GvIB Expertbrief – December 2005
ISSN 1872-4876, Jaargang 1 – Nr. 3

Security Principes: Informatiebeveiliging op de managementagenda

Aart Jochem

Alex Bewier

Lucien Bongers

Lex Borger

Henk Coenen

Ben Elsinga

Erik Jonkman

Renato Kuiper

Martijn Oostdijk

Daan Rijsenbrij

André Smulders

De inrichting van de informatievoorziening is ondertussen tot de directieagenda's van de meeste organisaties doorgedrongen. Nieuwe eisen op het gebied van governance en beheersing van de organisatie hebben ook informatiebeveiliging op deze agenda geplaatst. Tegelijkertijd vindt meer uitwisseling van informatie tussen organisaties plaats en het waarborgen van vertrouwen hiervan is een fundamentele kwestie geworden. Vaak worden losstaande security oplossingen geïntroduceerd waarbij de security experts een eigen weg volgen. De verschillende disciplines binnen een organisatie hebben behoefte aan een gemeenschappelijk kader om zaken als bedrijfsvisie, informatiearchitectuur en security met elkaar in verband te brengen en te houden. Security principes bieden in beginsel een handvat om grip te krijgen op deze complexe situatie.

Pagina

http://www.gvib.nl/
expertbrief@gvib.nl

1. INTRODUCTIE SECURITY PRINCIPES

Security en privacy worden steeds belangrijkere onderwerpen in een tijdperk waarin IT meer en meer ingebed wordt in onze businessprocessen, in onze maatschappij en in ons persoonlijk leven. **Eén van de redenen waarom e-business niet omvangrijker, grootser wordt ingevoerd is het gebrek aan voldoende security.** Denk hierbij bijvoorbeeld aan de onweerlegbaarheid (*non-repudiation*) van transacties. Ook bij outsourcingsoverwegingen speelt security een belangrijke factor. Enkele belangrijke vragen die in dit geval spelen zijn: 'hoe blijf ik de baas?' en 'is het wel veilig?'.

Security en privacy zijn twee zijden van dezelfde medaille. Waar in deze brief security wordt genoemd wordt ook privacy bedoeld.

Vaak worden gescheiden security oplossingen geïntroduceerd die geheel los staan van de informatiearchitectuur, terwijl juist de samenhang van belang is om grip te houden op de complexiteit van het geheel. Het achteraf integreren van beveiligingseisen met de informatiearchitectuur leidt bij veel ondernemingen tot problemen. Dit is zichtbaar in beveiligingsoplossingen die niet passen bij de opgestelde architectuurprincipes waardoor extra maatregelen voor het inpassen van de oplossing nodig zijn.. De gevolgen hiervan zijn nauwelijks te overzien, maar kunnen op veel manieren voor afbreuk, inconsistentie en onnodige complexiteit zorgen. Het juist onveiliger worden van applicaties en frustratie bij opdrachtgevers vanwege een niet passende menselijke maat zijn slechts enkele mogelijke problemen die kunnen ontstaan.

De aanpak van security experts bij het ontwerp van beveiligingsmaatregelen krijgt richting door het beantwoorden van de vragen:

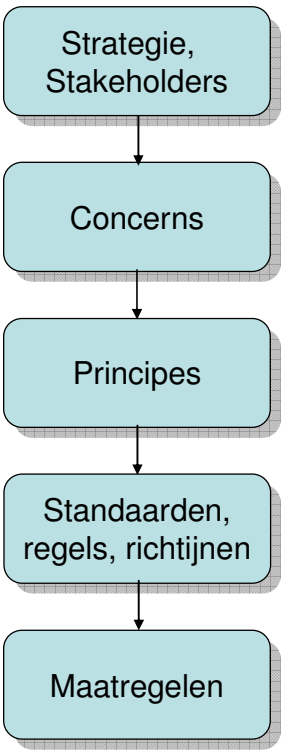
- Waarom is beveiliging belangrijk? Het beantwoorden van deze vraag geeft zicht op de organisatie, de context en de organisatiedoelen. Hierbij komen al principes aan de orde, bijvoorbeeld over de impact voor de gebruiker (beleving), kosten, beschikbaarheid en het voldoen aan wet- en regelgeving..
- Wat moet er beveiligd worden en waartegen? Vrijwel alle raamwerken die voor informatiebeveiliging gebruikt worden (CobiT, Code voor Informatiebeveiliging, VIR A&K), gaan uit van inventarisaties van middelen en bedreigingen en het opstellen van risicoprofielen.
- Wat zijn passende concepten? De architectuurprincipes die hierbij worden bedacht geven oplossingsrichtingen aan en bieden de structuur waarbinnen de maatregelen kunnen worden uitgewerkt
- Hoe worden de concepten uitgevoerd? Welke standaarden en richtlijnen worden ingezet
- Waarmee wordt de informatiebeveiliging geïmplementeerd en ondersteund?

Net als digitale architecten maken ook de security experts globale ontwerpen gebaseerd op principes, regels, standaarden en richtlijnen zodat de technisch ontwerpers hierop kunnen voortborduren. Vreemd is dan ook dat security en informatiearchitectuur bij veel ondernemingen niet geïntegreerd zijn.

1.1 DE ROL VAN PRINCIPES

Principes zijn richtinggevende uitspraken ten behoeve van essentiële beslissingen, een fundamenteel idee bedoeld om een algemene eis te vervullen. De eis komt voort uit een **concern** met betrekking tot de bedrijfsstrategie. Concerns geven aan welke aspecten de bedrijfsvoering kunnen hinderen, welke problemen er spelen. Principes verwoorden wat een organisatie belangrijk vindt, waar zij in gelooft en bakenen de ontwerpruimte af. Het zijn de

drijfveren voor gedrag in de organisatie en beïnvloeden daarom de informatiearchitectuur. Goede principes zijn daarom voor iedereen in de organisatie te begrijpen.



Principes bepalen de **koers** in het opstellen en uitwerken van de informatiearchitectuur en fungeren als **toetsingskader** om deze architectuur en het ontwerp van informatiesystemen te beoordelen.

Vandaag worden door **wetgeving** en **gedragscodes** concerns opgeroepen over de besturing van een organisatie of *corporate governance*, zoals Sarbanes-Oxley in de VS en de Code Tabaksblat in Nederland. Deze concerns worden vaak te snel met IT opgelost, waardoor de terugkoppeling met de opdrachtgever in de organisatie moeizaam of niet verloopt. Het definiëren van principes helpen hierin. Vanuit wetgeving worden bijna nooit universele principes aangedragen, hoewel de privacy wetgeving hierop een uitzondering vormt. Principes helpen wel bij de onderbouwing van de manier waarop aan de wetgeving wordt voldaan.

Zijn security principes anders dan architectuur principes? Met de inzet van ICT om de strategische doelen te behalen komen specifieke concerns over de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie aan bod. Deze concerns vragen om principes die dit adresseren. Maar de rol en plek van security principes in de security architectuur is gelijk aan die van principes in de informatiearchitectuur, alleen de concerns die ze adresseren zijn anders. Een verbijzondering, dus. Kun je dan eigenlijk wel spreken over een security architectuur? Security is een kwaliteitsaspect van informatievoorziening en dus een aspect van de informatiearchitectuur. Een informatiearchitectuur is niet compleet zonder de security te adresseren. In het ideale geval bestaat Security Architect niet als een aparte rol in een organisatie of project. De IT-architect moet alle gebruiksaspecten van de systemen en gegevens beschouwen en zal *security experts* inschakelen. Er bestaan in de fysieke architectuur toch ook geen Brandbeveiligingsarchitecten?

Zolang security apart van de informatiearchitectuur of later als zelfstandig aandachtsgebeid wordt toegevoegd, zullen er security architecturen nodig zijn, maar met het volwassen worden van de informatiearchitectuur zal security een integraal onderdeel van bedrijfsprocessen en informatiesystemen worden.

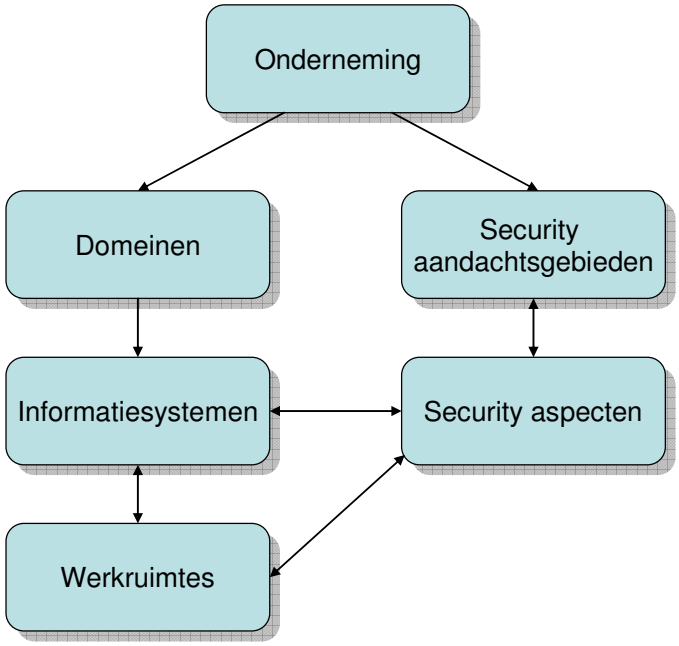
2. ONDERZOEKSVRAGEN

Deze expertbrief probeert een aanzet te geven tot een holistische aanpak, met als doel de integratie van security kwesties en informatiearchitectuur te bevorderen. Dit leidt tot de volgende onderzoeksvragen:

- Welke security aspectgebieden kunnen in het algemeen worden onderkend?
- Welke security principes worden doorgaans geformuleerd in die security aspectgebieden?
- Hoe worden security principes onderling geordend?
- Wat is de mogelijke werking/impact van security principes?
- Hoe worden de juiste security principes gekozen in een specifieke situatie?

3. SECURITY AANDACHTSGEBIEDEN EN ASPECTEN

De vraag over security aandachtsgebieden is niet eenduidig te beantwoorden. De keuze wordt ingegeven door het perspectief dat je op de organisatie neemt. Standaard perspectieven worden aangeboden door raamwerken zoals CobiT en de Code voor Informatiebeveiliging. De raamwerken vormen een set van beleidsuitspraken, procedures en technologie die de aanpak van security binnen een organisatie standaardiseert. Ze leveren perspectieven op security en maatregelen binnen de (IT-) organisatie. Voorbeelden van aandachtsgebieden zijn fysieke beveiliging, business continuïty, logische beveiliging, personeel, etc. Belangrijk is uit te gaan van de concerns die voortvloeien uit de strategie of die leven bij sleutelfiguren in de organisatie: 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?



Relaties tussen architectuur terreinen en security terreinen

Vanuit de informatiebeveiliging worden verschillende beschouwingen van security aspecten aangeboden. De Code voor Informatiebeveiliging rust op de aspecten voor de waarborging van *beschikbaarheid, integriteit* en *vertrouwelijkheid* van informatie. CobiT, mede gericht op assessment van de informatievoorziening, noemt de criteria *effectiviteit, efficiëntie, vertrouwelijkheid, integriteit, beschikbaarheid, compliance* en *betrouwbaarheid* van informatie als meer algemene aspecten voor de informatievoorziening.

4. KENMERKEN VAN GOEDE SECURITY PRINCIPES

Het opstellen van security principes gebeurt in de eerste fase van een architectuurtraject, bijvoorbeeld voor het opstellen van een informatiebeveiligingsbeleid of bij het kiezen van oplossingsrichtingen. Als er meerdere trajecten op deelaspecten van de architectuur worden uitgevoerd is het belangrijk enige samenhang aan te brengen tussen de pricipes in deze trajecten. Om goede principes op te stellen moeten de concerns helder gemaakt kunnen worden. Daarna worden, nadat de organisatie en de context zijn bestudeerd, de security principes opgesteld. Security principes zitten verstopt in bestaande beleidsdocumenten en procedures en in het gedrag en geloof van het management van de organisatie. Als je op zoek gaat kom je al snel aan een lange lijst van principes, die meestal zijn versneden met richtlijnen, ontwerpeisen en uitgangspunten voor de informatievoorziening.

Een goed principe heeft de volgende kenmerken:

- Het is een drijfveer voor gedrag in een organisatie;
- Het is een achterliggend uitgangspunt, dat de informatiearchitectuur beïnvloedt;

- Hij is goed te communiceren: hoe strategischer het principe, hoe simpeler hij te communiceren is;
- Hij is robuust:
  - Hij is niet eenvoudig lek te prikken;
  - Hij krijgt geen andere betekenissen in andere contexten;
  - Hij kan langere tijd meegaan;
- Hij wordt herkend en gedragen door het management.

Principes zijn er op alle niveaus: zowel strategisch, tactisch als operationeel van aard. Ze dwingen je tot een toelichting als je ervan afwijkt. Vaak brengen principes ook tegenstellingen naar voren en is er noodzaak tot weging en prioritering. Prioriteiten bepalen hoe met de tegenstellingen omgegaan wordt: een principe met een hoge prioriteit prevaleert boven een principe met een lagere prioriteit. Sommige principes, die wel herkend worden als uitgangspunt maar een lage prioriteit hebben, zijn “nice-to-have”-principes.

Principes dienen helder vastgelegd te worden: ze vormen een toetsingskader voor architectuur en implementatie van (beveiligings)maatregelen en leggen de relatie met de concerns. Daarnaast is het handiger te communiceren als de principes in duidelijke taal zijn opgeschreven. Het artikel *Architecture Principles* van de Open Group [8] geeft een bruikbaar format hiervoor.

5. Ordening van Security Principes

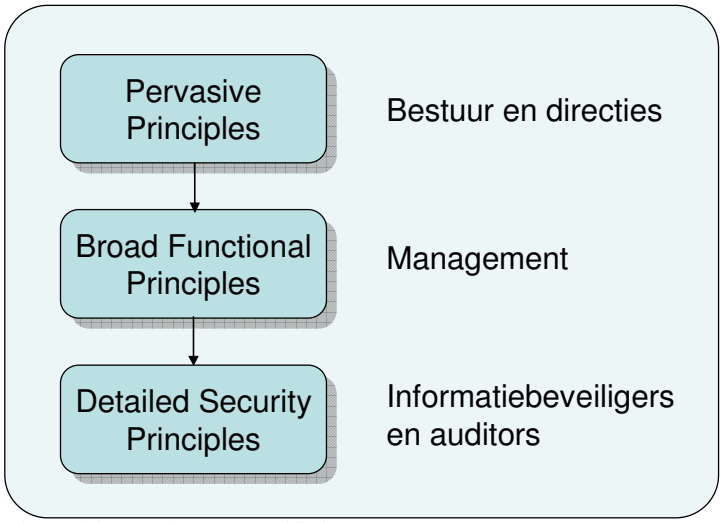
Gelijk met de ontwikkeling van het security vakgebied zijn algemeen bruikbare principes, patronen[1] en controls[2] verzameld en gedocumenteerd. Het abstractieniveau hiervan is erg verschillend, waardoor ordening noodzakelijk is. Er zijn diverse manieren om ordening aan te brengen, enkele hiervan worden hieronder besproken.

General accepted information security principles (GAISP)

Het raamwerk van GAISP is ontstaan nadat de US National Research Council aanbevelingen publiceerde voor de verbetering van de informatiebeveiliging in het rapport “Computers at Risk”. GAISP is van start gegaan als GASSP (general accepted system security principles)'.

De basis voor GAISP bestaat uit drie categorieën van principes [2]:

- Pervasive principles (PP’s) of fundamentele principes zijn gericht op beheersing van de organisatie en geven richtlijnen op strategisch niveau. Deze principes zijn enkele (9) basisprincipes die nauwelijks wijzigen in de loop van de tijd. Voorbeelden van pervasive principles zijn het *accountability principle* over de aansprakelijkheden en verantwoordelijkheden o.h.g.v. informatiebeveiliging, het *proportionality principle* over het in balans brengen van



[1] Security patronen zijn standaard oplossingen voor veel voorkomende problemen in een specifieke context [14].
[2] Security controls zijn maatregelen die het mogelijk maken de beschikbaarheid, integriteit en vertrouwelijkheid van informatiemiddelen te beheersen.

maatregelen en risico's en het *equity principle* over het respecteren van individuele rechten.

- Broad functional principles (BFP's) zijn meer gedetailleerd en definiëren aanbevolen tactieken vanuit het perspectief van management. Er zijn 14 BFP's gedefinieerd. Een BFP ondersteunt één of meerdere pervasive principles. BFP-1, de security policy, ondersteunt ze allemaal. Andere BFP's gaan over accountability, information management, access control, etc.
- Detailed security principles (DSP's) leveren specifieke en gedetailleerde aanpakken, geschreven voor de security en audit professionals en gericht op operationele beveiliging en risicomanagement. Deze principes leveren de methodes om de BFP's te realiseren. Er zijn veel DSP's die een BFP ondersteunen. Een voorbeeld is het gebruik van one-time passwords, om de BFP access control mede te kunnen realiseren en de PP proportionaliteit ondersteunt.

De indeling en principes die de GAISP levert zijn doordacht en onderbouwd. Een bezwaar bij 'standaard' principes is dat de relatie met de concerns niet is aangebracht, de principes zijn toch *best practice*. Bij GAISP is dit ondervangen doordat de principes op de drie niveaus gerelateerd zijn aan elkaar en elkaar ondersteunen. Het gebruik van een detailled principes is terug te voeren naar een pervasive principle, zodat de impact op aanpassingen nagegaan kan worden. De pervasive principles zijn zo fundamenteel en helder verwoord, dat de link met de concerns in de organisatie eenvoudig te leggen is. Detailled security principles zijn echter nog in ontwikkeling.

Security principes volgens Elsinga/Hofman

In hun artikel [4] beschrijven Elsinga en Hofman drie soorten principes:

- Mindset principles geven de denkrichting over security in een organisatie aan en worden gebruikt bij het formuleren van de security strategie;
- Architecture principles geven de oplossingsrichtingen aan met betrekking tot de inrichting van de beveiliging;
- Execution principles geven aan hoe te handelen bij complexe veranderingen.

De indeling is interessant, omdat ze security principes vanuit de opsteller en de werking van de security principes benaderen. Er hoeft niet direct een verband te bestaan tussen de drie lagen, maar er moet wel een harmonie bestaan.

Een **voorbeeld** is op zijn plaats:
Een concern dat leeft bij een organisatie die aangesloten is op Internet is de bedreiging van inbraak op de systemen. Een security principe dat geformuleerd wordt is het beveiligen van de voordeur (de aansluiting op het Internet) tegen onbevoegde toegang ("fortress mentality"). Als standaard architectuur principe wordt perimeter security gekozen, die wordt uitgevoerd met een centrale firewall.

Na de publicatie van de statistieken over interne bedreigingen verschuift het concern: het gaat niet meer louter om de beveiliging tegen inbraken van buitenaf, maar ook van binnen uit. Architectuurprincipes die hier bij horen zijn compartimentering, object security en individu gerichte beveiliging. Het Jericho-forum[3] spreekt hierbij zelfs over *de-perimeterization*, zo sterk is het perimeter security principe verankerd.

[3] Jericho Forum, *Visioning Whitepaper*, februari 2005

6. HET OPSTELLEN VAN SECURITY PRINCIPES

Het opstellen van security principes is in hoge mate een interactief proces. Omdat ze moeten leven in de organisatie kunnen ze nooit bij de security expert alleen vandaan komen. Deze kan ze wel ordenen. De principes geven richting aan de concerns die leven bij het management. Hier moet dan ook gestart worden: wat is er gezegd over missie en inrichting van de informatievoorziening, wat is vastgelegd in beleids- en architectuurdocumenten.

Het is sterk aan te bevelen om toegepaste principes, vooral principes die op het niveau van pervasive of mindset principes liggen, af te stemmen met het topmanagement en het management van de ICT-organisatie. Hiervoor moet informatiebeveiliging wel op de agenda van het management zijn gebracht. Ook is het van belang om goed te kijken naar de manier waarop ze verwoordt zijn: helder formuleren en het vermijden van techniek en jargon is essentieel. Laat het management ook helpen met het prioriteren van de principes.

De principes moeten ook getoetst worden of ze gerelateerd zijn aan in de organisatie levende concerns en voldoen aan de criteria van goede principes. De genoemde standaard principes geven houvast voor de uitwerking van de pervasive of mindset principes naar meer gedetailleerde principes. De GASSP/GAISP en de Elsinga/Hofman indeling geven goed houvast. Belangrijk is te blijven letten op de relatie tussen principes en concerns. De standaard principes geven een oplossing voor veel voorkomende problemen Ze vormen een handige checklist en kunnen het proces versnellen, maar de relatie met de concerns moet zelf aangebracht worden.

7. CONCLUSIES EN VERVOLG

- Er is nog veel verschil in definities van begrippen en de manier waarop security principes worden toegepast is nog erg divers. Er zijn veel ideeën, maar duidelijk is dat we er nog niet zijn op dit vakgebied. Ook lijkt er nog een kloof te bestaan tussen theorie en praktijk: hoe ga je aan de slag in de organisatie?
- Security principes zijn moeilijk grijpbaar en moeten met aandacht opgesteld worden. Een belangrijk kenmerk van principes is dat ze aan de basis staan van gedrag in de organisatie. Als de principes helder zijn, zijn ze van grote waarde in een organisatie en ontwerptraject.
- Nog te weinig wordt het management betrokken bij het opstellen van security principes. Op dit vlak valt nog veel te doen. Een juiste aanpak en formulering van de principes zijn belangrijke aspecten hiervoor.
- Er is een afhankelijkheid tussen de volwassenheid van een organisatie op het gebied van security en de security principes. Naarmate de kwaliteit, betrouwbaarheid en governance verbeteren, zullen ook de uitgangspunten veranderen en zullen principes meer formeel toegepast worden. Hierin ontstaat een balans. In het extreme geval heerst chaos en zullen weinig principes gelden. Teveel principes belemmeren de flexibiliteit van de organisatie.
- Het feit dat er generieke security principes bestaan betekent dat er binnen de informatiearchitectuur een apart security stroom bestaat. Belangrijk is dit te onderkennen en te werken aan afstemming tussen de stromen.

Hoe verder?

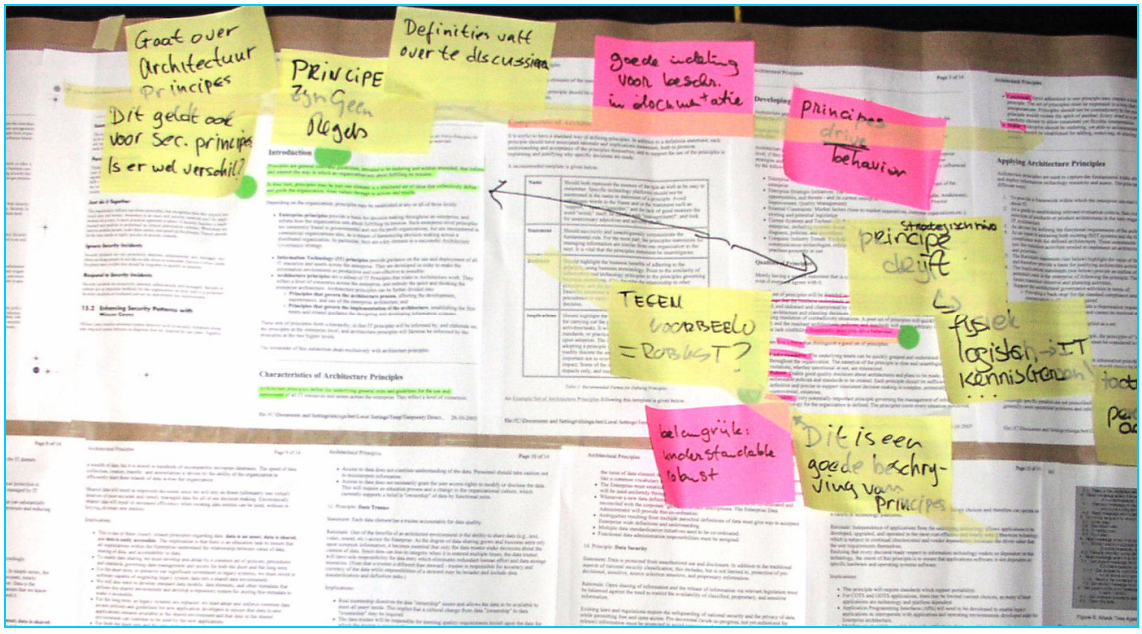
Door de complexiteit van de materie en de beperkte tijd waarin dit onderwerp besproken is, zijn er nog vele vragen onbeantwoord gebleven:

- Welke definities zijn er rond security principes en welke relatie bestaan er?
- Welke ramenwerken adresseren security principes, welke is het beste te gebruiken?
- Wie is eigenaar van de security principes, de business of het security team?
- Worden Security principes beschreven op organisatie niveau, domein niveau of een combinatie van beide?
- Hoe is de relatie tussen digitalen architecten en security architecten vandaag de dag, en hoe gaat deze verschuiven over de tijd?

Dit artikel is niet meer dan een eerste aanzet om een brede discussie op gang te brengen, waarbij de input van zoveel mogelijk betrokkenen gewenst is. De expertgroep nodigt u dan ook uit om te reageren. Daarnaast wijzen wij graag naar het afstudeerwerk van Lucien Bongers over dit onderwerp, dat begin 2006 afkomt*:*
http://www.student.ru.nl/l.bongers/onderzoek.htm

U kunt uw reactie op dit artikel sturen naar expertbrief@gvib.nl

Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!



GvIB-Expertbrief in wording

LITERATUURLIJST

Voor het tot stand brengen van deze expertbrief over *Security Principes* heeft de werkgroep de volgende literatuur geraadpleegd:

[1] Sietse Overbeek, Sergej van Middendorp en Daan Rijsenbrij, *De Digitale Werkruimte, een nieuw architectuurartefact*, juni 2005

[2] International Information Security Foundation, *GASSP (Generally Accepted System Security Principles)*, juni 1999

[3] US National Security Agency, *Defense in Depth*, juni 2001

[4] Ben Elsinga, Aaldert Hofman, *Security Principles,* pattern paper submitted for EuroPlop 2003.

[5] Bert Snel, *Informatie Beveiliging Opzet & Bewustzijn,* Siemens white paper, juni 2005

[6] Dan Blum, *Security and Risk Management Strategies Reference Architecture Principles*, Burton Group, jan 2005

[7] Lee Hopkins, *Dialogue: The Four Dialogic Principles For Successful Communication*, http://www.b2bhints.com/biz/2004/12/dialogue_the_fo.html

[8] Open group, *Architecture Principles*, http://www.opengroup.org/architecture/togaf8-doc/arch/p4/princ/princ.htm

[9] Lex Borger, *Presentatie Security Architectuur Principes*

[10] Gary Stoneburner, Clark Hayden, Alexis Feringa, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* NIST Special Publication 800-27 Rev A

[11] Bruce Schneier, *Modeling security threats*, in Dr. Dobbs Journal, december 1999

[12] Carl E. Landwehr, *Computer Security*, Springer-Verlag, juli 2001

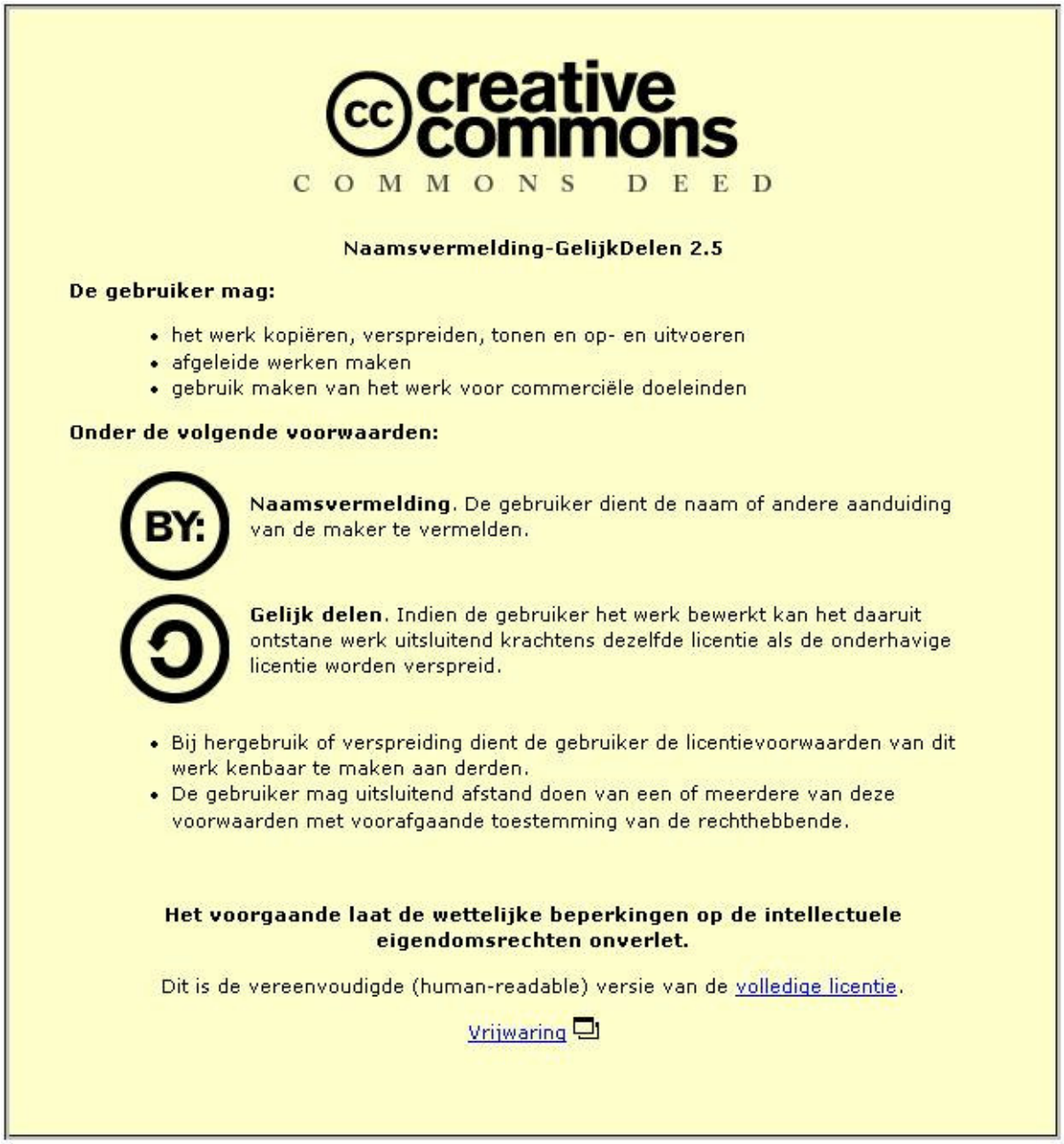
[13] M. Schumacher, *Foundations of Security Patterns*, uit Security Engineering with Patterns, Springer-Verlag, 2003

[14] Bijlage van het *Security Patterns boek,* http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470858842.html

10

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/



creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

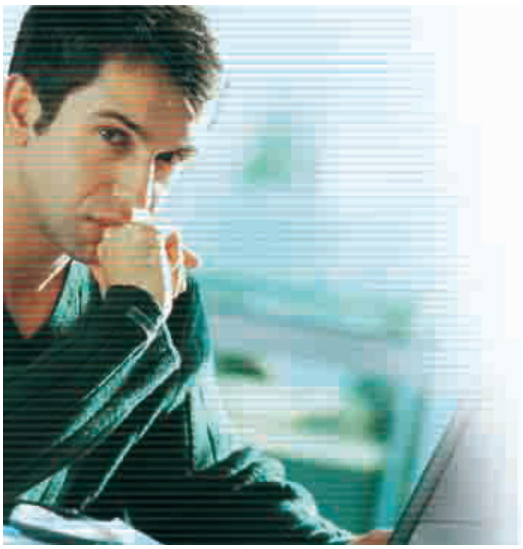
- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is al jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm