Security binnen Enterprise Architectuur

Radboud Universiteit Nijmegen

Universiteit	:	Radboud Universiteit Nijmegen
Faculteit	:	Faculteit Natuurwetenschappen, Wiskunde & Informatica
Opleiding	:	Informatiekunde
Opdrachtgever	:	Prof. Dr. D.B.B. Rijsenbrij
Referent	:	Dr. M.D. Oostdijk
Documentversie	:	3.0
Status	:	Definitief
Datum	:	10 februari 2006
Naam	:	Lucien Bongers
Studentnummer	:	S0366560
Afstudeernummer	:	21 IK

Colofon

Auteur:	Lucien Bongers	l.bongers@student.ru.nl
Opleiding:	Informatiekunde	
Specialisatie:	Digitale Architectuur	
Opdracht:	Security binnen Enterprise Architectuur	
Universiteit:	Radboud Universiteit Nijmegen (RU)	
Faculteit:	Faculteit Natuurwetenschappen, Wiskunde & Informatica (FNWI)	
Instituut:	Nijmeegs Instituut voor Informatica en Informatiekunde	
Opdrachtgever:	Prof. Dr. Daan Rijsenbrij	daan.rijsenbrij@capgemini.com
Referent:	Dr. Martijn Oostdijk	martijno@cs.ru.nl
Plaats, datum:	Nijmegen, februari 2006	
Versie:	3.0 Definitief	

Nijmeegs instituut voor Informatica en Informatiekunde	
Bezoekadres:	Comeniuslaan 4 6525 HP Nijmegen
Postadres:	Postbus 9102 6500 HC Nijmegen
Telefoon:	+31 24 361 61 61
E-mail:	info@cs.ru.nl

Voorwoord

In het kader van mijn studie informatiekunde aan de Radboud Universiteit Nijmegen (RU) heb ik een afstudeeronderzoek uitgevoerd binnen de subfaculteit Nijmeegs Instituut voor Informatica en Informatiekunde (NIII).

Met de constante toename van vaak on(be)grijpbare Informatie Technologie in onze maatschappij neemt de behoefte tot het aanbrengen van structuur en overzicht toe. Digitale architectuur is een middel om dit te bereiken. Net als in de fysieke wereld staat of valt het opstellen van een bruikbare architectuur in de digitale wereld met een degelijk security beleid. In tegenstelling tot de fysieke wereld zijn er in de digitale wereld weinig eenduidige, consistente en leidende regels, richtlijnen en wetten waaraan een ontwerp moet voldoen. Security in de digitale wereld wordt nog te vaak gezien als ongewild aanhangsel waaraan op een ad-hoc manier aandacht aan wordt geschonken.
In de wereld van het hoger onderwijs alsmede in het bedrijfsleven wordt dit onderwerp daarom steeds belangrijker en het wordt tijd dat er een gestructureerde aanpak komt waarbij tijdens het opstellen van de architecturale beginselen rekening gehouden wordt met security.
Met deze scriptie heb ik getracht een methodische aanpak neer te leggen welke gebruikt kan worden bij het opstellen van een enterprise architectuur waarbij security als elementair onderdeel wordt ingebouwd in plaats van aangebouwd.

Via deze weg wil ik prof. dr. (Daan) Rijsenbrij, dr. (Martijn) Oostdijk bedanken voor het begeleiden van het onderzoekstraject, het discussiëren over interessante stellingen, het reviewen van documenten en het introduceren van enkele nuttige contacten in de wereld van architectuur en security in het bedrijfsleven.

Ik wens U veel leesplezier!

Lucien Bongers
Nijmegen, februari 2006

Inhoudsopgave

Samenvatting

Veelal worden er separate security oplossingen geïntroduceerd waarbij de beveiligingsexperts geheel los staan van de digitale architectuur. Het achteraf integreren van beveiligingseisen in de digitale architectuur leidt bij veel ondernemingen tot problemen. Hierdoor ontstaan er oplossingen die niet passen bij de opgestelde architectuurprincipes waardoor misfits ontstaan. De gevolgen hiervan zijn nauwelijks te overzien, doch kunnen op veel manieren voor afbraak en inconsistentie zorgen. Het juist niet veiliger worden van applicaties, frustratie bij stake-holders vanwege een niet passende menselijke maat zijn slechts enkele mogelijke problemen die kunnen ontstaan. Er is behoefte aan een holistische aanpak om security met digitale architectuur te verenigen.

Architectuur is, volgens prof. dr. Daan Rijsenbrij, een coherente, consistente verzameling principes, verbijzonderd naar concerns, regels, richtlijnen en standaarden die beschrijft hoe een onderneming, de informatievoorziening, de applicaties en de infrastructuur zijn vormgegeven en zich voordoen in het gebruik. Deze definitie gaat uit van een coherente verzameling principes om de ordelijke samenhang te ondersteunen waarbij consistentie ervoor zorgt dat de principes elkaar niet tegenspreken. Deze definitie beslaat de gehele architectuur van een onderneming en is bruikbaar op bedrijfsniveau. Architectuur wordt bepaald door de missie, visie en de strategie van de onderneming. De missie beschrijft de bestaansreden van de onderneming. De visie wordt gevormd door het beeld dat een onderneming heeft richting de toekomst en de keuzes die men daarbij maakt. Op basis van die visie kunnen één of meerdere strategieën worden ontwikkeld die de richting naar de toekomst bepalen.
Architectuur kent vier werelden: de business-, informatie-, applicatie-, en de (technische) infrastructuurwereld. In de businesswereld worden de zaken gedaan waardoor de onderneming bestaansrecht krijgt. In de informatiewereld bevinden zich informatiestromen, informatiebehoeftes, informatiebronnen en de uitwisseling van informatie. Het applicatielandschap ondersteunt de informatiewereld met behulp van informatiesystemen en databases. De (technische) infrastructuur bevat gemeenschappelijke zaken die door alle applicaties kunnen worden gebruikt.
Architectuur zorgt voor complexiteitsreductie en het is een middel om de bestuurbaarheid, transformatieproces en outsourcing te beheersen.

Door de toenemende complexiteit, integratie en transparantie van organisaties wordt informatiebeveiliging steeds moeilijk te borgen. Beschrijvingen van terminologieën in de security wereld zijn echter vaak onduidelijk en/of onvolledig. Daarbij speelt invloed van slordig gebruik van de Engelse taal in het vakjargon een grote rol. De termen ‘security’ en ‘safety’ dienen eenduidig en correct te worden gebruikt. Security betekent beveiliging, safety betekent veiligheid. Altijd dient bij security de afweging gemaakt te worden ‘hoe veilig’ het systeem moet zijn ten opzichte van ‘hoe gebruiksvriendelijk’ en ‘in welke mate rekening gehouden wordt met ‘privacy’.
Een onderneming heeft te kampen met dreigingen vanuit een aantal hoeken; mens, omgeving, technologie en natuur. Deze dreigingen spelen in op de security binnen een onderneming. Hierdoor ontstaan aandachtsgebieden. Een aandachtsgebied is een cluster van bedrijfsprocessen waar men spe-

ciale aandacht moet besteden op het gebied van security. Een voorbeeld van een aandachtsgebied is 'klantrelatie' waarbinnen o.a. orderregistratie en klantcontact als bedrijfsprocessen kunnen worden herkend. Een aandachtsgebied is dus erg ondernemingsafhankelijk waarbij de invulling compleet afhangt van de toegekende waarde aan een aandachtsgebied, de voortgekomen concerns en de daarbij opgestelde principes.

Principes komen veelal voort uit omgevingsfactoren plus de interpretatie die een bestuurder daaraan geeft. Een principe geeft aan **wat** er geregeld moet worden. Het is een fundamenteel idee om een algemene eis te vervullen. Een onderneming begint met het opstellen van principes met als doel de ontwerpruimte te beperken. Architectuur is daarom een hulpmiddel om ontwerpbeslissingen te vereenvoudigen en te uniformeren.

De moeilijkheid bij het opstellen van security principes zit niet in het achterhalen en opstellen van de principes zelf. De moeilijkheid is het uitzoeken of alle principes ook echt principes zijn, of ze relevant zijn maar **vooral** om duidelijk te krijgen met welke terminologieën je te maken hebt en hoe die terminologieën met elkaar in relatie staan. Men moet een weg zien te vinden in de wirwar van terminologieën zodat uitspraken gedaan kunnen worden over de uiteindelijke invulling van principes in een tastbaar object, de onderneming! In dit onderzoek is een ER-diagram gemaakt (ERD) waarmee de belangrijkste terminologieën van dit onderzoek met elkaar in relatie worden gebracht. Het ERD dient als een metaplattegrond waarbij de waarde en bruikbaarheid zit in de overzichtelijkheid door het zichtbaar maken van relaties tussen de entiteiten binnen dit onderzoek. Het ERD zal in een later stadium uitstekend kunnen dienen als in te vullen plattegrond waarbij de entiteiten geen meta-entiteiten meer zijn maar ondernemingsspecifieke objecten waarbij voor iedere onderneming de principes kunnen worden geplaatst.

In de vakliteratuur wordt opvallend weinig aandacht besteed aan een ordening van principes. Hierdoor zijn de lijsten van principes vaak lang, onoverzichtelijk en lijken vaak op grote brainstormsessies. Het gebrek aan ordening resulteert in een ongestructureerde, niet-gevalideerde overvloed aan uitspraken die niet als principes bestempeld kunnen worden. Deze 'uitspraken' dienen dus eerst te worden herschreven alvorens ze door kunnen als principes. Daarnaast is a-transparantie en het gebrek aan traceerbaarheid naar de oorsprong van principes een groot probleem.
In dit onderzoek zijn de gevonden principes opgesomd, herschreven en zelf opgestelde principes ondergebracht in een ordening. Deze ordening bestaat uit pervasive principes, breed functionele principes en gedetailleerde principes. Met hulp van een kruisreferentie-tabel wordt de oorsprong en relaties tussen principes onderling duidelijk. Daarna zijn de principes in het Rijsenbrij-Framework[1] geplaatst om zo weer te geven in welke architectuurwereld het principe is geconcipieerd en tot welke wereld het principe doorwerkt. Dit alles om de architect meer houvast te geven bij het opstellen van de architectuur waarbij hij security in de enterprise architectuur moet integreren.

[1] Rijsenbrij-Framework in hoofdstuk 2.6

Er is een case studie uitgevoerd bij het UMC St. Radboud, een onderneming in de reële wereld. De case studie dient ervoor om te kijken welke security principes uit de theorie genest zijn binnen een reële onderneming, waar ze vandaan komen (vanuit welke concerns), welke invloed ze hebben en hoe ze worden nageleefd. De resultaten zijn weinig opmerkelijk te noemen. Ook binnen het security beleid van het UMC blijkt dat er nog (te) ad-hoc wordt gewerkt. Eenduidige beleidsdocumenten die volledige steun hebben van het management zijn er nog niet. Hier wordt weliswaar hard aangewerkt edoch wordt het meer gezien als dwang, door de overkoepelende zorgbranche met hun nieuwe standaarden en (NEN) normeringen, dan algehele bewustwording en begrip.
Van de beschikbare principes in de theorie wordt slechts een fractie teruggevonden in beleidsdocumenten. Kan hierdoor geconcludeerd worden dat men sommige principes niet heeft geïmplementeerd en men dus op dat punt in de security gevaar loopt? Of zijn er wel regels en richtlijnen aanwezig binnen de onderneming waarvan het principe in het securitybeleid ontbreekt?
Opmerkelijk is het feit dat het theoretische security principe '*Vertrouw niet iedereen blind*' (pervasive principe nr.12[2]) binnen het UMC geen beleidsinvulling kent. Het is mogelijk dat dit komt doordat het UMC van nature een sociale en open instelling is waarbij het overgrote deel van de medewerkers erg behulpzaam is. Men probeert mensen te helpen waarbij eventuele kwade bedoelingen onderbelicht raken.

[2] Pervasive principes in hoofdstuk 6

1 Inleiding

Dit hoofdstuk beschrijft de kernpunten uit het onderzoeksplan. De aanleiding voor het onderzoek, de probleemstelling, doelstellingen en natuurlijk de hoofdvraag. Het gehele onderzoeksplan is te vinden op de voor deze opdracht opgezette website [Web-1].

1.1 Aanleiding onderzoek

De opdracht wordt uitgevoerd in opdracht van de Radboud Universiteit, met name in opdracht van prof. dr. Daan Rijsenbrij. Hij zal tijdens het traject op het gebied van architectuur inhoudelijk advies geven. dr. Martijn Oostdijk treedt op als referent.

1.2 Probleemstelling

Veelal worden er separate security oplossingen geïntroduceerd waarbij de beveiligingsexperts geheel los staan van de digitale architectuur. Het achteraf integreren van beveiligingseisen met de digitale architectuur leidt bij veel ondernemingen tot problemen hetgeen blijkt uit de vele security incidenten. Hierdoor ontstaan er veel oplossingen die niet passen bij de opgestelde architectuurprincipes waardoor misfits ontstaan. De gevolgen hiervan zijn nauwelijks te overzien, doch kunnen op veel manieren voor afbraak en inconsistentie zorgen. Het juist niet veiliger worden van applicaties, frustratie bij stakeholders vanwege een niet passende menselijke maat zijn slechts enkele mogelijke problemen die kunnen ontstaan.

Net als digitale architecten maken ook de security experts high-level ontwerpen gebaseerd op principes, regels, standaarden en richtlijnen zodat de solution designers hierop kunnen voortborduren. Vreemd is dan ook dat security en digitale architectuur bij veel ondernemingen niet geïntegreerd is.

1.3 Doelstelling

In dit onderzoek is een aanzet gegeven tot een holistische aanpak om de integratie van security binnen enterprise architectuur te bevorderen. Er wordt onderzocht hoe de verschillende aspecten en aandachtsgebieden die bij security belangrijk zijn kunnen worden verkend. En hoe vervolgens deze worden geformuleerd naar principes, regels en concerns.
Ten slotte wordt gekeken welke veranderingen er nodig zijn in de enterprise architectuur als er zich (nieuwe) security principes voordoen die niet passen.

1.4 Hoofdvraag

De hoofdvraag van het onderzoek is als volgt geformuleerd:

Welke zijn de belangrijkste aandachtsgebieden en aspecten van security en hoe worden deze geformuleerd in principes en kunnen deze worden geïntegreerd in een enterprise architectuur?

Toelichting op de onderzoeksvraag en begripsbepaling

Aandachtsgebieden:

Binnen organisaties in z'n geheel alsook binnen domeinen en subdomeinen van organisaties kunnen aandachtsgebieden worden herkend. Een aandachtsgebied is een cluster van bedrijfsprocessen waar men speciale aandacht moet besteden op het gebied van security. Een voorbeeld van een aandachtsgebied is 'klantrelatie' waarbinnen o.a. orderregistratie en klantcontact als bedrijfsprocessen kunnen worden onderkend.

Belangrijkste aspecten:

Binnen de context van security zijn er drie aspecten te beschouwen: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV, of CIA Confidentiality, Integrity en Availability, in het Engels).
De aspecten zeggen iets over waaraan binnen het aandachtsgebied moet worden voldaan.

Principes:

Principes zijn richtinggevende uitspraken ten behoeve van essentiële beslissingen, een fundamenteel idee bedoeld om een algemene eis te vervullen. Principes beïnvloeden direct de wijze waarop de IT zal worden ingezet. Foute principes kunnen desastreus zijn bij transformaties. Principes dienen te worden geconcretiseerd naar zaken die moeten, dat zijn de regels en standaarden, en zaken die verstandig zijn: de richtlijnen, ook wel 'best practices' genoemd. [Rijsenbrij, 2003]

Integratie:

Integratie met de enterprise architectuur om security invulling en waarde te geven in elk van de vier werelden beschreven door Rijsenbrij: de business-, informatie-, applicatie-, en de (technische) infrastructuurwereld

Enterprise architectuur:

Enterprise architectuur is principe georiënteerd en dient om kaders te geven op enterprise niveau (het hoogste niveau) die leidend zijn voor alle onderliggende niveaus, zoals domeinen, informatiesystemen en digitale werkruimtes. Enterprise architectuur leidt tot een high-level ontwerp van de onderneming in zijn totaliteit. Het doel is een eerste indeling in domeinen bestaande uit bedrijfsprocessen, applicaties en de onderliggende technische infrastructuur. Een enterprise architectuur heeft meerdere gebruiksdoeleinden: atlas voor het topmanagement, beheersing van complexiteit, kaderzetting voor realisatie

en communicatiemiddel. Het atlasaspect van de enterprise architectuur wordt gestalte gegeven door een verdeling van de onderneming in een aantal redelijk autonome domeinen. Hoofddomeinen zijn vaak: delivery, marketing & sales, leveranciers & inkoop. Ondersteunende domeinen beslaan zaken als personeel, informatie, organisatie, financiën en huisvesting. [Rijsenbrij, 2002]

Om tot een oplossing te komen voor de onderzoeksvraag zijn de volgende deelvragen opgesteld:

1. Hoe worden security principes geordend?
2. Wat is de werking van security principes wat betreft interactie met andere principes?
3. Hoe worden security principes gekozen?

Binnen deze deelvragen zijn sub-deelvragen opgesteld die als doel hebben om op de overkoepelende deelvraag een antwoord te geven. De sub-deelvragen (zie paragraaf 1.10) zijn kleine vraagstukken en kunnen gezien worden als grondlegging van de bijhorende deelvraag.

1.5 Kennisgebied

Dit onderzoek richt zich op het achterhalen en in kaart brengen van aspecten en aandachtsgebieden van security geformuleerd in principes en hoe deze kunnen worden geïntegreerd in een enterprise architectuur. Hoe deze probleemstelling is ontstaan en hoe deze moet worden opgelost, zijn zaken die ingrijpen op de gebieden van security en digitale architectuur.

1.6 Relevantie

De onderzoeksvraag is de moeite van het beantwoorden waard, omdat uit meerdere literatuurbronnen en interviews met deskundigen op zowel het gebied van security alsook architectuur, blijkt dat er geen structurele methode is die geformuleerde security principes integreert met het opstellen van een enterprise architectuur.

1.7 Strategie / methodedomein

In een onderzoek kunnen de volgende drie onderzoeksstrategieën worden gehanteerd, waarbij een combinatie van strategieën mogelijk is:

- Case studie: intensief bestuderen en/of observeren van enkele, soms zelfs één, onderzoekseenheden.
- Survey: ondervragen en/of observeren van een grote groep mensen waarbij gekeken wordt naar een groot aantal kenmerken.
- Experiment: toetsing van een oorzakelijk verband door systematische variatie van mogelijke oorzaken.

1.8 Strategiekeuze

De onderzoeksaanpak is te karakteriseren als een combinatie van evaluerend en exploratief onderzoek. [Verschuren en Doorewaard, 2000]
Om beweringen hard te maken wordt gebruik gemaakt van literatuur- en veldonderzoek (interviews en casestudies). Het laatste levert empirische data op. De conclusies en aanbevelingen die hierop gebaseerd zijn, zijn deels te vergelijken met een hypothese, en zullen daadwerkelijk pas bij de integratie van de security principes in de enterprise architectuur getoetst kunnen worden. [Oost en Markenhof, 2003]

1.9 Methoden & technieken en data verzameling

Binnen kwalitatief onderzoek gebruiken onderzoekers veelal documentanalyses, interviews en observaties om informatie te verzamelen. Voor dit onderzoek zal voornamelijk gebruik worden gemaakt van literatuurstudie en interviews. Ook zullen discussiefora op het Internet worden geraadpleegd om met vakgenoten en geïnteresseerden te communiceren over stellingen binnen het vakgebied van digitale architectuur en de relatie met security.

Om empirische data te verzamelen voor het onderzoek (zowel technisch inhoudelijke informatie alsook informatie over de ervaringen in de praktijk) worden (semi)gestructureerde interviews afgenomen. De methode van interviewen bestaat uit het afnemen van de gesprekken in een rustige spreekkamer. Het doel van de interviews is om te komen tot een vergelijking van organisatiebeelden [Leeuw, 1996], en dient dus als doel van de analyse. Geselecteerde respondenten en informanten dienen nader te worden bepaald.

1.10 Werkwijze

De deelvragen en sub-deelvragen worden als volgt uitgewerkt:

Deelvraag 1: Hoe worden security principes geordend?

- Onderzoek naar welke security aspecten er zijn.
- Hoe zijn de gevonden aspecten onder te verdelen (aandachtsgebied of niveau, etc).
- Is er een (klein) overkoepelend aantal (6 tot 8??) principes, waaraan de overige gerelateerd kunnen worden.

Deliverable deelvraag 1:
Lijst van de belangrijkste security aspecten geformuleerd in principes + literatuuroverzicht.

Deelvraag 2: Wat is de werking van security principes?

- Onderzoek naar de invloed van de security principes op een architectuur.
- In welke aandachtsgebieden en op welke momenten zijn ze van invloed op het werk van de architect.

Deliverable deelvraag 2:
Resultaat van de case studie en gerapporteerde bevindingen.

Deelvraag 3: Hoe worden security principes gekozen?

- Onderzoek op basis van welke criteria een keuze uit security principes gemaakt kan worden.
- Onderzoek welke criteria daar een rol bij spelen. Expliciet dient daarbij aandacht besteed te worden aan de relatie met maturity models, organisatiecultuur en de invloed van compliance.

Deliverable deelvraag 3:
Vragenlijsten + antwoorden van architecten en security experts.

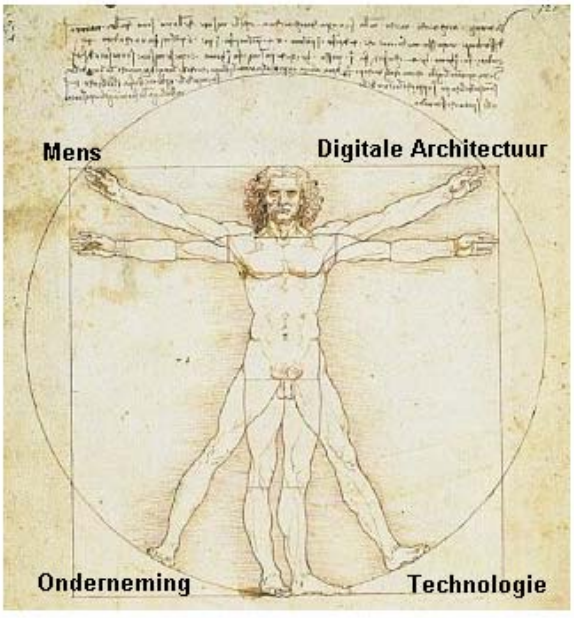
1.11 Opbouw van de scriptie

Hoofdstuk 2 geeft invulling aan de term digitale architectuur. Dit hoofdstuk beperkt de definitie voor dit onderzoek en dient als theoretische basis voor de overige onderwerpen in deze scriptie.
Hoofdstuk 3 geeft invulling aan de term security. Ook dit hoofdstuk is een theoretische basis welke noodzakelijk is overige onderwerpen te kunnen begrijpen en met elkaar in verband te kunnen brengen.
Hoofdstuk 4 beschrijft de rol van een ‘principe’. De term ‘principe’ is een kernwoord in het onderzoek en dient dus voldoende worden toegelicht.
Hoofdstuk 5 kan gezien worden als één van de twee kernpunten van dit onderzoek. Hierin worden de gebruikte terminologieën in context met elkaar in een diagram weergegeven. Dit moet ervoor zorgen dat er voor eens en voor altijd duidelijkheid is omtrent de inhoud alsmede de koppeling van begrippen.
In hoofdstuk 6 worden de belangrijkste security principes geordend opgesomd en toegelicht.
Hoofdstuk 7 kan gezien worden als het tweede kernpunt van dit onderzoek. De principes uit hoofdstuk 6 worden hier gepositioneerd in het Rijsenbrij-Framework waardoor er een transparante koppeling ontstaat tussen security principes en digitale architectuur.
In hoofdstuk 8 wordt afgestapt van de theoretische benadering van security principes binnen digitale architectuur. Het doel van dit hoofdstuk is een case studie naar één aandachtsgebied binnen het UMC St. Radboud. Binnen dit aandachtsgebied worden de toegepaste principes gedestilleerd en gekeken of, en zo ja welke, matches er zijn met de principes in hoofdstuk 6. In hoofdstuk 9 en 10 wordt een validatie en een conclusie gegeven.

2 Digitale architectuur

2.1 Inleiding

Alles en iedereen moet tegenwoordig digitaal. Bedrijven doen hun uiterste best bij te blijven bij de nieuwe ontwikkelingen om zo aan de wensen van hun veeleisende klanten te voldoen. De steeds toenemende mate van technologie, complexiteit en integratie van systemen en de informatievoorziening schreeuwt om structuur en houvast. Digitale architectuur, verder te noemen als architectuur, helpt deze complexiteit, d.m.v. aan te brengen structuur, te reduceren en begrijpbaar te maken. De rol van de architect is hier bepalend. In figuur 1 is de centrale positie van de architect te zien en de krachten die op hem inspelen die hij in evenwicht moet zien te houden. Hij dient een architectuur te concipiëren waarbij hij zowel kijkt naar wat de onderneming wil, de technologie kan en waarin de mens zich gelukkig voelt en kan ontplooien. Hij werkt vanuit een vraag, een concern uit de onderneming en niet vanuit oplossingen. Een concern werkt hij uit in principes, regels, richtlijnen en standaarden. Meer hierover in paragraaf 4.1. Eén van de hoofddoelen van een enterprise architectuur is het ondersteunen van een globale, bedrijfsbrede optimalisatie van processen, applicaties en infrastructuur in hun onderlinge samenhang. [Lankhorst, e.a, 2005]



Figuur 1: De architect in zijn rol

2.2 De definitie

In de literatuur zijn veel definities van architectuur te vinden. Er zijn definities die alleen de te gebruiken technieken noemen en zelfs definities die meer weg hebben van een beschrijvend technisch ontwerp. Andere definities gaan (te) diep in op de technische aspecten waardoor ze onleesbaar worden voor niet ingewijden en niet toepasbaar zijn voor andere projecten. Ook zijn er definities die geen rekening houden met het belevingsaspect waardoor de definitie nogal klinisch overkomt en de architectuur degradeert tot een soort meta-structuur.

Een aantal gevonden definities:
The manner in which a system (network, hardware and software) is structured. Architecture usually describes how the system is constructed, how the components fit together, and the protocols and interfaces used to integrate these components. It also defines the functions and description of data formats and procedures used for communication between nodes and workstations. [Web-2]

A description of all functional activities to be performed to achieve the desired mission, the system elements needed to perform the functions, and the designation of performance levels of those system elements. An architecture also includes information on the technologies, interfaces, and location of functions and is considered an evolving description of an approach to achieving a desired mission. [Web-3]

The structure of a system's components and connectors, their interrelationships, and the principles and guidelines governing their design and evolution over time. [Web-4]

The fundamental organization of a system embodied in its components, their relationships to each other and to the environment and the principles guiding its design and evolution. [IEEE]

De definitie van IEEE wordt veel gehanteerd binnen de academische wereld. Net als de andere definities wordt impliciet gerefereerd naar een software- of computersysteemarchitectuur. IEEE is van nature een techneutenclub die zich voornamelijk richt op software engineers en de architectuur van softwaresystemen. Zij richten zich niet per definitie op de businessaspecten die binnen de digitale architectuur een fundamentele rol spelen.

In dit onderzoek wordt de definitie van Rijsenbrij gebruikt.
Architectuur is een coherente, consistente verzameling principes, verbijzonderd naar concerns, regels, richtlijnen en standaarden die beschrijft hoe een onderneming, de informatievoorziening, de applicaties en de infrastructuur zijn vormgegeven en zich voordoen in het gebruik. [Rijsenbrij, 2003]
Deze definitie gaat uit van een coherente verzameling principes om de ordelijke samenhang te ondersteunen waarbij consistentie ervoor zorgt dat de principes elkaar niet tegenspreken. Deze definitie beslaat de gehele architectuur van een onderneming en is dus bijzonder bruikbaar op bedrijfsniveau.

Principes worden geconcretiseerd naar regels, standaarden en richtlijnen. Het principe geeft aan *wat* er geregeld moet worden. Regels, standaarden en richtlijnen geven aan *hoe* dat te regelen.
Regels *moeten* worden nageleefd, zij zijn een soort wet binnen de onderneming.
Standaarden *moeten* gevolgd worden om de aansluitbaarheid op de omgeving te borgen voor nu en de nabije toekomst. Standaarden betreffen een voorschrift of een set van voorschriften waarover overeenstemming bestaat in de IT-sector.
Richtlijnen *mogen* worden gebruikt. Zij zijn een soort best practices over hoe een bepaald principe kan worden gerealiseerd met een gezonde mate van vrijheid voor situatieafhankelijke interpretatie .

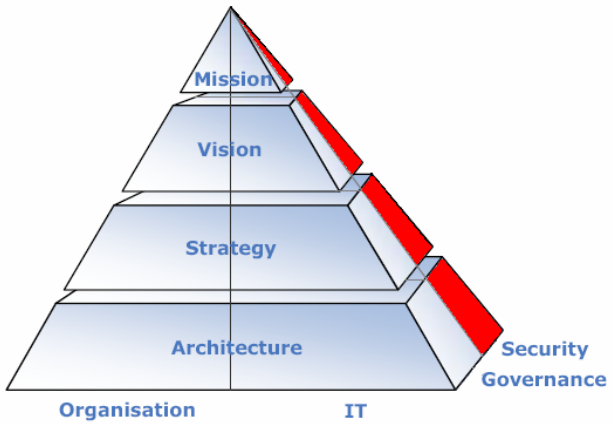
Vaak worden regels geformuleerd als: ‘in principe doen we zus en zo’. Dat is geen regel, maar een richtlijn! Concerns geven het *waarom* van het principe. Het is belangrijk te weten waarom zaken op een bepaalde manier zijn geformuleerd. Vooral als er in de toekomst veranderingen moeten worden doorgevoerd. [Rijsenbrij, 2002]

Rijsenbrij zegt in een update op zijn inaugurele rede, getiteld ‘Architectuur in de Digitale Wereld (versie nulpuntdrie) [Rijsenbrij, 2006] het volgende:
Dat woord ‘concern’ klinkt eigenlijk een beetje problematisch, architectuur als antwoord op een aantal probleempunten. Toch zit er achter architectuur een centraal idee of ideeënstelsel. Architectuur is de uitdrukking in steen of in bits van dat idee. Waarom dan toch zoveel nadruk op concerns? Er is veel mis in de huidige implementatie van IT. Daar moet duidelijk de nadruk op worden gelegd bij het hogere management. In hun perceptie is namelijk het opheffen van die concerns de bestaansreden van architectuur. Dus het etaleren van het opheffen van de concerns houdt het hogere management bij de les. Tweede reden van een architectuurbeschouwing vanuit de concerns is gelegen in het feit dat nooit van scratch een architectuur wordt opgesteld. Er is altijd een impliciete architectuur aanwezig, behalve als er een nieuwe onderneming wordt gestart dan wel een nieuwe business activiteit.

Juist deze uitleg blijkt bijzonder bruikbaar en relevant voor de afleiding van principes die te maken hebben met security. Immers komen security concerns voort uit slechte ervaringen, fouten en lekken en hebben meteen betrekking op het wel en wee van een organisatie. Het topmanagement heeft een beveiligingsconcern binnen haar onderneming waarna vanuit deze concerns security principes worden opgesteld.

2.3 Missie, visie en strategie

De Missie, Visie, Strategie (MVS) piramide (Figuur 2) maakt duidelijk waardoor architectuur wordt bepaald. [Rijsenbrij, 2002] Met name voor dit onderzoek is het belangrijk te kijken naar de positie van security in de piramide.



Figuur 2: Missie, visie strategie piramide

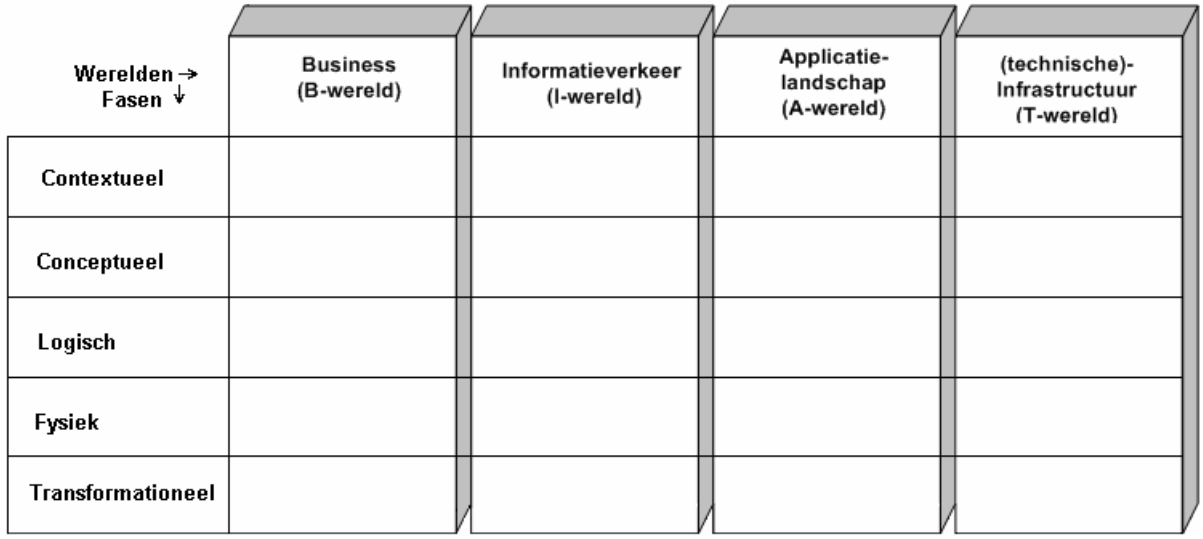
De missie beschrijft wat de bestaansreden/doel is van de onderneming.
De visie zegt iets over hoe de onderneming de toekomst ziet en de strategie geeft aan op welke koers gevaren moet worden om in de toekomst nog te kunnen bestaan. In de visie zijn minstens de volgende elementen opgenomen: de markt en zijn uitdagingen, economische en politieke ontwikkelingen, demografische en sociale trends, de concurrentie en de competitie en natuurlijk de technologische mogelijkheden en uitdagingen. Op basis van de visie kan een strategie worden ontwikkeld die de richting naar de toekomst aangeeft. Op basis van de overkoepelende bedrijfs- of organisatiestrategie kunnen vervolgens afgeleide strategieën worden ontwikkeld gericht naar bepaalde aspecten zoals de IT-strategie, de beveiligings- en beheerstrategie, die tezamen een holistische richting naar de toekomst aangeven.
Architectuur levert structuur om de koers te kunnen volgen met behulp van concepten en modellen. Daarbij wordt een integrale benadering gehanteerd vanuit zowel de organisatie als de IT en rekening gehouden met zaken als beveiliging en beheer. [Rijsenbrij, 2002]
Het rood gearceerde vlak geeft aan hoe en op welke momenten security belangrijk is en in welke mate. Het security beleid dient te worden vertaald vanuit het Corporate beleid en het IT beleid. De missie, visie en strategie van een organisatie is hiervan het fundament. Beleid voeren betekent in algemene zin ‘in control zijn’ van je organisatie. Dit wordt bereikt indien de strategie en bedrijfsdoelstellingen op elkaar zijn afgestemd en worden doorvertaald naar de organisatie waarbij iedereen binnen de organisatie zijn/haar verantwoordelijkheid dient te nemen om de juiste handelingen te verrichten conform interne en externe richtlijnen, waarbij het topmanagement de eindverantwoording draagt. Deze verantwoordelijkheden dienen dan wel duidelijk zijn vastgelegd en principes dienen deze verantwoordelijkheden te omsluiten.

2.4 Architectuurgebieden

Binnen digitale architectuur zijn er verschillende werelden waar naar wordt gekeken en waarbinnen verschillende niveaus worden gedefinieerd. De vier werelden waar dit onderzoek zich op richt zijn: business, informatie, informatiesystemen en (technische) infrastructuur.
Het gebruik van een framework biedt uitkomst om de architectuurprincipes, regels, richtlijnen en standaarden te rubriceren en duidelijk te kunnen plaatsen in deze vier werelden. Voor dit onderzoek wordt een afgeleide van het IAF Framework gehanteerd genaamd het Rijsenbrij-Framework.
Het IAF Framework zet de vier werelden van architectuur af tegen de fasen contextueel, conceptueel, logisch, fysiek en transformationeel (Figuur 3).
Over het IAF Framework zegt Rijsenbrij op zijn website [Web-5] het volgende:

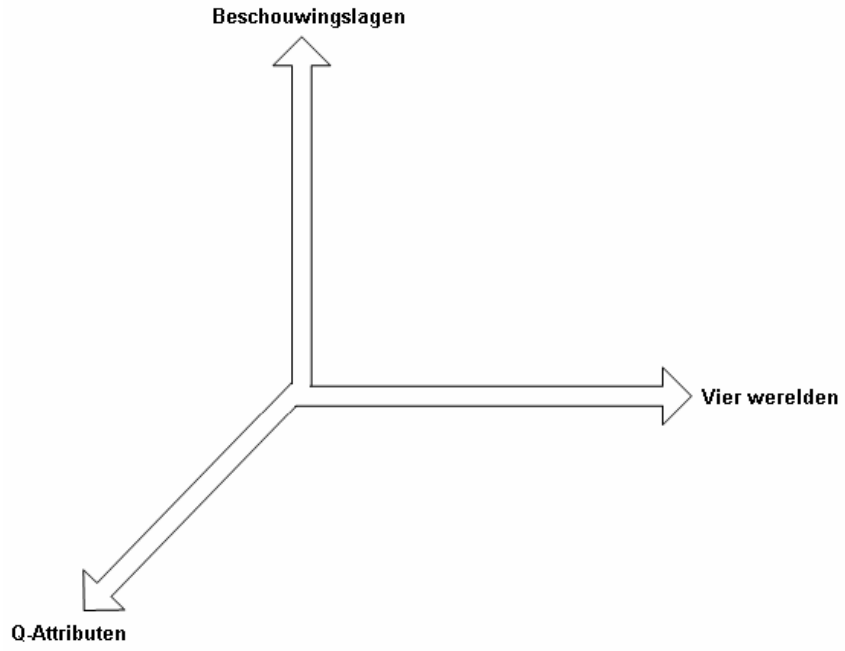
1. Any unified framework for modelling the business – IT relationship should include both management and design components: aligning business and IT is a matter of management and of design.
2. The generic framework for information management and the Integrated Architecture Framework in combination can be the basis for such a unified framework. The IAF framework offers in a certain way the third, design-related dimension of the information management framework.
3. The IAF framework offers more specifically an authoritative design substantiation for the structure level of the generic information management framework. The ultimate, yet to be defined, unified framework will need similar design interpretations for the strategic and operational levels.

Het IAF is dus een framework, dat beschrijft hoe een architectuur voor verschillende aspectgebieden, vanuit verschillende gezichtspunten en op verschillende beschouwingslagen wordt opgebouwd.



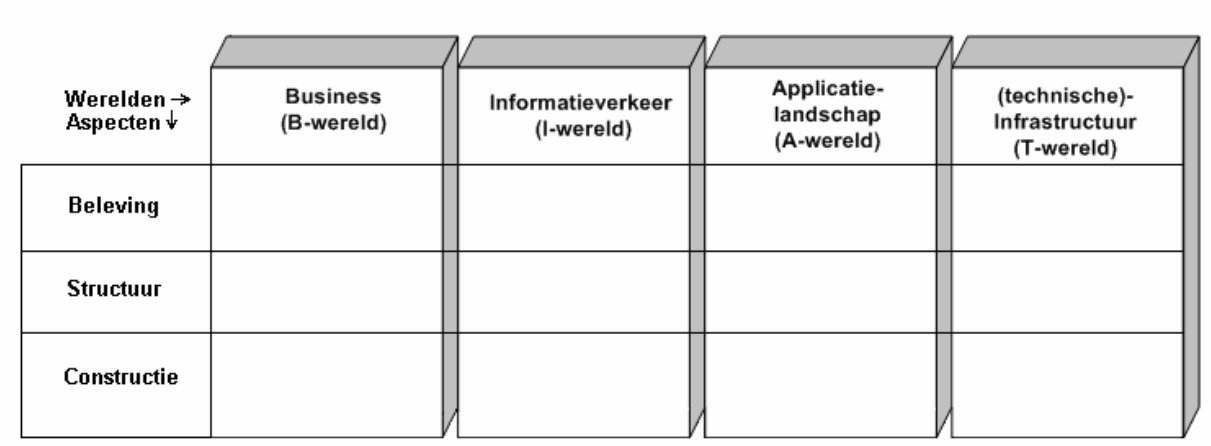
Figuur 3: IAF Framework

Het Rijsenbrij-Framework (Figuur 5) gebruikt andere aspecten, namelijk de architectuuraspecten beleving, structuur en constructie. Meer over deze aspecten in paragraaf 2.5. Rijsenbrij [Rijsenbrij, 2005] noemt deze aspecten ook wel de Q-Attributen van Vitruvius. Hij voegt aan deze drie aspecten nog twee andere toe, te weten governance en security/privacy waarna hij ze de Q-Attributen van Vitriuvius++ noemt (Figuur 4). De '++' staan dus voor de twee toegevoegde attributen. In het IAF Framework staan de beschouwingslagen loodrecht op de vier werelden van architectuur. De uitbreiding van de Q-Attributen wordt eveneens loodrecht op beide assen geplaatst. Deze driedimensionale ruimte die dan ontstaat beslaat de wereld waarin de architect werkzaam is en waarin hij alle principes, die te maken hebben met het opstellen van architectuur, kan onderbrengen. Meer over de rol van principes in hoofdstuk 4.



Figuur 4: Drie dimensies

Voor het rubriceren van security principes is de as van Q-Attributen erg bruikbaar daar de gevonden security principes vaak oplossingsgericht zijn en uit de engineering hoek komen. De principes zeggen vaak al iets over het conceptuele (wat is nodig), hoe we er invulling aan geven (logisch) en waarmee we het maken (fysiek). Interessanter is op welke architectuuraspecten ze betrekking hebben en tot in welke wereld ze actief zijn. Tevens komt de keuze voor dit framework voort uit de door de auteur opgedane ervaring hiermee tijdens de cursus 'Digitale Architectuur'. Het is mogelijk andere frameworks te gebruiken die in essentie hetzelfde voor ogen hebben, namelijk handvaten bieden voor structuur en ordening van termen en begrippen [Cohen, 2005]. Om echter alle frameworks te beschouwen is meer tijd nodig dan de tijd die staat voor het schrijven van een masterscriptie.



Figuur 5: Rijsenbrij-Framework

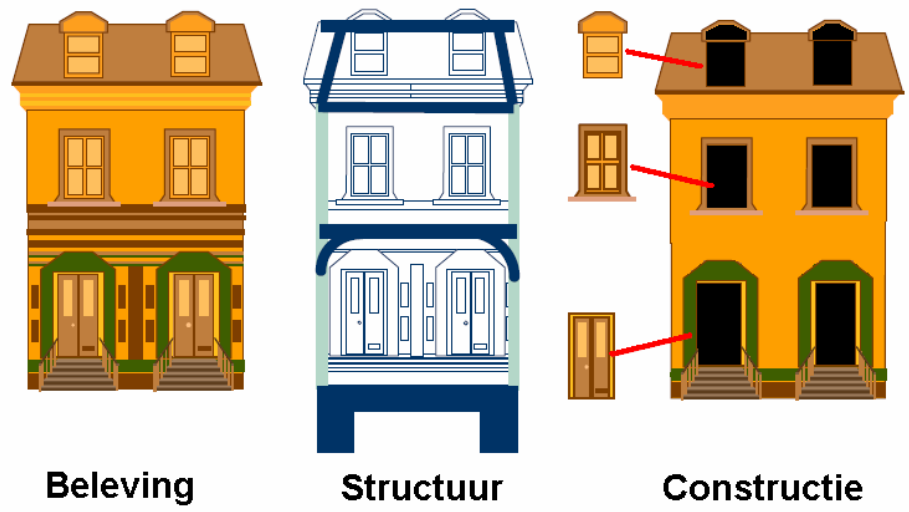
Rijsenbrij [Rijsenbrij, 2006] onderscheidt twee hoofdstromingen in de digitale architectuur, aangeduid als de prescriptieve benadering en de descriptieve benadering. Zijn voorkeur is dat architectuur een coherente en consistente verzameling principes is die de ontwerpruimte inperkt. Dit is een voorbeeld van de prescriptieve benadering. De descriptieve benadering gaat uit van IEEE-definitie 1471-2000. [IEEE] IEEE definieert architectuur, van software intensieve systemen, als 'the fundamental organisation of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution'. Dit klinkt als de metastructuur voor een oplossing.

Het essentiële verschil in deze twee benaderingen ligt in het feit dat de prescriptieve benadering uitgaat van de vraagkant, terwijl de descriptieve benadering uitgaat van de mogelijke oplossing. De descriptieve benadering is dus een benadering vanuit engineering, met het grote gevaar dat het belevingsaspect onderbelicht wordt en waarbij bedrijfsbrede flexibiliteit en optimalisatie wordt bemoeilijkt. Prescriptieve architectuur voldoet aan een service georiënteerde architectuur waarbij de trend juist deze brede flexibiliteit en optimalisatie is en niet alleen gedacht dient te worden in technische oplossingen. [Steen, e.a, 2005]

Voornamelijk is dit het geval bij security experts die oplossingsgericht denken. Hierin schuilt het gevaar. Namelijk het ongecontroleerd, ongedocumenteerd en vooral ongestructureerd aanbrengen van een ad-hoc security oplossing om een direct probleem te verhelpen. Gevolg is dat de oplossing niet past bij de enterprise architectuur. Inconsistentie, non-interoperabiliteit en in het ergste geval een breuk in de security in een ander (onbekend) onderdeel van het gehele systeem is mogelijk.

2.5 Architectuuraspecten

Zowel binnen de fysieke architectuur als binnen digitale architectuur zijn er drie architectuuraspecten waarop we een ontwerp beoordelen: structuur, constructie en beleving. De structuur zegt iets over de functionaliteit van het ontwerp, de constructie zegt iets over hoe het ontwerp in elkaar zit en de beleving zegt iet over hoe men het object ervaart (Figuur 6).



Figuur 6: Architectuuraspecten

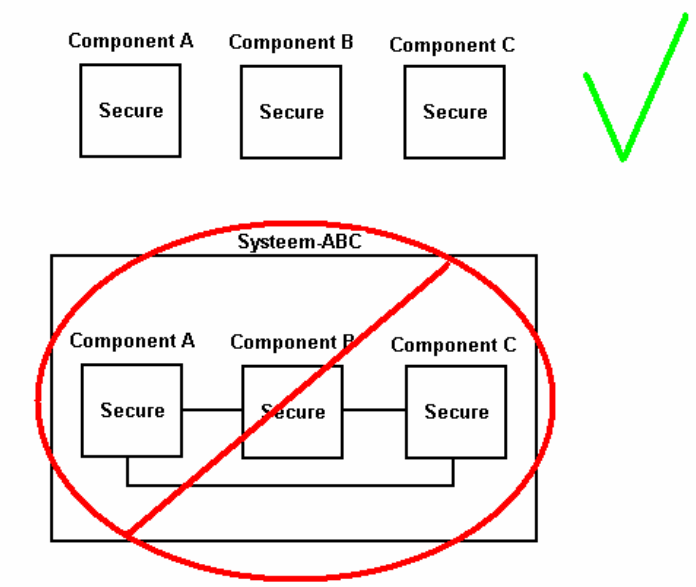
Beleving:'look and feel' (venustas)

Het linker huisje heeft te maken met harmonie en esthetiek. De toegepaste vormen en patronen leiden tot een kenmerkende verschijningsvorm en een kenmerkende wijze van gedragen. In de IT-wereld is beleving de 'look and feel' van het systeem voor de gebruikers en de wijze waarop het interacteert met de omgeving. De beleving bepaalt of het systeem geschikt is voor het doel ('firness for purpose') en of het bruikbaar is. De beleving moet de rol ondersteunen die het systeem in zijn omgeving speelt. Maar de beleving moet ook passen bij de cultuur en werkwijze van de externe betrokkenen en externe systemen waarmee het systeem interacteert. Vanuit security oogpunt is de beleving vaak het meest zichtbare aspect. Het zijn vaak tastbare objecten waarmee men te maken heeft. Een bewaker/portier bij de deur, persoonlijke identificatie pasjes, wachtwoorden en bijhorende applicaties en zelfs afgesloten serverruimten horen tot objecten die de look and feel binnen een organisatie qua security beïnvloeden.

Structuur: (utilitas)

Het middelste huisje is het huisje van de structuur of van de inhoud. Hoe zijn de verschillende functionaliteiten ten opzichte van elkaar gepositioneerd en hoe zijn de kwaliteitseisen daarbij verwerkt? Dus uit welke componenten bestaat het systeem en hoe werken die met elkaar samen. Security principes die betrekking hebben op het structuuraspect zeggen vaak iets over de aanpasbaarheid, interoperabiliteit en connectiviteit. In de fysieke wereld is het zaak componenten te onderkennen en te kijken hoe deze met elkaar interacteren. In wereld van security is dat niet zo eenvoudig. Security is van nature niet holistisch van karakter, zelfs niet compositioneel. Compositioneel betekent dat **niet** geldt dat wan-

neer componenten individueel secure zijn, ook het systeem waarin die componenten samenwerken (bij elkaar zijn gevoegd) dan secure is (Figuur 7).



Figuur 7: Security is niet compositioneel

Security kent niet dezelfde fundamentele zwaartekracht regels die bijvoorbeeld gelden in de bouwwereld waardoor veiligheid van één component niet betekent dat de combinatie met een andere veilige component het geheel ook veilig maakt. Hiervoor zijn wel principes, regels en richtlijnen opgesteld waarvan algemeen wordt aangenomen dat indien hieraan wordt voldaan, security gewaarborgd is. Meer hierover in hoofdstuk 6.

Constructie: (fermitas)

Het rechter huisje is het huisje van constructie. Het geeft antwoord op de vraag: 'Welke materialen worden gebruikt om het huisje te realiseren?' Hierin wordt gekeken naar welke technieken, technologieën en standaarden er gebruikt gaan worden. Het uiteindelijke streven van het aspect constructie is dat de keuzes zo worden gemaakt dat makkelijk meegegaan kan worden met wensen, eisen en veranderingen in de omgeving. Qua security dient hier bijvoorbeeld rekening gehouden te worden met toekomstige ontwikkelingen op het gebied van techniek. De in het verleden gekozen wachtwoorden kunnen met de tegenwoordige rekenkracht makkelijker worden achterhaald dan met de rekenkracht van vijftien jaar geleden. Dit heeft invloed op de te kiezen methode van cryptografie.

2.6 Architectuur in de boardroom

Hoe 'verkoop' je nu architectuur aan het management? Waarom moet er aan architectuur gedaan worden als organisatie? Rijsenbrij [Rijsenbrij, 2002] noemt in zijn boek een zevental algemene punten, waarom architectuur nuttig is.

1. Meer inzicht en overzicht met betrekking tot mogelijkheden en beperkingen van business transformaties. Voorts kan met architectuur op soepele wijze het continue transformatieproces in het gareel worden gehouden.
2. Meer adaptief (onder andere ruimte voor nieuwe relatievormen met klanten/lezers, partners en medewerkers).
3. Soepeler informatieverkeer ter vergroting van de bestuurbaarheid.
4. Rationalisatie van de geautomatiseerde informatiesystemen, databases, de outsourcing en hun onderling verband.
5. Efficiëntere systeemontwikkeling (programma's en projecten). Meer optimale supervisie bij outsourcing.
6. Uniformering van de (technische) infrastructuur.
7. Meer ruimte om nieuwe technologische mogelijkheden te kunnen incorporeren.

Een gedegen architectuur opstellen kost tijd en energie. Maar na verloop van tijd zal dit zich echter terugbetalen in tijdswinst, kostenbesparing en dus geld. [Rijsenbrij, 2002]
Enkele punten staan direct in relatie tot het security beleid binnen een organisatie. Punt 1 zorgt voor meer overzicht in transformaties en leidt dus direct tot een beter overzicht van knelpunten van security. Ook punt 4 waarbij de rationalisatie van geautomatiseerde informatiesystemen, databases en outsourcing en hun onderlinge verbanden in kaart worden gebracht, heeft dit voor het security beleid voordelen als zichtbaarheid en coördinatie. Immers, als het gaat om outsourcing, het aangaan van wereldwijde partners (samenwerkingsverbanden), het gebruik maken van globale netwerken, steeds meer aan elkaar gekoppelde databases en informatiesystemen, speelt zichtbaarheid, overzicht en structuur van de immense hoeveelheid gegevens, knooppunten en infrastructuur een belangrijke rol in de beveiliging van het geheel.

3 Security

De term ‘security’ is al meerdere malen gebruikt maar wat wordt er in dit onderzoek nu bedoeld? Dit hoofdstuk richt zich op operationalisering van de term alsmede de positionering ervan in dit onderzoek.

3.1 Inleiding

Door de toenemende complexiteit, integratie en transparantie van organisaties wordt security steeds moeilijker te borgen. Echter, security van systemen en security van informatievoorzieningen wordt vaak erg abstract omschreven. De welbekende uitspraak: ’het systeem moet veilig zijn’, is een hiervan een voorbeeld. Verkopers van security roepen vaak:’dit product maakt uw netwerk veilig’ of ‘wij beveiligen uw e-commerce’. Deze uitspraken zijn naïef en erg simplistisch. Het gaat hier namelijk om de beveiliging van een product in plaats van de beveiliging van een systeem. Je kunt je dus afvragen ‘beveiligd voor wie?’, ‘veilig tegen wat?’, ‘over welke wereld gaat het?’. Is het een conceptuele, logische of fysieke oplossing?

Daarnaast worden de termen ‘security’ en ‘veilig’ in vakjargon vaak door elkaar gebruikt waardoor ze contextloos raken. Tevens speelt slordig gebruik van de Engelse taal een belangrijke rol. Een eenduidig en correct gebruik van ‘security’ en ‘safety’ is in het Nederlands moeilijk te formuleren. Voor dit onderzoek wordt uitgegaan van de volgende vertalingen: Security betekent beveiliging, safety betekent veiligheid. Met security kom altijd privacy om de hoek kijken. Privacy is het recht om persoonlijke informatie voor jezelf, privé, te houden. Veel mensen willen niet dat sommige informatie over hen (zoals hun salaris, rekeningsaldo of strafblad) in de openbaarheid komt. Privacy betekent dat men dingen kan doen zonder dat de buitenwereld daar inbreuk op maakt.
Het betreft een eeuwige strijd der begrippen daar security en privacy als het ware elkaars tegenpolen zijn. Het is de taak van de architect beide zaken met elkaar zo goed mogelijk in evenwicht te houden tijdens het opstellen van een architectuur met als doel de optimale menselijk maat te borgen.

Het is van belang slordig taalgebruik te voorkomen en uniformiteit in de begripskeuze te waarborgen door consequent de correcte termen te gebruiken. Bij misplaatst gebruik ligt nergens de beperking tot informatie: de scope is de totale beveiliging van de organisatie inclusief de fysieke beveiliging van panden en medewerkers. Een architectuur framework beslaat deze scope.

3.2 Security en architectuur

In de term ‘IT security’ ligt de beperking tot de beveiliging van de IT-voorzieningen: uitgangspunt is de techniek en de mogelijkheden daarvan. De scope beperkt zich tot de beveiliging van en door technische infrastructuur. In de praktijk is ‘ICT-beveiliging’ synoniem voor ‘IT-beveiliging’, terwijl dat niet correct is. ICT-beveiliging bekommert zich ook om beveiliging van de communicatie, in IT-beveiliging is dat niet noodzakelijkerwijs het geval. De term ‘security’ geeft aan dat het de informatie is die beveiligd wordt. In vergelijking met ‘IT-beveiliging’ is het verschil duidelijk. Het doel is de beveiliging van informatie door (onder meer) ICT-middelen in te zetten. De zwaarte van de middelen moet een afgeleide zijn van het belang van de informatie. Discussies over security worden vaak gevoerd over de middelen en niet over het doel. Dit compliceert de discussie. [Hofman, 2004]

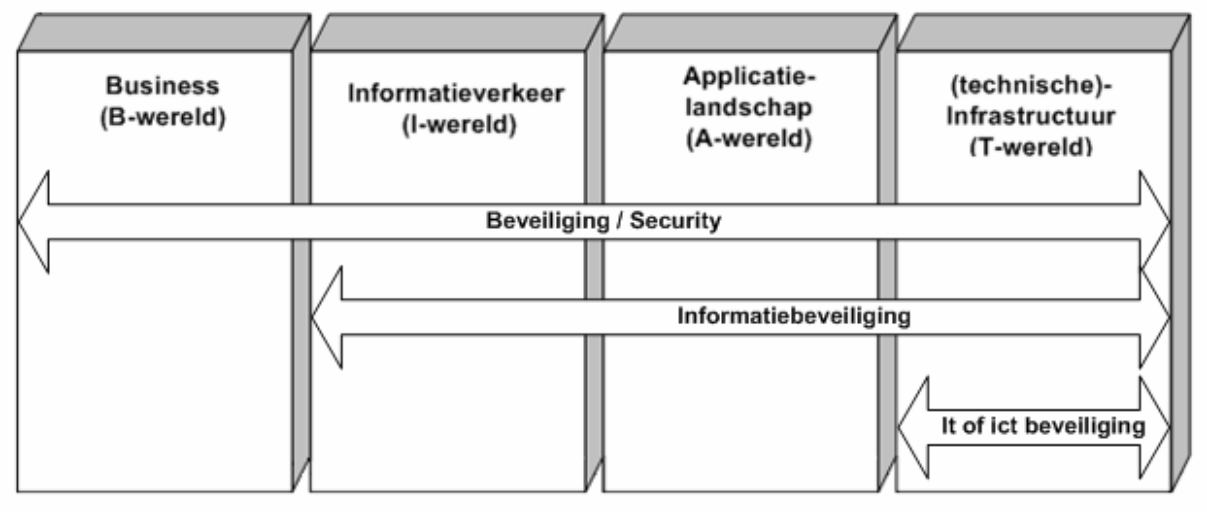
Verschillende security technologieën hebben belangrijke rollen en plaatsen in de totale beveiligingsoplossing maar belangrijk is te weten dat de context waarin ze worden afgebeeld belangrijker is dan de techniek. De context die voor structuur, begrijpbaarheid en dus helderheid moet zorgen komt terug in de architecturale beginselen. Immers beschikbaarheid, integriteit en vertrouwelijkheid (B.I.V. aspecten) kan op de niveaus van bedrijfsprocessen, informatie, informatiesystemen/applicaties en (technische)infrastructuur worden bezien. Complexiteit en onderlinge verbintenis tussen principes een grote rol. Stel dat binnen een enterprise architectuur de volgende twee principes voorkomen: ‘de klant kan 24 uur per dag, 7 dagen per week met ons zaken doen’ en ‘de klant kan waar ook ter wereld met ons zaken doen’. Deze twee principes hebben iets met elkaar te maken, dat behoeft geen discussie. Deze twee principes hebben erg veel invloed op het security beleid en dus ook op security principes. Het zou immers vanuit security oogpunt eenvoudiger zijn geweest wanneer we zeggen ‘de klant kan iedere dag van 9.00 tot 17.00 met ons zaken doen’ en ‘de klant kan alleen op de vestiging te Utrecht achter loket A met ons zaken doen’.

Het behoort niet tot dit onderzoek om de relaties van architectuurprincipes onderling, of relaties met security principes in kaart te brengen. Dit onderzoek noemt de belangrijkste security principes en hoe deze aan elkaar zijn gerelateerd. De link architectuur <-> security is hiermee gelegd.

.

3.3 Terminologie afbakening in het Rijsenbrij-Framework

Voor dit onderzoek zullen de terminologieën binnen het Rijsenbrij-Framework en de daarbij behorende afbakening worden gebruikt zoals in figuur 8 is weergegeven. De positie van de pijlen ten opzichte van elkaar en ten opzichte van de hoogte in de werelden (kolommen) hebben geen betekenis en zijn slechts geordend om het grafisch overzichtelijk te houden. Het zegt dus niets over de rangorde of belangrijkheid.



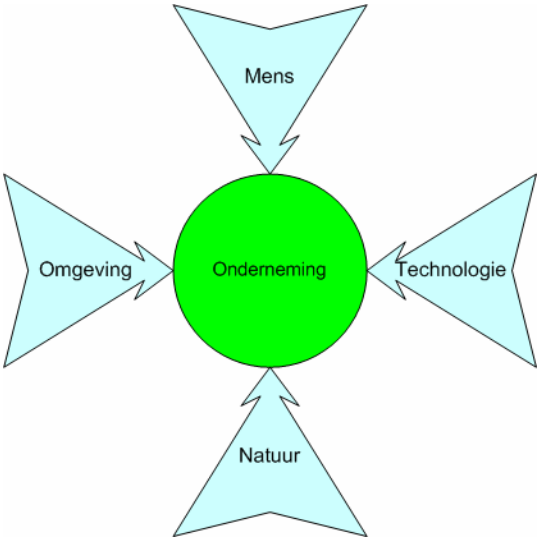
Figuur 8: Terminologie afbakening

In organisaties heeft een architect overleg met security experts zodat hij voldoende kennis heeft van de problematiek om architecturale principes verder uitwerken. Echter de concerns die de architect aanzetten tot actie komen voort uit het bedrijf. Het bedrijf, ook op boardroom niveau, hoort begaan te zijn met de security van bedrijfskritieke elementen en processen. Een architect kan deze aandachtspunten niet zelf destilleren. Hij gebruikt de concerns die het management formuleert en zet deze om naar principes. Daarna dient tussen de architect en de security experts een overeenkomst te ontstaan als basis voor wederzijds begrip die de 'Security Architectuur' in kaart brengt. De Security Architectuur is een overeenkomst waarin principes, grondbeginselen en belangrijke aandachtspunten van beide partijen zijn verwerkt. Kern van de zaak is dus het integreren van security met enterprise architectuur waarbij digitale architectuur het middel is om dit te bewerkstelligen.
Uit onderzoek blijkt dat 40% van de organisaties een Security Architectuur en 70% van de organisaties een Enterprise Architectuur heeft ontwikkeld. Echter slechts 10% van de organisaties beiden hebben geïntegreerd. [Burke en Scholtz, 2004]

3.4 Dreigingen en maatregelen

Een dreiging is de oorzaak waardoor informatie verloren kan raken of het informatiesysteem schade kan oplopen. Een organisatie heeft te maken met dreigingen uit de volgende verschillende gebieden, weergegeven in figuur 9 [Overbeek en Sipman, 1999]:

- Dreigingen vanuit de **mens.**
- Dreigingen vanuit de **omgeving.**
- Dreigingen vanuit de **technologie.**
- Dreigingen vanuit de **natuur.**



Figuur 9: Dreigingen waar de onderneming mee te kampen heeft

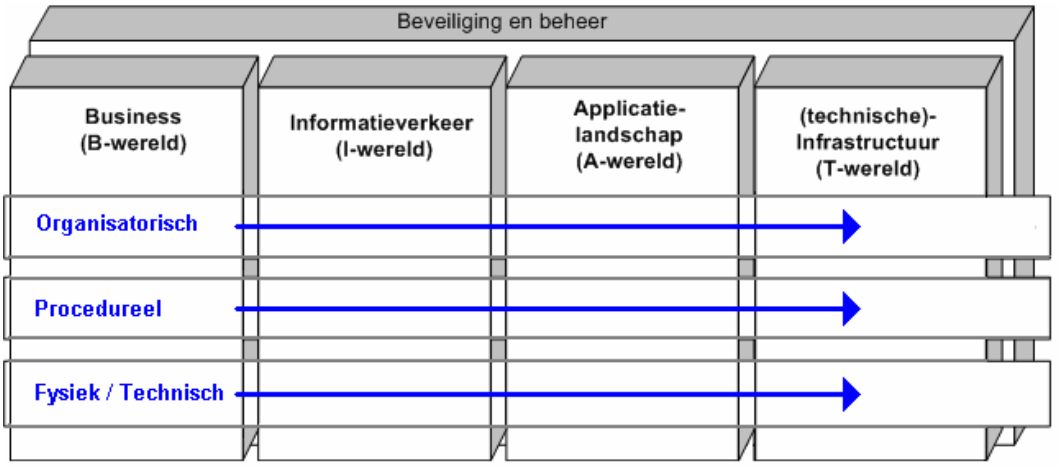
Na het bepalen van de verschillende bedreigende gebieden is het zaak te bepalen welke specifieke dreigingen inspelen op de organisatie, om aansluitend maatregelen te kunnen treffen. Dit behoort echter niet tot de scope van dit onderzoek. Voor dit onderzoek is het relevant om te weten dat er dreigingen zijn, uit welke gebieden ze voortkomen en dat de invloed hiervan in security principes tot uitdrukking komt.

Hoe gaan we nu met dreigingen om en welke maatregelen vloeien uit voort tot principes?

Voor de totale beveiliging van de organisatie worden een viertal beveiligingsmaatregelen naar werkwijze ingedeeld. Er wordt onderscheid gemaakt tussen:

- Organisatorische maatregelen.
- Procedurele maatregelen.
- Fysieke maatregelen.
- Technische maatregelen.

Organisatorische maatregelen zijn die maatregelen die betrekking hebben op de organisatie in z'n geheel. Het formuleren van het beveiligingsbeleid is een eerste stap. Dit bepaalt verder alle andere maatregelen. Het beleid moet vervolgens uitgewerkt worden in een beveiligingsplan. Dit geeft de concrete maatregelen aan die genomen worden. Tevens worden kaderstellende zaken geregeld als: verantwoordelijkhedenverdeling, controle en rapportagelijnen. Procedurele maatregelen zijn de regels die beschrijven hoe de diverse beveiligingsmaatregelen uitgevoerd moeten worden. Fysieke maatregelen zijn alle materiele producten die ingezet worden om de gewenste beveiliging te realiseren. Technische maatregelen zijn alle maatregelen die in de programmatuur ingebouwd zijn.
Figuur 10 laat zien hoe de maatregelen passen binnen het Rijsenbrij-Framework.



Figuur 10: Maatregelen in het Rijsenbrij-Framework

3.5 Risicomanagement als basis voor maatregelen

Risicomanagement en security gaan hand in hand. Het is noodzaak risico's te begrijpen en maatregelen voor te bereiden om te kunnen inspelen op dreigingen en gevolgen van een breuk in de beveiliging. GartnerGroup [Conference Presentatie, 1999] hanteert de volgende stadia binnen een business gedreven risicomanagement:

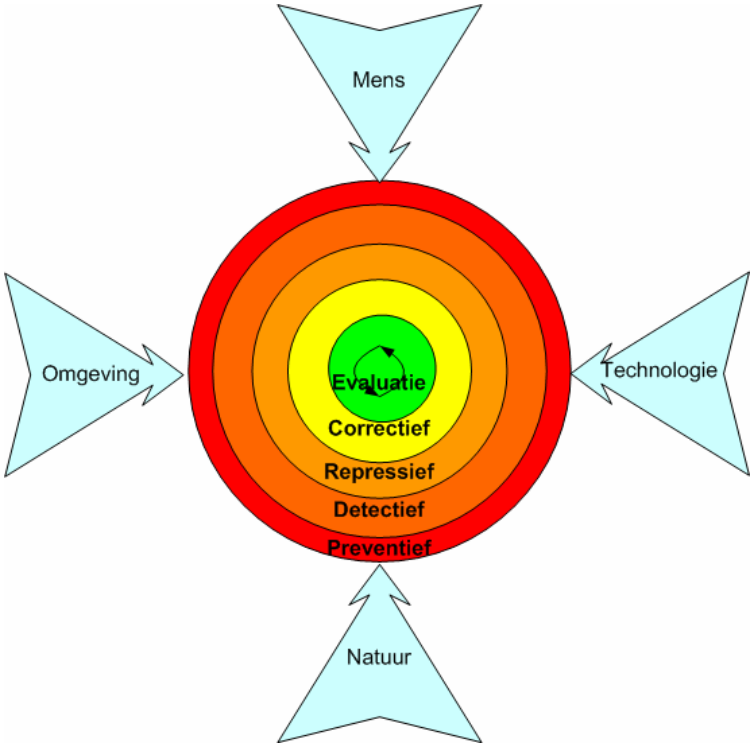
1. Risico identificatie en categorisatie
   - Breuktypering die schade toebrengt aan data (uitlekken van informatie, modificatie van informatie,etc).
   - Impact van de breuk (financiële verliezen, wettelijke aansprakelijkheid, etc).
   - Niveau van breuk (catastrofaal, behoorlijk, lokaal, etc).
2. Profielschets van de (te gebruiken) informatietechnologie.
3. Selectie van controls, het elimineren van redundantie.
4. Kostenanalyse.
5. Alternatieven analyse.

Risicomanagement, volgens GarnterGroup, onderscheidt dus al enkele kernpunten. Punten die belangrijk worden gevonden tijdens het security proces. Het is dus niet verwonderlijk dat bovengenoemde stadia impliciet voortkomen uit concerns. Concerns die leiden naar principes en principes weer verbijzonderd worden naar betreffende regels, maatregelen en richtlijnen. GartnerGroup noemt het misschien geen principes, wellicht zijn ze dat ook niet in de strikte definitie van een principe in dit onderzoek, echter het belang van de stadia zijn voedingsbodem voor het opstellen van principes die gebruikt dienen te worden in een enterprise architectuur.

3.6 Stadia in beveiligingscyclus

De beveiligingscyclus omvat vijf stadia die als schil om de organisatie heen zitten (Figuur 11) [Snel, 2005]:

- Preventie. Tracht problemen te voorkomen.
- Detectie. Indien probleem wel optreedt, dient dit zo snel mogelijk te worden gedetecteerd.
- Repressie. Bij een probleem zorgen repressieve maatregelen ervoor dat de schade beperkt blijft. Een voorbeeld in de reële wereld zijn automatische brandblussers.
- Correctie. Nadat een probleem is opgetreden dient de situatie weer te worden hersteld in originele status.
- Evaluatie. Is de situatie weer hersteld, dan is het nuttig om het incident te evalueren en lering te trekken uit de voorgaande handelingen. Dit is een continue repeterend proces.



Figuur 11: Stadia in de beveiligingscyclus

3.7 Security in de boardroom

In de boardroom wordt een degelijk security beleid vaak onderschat (of zelfs genegeerd). Veelal wordt informatie security gelijkgesteld aan 'iets' IT-achtigs en is het geen punt van discussie in de boardroom. Het risico dat zich daarbij voordoet is een eenzijdig monopolistisch beleid van de IT-afdeling die alle touwtjes wat betreft innovatie, implementatie en beheer. Het streven is dat security een corporate en strategisch issue wordt dat uit het IT-domein wordt getrokken en wordt toegevoegd aan de business, afgestemd op de algemene bedrijfsvoering en in het algemene risicomanagement beleid wordt opgenomen.
Om de boardroom duidelijk te maken hoe belangrijk het is om een degelijk informatie security beleid te voeren, moeten ook de concerns geformuleerd worden in de voor hun begrijpbare en relevante taal. LogicaCMG [IS-Governance, 2005] geeft enkele punten, geformuleerd op boardroomniveau, waarop een slechte security beleid invloed op kan hebben:

- Korte en lange termijn revenu voor het bedrijf.
- Klanttevredenheid en klantloyaliteit.
- Merk imago en reputatie in de markt (herstel duurt jaren).
- Aandelenwaarde.
- Investeringsgedrag en vertrouwen.
- Motivatie en tevredenheid van de werknemers.
- Public relations.
- Breuk van legale of regulerende controls.

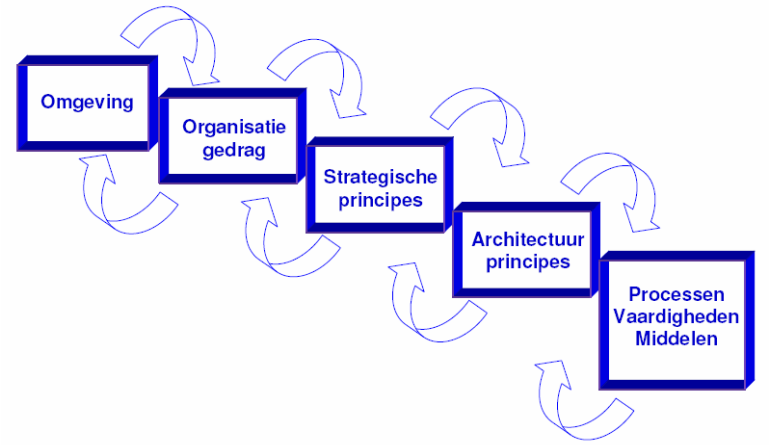
3.8 Aandachtsgebieden binnen Security

Zowel uit de theorie alsook uit interviews met security deskundigen blijkt dat het erg moeilijk is eenduidig 'de' aandachtsgebieden te formuleren. Reden hiervoor is de keuze die wordt ingegeven door het perspectief dat je op de organisatie neemt. Standaard perspectieven worden aangeboden door frameworks zoals CobiT[3] en de Code voor Informatiebeveiliging[4]. Voorbeelden van aandachtsgebieden zijn: fysieke beveiliging, business continuïty, logische beveiliging, personeel, commercieel, operationeel, administratie, financieel, informatie, juridisch, technologie, etc. Belangrijk is uit te gaan van de concerns die voortvloeien uit de strategie of leven bij stake-holders: bijvoorbeeld hoe te beveiligen tegen bewuste criminele acties of bedreigingen tegen onderbreking van de bedrijfsprocessen. Of hoe kan het vertrouwen tussen partners in een keten met maatregelen verbeterd worden?

[3] http://www.controlit.org/
[4] www.cvib.nl

4 De rol van principes

Principes komen veelal voort uit de omgevingsfactoren plus de interpretatie die een bestuurder daaraan geeft. Omgevingsfactoren zijn te clusteren in een aantal gebieden: overheidsregulering, maatschappelijke trends, industriecondities, industrieontwikkelingen, eigen missie statement, de visie en de gekozen concurrentiestrategie. Meestal beschrijft men niet meer dan vier tot acht strategische principes. Deze strategische principes zijn de 'dragers' van alle onderliggen en geabstraheerde principes waarlangs de architect zijn weg volgt. In figuur 12 wordt het speelveld van de architect weergegeven.



Figuur 12: Speelveld van de architect

4.1 De definitie van een principe

Het principe geeft aan WAT er geregeld moet worden. Het is een fundamenteel idee, bedoeld om een algemene eis te vervullen. Elk ontwerp van de onderneming dan wel haar ondersteuning met IT-middelen begint dus met een verzameling principes, die als het ware de ontwerpruimte inperkt. Architectuur is daarom een hulpmiddel om ontwerpbeslissingen te vereenvoudigen en te uniformiceren.
Principes komen terug in alle vier de werelden van architectuur. Van de business tot en met de infrastructuur. In de businesswereld worden enkele leidende strategische principes opgesteld. Principes uit de informatiewereld worden daarna afgeleid uit principes van de business wereld. Een principe uit de informatiewereld wordt afgeleid uit één of meerdere principes uit de businesswereld, principes uit de informatiesysteemwereld uit de informatiewereld en principes uit de infrastructuurwereld uit de informatiesysteemwereld. Belangrijk is het om te begrijpen dat er géén principes uit de informatiewereld mogen zijn die niet terug te herleiden zijn tot een principe uit de businesswereld en zo verder voor alle andere werelden.

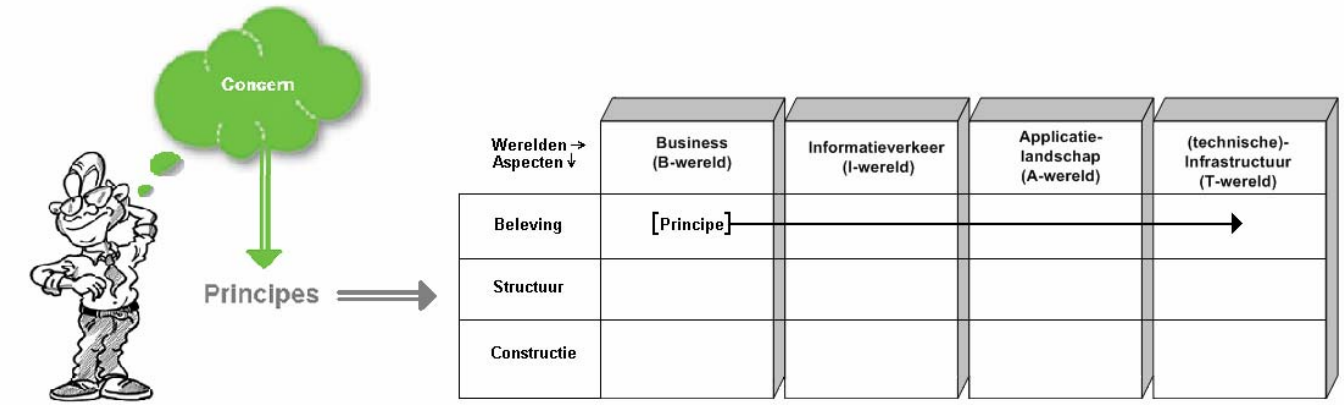
Zoals gezegd komen principes elementair voort uit concerns waarbij de principes de ontwerpruimte beperken en een voorschrijvend karakter hebben (Figuur 13). De principes worden geconcretiseerd naar regels, richtlijnen en standaarden. IEEE [IEEE] geeft de volgende zeer bruikbare definitie van een concern: "Concerns zijn zaken die te maken hebben met de ontwikkeling, de werking of andere

aspecten van een systeem die belangrijk zijn voor één of meerdere stake-holders. Concerns bevatten systeemeigenschappen als: prestaties, betrouwbaarheid, beveiliging, verspreidbaarheid en ontwikkelbaarheid.

Hierin kan een systeem ook worden opgevat als de onderneming in zijn geheel. Dit wetende rijst de vraag wat een concern binnen een onderneming betekent en hoe dit tot uitdrukking komt. Wordnet [5]geeft uitleg: a concern is something that interests you because it is important or affects you; "the safety of the ship is the captain's concern".

Dus een directeur van een consultancybureau kan het volgende concern hebben: ‘indien vertrouwelijke documenten openbaar worden gemaakt, leid ik verlies’. Dit kan worden verbijzonderd naar het principe ‘vertrouwelijke documenten moeten vertrouwelijk blijven’.

Principes moeten leesbaar, begrijpbaar en navolgbaar zijn. Dit betekent ze niet dienen te worden opgesteld voor één bepaald individu of groep. BurtonGroup zegt hierover het volgende: “Enterprises should be sure to include (nontechnical) business managers in the process of formulating their architecture principles. The more that such management is involved, the higher the likelihood that principles will be solid, understandable, and useful. Stated another way, consensus about principles among the top decision makers is essential for ensuring that the principles have the authority to guide decisions”.



Figuur 13: Concerns naar principes naar architectuur

[5] http://wordnet.princeton.edu

4.2 Principes in security context

In alle drie de huisjes (hoofdstuk 2, paragraaf 2.5, figuur 6) zijn principes te vinden die invloed hebben op het security beleid. Net als in de fysieke wereld staan de huisjes niet los van elkaar. Keuzes in de een kunnen de vrijheid in de ander beïnvloeden. Het is echter van belang om aan alle drie huisjes voldoende aandacht te besteden. Van oudsher krijgt het rechterhuisje het meeste aandacht en is het linkerhuisje een beetje het stiefkind. Vaak wordt in de wereld van security gebruik gemaakt van losse kortstondige oplossingen om een probleem ‘even snel’ op te lossen. Een extra wachtwoord, firewall of server, wordt ingezet om een security probleem op te lossen zonder te kijken wat de invloed is op het hele (beveiligings)geheel, laat staan wat de gevolgen zijn voor de beleving door de gebruikers. Indien gebruikers deze ‘oplossingen’ als hinderlijk ervaren en daarvoor zelf maatregelen treffen om de beveiliging te omzeilen, is het beoogde effect weg waardoor inzage in de problematiek juist verminderd.

4.3 De ideale weg naar security

Het succesvol integreren van security in een organisatie hang af van veel (niet-technische) factoren. Het type organisatie, de omgeving waarin de organisatie ‘leeft’, het type zaken dat het bedrijf doet, de volwassenheid van de managementfuncties en bedrijfsprocessen en de volwassenheid van de IT-processen, de mensen die werkzaam zijn binnen de organisatie en de cultuur waarin zowel de mens leeft als individu alsook de cultuur waarvan de organisatie deel uitmaakt, zijn zaken die inspelen op het integreren van een security beleid. Het is daardoor onmogelijk om een ideale weg te beschrijven die lijdt tot de ultieme combinatie van een werkbare-, leefbare-, optimaal op de menselijke maat afgestemde en volledig veilige omgeving.

4.4 Terminologieën recapitulerend

Een organisatie heeft te maken dreigingen uit een viertal hoeken:

- Dreigingen vanuit de **mens.**
- Dreigingen vanuit de **omgeving.**
- Dreigingen vanuit de **technologie.**
- Dreigingen vanuit de **natuur.**

Maatregelen tegen deze dreigingen worden onderverdeeld in de volgende categorieën:

- Organisatorische maatregelen.
- Procedurele maatregelen.
- Fysieke maatregelen.
- Technische maatregelen.

In elk van deze categorieën komen de volgende fasen terug:

- Preventie. Tracht problemen te voorkomen.
- Detectie. Indien probleem wel optreedt dient dit zo snel mogelijk te worden gedetecteerd.
- Repressie. Bij een probleem zorgen repressieve maatregelen ervoor dat de schade beperkt blijft, denk aan automatische brandblussers.
- Correctie. Nadat een probleem is opgetreden dient de situatie weer te worden hersteld in originele status.
- Evaluatie. Is de situatie weer hersteld, dan is het nuttig om het incident te evalueren en lering te trekken uit de voorgaande handelingen.

Architectuuraspecten hebben betrekking op:

- Beleving.
- Structuur.
- Constructie.

Welke security principes zijn er nu? En hoe zijn nu principes te ordenen? Er is voor dit onderzoek een lijst met security principes opgesteld op basis van:

- Principes uit de literatuur.
- Principes die voortkomen uit interviews met relevante personen uit de wereld van security .

In hoofdstuk 6 zullen deze principes worden opgesomd en uitgelegd waarna ze in hoofdstuk 7 worden gerubriceerd in het Rijsenbrij-Framework.

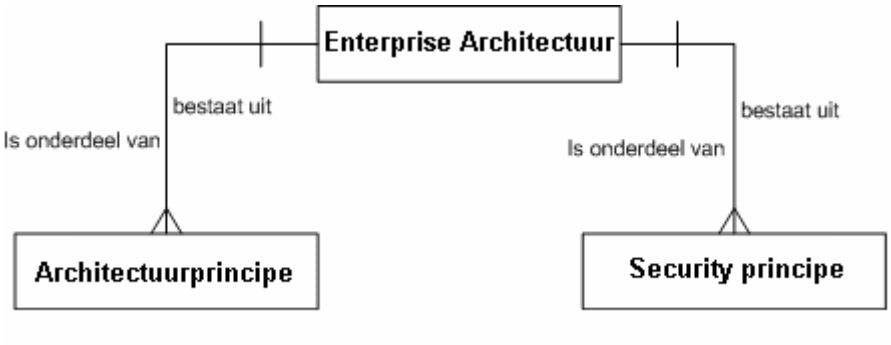
5 Terminologieën in context

Een belangrijk onderwerp in dit onderzoek is het operationaliseren van de gebruikte termen en relaties ertussen in kaart te brengen. Hierdoor wordt precies duidelijk wat we bedoelen met de gebruikte termen maar ook wat we niet bedoelen. Het in kaart brengen van relaties brengt structuur aan, zorgt voor overzicht en dient als metaplattegrond van het speelveld.
Hiervoor wordt gebruik gemaakt van een Entiteit Relatie Diagram (ERD). In een ERD worden entiteiten geplaatst, in dit geval de gebruikte termen, en de relaties die deze entiteiten met elkaar hebben. Op deze manier wordt de samenhang van termen duidelijk waardoor er makkelijker mee gewerkt en over geredeneerd kan worden in een later stadium.
De gebruikte ERD-methodiek wordt beschreven in AIV [AIV,1999].
Een entiteit is weergeven als rechthoek. Tussen entiteiten bestaan relaties. Een relatietype wordt weergegeven door een lijn (tussen entiteittypen) en de naam van het relatietype. Voor het noteren van de namen voor relatietypen in het ERD maken we de volgende afspraak, om het lezen van het schema gemakkelijk te houden:

- Boven de lijn: van linkerentiteit naar rechterentiteit lezen.
- Onder de lijn: van rechterentiteit naar linkerentiteit lezen.
- Rechts van de lijn: van bovenste entiteit naar onderste entiteit lezen.
- Links van de lijn: van onderste entiteit naar bovenste entiteit lezen.

5.1 Terminologieën, de kern

Zoals uit paragraaf 2.2 volgt zijn principes de kernelementen in een architectuur. In een ERD wordt dit weergegeven als in figuur 14. In dit onderzoek is de scope de rechtertak in het figuur, namelijk de security principes en hun rol in een enterprise architectuur.



Figuur 14: Kern ERD

5.2 Terminologieën, de scope

Van alle relevante termen voor dit onderzoek is onderstaand ERD het resultaat (Figuur 16). Om relaties van entiteiten te kunnen lezen is het zaak de entiteiten voldoende te operationaliseren. Dit gebeurd voor de leesbaarheid op alfabetische volgorde.

Aandachtsgebied

Zelfde definitie als in paragraaf in 1.4:

Binnen organisaties in z'n geheel alsook binnen domeinen en subdomeinen van organisaties kunnen aandachtsgebieden worden herkend. Een aandachtsgebied is een cluster van bedrijfsprocessen waar men speciale aandacht moet besteden op het gebied van security. Een voorbeeld van een aandachtsgebied is 'klantrelatie' waarbinnen o.a. orderregistratie en klantcontact als bedrijfsprocessen kunnen worden onderkend.

Aspect

Zelfde definitie als in paragraaf in 1.4:

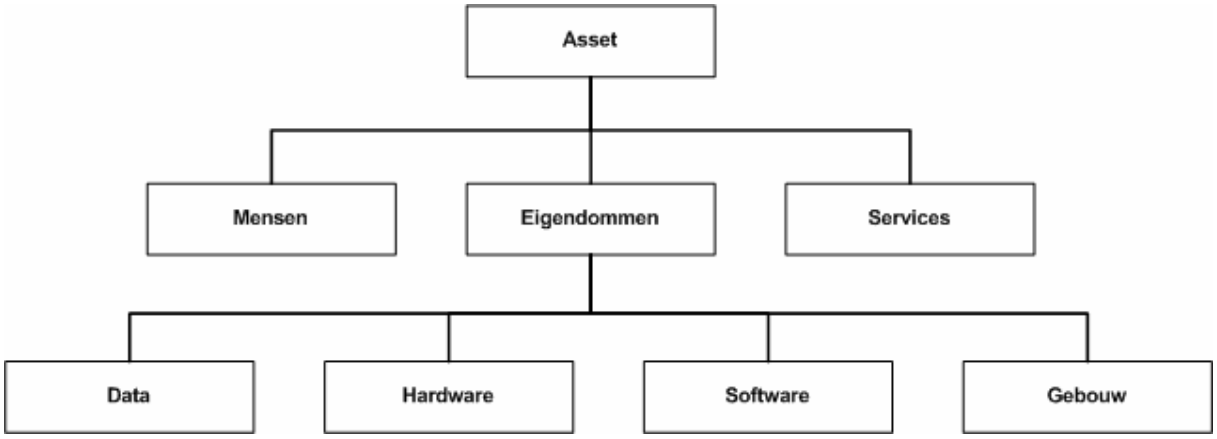
Binnen de context van security zijn er drie aspecten te beschouwen: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV, of CIA Confidentiality, Integrity en Availability, in het Engels).

De aspecten zeggen iets over waaraan binnen het aandachtsgebied moet worden voldaan.

Asset

Het begrip *asset* behoeft enige verduidelijking daar het een verzameling van entiteiten bevat. Onderstaande figuur (Figuur 15) laat de opbouw zien van een asset op de wijze waarop er in dit onderzoek naar wordt gekeken.

Voor dit onderzoek en dit ERD beperkt dit zich tot (te beveiligen) elektronische data die van waarde is voor de onderneming.



Figuur 15: Opbouw van een asset

Concern

De zorg van de belanghebbende die voortkomen uit hun verantwoordelijkheden of belangen. Concerns hebben te maken met de ontwikkeling, werking, voortbestaan of andere aspecten van een systeem die belangrijk zijn voor één of meerdere stake-holders. Concerns omvatten systeemeigenschappen als prestaties, betrouwbaarheid, beveiliging, verspreidbaarheid en ontwikkelbaarheid.

Dreiging

Kan met een bepaalde waarschijnlijkheid gebeuren en heeft impact op de (bedrijfs)doelstellingen.

Enterprise Architectuur

Zelfde definitie als in paragraaf in 1.4:

Enterprise architectuur is principe georiënteerd en dient om kaders te geven op enterprise niveau (het hoogste niveau) die leidend zijn voor alle onderliggende niveaus, zoals domeinen, informatiesystemen en digitale werkruimtes. Enterprise architectuur leidt tot een high-level ontwerp van de onderneming in zijn totaliteit. Het doel is een eerste indeling in domeinen bestaande uit bedrijfsprocessen, applicaties en de onderliggende technische infrastructuur. Een enterprise architectuur heeft meerdere gebruiksdoeleinden: atlas voor het topmanagement, beheersing van complexiteit, kaderzetting voor realisatie en communicatiemiddel. Het atlasaspect van de enterprise architectuur wordt gestalte gegeven door een verdeling van de onderneming in een aantal redelijk autonome domeinen. Hoofddomeinen zijn vaak: delivery, marketing & sales, leveranciers & inkoop. Ondersteunende domeinen beslaan zaken als personeel, informatie, organisatie, financiën en huisvesting. [Rijsenbrij, 2002]

Security principe

Zelfde definitie als in paragraaf in 1.4 met daarbij toegespitst op security:

Principes zijn richtinggevende uitspraken ten behoeve van essentiële beslissingen, een fundamenteel idee bedoeld om een algemene eis te vervullen. Principes beïnvloeden direct de wijze waarop de IT zal worden ingezet. Foute principes kunnen desastreus zijn bij transformaties. Principes dienen te worden geconcretiseerd naar zaken die moeten, dat zijn de regels en standaarden, en zaken die verstandig zijn: de richtlijnen, ook wel ‘best practices’ genoemd. [Rijsenbrij, 2003]

Maatregel

Beslissing, handeling waardoor men iets regelt.

Onderneming

Een doelgericht samenwerkingsverband van mensen.

Risico

Gevolg van een dreiging. Betekenis van risico heeft dan ook een toevoeging op de betekenis van een *dreiging* en wel als volgt: Kan met een bepaalde waarschijnlijkheid gebeuren, heeft een **negatieve** impact op het bereiken van (bedrijfs)doelstellingen en de continuïteit van bedrijfsvoering.
Dus: risico=dreiging x P.(voorkomen). In natuurlijke taal: een risico is een dreiging vermenigvuldigd met de kans dat de dreiging zich kan voordoen.

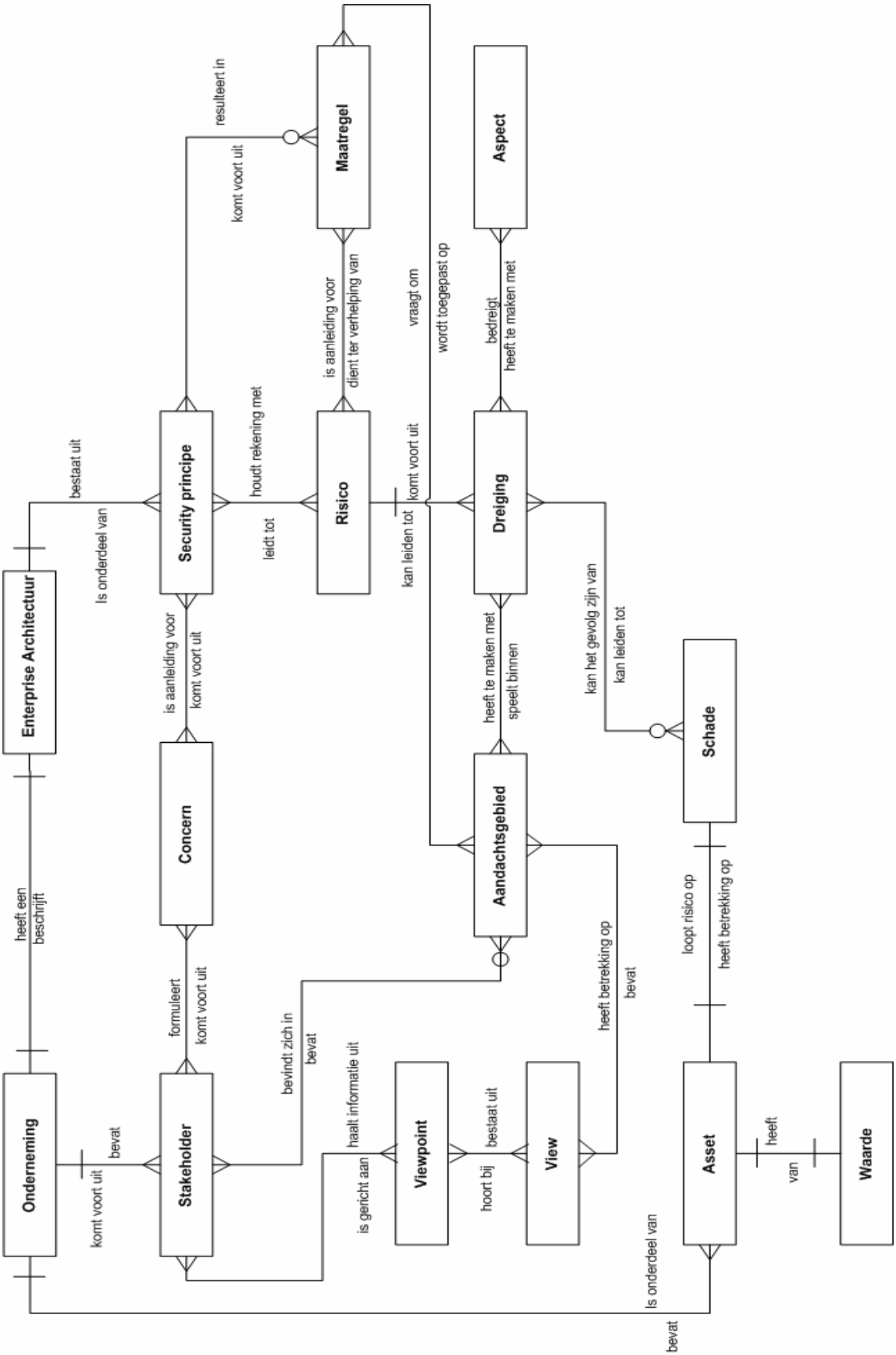
Schade
Het financiële verlies (waarde van het bijhorende asset) dat het gevolg kan zijn van een dreiging + het directe of indirecte financiële verlies van gevolgen die voortvloeien uit het verlies van het asset.

Stake-holder
Een persoon die enig belang heeft bij de inhoud van de betreffende architectuurbeschrijving en/of de security hiervan.

View
Een view is een onderwerp binnen security . Vanuit de relevante concerns kan inhoudelijk invulling worden gegeven aan views. Niet alle onderwerpen zijn voor iedere stake-holder belangrijk. Een view wordt gemaakt om deze aan een specifieke groep stake-holders te kunnen presenteren. Door deze selectie van onderwerpen wordt voorkomen dat zijn door de bomen het bos niet meer zien.

Viewpoint
Een viewpoint is een beschrijving vanuit het oogpunt en wordt er dus op een andere manier naar gekeken. Voorbeeld: een brandweerman kijkt naar een andere beveiliging van een gebouw dan een inbraakpreventiedeskundige en hebben beide andere belangen, terwijl ze beide kijken naar de beveiliging van het gebouw.

Voor figuur 16 geldt dat de entiteiten Stake-holder, Viewpoint, View, Aandachtsgebied en Concern gaan over security !!



Figuur 16: ERD van kernbegrippen

6 Security principes

In de vakliteratuur over security en security principes wordt opvallend weinig aandacht besteed aan een ordening van principes. Hierdoor zijn de lijsten van principes vaak lang, onoverzichtelijk en lijken ze vaak op grote brainstormsessies. Het gebrek aan ordening resulteert in een ongestructureerde, niet-gevalideerde overvloed aan uitspraken die niet als principes bestempeld kunnen worden. Deze 'uitspraken' dienen dus eerst te worden herschreven. Daarnaast is a-transparantie en het gebrek aan traceerbaarheid naar de oorsprong van principes een groot probleem.
Dit hoofdstuk somt de gevonden, herschreven en zelf opgestelde principes op en brengt deze onder in een raamwerk. Tevens wordt met behulp van een kruisreferentie-tabel de oorsprong en relaties van de principes in kaart gebracht.

6.1 Ordening van principes

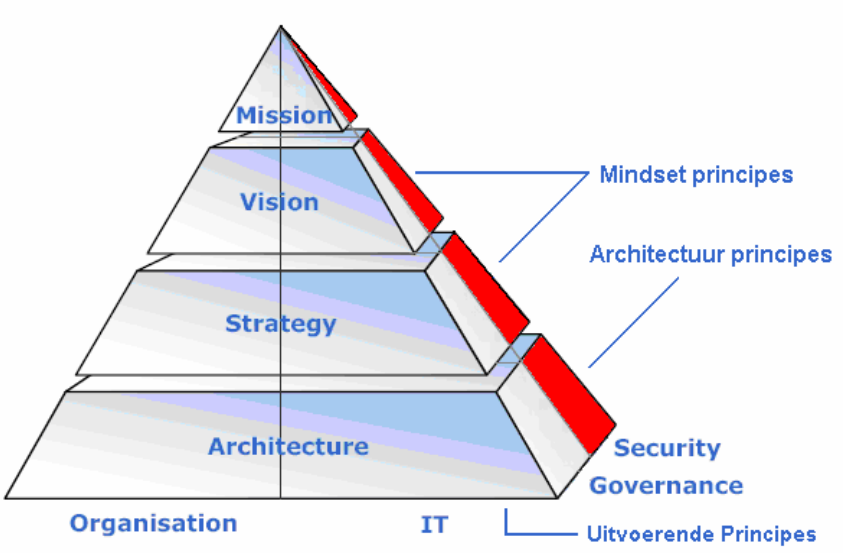
Binnen de (system)engineering hoek worden principes vaak op applicatie en procesniveau geordend. Doordat het aantal principes kleiner is dan bijvoorbeeld op ondernemingsniveau en het project of proces in het geheel is te overzien, is de kans op volledigheid nog reëel. Het National Institute of Standands and Technology (NIST) [Stoneburner,e.a, 2001] en Schumacher [Schumacher, 2003] schrijven artikelen over engineering principes waarbij ze enkele nuttige gedetailleerde principes aanwijzen die ook op hogere (bedrijfs)niveau bruikbaar zijn. Dit is verwonderlijk daar engineering normaliter oplossingsgericht en dus specifiek en gedetailleerd is.
Voor grotere projecten en het opstellen van principes op bedrijfsniveau is een andere ordening vereist waarbij complexe en meer specifieke principes afgeleid worden van overkoepelende principes.

In een rapport over security principes door Capgemini [Hofman en Elsinga, 2000] wordt de volgende ordening gehanteerd:

- Mindset principes op strategisch niveau (Hoe denkt de organisatie over security?).
- Architectuurprincipes op tactisch niveau (Hoe wil de organisatie verdedigen?[6]).
- Uitvoerende principes op operationeel niveau (Hoe wil de organisatie handelen?).

Verrassend is hier de naamgeving voor de categorie 'Architectuurprincipes'. Immers een ordening van principes heeft betrekking op de gehele architectuur en alle vier de werelden van architectuur. Mindset principes worden op het hoogste niveau geconcipieerd, en vormen de basis voor architectuur- en uitvoerende principes. In de Missie, Visie, Strategie – piramide uit paragraaf 2.3 kan deze ordening worden ingevuld als in figuur 17.

[6] Dus een inrichtingsvraagstuk. Inrichting lijkt veel op het middelste huisje van architectuur, vandaar dat hier over architectuurprincipes wordt gesproken.



Figuur 17: Oorsprong principes in MVS piramide

"*Mindset principles are used by the organisation to formulate its security strategy. The context of architecture principles is defined by the mindset and finally the context of the execution principles is highly dependant on the culture of the organization combined with the mindset principles the organisation uses to formulate its security strategy. Because implementing a corporate or enterprise security strategy consistently, requires a lot of change and this is where the human factor plays an important role"*. [Hofman en Elsinga, 2000]

Vrij vertaald: de inhoud van de architectuurprincipes wordt bepaald door de mindset en uiteindelijk zijn de uitvoerende principes afhankelijk van de cultuur van de organisatie gecombineerd met de mindset principes die de onderneming gebruikt om het security beleid te formuleren.

Natuurlijk houden principes rekening met de cultuur van de onderneming, maar cultuur is niet dominant en indien aanwezig geldt dit zeker niet voor alle principes. Er zijn immers principes die onafhankelijk van cultuur en algemeen geldend zijn. Bijvoorbeeld pervasive principe 10 (Paragraaf 6.1.1, PV-10): *Fysieke beveiliging is net zo belangrijk als logische beveiliging*.

De invulling die de onderneming hieraan geeft, dus de concretisering naar regels, richtlijnen en standaarden, is afhankelijk en onderhevig aan de cultuur die binnen de onderneming heerst. Het principe niet! De ordening in mindsetprincipes, architectuurprincipes en uitvoerende principes lijkt beter geschikt om gedetailleerde principes van extra informatie te voorzien, dan een algehele ordening op ondernemingsniveau te bewerkstelligen. De principes van Capgemini [Hofman en Elsinga, 2000] worden om deze reden onder verdeeld binnen de drielagen hiërarchie volgens de Generally Accepted System Security Principles (GASSP) [Gassp, 1999].

Een ordening die ruimte biedt voor deze cultuur onafhankelijke manier van opstellen van principes wordt geboden door het Generally Accepted System Security Principles Comité (GASSP). Het GASSP is een comité dat bestaat uit een groot aantal leden (wereldwijd) op het gebied van security. Het GASSP heeft een basis gelegd voor het opstellen van security principes die zeer bruikbaar is voor het opstellen van een architectuur.

GASSP is conventioneel, wat wil zeggen dat de principes geformuleerd in GASSP 'generally accepted' zijn door overeenkomsten en niet door formele verificatie of abstractie van basisconcepten.
De principes zijn opgesteld door ervaring, redelijkheid, aanpassing, gebruik en voor een groot deel praktisch nut. Generally accepted is iets anders dan universally accepted. Het verschil zit hem in het feit dat alle principes uitzonderingen kunnen hebben.
De ordening van principes is dermate belangrijk daar ze iets zeggen over hun reikwijdte binnen de vier werelden van architectuur en daarmee ook de scope en moment van implementatie bepalen waarmee de architect bij zijn ontwerp rekening dient te houden.

De drie lagen hiërarchie volgens het GASSP:

- Pervasive (iets wat het totale aangaat);
  Klein in aantal, fundamenteel, veranderen bijna nooit.
- Breed functioneel;
  Onderliggend aan één of meer pervasive principes. Groter in aantal en specifieker. Sturen en geven invulling aan het opstellen van gedetailleerde principes. Veranderen in principe alleen bij 'grove' ontwikkelingen in technologie en andere invloedrijke issues.
- Gedetailleerde principes;
  Onderliggend aan één of meer breed functionele principes. Groot in aantal, specifiek, er boven uit stekend, veranderen vaak door veranderingen in technologie en andere invloedrijke issues.

Het is onmogelijk om alle gedetailleerde principes te noemen, simpelweg omdat er teveel zijn. De gedetailleerde principes opgenomen in dit onderzoek zijn voortgekomen uit interviews met deskundigen op het gebied van security en uit relevante vakliteratuur. Indien nodig zal bij elk principe een korte toelichting worden gegeven. Indien een toelichting ontbreekt zal dit worden aangegeven met een '-'. Het principe beschrijft in voldoende mate de essentie en behoeft dan geen verdere toelichting.

De principes in de ordening van het GASSP is een compilatie van principes uit de volgende documenten waarbij enkele principes zijn herschreven:

- het GASSP. [Gassp,1999]
- het NIST. [Stoneburner,e.a, 2001]
- Capgemini. [Hofman en Elsinga, 2000]
- Burton Group. [Blum, 2005]

6.1.1 Pervasive principes

PV-1: Toekenning van verantwoordelijkheden.

Toekenning van verantwoordelijkheden worden duidelijk gedefinieerd, ondersteund en erkend.

Toelichting: rolverdeling, authorisatie niveaus van informatie, relaties van de partijen, processen, informatie moet duidelijk worden gedocumenteerd en worden erkend door alle partijen. Voor compliance, het naleven van gedragregels binnen een onderneming, speelt hierbij een grote rol.

PV-2: Need to know.

Het security beleid is gebaseerd op een need-to-know basis.

Toelichting: Personen met een ‘need to know’ moeten toegang hebben tot de toegepaste en beschikbare principes, regels en richtlijnen en mechanismen voor de beveiliging van informatie en informatiesystemen en moeten geïnformeerd worden over de mogelijk gevaren. Need to know wil zeggen dat alleen mensen toegang hebben die de juiste rechten hebben.

PV-3: Ethisch en wettelijk.

Security moet op een ethisch verantwoorde wijze en volgens naleving van de wet worden toegepast.

Toelichting: Individuele privacy moet worden gewaarborgd. Voorbeeld: een systeembeheerder moet toegang hebben tot privé informatie dan en slechts dan als er aanleiding toe is.

PV-4: Multidisciplinair.

Principes, regels, richtlijnen, standaarden en mechanismen voor de beveiliging van informatie en informatiesystemen moeten rekening houden met de viewpoints van alle betrokkenen.

Toelichting: Rekening houden met viewpoints betekent doen aan requirement engineering. Requirement engineering waarbij stake-holders betrokken worden tijdens het hele ontwerp/implementatie traject. Zie verklaring ‘Requirement Engineering’ in de Lijst van begrippen en terminologieën.

PV-5: Proportionaliteit.

Security controls moeten in verhouding staan t.o.v. de risico's.

Toelichting: Risico's zijn: modificatie, denial of use en onthulling. Waarde toekennen aan de informatie (niet meer beveiligen dan nodig is), risico analyse, kosten-baten analyse. Onnodig vermoeilijken -> risicomanagement. Met name genoemd in Wet Bescherming Persoonsgegevens (WBP). [Web-6]

PV-6: Integratie van principes.

Principes, regels, richtlijnen en standaarden moeten met elkaar worden gecoördineerd en geïntegreerd.

Toelichting: Dit voor een zo holistisch mogelijke benadering en het in lijn brengen met niet-security principes. Ook moet worden voldaan aan organisatie policies en procedures.

PV-7: Tijd.

Partijen met een toegekende verantwoordelijkheid moeten met tijd gebaseerde methoden werken.

Toelichting: Dit om poging tot inbraak en dreiging tegen te gaan en/of te voorkomen.
De te ondernemen stappen:

- log reviewers.
- loggen in het algemeen.
- wachtwoorden veranderen na bepaalde tijd procedures voor wat te doen bij…,
- procedures voor detectie waarbij een balans moeten worden gezocht tussen preventie, detectie en response.

PV-8: Evaluatie.

Risico's met betrekking tot informatie en informatiesystemen worden geëvalueerd op periodieke basis.

Toelichting: Continue verbeteren van processen en later eventueel groeien in bijvoorbeeld volwassenheidsmodellen voor security.
Enkele voorbeelden:

- Wezenlijke verandering aan het informatiesysteem. Bijvoorbeeld het uitbreiden of verwijderen van hardware.
- Wezenlijke verandering aan de informatie of de waarde ervan.
- Wezenlijke verandering in de technologie. Bijvoorbeeld revolutionaire uitvindingen.
- Wezenlijke verandering van bedreigingen of zwakheden.

- Wezenlijke verandering beschikbare safeguards.
- Wezenlijke verandering gebruikersprofielen.
- Wezenlijke verandering potentiële verlies van het systeem.
- Wezenlijke verandering organisatie/enterprise.
- Een voorafgestelde tijd is verlopen na de laatste evaluatie.

PV-9: Bedrijfsaandachtspunt.

Security is onderdeel van de bedrijfsvoering.

Toelichting: Security dient niet gezien te worden als een punt wat achteraf nog even gerealiseerd moet worden. Tijdens de bedrijfsvoering dient hier rekening mee te worden gehouden en security moet tijdens veranderingen worden meegenomen.

PV-10: Fysiek en logisch.

Fysieke beveiliging is net zo belangrijk als logische beveiliging.

Toelichting: Niet alleen dienen logische unieke gebruikersaccounts en wachtwoorden worden geïmplementeerd, ook fysieke identificatie als bedrijfspasjes moeten worden gebruikt. Tevens is het logisch beveiligen van bijvoorbeeld de serverruimte zinloos indien de fysieke beveiliging ontbreekt of wordt omzeild (blokje tussen de deur vanwege de warmte).

PV-11: Acceptatie van storingen.

Storingen moeten worden voorbereid en geaccepteerd, niet gevreesd.

Toelichting: Storingen zullen altijd voor blijven komen, ga hiervan uit en zorg voor goede voorbereidingen. Het is daarom zaak waakzaam te zijn en storingen te accepteren en niet te vrezen.

PV-12: Vertrouwen.

Vertrouw niet iedereen blind.

Toelichting: Niet iedereen is blind te vertrouwen, zelfs niet de eigen gebruikers. Interne controle en veiligheid zijn net zo belangrijk als controle op inbreuk van buiten de organisatie.

6.1.2 Breed functionele principes

BF-1: Security beleid.

Het security beleid ondersteunt en ontwikkelt regels, richtlijnen, standaarden en procedures.

Toelichting: Dit sturen kan alleen indien, verantwoordelijkheden, niveau van discretie, en hoeveel risico een individu of organisatie entiteit mag hebben, is gedaan.

BF-2: Educatie en bewustwording.

De gebruikers zijn bewust en op de hoogte van het security beleid en worden bijgeschoold bij alle relevante veranderingen daaraan.

Toelichting: Educatie bevat: standaarden, baselines, procedures, richtlijnen en verantwoordelijkheden, bijhorende maatregelen en consequenties van eventuele fouten. Bewustwording betekent het nut, de kracht en de moeite inzien en accepteren van een degelijk security beleid en security systeem.

BF-3: Accountabiliteit.

De gebruikers zijn ten alle tijden verantwoordelijk voor hun toegang en gebruik van informatiesystemen en informatie.

Toelichting: Het moet mogelijk zijn om de datum, tijd en verantwoordelijkheid op het niveau van een individu vast te leggen voor alle belangrijke gebeurtenissen (toevoegingen, modificaties, kopieën, verwijderingen).

BF-4: Informatiemanagement.

Van informatie wordt periodiek (routinematig) het niveau, sensitiviteit en kritiekheid bekeken en opgeslagen.

Toelichting: Informatie verandert. Zowel qua inhoud alsook sensitiviteit en kritiekheid. Bijhouden en bijwerken hiervan is een must.

BF-5: Informatie attributen.

Informatie wordt opgeslagen met toevoeging van attributen.

Toelichting:-
Deze attributen zijn als volgt:

- Identiteit.
- Eigenaar.
- Voogdij.
- Inhoud.
- Waarde (in geld).
- Sensitiviteit (confidentialiteit).
- Kritiekheid (beschikbaarheid, integriteit).

BF-6: Omgevingsmanagement.

Interne en externe bedreigingen worden onderzocht rekening houdend met de fysieke omgeving waar de informatie en de ondersteunende infrastructurele bronnen worden opgeslagen, verstuurd en gebruikt.

Toelichting: Analyse van alle invloedrijke bedreigingen uit de gebieden waaruit de dreigingen komen (zie paragraaf 3.4). Omgevingsmanagement is veelal onderdeel van het risicomanagement.

BF-7: Gekwalificeerd controlepersoneel.

Er is controle op de kwalificaties, integriteit, need-to-know en de technische competenties van alle partijen die toegang hebben tot informatie en ondersteunende technologieën.

Toelichting: Er moet personeel zijn met als hoofdtaak het controleren van kwalificaties, integriteit, need-to-know en de technische competenties. Deze moeten voldoende middelen en macht krijgen om op passende wijze te kunnen optreden. Uit dit principe volgt direct principe GP-28.

BF-8: Systeem integriteit.

Alle eigenschappen van systemen en applicaties die essentieel zijn voor de missie van de organisatie worden gewaarborgd.

Toelichting:-

BF-9: Informatiesysteem levenscyclus.

Security wordt gewaarborgd gedurende alle stadia in de systeem levenscyclus.

Toelichting: Levenscyclus bestaat uit: architectuur, ontwerp/ontwikkeling/acquisitie, implementatie, operationeel onderhoud, afstoting.

BF-10: Toegangcontrole.

Er zijn passende controle/methode/middelen om de toegang tot informatie in balans te houden.

Toelichting: Nauw verboden aan Pervasive principe nummer 5 (PV-5).

BF-11: Relevantie met waarde asset.

Beveiligingsmaatregelen zijn relevant en in verhouding met de waarde van het te beveiligen asset.

Toelichting: Niet alleen de fysieke waarde van het te beveiligen asset is hier van belang, ook de waarde van eventuele indirecte gevolgen van verlies van het asset. Denk hierbij aan contractbreuk, klantverlies, vertrouwens-breuk, etc.

BF-12: Netwerk en infrastructuur security.

De potentiële impact op de gedeelde globale infrastructuur, internet, publiekelijk verbonden netwerken en andere verbonden systemen bij de implementatie van netwerk security maatregelen is bekend.

Toelichting: heeft overeenkomsten met BF-2.

BF-13: Wettelijk.

Wettelijke regels en contractuele requirements van security zijn leidend.

Toelichting: Er wordt voldaan aan wettelijk geldende normen zowel binnen de onderneming alsook binnen cultu-rele, geografische ligging.

BF-14: Ethische onderdelen.

De rechten en waardigheden van werknemers worden gerespecteerd bij het opstellen van het beleid en bij de selectie, implementatie en naleving van beveiligingsmaatregelen.

Toelichting:-

BF-15: Het netwerk is een slagveld.

Het netwerk is een militaire arena.

Toelichting: Militaire concepten worden toegepast om de assets te beveiligingen. Voorbeelden zijn: diepteverdediging, waarschuwingssysteem, misleiding, camouflage, terugvechten. De verantwoordelijke teamleider gebruikt het netwerk als een diagram op dezelfde wijze als generaals hun landkaarten gebruiken.

BF-16: Veiligheidsniveaus.

De veiligheidsituatie wordt dynamisch weergegeven door veiligheidsniveaus.

Toelichting: Als voorbeeld kan gedacht worden aan het systeem dat gebruikt wordt door NORAD [Web-7]. NORAD onderscheidt een vijftal condities om het huidige veiligheidsniveau aan te geven waarbij 5 vrede en 1 oorlog betekent.

6.1.3 Gedetailleerde principes

Wanneer is een principe nu een gedetailleerd principe?
Gedetailleerde security principes gaan over methoden of creëren compliance met de breed functionele principes in een bestaande omgeving en beschikbare technologie. Deze principes formuleren het inhoudelijke gestel waarmee een architectuurraamwerk gevuld kan worden. Er zullen dus gedetailleerde principes zijn die direct afgeleid kunnen worden van pervasive en breedfunctionele principes. Principes waarvan meteen duidelijk is van welk bovenliggend principe (PV of BF) ze afstammen. Van andere gedetailleerde principes is niet meteen duidelijk bij welk bovenliggend principe ze horen of waar ze aan gerelateerd zijn. Daarnaast zijn er legio losse kreten die niet voldoende concreet zijn geformuleerd om bestempeld te kunnen worden als goede principes. Het is zaak om dit in harmonie te doen met het concipiëren van een architectuur en de invulling van het Rijsenbrij-Framework.

GP-1: Security beleid.

Security dient als basis voor design.

Toelichting: In het security beleid worden de security doelen opgenomen die het systeem moet ondersteunen. Deze doelen sturen de procedures, standaarden en controls. [Hofman, 2004]

GP-2: Duidelijke grenzen.

Fysieke en logische grenzen zijn vastgesteld in het security beleid.

Toelichting: Soms is een grens gedefinieerd door mensen, informatie en informatietechnologie op één fysieke locatie. Echter in de realiteit kan het voorkomen dat er op een en dezelfde locatie meerdere security policies van kracht zijn zoals publiekelijke informatie en betrouwbare informatie.
Soms is een grens gedefinieerd door een security policy die beschikt over een specifieke set van informatie en informatietechnologie die een fysieke grens kan overschrijden. Denk hierbij aan een enkele machine of server waarin zowel publiekelijke alsook betrouwbare informatie is opgeslagen. Er kunnen dus meerdere security policies worden toegepast op een machine binnen een systeem. Bij het ontwerp van het informatiesysteem moet over security grenzen worden nagedacht en gecommuniceerd in relevante systeem documentatie en security policy

GP-3: Gereduceerd risico.

Bekende risico's worden tot een acceptabel niveau gereduceerd.

Toelichting: Dit principe is vaak onderdeel van het risicomanagement. Aan het vaststellen van een acceptabel niveau gaat vaak een kosten/baten analyse aan vooraf.

GP-4: Diepteverdediging.

Security is opgebouwd uit verschillende lagen van protectie.

Toelichting: Essentieel bij diepteverdediging is dat er security mechanismen zijn die andere security mechanismen beschermen en security mechanismen die op verschillende plaatsen (onafhankelijk van elkaar) geïmplementeerd zijn om een object te beschermen.

GP-5: Systeem van meetwaarden.

Een specifiek op maat gemaakt systeem van meetwaarden wordt gebruikt om organisatorische security doelen meetbaar te maken.

Toelichting:-

GP-6: Eenvoud bij opstellen.

Principes en maatregelen zijn opgesteld om begrijpbaar te zijn voor een breed publiek.

Toelichting: Hoe complexer het systeem hoe meer risico op exploits en hoe meer onderhoud nodig is.

GP-7: Eenvoud bij gebruik.

Principes en maatregelen spelen in op maximale intellectuele zelfontplooiing van gebruikers.

Toelichting: Principes en maatregelen werken gebruikers niet tegen en zijn verfijnd afgesteld om tegemoet te komen aan de wensen/eisen van de gebruikers. Indien principes en maatregelen de gebruikers tegenwerken bestaat de kans dat gebruikers maatregelen gaan omzeilen wat onveiligheid van het systeem tot gevolg heeft.

GP-8: Limiteer kwetsbaarheid.

Het systeem is opgesteld om kwetsbaarheid te limiteren en resistent te zijn tegen uitval (non-response).

Toelichting: Informatie systemen moeten bestand zijn tegen aanvallen, schade beperkt houden en snel herstellen als er toch aanvallen plaatsvinden. Het principe zegt iets over de erkenning van adequate beveiligingstechnieken op alle niveaus om potentiële aanvallen te weerstaan. Er zijn echter zwakheden die niet verholpen kunnen worden, die nog niet verholpen zijn, die nog simpelweg niet bekend zijn en die we simpelweg niet willen verhelpen (operationele mogelijkheden te vergroten).

Wat een bedrijf moet hebben zijn detectie – reactie mogelijkheden, het managen van 'points of failure' en een reportage strategie.

GP-9: Minimaal aantal te vertrouwen elementen.

Het systeem bevat een minimaal aantal te vertrouwen elementen.

Toelichting: Een voorbeeld in de engineering wereld is kern gebaseerd ontwerp. De kern is klein en veilig. Een fysiek voorbeeld is: weinig administrators die wachtwoorden kennen en hoe minder te beveiligen elementen hoe veiliger en makkelijker systeem te onderhouden is.

GP-10: Bekende en te verwachten dreigingen.

Maatregelen zijn genomen tegen bekende en te verwachten dreigingen.

Toelichting: Er zijn dreigingen die vooraf bekend zijn of die te verwachten zijn. Hou dit in de gaten en leg eventueel vast in procedures zodat hier goed mee omgegaan kan worden bij optreden. Dit komt terug in het risicomanagement. Zodra je weet waar je kwetsbaarheden liggen kun je daar extra aandacht aan besteden.

GP-11: Overlap van principes.

Principes dienen te zorgen voor overlap tussen informatiedomeinen.

Toelichting: Er zijn informatiedomeinen waarbinnen dezelfde principes gelden. Dit dient consistent te worden vastgelegd zodat geen 'verschillende principes' ontstaan die hetzelfde doel voor ogen hebben maar anders worden geformuleerd.

GP-12: Publieke toegankelijkheid.

Kritieke resources en systemen zijn zowel fysiek alsook logisch geïsoleerd van publieke toegankelijkheid.

Toelichting: Geen aparte LAN's en infrastructuren voor verschillende security niveaus maar gedeelde publiekelijk toegankelijke infrastructuren met voldoende security . Een ander voorbeeld in de securitywereld is het Bell-la-padula model wat gebruik maakt van compartimenten wellicht. [Pfleeger en Pfleeger, 2002]

GP-13: Grensbewakingmechanismen.

Zowel fysieke als logische grenzen worden bewaakt.

Toelichting: Om de informatiestromen over de grenzen te controleren en te controleren welke gebruikersgroepen (en wellicht welke individuele gebruikers) met elkaar communiceren zijn grensbewakingmechanismen noodzaak.

GP-14: Open standaarden.

Waar mogelijk worden open standaarden gebruikt.

Toelichting: Open (geaccepteerde) standaarden hebben hun kracht in het gebruik bewezen. Een voorbeeld: men kiest voor een cryptografie methode die wereldwijd geaccepteerd wordt als ‘veilig’ in plaats van een eigen bedachte cryptografie methode. Tevens bieden open standaarden meer mogelijkheden voor portabiliteit en interoperabiliteit.

GP-15: Natuurlijke taal.

Eisen en wensen voor de security worden opgesteld in natuurlijke taal.

Toelichting: Natuurlijke taal zorgt ervoor dat iedereen de eisen en wensen van security kent en duidelijk kan maken. Vaak gaat het mis bij de communicatie tussen techneuten en niet-technische stake-holders omdat de techneuten zich uitdrukken in een taal die onbekend is voor de stake-holders (te technisch).

GP-16: Audit mechanismen.

Audit mechanism zijn aanwezig om niet-geautoriseerd gebruik te detecteren en incident onderzoek te ondersteunen.

Toelichting: Lijkt erg op grensoverschrijdende technieken. Wezenlijk verschil is dat grensoverschrijdende technieken alleen dienen als waarschuwing, detectie, waar audit mechanismen ook als vervolgstap kunnen worden ingezet.

GP-17: Innovatie.

Het beveiligingssysteem is in staat nieuwe adaptieve technologie toe te staan.

Toelichting: De missie en bedrijfsprocessen veranderen waardoor requirements en technische beveiligingsmethoden moeten worden geüpdated. IT-gevaren voor de missie en de business veranderen door tijd en ondergaan periodieke evaluatie. Dit hoort bij risicomanagement.

GP-18:Authentificatie en authorisatie van gebruikers en processen.

Authentificatie en authorisatie van gebruikers en processen om toegangscontrole te waarborgen wordt zowel binnen als buiten de domeinen toegepast.

Toelichting: Indien vaak om authentificatie wordt gevraagd volgt automatisch de afweging: 'hoe gebruiksvriendelijk wil je het hebben, tegenover welke mate van security'.
Identiteit van personen wordt vastgesteld op basis van [Web-8]:

- Iets wat je hebt. (Voorbeeld: gewone sleutel, airmilespas).
  Risico: (on)vrijwillige overdracht, kopiëren.
- Iets wat je weet (Voorbeeld: paswoord, PIN).
  Risico: afkijken, raden, beheer.
- Iets wat je bent. (Voorbeeld: vingerafdruk, irisscan, DNA).
  Risico false positives/negatives, privacy.

GP-19: Unieke identiteiten.

Er wordt gebruik gemaakt van unieke identiteiten.

Toelichting: Door gebruik van unieke identiteiten worden de volgende zaken gewaarborgd:

- Accountabiliteit en traceerbaarheid van een gebruiker of een proces.
- Mogelijkheid tot toekennen specifieke rechten van een gebruiker of een proces.
- Non-repudiation.
- Ondersteuning van toegangscontrole beslissingen.
- Vaststellen van de identiteit in een beveiligd communicatiepad.
- Niet-geautoriseerde gebruikers die zich voordoen als een geautoriseerde gebruiker.

GP-20: Privileges.

Implementeer zo min mogelijk privileges.

Toelichting: Niet meer autorisaties toestaan dan nodig is. Het beste is om zo min mogelijk mensen te hebben die toegang hebben tot kritieke functies. Best practise: liever meer administrators met minder privileges dan eentje met alle permissies. Geen super-user! Iemand heeft precies genoeg permissie om zijn/haar taken te vervullen.

GP-21: Onnodige mechanismen.

Implementeer geen onnodige security mechanismen.

Toelichting: Elk security mechanisme moet een security service of set van services ondersteunen en elke security service moet een of meer security doelen ondersteunen. Extra mechanismen zorgen voor onnodige complexiteit en zorgen voor potentiële zwakheden. Een voorbeeld is document-encryptie wat de toegangscontrole ondersteunt. Deze ondersteunt op haar beurt de doelen van confidentialiteit en integriteit door niet geautoriseerde toegang tot files te blokkeren. Als document-encryptie een nodig onderdeel is om de doelen te halen dan is het juist. Echter als de doelen worden behaald zonder dat document-encryptie nodig is, dan is het slechts onnodige complexiteit.

GP-22: Beveiligingsstadia van informatie.

Beveilig informatie als het wordt gemaakt, verstuurd en opgeslagen.

Toelichting: Niet alleen de opslag moet veilig zijn. Vaak wordt dit goed gedaan maar wordt het maken en het versturen van informatie ‘vergeten’.

GP-23: Rampen procedures.

Rampenprocedures zijn opgesteld om beschikbaarheid en continuïteit te waarborgen.

Toelichting: Komt terug in het risicomanagement.

GP-24: Buiten werking en verwijdering.

Security wordt ook gewaarborgd bij buiten werking stellen of verwijderen van een systeem.

Toelichting: Security speelt niet alleen een rol bij actieve en werkende systemen. Ook de security van buiten werking gestelde of verwijderde systemen moet worden gewaarborgd.

GP-25: Beveilig tegen alle bekende en te verwachten aanvallen.

Fouten en zwakheden zijn afgestemd op alle bekende en te verwachten aanvallen.

Toelichting: Je kunt je nooit voor de volle 100% beveiligen. Er zullen altijd nieuwe technieken en methoden worden ontwikkeld om systemen te breken. Echter uit het verleden opgedane kennis moet ter harte worden genomen en worden gebruikt. Men moet leren van fouten uit het verleden en aanpassingen verrichten zodat deze in de toekomst kunnen worden voorkomen.

GP-26: Training.

Ontwikkelaars en onderhoudsmensen van security systemen hebben trainingsmogelijkheden.

Toelichting: -

GP-27: Verdeel en heers.

De onderneming is opgedeeld in separate aandachtsgebieden.

Toelichting: Het beveiligingsprobleem op bedrijfsniveau wordt opgedeeld in domeinen. Een domein kan gebaseerd zijn op een aantal criteria zoals, platforms, organisatiegrenzen, geografische ligging, etc. De domeinen kunnen genest zijn waarbij elk domein zijn/haar eigen specifieke beveiligingsbeleid heeft en afgeleide procedures waarbij afgeleid wordt van de principes, regels, richtlijnen en procedures geconcipieerd op bedrijfsniveau.

GP-28: Controle en screening.

Controleer de controleurs en screening van nieuwe gebruikers.

Toelichting: Controleurs dienen geen alleenheersers te zijn. Hun bezigheden/bevoegdheden dienen ook te worden gecontroleerd. Tevens dienen nieuwe gebruikers (werknemers) gescreend te worden bij aanstelling en gebruik.

GP-29: Lijsten.

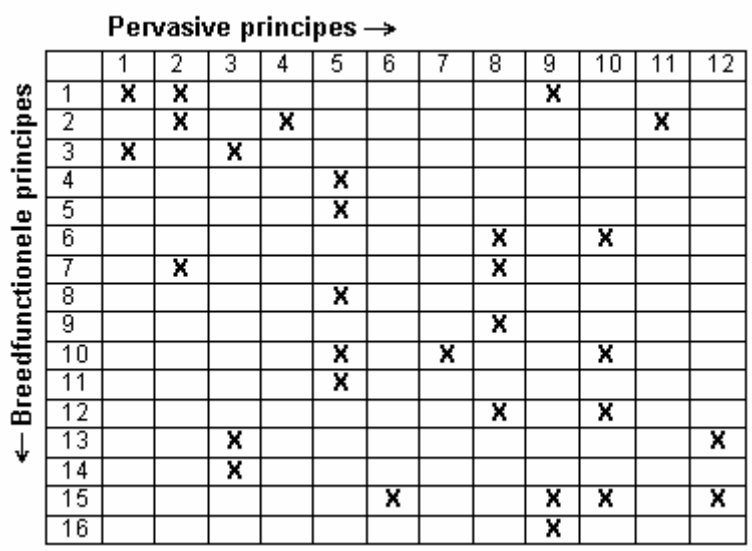
Gebruikers worden gegroepeerd opgenomen in lijsten en acties worden opgeslagen in logboeken.

Toelichting: Security werkt niet als de gebruikers van het eigen systeem niet te vertrouwen zijn. Het is nodig om alle gebruikers van het systeem te groeperen en in lijsten op te nemen. Er moet bekend zijn wie gebruik maakt van welke domeinen in het systeem. Dit heeft natuurlijk een impact op de beleving en privacy van de gebruikers, daar zij zich bewust zijn van het feit dat ze in een lijst worden opgenomen en hun acties worden opgeslagen.

6.2 Onderlinge relaties tussen principes

Een van de wensen is het inzichtelijk maken van relaties tussen principes: Welke principes zijn met welke andere principes gerelateerd (kruisreferentie).

De pervasive principes worden afgezet tegen de breedfunctionele principes (Figuur 18) en de breedfunctionele principes worden afgezet tegen de gedetailleerde principes (Figuur 19).



	1	2	3	4	5	6	7	8	9	10	11	12
1	X	X							X			
2		X		X							X	
3	X		X									
4					X							
5					X							
6								X		X		
7		X						X				
8					X							
9								X				
10					X		X			X		
11					X							
12								X		X		
13			X									X
14			X									
15						X			X	X		X
16									X			

Figuur 18: Pervasive principes afgezet tegen breedfunctionele principes

↓Gedetailleerde principes \ Breedfunctionele principes →	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	X															
2	X					X				X		X			X	
3						X					X					
4	X									X					X	
5	X															
6	X	X						X								
7										X				X		
8								X		X		X			X	
9								X							X	
10	X	X				X	X	X	X	X	X	X				X
11	X															
12	X					X	X	X	X	X	X	X			X	
13	X					X		X		X	X	X			X	X
14	X	X														
15	X												X			
16							X	X	X	X					X	
17		X				X	X								X	
18	X		X							X				X	X	
19	X	X	X	X	X					X					X	
20	X		X		X		X							X	X	
21						X				X						
22						X			X							
23	X					X						X			X	X
24	X								X							
25				X		X						X			X	X
26		X					X								X	
27			X	X	X	X	X	X	X						X	X
28		X	X				X			X			X	X	X	X
29		X	X				X						X	X	X	X

Figuur 19: Breedfunctionele principes afgezet tegen gedetailleerde principes

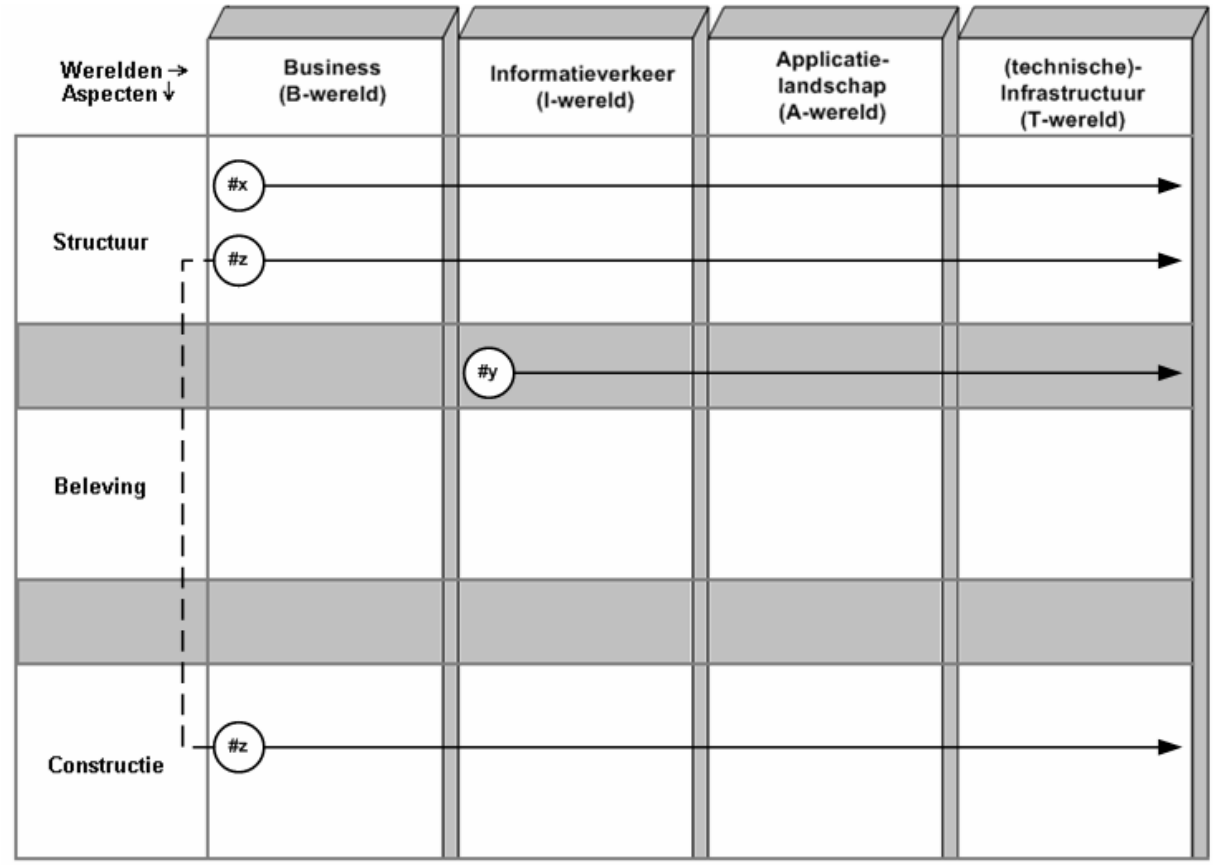
Het in kaart brengen van de relaties tussen principes zegt iets over de kwantitatieve relaties met andere principes. De tabel zegt niets over de mate waarin principes meer of minder belangrijk zouden zijn dan andere principes. Het kan niet worden gesteld dat een principe met bijvoorbeeld maar één relatie minder belangrijk zou zijn dan een principe met vijftien referenties. De mate van belangrijkheid kan alleen worden vastgesteld in een reële omgeving daar hier de bruikbaarheid en relevantie van een principe hier subjectief wordt gemaakt. De relevantie is ook hier ondernemingsuniek.

7 Security principes in het Rijsenbrij-Framework

In dit hoofdstuk worden de beschreven principes uit hoofdstuk 6 in het Rijsenbrij-Framework geplaatst. Om de overzichtelijkheid en leesbaarheid te waarborgen wordt gebruik gemaakt van een drietal aparte frameworks met daarin de principes op dezelfde wijze geordend als de gekozen ordening in hoofdstuk 6. Zo zijn de pervasive principes in het Rijsenbrij-Framework opgenomen in figuur 21, de breedfunctionele principes in figuur 22 en de gedetailleerde principes in figuur 23.

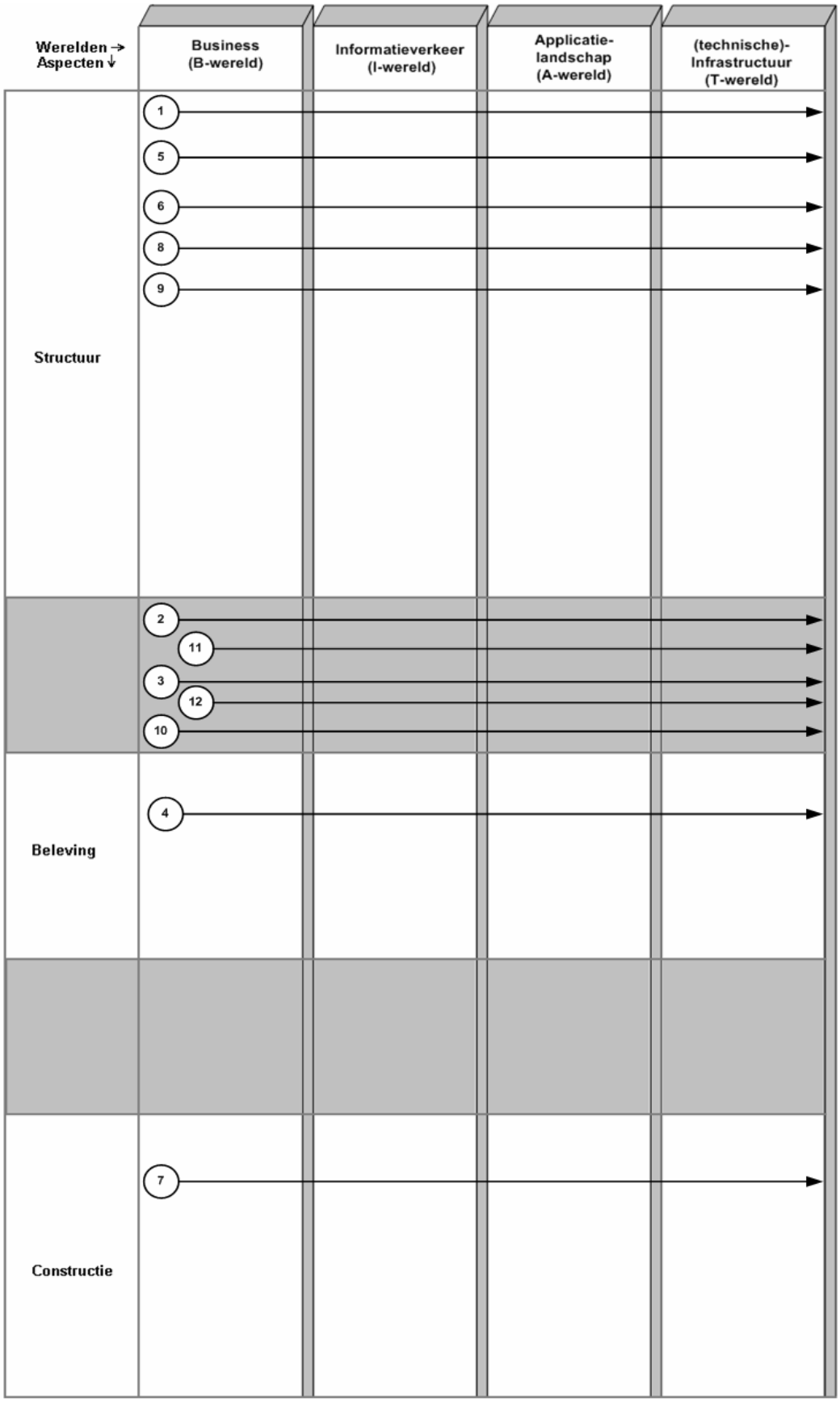
7.1 Hoe het framework te lezen?

In onderstaand framework (Figuur 20) zijn een drietal voorbeeld principes opgenomen te weten principe #x, #y en #z.
Principe #x speelt in op het architectuuraspect structuur, is in de B-wereld geconcipieerd en werkt door tot in de T-wereld.
Principe #y speelt in op de architectuuraspecten structuur **en** beleving (het grijze gebied), is in de I-wereld geconcipieerd en werkt door tot in de T-wereld.
Principe #z speelt in op de architectuuraspecten structuur **en** constructie, is in de BI-wereld geconcipieerd en werkt door tot in de T-wereld. Gekozen is voor een verbinding door middel van een stippellijn. Het is immers niet mogelijk gebruik te maken van het grijze grensvlak.



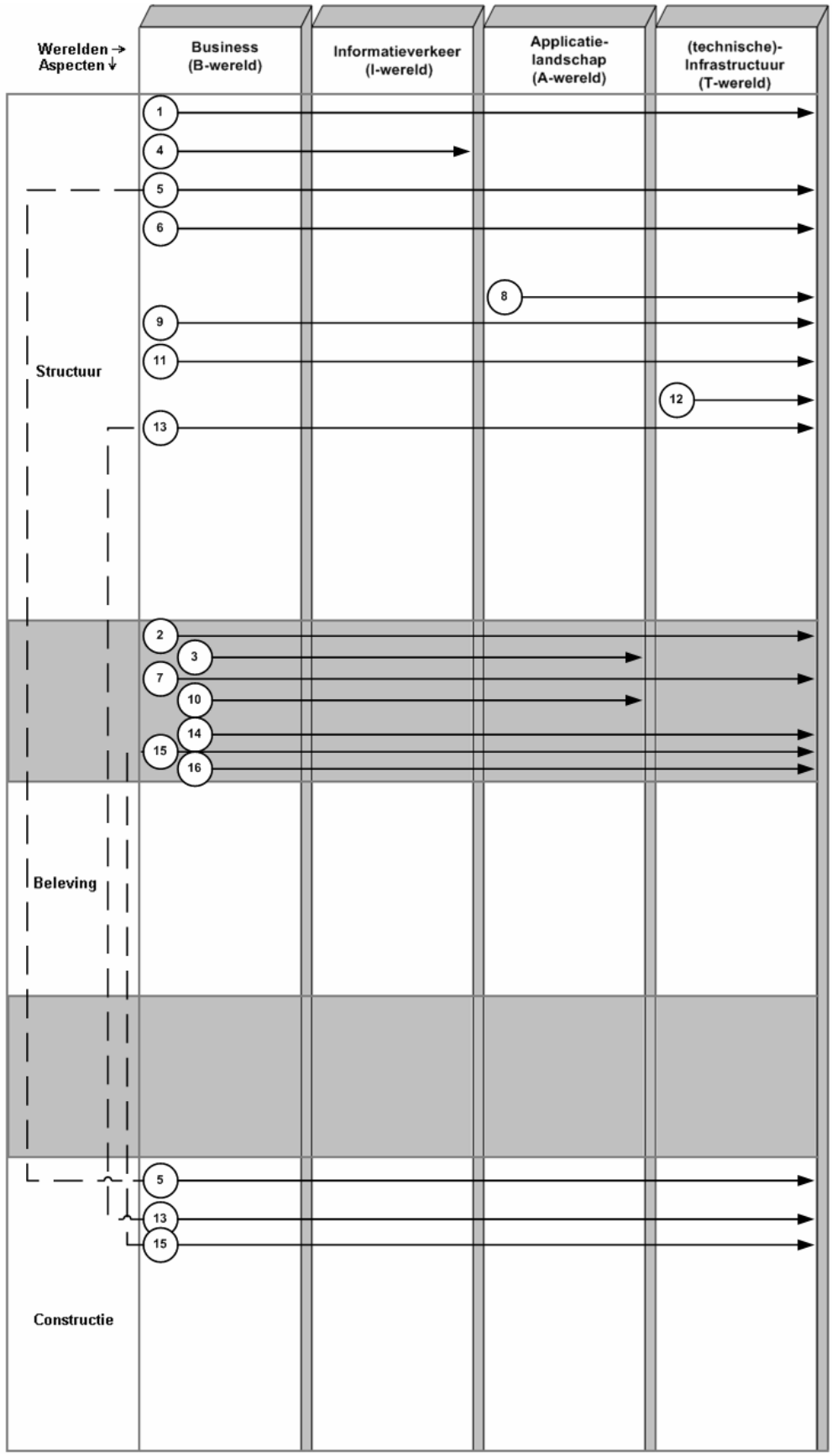
Figuur 20: Voorbeeld ingevuld framework

7.2 Pervasive principes in het Rijsenbrij-Framework



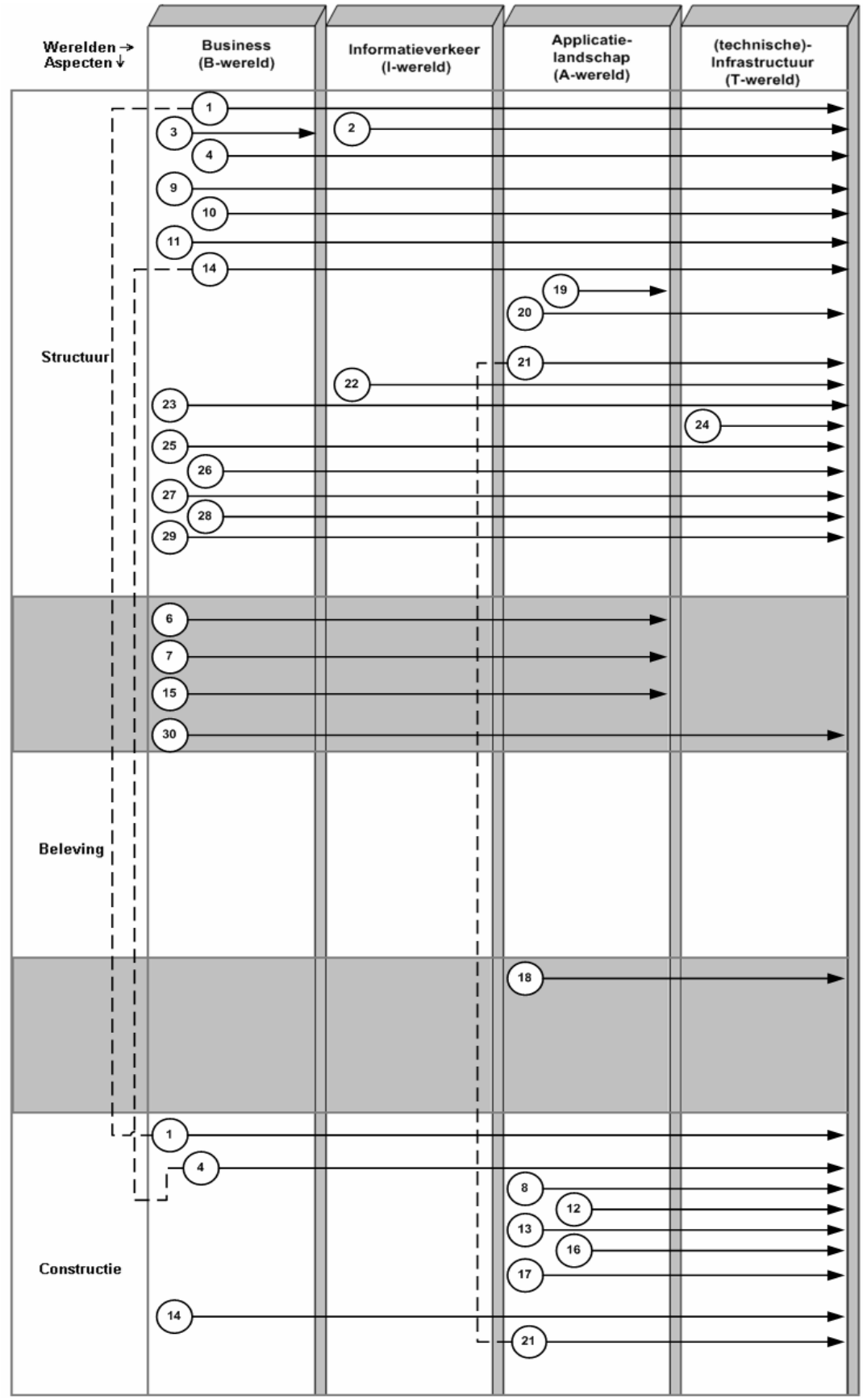
Figuur 21: Pervasive principes in het Rijsenbrij-Framework

7.3 Breedfunctionele principes in het Rijsenbrij-Framework



Figuur 22: Breedfunctionele principes in het Rijsenbrij-Framework

7.4 Gedetailleerde principes in het Rijsenbrij-Framework



Figuur 23: Gedetailleerde principes in het Rijsenbrij-Framework

8 Case studie: het UMC St. Radboud

Dit hoofdstuk dient als case studie om te kijken hoe het security beleid binnen een reële onderneming is geregeld. Er is gekeken of en zo ja hoe gebruik wordt gemaakt van security principes en welke concerns leiden tot principes en hoe dit is vastgelegd. In dit geval is gekozen voor het UMC St. Radboud, verder te noemen als UMC.

8.1 Definitie van security gehanteerd binnen het UMC

Het UMC definieert security als volgt:

> Informatiebeveiliging is het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen. [Steer, 2005]

Binnen het UMC wordt de term 'informatiebeveiliging' gehanteerd in tegenstelling tot de term 'security' die in dit onderzoek wordt gebruikt en de daarbij horende terminologieafbakening in paragraaf 3.3. Na overleg met het hoofd van security blijkt dat het UMC in feite dezelfde afbakening aanhangt en de keuze voor informatiebeveiliging voortkomt uit het idee dat alleen de informatie beveiligd moest worden. Hierbij wordt de fysieke beveiliging vergeten die direct invloed uitoefent op deze informatie.

Het informatiebeveiligingsbeleid is van toepassing op de drie kerntaken van het UMC namelijk patiëntenzorg, onderwijs en onderzoek en alle afgeleide ondersteunende diensten en richt zich op de eigen medewerkers, het tijdelijk personeel en op door derden ingezet personeel dat diensten verleend aan of betrekt van het UMC. [Steer, 2005]
De aandachtsgebieden waar het security beleid betrekking op heeft zijn expliciet benoemd. Hierdoor kan het security beleid in perspectief met de onderneming worden bezien. Zie paragraaf 3.8.

Binnen het UMC wordt de term 'principes' niet of nauwelijks gebruikt. Men spreekt daar over uitgangspunten voor beleid. Ook deze uitgangspunten hebben een voorschrijvend karakter en beperken de ontwerpruimte en dekken voor deze onderneming dezelfde lading als de term principes. Het moet worden opgemerkt dat terminologieën binnen ondernemingen erg kunnen verschillen maar dat in essentie het zelfde wordt bedoeld. Het is aan de onderzoeker om hier op de juiste manier mee om te gaan. Daarbij komt dat veel ondernemingen moeten voldoen aan (kwaliteits)normen die gelden binnen hun segment, geografische ligging, cultuur en overheidswetgeving. Het UMC dient aantoonbaar te voldoen aan de norm NEN7510 [Normcommissie, 2004] voor Informatiebeveiliging en de NEN 7512 [Normcommissie, 2005] voor de uitwisseling van gegevens. Dit zijn voorschriften, standaarden, regels en richtlijnen en komen voort uit principes die op hun beurt weer voortkomen uit concerns, zie paragraaf 4.1.

Voor dit onderzoek wordt aan de hand van beleidsdocumenten, interviews en common sense principes gedestilleerd. Van deze principes zal worden gekeken met welke principes uit hoofdstuk 6 ze overeenkomen. Het is niet de bedoeling van alle principes de regels, richtlijnen en standaarden te achterhalen. In dat geval zou deze case studie een stand alone opdracht worden waarvoor in dit onderzoek niet voldoende tijd is en waarbij een veel diepere kennis van het UMC benodigd is. Wat voor deze opdracht relevant is, is de herkenbaarheid van principes en de mate waarin het mogelijk is principes te achterhalen uit beleidsdocumenten en interviews.

8.2 Security principes binnen het UMC

Het destilleren van principes uit interviews en beleidsdocumenten binnen het UMC bleek een lastige aangelegenheid. Met name de gedetailleerde oplossingsgerichtheid van de beleidsdocumenten bemoeilijkt de overzichtelijke blik. Vaak zijn principes al geen principes meer, maar zijn ze door de bruikbaarheid en leesbaarheid te vergroten al verbijzonderd naar regels, richtlijnen en standaarden en zijn ze functioneel toegespitst op inhoudelijke zaken die spelen binnen de onderneming. Na nauwkeurige bestudering van beleidsdocumenten en het houden van interviews zijn de volgende principes gedestilleerd uit informatiebeveiliging beleidsdocumenten en interviews [Steer, 2005] en [Steer en Stroeken, 2005]:

Pervasive principes:

PV-1: Toekenning van verantwoordelijkheden worden duidelijk gedefinieerd, ondersteund en erkend.

PV-3: Informatie en de administratie van informatie alsmede de beveiliging moet op een ethisch verantwoorde wijze en volgens naleving van de wet worden toegepast.

PV-6: Principes, regels, richtlijnen en standaarden moeten met elkaar worden gecoördineerd en geïntegreerd.

PV-7: Partijen met een toegekende verantwoordelijkheid moeten met tijd gebaseerde methoden werken.

PV-8: Risico's met betrekking tot informatie en informatiesystemen worden geëvalueerd op periodieke basis.

PV-9: Security is onderdeel van de kernbedrijfsvoering.

PV-10: Fysieke beveiliging is net zo belangrijk als logische beveiliging.

Breedfunctionele principes:

BF-2: De gebruikers zijn bewust en op de hoogte van het security beleid en worden bijgeschoold bij alle relevante veranderingen daaraan.

BF-3: De gebruikers zijn ten alle tijden verantwoordelijk voor hun toegang en gebruik van informatiesystemen en informatie.

BF-4: Van informatie wordt periodiek (routinematig) het niveau, sensitiviteit en kritiekheid bekeken en opgeslagen.

BF-6: Interne en externe bedreigingen worden onderzocht rekening houdend met de fysieke omgeving waar de informatie en de ondersteunende infrastructurele bronnen worden opgeslagen, verstuurd en gebruikt.
BF-8: Alle eigenschappen van systemen en applicaties die essentieel zijn voor de missie van de organisatie worden gewaarborgd.
BF-9: Security wordt gewaarborgd gedurende alle stadia in de systeem levenscyclus.
BF-10: Er zijn passende controle/methode/middelen om de toegang tot informatie in balans te houden.
BF-11: Beveiligingsmaatregelen zijn relevant en in verhouding met de waarde van het te beveiligen asset.
BF-12: De potentiële impact op de gedeelde globale infrastructuur, internet, publiekelijk verbonden netwerken en andere verbonden systemen bij de implementatie van netwerk security maatregelen is bekend.
BF-16: De veiligheidsituatie wordt dynamisch weergegeven door veiligheidsniveaus.

Gedetailleerde principes:
GP-3: Bekende risico's worden tot een acceptabel niveau gereduceerd.
GP-7: Principes en maatregelen spelen in op maximale intellectuele zelfontplooiing van gebruikers.
GP-12: Kritieke resources en systemen zijn zowel fysiek alsook logisch geïsoleerd van publieke toegankelijkheid.
GP-16: Audit mechanism zijn aanwezig om niet-geautoriseerd gebruik te detecteren en incident onderzoek te ondersteunen.
GP-28: Controleer de controleurs en screening van nieuwe gebruikers.
GP-29: Gebruikers worden gegroepeerd opgenomen in lijsten en acties worden opgeslagen in logboeken.

9 Validatie

In dit hoofdstuk worden de gemaakte keuzen en genomen beslissingen toegelicht. Ook zal worden aangegeven hoe de kernhoofdstukken (5 en 6) zijn gevalideerd.

9.1 Manier van werken

Om het onderzoek op een voldoend wetenschappelijke manier te doorlopen is gebruik gemaakt van de opgedane kennis in de cursus 'Onderzoeksvaardigheden' van Dr. Erik Barendsen. [Web-9]
Kernpunten van deze cursus zijn het opstellen van een onderzoeksplan en de te kiezen onderzoeksmethode, de onderzoeksvragen die je wilt beantwoorden, hoe je de te raadplegen literatuur vindt en beoordeelt, hoe je zorgt dat wat je opschrijft controleerbaar is (geen gedragsfouten), je vakkundig blijft (geen strategiefouten), je logisch te werk gaat (geen redeneer fouten), je valide werkt (geen systematische fouten), je betrouwbaar werkt (toevalsfouten) en controleerbaar blijft. [Heinze & Markenhof, 2003] Tijdens het gehele traject is gepoogd de inhoud van onderzoeksvaardigheden te verenigen met het onderzoek.

9.2 Gemaakte keuzen

Er is gekozen voor de architectuur benadering van Rijsenbrij, de prescriptieve benadering. Een andere benadering zou de descriptieve benadering kunnen zijn geweest. Het essentiële verschil in deze twee benaderingen zit in het feit dat de prescriptieve benadering uitgaat van de vraagkant, terwijl de descriptieve benadering uitgaat van de mogelijke oplossing. De descriptieve benadering is dus een benadering vanuit engineering. Indien gekozen zou zijn voor de descriptieve benadering van architectuur had dit invloed gehad op de oplossingsgerichtheid van de resultaten. Architectuur is dan meer oplossingsgericht, terwijl voor dit onderzoek het voorschrijvende karakter meer aansluit daar het doel was security principes te achterhalen en op te stellen en geen security oplossingen te introduceren. Indien oplossingen waren vereist had wellicht een ISO standaard uitkomst geboden. ISO bevat namelijk standaarden die op hun beurt weer voortkomen uit concerns en principes. Principes zorgen er immers voor dat de volgende stap, de verbijzondering naar regels, richtlijnen en standaarden, mogelijk wordt. De volgende stap is invulling geven aan deze regels, richtlijnen en standaarden. Veel van deze invullingen zijn al beschikbaar in allerlei normeringen en zijn voor dit onderzoek niet relevant.

9.3 Genomen beslissingen

Samen met de begeleiders is besloten om niet alle gangbare raamwerken te gebruiken voor de positionering van de principes. Dit zou simpelweg teveel tijd hebben gekost. Ook is beslist om niet 'alle' gedetailleerde principes te achterhalen. Dit is een onmogelijke klus omdat gedetailleerde principes ondernemingsafhankelijk en dus subjectief zijn.

9.4 Selectie van literatuur

Tijdens de selectie van literatuur voor dit onderzoek is continu gewaakt voor wetenschappelijk verloedering. Deze verloedering is duidelijk voelbaar bij een medium als het Internet en dan met name bij populistische onderwerpen. Documenten lijken in eerste instantie bruikbaar waarna informatie als de bronvermelding, achtergrond van de auteurs, doelgroep en reden voor publicatie ontbreekt. Bij de gebruikte literatuur voor dit onderzoek is hier veel aandacht aan besteed en van alle wetenschappelijke artikelen zijn bronvermeldingen en referenties opgenomen.
Het vergaren van literatuur is gedaan door wetenschappelijke tijdschriften en vakbladen te raadplegen, op het Internet te zoeken, op advies van experts en door referenties van artikelen te raadplegen. Met name de adviezen van experts bleken erg relevante informatie op te leveren temeer doordat zij een grote kennisbron in de vorm van onderzoeksbureaus en expertgroepen ter beschikking hadden.

9.5 Validatie van kernhoofdstukken

De twee kernhoofdstukken van dit onderzoek, hoofdstukken 5 en 6, zijn ter validatie opgestuurd naar een expertgroep van het Genootschap voor Informatiebeveiliging (GvIB). [Web-10] Het contact met het GvIB is gelegd na deelname aan een Expertbrief-sessie met als titel '*Security Principes: Informatiebeveiliging op de managementagenda*'. Deze expertbrief is te vinden op de website van het GvIB [Web-10] op het speciaal voor deze expertbrief geopend forum. Alle opmerkingen van de expertgroep zijn besproken en indien nodig zijn er punten in de scriptie aangepast. Verder zijn er een aantal interviews afgenomen ter begripsvorming. Deze interviews zijn afgenomen bij security experts en architecten bij verschillende ondermeningen, o.a: Security experts en architecten bij Capgemini[7], Interaccess[8], PriceWaterhouseCoopers[9] en bij het UMC St. Radboud[10].

[7] www.capgemini.com
[8] www.interaccess.nl
[9] www.pwc.nl
[10] www.umcn.nl

10 Conclusie

In dit hoofdstuk wordt antwoord gegeven op de hoofdvraag, bijhorende deelvragen en subdeelvragen. Tevens wordt een conclusie gegeven over het onderzoek en zullen aanbevelingen worden aangedragen welke nuttig zijn ter uitbreiding en verdieping voor eventueel vervolg onderzoek.

10.1 Antwoord op de vragen

Allereerst zal antwoord gegeven worden op de deelvragen en subdeelvragen om op die manier te komen tot een antwoord op de hoofdvraag.

Deelvraag 1: Hoe worden security principes geordend?
• Onderzoek naar welke security aspecten er zijn. • Hoe zijn de gevonden aspecten onder te verdelen (aandachtsgebied of niveau, etc). • Is er een (klein) overkoepelend aantal (6 tot 8??) principes, waaraan de overige gerelateerd kunnen worden.

Vanuit het oogpunt om de security van informatie te waarborgen zijn de aspecten beschikbaarheid, integriteit en vertrouwelijkheid leidend. Voor evaluatie en beoordeling van de security van de gehele informatievoorziening worden bovengenoemde aspecten vaak uitgebreid met compliance, effectiviteit, efficiëntie en betrouwbaarheid van informatie.
Het apart onderverdelen van aspecten ligt niet voor de hand. Immers security principes worden opgesteld met het doel om aan deze aspecten te voldoen! Ze staan niet los van elkaar maar dienen elkanders bruikbaarheid. De ordening, gekozen voor dit onderzoek bestaat uit de GASSP-ordening die bestaat uit pervasive principes, breedfunctionele principes en gedetailleerde principes. Alle drie de leidende aspecten hebben betrekking op alle drie de ordeningen. Er is geen overkoepelend aantal principes aan te duiden dat algemeen geldend als ‘de belangrijkste’ geldt en daarmee belangrijker zou zijn dan de principes in andere ordeningen. Wel is aangetoond met behulp van de kruisreferentie-tabel in paragraaf 6.2 dat principes aan elkaar kunnen worden gerelateerd waarbij de pervasive principes de basiselementen zijn voor de breedfunctionele- en gedetailleerde principes.

Deelvraag 2: Wat is de werking van security principes?
• Onderzoek naar de invloed van de security principes op een architectuur. • In welke aandachtsgebieden en op welke momenten zijn ze van invloed op het werk van de architect.

Door de security principes te positioneren in het Rijsenbrij-Framework is de overeenkomst aangetoond tussen security en architectuur en vooral de bruikbaarheid van architectuurraamwerken om met security principes om te gaan. Security principes hebben hetzelfde doel voor ogen als architectuur principes, namelijk het reduceren van complexiteit en aan aanbrengen van structuur, waardoor ze op

dezelfde wijze te hanteren zijn binnen een architectuur. Net als 'gewone' architectuur principes ontstaan principes vanuit concerns in één van de vier werelden hebben ze daarin een bepaalde reikwijdte hebben. Het verschil met 'gewone' architectuur principes zit hem in de acceptatie. Generally accepted of universally accepted (zie paragraaf 6.1). Over veel security principes zijn de meningen van experts nog verdeeld en de lijst van algemeen geldende en geaccepteerde principes is klein. Wellicht heeft dit te maken met de leeftijd van het vakgebied (informatietechnologie is nog geen 60 jaar oud) en de daarbij komende noodzaak om aan security te doen. Aan de andere kant kan het zijn dat er simpelweg niet meer algemeen geldende geaccepteerde principes zijn en dat men te pietluttig opzoek is naar 'de beste manier van beveiligen'.

Deelvraag 3: Hoe worden security principes gekozen?
• Onderzoek op basis van welke criteria een keuze uit security principes gemaakt kan worden. • Onderzoek welke criteria daar een rol bij spelen. Expliciet dient daarbij aandacht besteed te worden aan de relatie met maturity models, organisatiecultuur en de invloed van compliance.

De literatuur biedt geen methodiek of stappenplan dat beschrijft welke principes je als onderneming wel of niet moet hanteren. Dit is niet bijzonder verassend daar de implementatie van een security beleid erg ondernemingsafhankelijk is gezien de vele mogelijke uitwerkingen en invullingen die gegeven kunnen worden aan principes. Er is niet een ideale weg die leidt naar een veilig systeem.
Om te ondervinden hoe een reële onderneming security principes formuleert is voor het beantwoorden van deze vraag een case studie uitgevoerd van het UMC St. Radboud. Hieruit is gebleken dat de keuze van security principes voortkomt uit concerns die zijn vastgelegd in beleidsdocumenten. Dit gebeurt echter nog veel te vaak op een ad-hoc manier. Binnen het UMC wordt security nog altijd gezien als 'iets' van de IT in plaats van 'het' van de gehele onderneming. Er is nog te weinig commitment van het management om een daadkrachtig, consistent en coherent security beleid te vormen. Wel wordt hier op het moment van schrijven hard aan gewerkt en langzaam maar zeker wordt de noodzaak tot het integraal toepassen van security binnen architectuur duidelijk. Dit blijkt uit recente inspanningen van Koninklijk Nederlandsche Maatschappij tot bevordering der Geneeskunst[11] (KNMG) in samenwerking Nederlands Normalisatie-Instituut om informatiebeveiliging in de zorg te normaliseren en te standaardiseren door middel van normen als de NEN7510 [Normcommissie, 2004] en de NEN7512 [Normcommissie, 2005].

Hoofdvraag:
Welke zijn de belangrijkste aandachtsgebieden en aspecten van security en hoe worden deze geformuleerd in principes en kunnen deze worden geïntegreerd in een enterprise architectuur?

Aandachtsgebieden zijn ondernemingsafhankelijk. Er zijn dus geen algemeen geldende 'belangrijkste' aandachtsgebieden te definiëren. De security aspecten beschikbaarheid, integriteit en vertrouwelijkheid zijn de aspecten die gewaarborgd dienen te worden binnen de aandachtsgebieden. Deze aspec-

[11] www.knmg.nl

ten komen tot uitdrukking in een aantal principes. Bij het opstellen van een enterprise architectuur dient vanaf het begin met deze principes rekening te worden gehouden daar deze net als architectuur principes toepasbaar zijn op de gehele onderneming en werkzaam zijn in alle vier de werelden van architectuur. Door te kijken naar de positionering van de security principes in het Rijsenbrij-Framework kan, indien bekend is welke overige architectuur principes er zijn, gekeken worden hoe/waar de principes met elkaar interacteren zodat hierop een strategie tot afstemming kan worden bepaald.

10.2 Conclusie en aanbevelingen algemeen

De moeilijkheid bij het opstellen van security principes zit niet in het achterhalen en opstellen van de principes zelf. De moeilijkheid is het uitzoeken of alle principes ook echt principes zijn, of ze relevant zijn maar **vooral** om duidelijk te krijgen met welke terminologieën je te maken hebt en hoe die terminologieën met elkaar in relatie staan.
Hier is binnen de expertwerelden van security en architectuur nog weinig tot geen aandacht aan besteed. Het uiteindelijke product van beiden, dat zou moeten leiden tot een geïntegreerde aanpak van security binnen het opstellen van een enterprise architectuur, bestaat daarom vaak uit een lappendeken aan oplossingen.
Security wordt vanuit bedrijfsoptiek (lees: management) nog te vaak gezien als een vervelend aanhangsel waarin de overheersende oplossingen aangedragen worden door de engineering hoek en dus technisch van aard zijn. Men spreekt graag over beperkingen van techniek bij het falen van security. Edoch waar het eigenlijk aan schort is, bewustwording en acceptatie van security als bedrijfsaandachtspunt waarbij pervasive principes leidraad dienen te zijn voor een veilig systeem. Vrijwel overal worden beschikbaarheid, integriteit en vertrouwelijkheid aangewezen als de belangrijkste aspecten die geborgd moeten worden, edoch worden deze te weinig en te ongestructureerd vastgelegd in beleidsdocumenten waarbij de overgang naar duidelijke security principes al helemaal ontbreekt. Hierin speelt de toewijding van het management een grote rol. Een degelijk security beleid dient een top-down proces te zijn waarbij concerns omgezet worden in principes die verbijzonderd kunnen worden naar regels, richtlijnen, standaarden en procedures. Dit proces is weliswaar opgang gebracht en grote ondernemingen geven aan deze aanpak steeds meer aandacht wat blijkt uit de vele interviews met experts. Echter voordat we kunnen spreken van een volledige integratie van het security beleid tijdens de ontwikkeling van enterprise architecturen is er nog heel wat werk te doen. Zo moet allereerst duidelijk zijn voor alle partijen waarover wordt gesproken. Een coherent en consistent gebruik van termen is een absolute must. Met deze overeenstemming van termen dient bewustwording zich aan. Zonder bewustwording en compliance van de noodzaak en bereidheid kan niet worden gestart.
In dit onderzoek is gekeken welke security principes er zijn en hoe deze passen in het opstellen van een enterprise architectuur, echter is niet onderzocht hoe security principes interacteren met architectuur principes. Eventueel vervolgonderzoek kan dus gaan over hoe security principes in relatie staan met architectuur principes. Verder is het mogelijk om de security principes uit dit onderzoek te positioneren in andere raamwerken dan alleen het Rijsenbrij-Framework.

Appendix A: Reflectie

De colleges ‘digitale architectuur’ aan de Radboud Universiteit zetten mij er toe aan kritisch te kijken naar digitale architectuur heden ten dage. Met name dat architectuur zorgt dat de informatievoorziening van een organisatie transparant wordt gehouden, onafhankelijk van de automatiseringsgraad en zo goed mogelijk aansluit aan de wensen van diegenen die in de gecreëerde wereld ‘leven’, spreekt mij enorm aan. Het niet vastzitten aan een technologie, maar juist in essentie werk verrichten dat voor mensen voelbaar en tastbaar is, wordt in de veelal technische studies naar mijn mening onderbelicht.
Vrijwel parallel aan de colleges van Prof. Daan Rijsenbrij besteedde ik aandacht aan de colleges ‘Information Security’ van Dr. Martijn Oostdijk. Hierin werd mij duidelijk dat security niet alleen tot uitdrukking komt op infrastructuur- en applicatieniveau maar dat de grote beslissingen op enterprise niveau worden genomen. Een securitybeleid is niet het installeren van een firewall en/of het toepassen van gebruikersaccounts en wachtwoorden. Security moet net als architectuur van ‘boven af’ worden opgelegd waarbij bewustwording en beleving van de eindgebruikers zwaar meetelt. Security moet ervoor zorgen dat de bedrijfsdoelstellingen kunnen worden behaald en veilig worden gesteld en heeft dus een bedrijfsstrategisch karakter waarbij de kernbeslissingen (wat wel en wat niet beveiligen) op strategisch niveau worden genomen. Het verbaasde mij dan ook dat, hoewel architectuur en security issues zijn op boardroom niveau, er niet op een samenhangende manier over wordt geredeneerd. Veel te vaak nog wordt security aan de architectuur gelijmd terwijl inbedding juist het doel zou moeten zijn. Het lijmen van verschillende securityoplossingen aan een bestaande architectuur zorgt voor een ongestructureerde lappendeken die onveiligheid in het leven roept. Gekeken naar het maatschappelijk belang, het ontbreken van gestructureerde aanpakken en mijn interesse in beide vakgebieden ben ik gekomen tot dit onderzoek.

Aan het begin van het onderzoek kwam ik erachter dat er veel definities zijn van digitale architectuur. Ik heb bewust gekozen om zoveel mogelijk definities te bekijken om uiteindelijk voor dit onderzoek de meest passende definitie te kunnen gebruiken. Hetzelfde heb ik gedaan voor begrippen binnen de wereld van security. Hieruit bleek dat ik een onaangetast en zeer interessant gebied had aangeboord. Zelfs na vele discussies en een expertbriefsessie met deskundigen op de gebieden architectuur en security, bleek dat de definities van gehanteerde termen vaak onduidelijk waren. Indien definities van termen wèl duidelijk waren ontbrak een heldere relatie met andere termen. Dit zette mij aan tot het concipiëren van een zo volledig en correct mogelijk Entiteit Relatie Diagram (ERD) waarin de voor dit onderzoek en de door mij gebruikte termen helder werden geoperationaliseerd en met elkaar in verband gebracht. Het ERD lijkt in eerste instantie een ‘een-van-de-velen-product’, edoch ben ik van mening dat dit ERD ontstaan is op basis van een goed totaalbeeld en inlevingsvermogen in de kernproblematiek. Het ERD biedt houvast om de vele terminologieën van beide vakgebieden te begrijpen, te combineren en vooral met elkaar in samenhang te brengen. De problematiek en complexiteit worden duidelijk en zoals later zal blijken is het ERD de voedingsbodem voor principes.

Evenwel gelijktijdig met het maken van het ERD ben ik opzoek gegaan naar algemeen geldende principes binnen de securitywereld. Dit bleek een hele kluif. De securitywereld lijkt nog steeds verdeeld

waarbij de bedenkers vaak niets anders zijn dan de uiteindelijke verantwoordelijken en de uitvoerders met wat lijkt de normaalste zaak van de wereld, de rol van de bedenkers en beslissers hebben overgenomen. Security wordt bestuurd, geleid, en geïmplementeerd vanuit de laagste niveaus binnen de onderneming waarbij systeembeheerders en engineers vrij spel hebben. De resultaten zijn vrijwel altijd oplossingsgericht zonder in achtneming van eventuele gevolgen. Gevolgen die overigens niet bij naam kunnen worden genoemd daar de complexiteit dermate groot is dat overzicht en inzicht onmogelijk wordt gemaakt. Is het management dan niet betrokken bij de security in hun onderneming? Betrokkenheid zal er wel zijn, maar aan eendracht, begrip en bewustwording schort het denk ik behoorlijk. Het resultaat is dat security een ondergeschoven bedrijfsissue blijft en de controle, uitvoer en implementatie aan lagere niveaus wordt overgelaten. Dit komt ook terug in de vele documenten over securityprincipes. De meeste van deze documenten beschrijven securityprincipes van een (software)product, technische infrastructuur of zelfs elementaire componenten van deze twee. Zijn deze principes dan niet bruikbaar of herleidbaar naar hogere denkniveaus en/of architectuurwerelden? In mijn onderzoek heb ik getracht dit te doen. Ik heb daarvoor gevonden principes vaak moeten herschrijven en/of zelf moeten formuleren. Een voorbeeld na aanleiding van een gesprek met een architect van een penitentiaire inrichting luidt als volgt: de regel was dat het aantal sleutels aanwezig binnen de inrichting niet méér mocht zijn dan strikt noodzakelijk. Vertaald naar digitale security betekent dit dat er niet meer unieke autorisaties mogen zijn dan strikt noodzakelijk. Deze vertaalslag heb ik dus met andere principes ook gedaan. Natuurlijk waren er ook documenten waarvan de bruikbaarheid meteen duidelijk was en de principes eruit zonder al teveel moeite konden worden gebruikt. Met name documenten die het resultaat waren van gemengde onderzoeksgroepen zoals het GASSP en de expertsessies bleken waardevol omdat daar al dieper zonder voorbedachte rade over was nagedacht in tegenstelling tot interne documenten van ondernemingen, die vooral oplossingsgericht en erg speciek voor de eigen onderneming zijn opgezet. Algemene gedachte erachter was dat onderzoeksgroepen en expertsessies meer geïnteresseerd zijn in het waarom dan in het hoe en dat is juist voor enterprise architectuur en dus ook voor security binnen enterprise architectuur van belang.

De contacten die ik heb gelegd waren van zeer grote waarde. Vrijwel iedereen die ik heb benaderd was zeer bereid te helpen en mee te denken. Dit gaf nogmaals de waarde en de noodzaak aan van mijn onderzoek. Vaak heb ik gepoogd een win-win situatie te creëren. Er zijn nu eenmaal zaken die aan bod komen die een onderneming niet zomaar openbaar wenst te maken. Het feit dat ik een opdracht deed in naam van de Radboud Universiteit liet deuren openen hetgeen waarschijnlijk niet het geval was geweest indien ik uit naam van een onderneming had gewerkt. Dit alles natuurlijk met het oog op concurrentievoordeel.

De relatie met de afstudeerbegeleider en de opdrachtgever is uitstekend verlopen wetende dat vooral de opdrachtgever (prof. dr. Rijsenbrij) te maken heeft met een strak tijdschema. De opdrachtgever heeft mij op enkele punten in het onderzoekstraject in contact gebracht met personen van zijn eigen kennisnetwerk. Hierdoor is niet alleen het speurwerk naar relevante personen sneller verlopen, ook de introductie en formele barrière werd aanzienlijk verkleind. Desalniettemin heb ik gepoogd zo objectief

mogelijk te blijven en heb ik zelf ook mensen buiten het netwerk van de opdrachtgever benaderd. Erg leerzaam vond ik de deelname aan het itSMF congres. [Web-11] Op dit congres waren veel mensen aanwezig die hun sporen op de gebieden van architectuur en security al hadden verdiend. Echter ook hier bleek veel inhoudelijke, detail en oplossingsgerichte principes te worden gebruikt terwijl de behoefte naar algemeen geldende principes steeds groter werd. De contacten die ik hier gelegd heb en de discussies die ik heb gevoerd bleken achteraf erg nuttig.

Wat is nu voor mij persoonlijk het resultaat van deze scriptie afgezien van het feit dat het ter afsluiting dient voor mijn studie Informatiekunde? Kan ik mezelf nu architect noemen? Het antwoord daarop is eenvoudig: Neen! Ik heb kennis genomen van de theoretische benadering van digitale architectuur en de ideeën en opvattingen van de professor die het vak geeft. Ik heb mogen proeven hoe architectuur in het bedrijfsleven is geïntegreerd en welke zaken er spelen. Ben ik dan security expert? Ook hier is het antwoord: Neen! Tijdens de cursus Information Security heb ik kennis genomen van enkele zaken die een onderneming en de bedrijfsvoering secure maken, maar ik ben nog niet in staat dat ook daadwerkelijk te implementeren. Ik ben meer bewust geworden van welke dreigingen en risico's er inspelen op een onderneming en welke middelen er zijn om je er tegen te wapenen. Wat kan ik mezelf dan wel noemen? Ik denk dat ik mezelf iemand mag noemen die erg actief, bewust, doeltreffend, gestructureerd en objectief kan kijken naar zaken die inspelen op de security binnen een onderneming vastgelegd in principes, regels, richtlijnen voortkomend uit concerns, inspelend op de structuur, constructie en beleving. Iets minder vaag: ik weet welke zaken vastgelegd moeten worden in principes, in harmonie met architectuur, zodat security op bedrijfsniveau kan worden gewaarborgd.
Ik denk dat ik met deze scriptie een succesvolle poging heb gedaan om de problematiek en integratie van de gebieden architectuur en security voelbaar en oplosbaar te maken. Dit onderwerp staat echter nog in de kinderschoenen en zal in de toekomst onderhevig zijn aan vele aanpassingen. Ik hoop dat het entiteit relatiediagram (Hoofdstuk 5, Figuur 16), waarmee de kernbegrippen en hun relaties met elkaar zijn vastgelegd, meer houvast biedt bij het discussiëren, achterhalen, opstellen en implementeren van security principes en dat de geboden ordening en invulling van principes leidraad mag zijn naar een meer secure onderneming. Tevens hoop ik dat ik met de plaatsing van principes in het Rijsenbrij-Framework, de kracht en overeenkomst aangetoond heb indien security met digitale architectuur wordt verenigd.
Al met al kijk ik terug op een leerzame en zeer interessante periode waarin ik veel diverse kennis en vaardigheden heb opgedaan. Met name de volledige controle en mogelijkheid tot zelfinvulling van de te bewandelen weg is mij zeer positief bevallen. De combinatie van security en architectuur is erg boeiend veelzijdig en zeer nuttig. Ik hoop dan ook in het arbeidsproces hier nog mijn aandacht en energie aan mag besteden.

Lijst van figuren

Lijst van begrippen en terminologieën

Aandachtsgebied	Binnen organisaties in z'n geheel alsook binnendomeinen en sub-domeinen van organisaties kunnen aandachtsgebieden worden onderkend. Een aandachtsgebied is een cluster van bedrijfsprocessen waar in dit onderzoeken men speciale aandacht moet besteden op het gebied van security.
Applicatie	Is een computerprogramma dat is bedoeld om door de gebruiker direct te worden gebruikt. Dit in tegenstelling tot een server-taak of andere taken die door een besturingssysteem in de achtergrond worden uitgevoerd.
Aspect	Binnen de context van security zijn er drie aspecten te beschouwen: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV, of CIA Confidentiality, Integrity en Availability, in het Engels). De aspecten zeggen iets over waar binnen het aandachtsgebied aan moet worden voldaan.
Asset	Alle bezittingen van een onderneming die commerciële en verhandelbare waarde hebben. Voor dit onderzoek en dit ERD beperkt dit zich tot (te beveiligen) elektronische data dat van waarde is voor de onderneming.
Authentificatie	Controleer wie je tegenover je hebt: "wie ben jij?"
Autorisatie	Controleer wat diegene mag: "wat ga jij daar doen?"
Boardroom	Het management van een onderneming. Fysiek: de kamer waar het management bijeenkomt.
Coherent	Met ordelijke samenhang.
Compliance	Het naleven van gedragregels binnen een onderneming.

Concern	De zorg van de belanghebbende die voortkomt uit hun verantwoordelijkheden of belangen. Concerns hebben te maken met de ontwikkeling, werking, voortbestaan of andere aspecten van een systeem die belangrijk zijn voor één of meerdere stake-holders. Concerns omvatten systeemeigenschappen als prestaties, betrouwbaarheid, beveiliging, verspreidbaarheid en ontwikkelbaarheid.
Consistent	Vrij van innerlijke tegenspraak.
Cryptografie	Cryptografie houdt zich bezig met technieken voor het zodanig versleutelen van te verzenden informatie, dat het voor een cryptoanalist, een persoon die toegang heeft tot het kanaal tussen zender en ontvanger, en dus als het ware 'mee kan luisteren', onmogelijk is om tegen aanvaardbare inspanning uit de getransporteerde data af te leiden welke informatie er door de zender was verzonden.
Digitale Architectuur	Architectuur is een coherente, consistente verzameling principes, verbijzonderd naar uitgangspunten, regels, richtlijnen en standaarden –soms vastgelegd in paterns- die beschrijft hoe een onderneming, de informatievoorziening, een informatiesysteem of infrastructuur is vormgegeven en zich voordoet in het gebruik.
Dreiging	Kan met een bepaalde waarschijnlijkheid gebeuren en heeft impact op de (bedrijfs)doelstellingen.
Enterprise Architectuur	Enterprise architectuur dient om kaders te geven op enterprise niveau (het hoogste niveau) die leidend zijn voor alle onderliggende niveaus, zoals domeinen, informatiesystemen en digitale werkruimtes. Enterprise architectuur leidt tot een high-level ontwerp van de onderneming in zijn totaliteit. Het doel is een eerste indeling in domeinen bestaande uit bedrijfsprocessen, applicaties en de onderliggende technische infrastructuur. Een enterprise architectuur heeft meerdere gebruiksdoeleinden: atlas voor het topmanagement, beheersing van complexiteit, kaderzetting voor realisatie en communicatiemiddel. Het atlasaspect van de enterprise architectuur wordt gestalte gegeven door een verdeling van de onderneming in een aantal redelijk autonome domeinen. Hoofddomeinen zijn vaak: deli-

	very, marketing & sales, leveranciers & inkoop. Ondersteunende domeinen beslaan zaken als personeel, informatie, organisatie, financiën en huisvesting.
Exploit	Vaak gebruikte term in de computer security wereld om aan stukje software aan te duiden dat voordeel haalt uit een foutje of een zwakheid in het systeem.
Firewall	Een veiligheidsvoorziening die probeert te voorkomen dat onbevoegden toegang krijgen tot het interne netwerk (LAN) of uw eigen PC. Een internetgebruiker die een firewall heeft geïnstalleerd kan wel toegang krijgen tot het internet, maar er kan slechts beperkt verkeer binnenkomen.
Informatiesysteem	Een georganiseerde combinatie van mensen, hardware, software, communicatienetwerken en gegevensbronnen , die informatie verzamelt, verwerkt en verspreidt binnen een organisatie.
ICT	Informatie Communicatie Technologie.
ISO	De International Organization for Standardization (ISO) is een internationale organisatie die normen vaststelt. De organisatie is een samenwerkingsverband van nationale standaardisatieorganisaties in 148 landen.
IT	Informatie Technologie.
LAN	Local Area Network.
Logische beveiliging	Beveiliging op bit-niveau met behulp cryptografische technieken.
Maatregel	Handeling waardoor men iets regelt.
Non-repudiation	Onweerlegbaarheid.

Onderneming	Een doelgericht samenwerkingsverband van mensen.
Requirement Engineering	Requirement engineering beschrijft alle taken die te maken hebben met het in kaart brengen van de scope van een project waarbij het vergaren, analyseren, definiëren en rapporteren van een nieuw te bouwen of aan te passen (computer) systeem het doel is. Requirement engineering is een belangrijk deel van het ontwerpproces waarbij de wensen/eisen van de gebruiker centraal staan en waarbij de gebruiker direct bij het ontwerpproces wordt betrokken.
Risico	Gevolg van een dreiging. Betekenis van risico heeft dan ook een toevoeging op de betekenis van een dreiging en wel als volgt: Kan met een bepaalde waarschijnlijkheid gebeuren heeft een **negatieve** impact op het bereiken van (bedrijfs) doelstellingen en de continuïteit van bedrijfsvoering.
Risicomanagement	Risicomanagement is het identificeren en kwantificeren van risico's (bijvoorbeeld in een project) en het vaststellen van beheersmaatregelen. Met beheersmaatregelen worden activiteiten bedoeld waarmee de kans van optreden of de gevolgen van risico's worden beïnvloed.
Security principe	Principes zijn richtinggevende uitspraken ten behoeve van essentiële beslissingen, een fundamenteel idee bedoeld om een algemene eis te vervullen. Principes beïnvloeden direct de wijze waarop de IT zal worden ingezet. Foute principes kunnen desastreus zijn bij transformaties. Principes dienen te worden geconcretiseerd naar zaken die moeten, dat zijn de regels en standaarden, en zaken die verstandig zijn: de richtlijnen, ook wel ‘best practices’ genoemd.
Schade	Het financiële verlies (waarde van het bijbehorende asset + indirecte gevolgen die het verlies van het asset met zich mee brengt) dat het gevolg kan zijn van een dreiging.
Stake-holder	Een persoon die enig belang heeft bij het artefact waarvoor een architectuur wordt opgesteld dan wel een security beschouwing wordt gedaan.

View	Een view is een onderwerp binnen security. Vanuit de relevante concerns kan inhoudelijk invulling worden gegeven aan views. Niet alle onderwerpen zijn voor iedere stake-holder belangrijk. Een view wordt gemaakt om deze aan een specifieke groep stake-holders te kunnen presenteren. Door deze selectie van onderwerpen wordt voorkomen dat ze door de bomen het bos niet meer zien.
Viewpoint	Een viewpoint is een view vanuit het oogpunt van een stake-holder. Voorbeeld: een brandweerman kijkt op een andere manier naar de veiligheid van een gebouw dan een inbraakpreventiedeskundige en hebben beide andere belangen, terwijl ze beide kijken naar de veiligheid van het zelfde gebouw.

Literatuurlijst

AIV, 1999	Th.J.G. Derksen, *AIV Informatiekunde voor het HBO,* 5e druk, Uitgeverij: Academic Service, 1999.
Blum, 2005	Dan Blum*, Security and Risk Management Strategies Reference Architecture Principles*, Burton Group, januari 2005.
Burke en Scholtz, 2004	Brian Burke en Tom Scholtz, *Aligning Information Security Architecture With Enterprise Architecture,* Meta Practice 2262, MetaGroup, oktober 2004.
Cohen, 2005	Fred Cohen, *Security and Risk Management Strategies Reference Architecture Principles,* Burton Group, 2005.
Conference Presentatie, 1999	GartnerGroup, *European Information Security Conference*, 1999.
Gassp, 1999	International Information Security Foundation, *GASSP (Generally Accepted System Security Principles)*, juni 1999.
Hofman, 2004	Aaldert Hofman, *Inbouwen in plaats van aanbouwen,* Artikel in het tijd-schrift 'Informatiebeveiliging', mei 2004.
Hofman en Elsinga, 2000	Ben Elsinga, Aaldert Hofman, *Security Principles,* pattern paper ingestuurd voor EuroPlop 2003.
IS-Governance, 2005	Board Briefing, *Information security governance,* LogicaCMG.
Lankhorst, e.a, 2005	M. Lankhorst, e.a, *Enterprise Architecture at Work*, Uitgeverij: Springer, 2005.
Leeuw, 1996	A.C.J. de Leeuw, *Bedrijfskundige methodologie, management van onder-zoek,* Uitgeverij: van Gorcum, 1996.

Normcommissie, 2004	Normcommissie 303 001, *NEN 7510 Informatiebeveiliging in de zorg – Algemeen*, april 2004.
Normcommissie, 2005	Normcommissie 303 001, *NEN 7512 Medische informatica – Informatiebeveiliging in de zorg – Toetsbaar voorschrift bij NEN 7510 voor complexe organisaties,* mei 2005.
Oost en Markenhof, 2003	Heinze Oost en Angela Markenhof, *Een onderzoek voorbereiden,* Uitgever: HBuitgevers, 2003.
Overbeek en Sipman, 1999	Paul Overbeek, Wim Sipman, *Informatiebeveiliging,* 2e druk, Uitgever: Tutein Nolthenius, september 1999.
Pfleeger en Pfleeger, 2002	Charles P. Pfleeger, Shari Lawrence Pfleeger, *Security in Computing,* Uitgeverij: Prentice Hall PTR, december 2002.
Rijsenbrij, 2002	Daan Rijsenbrij, Jaap Schekkerman, Harry Hendrickx, *Architectuur, besturingsinstrument voor adaptieve organisatie*, Lemma, 2002.
Rijsenbrij, 2003	Daan Rijsenbrij, *Studiehandleiding bij de cursus Digitale Architectuur*, Radboud Universiteit Nijmegen, 2003. (www.digital-architecture.net/collegedictaat.htm)
Rijsenbrij, 2006	Daan Rijsenbrij, *Kanttekeningen bij'Architectuur in de Digitale Wereld'(versie nulpuntzes)*, oktober 2005. (www.digital-architecture.net)
Rijsenbrij, 2006	Daan Rijsenbij, *Sheets bij de cursus Digitale Architectuur,* Radboud Universiteit Nijmegen, 2006. (www.digital-architecture.net/collegedictaat.htm)
Schumacher, 2003	M. Schumacher, *Foundations of Security Patterns*, uit Security Engineering with Patterns, Springer-Verlag, 2003.

Snel, 2005	Bert Snel, *Informatie Beveiliging Opzet & Bewustzijn,* Siemens whitepaper, juni 2005.
Steen, e.a, 2005	M.W.A. Steen, M.M. Lankhorst, H. ter Doest, P. Strating, M. –E.lacob, *Service-Oriented Enterprise Architecture* en Hoofdstuk 7 van Z. Stojanovic en A. Dahanayake uit *Service-Oriented Software System Engineering: Challenges and Practices,* IDEA Group, 2005.
Steer, 2005	Berrie Steer, *Beleidsnota informatiebeveiliging UMC St Radboud Beveiliging van informatie,* mei 2005.
Steer en Stroeken, 2005	Berrie Steer, Jan Stroeken, *Informatiebeveiligingsbeleid,* mei 2005.
Stoneburner,e.a, 2001	Gary Stoneburner, Clark Hayden, Alexis Feringa*, Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* NIST Special Publication 800-27 Rev A.
Verschuren en Doorewaard, 2000	Piet Verschuren, Hans Doorewaard, *Het ontwerpen van een onderzoek,* derde druk, Uitgeverij: Lemma, 2000.

Internet locaties

Web-1	http://www.student.ru.nl/l.bongers/
Web-2	http://www.rvcomp.com/wiring/EIA/glossary.htm
Web-3	http://www.garlic.com/~lynn/secgloss.htm
Web-4	http://www.nap.edu/books/0309055970/html/88.html
Web-5	http://home.hetnet.nl/~daan.rijsenbrij/uvacap/alignment/chapter7.htm

Web-6	http://www.justitie.nl/themas/meer/
Web-7	http://en.wikipedia.org/wiki/NORAD
Web-8	http://www.cs.ru.nl/~bart/TALKS
Web-9	http://www.niii.ru.nl/home/Erik.Barendsen/onderwijs/ onderzoeksvaardig-heden/
Web-10	http://www.gvib.nl/
Web-11	http://www.itsmf.nl/
IEEE	http://standards.ieee.org/

Overige literatuur en websites

Sietse Overbeek, Sergej van Middendorp en Daan Rijsenbrij, Tijdschrift Informatie en Architectuur, Artikel:*De Digitale Werkruimte, een nieuw architectuurartefact*, juni 2005.
US National Security Agency, *Defense in Depth*, juni 2001.
Lex Borger, *Presentatie Security Architectuur Principes.*
Bruce Schneier, *Modeling security threats*, in Dr. Dobbs Journal, december 1999.
Carl E. Landwehr, *Computer Security*, Springer-Verlag, juli 2001.
Ruben Melaard, *Ondernemingstypering uit architectuurcontext*, Scriptie Digitale Architectuur, augustus 2005.

Ron van Nuland, *Architectuurprincipes van de Radboud Universiteit*, Scriptie Digitale Architectuur, augustus 2005.

Tom Scholtz, F. Christian Byrnes, Jay Heiser, *Establish an Effective Information Security Program,Part 1: Structure and Content*, Gartner, 2005.

L.C.M. van Knoppen, *Ontwikkeling van een security architectuur voor de Haagse Hogeschool gebruik makend van TOGAF*, Tias Business School Eindhoven, 2005.

Website Daan Rijsenbrij, http://www.digital-architecture.net/