

Over Rechtsbescherming en Informatiebeveiling

Maurice Gittens <maurice at gittens dot nl>

20 januari 2004

Samenvatting

Voorwaarde bij de handhaving van het recht in de Nederlandse rechtsstaat is dat overheidsinstellingen bij de uitvoering van de taken waaraan deze instellingen hun bestaansrecht ontleen, geldende wet en regelgeving in acht nemen. Als verantwoordelijkheid van overheidsinstellingen geldt tevens dat deze instellingen dienen te waarborgen dat hun taakstelling niet anders dan van rechtswege is te ontregelen. Beide genoemde verantwoordelijkheden van overheidsinstellingen worden in dit document samengevoegd onder de noemer *rechtsbescherming*. Op basis van in het Nederlandse rechtssysteem bestaande rechtsconcepten wordt in dit document een invalshoek voor de informatiebeveiling gepresenteerd dat als doel heeft een bijdrage te leveren aan de rechtsbescherming bij (overheids)instellingen.

Auteursrechten van dit document zijn eigendom van de Maurice Gittens.

Status: Pril Concept

1 Inleiding

In een fundamentele zin is een belangrijke verantwoordelijkheid van een rechtstaat het beschermen van het recht. Dit volgt direct uit het gegeven dat in het geval van een rechtsstaat, zelfbehoud en rechtsbescherming synoniem zijn. Volgt deze stellingname niet direct uit het antwoord op een vraag als:

Is niet iedere rechtsstaat verantwoordelijk voor de bescherming van de rechten van haar constituenten?

En volgt niet uit de taak de rechten van constituenten met bestendigheid te beschermen dat een rechtsstaat ook zijn eigen bestaan dient te bestendigen?

Over het algemeen geldt dat de rechtstaat der Nederlanden ons als Nederlanders een dierbaar goed is. Onze rechtsstaat waarborgt de rechtszekerheden die ten grondslag liggen aan de vrijheden die we doorgaans als vanzelfsprekend zien. Het in stand houden van de deugden van onze rechtstaat wordt in dit document gezien als een doel dat in het algemeen mag worden nagestreefd. In dit document worden de volgende stellingen geponeerd:

- De rechtsbeschermingsmiddelen voor onze rechtstaat in de digitale tijdperk dienen de rechtsbeschermingsmiddelen die ten grondslag liggen aan ons bestaand rechtssysteem te weerspiegelen.
- Bij het instandhouden van het recht in de digitale tijdperk is de informatiebeveiliging onontbeerlijk

Het doel van dit document is de onderbouwing van deze stellingen.

2 Het rechtssysteem als sjabloon voor de inrichting van de informatiebeveiliging

Overheidsinstellingen zijn van rechtswege belast met de uitvoering van een overheidsdienst. Deze overheidsdiensten behelzen de effectuering van geldende wet- en regelgeving in een bepaald domein. Voorbeelden van de overheidsdiensten waar in deze op bedoeld wordt zijn het onderwijs, de sociale zekerheid en de rechtszekerheid. Het uitvoeren van deze diensten is dan ook een hoofdtaak van deze organisaties. Krachtens de algemene rechtsbeschermde taak van onze rechtstaat zijn overheidsinstellingen gehouden zich te onderwerpen aan algemeen geldende wet en regelgeving zoals bijvoorbeeld de Wet Bescherming Persoonsgegevens (WBP) en de Archief Wet die de rechtsbescherming van constituenten op respectievelijke deelgebieden waarborgen. In dit document wordt de informatiebeveiliging gezien als een middel dat in essentie op twee manieren door overheidsinstellingen kan worden ingezet:

- t.b.v. effectueren van de wet en regelgeving dat gekoppeld is aan de taak dat bestaansrecht geeft aan de betreffende overheidsdienst (b.v het voorkomen van fraude of andere vormen van afbreuk bij sociale zekerheidsinstellingen)
- Het in acht nemen van algemeen geldende wet en regelgeving zoals de b.v. WBP.

Dus de informatiebeveiliging bij overheidsinstellingen heeft in het algemeen een wetshandhavende taak en een rechtsbeschermende taak. Door wetshandhaving als een vorm van rechtsbescherming te zien wordt gededuceerd dat de informatiebeveiliging bij overheidsinstellingen wordt ingezet ten behoeve van de rechtsbescherming. De grondslagen van de rechtsbescherming in de Nederlandse rechtstaat zullen in dit document als grondslagen van rechtsbescherming (en de dus informatiebeveiliging) bij overheidsinstellingen worden gepositioneerd. Deze rechtsbeschermende grondslagen passeren in deze paragraaf kort het revú.

In Nederland gelden voor alle juridische personen een aantal rechten zoals als deze bij wet zijn vastgelegd. Hierbij valt te denken aan:

- Het bestaansrecht
- Het eigendomsrecht
- Het privacy recht
- Etc.

Deze rechten belichamen een aantal vrijheden zoals deze voor Nederlandse juridische personen gelden in rechtstaat der Nederlanden. Om deze vrijheden te beschermen is het rechtssysteem in Nederland georganiseerd rond drie gescheiden machten; te weten de rechterlijke, wetgevende en uitvoerende machten. Het scheiden van deze machten binnen onze samenleving is een waarborg tegen willekeur en/of machtsmisbruik in verschillende aspecten van het recht binnen de rechtsstaat der Nederlanden. Het principe dat achter het scheiden van deze machten schuil gaat is in essentie een beginsel dat ook in andere delen van de wetenschap wordt toegepast. Men spreekt in de algemene wetenschap van het *orthogonaliseren van de primitieven*. Dit beginsel leidt in het verband van de inrichting van ons rechtssysteem tot een inrichting waarbij functionarissen die beslissen over rechtmatigheid geen invloed hebben op de rechtspraak of de effectuering van de rechtspraak. Terwijl functionarissen die rechtspreken geen invloed hebben op wat rechtmatig is een ook geen invloed hebben op de effectuering van het recht. Onverminderd geldt dan dat hij die de rechtspraak effectueert noch invloed heeft op wat rechtmatig is en noch invloed heeft op de rechtspraak.

In dit document wordt gesteld dat met het oog op de rechtsbeschermingstaak van de overheid en in het verlengde daarvan de rechtsbeschermingstaak van overheidsinstelling het principe van het orthogonaliseren van de primitieven van toepassing dient te zijn op de rechtsbescherming en dien ten gevolge ook op de informatiebeveiliging bij deze instellingen.

Uit de rechtsbeschermingsgrondslagen die voor de rechtsbescherming in Nederland zorgen kunnen bijvoorbeeld de volgende rechtsbeginselen gedestilleerd

- Juridische personen hebben van rechtswege identiteit en bestaansrecht
- Bevoegdheden worden door de wet toegekend en erkend
- Verantwoordelijkheden door de wet toegekend en erkend
- De wet bepaald hoe voor een bepaalde constellatie bevoegdheid aan verantwoordelijkheid gekoppeld is
- Het scheiden van machten (zoals wetgevende, rechterlijke en uitvoerende machten)
- etc.

Deze beginselen zullen in de in dit document voorgestelde informatiebeveiligingsmechanieken worden weerspiegeld. Deze beginselen geven in weze ook het antwoordt of de vraag hoe het recht met de informatiebeveiliging te beschermen.

Om een helder beeld te krijgen van de normen waaraan de rechtsbescherming en de informatiebeveiliging bij overheidsinstellingen dient te voldoen is in deze inleiding informatiebeveiliging bij de overheidsinstellingen geplaatst in een juridisch kader. In dit kader is het doel van de informatiebeveiliging bij overheidsinstellingen het beschermen van de rechten van de overheidsinstellingen en de bij haar bedrijfsprocessen betrokken juridische personen. Het juridische kader waarbinnen de informatiebeveiliging in deze geplaatst is een imperatief dat direct of indirect weerspiegelt zal worden in de architectuur, ontwerp en inrichting van de informatiebeveiliging bij deze overheidsinstellingen. Daar waar de fundamentele Nederlandse rechtsbeginselen van de Nederlandse rechtstaat niet in de inrichting van de informatiebeveiliging is terug te vinden is naar mening van de auteur een punt van zorg aan te wijzen.

3 Essentiële vragen bij het beveiligen

Wanneer er in een bepaalde context sprake is van beveiliging, is telkens het antwoord op de volgende vragen relevant.

1. Wat wordt er beveiligd of wat is het object dat beveiligd wordt?
2. Tegen wie wordt er beveiligd of wie is de vijand/bedreiger?
3. Tegen wat wordt er beveiligd; welke bedreigingen of risico's worden door de beveiliging gedekt?

Het antwoord op deze vragen identificeert per definitie het doel van het beveiligen. Vanuit juridisch perspectief is het doel van beveiliging telkens voorkomen van de schending van de rechten van constituenten van een rechtsstaat. Vanuit een algemeen beveiligingsperspectief is het doel van het beveiligen in alle gevallen het voorkomen van de compromittatie van de te beveiligen objecten, door een partij die de rol van vijand of bedreiger speelt, ongeacht de door deze gebruikte middelen. Het beperken van het discussiedomein tot het domein van de informatiebeveiliging doet niets af aan de geldigheid van het bovenstaande.

3.1 Wat wordt er beveiligd?

Waar er sprake is van beveiliging is er telkens direct of indirect ook sprake van eigendom en/of verantwoordelijk. Het recht om onze eigendommen en belangen te beschermen tegen onrechtmatige bedreigingen is in onze maatschappij dan ook een vanzelfsprekendheid. Minder vanzelfsprekend is de van rechtswege geldende plicht van juridische personen om er zorg voor te dragen dat de middelen waar zijn conform het recht eigenaar van zijn of verantwoordelijkheid voor dragen (b.v. door nalatigheid) gebruikt kunnen worden voor het schenden van rechten van derden. In de context van informatiebeveiliging is het te beveiligen object dan duidelijk de informatie dat conform het recht eigendom en/of verantwoordelijkheid is van een juridische partij (of juridische partijen). Ruimer gezien geldt in het geval van de informatiebeveiliging dat het te beveiligen object niet uitsluitend informatie is, maar ook de informatiesystemen die diensten aanbieden op basis van het de te beveiligen informatie. Dit geldt omdat de compromittatie van zulk een informatiesysteem tot de compromittatie van de te beveiligen informatie kan leiden.

Hierbij valt bijvoorbeeld te denken aan:

- Informatieverwerking processen
- Informatieverwerkingssystemen
- Transportsystemen voor informatie
- Opslagsystemen voor informatie

Invulling geven aan de informatiebeveiliging in een concern of overheidsinstelling impliceert de beveiliging van informatiesystemen en dus ook de beveiliging van de informatiediensten die door de informatiesystemen in kwestie worden gebruikt.

3.2 Tegen wie wordt er beveiligd?

In het algemeen bestaat voor ieder informatiedienst een verzameling bevoegde gebruikers. Deze verzameling bevoegde gebruikers zijn juridische personen die langs rechtsgeldige weg bevoegd zijn om gebruik te maken van de diensten van een informatiesysteem. Als functionaliteit van een informatiesysteem door anderen dan de aangewezen bevoegde gebruikers wordt benut, spreken we van onbevoegd gebruik van het informatiesysteem. Er is dan ook sprake van compromittatie van het betreffende informatiesysteem. Voorwaarde bij een juridisch verantwoorde inrichting van een informatiedienst is dus is alle gevallen dat er langs rechtsgeldige weg gespecificeerd dienen te zijn:

- Welke partijen bevoegde gebruikers zijn
- Aan welke rechtsgeldige gronden partijen hun status van bevoegd gebruiker ontleen

Deze informatie is noodzakelijk om in het algemeen te kunnen vaststellen wanneer er sprake is van bevoegd gebruik van een informatie systeem. De gronden op basis waarvan een partij een bevoegd gebruiker mag heten zullen in het algemeen bepalend zijn voor de rollen die deze gebruiker binnen een informatie systeem mag vervullen.

3.3 Tegen welke bedreigingen wordt er beveiligd?

Een informatiesysteem is in essentie op twee manieren door een onbevoegde te compromitteren, namelijk:

- Door de compromittatie van de identiteit van bevoegde gebruikers (dit kan ook als de betreffende gebruiker daar geen weet van heeft).
- Door de compromittatie van faciliterende diensten

Ter voorkoming van de compromittatie van de identiteit van bevoegde gebruikers dienen er faciliteiten voorhanden te zijn de het vastleggen van de authenticiteit van identiteit van een gebruiker op onweerlegbare wijze mogelijk maakt. Binnen de informatiebeveiliging bestaan er een aantal technische en procedurele maatregelen die bij de inrichting van zulk een faciliteit dienst kunnen doen.

Tevens geldt dat er in organisaties risicoprofielen voor applicaties, faciliterende diensten en opslagsystemen nodig zijn die in kaart brengen welke bedreigingen er onderkend worden voor de verschillende te beveiligen objecten. Op basis van de onderkende risico's wordt per applicatie, applicatieklasse en/of faciliterende dienst een gepast maatregelenpakket (Engels: containment profile of protection profile) geformuleerd dat het reduceren van de onderkende risico's tot doel heeft.

4 Over Risicoprofielen, risicobeperkingsprofielen, beveiligingsbarrières en placebo's

4.1 Introductie

Vanuit juridisch perspectief is de extensie van de vraag "Wat wordt er beveiligd?" in het algemeen een verzameling rechten door de rechtstaat aan een constituent zijn toegekend. Middels wet en regelgeving wordt door aangewezenen de rechten van alle constituenten gewaarborgd. Veel gewenste kenmerken van wet en regelgeving hebben een direct aanwijsbare tegenhanger in de informatiebeveiliging. In dit hoofdstuk gaat vanuit het perspectief van de informatiebeveiliging hier op in.

Vanuit het perspectief van de informatiebeveiliging is de extensie van de vraag: "Wat wordt er beveiligd?" is een verzameling objecten die te beveiligen zijn. Over het algemeen zijn de te beveiligen objecten een verzameling bedrijfsmiddelen die bij de bedrijfsvoering gebruikt worden; deze objecten worden in dit document eerste orde beveiligingsobjecten genoemd. De beveiliging van deze bedrijfsmiddelen is een verzameling technische en organisatorische maatregelen die de kans op compromittatie van deze bedrijfsmiddelen significant reduceren. In algemeen zijn deze bedrijfsmiddelen te associëren met één of meerdere informatiebeveiligingsdomeinen. Deze informatiebeveiligingsdomeinen die in deze onderscheiden worden zijn:

- * inter-company communicatie domein
- * concernapplicatie domein
- * concernnetwerk domein
- * concern gegevens banken domein

Het doel van de informatiebeveiliging is in het algemeen het voorkomen van onbevoegd gebruik van deze bedrijfsmiddelen en het minimaliseren van afbreukrisico's bij compromittatie van deze bedrijfsmiddelen.

Uitgaande van een risicoanalyse voor bedrijfsmiddelen (zoals concernapplicaties, concernnetwerken etc.) wordt voor bedrijfsmiddelen (of klasse van bedrijfsmiddelen) een risicoprofiel opgesteld. Een risicoprofiel wordt dan ook gedefinieerd als een verzameling kwetsbaarheden die volgen uit de inzet van (een) bepaalde (klasse) bedrijfsmiddelen. Een risicoprognose geeft inzicht in de waarschijnlijkheid dat een kwetsbaarheid (dat deel uit maakt van het risicoprofiel van een bedrijfsmiddel) daadwerkelijk geëxploiteerd zal worden. Op basis van risicoprofielen worden bijpassende maatregelen getroffen die tot doel hebben het minimaliseren van de in het risicoprofiel onderkende risico's. Deze maatregelen wordt in dit document een risicobeperkingsprofiel genoemd.

Anders gezegd: Een risicobeperkingsprofiel definieert een verzameling beveiligingsbarrières die gezamenlijk de risico's minimaliseren die in een risicoprofiel gedefinieerd zijn. Inzicht in risicoprognoses, de aard van beveiligingsbarrières en de gewenste kenmerken van deze beveiligingsbarrières wordt in deze gezien als een goed bruikbaar hulpmiddel bij de selectie van deze beveiligingsbarrières.

De mate waarin risicoprognoses consequenties hebben voor de samenstelling van risicobeperkingsprofielen is sterk afhankelijk van het binnen een organisatie gevoerde informatiebeveiligingsbeleid.

4.2 Kenmerken van risicobeperkingsprofielen en beveiligingsbarrières

Bij het ontwerpen van risicobeperkingsprofielen zijn, in het algemeen, twee aspecten van beveiligingsbarrières van kritisch belang voor de kwaliteit van de risicodekking van risicobeperkingsprofielen. Deze aspecten zijn respectievelijk het risicodekkingsprofiel en het kwetsbaarheidsprofiel van beveiligingsbarrières.

Het risicodekkingsprofiel van een beveiligingsbarrière is dat deel van een risicoprofiel dat door de betreffende beveiligingsbarrière wordt gedekt. M.a.w. een risicodekkingsprofiel van een beveiligingsbarrière verkleint een risico dat in een risicoprofiel gespecificeerd is. Het kwetsbaarheidsprofiel van een beveiligingsbarrière definieert een verzameling middelen waarmee de risicodekking van de betreffende beveiligingsbarrière gereduceerd kan worden.

Omdat een risicobeperkingsprofiel uit een verzameling beveiligingsbarrières bestaat geldt dat voor ieder risicobeperkingsprofiel ook een risicodekkingsprofiel en een kwetsbaarheidsprofiel te onderscheiden is.

4.2.1 Tweede orde beveiligingsobjecten

In een eerdere paragraaf zijn eerste orde beveiligingsobjecten gedefinieerd als de verzameling bedrijfsmiddelen die beveiligd worden. De onderkende risico's voor klassen van eerste orde beveiligingsobjecten zijn ondergebracht in risicoprofielen die eerste orde risicoprofielen genoemd worden. De onderkenning dat risicobeperkingsprofielen in het algemeen een bijbehorend kwetsbaarheidsprofiel hebben, heeft tot gevolg dat ook het kwetsbaarheidsprofiel van een risicobeperkingsprofiel een te beveiligen object is. Deze beveiligingsobjecten worden tweede orde beveiligingsobjecten genoemd. Een kwetsbaarheidsprofiel wordt in deze een tweede orde risicoprofiel genoemd. Het ligt voor de hand dat er langs analoge weg in het algemeen ook hogere (derde, vierde etc) orde beveiligingsobjecten en risicoprofielen te onderscheiden zijn. In dit document wordt hier niet verder op ingegaan.

4.2.2 Beveiligingsmaatregelen voor tweede orde beveiligingsobjecten.

Hogere orde risicoprofielen en risicobeperkingsprofielen In het algemeen worden risico's die in eerste orde risicoprofielen zijn onderkend middels eerste orde risicobeperkingsprofielen tot een aanvaardbaar niveau gereduceerd. Het is mogelijk om de volgende aanpak te volgen:

* voor tweede orde risicoprofielen definieert men tweede orde risicobeperkingsprofielen

* voor derde orde risicoprofielen definieert men derde orde risicobeperkingsprofielen

* etc.

Deze aanpak kan leiden tot complexe risicobeperkingsprofielen terwijl een hun effectiviteit niet optimaal is verleggen met de volgende opties.

Het gebruik van redundante risicodekkingsprofielen Een andere aanpak voor de beveiliging van tweede orde objecten is het samenstellen van de eerste orde risicobeperkingsprofielen op basis van beveiligingsbarrières die dezelfde risicodekking hebben terwijl hun kwetsbaarheidsprofielen disjunct en dus niet overlappend zijn. Het gebruik van redundantie is in deze tevens gewenst omdat de genoemde redundantie zogenaamde Single Points of Failure uitsluiten. Het gebruik van redundante risicodekkingsprofielen met disjuncte kwetsbaarheidsprofielen is uiterst effectief omdat volgens de elementaire statistiek de kans op compromittatie van het totale maatregelen pakken het product is van de kans op compromittatie van de individuele risicobeperkingsprofielen.

4.2.3 Wat zijn de gewenste kenmerken van deze beveiligingsbarrières?

In het volgende wordt ingegaan op een aantal kenmerken van beveiligingsbarrières die los van specifieke kwetsbaarheden gelden; te weten:

- * Orthogonaliteit
- * Genericiteit
- * Transparantie

Beveiligingsbarrières die voldoen aan de bovenstaande hebben beheersbare en inzichtelijke risicobeperkingsprofielen tot gevolg.

Orthogonaliteit of intransitiviteit De erkenning van het feit dat het plaatsen van verschillende beveiligingsbarrières slechts dan zin heeft als de compromittatie van de ene barrière niet de compromittatie van een andere barrière impliceert leidt tot de eerste gewenste kenmerk van beveiligingsbarrières. Beveiligingsbarrières moeten binnen een risicobeperkingsprofiel orthogonaal zijn. Een beveiligingsbarrière wordt als orthogonale barrière gezien (in een bepaald risicobeperkingsprofiel) als de compromittatie van deze barrière niet leidt tot de compromittatie van andere beveiligingsbarrières.

Anders geformuleerd: beveiligingsbarrières in een risicobeperkingsprofiel dienen intransitief te zijn voor compromittatie.

Genericiteit Beveiligingsbarrières die een grotere risicodekking hebben genieten in het algemeen de voorkeur boven beveiligingsbarrières met kleinere risicodekking. Dit geldt met name als het orthogonaliteitsbeginsel niet wordt aangetast.

Transparantie De transparantie van beveiligingsbarrières wordt in deze langs twee dimensies gezien.

- * doorzichtigheid van de beveiligingsmaatregelen
- * de mate waarin bestaande werkwijzen ontregeld worden (Engels: intrusive)

Analoog aan de transparantie die volgt uit de formulering van expliciete risicoprofielen en risicobeperkingsprofielen is het tevens wenselijk doorzichtigheid verhogende beveiligingsbarrières te prefereren boven in verhouding minder doorzichtige beveiligingsbarrières. Dit geldt met name als de orthogonaliteits- en genericiteitsbeginselen niet worden aangetast. Ook is het gewenst dat beveiligingsbarrières zo min mogelijk

bestaande werkwijzen en procedures ontregelen. Tevens zijn beveiligingsbarrières die in mindere mate bestaande werkwijzen ontregelen te prefereren boven beveiligingsbarrière die dat in meerdere mate doen.

4.2.4 Informatiebeveiligingsplacebo's

Beveiligingsplacebo's worden in deze gedefinieerd als beveiligingsmaatregelen die op andere gronden dan hun doeltreffendheid toegevoegd worden aan risicobeperkingsprofielen. In deze sectie worden twee beveiligingsplacebo's beschreven, namelijk de inzet van sommige vormen van geheimen en de inzet van het vertrouwen.

Wanneer zijn geheimen gewenst? Een geheim is informatie dat voor onbevoegden onbekend is. Op basis van geheimen kunnen zeer effectieve beveiligingsmaatregelen getroffen worden. Geheimen worden dan ook veelvuldig als beveiligingsmaatregel toegepast. Hierbij valt te denken aan: PIN-codes, passwords, cryptografische sleutels etc. De geschiedenis heeft uitgewezen dat de inzet van op geheimen gebaseerde beveiligingsbarrières ook zeer compromitterend kan zijn.

In de woorden van Whitfield Diffie:

It isn't that secrets are never needed in security. It's that they are never desirable. This has long been understood in cryptography, where the principle of openness was articulated as far back as the 1870s (though it took over a century to come to fruition). On the other hand, the weakness of secrecy as a security measure was painfully evident in World War II, when the combatants were highly successful at keeping knowledge of their cryptosystems out of general circulation but far less successful at keeping them from their enemies.

Geheimen vormen een bijzondere kwetsbaarheid omdat de compromittatie van een geheim vaak slechts door de compromittatie van het te beveiligen object gedetecteerd kan worden. Vaak kan door compromittatie van een geheim afbreuk zich lange tijd accumuleren zonder dat de afbreuk (als deze überhaupt geconstateerd wordt) tot het gecompromiteerd geheim herleid kan worden. Geheimen vormen een nog grotere kwetsbaarheid als deze geheimen niet eenvoudig veranderd kunnen worden. De lezer mag voor zichzelf scenario's voor de geest halen die dit feit zullen bevestigen. Het antwoord op de vraag die in de van deze paragraaf is gesteld mag de lezer zelf formuleren.

En hoe gaan we om met het vertrouwen? Vertrouwen bestaat als een relatie tussen partijen. Intrinsiek aan het vertrouwen en de bijbehorende vertrouwensrelaties is het feit dat het vertrouwen en dus vertrouwensrelaties geschaad kunnen worden. De op vertrouwensrelaties gebaseerde beveiligingsmaatregelen hebben in het algemeen dezelfde kwetsbaarheden als geheimen. Ook voor deze relaties geldt de vraag: Wanneer zijn vertrouwensrelaties gewenst? Het antwoord op deze vraag wordt geformuleerd als:

Als zonder de betreffende vertrouwensrelatie noodzakelijke systeemfunctionaliteit uitgesloten zou zijn.

De omgang met vertrouwensrelaties zo als hier geformuleerd sluit naadloos aan bij het doelbindingsprincipe dat in de Wet Bescherming Persoon Gegevens wordt gehanteerd.

5 Resumerend

In dit document is de informatie beveiliging in een juridisch kader geplaatst. Op basis van het grondslag dat in dit document is vastgelegd zullen een infrastructurele componenten van de informatiebeveiliging bij overheidsinstellingen worden ingericht. Te specifiek wordt in deze bedoeld op :

- een referentie architectuur voor de beveiliging bedrijfsnetwerken (inter-company) bericht uitwisseling
- een referentie model voor autorisatie

References

- [1] Wet bescherming persoonsgegevens; Staatsblad 302
- [2] Handbook of Information Security (www.cccure.org)ICT-referentie architectuur, UWV, versie 2.0, 18 maart 2002.
- [3] B. Schneier 2000, Secrets and Lies, John Wiley and Sons
- [4] Rescorla 2001, SSL and TLS, Addison Wesley
- [5] Doraswamy, Harkins 1999, IPSEC, Prentis-Hall
- [6] K. Siyan 1995, Internet Firewalls and Network Security, NRP
- [7] Cheswick, Bellovin 1994, Firewalls and Internet Security, Addison Wesley
- [8] Garfinkel, Spafford 1996, Practical Unix & Internet Security O'Reilly & Associates
- [9] The Inevitability of Failure; The flawed assumptoin of security in Modern Computing Environments; National Security Agency of the USA