen, maar dat de beschikbare technieken ingewikkeld zijn, onduidelijke resultaten opleveren en ervaren risicoanalyse uitvoerders vereist. De SPRINT methode wordt hier tegenover gesteld als business georiënteerd en gemakkelijk te gebruiken. De methode is een *best business practice* zou te gebruiken zijn in samenwerking met managers, resultaten opleveren die aan de business te relateren zijn en toe te passen zijn door niet–experts op het gebied van risicoanalyse. Volgens het ISF is de methode weliswaar ontworpen om de risico's gerelateerd aan belangrijke maar niet kritische systemen in te schatten, maar kan de methode ook een nuttige 'eerste blik' werpen op de risico's van kritische informatiesystemen. [ISF1997]

Bovenstaande beschrijving van de SPRINT methode geeft aanknopingspunten die sterk gerelateerd zijn aan de doelen die ik nastreef. Ook ik zoek naar een risicoanalyse op business–

niveau (tactisch en strategisch) die eenvoudig (efficiënt en effectief) uit te voeren is. Daarbij komt dat de SPRINT uit twee delen bestaat, te weten een afhankelijkheidsanalyse en een kwetsbaarheidsanalyse. Aangezien voor de betrouwbaarheidsbehoefte alleen de afhankelijkheid van belang is (zie hoofdstuk vier), kan daar met de SPRINT methode uitstekend op aangesloten worden door te focussen op het deel afhankelijkheidsanalyse.

Een andere eigenschap waardoor de SPRINT methode goed aansluit bij de in hoofdstuk vier uitgewerkte betrouwbaarheidsbehoefte is dat onderscheid wordt gemaakt in de begrippen beschikbaarheid, integriteit en vertrouwelijkheid, zoals ik deze ook heb aangeduid als aspecten van betrouwbaarheid.

6.3.2 Gebruik van de SPRINT afhankelijkheidsanalyse in het kader van dit onderzoek

Ondanks de bovenstaande positieve eigenschappen (voor mijn onderzoek), sluit de methode op belangrijke punten niet direct aan bij de eisen die gesteld moeten worden aan een methode voor het bepalen van de betrouwbaarheidsbehoefte. De SPRINT methode is namelijk gericht op individuele informatiesystemen en niet op een organisatie als geheel. Voordat de SPRINT bruikbaar is om de betrouwbaarheidsbehoefte van een organisatie te bepalen zal de methode op deze punten moeten worden aangepast.

Ten eerste moet de SPRINT methode worden omgevormd om de betrouwbaarheidsbehoefte te bepalen voor de informatievoorziening als geheel in plaats van voor individuele informatiesystemen. Daartoe is het een mogelijkheid [een subset van] de informatiesystemen van een organisatie individueel te 'scoren' met SPRINT en die resultaten vervolgens te bundelen tot één score voor de gehele informatievoorziening. Deze laatste mogelijkheid leidt echter weer tot een complexiteit die ik nu juist probeer te vermijden. Een geschiktere mogelijkheid is om de vragen van de SPRINT methode aan te passen zodat de vragen worden gericht op de informatievoorziening en niet op een individueel informatiesysteem. Deze methode heeft mijn voorkeur, omdat dit de eenvoud van de methode niet aantast.

Tevens onderscheidt de SPRINT methode voor de beschikbaarheid, de integriteit en de vertrouwelijkheid vijf gradaties in plaats van de door mij gekozen drie. Dit pas ik in de methode

aan door de drie waarden te hanteren die ik in 5.4 heb beschreven. In bijlage C heb ik de vragenlijsten van SPRINT opgenomen met daarin deze twee aanpassingen verwerkt. In paragraaf 6.5 zal ik evalueren hoe deze aanpassingen in de praktijk blijken te werken.

Bij het voornoemde komt dat ISF zelf aangeeft dat SPRINT geschikt is voor belangrijke, maar niet voor kritische informatiesystemen. Omdat de methode echter gericht wordt op de informatievoorziening als geheel is dit mijns inziens echter geen onoverkomelijk punt. Binnen het geheel van de informatievoorziening en de betrouwbaarheidsbehoefte die daarbij hoort is volgens mij namelijk ruimte om per informatiesysteem een hogere of lagere beveiliging te richten. Daarmee kunnen ook kritische informatiesystemen individueel passend worden beveiligd terwijl de betrouwbaarheidsbehoefte als geheel globaal is vastgesteld met de aangepaste SPRINT methode.

Wel kan dit aspect impact hebben op de mate waarin de betrouwbaarheidsbehoefte van alle mogelijke organisaties kan worden bepaald. Omdat SPRINT niet geschikt is voor kritische informatiesystemen, zou het zo kunnen zijn dat met SPRINT niet de beveiligingsbehoefte is vast te stellen voor organisaties waarvoor de betrouwbaarheid van de informatievoorziening zeer kritisch is. Hieraan zal in paragraaf 6.5 verder aandacht worden besteed.

6.4 Gebruik van de SPRINT methode

Het uitvoeren van de afhankelijkheidsanalyse (“*Assess the level of business risk associated with an information system*”) is de eerste stap van de SPRINT methode. De afhankelijkheid wordt bepaald door de impact te bepalen van aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van een informatiesysteem. Binnen dit onderzoek wordt deze analyse geprojecteerd op de informatievoorziening als geheel. In deze paragraaf geef ik hoofdlijnen weer hoe de afhankelijkheidsanalyse volgens de SPRINT methode moet worden uitgevoerd. Voor detailinformatie verwijs ik naar de SPRINT User Guide [ISF1997].

6.4.1 Uitvoeren van de afhankelijkheidsanalyse

De SPRINT afhankelijkheidsanalyse wordt bij voorkeur uitgevoerd door een assessor die bekend is met security management samen met bedrijfsfunctionarissen verantwoordelijk voor de (beveiliging van) de informatievoorziening. De assessor kan bijvoorbeeld een bevei-

ligingsspecialist, een IT auditor, een internal auditor of security consultant zijn. Vanuit de betrokken organisatie dien één of meer personen betrokken te zijn die onderdeel zijn van het management en bekend zijn met het gebruik en eventueel de beveiliging van de informatie–voorziening. Hierbij kan worden gedacht aan een bestuurder met IT in de portefeuille, een Chief Information Officer of een IT manager.

In de analyse wordt per betrouwbaarheidsaspect een vragenlijst behandeld waarbinnen voor verschillende gevallen van aantasting van het betrouwbaarheidsaspect wordt bepaald wat de impacts is op de bedrijfsvoering. Voor elk van deze vragen wordt aangegeven welke impact de aantasting heeft op de bedrijfsvoering. De te hanteren vragenlijsten van SPRINT, vertaald naar het Nederlands en herschreven naar de informatievoorziening als geheel, zijn opgenomen in bijlage E. De assessor moet de bedrijfsfunctionaris begeleiden bij het bepalen van de waar–den, waarbij hij deze laatste stuurt op basis van de in 5.4 geschetste afbakeningen.

6.4.2 Bepalen van de overall afhankelijkheid per betrouw-baarheidsaspect

Aansluitend wordt de afhankelijkheid van het betrouwbaarheidsaspect voor het gehele beoor–deelde object (in mijn geval de gehele informatievoorziening) bepaald op basis van de gegeven antwoorden. Daarbij wordt door SPRINT op het niveau van het individuele informatiesy–steem de impact bepaald uitgaand van een *worst case scenario*. Dat betekent dat geneigd wordt naar de zwaarste score, aansluitend bij het motto ‘een ketting is zo sterk als de zwakste scha–kel’. Is dus op één van de vragen ‘hoog’ geantwoord, dan wordt de algehele afhankelijkheid van het beoordeelde informatiesysteem als hoog beoordeeld.

Voor de bepaling van de overall afhankelijkheid gericht op de informatievoorziening als geheel is het echter maar de vraag of dat de juiste manier is. Het betreft immers de organisatie als geheel en bepaalt de strengheid van het beveiligingsbeleid. Ook al is het antwoord op één van de vragen ‘Hoog’ dan betekent dat nog niet dat de gehele informatievoorziening een hoge afhankelijkheid kent. In veel gevallen zal dit juist een selectie van één of meer informatie–systemen betreffen. Indien gekozen wordt voor de zwaarste classificatie als maatstaf voor de gehele organisatie, kan de beveiliging te rigide worden.

Beter lijkt het bijvoorbeeld om de algehele classificatie afgewogen te kiezen, waarbij niet persé de hoogste classificatie wordt gekozen. Bij de tactische en operationele beveiliging van indi–

viduele informatiesystemen kan dan zwaarder of lichter worden beveiligd op basis van een detailrisicoanalyse. Om een volledig beeld te hebben van de mogelijkheden tot het bepalen van de overall afhankelijkheid per betrouwbaarheidsaspect worden onderstaand de mogelijkheden geëvalueerd.

Gemiddelde van de scores

Wanneer per betrouwbaarheidsaspect B, I en V het gemiddelde van alle antwoorden wordt genomen kan daarmee voor de organisatie de betrouwbaarheidsbehoefte per aspect worden bepaald. Simpel gezegd is dit dus het gemiddelde van alle resultaten per aspect. Voordeel van deze methode is dat een algemeen beveiligingsniveau wordt gegeven. Daar staat tegenover dat hoge of lage scores tegen elkaar weg kunnen vallen en onterecht de indruk kan ontstaan dat de organisatie een gemiddelde betrouwbaarheidsbehoefte heeft. Dit zou tot gevolg hebben dat de betrouwbaarheidsbehoefte niet aansluit bij de organisatie.

Gewogen gemiddelde van de scores

Hierbij wordt uitgegaan van de vorige methode maar dan met een weging per antwoord. Dit betekent dat hierbij ook het belang van iedere vraag wordt meegenomen in de bepaling van het risicoprofiel. Aangezien de afhankelijkheidsanalyse scores geeft aan voorbeeldsituaties van aantasting, kan het zijn dat sommige situaties relevanter zijn dan andere. Complicatie van deze methode is de vraag op basis waarvan deze weging plaats dient te vinden. Ook bestaat nog steeds het gevaar van gelijkwegende antwoorden die tegen elkaar wegvallen.

Maximum betrouwbaarheidsbehoefte

Een derde mogelijkheid is om de betrouwbaarheidsbehoefte te kiezen aan de hand van de hoogste waarde van de antwoorden, oftewel het hoogste betrouwbaarheidsbehoefte. Dit heeft tot gevolg dat de beveiliging altijd voldoende gedekt is. Nadeel is dat dit een enorme *overkill* kan geven wanneer er slechts één vraag een hoge score heeft en de rest een lage. Aangezien informatiebeveiliging een afweging is tussen risico en kosten lijkt dit niet de ideale oplossing.

Het gebruik van een gewogen gemiddelde laat ik, gezien de extra complexiteit van het gebruik van gewichten maar vooral wegens het ambigue vraagstuk van het toewijzen van gewichten, verder buiten beschouwing. In de proefanalyse van paragraaf 6.5 zal ik het gebruik in de praktijk van de maximum score en de gemiddelde score evalueren en op basis daarvan komen tot een definitieve keuze voor één van deze werkwijzen.

6.5 Proefanalyse met behulp van de aangepaste SPRINT methode

Teneinde de praktische bruikbaarheid van de SPRINT methode voor het vaststellen van de betrouwbaarheidsbehoefte te bepalen heb ik met materie–experts een proefanalyse uitgevoerd. Daartoe is een fictieve casus geschetst op basis van een praktijkvoorbeeld van een organisatie waarvoor beveiligingsbeleid moet worden opgesteld. In de casus, welke in z'n geheel is opgenomen in bijlage C, zijn de aard van de organisatie, diverse organisatiekenmerken en het gebruik van de informatievoorziening beschreven.

De materie–experts is gevraagd op basis van deze (beperkte) informatie de aangepaste SPRINT methode uit te voeren. Teneinde de scope beperkt te houden is daarbij alleen de vertrouwelijkheidsbehoefte bepaald, aangezien het een verkennend onderzoek betreft. Doel van de proefanalyse was te bepalen of de aangepaste SPRINT analyse geschikt is en voldoende kwaliteit biedt voor het bepalen van de betrouwbaarheidsbehoefte. Daartoe heb ik de volgende te evalueren kwaliteitscriteria opgesteld:

- **Stabiliteit:** zijn de vastgestelde betrouwbaarheidsbehoeften consistent?
- **Gebruiksgemak:** is de methode eenvoudig en prettig in gebruik?
- **Efficiëntie en effectiviteit:** is het gebruik van de methode efficiënt en effectief?
- **Detaillering:** Biedt de methode voldoende detail om de betrouwbaarheidsbehoefte vast te kunnen stellen?
- **Algehele geschiktheid:** is de methode geschikt om de betrouwbaarheidsbehoefte van een organisatie als geheel te beoordelen?

Tevens is de proefanalyse gebruikt om te bepalen op welke wijze het beste de eindwaarde per kwaliteitsaspect B,I,V kan worden bepaald. In bijlage D zijn de detailuitkomsten van dit onderzoek opgenomen, onderstaand volgen de belangrijkste uitkomsten.

Op basis van de uitkomsten van de uitgevoerde proefanalyses kan worden geconcludeerd dat de SPRINT methode zeker bruikbaar is om de betrouwbaarheidsbehoefte mee te bepalen. Weliswaar verschillen de antwoorden op detailvragen in enkele gevallen: in vier van de zeven vragen week één antwoord af, voor de overige drie vragen waren alle de antwoorden identiek. De vastgestelde algehele eindwaarden van de betrouwbaarheidsbehoefte zijn alle gelijk. De methode is derhalve binnen de proefanalyse consistent gebleken.

De consensus onder de materie–experts is dat de algehele eindscore per kwaliteitsaspect B,I,V dient te worden bepaald op basis van het volledige beeld van de detailantwoorden. Daarbij dient in aanmerking te worden genomen dat een hogere score zwaarder moet meewegen. Dit om te voorkomen dat onvoldoende wordt beveiligd, analoog aan het voorzichtigheidsprin–cipe. Op basis van dit uitgangspunt kunnen als hulpmiddel aan de antwoorden punten worden toegekend om dit verschillende gewicht tot uiting te laten komen. Daarbij is gekozen voor de volgende puntentoewijzing: Laag = 1, Middelmatig = 2, Hoog = 3. Dit leidt ertoe dat na beantwoording van de deelvragen een indicatieve score kan worden berekend. Wanneer deze score wordt gekoppeld aan de spectrumverdeling uit 5.3.2 ontstaat een concreet hulpmid–del om de eindscore te bepalen. Daarbij merk ik op dat ik de betrouwbaarheidsbehoefte, zoals eerder aangegeven, als niet wiskundige exacte waarde blijf zien. De getallen vormen puur een indicatie.

De materie–experts gaven aan de methode als prettig en eenvoudig te ervaren, met con–crete en relevante vragen . De vragenlijsten van SPRINT sluiten goed aan bij de aspecten die relevant zijn voor de betrouwbaarheidsbehoeften. Daarbij werd de vaststelling van de vertrouwelijkheidsbehoefte binnen de proefanalyse als efficiënt gekenmerkt. De effectiviteit is moeilijker te beoordelen, vanwege het feit dat de casus niet alle informatie bevat die in de praktijk ook beschikbaar zou zijn. Gebruik in de praktijk zal derhalve meer zekerheid moeten geven over de effectiviteit van de methode.

Bijkomend voordeel is volgens de experts dat de SPRINT methode sterk bijdraagt aan de betrokkenheid van het management, door hun directe betrokkenheid bij de uitvoering. Hen worden als het ware de ogen geopend voor de mate waarin hun organisatie afhankelijk is van informatie en de automatisering daarvan.

Ondanks dat de originele SPRINT methode niet geschikt is voor kritische informatie–systemen, is de hier gehanteerde vorm toch geschikt om te gebruiken voor de algehele betrouwbaarheidsbehoefte, omdat het over een algemene lijn gaat die per informatiesysteem nog aan te vullen/uit te werken is. De SPRINT methode wordt echter minder geschikt geacht om de betrouwbaarheidsbehoefte vast te stellen van grote organisaties die meerdere landen, meerder vestigingen en/of een complexe structuur hebben. De methode is meer geschikt voor kleine tot middelgrote bedrijven. Binnen grote complexe organisaties is de methode wel geschikt om de betrouwbaarheidsbehoefte van een lokatie, afdeling of divisie te bepalen.

De experts geven wel aan dat de methode een nuttige leidraad is, maar dat gebruik van expert–kennis altijd gewenst is. De expert zal tijdens het proces de vinger aan de pols moeten houden of de eindscore aansluit bij zijn/haar beeld van de organisatie en of de organisatie geen bijzonderheden of complexiteiten kent die het gebruik van de methode beïnvloeden. De experts zien de methode derhalve als hulmiddel dat het proces structureert en stuurt en dat als toetsing en vastlegging van hun eigen beeld (de expert knowledge) kan dienen.

Hiermee bestaat voldoende grond om de SPRINT methode te hanteren binnen de nagestreefde methode voor het systematisch opstellen van informatiebeveiligingsbeleid, onder voorwaarde van uitvoering met expert kennis. Uiteraard is deze proefanalyse slechts een beperkte toets, die vooral een indruk van de bruikbaarheid geeft. Teneinde meer zekerheid te verkrijgen over de stabiliteit en bruikbaarheid zullen meer en volledige toetsen plaats moeten vinden.

6.6 Conclusie

In dit hoofdstuk is onderzocht hoe de factoren die bepalend zijn voor het beveiligingsbeleid, de betrouwbaarheidsbehoefte, kunnen worden vastgesteld zodat op basis daarvan het beveiligingsbeleid kan worden opgesteld. Daarbij is teruggegrepen naar de in hoofdstuk vijf beschreven gewenste koppeling tussen waarden van de betrouwbaarheidsbehoefte en directe gekoppelde vormen van beveiligingsbeleid.

Om de waarde van de betrouwbaarheidsbehoefte – de triple (B,I,V) – vast te kunnen stellen is allereerst het gebruik van reguliere risicoanalyses onderzocht. Daarbij is aangegeven dat deze niet goed passen in de behoefte om de betrouwbaarheidsbehoefte efficiënt en effectief vast te stellen, omdat uitvoering gericht is op individuele informatiesystemen. Dit zal veel tijd en inzet vergen, waarbij tevens het combineren van alle resultaten tot één betrouwbaarheidsbehoefte een complexiteit op zichzelf vormt.

Als alternatief is het begrip ‘macrorisicoanalyse’ uitgewerkt, gericht op het analyseren van de risico’s waarvoor een organisatie zich geplaatst ziet op het hoogste niveau. Als concrete uitwerking van een macrorisicoanalyse is de SPRINT methode van het International Security Forum (ISF) beschreven. Deze methode is gericht op het snel en eenvoudig op hoofdlijnen bepalen van de afhankelijkheid en kwetsbaarheid van informatiesystemen middels vragenlijsten. Aangezien eerder is bepaald dat de betrouwbaarheidsbehoefte, die bepalend is voor de

invulling van het beveiligingsbeleid, in essentie bestaat uit de afhankelijkheid van de informatievoorziening, is alleen het deel 'afhankelijkheidsanalyse' van de SPRINT methode van belang.

De SPRINT methode is business georiënteerd, waarbij in samenwerking met managers de afhankelijkheid (en kwetsbaarheid) van informatiesystemen op hoofdlijnen worden bepaald. De SPRINT methode sluit nauw aan bij de doelen van dit onderzoek, met name de behoefte aan efficiëntie en effectiviteit. Door het karakter van hoofdlijnen is SPRINT volgens ISF echter niet geschikt voor kritische informatiesystemen. Daarbij komt dat SPRINT gericht is op informatiesystemen, terwijl de betrouwbaarheidsbehoefte voor een organisatie als geheel geldt.

De bruikbaarheid van de SPRINT methode als macro–risicoanalyse voor het opstellen van beveiligingsbeleid is op basis van een casus getoetst aan expert knowledge. Met drie experts is een proefanalyse uitgevoerd op een geschetste fictieve casus. Uit de proefanalyse komt naar voren dat de SPRINT methode geschikt is om te gebruiken binnen de te ontwikkelen methode voor het systematisch opstellen van informatiebeveiligingsbeleid. De methode biedt voldoende stabiliteit, gezien de gelijkheid in uitvoering door de experts.

Voorzichtigheid dient wel te worden betracht in geval van zeer grote of complexe organisaties, bijvoorbeeld met meerdere divisies of landenlocaties. In dat geval wordt de methode niet geschikt geacht om de betrouwbaarheidsbehoefte voor de organisatie als geheel te bepalen. In dat geval is de methode wel geschikt om te gebruiken per divisie of land. De experts benadrukken dat bij gebruik van de methode expert knowledge vereist is. De uitvoering en uitkomst van de methode moet altijd een wisselwerking zijn tussen het de methode en de expert. Een expert dient de uitkomsten en toepasbaarheid van de methode te toetsen aan het beeld dat hij/zijn heeft bij een organisatie. De methode kan worden gehanteerd als leidraad om het proces te structureren en leiden, maar kan niet worden gebruikt als geïsoleerd instrument zonder expert knowledge.

Van betrouwbaarheids-behoefte naar beveiligingsbeleid

7

"Ook bij intelligent gebruik van checklists moet altijd zorgvuldig worden overwogen welke maatregelen wel en welke niet moeten worden getroffen, afhankelijk van het belang van het te beschermen informatiesysteem voor de organisatie en de dreigingen waaraan dit systeem is blootgesteld."

dr. E.E.O. Roos Lindgreen [ROOS1998]

In hoofdstuk 6 is een systematiek geschetst voor het kwantificeren van de betrouwbaarheidsbehoefte. Daarbij is aangegeven dat een dergelijke kwantificering het mogelijk maakt om een directe relatie te leggen tussen de betrouwbaarheidsbehoefte en de invulling van het beveiligingsbeleid. Om uitvoering te kunnen geven aan deze relatie is niet alleen de kwantificering van de betrouwbaarheidsbehoefte vereist, maar dient ook te worden bepaald op welke wijze het beveiligingsbeleid van de gekwantificeerde betrouwbaarheidsbehoefte kan worden afgeleid. Dit laatste deel wordt in dit hoofdstuk uitgewerkt op basis van de volgende kernvraag:

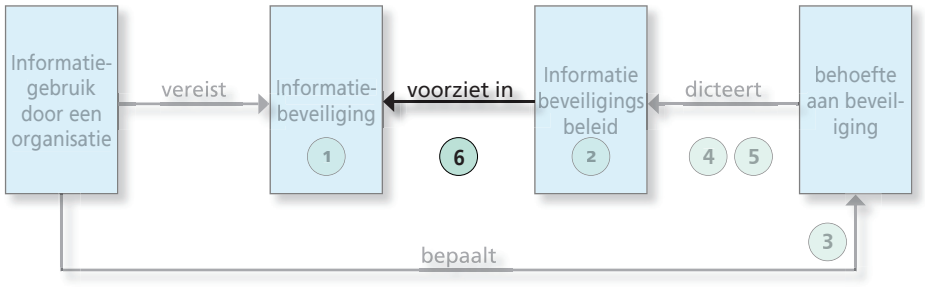
Kernvraag 6:

Op welke wijze kan de inhoud van het informatiebeveiligingsbeleid efficiënt en effectief worden afgeleid van de gekwantificeerde beveiligingsbeleid bepalende factoren zodat het beleid voorziet in de voor een organisatie benodigde informatiebeveiliging?

In hoofdstuk 5 en 6 is de doelstelling beschreven om de invulling van het beveiligingsbeleid direct te relateren aan de betrouwbaarheidsbehoefte. In paragraaf 7.1 wordt allereerst deze doelstelling gekoppeld aan de samenstelling van beveiligingsbeleid uit beschrijvende teksten en beveiligingsrichtlijnen. Die samenstelling is eerder in hoofdstuk 3 beschreven. In paragraaf 7.2 wordt vervolgens beschreven dat de in de kernvraag gezochte efficiëntie en effectiviteit kan worden bereikt middels de standaardisatie van beschrijvende teksten. Aansluitend wordt in paragraaf 7.3 een theoretisch kader geschetst voor de standaardisatie van beveiligingsrichtlijnen uitgewerkt, teneinde verdere invulling te geven aan de efficiëntie en effectiviteit.

Naar aanleiding van het in 7.3 geschetste theoretische kader is een verkennend onderzoek uitgevoerd naar het werkelijk standaardiseren van beveiligingsrichtlijnen. De resultaten daarvan zijn beschreven in paragraaf 7.4. Aansluitend wordt in paragraaf 7.5 op basis van de gestandaardiseerde beveiligingsrichtlijnen als praktijktoets de invulling van het beveiligingsbeleid bepaald voor de fictieve organisatie waarvoor in hoofdstuk 6 de betrouwbaarheidsbehoefte is bepaald. Tenslotte wordt in paragraaf 7.6 met materie-experts getoetst of het opgestelde aansluit bij de eerder bepaalde betrouwbaarheidsbehoefte.

Ter illustratie is in afbeelding 15 de plaats van deze kernvraag binnen het gehele onderzoek uitgelicht.



Figuur 15: De kernvraag van dit hoofdstuk is uitgelicht in het schema

7.1 Invulling van beveiligingsbeleid op basis van de betrouwbaarheidsbehoefte

In hoofdstuk 3 is aangegeven dat beveiligingsbeleid in essentie bestaat uit beveiligingsrichtlijnen, ingebed in prozaïsche beschrijvingen. Daarbij is beschreven dat mogelijkheden tot het systematiseren van het opstellen van beveiligingsbeleid liggen in enerzijds standaardisatie van beschrijvende teksten en anderzijds door standaardisatie van de selectie van op te nemen richtlijnen. Concreet betekent dit dat moet worden gezocht naar mogelijkheden om de keuze van beschrijvende teksten en beveiligingsrichtlijnen te koppelen aan de vastgestelde betrouwbaarheidsbehoefte.

Om dit mogelijk te maken moet aan de gestandaardiseerde teksten en richtlijnen een classificatie worden gekoppeld die aansluit bij de mogelijke waarden van de betrouwbaarheidsbehoefte zoals die in hoofstuk vijf zijn beschreven. Dat wil zeggen dat duidelijk moet zijn welke beschrijvende teksten en richtlijnen moeten worden gekozen indien de beschikbaarheidsbehoefte bijvoorbeeld hoog is. Daartoe dienen de mogelijke beschrijvende teksten en richtlijnen te worden gekenmerkt volgens dezelfde indeling als de mogelijke waarden van de betrouwbaarheidsbehoefte. Op die manier wordt de eerder beschreven één-op-één relatie mogelijk tussen de betrouwbaarheidsbehoefte en de invulling van het beveiligingsbeleid. In de volgende twee paragrafen wordt dit uitgewerkt voor respectievelijk de beschrijvende teksten en de beveiligingsrichtlijnen.

7.2 Standaardisatie van teksten

In hoofdstuk 3 is aangegeven dat de onderzochte voorbeelden van beveiligingsbeleid allemaal beschrijvende teksten bevatten, maar dat deze onderling verschillend zijn. Het is daarom zaak te bepalen in hoeverre de teksten kunnen worden gestandaardiseerd, zonder de bruikbaarheid van het beleid aan te tasten. Het standaardiseren van de prozaïsche beschrijvingen kan in elk geval niet volledig worden doorgevoerd omdat in dat geval het beleid veelal onvoldoende bij een organisatie zal passen. De praktijk is namelijk complexer en veelvormiger dan de hier gevolgde modelmatige aanpak kan beschrijven. Het is niet mogelijk om in standaard teksten te voorzien om alle mogelijk praktijksituaties af te dekken. Anderzijds is dat ook niet wenselijk, omdat het beleid specifiek van en voor een organisatie moet zijn, en het oplepelen van standaard teksten zal niet de beste manier zal zijn om personeel enthousiast te maken voor de boodschap ervan.

De onderzochte praktijkvoorbeelden wijzen wel uit dat grotendeels dezelfde onderdelen met beschrijvende teksten zijn opgenomen, zoals bijvoorbeeld de doestelling, de doelgroep, de plaats binnen de organisatie en dergelijke. Uit gesprekken met materie–experts blijkt, dat in de praktijk zelfs wel wordt uitgegaan van een standaard raamwerk van teksten dat voor elke organisatie in beginsel kan worden gebruikt. Wel worden daarbij de teksten, waar mogelijk, voorzien van extra of aangepaste teksten welke de 'eigenheid' van het beleid vergroten.

In de literatuur en diverse (bedrijfs)publicaties (whitepapers, toolkits et cetera) zijn diverse van dergelijke standaard teksten voor informatiebeveiligingsbeleid te vinden. Een voorbeeld is de NGI publicatie 'Beveiligingsbeleid en beveiligingsplan' [NGI1992], maar ook op inter–net is eenvoudig een groot aantal voorbeelden van beveiligingsbeleid (veelal in het Engels) te vinden. Het probleem van deze voorbeelden is dat ze enerzijds niet of niet volledig aan–sluiten bij de opbouw van beveiligingsbeleid zoals ik die in de voorgaande hoofdstukken heb ontwikkeld. Anderzijds is de autoriteit van de op internet circulerende voorbeelden veelal onduidelijk; het feit dat een voorbeeld of een template op internet is geplaatst betekent nog niet dat het dus ook een goed stuk betreft. Daarom heb ik geen van de beschikbare voorbeel–den gehanteerd als raamwerk binnen mijn methode.

Gezien het streven naar een pragmatische aanpak heb ik in het kader van dit onderzoek bij gebrek aan een geschikte template zelf een standaard tekstraamwerk (of blauwdruk) voor informatiebeveiligingsbeleid opgesteld dat aansluit bij de gekozen insteek van beveiligings–beleid. Dit raamwerk is gebaseerd op de verschillende literatuur en praktijkvoorbeelden die voorhanden waren. Het raamwerk is ondergebracht in bijlage D. In het raamwerk zijn de vereiste en meest voorkomende onderdelen van beveiligingsbeleid opgenomen zoals die in hoofdstuk 3 zijn beschreven. Het raamwerk is bedoeld als een kapstok om de uiteindelijke invulling van het beveiligingsbeleid aan op te hangen.

In elke situatie dat beveiligingsbeleid wordt opgesteld volgens deze methode kan dit raamwerk worden gebruikt als basis. Zoals aangegeven aan het begin van deze paragraaf is volledige standaardisatie van de beschrijvende teksten echter niet haalbaar en niet wenselijk. Daarom zal in de praktijk bij het opstellen van beveiligingsbeleid fine–tuning van de raamwerktekst moeten plaatsvinden. Hierbij dient elke keer te worden afgewogen of de tekst gepast is voor een organisatie en op welke wijze de tekst kan worden gewijzigd om de teksten meer op de organisatie af te stemmen.

In het raamwerk zijn in elk geval de standaard teksten opgenomen die in het overgrote- groot deel van de beschikbare praktijkvoorbeelden voorkomen of worden geadviseerd in de relevante literatuur (zie paragraaf 3.4 en bijlage A). Anderzijds zijn in het raamwerk teksten opgenomen die per praktijksituatie kunnen worden bijgesteld. Dit betreft in ieder geval de aanduiding van betrouwbaarheidsbehoefte van de organisatie. Dit is immers de kern waarop de invulling van het beveiligingsbeleid is gestoeld.

In de beschrijvende teksten zullen de bedrijfs-eigen kanten van het beveiligingsbeleid sterk naar voren moeten komen. Dit betreft onder andere de relatie met primair het informatiebe- leid en secundair met de ander gerelateerd beleidsgebieden (facilitair beleid, financieel beleid, personeelsbeleid; zie afbeelding 7 in paragraaf 3.2). De teksten kunnen hiernaar verwijzen en eventuele beperkingen, relevante wetgeving of voorwaarden uit deze gerelateerde beleidsge- bieden kunnen hierin worden weergegeven.

Ten aanzien van de beschrijving van de beveiligingsorganisatie als onderdeel van de beschrij- vende teksten moet wel een aanvullende kanttekening worden geplaatst. Ondanks dat nagenoeg alle onderzochte voorbeelden van beveiligingsbeleid de beveiligingsorganisatie beschrijven, verschilt de exacte invulling ervan namelijk per organisatie (aantal functies, benaming van functies, verdeling van verantwoordelijkheden et cetera). De optimale invul- ling van de beveiligingsorganisatie rechtvaardigt een onderzoek op zich. In het raamwerk is daarom een basale beveiligingsorganisatie beschreven op basis van de grootste gemene deler van de voorbeelden en de literatuur, zoals beschreven in paragraaf 2.4. Bij de werkelijke invulling dient de organisatie specifiek te worden gemaakt op basis van de betrokken organi- satie en relevante literatuur op dat specifieke gebied.

Het voorgaande samenvattend vormt het opgestelde raamwerk niet *out-of-the-box* het per- fecte beveiligingsbeleid. Het vormt echter wel een goede basis welke in de praktijk tijdens het gebruik per organisatie kan worden gefinetuned.

7.3 Standaardisatie van beveiligingsrichtlijnen

Naast standaardisatie van beschrijvende teksten kan het opstellen van beveiligingsbeleid ook worden gesystematiseerd door de in het beveiligingsbeleid te stellen richtlijnen te koppelen aan de vastgestelde beveiligingsbehoefte. Dit betekent dat moet worden bepaald bij welke beveiligingsbehoefte welke beveiligingsrichtlijnen van toepassing zijn. Om dit te bereiken

dienen twee stappen te worden genomen. Ten eerste moet een universum van beveiligingsrichtlijnen worden bepaald waaruit richtlijnen gekozen kunnen worden voor een bepaalde beveiligingsbehoefte. Ten tweede moet worden bepaald in welk geval (bij welke betrouwbaarheidsbehoefte) welke richtlijn van toepassing is. Deze twee stappen worden hierna verder uitgediept.

7.3.1 Samenstellen van een universum van informatiebeveiligingsrichtlijnen

Om het mogelijk te maken richtlijnen te kiezen bij een specifieke beveiligingsbehoefte dient dus allereerst een verzameling beveiligingsrichtlijnen te bestaan waaruit gekozen kan worden. Een dergelijk universum kan bijvoorbeeld worden opgebouwd uit de beschikbare voorbeelden van beveiligingsbeleid. Daarnaast zijn diverse boeken en rapporten beschikbaar die voorbeeldrichtlijnen bevatten. Voorbeelden van werken die hiervoor geschikt zijn:

- *Informatiebeveiliging in de praktijk,* RCC [RCC1999]
  Dit boekje is bedoeld als praktische handreiking voor het uitvoering geven aan informatiebeveiliging, door een verzameling voorbeeldrichtlijnen en –maatregelen te beschrijven.
- *Code voor Informatiebeveiliging*, NNI [NNI2000]
  Dit document is reeds beschreven in paragraaf 2.x
- *Information Security Policies made easy,* Charles Cresson Wood [WOOD1994]
  Dit boek is één grote verzameling van voorbeeld beveiligingsrichtlijnen, verdeeld naar onderwerp.

Deze werken leveren een grote hoeveelheid kant en klare richtlijnen aan (soms neigend naar maatregelen), maar daarbij wordt echter niet ingegaan op het systematisch kiezen van richtlijnen op basis van de behoeften van een organisatie. Ondanks dat voldoende voorbeeldrichtlijnen beschikbaar zijn moet de aansluiting bij de betrouwbaarheidsbehoefte derhalve nog worden gemaakt. In de volgende paragraaf wordt daarop verder ingegaan.

7.3.2 Classificeren van de richtlijnen in het universum

Om de beveiligingsrichtlijnen aan de betrouwbaarheidsbehoefte te kunnen koppelen dienen de beveiligingsrichtlijnen te worden geclassificeerd volgens hetzelfde principe als de betrouw–

baarheidsbehoefte (zoals beschreven in hoofdstuk 5 en 6). Alleen dan kan een directe relatie worden gelegd tussen de betrouwbaarheidsbehoefte en de invulling van de richtlijnen. Dit betekent dat per beveiligingsrichtlijn dient te zijn aangegeven op welke beveiligingsbehoefte deze betrekking heeft.

Aangezien de betrouwbaarheidsbehoefte bestaat uit de aspecten beschikbaarheid, integriteit en vertrouwelijkheid dienen ook alle richtlijnen te worden geclassificeerd naar deze drie aspecten. In concreto zal dus voor elke richtlijn moeten worden vastgesteld of deze van toepassing is voor een lage, middelmatige of hoge beschikbaarheids–, integriteits– en vertrouwelijkheids behoefte. Elke richtlijn krijgt dus een label $R_{(B,I,V)}$. Omdat de classificatie van de betrouwbaarheidsbehoefte oplopend is (Laag – Midden – Hoog), geldt dat richtlijnen van toepassing zijn vanaf een bepaalde classificatie. Dat wil zeggen dan een richtlijn die van toepassing is bij een classificatie 'Laag' ook van toepassing zal zijn voor de classificaties 'Midden' en 'Hoog'.

7.3.3 Volledigheid van het universum

Wanneer een universum van beveiligingsrichtlijnen wordt samengesteld, dan moet daarbij worden afgewogen wat de kwaliteit van het universum is. De verzameling richtlijnen moet bruikbaar zijn en die bruikbaarheid moet ook te bepalen zijn. Onder kwaliteit van het universum kunnen daar diverse kwaliteitsaspecten voor worden erkend. Om te beginnen zal bekend moeten zijn in hoeverre het universum volledig is. Om kwalitatief hoogstaand beveiligingsbeleid op te kunnen stellen moeten namelijk voldoende beveiligingsrichtlijnen beschikbaar zijn om in alle aspecten en behoeften van het beleid te kunnen voldoen. Het bereiken van absolute volledigheid van het universum is gezien de complexiteit van het onderwerp (zie ook 7.2) niet realistisch. Er is altijd ruimte voor nieuwe of nog niet opgenomen richtlijnen.

Ondanks deze beperking kan wel worden gezocht naar mogelijkheden om de volledigheid van het universum inzichtelijk te maken, opdat kan worden vastgesteld dat het universum voldoende gevuld is om in alle behoeften en aspecten van beveiligingsbeleid te voorzien. Allereerst is er de betrouwbaarheidsbehoefte, welke is opgebouwd uit de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Goed beveiligingsbeleid zal richtlijnen gericht op deze drie deze kwaliteitsaspecten moeten bevatten. In paragraaf 7.3.2 is reeds aangegeven dat aan de beveiligingsrichtlijnen een classificatie $R_{(B,I,V)}$ moet worden toegekend om selectie op

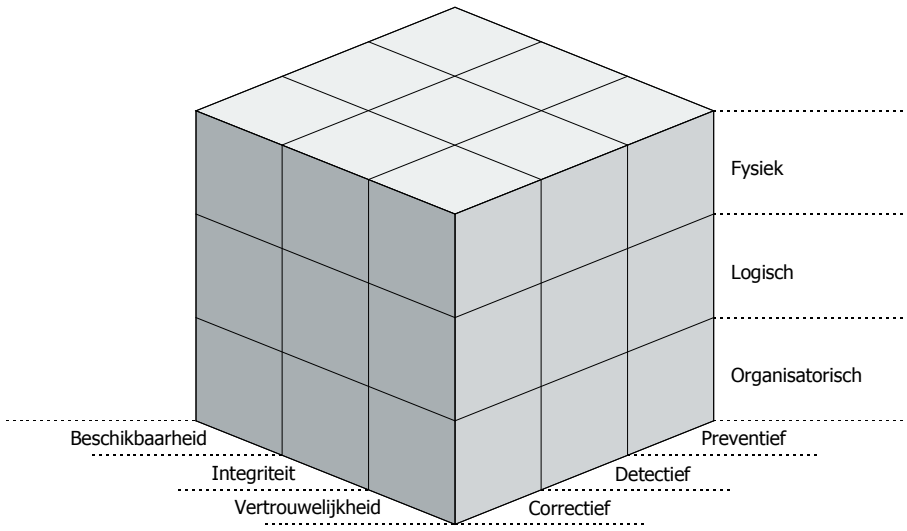
basis van de betrouwbaarheidsbehoefte mogelijk te maken. Deze classificatie kan gebruikt worden om te bepalen hoe de verzamelde richtlijnen verdeeld zijn over de drie kwaliteitsaspecten.

Naast de betrouwbaarheidsbehoefte (en daarmee de kwaliteitsuitwerking van een richtlijn) kennen beveiligingsrichtlijnen (maar ook beveiligingsmaatregelen) nog twee andere veel gehanteerde eigenschappen, te weten de werkingssfeer en de aard ([OVER2000], [RCC1996], [STAR1997]) De werkingssfeer betreft het werkingsgebied waarop een richtlijn gericht is, onderverdeeld in fysieke beveiliging, logische beveiliging en organisatorische beveiliging. De aard betreft het moment waarop richtlijnen van kracht worden in relatie tot het optreden van een verstoring, onderverdeeld in preventief, detectief en correctief. Correctieve richtlijnen zijn zowel gericht op het beperken van schade (repressief) als het herstellen van schade (reconstructief). Ook voor deze beide eigenschappen kan worden vastgesteld of alle 'waarden' voldoende worden afgedekt. Daartoe zal voor de richtlijnen in het universum moeten worden bepaald wat hun aard en werkingssfeer is.

De betrouwbaarheidsbehoefte, aangevuld met de werkingssfeer en de aard, kunnen worden gezien als drie dimensie van het universum van beveiligingsrichtlijnen. Aangezien elk van deze eigenschappen drie 'waarden' heeft, kan het universum van beveiligingsrichtlijnen in 3×3×3=27 categorieën worden verdeeld. In figuur 16 zijn deze drie dimensies van het universum grafisch weergegeven. Wanneer per partje aannemelijk kan worden gemaakt dat deze afdoende is beveiligd dan kan daarmee aannemelijk gemaakt dat alle dimensie van het universum voldoende zijn afgedekt en het universum derhalve volledig is.

Overigens is het eenvoudig te beredeneren dat bij het samenstellen van het universum het zwaartepunt (meerendeel) van de richtlijnen zal liggen in de preventieve kant. Organisaties zullen bij het inrichten van hun beveiliging immers het adagium 'voorkomen is beter dan genezen' aanhangen. Daarbij geldt wel dat de kosten van preventie nooit hoger zullen zijn dan de mogelijke schade van een incident. In dat geval is het immers goedkoper om het risico te nemen.

Naast volledigheid zijn er nog andere criteria waarop de kwaliteit van het samen te stellen universum kan worden beoordeeld. Zo zullen de richtlijnen in het universum consistent moeten zijn, (de ene richtlijn mag niet verbieden wat een andere richtlijn vereist). Daarnaast moeten allen richtlijnen een redelijke gelijke mate van abstractie hebben (het moet gaan om richtlijnen, niet om maatregelen). Verder moet duidelijkheid bestaan over onderlinge afhan-



Figuur 16: Dimensies van het universum van beveiligingsrichtlijnen

kelijkheid van richtlijnen; richtlijnen dienen óf volledig disjunct te zijn, óf er dient duidelijk te zijn welke richtlijnen onderling afhankelijk zijn en derhalve niet individueel kunnen worden opgenomen.

7.4 Verkennend onderzoek naar het samenstellen van het universum van richtlijnen

Teneinde de haalbaarheid en bruikbaarheid van het idee om een 'universum van richtlijnen' samen te stellen te bepalen heb ik een verkennend onderzoek uitgevoerd. Daarbij heb ik beveiligingsrichtlijnen verzameld om een (deel van) een universum van beveiligingsrichtlijnen samen te stellen. Om de scope te beperken tot wat binnen een afstudeeronderzoek haalbaar is, heb ik mij gericht op één deelgebied van informatiebeveiliging, te weten richtlijnen gericht op fysieke beveiliging.

7.4.1 Verzamelen van beveiligingsrichtlijnen

Zoals reeds in 7.3 is beschreven, zijn diverse bronnen beschikbaar met bruikbare beveiligingsrichtlijnen. Ik zal de Code voor Informatiebeveiliging gebruiken om het deeluniversum op te bouwen omdat dit een algemeen aanvaarde standaard is die direct bruikbare richtlijnen biedt. De samengestelde lijst van beveiligingsrichtlijnen is ondergebracht in bijlage E. (In de richtlijnen worden soms functionarissen genoemd. Ik heb deze herschreven naar de functionarissen zoals die voor komen in de standaard beveiligingsorganisatie die ik in hoofdstuk heb opgenomen.)

Bij het samenstellen van een volledig universum verdient het aanbeveling niet alleen de Code voor Informatiebeveiliging als bron te nemen, maar ook de andere in 7.3 genoemde bronnen. In dat geval is wegens de verschillende bronnen wel nadrukkelijk aandacht nodig voor waarborging van de in 7.3 genoemde kwaliteitsaspecten van het universum. Voor elke richtlijn zal bijvoorbeeld afgewogen moet worden of deze voldoende abstractieniveau heeft om als richtlijn te kunnen worden geclassificeerd en of het abstractieniveau aansluit bij de andere richtlijnen.

7.4.2 Classificeren van beschikbare richtlijnen

Bij het koppelen van richtlijnen aan betrouwbaarheidsclassificaties is geen wiskundige exactheid te gebruiken. Ik heb ervoor gekozen de classificatie van richtlijnen te baseren op de kennis en ervaring van materie–experts. Daarbij heb ik in overleg met de materie–experts aan elke richtlijn een classificatie toegekend op basis van consensus. Hierbij is door mijzelf als eerste een classificatie gegeven per richtlijn, waarna drie materie–deskundigen de scores hebben geïnterpreteerd en eventueel aangepast. De uiteindelijke consensus die uit dit proces is voortgekomen is per richtlijn aangegeven in bijlage E.

Per richtlijn is op basis van deze excercitie aangegeven bij welke beveiligingsbehoefte hij van toepassing is, gesplitst naar beschikbaarheid, integriteit en vertrouwelijkheid. Dat wil zeggen dat bij elke richtlijn is aangegeven vanaf welke waarde van respectievelijk de beschikbaarheidsbehoefte, de integriteitsbehoefte en de vertrouwelijkheidsbehoefte de richtlijn van toepassing is. Wanneer aan een richtlijn de classificatie $R_{(B,I,V)}$=(L,M,M) is gekoppeld, dan is deze van toepassing voor iedere organisatie waarvoor de beschikbaarheidsbehoefte L (laag) of hoger is of waarvoor de integriteitsbehoefte of de vertrouwelijkheidsbehoefte M (middelmatig) of hoger is.

Het classificeren van de richtlijnen bleek in de gekozen consensus–discussie over het algemeen een eenduidige uitkomst op te leveren. In geen geval bestond er een tegenstelling tussen de experts waarbij iemand H en iemand L koos. In enkele gevallen van discussie tussen twee waarden (L of M danwel M of H) werd consensus snel bereikt. Het classificeren op basis van consensus is dus relatief soepel verlopen. Daarbij moet worden opgemerkt dat ook hier sprake is van een classificatie op basis van een beperkte testgroep en een fictieve casus.

De materie–experts geven echter wel aan dat bij gebruik in de praktijk de keuze van een richtlijn op basis van de hier toegekende score niet bindend hoeft te zijn. De reden hiervoor is dat het heel wel mogelijk is dat zich in de praktijk gevallen voordoen waarin de voorgeschreven classificatie toch niet aansluit bij de organisatie. Hiermee wordt gesteld dat de aangegeven classificaties naar verwachting gepast zullen zijn voor de meeste organisaties, maar dat altijd uitzonderingen kunnen bestaan waar de standaard classificatie passend zal zijn. Dit is inherent aan de basering van de methode op expert–kennis en het niet ontwikkelen van een beveiligingsbeleid genererende *black box*.

Tijdens het classificeren van de richtlijnen kwam naar voren dat de keuze voor drie categorieën L, M en H soms wat te beperkend is. Sommige richtlijnen liggen vrij ver op het spectrum van beveiligingsbehoeften (meer dan gewoon hoog). Een extra categorie voor ‘zeer hoog’ zou daarom nuttig kunnen zijn. Wat verder opvalt aan de hier geclassificeerde richtlijnen voor fysieke beveiligingsmaatregelen is dat deze in veel gevallen op alle drie de kwaliteitsaspecten werken. De assessoren hebben geven echter aan dat dit vooral dit specifieke onderdeel betreft. Andere categorieën richtlijnen zullen meer diversiteit in hun kwaliteitsuitwerking hebben.

7.5 Proefinvulling van het beveiligingsbeleid op basis van de betrouwbaarheidsbehoefte

7.5.2 Selectie van richtlijnen voor de casusorganisatie

Op basis van het geclassificeerde universum van beveiligingsrichtlijnen en de eerder bepaalde betrouwbaarheidsbehoefte van de fictieve casusorganisatie kan nu bepaald worden hoe het (partiële) beveiligingsbeleid van de casusorganisatie zou moeten worden ingevuld. In hoofdstuk 6 is bepaald dat de casusorganisatie een hoge vertrouwelijkheidsbehoefte heeft. In bijlage

E is per richtlijn in de derde kolom met een asterix (*) aangegeven of de richtlijn op basis van de kwalificatie van toepassing is voor de casusorganisatie. Aangezien de vertrouwelijkheidsbehoefte hoog is, zijn dit alle richtlijnen waaraan de score L, of H is toegekend voor vertrouwelijkheid.

Hierbij kan het voor komen dat bepaalde richtlijnen op basis van alleen de vertrouwelijkheidsbehoefte niet worden geselecteerd. Dit kan op het eerste gezicht een vreemde indruk wekken. Dit betekent echter niet dat deze richtlijnen in geen geval van toepassing zijn voor de casusorganisatie. Bij een 'normale' volledige exercitie van het opzetten van beveiligingsbeleid worden ook de beschikbaarheids- en integriteitsbehoefte opgenomen, op basis waarvan andere richtlijnen ook kunnen worden geselecteerd.

7.5.2 Kwaliteit van de gemaakte richtlijnenselectie

De kwaliteit (juistheid) van de gemaakte selectie is nog onduidelijk; het is nog niet zeker dat de geselecteerde richtlijnen ook gepast zijn voor de casusorganisatie. Teneinde de kwaliteit van het eindproduct van de uitgevoerde methode te bepalen heb ik de proef op de som genomen. Na selectie van de richtlijnen heb ik met de eerder geraadpleegde materie-experts in groepsverband geëvalueerd of deze richtlijnen passen bij de proeforganisatie. Daarbij is afgewogen of de gekozen richtlijnen allen echt 'gewenst' zijn op basis van kennis die vanuit de casus over de organisatie bestaat. Hierbij moet worden benadrukt dat alleen is gekeken naar het aspect vertrouwelijkheid. De vraag die in essentie per richtlijn is gesteld, is: "is het terecht dat deze richtlijn is geselecteerd, gezien de vertrouwelijkheidsbehoefte van de casusorganisatie".

Dit vormt ten eerste een indicatie van de behoefte om de classificatie van richtlijnen verder te verbeteren. Ten tweede is het een indicatie in hoeverre de richtlijnen na selectie voor het beveiligingsbeleid op basis van de betrouwbaarheidsbehoefte nog globaal moeten worden beoordeeld op hun gewenstheid. Dit laatste grijpt weer terug naar hetgeen hierover in paragraaf 7.4.2 is geschreven. Uiteraard hangen deze twee aspecten samen: een betere classificatie kan ertoe leiden dat minder bijstelling achteraf nodig is.

De uitkomsten van de toetsing zijn per richtlijn in bijlage E opgenomen in de derde kolom in de vorm van een + (terecht geselecteerd) of een – (ten onrechte geselecteerd). Uit de toetsing komt naar voren dat het overgrote deel van de richtlijnen (32 van de 39) in de selectie als

terecht geselecteerd wordt aangemerkt. Van de zeven richtlijnen die niet als 'terecht' zijn aangemerkt zijn er 2 aangemerkt als 'niet relevant voor deze organisatie' en 5 als 'te stringent voor deze organisatie'.

De afwijzingen van de eerste categorie zijn te wijten aan het feit dat de casusorganisatie niet of nauwelijks goederen ontvangt, waardoor richtlijnen gericht op een afzonderlijke goederenontvangstruimte niet relevant zijn. De vijf te stringent geachte richtlijnen zijn in twee categorieën te verdelen, namelijk te stringent gezien de aard van de organisatie en te stringent gezien de vetrouwelijkheid van de gegevens. De eerste wordt veroorzaakt doordat het hier een kleine organisatie betreft alle medewerkers elkaar goed kennen en binnen de organisatie nauwelijks verschillen in toegang tot vertrouwelijke informatie bestaan. Daardoor zijn visuele identificatie van medewerkers en steekproeven op meegenomen bedrijfsmiddelen beperkt relevant. Ook is de kans op intern uitlekken van informatie zo beperkt dat extra afscherming van post en faxverkeer niet relevant wordt geacht.

De afwijzingen van de tweede categorie hebben betrekking op de vertrouwelijkheid van informatieuitwisseling via datakabels. Deze worden te stringent geacht omdat de kans op het afvangen van informatie via datakabels klein wordt geacht, mede gezien de vetrouwelijkheid van de gegevens die erover worden gecommuniceerd. De informatie is dus niet vertrouwelijk genoeg om dit beperkte risico af te dekken.

Gezien dit alles kom ik tot de conclusie dat de gehanteerde selectiemethode in grote lijnen acceptabel werkt. De niet relevant geachte richtlijnen zijn weliswaar niet geheel relevant, maar zijn ook niet schadelijk voor het beleid of de organisatie. Het alsnog verwijderen hiervan is een verdere optimalisatie van de effectiviteit van het opgestelde beleid. Het is moeilijk om in de selectiemethode een selectiecriterium op te nemen dat hier rekening mee houdt. Behalve het hier bepalende aspect van de goederenontvangstruimte zullen andere organisaties namelijk weer op andere punten afwijken van een gemiddelde organisatie en het is onbegonnen werk om met alle uitzonderingen rekening te houden.

De impact van de te stringent geachte richtlijnen is groter, omdat deze onnodig hoge eisen aan de organisatie zouden stellen. Voor zo ver deze veroorzaakt worden door de aard van de organisatie zou kunnen worden onderzocht of criteria gerelateerd aan de aard van een organisatie (bijvoorbeeld formeel/informeel of klein/gemiddeld/groot) kunnen worden ingebouwd in de methode. Voor zover de te stringente richtlijnen worden veroorzaakt doordat de vertrouwelijkheid van de informatie niet hoog genoeg wordt geacht, kan worden overwogen

een extra waarde (bijvoorbeeld 'zeer hoog') aan de mogelijke waarden toe te voegen. Dit maakt het gebruik van de methode echter weer omslachtiger, waardoor een gedegen afweging zal moeten worden gemaakt tussen de verbetering in effectiviteit en de vermindering van de efficiëntie.

7.5.3 Efficiëntie van de gevolgde selectiemethode

Naar aanleiding van de evaluatie van het proefbeleid kan de vraag gesteld worden of het niet efficiënter en/of effectiever zou zijn om de stap van het bepalen van de betrouwbaarheidsbehoefte over te slaan en direct per mogelijke beveiligingsrichtlijn te evalueren of deze gewenst (vereist) is voor de betreffende organisatie. In dat geval zou echter het nut worden geëlimineerd van de eerste grove selectie op basis van de betrouwbaarheidsbehoefte. Dan zou namelijk iedere richtlijn door de expert opnieuw moeten worden beoordeeld op relevantie voor de betrokken organisatie. Zowel de (impliciete) inschatting van de beveiligingsbehoefte van de organisatie als (ongestructureerde) keuze van de richtlijnen zouden telkens opnieuw moeten worden uitgevonden. Het is mijn overtuiging dat de inspanning voor het gestructureerd vaststellen van de betrouwbaarheidsbehoefte ruim overtroffen wordt door de winst in efficiëntie en effectiviteit.

Een nog belangrijker punt van het overslaan van de expliciete classificatie van organisaties en richtlijnen is dat dan de in de classificatie van de richtlijnen bevatte expert–knowledge buiten beschouwing worden gelaten. De betrokken expert moet bij zijn afweging van richtlijnen namelijk telkens zelf op basis van alleen zijn eigen kennis en ervaring een inschatting maken van de toepasbaarheid van een richtlijn. Dit kan ten koste gaan van zowel de efficiëntie als de effectiviteit van de werkzaamheden. Wanneer wel gebruik gemaakt wordt van reeds geclassificeerde richtlijnen, dan ligt daarin waardevolle expert–kennis besloten die de betrokken expert ondersteunt in zijn beslissingen.

Het is in aanvulling op het bovenstaande belangrijk nog te stellen dat het kiezen van richtlijnen ondanks de geïncorporeerde expert–kennis geen wiskundige aangelegenheid is, maar deels een kwestie blijft van interpretatie door de betrokkenen. De richtlijnen die op basis van de betrouwbaarheidsbehoefte worden geselecteerd, dienen daarom na selectie te worden getoetst. Daarnaast dient te worden bepaald door de auditor of er geen omissies zijn doordat het bedrijf op bepaalde punten sterk afwijkt van het gemiddelde. Dat hoeft geen evaluatie van alle niet gekozen richtlijnen te zijn, maar vooral een inschatting op basis van *professional judgement* of het beleid volledig is en niet tekort schiet op bepaalde vlakken.

7.5 Conclusie

Op basis van de in hoofstuk zes ontwikkelde methode om de beveiligingsbehoefte van een organisatie te bepalen is in dit hoofdstuk daarop aansluitend onderzocht hoe het beveiligingsbeleid kan worden ingevuld op basis daarvan. Daarbij is aangegeven dat dit mogelijk wordt middels de standaardisatie van de mogelijke onderdelen van beveiligingsbeleid, te weten beschrijvende teksten en beveiligingsrichtlijnen.

Standaardisatie van beschrijvende teksten kan niet volledig plaatsvinden, omdat deze het karakter van het bedrijf weerspiegelen in het beveiligingsbeleid en beleid 'eigen' maken voor een organisatie. Wel is het mogelijk een standaard raamwerk te gebruiken als uitgangspunt voor de beschrijvende teksten. Dit raamwerk biedt een voorbeeldstructuur en teksten die op basis van de analyse van beveiligingsbeleid in hoofdstuk drie als standaard onderdelen zijn geïdentificeerd. Naar aanleiding van dit hoofdstuk is in de appendices zo'n raamwerk opgenomen.

Een specifiek onderdeel van het raamwerk dat nadere toelichting vereist is de informatiebeveiligingsorganisatie. In het raamwerk is daarom een basale beveiligingsorganisatie beschreven op basis van de grootste gemene deler van de voorbeelden en literatuur. Bij de werkelijke invulling dient de organisatie specifiek te worden gemaakt op basis van de betrokken organisatie en relevante literatuur op dat specifieke gebied.

De standaardisatie van beveiligingsrichtlijnen kan concreter worden uitgevoerd. Om standaardisatie van beveiligingsrichtlijnen mogelijk te maken is allereerst een verzameling van alle mogelijke richtlijnen vereist: het universum van beveiligingsrichtlijnen. Dit universum van mogelijke richtlijnen vormt de basis voor maken van de selectie van beveiligingsrichtlijnen die in het beveiligingsbeleid moeten worden opgenomen.

Omdat in hoofdstuk zes is bepaald dat de invulling van beveiligingsbeleid wordt bepaald door de betrouwbaarheidsbehoefte, is gekozen om de keuze van beveiligingsrichtlijnen daarop aan te laten sluiten. Daartoe moeten alle beveiligingsrichtlijnen in het universum worden geclassificeerd volgens dezelfde indeling als de betrouwbaarheidsbehoefte. Concreet betekent dit dat aan alle beveiligingsrichtlijnen een classificatie $R_{(B,I,V)}$ moet worden gekoppeld die aangeeft bij welke betrouwbaarheidsbehoefte een richtlijn van toepassing is. Aansluitend kan door koppeling van de voor een organisatie vastgestelde betrouwbaarheidsbehoefte aan de richtlijnen met een overeenkomstige classificatie.

Teneinde inzicht te verkrijgen in de toepasbaarheid van deze werkwijze is met materie–experts een praktijktoets uitgevoerd op zowel het classificeren van richtlijnen als het op basis van de classificatie samenstellen van beveiligingsbeleid. Hieruit is gebleken dat de voorgestelde methode praktisch bruikbaar is. Daarbij is echter wel aangegeven dat de toegekende classificatie op basis van de beperkte testgroep en de fictieve casus door gebruik in de praktijk verder geoptimaliseerd kan worden.

Naar aanleiding van de evaluatie van het proefbeleid kan de vraag gesteld worden of het niet efficiënter en/of effectiever zou zijn om de stap van het bepalen van de betrouwbaarheidsbehoefte over te slaan en direct per mogelijke beveiligingsrichtlijn te evalueren of deze gewenst (vereist) is voor de betreffende organisatie. In dat geval zou echter het nut worden geëlimineerd van de eerste grove selectie op basis van de betrouwbaarheidsbehoefte. Dan zou namelijk iedere richtlijn door de expert opnieuw moeten worden beoordeeld op relevantie voor de betrokken organisatie. Zowel de (impliciete) inschatting van de beveiligingsbehoefte van de organisatie als (ongestructureerde) keuze van de richtlijnen zouden telkens opnieuw moeten worden uitgevonden. Het is mijn overtuiging dat de inspanning voor het gestructureerd vaststellen van de betrouwbaarheidsbehoefte ruim overtroffen wordt door de winst in efficiëntie en effectiviteit.

Het belangrijke voordeel van de classificatie van richtlijnen is dat in de classificatie van de richtlijnen expert–knowledge besloten ligt die uitvoerende experts ondersteunt bij hun werkzaamheden. De betrokken expert hoeft daardoor niet telkens zelf op basis van alleen zijn eigen kennis en ervaring een inschatting maken van de toepasbaarheid van een richtlijn. Daarbij is wel aangegeven dat de selectie van beveiligingsrichtlijnen op basis van de classificaties en de betrouwbaarheidsbehoefte niet 100% bindend hoeft te zijn. In de praktijk kunnen zich situaties voordoen waarin de standaard classificatie niet gepast is. Derhalve moet de geselecteerde richtlijnen altijd globaal worden beoordeeld op wenselijkheid, op basis van *professional judgement* van de betrokken expert(s).

Conclusies en aanbevelingen

Na de beantwoording van alle kernvragen kan nu de probleemformulering van het onderzoek worden geëvalueerd. Daartoe bundelt dit hoofdstuk de antwoorden die in de verschillende hoofdstukken zijn gegeven op de kernvragen tot een antwoord op de probleemstelling en een toelichting op de realisatie van de doelstelling. Aansluitend zal ik in de aanbevelingen ingaan op de facetten van het onderwerp informatiebeveiligingsbeleid die ik in mijn onderzoek niet heb meegenomen maar die wel relevant kunnen zijn voor verbreding of uitbreiding van dit onderzoek.

8.1 Conclusie

Allereerst zal ik in de conclusie ingaan op de beantwoording van de in hoofdstuk 1 geformuleerde probleemstelling en aansluitend de realisatie van de geformuleerde doestelling evalueren.

8.1.1 Beantwoording van de probleemstelling

In dit afstudeeronderzoek is de volgende probleemstelling uitgewerkt:

> *Welke factoren zijn voor een organisatie bepalend voor de invulling van het informatiebeveiligingsbeleid, in welke mate zijn deze factoren bepalend en op welke wijze is het mogelijk het informatiebeveiligingsbeleid voor een organisatie systematisch van deze factoren af te leiden?*

De uitkomst van mijn onderzoek is dat de invulling van het informatiebeveiligingsbeleid wordt bepaald door de zogenaamde betrouwbaarheidsbehoefte, welke een maat is voor de afhankelijkheid van een organisatie van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.

De betrouwbaarheidsbehoefte heeft invloed op de keuze en invulling van de onderdelen van beveiligingsbeleid, te weten beschrijvende teksten en beveiligingsrichtlijnen. De betrouwbaarheidsbehoefte is bepalend voor de mate waarin deze onderdelen stringent zijn. Anders gezegd: de betrouwbaarheidsbehoefte bepaalt hoe streng het informatiebeveiligingsbeleid van een organisatie moet zijn.

De invulling van het beveiligingsbeleid kan van de betrouwbaarheidsbehoefte worden afgeleid door het standaardiseren van de genoemde onderdelen van beveiligingsbeleid: beschrijvende teksten en beveiligingsrichtlijnen. Om dit mogelijk te maken is het vereist om de standaard onderdelen te koppelen aan de betrouwbaarheidsbehoefte op basis van een gelijke classificatie. Dit betekent dat zowel de betrouwbaarheidsbehoefte als de standaard onderdelen in bepaalde klassen moeten worden ingedeeld, waarna bepaalde standaard onderdelen kunnen worden gekoppeld aan bepaalde waarden van de betrouwbaarheidsbehoefte.

De betrouwbaarheidsbehoefte kan in klassen worden ingedeeld door deze te kwantificeren (meetbaar te maken) voor de onderdelen beschikbaarheid, integriteit en vertrouwelijkheid. Deze kwantificering leidt tot een beperkt aantal mogelijk waarden die de betrouwbaarheidsbehoefte kan aannemen, waarbij drie klassen per onderdeel vanuit praktische overwegingen de voorkeur hebben. Door de standaard onderdelen tevens op deze klassen in te delen kan een koppeling worden gelegd tussen een bepaalde klasse betrouwbaarheidsbehoefte en de standaard onderdelen met dezelfde klasse die bij de betreffende betrouwbaarheidsbehoefte horen.

8.1.2 Realisatie van de doelstelling

Op basis van de antwoorden op de kernvragen en daarmee uiteindelijk het antwoord op de probleemstelling is gestreefd naar realisatie van de volgende doelstelling:

> *Het ontwikkelen van een algemene methode voor het opstellen van informatiebeveiligingsbeleid, waarmee op basis van de (informatie)behoeften van een organisatie het informatiebeveiligingsbeleid voor de organisatie efficiënt en effectief kan worden opgesteld.*

Deze doelstelling is gerealiseerd door de in de vorige paragraaf genoemde kwantificering van de betrouwbaarheidsbehoefte en classificatie van de standaard onderdelen van beveiligingsbeleid in de praktijk te brengen.

De betrouwbaarheidsbehoefte kan worden gekwantificeerd door gebruik te maken van een op de door het International Security Forum ontwikkelen SPRINT methode gebaseerde afhankelijkheidsanalyse. Daarbij wordt op basis van een serie *business*–georiënteerde vragen de impact van aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid bepaald. Deze uitkomst kan drie waarden hebben: laag (L), middelmatig (M) en hoog (H). Hiermee wordt de betrouwbaarheidsbehoefte $B_{(B,I,V)}$ dus een triple van de linguïstische variabelen beschikbaarheid, integriteit en vertrouwelijkheid.

Om gebruik te kunnen maken van standaard onderdelen van beveiligingsbeleid als bouwstenen, is een verzameling opgesteld van mogelijke beschrijvende teksten en beveiligingsrichtlijnen. De beschrijvende teksten zijn niet geheel standaardiseerbaar gebleken. Daarom is als alternatief een raamwerk van beschrijvende teksten gemaakt dat als kapstok kan dienen voor het werkelijke beveiligingsbeleid. Daarnaast is een universum van mogelijk beveiligingsrichtlijnen opgesteld, waaruit een selectie kan worden gemaakt voor het beveiligingsbeleid van ieder organisatie.

Om de richtlijnen te kunnen koppelen aan de betrouwbaarheidsbehoefte is iedere richtlijn door materie–experts voorzien van een classificatie op basis van de voor de betrouwbaarheidsbehoefte afgebakende drie waarden van de beschikbaarheid, integriteit en vertrouwelijkheid. Op basis van deze classificatie is het mogelijk voor een organisatie de betrouwbaarheidsbehoefte te bepalen, en vervolgens op basis daarvan de van toepassing zijnde beveiligingsrichtlijnen te selecteren en deze in te bedden in het raamwerk nog voor een organisatie te ‘personaliseren’ van beschrijvende teksten.

Uit toetsing van deze methodiek op basis van een fictieve casus is gebleken dat de voorgestelde methode praktisch bruikbaar is. Daarbij is echter wel gebleken dat de toegekende classificatie door gebruik in de praktijk verder geoptimaliseerd kan worden. Tevens is aangegeven dat na selectie van beveiligingsrichtlijnen op basis van de classificaties en de betrouwbaarheidsbehoefte niet 100% bindend hoeft te zijn. In de praktijk kunnen zich naar verwachting situaties voordoen waarin de standaard classificaties niet gepast is. Derhalve moet de geselecteerde richtlijnen altijd globaal worden beoordeeld op wenselijkheid, op basis van *professional judgement* van de betrokken expert(s).

Op basis van dit alles kom ik tot de evaluatie dat ik geslaagd ben in de doelstelling een methode te ontwikkelen, waarmee op basis van de betrouwbaarheidsbehoefte van een organisaties met behulp van een standaard raamwerk voor beveiligingsbeleid en een selectie van beveiligingsrichtlijnen uit een universum van richtlijnen op relatief efficiënte en effectieve wijze informatiebeveiligingsbeleid kan worden opgesteld.

Tijdens het onderzoek is nadrukkelijk gebleken dat deze methode een duidelijk toegevoegde waarde heeft ten opzicht van het 'handmatig' opstellen van beveiligingsbeleid. Het gebruik van de ontwikkelde methode voorkomt dat bij het opstellen van beveiligingsbeleid iedere mogelijke beveiligingsrichtlijn door een betrokken expert opnieuw moeten worden beoordeeld op relevantie voor de betrokken organisatie. Zowel de (impliciete) inschatting van de beveiligingsbehoefte van de organisatie als (ongestructureerde) keuze van de richtlijnen zouden telkens opnieuw moeten worden uitgevonden.

Tevens ligt in de classificatie van de richtlijnen zeer waardevolle bevatte expert-knowledge besloten waarop experts bij de uitvoering kunnen steunen. De betrokken expert hoeft bij zijn afweging van richtlijnen namelijk niet alleen op basis van zijn eigen kennis en ervaring een inschatting maken van de toepasbaarheid van een richtlijn. Dit levert een grote bijdrage aan de efficiëntie en de effectiviteit van het opstellen van informatiebeveiligingsbeleid.

Desondanks is ook aangegeven dat nog steeds de betrokkenheid van deskundigen vereist is. De methode is namelijk in geen geval een black box is waar je de betrouwbaarheidsbehoefte in stop en waar vervolgens een kant en klaar beveiligingsbeleid uit komt. De methode biedt een grove aanzet die vervolgens op basis van ervaring, deskundigheid en professional judgement moet worden vervolmaakt.

8.2 Aanbevelingen

Zoals in de vorige paragraaf aangegeven is de ontwikkelde methode geen beveiligingsbeleid–machine die door iedereen kan worden bediend. In mijn onderzoek zijn echter diverse zaken naar voren gekomen die erop duiden dat de werking van de methode nog verder verbeterd kan worden, waardoor de noodzaak voor aanvullende handwerk wordt verminderd. Hierop zal navolgend ingaan.

8.2.1 Verfijning van de kwantificering van de betrouwbaarheidsbehoefte

Om te beginnen is gebleken dat de betrouwbaarheidsbehoefte in essentie bepalend is voor het informatiebeveiligingsbeleid, maar tevens is gebleken dat de op basis hiervan gekozen beveiligingsrichtlijnen niet aansluiten bij de behoeften van een organisatie. Enerzijds wordt dit veroorzaakt doordat een organisatie bepaalde specifieke kenmerken heeft (bijvoorbeeld in het voorbeeld van de casusorganisatie een kleine hechte organisatie) waardoor bepaalde specifieke richtlijnen minder van toepassing zijn. Voor optimalisatie van de methode zie ik mogelijkheden in het onderzoeken van mogelijke secundaire invloedsfactoren die in aanvulling op de betrouwbaarheidsbehoefte mede bepalend zijn voor de invulling van het beveiligingsbeleid. Daarmee wordt een verfijning aangebracht in de werking van de methode. Uiteraard moet in dat geval ook de classificatie van de beveiligingsrichtlijnen hieraan worden aangepast.

Een ander punt dat naar voren is gekomen, is dat de gekozen indeling van de betrouwbaarheidsbehoefte in drie mogelijke linguïstische waarden per aspect in sommige gevallen een beperking vormt. In het geval van de casusorganisatie kwam voor een aantal geselecteerde beveiligingsrichtlijnen naar voren dat deze te stringent zijn voor de organisatie, terwijl wel de hoogste score was toegekend aan de betrouwbaarheidsbehoefte. Hieruit is af te leiden dat in sommige gevallen een extra mogelijke waarde voor een nog hogere betrouwbaarheidsbehoefte gewenst zou zijn, om de extremen van het beveiligingsspectrum af te dekken. Deze verfijning van de methode kan het mogelijk maken de beveiligingsrichtlijnen nog beter te kiezen.

Voor beide uitbreidingen/aanpassingen van de methode geldt dat deze kunnen (en zeer waarschijnlijk zullen) leiden tot een complexere methode, waardoor een deel van de efficiëntie

verloren kan gaan. Indien eventuele aanpassingen worden geëvalueerd is het vereist om altijd de afweging te maken tot de verhoging van de effectiviteit enerzijds en een mogelijke vermindering van de efficiëntie anderzijds.

8.2.2 Optimalisatie van het universum van beveiligingsrichtlijnen

In dit onderzoek is beschreven hoe een universum van beveiligingsrichtlijnen kan worden opgesteld en geclassificeerd. Daarbij is als toetsing een deel van dit universum samengesteld en is hierop met materie–experts een classificatie uitgevoerd. Doordat slechts een deel van het universum is afgedekt en doordat de classificatie door een klein aantal experts heeft plaatsgevonden biedt dit geen volledig gereedschap voor het opstellen van informatiebeveiligingsbeleid. Om de methode volledig toepasbaar te maken zal het universum daarom allereerst volledig moeten worden gemaakt.

Dat kan door zoals bij het opstelde deeluniversum door gebruik te maken van de code voor informatiebeveiliging, maar dit heeft twee nadelen. Ten eerste is dit weliswaar een breed geaccepteerde best practice, maar vooral bedoeld als globale aanzet. Afgevraagd kan worden hoe volledig de daarin opgenomen lijst van richtlijnen is. De code vormt vooral een algemene aanzet. Daarom acht ik het wenselijk bij het aanvullen van het universum ook gebruik te maken van andere bronnen. Dit betekent echter wel dat extra aandacht nodig is om bijvoorbeeld overlapping of tegenstrijdigheid van richtlijnen te voorkomen. Ten tweede heb ik aangegeven dat de richtlijnen in de code voor informatiebeveiliging soms meer het karakter hebben van maatregelen. In dit onderzoek getracht in de theorie van beveiligingsbeleid zo zuiver mogelijk aan te sluiten bij beveiligingsbeleid als middel om op basis van afhankelijkheid (de betrouwbaarheidsbehoefte) op hoog niveau via beveiligingsrichtlijnen het vereiste beveiligingsniveau te stellen. Wanneer die lijn gevolgd wordt is het wenselijk om bij het opstellen universum nauw te letten op het onderscheid tussen richtlijnen en maatregelen, teneinde een zuiver universum van richtlijnen te creëren.

Naast het completeren van het universum zullen alle richtlijnen het universum ook geclassificeerd moeten worden. In dit onderzoek is op het deeluniversum een classificatie met drie materie–experts uitgevoerd. De kwaliteit van de classificatie kan nog verder worden verhoogd door meer materie–experts bij de classificatie te betrekken. Hoe meer expert–kennis in de classificatie is bevat, hoe betrouwbaarder deze mag worden geacht.

Gezien de conclusie van het onderzoek dat het gebruik van een gestructureerde methode de efficiëntie en effectiviteit van het opstellen van beveiligingsbeleid verhoogt acht ik de completering van het universum en classificatie daarvan met meer experts zeer wenselijk. In mijn ogen bestaat er behoefte aan een volledig gereedschap voor het opstellen van beveiligingsbeleid in de vorm van een beschrijving van de methode en het bijbehorende volledige universum van geclassificeerde beveiligingsrichtlijnen waarin alle expert–kennis op dit gebied gebundeld is. Zo'n gereedschap zou analoog aan de code voor informatiebeveiliging een **'Code voor Informatiebeveiligingsbeleid'** moeten zijn die organisaties als de ultieme best practice voor beveiligingsbeleid kunnen hanteren.

8.2.3 Onderzoeksuitkomsten als toetsingskader voor beveiligingsbeleid

Een bijkomstigheid van dit onderzoek dat in het onderzoek naar literatuur over beveiligingsbeleid gecombineerd met de uitkomensen van de analyse van de verschillende voorbeelden van informatiebeveiligingsbeleid een normenkader (eisenpakket) voor de beoordeling van informatiebeveiligingsbeleid ligt besloten. De uitgevoerde analyse vormt een prima basis om te kunnen bepalen of in een bepaald beveiligingsbeleid de vereiste onderdelen zijn opgenomen. Tevens zou op basis een vast te stellen betrouwbaarheidsbehoefte van een organisatie kunnen worden beoordeeld of de in het beveiligingsbeleid van de betreffende organisatie opgenomen beveiligingsrichtlijnen volledig zijn en aansluiten bij de behoeften van de organisatie. Om hiertoe over te gaan zal de ontwikkelde methode echter wel eerst voldoende in de praktijk zijn getoetst om zeker te weten dat de in de methode gestelde eisen ook werkelijk juist zijn.

Literatuuropgave

[ALBR2002] Albright, J.G. (2002). The Basics of an IT Security Policy. GSEC, 5, 1–11.

[ALLEN2002] Allen, J.H. et al. (2002). Common Sense Guide for Senior Managers. ISA, 1, 1–20.

[BEA1993] Beatrix, Koningin der Nederlanden (1993). Wet Computercriminaliteit. Staatsblad 1993, 33

[BEA2000] Beatrix, Koningin der Nederlanden (2000). Wet Bescherming Persoons–gegevens. Staatsblad 2000, 302

[BELL1973] Bell, D. E. and LaPadula, L. J. (1973), "Secure Computer Systems: Mathematical Foundations and Model," M74–244. Bedford: Mitre Corp

[BIZA1994] Ministerie van Binnenlandse Zaken. (1994). Voorschrift Informatiebe–veiliging Rijksoverheid. Den Haag: Ministerie van Binnenlandse Zaken.

[BROCK1998] Brock, J.L. (Red.) (1998). Executive Guide: Information Security Management. GAO, 68, 1–19.

[BRUI2000] De Bruin en Schönfeld. (2000). Informatiebeveiligingsbeleid. In Redactie, Handboek EDP Auditing. Deel B Kwaliteitsbeheersing van de informatievoorziening. blz. pagina's. Plaats: uitgever.

[BSI1999] British Standards Institution (1999). BS7799: A Code of Practice for Information Security Management. London: BSI–DISC

[BURG1997] Van der Burg, M.C.C., Van de Garde, J.M.W. (1997). Voorschrift Informatiebeveiliging Rijksdienst. Compact, 3, 33–42.

[CBS1999] CBS. Automatisering bij bedrijven en overheid 1997–1999. Voorburg/Heerlen. CBS, 1999

[CLARK1987] Clark, D.D., Wilson, D.R. (1987). A Comparison of Commercial and Military Computer Security Policies, Tijdschrift, 6, 184–194.

[COUM1998] Coumou en Schoemaker. (1998). Hoe helpen we de probleemeigenaar? Ondersteuning bij het opstellen van een informatiebeveiligingsbeleid. Compact, 1998/5, blz. 3–11.

[DALE1999] G. Geerts, T. den Boon (1999). Van Dale. Groot woordenboek der Nederlandse taal. 13e dr. Utrecht/Antwerpen: Van Dale Lexicografie

[ECP2003] ECP.NL (2003). Schema voor Certificatie van informatiebeveiliging op basis van BS 7799–2. http://www.ecp.nl

[FAGAN1993] Fagan, P. (1993). Organizational Issues in IT Security. Computers & Security, 12, 710–715.

[HART1995] Hartman. (1995). Organisatie van de Informatieverzorging. (derde druk). 's–Gravenhage: DELWEL Uitgeverij B.V.

[INTER2001] Interprom Consultants (2001): Zonder informatiebeveiliging is beheer niet compleet. Security Whitepaper.

[ISF1999] International (European) Security Forum (1997). SPRINT Risk analysis for Information Systems: User Guide. London: ISF.

[KELL1999] Kelly (1999). New rules for the new economy. Geraadpleegd op 12 augustus 2003 via http://www.wired.com/wired/archive/5.09/newrules_pr.html

[LAND1981] Landwehr, C.E. (1981). Formal Models for Computer Security. Computing Surveys, 3, 247–275.

[MCON2000] McConnell, K.D. (2000). How to Develop Good Security Policies and Tips on Assessment and Enforcement. Sans Security Essentials, 1.3, 1–13.

[NGI1979] NGI, sectie beveiliging. (1979). Computerbeveiliging. Een overzicht van de belangrijkste aspecten. Nederlands Genootschap voor Informatica.

[NGI1990] NGI sectie EDP–Auditing. (1990) Beveiligingssystemen: een visie op toegang tot een visie. Amtserdam: NOVEP Congresorganisatie

[NGI1991] NGI sectie EDP–Auditing. (1991) Studierapport inzake toeapssing van risico–analyse bij geautomatiseerde gegevensverwerking.

[NGI1992] NGI Afdeling beveiliging. (1992) Informatiebeveiligingsbeleid en –plan. Deventer: Kluwer Bedrijfswetenschappen.

[NGI1992b] NGI Afdeling beveiliging. (1992) Risico–analyse en risicomanagement. Deventer: Kluwer Bedrijfswetenschappen.

[NGI1993] NGI Afdeling beveiliging. (1993) Standaardisatie van informatiebeveiliging. Deventer: Kluwer Bedrijfsinformatie.

[NGI1995] NGI Afdeling beveiliging. (1995) Organiseren van gegevensbeveiliging. Deventer: Kluwer Bedrijfsinformatie.

[NGUY1997] Nguyen, Walker. (1997) A first course in fuzzy logic. Las Cruces, New Mezico: CRC Press, Inc.

[NNI2000] Nederlands Normalisatie Instituut (2000). Code voor Informatiebeveiliging – Een leidraad voor beleid en implementatie. Delft: NNI.

[OECD2002] Organisation for Economic Co-operation and Development (2002). OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.

[OVER2000] Overbeek, Roos Lindgreen en Spruit. (2000). Informatiebeveiliging onder controle. Pearson Education Uitgeverij BV.

[PELT1994] Peltier, T., Edison, D. (1994). Developing an Information Security Policy Statement.

[PIJL2004] Pijlgroms (2004). Fuzzy Logic: logisch of vaag? Geraadpleegd op 18 april 2004 via www.htsa.ie.hva.nl/~pylgroms/fuzart1.htm

[PRUI2000] Pruijm (2000). Collegesheets Informatiebeleid. Erasmus Universiteit Rotterdam.

[RCC1996] RCC. (1996). Informatiebeveiliging in de praktijk. Apeldoorn: RCC.

[REYES2003] Reyes, C. (2003). What makes a good security policy and why is one necessary? GSEC, 6, 1–12.

[ROOS1998] Roos Lindgreen. (1998). Corporate Information Security. Geen halve maatregelen. Compact, 1998,5, blz. 12–19.

[STAL2000] Stallings. (2000) Netwerkbeveiliging en cryptografie. Beginselen en praktijk. Schoonhoven: Academic Service.

[STAR1997] Starreveld e.a. (1997). Bestuurlijke informatieverzorging deel 1. Alphen aan de Rijn: Samsom.

[STUL2004] G. Stults (2004). An Overview of Sarbanes-Oxley for the Information Security Professional. Geraadpleegd op 28 augustus 2004 via http://www.giac.org/practical/GSEC/Gregg_Stults_GSEC.pdf

[VASKO1999] Vasko, E. (1999). Policy Management. SC Security Magazine, 4, 1–9. Geraadpleegd op 10 september 1999 http://194.202.195.4/securecomputing/1999_04/cover/cover.html

Vergelijking voorbeelden van beveiligingsbeleid

Voor mijn onderzoek heb ik de beschikking gehad over een divers aantal praktijkvoorbeelden van informatiebeveiligingsbeleid. Teneinde meer duidelijk te krijgen over wat beveiligingsbeleid is heb ik een vergelijkend onderzoek uitgevoerd op de voorbeelden. Allereerst geef ik in A.1 een overzicht van de organisaties waarvan ik het beveiligingsbeleid tot mijn beschikking had. Vervolgens geef ik in A.2 een overzicht van de verschillen en overeenkomsten tussen de hoofdlijnen van de onderzochte voorbeelden. Aansluitend vergelijk ik in hoeverre de volgende de theorie op te nemen onderdelen ook daadwerkelijk in de praktijkvoorbeelden voorkomen.

A.1 De organisaties van de beschikbare voorbeelden

Ik heb het beveiligingsbeleid onderzocht van acht verschillende organisaties. In deze paragraaf benoem en beschrijf ik deze organisaties. De organisaties zijn geanonimiseerd omdat het hier om gevoelige bedrijfsinformatie gaat. Per organisatie heb ik een korte beschrijving opgenomen van de activiteiten van de organisatie en de branche waarin deze actief is. Tevens heb ik enkele kerneigenschappen weergegeven, zoals het aantal werknemers dat een organisatie heeft (voor zover deze onder het beoordeelde beleid vallen) en de omzet in het jaar waarin het beleid is opgesteld.

Amerikaanse hotelketen

Dit betreft een organisatie die ten tijde van het beveiligingsbeleid (1998) in bezit is van en het beheer voert over een kleine honderd hotels (deels franchise) in de Verenigde Staten. De organisatie beschikt over een hoofdkantoor, diverse regionale kantoren en hotels verspreid over het gehele land. De omzet bedraagt zo'n $200 miljoen.

Handelsorganisatie in bouwmaterialen

Deze detailhandelsorganisatie bezit enkele tientallen bouwmarkten in met name de randstad. Het betreft hier één van de grote spelers in de 'doe het zelf' markt. Het beoordeelde informatiebeveiligingsbeleid van deze organisatie is opgesteld in 1999. Op dat moment beschikte de organisatie over waren enkele honderden medewerkers subject van het beveiligingsbeleid.

Data- en telecomleverancier

Het beveiligingsbeleid van deze betreffende data- en telecomleverancier dateert uit 1997. Op dat moment was de organisatie nog relatief jong en actief in een nog maar kort geliberaliseerde markt. Op dat moment bood het bedrijf aan vaste klanten vaste en mobiele telefonie en diverse datanetwerkdiensten aan.

Een grote internationaal opererende Nederlandse bank

Deze internationaal opererende bank van Nederlandse origine behoort tot de top vijf van Nederlandse banken. De bank is actief in vele landen. Het beschikbare beleid dateert uit september 1995. Het beleid is van toepassing op de Nederlandse organisatie van de bank.

Middelgrote Nederlandse gemeente

Ten tijde van het opstellen van het beveiligingsbeleid (1998) telde deze Zuidhollandse gemeente iets meer dan 70.000 inwoners. Het aantal personen dat binnen de reikwijdte van het beleid viel is niet bekend.

Grote landelijke administratieve overheidsorganisatie

Het betreft hier een grote landelijke opererende administratieve organisatie van Rijksoverheid. De organisatie fungeert als inner en uitkeerder van diverse geldelijke middelen. De organisatie

is georganiseerd in diverse lokaal opererende organisatieonderdelen. Het onderzochte beveiligingsbeleid is afkomstig uit 1997 en was van toepassing op de meer van 5000 medewerkers van de organisatie.

Middelgrote sectorbank

Deze bank is een sectorbank, gelieerd aan een grote internationaal opererende verzekeraar. De bank faciliteert diverse financiële diensten van de verzekeraar en diens deelnemingen. Het beoordeelde beveiligingsbeleid dateert uit 1998.

Grote uitgeverij

Deze uitgeverij is internationaal actief in de uitgifte van diverse media, waaronder dagbladen, tijdschriften en elektronische informatiediensten. Het onderzochte beveiligingsbeleid is opgesteld in 1997. Destijds bedroeg de omzet zo'n 700 miljoen euro, met een winst van zo'n 60 miljoen euro. Binnen de gehele organisatie waren ruim 5500 medewerkers in dienst. Het is onduidelijk hoeveel hiervan binnen het beoordeeld beleid vielen.

A.2 Vergelijking op hoofdlijnen van de beschikbare voorbeelden

De beschikbare voorbeelden van beveiligingsbeleid zijn door mij onderzocht en vergeleken teneinde meer inzicht te krijgen in de wijze waarop beveiligingsbeleid in de praktijk wordt uitgewerkt en in hoeverre dit aansluit bij de theorie omtrent beveiligingsbeleid. Daartoe heb ik allereerst een globale vergelijking uitgevoerd van de voorbeelden. Daarbij heb ik mij gericht op de aspecten vorm, omvang, indeling en de plaats binnen de organisatie. De uitkomsten van de vergelijking op hoofdlijnen wordt hierna per aspect beschreven.

A.2.1 Doel van het beveiligingsbeleid

In alle voorbeelden is impliciet of expliciet de doelstelling van het beveiligingsbeleid beschreven. De doelstellingen van alle voorbeelden verschillen in diepgang, maar sluiten alleen (deels) aan bij de definitie van informatiebeveiligingsbeleid zoals ik die in hoofdstuk drie heb geformuleerd. De doelstelling wordt nergens verder toegelicht in secundaire doelen, zoals ik die heb opgesomd in paragraaf 3.2.

A.2.2 Vorm en indeling van het beveiligingsbeleid

De vorm in indeling van het beveiligingsbeleid komt voor een meerderheid van de voorbeelden op hoofdlijnen overeen. Op de uitgeverij na, zijn alle voorbeelden ingedeeld in een deel algemene beschrijvingen en een deel beveiligingsrichtlijnen. In de algemene beschrijvingen komen zaken aan de orde als de doelstelling, uitgangspunten, verantwoordelijkheden en de classificatie van informatiesystemen. Het beleid van de uitgeverij bestaat alleen maar uit algemene beschrijvingen.

In de voorbeelden met een deel richtlijnen (zeven van de acht) wordt in dat deel een opsomming gegeven van de richtlijnen die gelden ten aanzien van informatiebeveiliging. Hiermee wordt concreet invulling gegeven aan de sturing van het informatiebeveiligingsproces. Van de zeven stukken met richtlijnen zijn er zes waarin de richtlijnen puntsgewijs en genummerd zijn opgenomen. Eén voorbeeld (de handelsorganisatie) beschikt wel over concrete richtlijnen, deze zijn echter gebundeld in prozaïsche alinea's in plaats van puntsgewijs opgenomen.

A.2.3 Omvang van het beveiligingsbeleid

De omvang van de onderzochte voorbeelden ligt voor vijf van de acht exemplaren tussen de 29 en 42 bladzijden. De andere drie voorbeelden wijken sterk af naar boven (67 voor de overheidsorganisatie en 85 voor de hotelketen) of naar beneden (16 voor de uitgeverij).[1] De vijf in omvang overeenkomende voorbeelden komen ook qua indeling en voorkomende onderdelen overeen.

De oorzaken van de afwijkingen blijken duidelijk uit de voorbeelden. Het beveiligingsbeleid van de hotelketen bevat namelijk extra onderdelen ten opzichte van de middenmoot, zoals een beschrijving van relevante risico's en risicomanagement en een uitgebreide set van maatregelen gericht op internetbeveiliging. Het beveiligingsbeleid van de overheidsorganisatie bevat ten opzicht van de andere voorbeelden meer beveiligingsrichtlijnen. Daarnaast is het strategische kader waarbinnen het beleid is geplaatstuitgebreider beschreven. Het beperkte omvang van het beleid van de uitgeverij is het gevolg van het niet opnemen van een opsomming van concrete beveiligingsrichtlijnen.

Gezien dit alles kan een omvang van dertig tot veertig bladzijden worden gezien als de gemiddelde omvang van beveiligingbeleid dat de meest voorkomende onderdelen bevat.

A.2.4 Plaats binnen de organisatie van het beveiligingsbeleid

Uit de vergelijking van de doelstellingen is al gebleken dat de voorbeelden allen een zelfde doel nastreven. In aanvulling daarop heb ik bekeken of de plaats die het beveiligingsbeleid binnen de organisatie inneemt om dat doel te bereiken ook overeenkomt. Dat is echter niet zonder meer vast te stellen, omdat de plaats binnen de organisatie niet in alle gevallen is beschreven in het beleid.

Het meest uitgebreid is de plaats binnen de organisatie beschreven voor de overheidsorganisatie. De hotelketen, de kleine bank, de data- en telecomleverancier en de gemeente hebben beschreven dat het beleid aan de basis staat van de uitwerking van informatiebeveiliging en dat uitwerking plaats heeft in beveiligingsplannen, procedures en maatregelen. De uitgeverij, de grote bank en de handelsorganisatie beschrijven behalve de doelgroep niet wat de plaats van het beleid is binnen de organisatie.

In alle onderzochte voorbeelden is de personele doelgroep beschreven (de 'subjecten van het beleid'), in sommige is ook de materiële doelgroep beschreven (de 'objecten van het beleid'). In alle onderzochte voorbeelden is de personele doelgroep beschreven (de 'subjecten van het beleid'), in sommige is ook de materiële doelgroep beschreven (de 'objecten van het beleid').

Wat verder opvalt is dat alleen de grote bank niet beschrijft dat het beveiligingsbeleid de van toepassing zijnde wetten en standaarden volgt. Verder is in geen van de onderzochte voorbeelden de invloeden het informatiebeleid en van de andere beleidsgebieden (facilitair beleid, financieel beleid en personeelsbeleid; zie paragraaf 3.3.1) beschrijft. Uit de voorbeelden is mij ook niet gebleken wat de eventuele invloed van de andere beleidsgebieden is geweest op de invulling van het beleid.

A.3 Vergelijking van de onderdelen van de beschikbare voorbeelden

Naast de vergelijking op hoofdlijnen heb ik vergeleken welke onderdelen voorkomen in de verschillende beschikbare voorbeelden. Deze vergelijking heb ik gebaseerd op de onderdelen

van informatiebeveiligingsbeleid zoals die in de theorie worden voorgesteld. Deze onderdelen heb ik in hoofdstuk drie beschreven. In de tabellen op de volgende twee bladzijden is de inventarisatie van alle onderdelen opgenomen.

Uit de vergelijking blijkt dat de uitwerking van de onderdelen divers is, maar dat het grootste deel van de door de theorie voorgestelde onderdelen ook daadwerkelijk in de meeste praktijkexemplaren zijn opgenomen. In de volgende paragrafen zal ik de meest opvallende zaken toelichten.

Doelstelling van informatiebeveiliging

Terwijl de doelstelling van het beveiligingsbeleid in nagenoeg alle exemplaren expliciet aangegeven, wordt de doelstelling van informatiebeveiliging in de meest gevallen niet of alleen impliciet beschreven. Een expliciete managementverklaring is in slechts twee van de voorbeelden opgenomen. Dit heeft tot gevolg dat het 'hogere doel' van het informatiebeveiligingsbeleid veelal niet duidelijk is, waardoor het risico bestaat dat het beleid meer dan gewenst een geïsoleerd stuk wordt. In een op te stellen beveiligingsbeleid acht ik het daarom wenselijk deze onderdelen wel op te nemen.

Organisatie van de informatiebeveiliging

Alle onderzochte voorbeelden gaan in op de organisatie van informatiebeveiliging. De diepgang waarmee dat gebeurt verschilt echter. De verschillen zitten in de verschillende verantwoordelijken die worden onderkend en de mate waarin de verantwoordelijkheden per verantwoordelijke zijn uitgewerkt. De grote lijn is dat de functies worden benoemd die verantwoordelijkheden hebben binnen het informatiebeveiligingsproces. Per functie wordt globaal beschreven of opgesomd wat de verantwoordelijkheden zijn. Functies die veelal voorkomen in de beschreven beveiligingsorganisaties zijn:

- Directie/topmanagement: de hoogstverantwoordelijke binnen een organisatie.
- Lijnmanagement: de verantwoordelijken binnen de lijnorganisatie (middenmanagement)
- Systeemeigenaren: de personen die aangewezen zijn als verantwoordelijke voor een specifiek informatiesysteem.
- Security coordinator/security officer: de verantwoordelijke coördinator voor informatiebeveiliging.

- Security Administrator/beheerder: de functionaris die de configuratie van beveiligingsmaatregelen in informatiesystemen voor zijn/haar rekening neemt.
- Interne of externe auditor: de partij die periodiek controleerd of (delen van) de informatiebeveiliging nog voldoen aan de eisen van de organisatie.

Classificatievoorschrift

Op twee na bevatten alle exemplaren een classificatievoorschrift waarin wordt voorgeschreven op welke wijze organisaties hun informatiesystemen moeten classificeren. Een classificatievoorschrift geeft aan hoe het belang van een informatiesysteem voor de organisatie moet worden bepaald. In veel gevallen is het classificatievoorschrift gericht op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. De classificatie dient als hadvat voor het per informatiesysteem uitwerken van het beveiligingsbeleid in systeemmaatregelen.

Financiering van informatiebeveiliging

In geen van de onderzochte voorbeelden is de financiering van informatiebeveiliging en/of de implementatie van het beveiligingsbeleid beschreven.

Beschrijving van informatiesystemen

In geen van de onderzochte voorbeelden zijn de informatiesystemen van de organisatie beschreven.

Uitgangspunten en randvoorwaarden

Drie onderzochte exemplaren bevatten in geen afzonderlijk geformuleerde uitgangspunten en/of randvoorwaarden. Vier exemplaren bevatten een aantal (vijf tot twintig) uitgangspunten. De uitwerking hiervan verschilt echter per exemplaar. Zo worden in een exemplaar de randvoorwaarden ingevuld als een soort wijze beveiligingslessen, terwijl in een ander exemplaar de randvoorwaarden vooral algemeen geldende beveiligingsrichtlijnen zijn. Het is moeilijk hierover een sluitend oordeel te vormen.

Gezien de voorbeelden acht ik het gewenst in beveiligingsbeleid een beperkt aantal randvoorwaarden op te nemen die bestaan uit algemeen geldende beveiligingsprincipes en

richtlijnen die zo basaal en algemeen zijn dat ze geen verdere uitwerking vereisten in plannen of systemen, maar algemeen gelden. In bijlage B wordt een overzicht gegeven van mogelijke randvoorwaarden.

Visie op informatiebeveiliging

Kort gezegd kan worden gesteld dat het informatiebeveiligingsbeleid in z'n geheel de visie van een organisatie op informatiebeveiliging is. Desondanks is in drieexemplaren de visie nog eens expliciet of impliciet geformuleerd. Een degelijke formulering kan een nuttige aanvulling zijn op de doelstelling van informatiebeveiliging en het verdient dan ook dit daaronder in het beleid op te nemen.

Wijze van toetsing

In vijf van de acht voorbeelden is de wijze van toetsing van het beveiligingsbeleid en/of de informatiebeveiliging beschreven. In drie gevallen is dit beschreven als onderdeel van de beveiligingsrichtlijnen, in één geval onder de beveiligingsorganisatie en in één geval als onderdeel van de rapportagestructuur. Gezien de voorbeelden acht ik het gewenst in algemene bewoordingen te stellen dat toetsing vereist is en dat in de richtlijnen wordt uitgewerkt op welk wijze toetsing dient plaats te vinden.

Afhandeling van incidenten

Afhandeling van incidenten is in drie voorbeelden expliciet beschreven, veelal als onderdeel van de beveiligingsrichtlijnen. In drie gevallen zijn alleen continuïteitsrichtlijnen beschreven. Gezien de voorbeelden heeft het de voorkeur de afhandeling van incidenten op te nemen als onderdeel van de beveiligingsrichtlijnen.

A.4 Conclusie

Uit de vergelijking van een achttal voorbeelden van informatiebeveiligingsbeleid blijkt dat de voorbeelden van beveiligingsbeleid op hoofdlijnen overeenkomen. Blijkbaar verstaan bedrijven onder beveiligingsbeleid hetzelfde. De insteek van het beveiligingsbeleid (doel, niveau, plaats binnen de organisatie) sluit aan bij de theoretisch inzichten daaromtrent.

Ondanks de overeenkomsten zitten er wel vormverschillen tussen de verschillende voorbeelden. In essentie bestaan alle voorbeelden uit een prozaïsche beschrijving van de algemene setting en een verzameling beveiligingsrichtlijnen. De invulling van deze twee elementen verschilt tussen de onderzochte exemplaren. De detaillering en mate van toelichting van de algemene setting varieert. Tevens verschillen de exemplaren in de hoeveelheid en mate van stringentie van de beveiligingsrichtlijnen; het ene voorbeeld bevat strengere richtlijnen dan het andere. Hierin komt het verschil in aansturing van de informatiebeveiliging naar voren. De ene organisatie stelt hogere eisen aan de informatiebeveiliging dan de andere.

De voorbeelden sluiten qua overige onderdelen redelijk tot goed aan bij de theorie. Het beeld ontstaat echter wel dat de onderzochte voorbeelden pragmatischer zijn opgesteld dan de theorie, die meer vanuit idealistische situaties denkt.

Wat verder opvalt aan de theoretische en praktische onderdelen, is dat de theoretisch beschreven onderwerpen soms wat arbitrair zijn omdat ze net als veel andere onderwerpen onderdeel zijn van de richtlijnen. Het is de vraag wat rechtvaardigt dat onderwerpen apart worden vermeld, in plaats als deel van de richtlijnen. Waarom zou bijvoorbeeld de afhandeling van incidenten een apart onderwerp moeten zijn terwijl fysieke beveiliging niet expliciet wordt genoemd en gewoon onder de richtlijnen valt. Mijns inziens kunnen de onderdelen die gericht zijn op de werkelijke uitvoering van informatiebeveiliging het beste als richtlijnen worden opgenomen.

De indeling van de beveiligingsrichtlijnen verschilt tussen de voorbeelden. Zo maken sommigen de ordening naar werkingssfeer (fysiek, logisch, organisatorisch), sommigen houden de indeling van de code voor informatiebeveiliging (zie paragraaf 2.5) aan en de anderen kiezen een variant op deze indelingen. Het is dus niet te zeggen wat de meest gebruikte indeling is.

Noten

1 Uiteraard is het aantal bladzijden geen universele maatstaf voor de omvang van het beveiligingsbeleid. Zaken als lettergrootte, bladspiegel, opmaak, et cetera kunnen een belangrijke rol spelen in de omvang. De vergeleken voorbeelden komen echter goed overeen qua bladvulling, waardoor het aantal bladzijden een goede vergelijkingsbasis vormt.

(1/2)	Handelsorganisatie	Hotelketen	Bank 1	Bank 2	Gemeente	Overheid	Uitgeverij	Data- en telecom
Omvang (blz.)	29	85	42	38	38	67	16	32
Doelstelling informatiebeveiliging	Niet beschreven	Globale beschrijving van de informatiebeveiliging	Expliciet beschreven (beknopt)	Niet beschreven	Niet beschreven	Expliciet beschreven	Niet beschreven.	Niet beschreven
Doelstelling beveiligingsbeleid	Expliciet beschreven	Impliciet beschreven	Expliciet beschreven	Expliciet beschreven	Expliciet beschreven	Expliciet beschreven	Expliciet beschreven	Expliciet beschreven
Plaats in de organisatie/doelgroep en Reikwijdte	De personele doelgroepen zijn beschreven. Tevens is de plaats van het beleid in de 'security architecture' aangegeven.	Personele doelgroepen beschreven. Daarnaast is de plaats van het beleid in de *security architecture* weergegeven.	Alleen personele doelgroepen beschreven.	Middels een 'beveiligingsraamwerk' is de plaats van het beleid in de beveiligingshiërarchie beschreven. Tevens wordt de doelgroep (mensen en systemen) aangegeven.	Middels een 'beveiligingsraamwerk' is de plaats van het beleid in de beveiligingshiërarchie beschreven. Tevens wordt de doelgroep (mensen en systemen) aangegeven.	Expliciet beschreven in het beveiligingsbeleid.	Objecten en subjecten waar het beleid op gericht is zijn beschreven.	Middels een 'beveiligingsraamwerk' is de plaats van het beleid in de beveiligingshiërarchie beschreven. Tevens wordt de doelgroep (mensen en systemen) aangegeven.
Globale visie op informatiebeveiliging	Beleid bevat een expliciete *mission statement* van informatiebeveiliging. Verder uitwerking in de overige onderdelen, met name de uitgangspunten.	Beknopte beschrijving van het belang van informatiebeveiliging en een globale schets van het risicomanagementproces.	Beknopt beschreven, verder vooral naar voren komend in de uitgangspunten.	Niet expliciet opgenomen. Wel naar voren komend in de overige onderdelen.	Niet expliciet beschreven, komt slechts beperkt naar voren in de overige onderdelen.	De visie op informatiebeveiliging wordt uitgebreid beschreven, gekoppeld aan de reikwijdte en risicomanagement.	Niet expliciet genoemd. Insteek van het beleid is globaal beschrijvend. In de diverse beschrijvingen komt de visie globaal naar voren.	Niet expliciet beschreven, komt slechts beperkt naar voren in de overige onderdelen.
Beveiligingsorganisatie	Beschrijving van de beveiligingsorganisatie op hoofdlijnen in algemene bewoordingen. Geen toewijzing van taken aan functionarissen.	Toekenning van taken en verantwoordelijkheden aan betrokken functionarissen.	Beschrijving van verantwoordelijkheden op hoofdlijnen (eindverantwoordelijkheid, management, persoonlijk) en toewijzing van richtlijnen aan betrokken functionarissen.	Beschrijving van taken en verantwoordelijkheden voor de betrokken functionarissen.	Beschrijving van de beveiligingsorganisatie en algemene verantwoordelijkheden op hoofdlijnene.	Geen afzonderlijke beschrijving van de beveiligingorganisatie. Wel toewijzing van taken en verantwoordelijkheden in de richtlijnen.	Beschrijving van verantwoordelijkheden voor de betrokken functionarissen, in algemene bewoordingen.	Rolbeschrijving van de betrokken functionarissen, verantwoordelijkheden op hoofdlijnen
Managementverklaring	Geen managementverklaring, wel een mission statement.	Expliciet aangegeven, 1 pagina	Geen managementverklaring	Geen managementverklaring	Expliciete managementverklaring	Geen	Geen	Geen managementverklaring

(2/2)	Handelsorganisatie	Hotelketen	Bank 1	Bank 2	Gemeente	Overheid	Uitgeverij	Data- en telecom
Classificatie	Classificatievoorschrift naar vertrouwelijkheid en beschikbaarheid. Geen koppeling aan richtlijnen. Wel aan aanzet voor de toepassing van maatregelen per niveau.	Classificatie naar vertrouwelijkheid en beschikbaarheid/ integriteit (samen). Richtlijnen zijn gekoppeld aan gebundelde eindscore hiervan.	Classificatievoorschrift naar BIV. Geen koppeling aan de richtlijnen.	Classificatievoorschrift naar BIV. Geen koppeling aan de richtlijnen.	Classificatievoorschrift naar vertrouwelijkheid. Geen koppeling aan de richtlijnen. Wel aan aanzet voor de toepassing van maatregelen per classificatieniveau.	Als onderdeel van de richtlijnen is een specifieke classificatie per aandachtsgebied beschreven.	Geen expliciet classificatievoorschrift. Wel in globaal voorgeschreven dat beveiliging moet worden ingericht op basis van risicoanalyse.	Classificatievoorschrift naar BIV. Geen koppeling aan de richtlijnen.
Beschrijving informatiesystemen	De informatiesystemen zijn niet in het beleid beschreven.	De informatiesystemen zijn niet in het beleid beschreven.	De informatiesystemen zijn niet in het beleid beschreven.	De informatiesystemen zijn niet in het beleid beschreven.	De informatiesystemen zijn niet in het beleid beschreven.	De informatiesystemen zijn niet in het beleid beschreven.	De informatiesystemen zijn niet in het beleid beschreven.	De informatiesystemen zijn niet in het beleid beschreven.
Uitgangspunten en randvoorwaarden	Beleid bevat 20 beleidsprincipes die de tuigangspunten vormen.	Beleid bevat zes beknopt beschreven primaire beveiligingsprincipes.	Beleidsuitgangspunten beschreven in 5 categorieën.	Geen afzonderlijke uitgangspunten beschreven.	Geen afzonderlijke uitgangspunten beschreven.	Geen afzonderlijke uitgangspunten beschreven.	Beleid beschrijft een klein aantal uitgangspunten op hoog niveau.	Geen afzonderlijke uitgangspunten beschreven.
Wijze van toetsing	Onder de beveiligingsorganisatie is beschreven dat de informatiebeveiliging door een onafhankelijke (interne of externe) partij.	Niet beschreven in het beveiligingsbeleid.	Het beleid bevat een richtlijn dat door of namens het management of de informatiebeveiliging effectief is.	Als onderdeel van de beveiligingsrichtlijnen is de naleving van het beveiligingsbeleid en toetsing daarop beschreven.	Als onderdeel van de beveiligingsrichtlijnen is de toetsing van de informatiebeveiliging beschreven.	Niet beschreven in het beleid.	In het beleid is als onderdeel van de rapportagestructuur de toetsing van de informatiebeveiliging beschreven.	Toetsing van de informatiebeveiliging is niet beschreven in het beleid.
Afhandeling van incidenten	Afhandeling van incidenten is niet beschreven. Wel richtlijnen voor continuïteit.	Afhandeling van incidenten is niet beschreven. Wel richtlijnen voor continuïteit.	Beknopt beschreven als onderdeel van de verantwoordelijkheden van het personeel.	Expliciet beschreven in het beveiligingsbeleid.	Expliciet beschreven in het beveiligingsbeleid.	Geen afzonderlijk beschreven algemene afhandeling van incidenten. Wel voor specifieke onderwerpen in de richtlijnen.	`Niet expliciet beschreven. Impliciet wel kort genoemd onder vereiste rapportages.	Expliciet, maar beknopt beschreven.
Financiering	Financiering van informatiebeveiliging is niet beschreven.	Financiering van informatiebeveiliging is niet beschreven.	Financiering van informatiebeveiliging is niet beschreven.	Financiering van informatiebeveiliging is niet beschreven.	Financiering van informatiebeveiliging is niet beschreven.	Financiering van informatiebeveiliging is niet beschreven.	Financiering van informatiebeveiliging is niet beschreven.	Financiering van informatiebeveiliging is niet beschreven.
Beveiligingsrichtlijnen	Het beleid bevat beveiligingsrichtlijnen, verdeeld in 6 onderwerpen.	Het beleid bevat beveiligingsrichtlijnen, verdeeld in 8 onderwerpen.	Het beleid bevat beveiligingsrichtlijnen, verdeeld in 9 onderwerpen.	Het beleid bevat beveiligingsrichtlijnen, verdeeld in 4 onderwerpen.	Het beleid bevat beveiligingsrichtlijnen, verdeeld in 7 onderwerpen.	Het beleid bevat beveiligingsrichtlijnen, verdeeld in vijf categorieën.	Het beleid bevat geen concrete richtlijnen, alleen globale beschrijvingen.	Het beleid bevat beveiligingsrichtlijnen, verdeeld in 4 onderwerpen.

Raamwerk informatie-beveiligingsbeleid

B

Wanneer informatiebeveiligingsbeleid op hoofdlijnen wordt bekeken, dan bestaat dit enerzijds uit beschrijvende teksten die zaken als de doelstelling, de reikwijdte, verantwoordelijkheden en de beveiligingsorganisatie bevatten en anderzijds uit beveiligingsrichtlijnen die invulling geven aan de sturing van informatiebeveiliging. Dit is in meer detail beschreven in hoofdstuk 3. Daarbij is ook aangegeven dat het opstellen van informatiebeveiligingsbeleid kan worden gesystematiseerd door deze beide elementen te standaardiseren.

Deze bijlage gaat in op de standaardisatie van het eerste element, de beschrijvende teksten. In paragraaf 7.2 is nader beschreven dat de beschrijvende teksten vorm geven aan de algemeen voorkomende onderdelen van informatiebeveiligingsbeleid. Dit wordt bevestigd in de onderzochte praktijkvoorbeelden.

In de navolgende pagina's is een aanzet gegeven tot gestandaardiseerde beschrijvende teksten. Deze aanzet is gebaseerd op de beschikbare praktijkvoorbeelden van informatiebeveiligingsbeleid en voorbeelden uit de beschikbare literatuur. In de aanzet zijn de onderdelen opgenomen die in hoofdstuk drie zijn beschreven en in bijlage A zijn geëvalueerd op basis van de praktijkvoorbeelden. De aanzet is bedoeld als een kapstok om de uiteindelijk invulling van

het beveiligingsbeleid en met name de beveiligingsrichtlijnen aan op te hangen. Per situatie waarin beveiligingsbeleid wordt opgesteld kan waar mogelijk en gewenst worden afgeweken van de standaard indeling. Dit zal in de praktijk met name afhankelijk zijn van de omvang van de organisatie; bij grote organisaties zullen enerzijds meer middelen beschikbaar zijn om het beveiligingsbeleid op te stellen waardoor het mogelijk wordt meer tijd in maatwerk te stoppen. Anderzijds zullen grote organisaties een grotere behoefte hebben aan het verwerken van een eigen identiteit in het beveiligingsbeleid.

In dit raamwerk zijn nog geen beveiligingsrichtlijnen opgenomen. Wel zijn de categorieën van beveiligingsrichtlijnen opgenomen, zoals die voorkomen in de Code voor Informatiebeveiliging [NNI2000]. Op de keuze van beveiligingsrichtlijnen wordt ingegaan in hoofdstuk 7.

De tekst van het raamwerk is hierna opgenomen in de gearceerde vlakken. Cursieve teksten zijn opmerkingen bij tekst, en zijn tekstueel geen onderdeel van de aanzet. Variabele teksten staan tussen rechten haken ([ ]), welke per individuele organisatie moeten worden gespecificeerd.

Voorwoord

In het voorwoord, persoonlijk geschreven door de directie, dient duidelijk te worden aangegeven welk belang het management hecht aan een goede organisatie, systematische aanpak en een gepast bewustzijn van de informatiebeveiliging.

Dit voorwoord dient onder alle omstandigheden door de organisatie zelf te worden ingevuld omdat het management zelf eindverantwoordelijk is voor het informatiebeveiligingsbeleid en de informatiebeveiliging.

[Expliciete ondertekening management]

Inleiding

Geautomatiseerde informatievoorziening speelt een steeds grotere rol binnen [Organisatie]. De betrouwbaarheid van informatiesystemen is van essentieel belang voor de dagelijkse bedrijfsvoering en de continuïteit van de organisatie. Dit maakt het noodzakelijk dat de

afhankelijkheid van informatie, software, hardware en andere faciliteiten wordt onderkend en de beveiliging ervan systematisch en goed georganiseerd wordt opgezet. Dit informatiebeveiligingsbeleid is opgesteld om daar invulling aan te geven.

Het [Organisatie] Informatiebeveiligingsbeleid is opgebouwd uit de twee onderdelen. Het eerste deel 'Informatiebeveiligingsraamwerk' gaat in op de basisprincipes van informatiebeveiliging binnen [Organisatie]. Het tweede deel 'beveiligingsrichtlijnen' bevat de beveiligingsrichtlijnen die sturing geven aan de uitvoering van informatiebeveiliging.

De detailindeling van het beveiligingsbeleid is als volgt:

Deel 1: Informatiebeveiligingsraamwerk

1. Doelstelling en reikwijdte
2. Uitgangspunten
3. Betrouwbaarheidsbehoefte en classificatie
4. Beveiligingsorganisatie

Deel 1: Informatiebeveiligingsrichtlijnen

5. Beveiligingseisen ten aanzien van personeel
6. Fysieke beveiliging en beveiliging van de omgeving
7. Beheer van communicatie- en bedieningsprocessen
8. Toegangsbeveiliging
9. Ontwikkeling en onderhoud van systemen
10. Continuïteitsmanagement
11. Naleving

1 Doelstelling en reikwijdte

1.1 Doelstelling van het informatiebeveiligingsbeleid

De basis van goed georganiseerde en systematisch opgezette informatiebeveiliging wordt gevormd door het informatiebeveiligingsbeleid. Onder het informatie–beveiligingsbeleid wordt het volgende verstaan:

Het informatiebeveiligingsbeleid is het organisatiebeleid dat –middels strategische doelstellingen, richtlijnen en procedures– richting en ondersteuning geeft aan informatiebeveiliging, teneinde de inbreuken op de betrouwbaarheid van de informatievoorziening zoveel mogelijk te voorkomen en de gevolgen van inbreuken te beheersen.

De hier genoemde 'betrouwbaarheid van de informatievoorziening' is opgebouwd uit de componenten beschikbaarheid, integriteit en vertrouwelijkheid. Deze termen worden als volgt gedefinieerd:

Beschikbaarheid: Het zekerstellen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers.
Integriteit: Het waarborgen van de correctheid en de volledigheid van informatie en computerprogrammatuur.
Vertrouwelijkheid: Het beschermen van gevoelige informatie tegen onbevoegde kennisname.

Het primaire doel van dit informatiebeveiligingsbeleid is, zoals in de bovenstaande definitie genoemd, het richting en ondersteuning geven aan de bescherming van de geautomatiseerde informatievoorziening en gegevensverwerking, oftewel de informatiebeveiliging.

Tevens dient dit informatiebeveiligingsbeleid de volgende secundaire doelen:

- Via het opstellen van dit beveiligingsbeleid voldoen wij aan wettelijke en commerciële eisen die door de overheid, branche en controlerende instanties worden gesteld.

- Door het belang van informatiebeveiliging voor onze organisatie aan te duiden en uit te dragen via dit beleid wordt gestreefd naar het verbeteren van de houding van onze medewerkers (en dat zijn wij allemaal) ten opzichte van informatiebeveiliging.
- De in dit beleid geformuleerde doelstellingen voor en eisen aan informatiebeveiliging vormen een basis voor toekomstige toetsing, zowel intern als extern.
- Dit beveiligingsbeleid is niet vrijblijvend, maar vormt een verplichte richtlijn voor alle mensen, middelen en activiteiten binnen onze organisatie. Daarmee vormt het beleid meteen van een basis voor disciplinaire acties, doordat uitdrukkelijk vast ligt welke handelswijzen wel en niet te volgen in het kader van informatiebeveiliging.

1.2 Reikwijdte van het informatiebeveiligingsbeleid

Context van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is onderdeel van het [Organisatie] Informatiebeveiligings–raamwerk. Dit raamwerk bestaat uit drie hiërarchische niveau's.

Op het hoogste niveau wordt het informatiebeveiligingsbeleid gedefinieerd. De uitgangspunten in dit beleid worden beïnvloed door algemeen geldende standaarden en normen alsmede de wettelijke bepalingen waaraan [Organisatie] onderhevig is. Daarnaast wordt het beleid ingevuld op basis van randvoorwaarden zoals het algemene bedrijfsbeleid en mogelijke geldende externe normen. Het gaat hier om algemeen geldende richtlijnen, niet om op specifieke informatiesystemen gerichte maatregelen.

Op het tweede niveau worden de beveiligingsmaatregelen beschreven als uitwerking van de richtlijnen in het informatiebeveiligingsbeleid Het gaat hierbij om zowel organisatorische als om technische beveiligingsmaatregelen. Deze kunnen gedefinieerd zijn voor de informatiebeveiliging in het algemeen of voor specifieke informatiesystemen.

Op het laagste niveau zijn de procedures en werkinstructies gedefinieerd die bestaan uit dagelijkse beheersactiviteiten met betrekking tot de informatiebeveiliging.

Het is van essentieel belang te realiseren dat het informatiebeveiligingsbeleid in algemene termen uitspraken doet over beveiligingsaspecten. Het geeft middels richtlijnen dwingend richting aan de implementatie van een adequaat beveiligingsniveau voor alle (geautomatiseerde) informatie. Maatregelen op systeemniveau komen in het beleid niet aan de orde.

Subjecten van het informatiebeveiligingsbeleid

Alle personeelsleden en alle derde partijen (leveranciers, consultants, et cetera) dienen overeenkomstig het beveiligingsbeleid te handelen en zijn dus verantwoordelijk voor het toepassen van het beveiligingsbeleid binnen hun verantwoordelijkheidsgebied.

Objecten van het informatiebeveiligingsbeleid

Het beveiligingsbeleid geldt voor alle informatie, hetzij mondeling, hetzij geschreven, geprint of elektronisch opgeslagen, die eigendom is van, in bewaring is bij of gebruikt wordt door welk gedeelte van een organisatie dan ook. Het beveiligingsbeleid geldt ook voor alle resources gebruikt in het creëren, verwerken, versturen sorteren, gebruiken of controleren van gegevens en informatie.

2 Uitgangspunten

2.1 Risicoafweging

De informatiesystemen en de daarin bevatte informatie zijn voor [Organisatie] een waardevol bezit en deze dienen als zodanig beschermd te worden. De kosten van de maatregelen en de gevolgen van maatregelen voor de werkbaarheid dienen bij het formuleren van de uitwerking van het beveiligingsbeleid in ogenschouw te worden genomen. Maatregelen dienen in verhouding te staan tot het risico dat wordt gelopen en dient geen belemmering te vormen voor de dagelijkse uitvoering van de werkzaamheden.

Beveiligingsmaatregelen kunnen worden onderverdeeld naar hun werking: preventief, detectief of correctief. Bij de bepaling van de beveiligingsmaatregelen voor een bepaalde gegevensverzameling verdient het aanbeveling de nadruk te leggen op preventieve maatregelen. Dit betekent echter niet dat de detectieve en correctieve beveiligingsmaatregelen geen of minder aandacht behoeven. De nadruk op de preventie komt voort uit het feit dat sommige kosten van een incident moeilijk in te schatten zijn. Hierbij valt te denken aan het verlies van goodwill als gevolg van inbreuken op de betrouwbaarheid van informatie.

2.2 Wetten en standaarden

Dit beveiligingsbeleid is gebaseerd op en voldoet aan vakstandaarden en 'best business practices' waaronder [de Code voor Informatiebeveiliging], [het Voorschrift Informatiebeveiliging Rijksoverheid], *van toepassing zijnde wet en regelgeving opnemen*.

Bij het gebruik, opslag, verstrekken van gegevens worden de wettelijke eisen in acht genomen, zoals opgenomen in onder andere de Wet Persoonsregistratie, de Auteurswet en de Wet Computercriminaliteit.

2.3 Implementatie en geldigheidstermijn

Het informatiebeveiligingsbeleid is van kracht per [begindatum] en is aansluitend geldig tot [einddatum]. Periodiek dient opnieuw bepaald te worden of de opgestelde richtlijnen nog steeds voldoen aan de beveiligingseisen van de organisatie.

3 Betrouwbaarheidsbehoefte en classificatie

3.1 Betrouwbaarheidsbehoefte

Het informatiebeveiligingsbeleid geeft zoals eerder gesteld dwingend richting aan de informatiebeveiliging van [Organisatie]. Deze richting wordt bepaald door de mate waarin de [Organisatie] behoefte heeft aan bescherming van de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatievoorziening. Deze beveiligingsbehoeften vormen tezamen de betrouwbaarheidsbehoefte van [Organisatie].

De betrouwbaarheidsbehoefte geeft de beveiligingsbehoefte van de organisatie als geheel aan, bepaald door de beveiligingsbehoefte op de gebieden beschikbaarheid, integriteit en vertrouwelijkheid.

De betrouwbaarheidsbehoefte van [Organisatie] is als volgt vastgesteld:

Hier de vastgestelde betrouwbaarheidsbehoefte van de organisatie opnemen, op basis van de formuleringen zoals die in paragraaf 5.4 van de scriptie zijn opgenomen.

Het beveiligingsbeleid geeft op basis van de betrouwbaarheidsbehoefte dwingend richting aan de invulling van de informatiebeveiliging. Dit wil niet zeggen dat alle informatiesystemen een gelijke, gemiddelde beveiliging behoeven. Per informatiesysteem kan (en zal) de informatiebeveiliging anders worden ingevuld al naar gelang de classificatie van het systeem. Hierop wordt in paragraaf 3.2 verder ingegaan.

3.2 Classificatie van informatiesystemen

Om op bassis van het informatiebeveiligingsbeleid te komen tot een adequaat niveau van beveiliging op tactisch en operationeel niveau is het van belang dat de informatiesysteem worden geclassificeerd. De keuze van de treffen beveiligingsmaatregelen per informatiesysteem wordt daarbij afgestemd met de classificatie die aan het informatiesysteem is toegekend. Voor de classificatie worden de kwaliteitscriteria beschikbaarheid, integriteit en vertrouwelijkheid gehanteerd. De producteigenaar, systeemeigenaar en verwerkingseigenaar is verantwoordelijk voor het classificeren van zijn producten, systemen en verwerkingen.

Bij het classificeren wordt gebruik gemaakt van de zogenaamde BIV–triple, een combinatie van drie letters. De eerste letter geeft de classificatie voor beschikbaarheid, de tweede voor integriteit en de derde voor vertrouwelijkheid. De mogelijke waarden zijn laag (L), middelmatig (M) en hoog (H). Hierna is beschreven wat onder de mogelijke waarden van de betrouwbaarheidsaspecten wordt verstaan.

Beschikbaarheid

H: Informatiesystemen waarvan de beschikbaarheid essentieel is voor de bedrijfsvoering. De informatiesystemen zijn zeer tijdskritisch, gebrek aan beschikbaarheid kan niet geaccepteerd worden.

M: Informatiesystemen waarvan de beschikbaarheid belangrijk is voor de bedrijfsvoering. De informatiesystemen zijn tijdskritisch, gebrek aan beschikbaarheid kan slechts voor een beperkte tijdsduur geaccepteerd worden.

L: Informatiesystemen waarvan de beschikbaarheid niet van primair belang is voor de bedrijfsvoering. De informatiesystemen zijn niet tijdskritisch, gebrek aan beschikbaarheid kan voor een langere periode geaccepteerd worden.

Integriteit

H: Informatiesystemen waarvan den integriteit van essentieel is voor de bedrijfsvoering. Onvolledige of niet correcte informatie leidt tot zeer grote schade voor de organisatie.

M: Informatiesystemen waarvan de integriteit belangrijk is voor de bedrijfsvoering. Onvolledige of niet correcte informatie leidt tot grote schade voor de organisatie.

L: Informatiesystemen waarvan de integriteit niet van primair belang is voor de bedrijfsvoering. Onvolledige of niet correcte informatie leidt tot geringe schade voor de organisatie.

Vertrouwelijkheid

H: Informatiesystemen waarvan de vertrouwelijkheid essentieel is voor de bedrijfsvoering. De informatiesystemen bevatten geheime informatie welke bij ongeautoriseerde kennisname of frauduleus gebruik direct of indirect significante schade voor de organisatie zal veroorzaken.

M: Informatiesystemen waarvan de vertrouwelijkheid belangrijk is voor de bedrijfsvoering. De informatiesystemen bevatten vertrouwelijke informatie welke bij ongeautoriseerde kennisname of frauduleus gebruik direct of indirect schade kan veroorzaken voor de organisatie.

L: Informatiesystemen waarvan de vertrouwelijkheid slechts van laag belang is voor de bedrijfsvoering. De systemen bevatten interne informatie welke bij ongeautoriseerde kennisname of frauduleus gebruik de organisatie in verlegenheid kan brengen en niet is bedoeld voor verspreiding buiten de organisatie.

4 Beveiligingsorganisatie

Om de informatiebeveiliging binnen [Company] vorm te geven, dienen de hieraan verbonden verantwoordelijkheden en taken in de organisatie te worden ingebed. Hiertoe dient er binnen [Company] een informatiebeveiligingsorganisatie gevormd te worden.

Binnen de beveiligingsorganisatie bestaan de volgende rollen:

- Directie/Topmanagement;
- Lijnmanagement;
- Informatie–eigenaar;
- Security officer (ook wel Security coordinator of beveiligingscoördinator);
- Security administrator (ook wel beveiligingsbeheerder);
- (Externe) controleur.

Hier de beschrijving van de taken en verantwoordelijkheden uit paragraaf 2.3 invoegen.

5 Beveiligingseisen ten aanzien van personeel

Deze beveiligingsrichtlijnen zijn gericht op het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen. *Hier de van toepassing zijnde beveiligingsrichtlijnen voor dit onderwerp opnemen.*

6. Fysieke beveiliging en beveiliging van de omgeving

Deze beveiligingsrichtlijnen zijn gericht op het voorkomen van ongeautoriseerde toegang tot, schade aan of verstoring van de gebouwen en informatie van de organisatie. *Hier de van toepassing zijnde beveiligingsrichtlijnen voor dit onderwerp opnemen.*

7. Beheer van communicatie- en bedieningsprocessen

Deze beveiligingsrichtlijnen zijn gericht op het garanderen van een correcte en veilige bediening van IT–voorzieningen. *Hier de van toepassing zijnde beveiligingsrichtlijnen voor dit onderwerp opnemen.*

8. Toegangsbeveiliging

Deze beveiligingsrichtlijnen zijn gericht op het beheersen van de toegang tot informatie. *Hier de van toepassing zijnde beveiligingsrichtlijnen voor dit onderwerp opnemen.*

9. Ontwikkeling en onderhoud van systemen

Deze beveiligingsrichtlijnen zijn gericht op waarborgen dat beveiliging wordt ingebouwd in informatiesystemen. *Hier de van toepassing zijnde beveiligingsrichtlijnen voor dit onderwerp opnemen.*

10. Continuïteitsmanagement

Deze beveiligingsrichtlijnen zijn gericht op het reageren op verstoringen van bedrijfsactiviteiten en het beschermen van de kritieke bedrijfsprocessen tegen de effecten van grootschalige storingen of calamiteiten. *Hier de van toepassing zijnde beveiligingsrichtlijnen voor dit onderwerp opnemen.*

11. Naleving

Deze beveiligingsrichtlijnen zijn gericht op het voorkomen van schending van strafrechtelijke of civielrechtelijke wetgeving, wettelijke, reglementaire of contractuele verplichtingen of beveiligingseisen. *Hier de van toepassing zijnde beveiligingsrichtlijnen voor dit onderwerp opnemen.*

Vragenlijsten bepaling betrouwbaarheids-behoefte

Om de afhankelijkheid van de informatievoorziening te bepalen wordt gebruik gemaakt van een aangepaste SPRINT methode, zoals beschreven in hoofdstuk 5. In deze bijlage zijn de vragenlijsten opgenomen zoals die gebruikt kunnen worden om de afhankelijkheid te bepalen op basis van de SPRINT methode.

De vragenlijsten zijn in essentie de vertaling van de originele vragen van de SPRINT methode naar het Nederlands. In vergelijking met SPRINT zijn twee wijzigingen doorgevoerd. Ten eerste zijn de vragen gericht op de informatievoorziening als geheel in plaats van op een individueel informatiesysteem. Ten tweede kennen de vragen drie mogelijke antwoorden in plaats van vijf. De achtergrond van deze wijzigingen is beschreven in paragraaf 6.4.

C.1 Beschikbaarheid

H: Hoge impact, variërend van ernstige schade tot het in gevaar brengen van het voortbestaan van de organisatie.
M: Matige impact, variërend van lichte schade tot matige schade.
L: Lage impact, variërend van geen schade tot lichte schade.

	Impact	
Concurrentienadeel In welke mate kan de organisatie schade oplopen wanneer een concurrent toegang heeft tot de in de informatievoorziening bevatte informatie?		
Direct verlies van omzet In welke mate kan er omzet verloren gaan als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?		
Publiek vertrouwen In welke mate kan het vertrouwen van de klanten, het publiek of de aandeelhouders en leveranciers geschaad worden als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?		
Bijkomende kostend In welke mate kunnen extra kosten ontstaan als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?		
Juridische aansprakelijkheid In welke mate kan het uitlekken van in de informatievoorziening bevatte informatie tot gevolg hebben dat juridische, contractuele of anderszins voorgeschreven richtlijnen worden doorbroken?		
Moraal van de medewerkers In welke mate kan het uitlekken van in de informatievoorziening bevatte informatie een schadend effect hebben op de moraal en/of de motivatie van de medewerkers?		
Fraude In welke mate kunnen goederen of geld worden verduisterd als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?		
Algehele score		

C.2 Integriteit

H: Hoge impact, variërend van ernstige schade tot het in gevaar brengen van het voortbestaan van de organisatie.
M: Matige impact, variërend van matige schade tot *behoorlijke* schade.
L: Lage impact, variërend van geen schade tot lichte schade.

	Impact	
Managementbeslissingen In welke mate kunnen managementbeslissingen negatief worden beïnvloed als gevolg van onjuistheden in de in de informatiesystemen bevatte informatie?		
Direct verlies van business In welke mate kan omzet verloren gaan als gevolg van onjuistheden in de in de informatiesystemen bevatte informatie?		
Publiek vertrouwen In welke mate kan het vertrouwen van de klanten, het publiek en/of de aandeelhouders en leveranciers worden geschaad als gevolg van onjuistheden in de in de informatiesystemen bevatte informatie?		
Bijkomende kosten In welke mate kunnen extra kosten ontstaan als gevolg van onjuistheden in de in de informatievoorziening bevatte informatie?		
Juridische aansprakelijkheid In welke mate kunnen onjuistheden in de in de informatievoorziening bevatte informatie tot gevolg hebben dat juridische, contractuele of anderszins voorgeschreven richtlijnen worden doorbroken?		
Moraal van de medewerkers In welke mate kunnen de moraal en/of de motivatie van de medewerkers worden geschaad indien zij niet op de in de informatiesystemen bevatte informatie kunnen steunen?		
Fraude In welke mate kan het verduisteren van goederen of geld het gevolg zijn van of onopgemerkt blijven door ongeautoriseerde wijzigingen in de in de informatievoorziening bevatte informatie?		
Verstoring van bedrijfsprocessen In welke mate kunnen de primaire bedrijfsprocessen op enige andere wijze worden verstoord door onjuistheden in de in de informatievoorziening bevatte informatie?		
Algehele score		

C.3 Vertrouwelijkheid

H: Hoge impact, variërend van ernstige schade tot het in gevaar brengen van het voortbestaan van de organisatie.
M: Matige impact, variërend van lichte schade tot matige schade.
L: Lage impact, variërend van geen schade tot lichte schade.

	Impact				
	een uur	een dag	2-3 dagen	een week	een maand
Managementbeslissingen In welke mate kunnen managementbeslissingen negatief worden beïnvloed als gevolg van het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie?					
Direct verlies van omzet In welke mate kan er omzet verloren gaan als gevolg van het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie?					
Publiek vertrouwen In welke mate wordt het vertrouwen van de klanten, het publiek of de aandeelhouders en leveranciers geschaad als gevolg van het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie?					
Bijkomende kostend In welke mate kunnen extra kosten ontstaan als gevolg van het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie?					
Juridische aansprakelijkheid In welke mate kan het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie tot gevolg hebben dat juridische, contractuele of anderszins voorgeschreven richtlijnen worden doorbroken?					
Moraal van de medewerkers In welke mate kunnen de moraal en/of de motivatie van de medewerkers geschaad worden als gevolg van het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie?					
Fraude In welke mate kan het verduisteren van goederen of geld het gevolg zijn van of onopgemerkt blijven door het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie?					
Verstoring van bedrijfsprocessen In welke mate kunnen de primaire bedrijfsprocessen op enige wijze worden verstoord door het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie?					
Herstelwerkzaamheden In welke mate kunnen extra kosten ontstaan in verband met het herstel van de achterstand in werkzaamheden als gevolg van het niet beschikbaar zijn van de in de informatievoorziening bevatte informatie.					
Algehele score					

Verkennend onderzoek naar de bruikbaarheid van de SPRINT methode

D

Teneinde de bruikbaarheid te bepalen van de SPRINT afhankelijkheidsanalyse voor het vast-stellen van de betrouwbaarheidsbehoefte heb ik een verkennend onderzoek uitgevoerd door voor een fictieve casus een proefanalyse uit te voeren. De casus is in de kern gebaseerd op een parktijksituatie, geanonimiseerd en met diverse aanpassingen en wijzigingen om de privacy van de betreffende organisatie niet te schaden.

D.1 Criteria voor de bruikbaarheid van de SPRINT afhankelijkheidsanalyse

De proefanalyse is uitgevoerd door onafhankelijk van elkaar met drie materie-experts (ME's) de proefanalyse uit te voeren op basis van de geschetste casus. Daarbij is de bruikbaarheid van de methode beoordeeld op de volgende aspecten:

- Stabiliteit: zijn de vastgestelde betrouwbaarheidsbehoeften consistent?
- Gebruiksgemak: is de methode eenvoudig en prettig in gebruik?
- Efficiëntie en effectiviteit: is het gebruik van de methode efficiënt en effectief?

- Detaillering: Biedt de methode voldoende detail om de betrouwbaarheidsbehoefte vast te kunnen stellen?
- Algehele geschiktheid: is de methode geschikt om de betrouwbaarheidsbehoefte van een organisatie als geheel te bepalen en als basis voor het beveiligingsbeleid?

Tevens is de proefanalyse gebruikt om te bepalen op welke wijze het beste de eindwaarde per kwaliteitsaspect B,I,V kan worden bepaald.

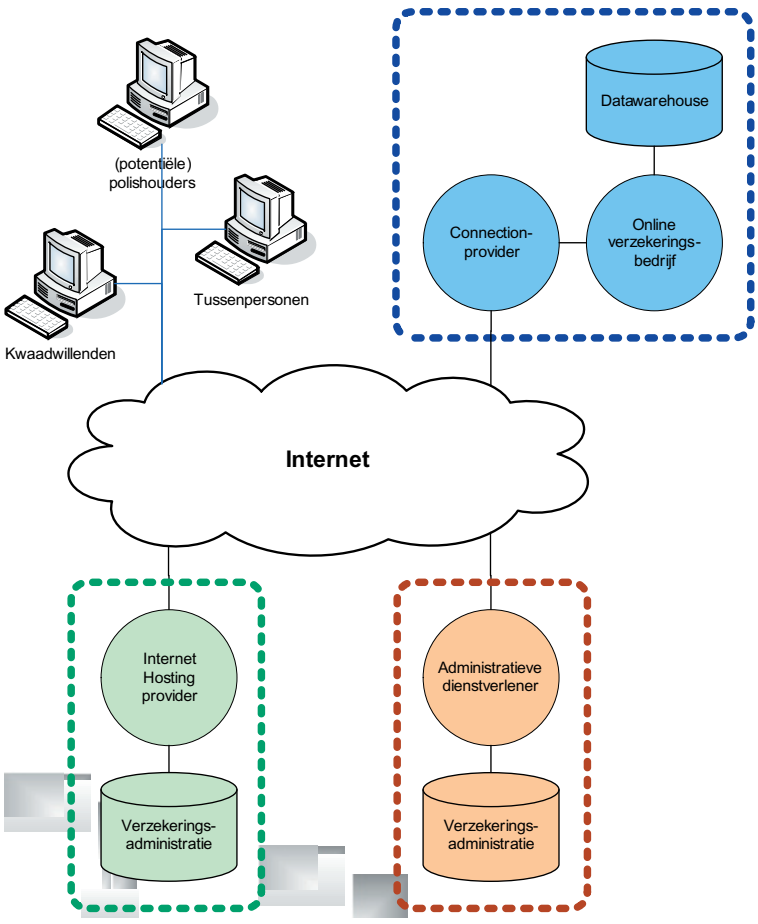
D.2 De gehanteerde casus

De organisatie die centraal staat in de casus is een bedrijf dat online kapitaalverzekeringen aanbiedt, waarbij hoofdzakelijk gebruik wordt gemaakt van tussenpersonen. Het betreft een organisatie die nog niet over informatiebeveiligingsbeleid beschikt, noch over enige andere vorm van geformaliseerde beveiligingsdocumentatie en/of –procedures. De organisatie is nog erg jong (minder dan twee jaar geleden opgericht) en wordt gevormd door een klein maar zeer gemotiveerd team van medewerkers. De organisatiestructuur is plat en communicatie daardoor direct.

De organisatie maakt intensief gebruik van informatievoorziening en met name geautomatiseerde informatieverwerkende systemen. Ik geef hieronder een schets van deze informatiesystemen van de organisatie. Deze informatie is opgenomen ter compensatie van het feit dat er geen manager van het bedrijf beschikbaar is waarmee een interview kan worden gevoerd. Er moet immers toch voldoende bekend zijn over een organisatie om de afhankelijkheid te beoordelen.

De organisatie beschikt over de volgende informatiesystemen:

1 Extern webserver;
2 Interne webserver & Datawarehouse;
3 Gegevensopslag & –verwerking (back office).



Figuur 2: De infrastructuur van de casusorganisatie schematisch weergegeven

Extern gehoste webserver

Een externe webhosting provider verzorgt de hosting van het publieke deel van de website van de verzekeraar en de koppeling hiervan aan het internetadres van het bedrijf. De web-server vormt het eerste communicatiepunt tussen de verzekeraar en (potentiële) polishouders, tussenpersonen en andere bezoekers.

De webhosting provider draagt behalve voor de hosting tevens zorg voor het ontwerp en het onderhoud van de site. Op het publieke deel van de website is geen persoonsgebonden informatie aanwezig van bijvoorbeeld klanten of tussenpersonen. Wanneer informatie op de publieke website moet worden aangepast levert de verzekeraar de informatie aan, waarna de

hosting provider de aanpassing van de site verzorgt. De verzekeraar heeft zelf geen speciale toegang tot de webserver. De website is ingericht op een Windows NT server met Internet Information Server.

Webserver & Datawarehouse

De verzekeraar heeft in het eigen pand een computersysteem ingericht met daarop een data–warehouse waarin alle polishouder–, tussenpersoons– en polisinformatie aanwezig is. De informatie in het datawarehouse wordt dagelijks bijgewerkt met behulp van XML–bestanden ontvangen van het moederbedrijf via FTP–communicatie . Hierbij maakt Het moederbedrijf contact met de FTP–server van de verzekeraar waarna het XML–bestand op de machine wordt geplaatst. Deze XML–bestanden bevatten alleen de wijzigingen ten opzichte van de reeds aanwezige informatie.

In de eigen computerruimte bevindt tevens zich een webserver welke polishouders en tussenpersonen toegang verschaft tot de polishouder– en polisgegevens die zich in het data–warehouse bevinden. De webpagina's die door deze webserver worden aangeboden zijn visueel geïntegreerd in de publieke website van de verzekeraar.

Elke klant heeft een eigen gebruikersnaam en wachtwoord waarmee hij/zij toegang kan krijgen tot de informatie betreffende zijn of haar polis. Tussenpersonen hebben een gebrui–kersnaam en wachtwoord op verschillende niveaus waarmee de informatie ingezien kan worden betreffende de polissen van de door de tussenpersoon vertegenwoordigde klanten. Deze verschillende niveaus houden in dat een organisatie die als tussenpersoon fungeert (een TP–organisatie) om te beginnen een gebruikersnaam en wachtwoord heeft waarmee alle gegevens van door deze organisatie vertegenwoordigde polishouders kunnen worden ingezien. Daarnaast kunnen binnen een dergelijke organisatie aparte afdelingen/locaties een gebruikersnaam/wachtwoord krijgen waarmee alleen gegevens van voor de betreffende afde–ling/locatie relevante gegevens kunnen worden ingezien. Ten slotte kan aan een medewerker van een TP–organisatie een gebruikersnaam en wachtwoord toegekend krijgen waarmee hij/zij alleen de door hem of haar vertegenwoordigde polisinformatie kan worden ingezien.

Toegang tot deze besloten pagina's wordt verkregen na opgave van gebruikersnaam en wacht–woord. De medewerkers van de verzekeraar gebruiken één gebruikersnaam en wachtwoord waarmee alle polissen kunnen worden ingezien. Daarnaast is er voor de directeur en de con–troller een mogelijkheid om het datawarehouse in alleen–lezen–modus te benaderen via een databasekoppeling om gegevensanalyses uit te voeren.

Het onderhoud en beheer van zowel de webserver als het datawarehouse is uitbesteed aan een IT dienstverlener. De verzekeraar heeft directe invloed op de inrichting en het beheer van de webserver en het datawarehouse. De IT dienstverlener is hierbij de uitvoerende partij van de wensen en eisen van de verzekeraar. Met de IT dienstverlener is een SLA afgesloten waarin onder andere afspraken zijn vastgelegd omtrent de te leveren diensten en de daaraan te stellen eisen.

De webserver is gekoppeld aan internet middels een verbinding met een internetprovider. Toegang tot de webserver vanaf internet verloopt via een firewall. Met de internetprovider is een SLA gesloten waarin afspraken zijn opgenomen met betrekking tot onder andere beschikbaarheid van de verbinding.

Gegevensopslag en -verwerking (back office)

Het moederbedrijf verzorgt de back–office activiteiten voor de organisatie, betreffende alle administratieve activiteiten gerelateerd aan cliënten, tussenpersonen en polissen. Deze informatie wordt opgeslagen in het speciale applicatie. Elke nacht wordt automatisch via FTP–verkeer een XML–bestand naar de organisatie verstuurd dat de wijzigingen van de polisgegevens bevat. Alle inschrijvingen, offertes et cetera worden door het moederbedrijf verwerkt en via het XML–verkeer doorgegeven aan de organisatie. Het beheer en onderhoud van de informatievoorziening is volledig in handen van het moederbedrijf. De organisatie heeft met het moederbedrijf alleen afspraken gemaakt over het niveau van de dienstverlening. De organisatie is nauw betrokken bij ontwikkeling van de back office software. Wanneer de organisatie nieuwe producten wenst te introduceren wordt dit in overleg met het moederbedrijf geïntegreerd in de applicatie.

Behalve de bestandsoverdracht vanuit het moederbedrijf naar de organisatie vindt ook bestandsoverdracht plaats vanuit de organisatie naar het moederbedrijf. Middels een FTP–verbinding worden door de organisatie vanuit het datawarehouse eventuele wijzigingen in agenteninformatie gecommuniceerd naar het moederbedrijf.

D.3 Proefbepaling van de vertrouwelijkheid

Op basis van de geschetste casus heb ik samen met twee andere terzake deskundigen een proefbepaling van de exclusiviteit uitgevoerd. Allereerst heb ik zelf de analyse zelfstandig

uitgevoerd. In aanvulling daarop hebben de materie–experts onafhankelijk van elkaar als assessor de vertrouwelijkheidsbehoefte van de casusorganisatie bepaald. Daartoe hebben zij de casus doorgelezen, en vervolgens ondersteund door mij de vragenlijst ingevuld en de vertrouwelijkheidsbehoefte bepaald. Als leidraad voor de uitvoering heb ik de afbakeningen zoals beschreven in paragraaf 5.4 aan de assessoren beschikbaar gesteld. Deze dienden als referentie voor het kiezen van het antwoorden per vraag. De algehele eindscore heb ik de assessoren zelfstandig laten bepalen, teneinde in te kunnen schatten op welke wijze (gemiddelde score, hoogste score of anders) deze het best kan worden vastgesteld.

Middels vergelijking van de door de materie–experts bepaalde vertrouwelijkheidsbehoeften heb ik de stabiliteit van de methode onderzocht. Aansluitend op het vaststellen van de vertrouwelijkheidsbehoefte heb ik de assessoren de volgende vragen gesteld om de bruikbaarheid van de methode in te schatten op basis van de in D.1 genoemde aspecten:

- Is de gebruikte methode voldoende duidelijk, eenvoudig en prettig in gebruik?
- Is het gebruik van de methode efficiënt en effectief?
- Is de vragenlijst voldoende uitgebreid en gedetailleerd om een volledig beeld te hebben van de vertrouwelijkheidsbehoefte?
- Is de methode geschikt om de betrouwbaarheidsbehoefte van elke organisatie te bepalen als basis voor het beveiligingsbeleid?

D.4 Resultaten van de proefuitvoering

Hierna zijn allereerst de uitkomsten weergegeven van de drie materie–experts die onafhankelijk van elkaar op basis van de casus de vertrouwelijkheidsbehoefte hebben vastgesteld. Aansluitend wordt ingegaan op de beste wijze om de totaalscore te bepalen op basis van de antwoorden op de deelvragen. Ten slotte worden de antwoorden van de materie–experts op de hiervoor geformuleerde vragen weergegeven.

D.4.1 Scoretabel vertrouwelijkheidsbehoefte

H: Hoge impact, variërend van ernstige schade tot het in gevaar brengen van het voortbestaan van de organisatie.
M: Matige impact, variërend van lichte schade tot matige schade.
L: Lage impact, variërend van geen schade tot lichte schade.

	Impact		
	ME1	ME2	ME3
Concurrentienadeel In welke mate kan de organisatie schade oplopen wanneer een concurrent toegang heeft tot de in de informatievoorziening bevatte informatie?	H	H	H
Direct verlies van omzet In welke mate kan er omzet verloren gaan als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?	M	M	H
Publiek vertrouwen In welke mate kan het vertrouwen van de klanten, het publiek of de aandeelhouders en leveranciers geschaad worden als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?	H	H	H
Bijkomende kostend In welke mate kunnen extra kosten ontstaan als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?	M	M	M
Juridische aansprakelijkheid In welke mate kan het uitlekken van in de informatievoorziening bevatte informatie tot gevolg hebben dat juridische, contractuele of anderszins voorgeschreven richtlijnen worden doorbroken?	H	H	M
Moraal van de medewerkers In welke mate kan het uitlekken van in de informatievoorziening bevatte informatie een schadend effect hebben op de moraal en/of de motivatie van de medewerkers?	H	M	H
Fraude In welke mate kunnen goederen of geld worden verduisterd als gevolg van het uitlekken van de in de informatievoorziening bevatte informatie?	M	M	L
Algehele eindscore	**H**	**H**	**H**

Uit deze blijkt dat de methode binnen de casus relatief stabiel is. Van de zeven vragen worden er drie door alle experts hetzelfde beantwoord. In de andere vier vragen verschilde altijd maar één expert in zijn antwoord. Het afwijkende antwoord verschilde in alle gevallen slechts één nvieau van de andere antwoorden. De bepaalde algehele eindscore is in alle gevallen gelijk.

Gezien de beperkte verschillen in de beantwoording van de detailvragen en de overeenstemming in de algehele eindscore, waarop binnen de methode de nadruk ligt, beschouw ik de methode als voldoende stabiel om te hanteren als macro–risicoanalyse binnen de methode voor het systematisch opstellen van informatiebeveiligingsbeleid.

D.4.2 Bepaling van de algehele eindscore

Bepaling van de totaalscore door de materie–experts is in eerste instantie niet eenduidig gebleken. Weliswaar gaven alle experts een algehele score 'Hoog', echter de wijze waarop zij daartoe kwamen werd door hen niet eenduidig verklaard. ME1 gaf aan voor hoog te kiezen omdat de scores weliswaar divers zijn, maar omdat hij de 'Hoog' scores een groter belang toekent dat de scores 'Middelmatig' en de score 'Laag' nog minder belang. ME2 gaf aan voor 'Hoog' te kiezen op basis van de drie deelscores 'Hoog' die hij had gegeven, omdat hij drie keer hoog reden genoeg acht om de gehele organisatie als hoog te classificeren. ME3 gaf aan te kiezen voor een globaal gemiddeld, gekoppeld aan het beeld dat hij van de organisatie had op basis van de casus. Geen van de experts gaf aan bij het bepalen van de algehele score de vragen een verschillende gewicht toe te kennen.

Teneinde te komen tot een eindconclusie hoe de algehele score het beste te bepalen, heeft een aanvullende plenaire sessie plaatsgevonden met de betrokken materie–experts. Daarbij is op basis van de drie geschetste meningen een consensus bepaald. Naar aanleiding van de standpunten van ME1 en ME2 acht men de beste manier om de algehele score te bepalen het toekennen van een toenemend belang aan respectievelijk de scores L, M en H. Reden hiervoor is het voorzichtigheidsbeginsel dat liever teveel wordt beveiligd dan te weinig. Dus een score Hoog wordt belangrijker geacht van een score Laag, ongeacht de vraag. Daarbij dient in lijn met de ideeën van ME3 de expert altijd de bepaalde algehele score te toetsen aan het beeld dat hij/zij heeft van de organisatie op basis van zijn/haar ervaring en expertise.

In de discussie is voorgesteld als globale indicatie aan te houden dat een score Hoog 3 punten is, Midden 2 punten en Laag 1 punt. Een dergelijke telling maakt het mogelijk aan te sluiten bij de verdeling die in paragraaf 5.3.2 is geschetst. Wanneer vervolgens de punten worden opgeteld en de score wordt gedeeld door het maximale aantal punten (in dit geval 7×3=21) wordt een procentuele score bepaald. Wanneer deze wordt aangesloten bij de verdeling van paragraaf 5.3.2 kan aan elke totaalscore een indicatieve algehele score worden toegekend. In het geval van de door de materie–experts bepaalde vertrouwelijkheidsbehoeften wordt de uitkomst als volgt:

Score ME1: 18/21 = 85,7% → Hoog
Score ME2: 17/21 = 81,0% → Hoog
Score ME3: 16/21 = 76,2% → Hoog

Deze indicatieve uitkomsten sluiten aan bij de door de experts individueel bepaalde algehele scores. Daaruit blijkt dat de indicatieve verdeling voor deze proefanalyse aansluit bij de *professional judgement* van de materie–experts. Tevens mag worden aangenomen dat de indicatieve verdeling een goede maat is voor de bepaling van de betrouwbaarheidsbehoefte in het algemeen. Uiteraard zal de verdeling bij frequente uitvoering van de methode kunnen worden bijgesteld. Een mogelijkheid om dit te doen is bijvoorbeeld door het gebruik van een neuraal netwerk.

D.4.2 Beantwoording van de aanvullende vragen

Hieronder volgt de weergave van de antwoorden die de materie–experts hebben gegeven op de vragen ter evaluatie van de bruikbaarheid van de (aangepaste) SPRINT methode.

Is de gebruikte methode voldoende duidelijk, eenvoudig en prettig in gebruik?

ME1: Jazeker. De methode is snel inzetbaar en voldoende eenvoudig om ook met niet–experts te gebruiken. De vragen zijn duidelijk geformuleerd en geven concreet aan wat het issue is.

ME2: Ja. De vragen zijn helder en pakkend. Dit heeft als voordeel dat de vertegenwoordiger van de organisatie waarvoor de vraag wordt beantwoord echt wordt geconfronteerd met waar het echt om gaat: business impact.

ME3: Door de eenvoud is de methode makkelijk te gebruiken. De vragen zijn voldoende duidelijk en concreet met de juiste diepgang voor het onderwerp: beveiligingsbeleid op strategisch niveau.

Is het gebruik van de methode efficiënt en effectief?

ME1: Gezien het gemak waarmee in korte tijd de vertrouwelijkheidsbehoefte is vastgesteld, kan de methode zeker als efficiënt worden aangemerkt. De effectiviteit is moeilijk in te schatten op basis van een casus. De vastgestelde waarde komt overeen met het beeld dat ik als expert heb van de geschetste organisatie. De praktijk zal echter moeten uitwijzen of dit in het algemeen zal gelden.

ME2: De vragenlijst lijkt een geschikte methode te zijn om op strategische niveau snel tot de kern van de zaak door te dringen. Mijn eerste beeld is dat de methode dus in aanleg efficiënt en effectief is. Echter de vraag of de uitkomst goed aansluit bij praktijkgevallen is nu nog niet volledig in te schatten. Positief punt is wel dat SPRINT de betrokkenheid van een vertegenwoordiger van het betreffende bedrijf sterk stimuleert en in dat opzicht zeer nuttig is in het risicobewustwordingsproces. In die zin is de methode op dat punt in elk geval effectief.

ME3: Ja, zo op het eerste gezicht wel. De vertrouwelijkheidsbehoefte is in korte tijd bepaald. Daarbij is echt de kern van de zaak geraakt, zonder teveel in te gaan op informatiesystemen, kans op incidenten en dergelijke die niet direct relevant zijn op strategisch niveau.

Is de vragenlijst voldoende uitgebreid en gedetailleerd om een volledig beeld te hebben van de vertrouwelijkheidsbehoefte?

ME1: De vragen zijn voldoende uitgebreid om een goed beeld van de vertrouwelijkheidsbehoefte te vormen. De volledigheid van een dergelijk vragenlijst kan echter nooit zo vluchtig worden vastgesteld. Zie de vragenlijst als niet–puttend. Uiteraard heeft het ISF goed nagedacht over de vragen en kun je ervan uitgaan dat deze goed is. Er zijn echter altijd nog wel vragen bij te bedenken die de lijst nog zouden kunnen verbeteren.

ME2: De vragen die gesteld zijn, zijn allemaal relevant. De in de vragen behandelde onderwerpen raken voldoende onderwerpen om de vertrouwelijkheidsbehoefte op te baseren.

ME3: Een expert heeft snel de neiging om heel snel een ‘oordeel’ te vellen. Gevolg daarvan is dat de expert vaak al een beeld van de betrouwbaarheidsbehoefte heeft voordat nog maar begonnen is met de SPRINT analyse. De methode is in dit geval nuttig om het initiële beeld van de expert te toetsen en het beeld voor de organisatievertegenwoordiger te schetsen. Je zou het kunnen zien als een ‘verantwoording’ van het gevoeld van de expert. Daarvoor is de lijst uitgebreid en gedetailleerd genoeg.

Is de methode geschikt om de betrouwbaarheidsbehoefte van elke organisatie te bepalen als basis voor het beveiligingsbeleid?

ME1: In principe wel, het maakt bijvoorbeeld niet uit in welke branche in welke branche een organisatie actief is. Wel kan het zo zijn dat een organisatie intern te zeer gediversifieerd is om één beveiligingsbeleid op te leggen. In dat geval verdient het aanbeveling om het beveiligingsbeleid per bedrijfsonderdeel of divisie op te zetten. Daarbij is de methode dan zeker weer toepasbaar.

ME2: De methode is zal met name nuttig zijn binnen het midden– en kleinbedrijf. Voor complexere organisaties zal het lastiger zijn het beleid volgens standaard methodiek te bepalen omdat de uitzonderingen en specifieke situaties hier groter zullen zijn.

ME3: Ja, omdat het bedoeld is om een globale indruk te krijgen van de vertrouwelijkheids–behoefte. Het is aan de betrokken expert om de beantwoording te toetsen aan het beeld dat bij zelf van een organisatie heeft op basis van zijn kennis er ervaring. Het uiteindelijke vaststellen van de vertrouwelijkheidsbehoefte (en ook de andere kwa–liteitsaspecten) is altijd een wisselwerking tussen het gebruik van de vragenlijst en de aanwezige expert knowledge. Mocht de situatie binnen een organisatie aanleiding geven te twijfelen aan de bruikbaarheid van de methode, dan is het aan de expert om dit tijdig te signaleren.

Universum van beveiligingsrichtlijnen

In deze bijlage is de verzameling van beveiligingsrichtlijnen opgenomen die een deel van het universum beslaat, zoals aangegeven in hoofdstuk 7. Dit deeluniversum is opgebouwd uit de Code voor Informatiebeveiliging [NNI2000] omdat dit een algemeen aanvaarde standaard is die direct bruikbare richtlijnen biedt. Om de scope te beperken tot wat binnen een afstudeeronderzoek haalbaar is, heb ik mij gericht op één deelgebied van informatiebeveiliging, te weten richtlijnen gericht op fysieke beveiliging.

De hier opgenomen richtlijnen dienen primair om de voorgestelde methode te illustreren en te toetsen. Het betreft geen uitputtend overzicht van beveiligingsrichtlijnen voor het betreffende onderwerp. Indien op basis van deze methode een volledig universum wordt opgesteld verdient het aanbeveling ook andere bronnen voor beveiligingsrichtlijnen te betrekken.

E.1 Beveiligde ruimten

E.1.1 Fysiek beveiliging van de omgeving

E.1.1.1	Verscheidene fysieke barrières dienen te worden opgeworpen rond terreinenen en IT voorzieningen. Elke barrière creëert een beveiligde zone. De grenzen van de beveiligde zone dienen duidelijk te worden gedefinieerd.	L - L	B I V	*	+
E.1.1.2	De beveiligde zone van een gebouw of lokatie waarin zich IT voorzieningen bevinden, dient fysiek sluitend te zijn. De buitenmuren van de lokatie dienen solide te zijn en alle buitendeuren dienen op de juiste manier beveiligd te zijn tegen toegang door onbevoegden.	L - L	B I V	*	+
E.1.1.3	Er dient een bemande receptie aanwezig te zijn of een andere middel om de fysieke toegang tot het bebouw te beheersen. Alleen geautoriseerde personeel mag toegang hebben tot de lokatie of het gebouw.	M - M	B I V	*	+
E.1.1.4	Fysieke barrières dienen te worden uitgebreid van de harde vloer tot het harde plafond om ongeautoriseerde toegang en verontreiniging van het milieu, bijvoorbeeld bij brand of wateroverlast te voorkomen.	H - -	B I V		
E.1.1.5	Alle branddeuren in een beveiligde zone dienen te zijn voorzien van een alarm en dienen automatisch te sluiten.	M - -	B I V		

E.1.2 Fysiek toegangsbeveiliging

E.1.2.1	Bezoekers van beveiligde gebieden dienen altijd begeleid te worden of toestemming hebben om het gebied te betreden en de datum en het tijdstip van hun aankomst en vertrek dienen te worden genoteerd, Ze dienen alleen toegang te krijgen voor bepaalde, geautoriseerde doeleinden.	M M M	B I V	*	+
E.1.2.2	Bezoekers dienen instructies te ontvangen over de beveiliggingseisen van het gebied en over de te volgen procedures in geval van calamiteiten.	H - -	B I V		
E.1.2.3	Toegang tot gevoelige informatie en IT–voorzieningen dient te worden gecontroleerd en beperkt te zijn tot geautoriseerde personen.	L L L	B I V	*	+
E.1.2.4	Met behulp van authenticatie–maatregelen, bijvoorbeeld een toegangspasje en/of pincode, dient alle toegang geautoriseerd en gevalideerd te worden.	M M M	B I V	*	+
E.1.2.5	Een zorgvuldige 'audit trail' (logboek waarin alle relevante gegevens worden geadministreerd) moet worden bijgehouden van iedereen die toegang heeft gekregen.	H H H	B I V	*	+
E.1.2.6	Al het personeel dient een zichtbare identificatie te dragen en dient te worden aangemoedigd om ontbrekende personen zonder begeleiding en iedereen die geen zichtbare identificatie draag daarop aan te spreken.	H H H	B I V	*	X

E.1.3 Beveiliging van kantoren, ruimten en voorzieningen

E.1.3.1	De belangrijkste voorzieningen dienen geplaatst te worden in gebieden die niet publiekelijk of algemeen toegankelijk zijn.	L L M	B I V	*	+
E.1.3.2	De gebouwen dienen onopvallend te zijn en zo min mogelijk aanwijzingen te geven over wat er binnen plaatsvindt en er mogen geen duidelijke tekenen binnen of buiten het gebouw zijn aangebracht die op de aanwezigheid van IT–activiteiten duiden.	L - -	B I V		
E.1.3.3	Ondersteunende apparatuur, zoals kopieermachines en faxapparatuur, dienen op een geschikte plaats binnen de beveiligde zone te worden opgesteld, om aantasting van de vertrouwelijkheid van informatie te vermijden.	L - L	B I V	*	+
E.1.3.4	Deuren en ramen dienen te worden afgesloten als er niemand aanwezig is en extra beveiliging dient te worden overwogen voor ramen; dit geldt met name voor ramen op de begane grond.	L - L	B I V	*	+
E.1.3.5	Er dienen geschikte anti–inbraaksystemen te worden geïnstalleerd conform professionele normen. Deze anti–inbraaksystemen dienen regelmatig getest te worden en alle buitendeuren en toegankelijke ramen bestrijken. Onbemande ruimten dienen te allen tijde van een alarmsysteem te zijn voorzien. Ook andere ruimte, bijvoorbeeld de computerruimte of de communicatieruimte, dienen door het alarmsysteem te worden bestreken.	M - M	B I V	*	+
E.1.3.6	IT–voorzieningen die door de organisatie zelf gemanaged worden, dienen fysiek gescheiden te zijn van systemen die door derden worden gemanaged.	M M M	B I V	*	+
E.1.3.7	Adresboeken en interne telefoongidsen van de organisatie waarin de gebieden vermeld staan waar gevoelige informatie wordt verwerkt, dienen niet vrij toegankelijk te zijn voor het publiek.	- - M	B I V	*	+
E.1.3.8	Gevaarlijke en brandbare materialen dienen te worden opgeslagen op een veilige afstand van een beveiligde zone. Grote voorraden, zoals van kantoorartikelen, mogen pas op het moment dat ze nodig zijn in de beveiligde ruimte worden opgeslagen.	L - -	B I V		
E.1.3.9	Reserveapparatuur en media met reservekopieën dienen op veilige afstand te worden bewaard, om te voorkomen dat ze beschadigd raken wanneer zich op de hoofdlokatie een calamiteit voordoet.	M M -	B I V		

E.1.4 Werken in beveiligde ruimten

E.1.4.1	Het personeel dient alleen indien noodzakelijk op de hoogte te zijn van het bestaan van of de activiteiten binnen een beveiligde ruimte.	H H H	B I V	*	
E.1.4.2	Zonder toezicht werken in beveiligde ruimten dient te worden voorkomen, zowel om veiligheidsredenen als om de kans op kwaadwillige handelingen te voorkomen.	M M M	B I V	*	
E.1.4.3	Leegstaande beveiligde ruimten dienen fysiek te zijn afgesloten en periodiek te worden gecontroleerd.	H H H	B I V	*	

E.1.4.4	Aan personeel van externe ondersteunende diensten dient alleen wanneer dit noodzakelijk is beperkte toegang te worden verleend tot beveiligde ruimten of voorzieningen waar gevoelige informatie wordt verwerkt. Deze toegang dient goed–gekeurd en bewaakt te worden. Aanvullende barrières en beveiligde gebieden kunnen nodig zijn om de fysieke toegang tussen twee ruimtes binnen de beveiligde zone met verschillende beveiligingseisen te beheersen.	L L L		*	+
E.1.4.5	Fotografische, video–, audio– of andere opnameapparatuur dient niet te worden toegestaan, tenzij hier autorisatie voor is verleend.	- - M		*	+

E.1.5 Afgescheiden ruimten voor laden en lossen van goederen

E.1.5.1	De toegang tot de voorraadruimte van buitenaf dient te zijn voorbehouden aan geautoriseerd personeel met een geldige identificatie.	M - M	B I V	*	+
E.1.5.2	De voorraadruimte dient zodanig ontworpen te zijn dat voorraden binnengebracht kunnen worden, zonder dat men andere delen van het gebouw kan betreden.	M M M	B I V	*	N
E.1.5.3	De buitendeur(en) van de ruimte dient / dienen te worden afgesloten wanneer de binnendeur wordt geopend.	H H H	B I V	*	N
E.1.5.4	Binnenkomende materialen dienen te worden gecontroleerd op mogelijke gevaren voordat zij worden overgebracht van de voorraadruimte naar de lokatie waar zij nodig zijn.	H H -	B I V		
E.1.5.5	Binnenkomende materialen dienen bij aankomst op de lokatie te worden geregistreerd.	M - -	B I V		

E.2 Beveiliging van apparatuur

E.2.1 Het plaatsen en beveiligen van apparatuur

E.2.1.1	Als het mogelijk is, dient de apparatuur zodanig te worden geplaatst dat er zo min mogelijk toegang tot de werkvloer nodig is.	L L L	B I V	*	+
E.2.1.2	IT– en opslagvoorzieningen met gevoelige gegevens, dienen zodanig te worden geplaatst dat er tijdens het gebruik ervan zo min mogelijk kans op toevallige waarneming is.	- - M	B I V	*	+
E.2.1.3	Apparatuur die speciale beveiliging nodig heeft, dient te worden geïsoleerd, zodat de eisen ten aanzien van het algemene beveiligingsniveau kunnen worden verminderd.	H H H	B I V	*	+

E.2.1.4	Er dienen maatregelen te worden genomen om het risico te minimaliseren van mogelijke gevaren, zoals diefstal, brand, explosieven, rook, wateroverlast, stof, trillingen, chemische reacties, interferentie via elektriciteitsvoorziening en elektro–magnetische straling.	L - -	B I V		
E.2.1.5	De organisatie dient haar beleid te bepalen ten aanzien van eten, drinken en roken in de nabijheid van IT–apparatuur.	L - -	B I V		
E.2.1.6	De omgeving dient te worden gecontroleerd op omstandigheden die de werking van de IT–apparatuur negatief zou kunnen beïnvloeden.	L - -	B I V		
E.2.1.7	Het gebruik van speciale beschermende middelen, zoals toetsenbordhoezen voor apparatuur in industriële omgevingen is vereist.	L - -	B I V		
E.2.1.8	Over de invloed van een catastrofe in de buurt van het bedrijfsterrein, bijvoorbeeld brand in een aangrenzend gebouw, waterlekkage vanaf het dak of in kelderverdie–pingen onder de begane grond, of een explosie op straat dient een risicoanalyse te zijn uitegevoerd.	M - -	B I V		

E.2.2 Stroomvoorziening

E.2.2.1	Apparatuur dient te worden beveiligd tegen stroomstoringen en andere elektrische storingen. Er dient een geschikte stroomvoorziening aanwezig te zijn die voldoet aan de specificaties van de leverancier van de apparatuur.	L - -	B I V		
E.2.2.2	Voor apparatuur waarop kritieke bedrijfsgegevens worden verwerkt, is een UPS vereist, om een goede afsluitperiode te waarborgen of de apparatuur aan de gang te houden. Er dient een noodprocedure te zijn opgesteld voor het geval de UPS niet meer werkt. UPS apparatuur dient regelmatig te worden getest volgens de voor–schriften van de fabrikant.	L - -	B I V		
E.2.2.3	Teneinde de verwerking ook tijdens langdurige stroomuitval te waarborgen dient een noodgenerator te zijn geïnstalleerd. Geïnstalleerde generatoren dienen regelmatig te worden getest volgens de aanwijzingen van de fabrikant. Een adequate brandstoftoe–voer dient beschikbaar te zijn om ervoor te zorgen dat de generator langere tijd kan blijven werken.	H - -	B I V		
E.2.2.4	Er dienen noodschakelaars te zijn in de buurt van nooduitgangen in computerruim–ten, teneinde snel de stroom uit te kunnen schakelen in geval van een calamiteit.	L - -	B I V		
E.2.2.5	Er dient noodverlichting aanwezig te zijn in geval van een algehele stroomstoring.	M - -	B I V		
E.2.2.6	Alle gebouwen dienen te zijn voorzien van bliksembeveiliging en op alle externe communicatielijnen dienen bliksembeveiligingsfilters te worden aangebracht.	M - -	B I V		

E.2.3 Beveiliging van kabels

E.2.3.1	Kabels voor stroomvoorziening en telecommunicatiekabels voor IT–voorzieningen dienen bij voorkeur ondergronds te worden aangelegd of op andere wijze voldoende te worden beschermd.	L M L	B I V	*	+
E.2.3.2	Netwerkkabels dienen te worden beschermd tegen ongeautoriseerd aftappen of beschadiging, bijvoorbeeld door ze in buizen of kabelgoten te leggen en zo min mogelijk door publieke ruimten te laten lopen.	L - M	B I V	*	+
E.2.3.3	Netsnoeren dienen gescheiden te worden gehouden van de communicatiekabels, om interferentie te voorkomen.	L M -	B I V		
E.2.3.4	Voor gevoelige of kritieke systemen dienen gesloten kabelgoten en afgesloten ruimten of dozen voor controlepunten en eindpunten te worden geïnstalleerd.	M - M	B I V	*	+
E.2.3.5	Voor gevoelige of kritieke systemen dienen alternatieve routes of transportmedia te worden gebruikt.	H - H	B I V	*	X
E.2.3.6	Voor gevoelige of kritieke systemen dienen periodiek “schoonmaakacties”te worden georganiseerd om niet geautoriseerde apparatuur die op de bekabeling is aangesloten, op te sporen.	H H H	B I V	*	X

E.2.4 Onderhoud van apparatuur

E.2.4.1	Apparatuur dien te worden onderhouden overeenkomstig de door de leverancier aanbevolen voorschriften en service–tijdstippen.	L - -	B I V		
E.2.4.2	Reparatie en onderhoud van apparatuur mogen alleen worden uitgevoerd door geautoriseerd onderhoudspersoneel.	L - -	B I V		
E.2.4.3	Er dient een overzicht te worden bijgehouden van alle storingen of mogelijke storingen en alle preventief onderhoud en reparaties.	M - -	B I V		
E.2.4.4	Er dienen passende maatregelen te worden genomen wanneer apparatuur het bedrijfsterrein verlaat voor onderhoud. Verder dienen alle eisen die door de verzekeringsmaatschappij worden gesteld, te worden nageleefd.	M - M	B I V	*	+

E.2.5 Beveiliging van apparatuur buiten de lokatie

E.2.5.1	Tijdens het vervoer mogen apparatuur (en media) niet onbeheerd worden achtergelaten in publieke ruimten. Draagbare computers dienen tijdens het reizen als handbagage te worden vervoerd en zo mogelijk niet duidelijk herkenbaar te zijn.	- - L	B I V	*	+
E.2.5.2	De instructies van de fabrikant ter bescherming van de apparatuur dienen steeds in acht te worden genomen, bijvoorbeeld als de apparatuur niet mag worden blootgesteld aan sterke elektromagnetische velden.	L - L	B I V	*	+

E.2.5.3	Maatregelen voor thuiswerken dienen te worden bepaald aan de hand van een risico–analyse en zo nodig dienen passende maatregelen te worden toegepast, bijvoorbeeld afsluitbare archiefkasten “clear desk policy” en toegangsbeveiliging voor computers.	- M M	B I V	*	
E.2.5.4	Er dient een passenden verzekering te worden afgesloten om apparatuur die zich buiten de eigen lokatie bevindt te beschermen.	L L L	B I V	*	

E.2.6 Veilig afvoeren en hergebruiken van apparatuur

E.2.6.1	Opslagmedia die gevoelige informatie bevatten dienen, in plaats van op de standaard manier te worden gewist, fysiek te worden vernietigd of op een veilige manier te worden overschreven.	- - L	B I V	*	+
E.2.6.2	Alle onderdelen van de apparatuur waarop gegevens kunnen worden opgeslagen, bijvoorbeeld vaste schijven, dienen te worden gecontroleerd om te waarborgen dat alle gevoelige gegevens en in licentie gebruikte software zijn verwijderd of overschreven voordat de apparatuur wordt afgevoerd.	- - L	B I V	*	+

E.3 Algemene beveiligingsmaatregelen

E.3.1 Clear desk en clear screen policy

E.3.1.1	Papieren en computermedia dienen te worden opgeborgen in kasten met een deugdelijk slot en / of andere typen beveiligingsmeubilair, wanneer zij niet gebruikt worden en in het bijzonder buiten werktijd.	- M M	B I V	*	+
E.3.1.2	Gevoelige of kritische bedrijfsinformatie dient achter slot en grendel te worden bewaard (in het ideale geval in een brandwerkende safe of kast), vooral wanneer het kantoor verlaten is.	- - L	B I V	*	+

E.3.1.3	Personal computers en computerterminals en printers dienen niet aangelogd te blijven wanneer zij onbeheerd achterblijven en dienen te worden beveiligd door middel van sloten, wachtwoorden of andere maatregelen wanneer zij niet worden gebruikt.	L L L	B I V	*	+
E.3.1.4	Ruimten waar post binnenkomt en uitgaat en onbeheerde fax– en telexapparatuur staat opgesteld, dienen te worden beveiligd.	- - H	B I V	*	X
E.3.1.5	Buiten kantooruren dienen fotokopieerapparaten te worden afgesloten (of op een andere manier worden beveiligd tegen ongeautoriseerd gebruik).	- H H	B I V	*	+
E.3.1.6	Gevoelige of geheime informatie dient na het afdrukken onmiddellijk van de printer te worden verwijderd.	- - L	B I V	*	+

E.3.2 Het verwijderen van bedrijfseigendommen

E.3.2.1	Apparatuur, informatie en software van de organisatie mogen niet zonder autorisatie meegenomen worden van het bedrijfsterrein.	L L L	B I V		+
E.3.3.2	Waar mogelijk dient op een lijst te worden geregistreerd wanneer apparatuur wordt meegenomen en weer wordt teruggebracht.	M M M	B I V		+
E.3.3.3	Steekproeven dienen te worden ondernomen om het ongeautoriseerd meenemen van bedrijfseigendommen op te sporen. Het personeel dient van deze steekproeven op de hoogte te worden gesteld.	H H H	B I V		X