juni 2009 nummer 4

Special: Architectuur en Security

Open Security Architecture: een open source architectuur

Beveiligingsarchitectuur in Jericho-stijl

Beveiliging en architectuurraamwerken: de rol van audits

Architectuurprincipes versus projectmatig opportunisme

Het SABSA® Model

INFORMATIEBEVEILIGING

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

Ik ben de laatste tijd volop bezig met architectuur. Enterprise architectuur, informatiearchitectuur, referentie-architectuur, securityarchitectuur. Dat varieert van het nadenken over de begrippen en het ontwerpen ervan, tot het beoordelen van implementatie-voorstellen. We zijn echt wel goed bezig. En ik vind het dan ook leuk; dat denken 'onder architectuur'. Het leuke ervan is dat je af en toe gewoon een whiteboard kunt voltekenen. Zo'n tekenbord is volgens mij het belangrijkste instrument voor een architect. En als je maar ver genoeg van de harde praktijk af blijft, vindt iedereen de platen mooi. Mooi generiek werk vindt overal wel een plaatsje.

Wat minder leuk is? Methodes. Wat blijkt? Ik ben eigenlijk al jaren architect. Nooit geweten, maar ja, dat is dan het noodlot. Ik heb me al jaren beziggehouden met het ontwikkelen van architecturen voor beveiliging, maar ik noemde het nooit zo. Het waren visies, ideeën, concepten, ontwerpen... Het was van alles behalve architectuur. Waarom? Geen idee. Misschien omdat ik me uit het verleden enkele heftige discussies herinner in diverse vakbladen over de functie-benaming Architect. Dat was immers een beroep voor mensen die gebouwen en bruggen bedachten. Nog een oorzaak voor mijn aarzeling mezelf architect te noemen, was dat het een bijzonder vakgebied is, waarvoor je over specifieke kennis en vaardigheden moet beschikken, die ik mezelf nooit had toegedicht.

En architectuur is natuurlijk een vakgebied waarin professionals op een gestructureerde manier mooie dingen maken. Ik ben veel, maar niemand heeft mij ooit gestructureerd genoemd.

Inmiddels loop ook ik al enkele jaren rond in de wereld van architecten en ik denk dat ik ook kan meepraten, ik durf dingen te roepen en te beoordelen en zoals gezegd, ik vind whiteboards gewoon heel handig. Dat impliceert dan misschien dat ik toch ook een architect ben. Maar daar wringt dan meteen de schoen, ik kan niet methodisch werken. Dat kost toch te veel tijd?

Klopt, en daarom is hergebruik van bouwblokken een wet uit de architectuur. En heeft deze special dan een functie: we leveren enige kennis over architectuur als bouwblokken aan. In dit nummer publiceren we een introductie op het onderwerp architectuur en belichten we het onderwerp vanuit diverse gezichts-punten. Methoden (daar zijn ze), cases, een paar interviews. We raken lang niet alles, beschouw dit gewoon als een set bouwblokken om zelf met architectuur aan de slag te gaan. Ik vermoed dat we binnenkort nog meer artikelen over architectuur zullen plaatsen.

Veel leesplezier,

André Koot
Hoofdredacteur

PS: op 12 juni jl heeft Saïd el Aoufi (de auteur van onder meer het eerste artikel in deze special) zijn proefschrift over *'Economic Evaluation of Information Security'* met succes verdedigd. Dat gebeurt nog niet zo vaak een promotie binnen ons vakgebied. Saïd: proficiat!

Informatiebeveiliging is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Peter Westerling/Monique van Diessen (eindredactie, TOPpers Media bv, Berlicum)

Redactieraad
Tom Bakker (Delta Lloyd)
Mario de Boer (Logica)
Lex Borger (Domus technica)
Lex Dunn (Capgemini)
Rob Greuter (Secode Nederland)
Aart Jochem (GOVCERT.NL)
Renato Kuiper (HP)
Henk Meeuwisse (Sogeti)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving
Van Velzen Grafisch Ontwerp, 's-Hertogenbosch

Uitgever
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
E-mail: secretariaat@pvib.nl
Website: www.pvib.nl

Abonnementen
De abonnementsprijs bedraagt 115 euro per jaar (exclusief BTW), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

Inhoud

Beveiliging en architectuurraamwerken

De rol van audits

Auteurs: Saïd El Aoufi > Saïd El Aoufi is werkzaam als senior consultant bij MetaPoint BV en is bereikbaar via said.el.aoufi@metapoint.nl.
Met dank aan Norien Kuiper en Louis van Hemmen voor de review van dit artikel.

Architectuur is een instrument dat bijdraagt aan een optimale afstemming tussen processen en de informatievoorziening. In de architectuur worden de afspraken vastgelegd waar iedereen (business en IT) zich aan heeft te houden ter waarborging van de afstemming tussen business en IT. Architectuur, ofwel duidelijk vastgelegde ontwerpprincipes en afspraken, is onmisbaar om de inrichting en het beheer & beveiliging van processen en informatiesystemen beheerst te laten plaatsvinden. Dit artikel geeft een overzicht van de verschillende architectuurraamwerken en de rol van audits.

Theoretisch kader

Architectuur wordt algemeen beschouwd als een middel om de complexe relatie tussen business en IT te beheersen. Zoals er geen uniforme terminologie en definitie bestaat binnen de architectuur, bestaat er ook geen uniforme theorievorming en begripsbepaling betreffende architectuur. Zo is er theorievorming over architectuur te vinden onder termen als IT-architectuur, informatiearchitectuur, business architectuur, digitale architectuur en enterprise architectuur. Enterprise architectuur is een centraal referentiepunt voor business en IT-kwesties en de relatie daar tussen, en daardoor geschikt als (a) een abstractiemiddel, (b) een communicatiemiddel en (c) managementinstrument (Van der Raadt et al., 2004). De termen business, informatie en IT architectuur refereren naar verschillende ontwerpdomeinen binnen de organisatie. Digitale architectuur, een term onder andere gebruikt door Rijsenbrij, Gartner en Forrester, verwijst impliciet naar het digitale of IT aspect binnen de onderneming, terwijl dit ook een ontwerpdomein is binnen het systeemtype enterprise (Buitenhuis, 2007).

Wat is architectuur?

Rijsenbrij (2005) definieert architectuur als *een verzameling van architectuurprincipes, verbijzonderd naar regels, richtlijnen en standaarden*. Hierbij zijn principes richtinggevende uitspraken ten behoeve van essentiële beslissingen, een fundamenteel idee, bedoeld om een algemene eis te vervullen. Een goed en relevant principe heeft verschillende kenmerken (Jochem et al., 2005), namelijk:

- het is een drijfveer voor gedrag in een organisatie,
- het is een achterliggend uitgangspunt,
- het is goed te communiceren,
- het is robuust, en
- het wordt herkend en gedragen door het management.

Een ander definitie is die van IEEE 1471 (2000). Architectuur is gedefiniëerd in IEEE 1471-2000 als *'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'*.

Volgens de definitie beschrijft een architectuur niet alleen componenten en hun samenhang, maar ook de relatie met de omgeving is van essentieel belang. Naast een modelmatige benadering van architectuur geeft de definitie aan dat architectuur ook procesmatige aspecten bevat. In het bijzonder geeft het principes voor het werken (ontwerpen) onder architectuur en zou een architectuur expliciet aandacht moeten besteden aan evolutie-aspecten.

Bij het kiezen van een definitie voor de eigen organisatie is het van belang een definitie te kiezen die zo concreet mogelijk aangeeft wat aard en scope zijn van architectuur. Als architectuur zich vooralsnog beperkt tot IT is het raadzaam om dat in de definitie ook aan te geven. Als de architectuur zich louter beperkt tot het opstellen van principes en standaarden die richting geven aan het ontwerp, is het aan te bevelen deze te noemen.

Beveiliging als vast onderdeel van architectuur

Volgens Rijsenbrij (2005) is beveiliging een vast onderdeel van een geïntegreerde architectuurbenadering en beslaat alle vier werelden in samenhang. Deze vier werelden zijn het organisatiegebeuren, informatieverkeer, applicatielandschap en de technische infrastructuur.
De beveiligingsarchitectuur beschrijft de manier waarop beveiliging wordt vormgegeven en beschouwt de beveiligingsmaatregelen van gebruiker tot dienst, een end-to-end beschouwing.
Elke wereld heeft zijn eigen beveiligingsprincipes, die soms ook nog op gespannen voet staan met de principes uit die wereld zelf (Rijsenbrij, 2005).

Het bovengenoemde houdt dus in dat een beveiligingsarchitectuur geen ander document hoeft te zijn dan de andere architecturen. Beveiligingsaspecten kunnen dus ook in elk van de onderliggende architecturen zijn beschreven. Het is wel belangrijk dat het geheel is aangesloten, waardoor de traceerbaarheid van uitgangspunten en eisen naar maatregelen gewaarborgd wordt.

Volgens de GvIB Expert Brief (Bel et. Al., 2006) zijn kritieke succesfactoren voor het ontwikkelen van een beveiligingsarchitectuur:

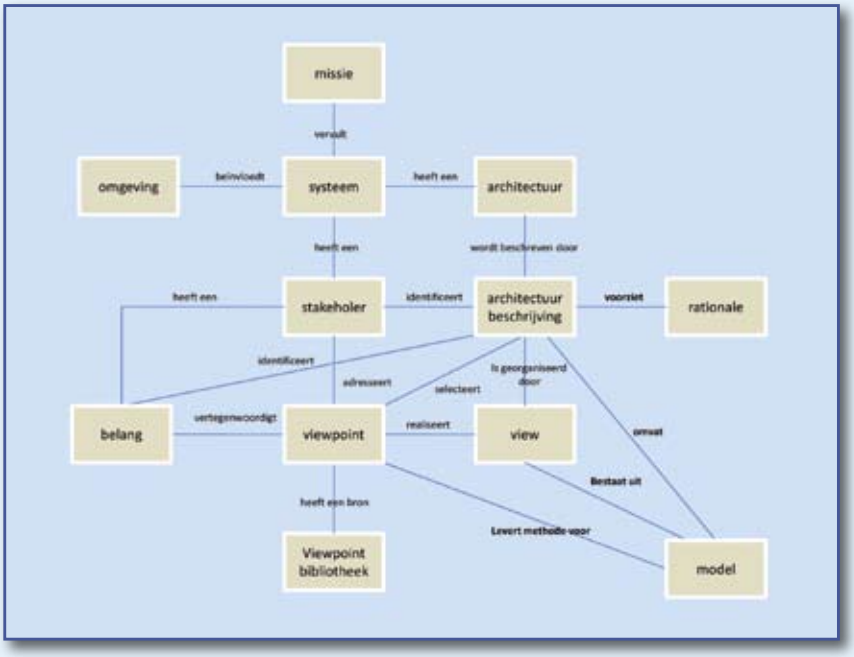
- het hebben van beleid en een classificatiesysteem voor beveiliging,
- bruikbaarheid voor de doelgroepen en de beleving dat met een beveiligingsarchitectuur de complexiteit wordt gereduceerd, en
- een betere beveiliging kan worden gerealiseerd.

Wat zijn de drijfveren voor architectuur?
Burke (2002)[2] noemt drie belangrijke drijfveren voor het inzetten van (enterprise) architectuur in organisaties, namelijk:

1. Business - IT alignment
2. De wendbaarheid van de business ook wel 'business agility' genoemd
3. Kostenbesparing op de IT middelen

Business - IT alignment is historisch gezien het belangrijkste argument geweest om enterprise architectuur op de agenda te zetten en blijft nog steeds een belangrijke drijfveer (Burke, 2002; Van der Raadt et al., 2004). De laatste tijd wordt ook wendbaarheid als drijfveer steeds vaker genoemd. Niet alleen in de IT-landschap maar ook in de business neemt de complexiteit toe. Van organisaties wordt verwacht dat zij de maatschappij efficiënter gaan bedienen en zich sneller aan kunnen passen aan gewijzigde omstandigheden, kortom dat zij wendbaar worden (Hendriks & Oosterhaven, 2006).
Een andere drijfveer die de laatste jaren wordt genoemd voor het inzetten van enterprise architectuur is het verminderen van de IT kosten. Veel organisaties worden namelijk geconfronteerd met de kosten in relatie tot de toegevoegde waarde van hun IT activiteiten (Maes, 2007).

Conceptueel Model
De architectuur van een systeem kan beschreven worden vanuit vele gezichtspunten, afhankelijk van de belangen die spelen in het veranderingsproces. Een belangrijke bijdrage van de IEEE/ANSI standaard P1471 is een conceptueel model waarin de samenhang tussen de verschillende architectuurbegrippen is beschreven. Figuur 1 geeft een abstract niveau overzicht van dit conceptueel model. IEEE maakt het onderscheid tussen een architectuur hebben en een architectuur opstellen. Ieder systeem heeft een inherente architectuur: de architectuurbeschrijving (architectural description) moet deze architectuur beschrijven. Een ander belangrijk inzicht



Figuur 1 - Architectuurstandaard IEEE

is dat er meerdere gezichtspunten op architectuur zijn, die in een standaard 'views' en 'viewpoints' worden genoemd. Een viewpoint is een voorschrift voor een view op een specifiek systeem. Elk viewpoint geeft een unieke manier aan om naar een systeem te kijken. Het viewpoint bevat tevens aanwijzingen voor hoe deze manier van kijken moet worden opgeschreven. Viewpoints worden altijd gedefinieerd voor belangen (concerns) van bepaalde belanghebbenden (stakeholders).

Architectuurraamwerken
Volgens Greefhorst et al. (2003) komen architectuurraamwerken voor in twee smaken: enterprise-raamwerken en applicatieraamwerken. Hierbij hebben enterprise-raamwerken de hele organisatie op het oog en ze bevatten vaak meerdere dimensies. Greefthorst et al. (2003) analyseerden de architectuurraamwerken hetgeen heeft geleid tot negen basisdimensies: informatie, bereik, detailniveau, belanghebbenden, transformatie, kwaliteitseigenschappen, metaniveau, aard en representatie. Uit interviews bleek dat het niet veel uitmaakt welk architectuurraamwerk wordt gebruikt, als er maar een raamwerk wordt gebruikt. Het algemene doel van een raamwerk blijft toch het ondersteunen van de architect bij het creëren van samenhang, overeenstemming en begrip tussen de verschillende componenten van een organisatie.

Voorbeelden van bekende raamwerken zijn
- Het Zachman raamwerk (Zachman, 1987)
- Het TOGAF raamwerk (TOGAF, 2004)
- IAF (Goedvolk et al., 1999)
- Tapscott (Tapscott & Caston, 1993)
- DYA (Wagter et al., 2001)
- 2+2-model (Lassing et al., 2001)
- Dragon1 (Paauwe, 2006)

Specifiek voor beveiliging zijn er in de loop van de jaren een aantal raamwerken ontwikkeld. Dit zijn onder andere:
- Open Security Architecture (OSA, zie ook het artikel van André Koot op pagina 12, 13 en 14)
- Sherwood Applied Business Security Architecture (SABSA) framework
- Enterprise Information Security Architecture (EISA)

Volgens Greefhorst et al. (2003), vallen een aantal dingen op bij de verschillende architectuurraamwerken, namelijk:
- Er worden verschillende termen voor vergelijkbare aspecten gebruikt, en vice versa.
- Veel termen zijn niet duidelijk gedefiniëerd, waardoor de exacte betekenis niet duidelijk is.
- Sommige raamwerken lijken sterk op elkaar, maar zijn toch net weer 'even anders'.
- De relatie tussen de waarden binnen een

dimensie is soms moeilijk te ontdekken, waardoor de dimensie moeilijk te begrijpen valt.

Een verklaring voor de verschillen in de raamwerken is dat de auteurs hebben gepoogd om, gegeven een bepaalde context en een bepaald doel, alle relevante aspecten te combineren. Verder zien de auteurs dat raamwerken vaak uit twee dimensies bestaan. De eerste dimensie beschrijft vaak de typen informatie (onderwerpen) die kunnen voorkomen in een architectuurbeschrijving. Een grove onderverdeling in typen informatie is het onderscheid tussen IT en business. De tweede dimensie in raamwerken is vaak sequentieel van aard; er is een bepaalde volgorde waarin de modellen binnen deze dimensie opgesteld worden.

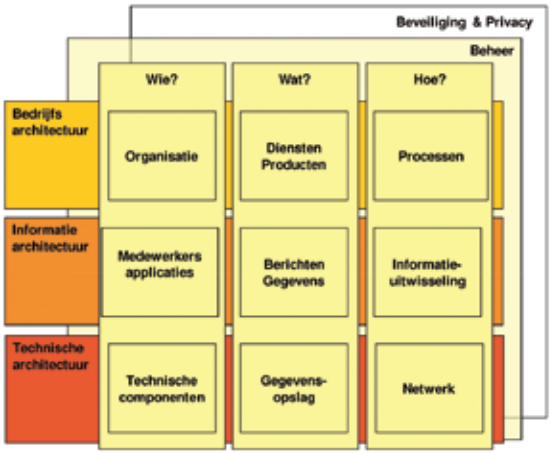
Een korte beschrijving van NORA

Burgers en bedrijven verwachten een goed functionerende overheid. Interoperabiliteit [1] is hiervoor een belangrijke voorwaarde. NORA, de Nederlandse Overheid Referentie Architectuur [2], is een raamwerk dat overheidsorganisaties helpt om deze interoperabiliteit te realiseren.
De NORA hanteert de definitie van het IEEE voor architectuur, namelijk: Architectuur is de beschrijving van de fundamentele opbouw van een systeem, bestaande uit:

- zijn componenten;
- hun onderlinge relaties en die tot hun omgeving;
- de principes voor hun ontwerp en evolutie.

In de NORA versie 2.0 worden 'fundamentele principes' en 'architectuurprincipes' voor de inrichting van de e-overheid gepresenteerd.
De fundamentele principes hebben betrekking op:

- hogere kwaliteit van de dienstverlening;
- administratieve lastenverlichting;
- transparantie;
- proactieve dienstverlening;
- een integrale en betrouwbare overheid;
- verbeteren van de doelmatigheid.



Figuur 2 - Architectuurraamwerk voor de NORA

De architectuurprincipes zijn geordend op basis van een 'architectuurraamwerk' (zie onderstaande figuur). Het architectuurraamwerk bestaat uit een matrix met drie architectuurlagen (bedrijfsarchitectuur, informatiearchitectuur, technische architectuur) en drie dimensies (wie, wat, hoe). Deze dimensies representeren verschillende componenten binnen een laag. Daarnaast zijn er twee algemene dimensies die op alle lagen en componenten betrekking hebben: beheer en beveiliging & privacy. Op de bedrijfslaag gaat het bijvoorbeeld om de veiligheid van medewerkers, producten en bedrijfsprocessen. Op de middelste laag ligt de nadruk op de informatiebeveiliging: van applicaties (beschikbaarheid), van gegevens (integriteit) en van de communicatie (vertrouwelijkheid). Op de onderste laag (techniek) spreken we over authenticatie (PKI, etc.) en encryptie, naast de fysieke aspecten (firewalls, etc.).

Beveiliging & privacy

Een goed functionerende informatievoorziening is een belangrijk onderdeel van de bedrijfsvoering van de overheid geworden en het wordt, met onder meer de komst van de e-overheid, steeds belangrijker. Samenwerking van de overheidsorganisaties brengt een aantal zaken met zich mee. Een organisatie moet een bepaald niveau van beheersing hebben bereikt om op een verantwoorde wijze te kunnen samenwerken en aan de e-overheid te kunnen bijdragen. Dit kan worden gezien als de baseline voor security. Een mate van beheersing waarover zij ook verantwoording aflegt. Het betreft de volgende aspecten:

- De organisatie beheerst haar informatiebeveiliging.
- De organisatie beheerst haar bescherming van persoonsgegevens ter bescherming van de persoonlijke levenssfeer van de betrokkenen. Hierbij speelt de WBP (Wet Bescherming Persoonsgegevens) een grote rol.
- De organisatie beheerst de continuïteit van haar belangrijkste bedrijfsprocessen.

Samenwerking van organisaties leidt tot het maken van gezamenlijke afspraken over het op elkaar afstemmen en afgestemd houden van de informatiebeveiliging- en privacystelsels, van beleid tot en met controle. Hierbij kunnen ook afspraken over gemeenschappelijke voorzieningen een rol spelen. De NORA geeft richtlijnen betreffende deze afspraken:

- De samenwerkende partijen richten gezamenlijk de governance in voor hun informatiebeveiliging, privacy en continuïteit van de bedrijfsvoering.
- Alle organisaties in de e-overheid dragen bij en maken gebruik van een te ontwikkelen gemeenschappelijk normenkader ten behoeve van bijvoorbeeld audits.
- E-overheidsorganisaties zorgen voor een uniforme en betrouwbare wijze waarmee burgers en bedrijven zaken met haar kunnen doen.
- Informatiebeveiliging, privacy en continuïteit van bedrijfsprocessen vormen een integraal onderdeel van een service of dienst.

[1] Het delen van informatie door overheidsorganisaties.

[2] Een referentiearchitectuur is een instantie van een architectuur welke in vergelijkbare situaties hergebruikt kan worden.

Architectuur en audit

De auditfunctie staat onafhankelijk van de primaire processen van de organisatie en kan worden ingezet om te bepalen of en hoe een instrument als architectuur bijdraagt aan de beheersing (Campbell & De Vries, 2009). Volgens David Campbell en Arjan de Vries (2009) kan de auditfunctie worden ingezet om de kwaliteit van architectuur te beoordelen. Hierdoor krijgen de belanghebbenden een indruk van de effectiviteit van architectuur als beheersmaatregel. In hoofdlijn zien de auteurs drie soorten audits die van toegevoegde waarde kunnen zijn bij het bepalen van de beheersbaarheid en de controleerbaarheid van architectuur als beheersmaatregel.

1. Een audit naar het proces van totstandkoming en onderhoud van de architectuur (architectuur governance).
2. Een audit naar het werken onder architectuur (architectuur compliance).
3. Een audit naar de kwaliteit van de architectuur. Deze audit is over het algemeen gericht op de verschaffing van aanvullende zekerheid of de beoogde rol van het instrument architectuur in een beheersbare en controleerbare ontwikkeling c.q. toekomstige exploitatie feitelijk wordt bereikt.

Daan Rijsenbrij (2009) onderkent vijf onderzoeksterreinen voor een architectuurauditor: de architectuurgovernance, de architectenpopulatie, de architectuur, het architectuurgebruik en de architectuurimplementatie. Een audit over de architectuurgovernance betreft het functioneren van de verschillende architectuurprocessen, de organisatorische inbedding in de businessbeslissingen en de relatie met de IT-governance. Een audit over de architectenpopulatie betreft het functioneren van die architectenpopulatie, haar opbouw, de competenties van de aanwezige architecten en de relaties met de overige deskundigen die assisteren bij het formuleren van een architectuur.
De omvang van deze beide auditsoorten is sterk afhankelijk van de volwassenheid van de architectuurfunctie. Een audit van de architectuurimplementatie betreft een onderzoek in hoeverre de vastgestelde architectuur daadwerkelijk is geïmplementeerd in de infrastructuur, het applicatielandschap, het informatieverkeer en de gedigitaliseerde businessproducten en diensten. Afhankelijk van de afgesproken scope is dit een zeer tijdrovend onderzoek.

Campbell en De Vries (2009) zijn van mening dat een audit van een architectuur slechts een middel is om de kwaliteit van de architectuur en het werken onder architectuur te waarborgen.
De toegevoegde waarde van een architectuuraudit is er wanneer de organisatie dit proces zodanig heeft ingericht dat de auditor de kwaliteit daadwerkelijk kan vaststellen. Dit houdt in dat de organisatie zelf een controleerbare en beheersbare architectuur governance moeten opzetten.

Waarom architectuur audits in de praktijk worden overgeslagen

Volgens Daan Rijsenbrij[3] kunnen drie hoofdredenen worden genoemd waarom de architectuuraudit in de praktijk wordt overgeslagen. Als eerste merkt hij op dat de noodzaak van een goede architectuur onvoldoende duidelijk is. Met andere woorden; de grote potentiële schade van een verkeerde architectuur is niet helder. Als tweede zijn de architecten zo zelfverzekerd dat ze zich niet kunnen voorstellen dat het nodig is om een onafhankelijke, onpartijdige architectuurauditor een blik te laten werpen op hun architectuur. Architecten zijn trots op hun eigen werk en kunnen niet meer objectief kijken naar de gemaakte keuzes. De derde reden heeft te maken met geld. Het opstellen van de architectuur kost veel inspanning en geld, waardoor een architectuuraudit wordt overgeslagen.

Wat is een volwassen enterprise architectuur?

Uit de methode Dragon1 komen de volgende kenmerken die passen bij een volwassen enterprise architectuur (Vos, 2009):

1. De architectuur wordt gedragen en erkend door de business en IT directie van de organisatie en de belangrijkste klanten, ketenpartners van de organisatie.
2. Het bestuur, directie en management maakt gebruik van de architectuur (met name de concepten, principes, modellen en visualisaties) van een bepaald domein, systeem of oplossing voor het nemen van strategische beslissingen.
3. Projecten, leveranciers en ontwikkelaars maken gebruik van de architectuur als richtinggevend kader, om vooruit te kijken en voor het oplossen van problemen.
4. Klanten, ketenpartners en leveranciers maken gebruik van de architectuur om er op aan te sluiten.
5. De architectuur is een up-to-date consistent gedocumenteerd en goed toegankelijk geheel van uitgangspunten, concepten, principes, regels, artifacten/elementen, modellen, oplossingen, visualisaties en views.
6. De architectuur is een soort conceptueel ontwerp van een domein, systeem of solution, waarbij de architectuur is te relateren aan de strategische uitgangspunten, functionele eisen en bedrijfsdoelen van een organisatie.
7. De architectuur beschikt over een gebruikt begrippenkader.
8. De architectuur zorgt ervoor dat logische en fysieke ontwerpen die gemaakt worden onder de architectuur hoger van kwaliteit zijn.
9. De architectuur is gekoppeld aan het transformatieproces, het innovatieproces en de planningen-control-cyclus van de organisatie.
10. De architectuur en onderdelen eruit wordt vaak hergebruikt en niet steeds opnieuw gemaakt en weer teruggekoppeld naar de architectuur. De architectuur is daarmee proactief voorschrijvend en niet reactief beschrijvend.

[3] Gepubliceerd in de Automatisering Gids, 30 januari 2009, nummer 5, pagina 16.

Tot slot

Architectuur wordt gebruikt als communicatiemiddel. Heldere communicatie tussen technici, business experts en stakeholders wordt mogelijk door gebruik te maken van de architectuurmodellen en de beschrijvingen om te komen tot de juiste eisen en om ideeën uit te wisselen voor verschillende ontwerpdomeinen.

Als architectuur is opgesteld, dient het als managementinstrument waar de strategie uitgewerkt kan worden om grip te krijgen op de dynamische veranderingen in de business, de IT en de relatie daartussen. Hierdoor kunnen er geen ontwikkelingen in isolement plaatsvinden die niet in lijn zijn met de bedrijfsstrategie. Beveiligingsaspecten kunnen dus ook in elk van de onderliggende architecturen zijn beschreven. Een architectuuraudit biedt aanvullende zekerheid aan organisaties over het werken onder architectuur. Echter, de verantwoordelijkheid voor een beheersbare en controleerbare architectuur governance en architectuur ligt in eerste instantie bij de organisatie zelf.

Referenties

(Bel et al., 2006)
GvIB Expert Brief, (2006), *Security architectuur: Nieuwe hype voor specialisten of nuttig communicatiemiddel?*, Genootschap van Informatie Beveiligers.

(Buitenhuis, 2007)
Pieter Buitenhuis, (2007), *Fundamenten van het principe Op weg naar een prescriptieve architectuurmodelleertaal*, Master thesis, Radboud Universiteit Nijmegen.

(Burke, 2002)
Burke, B. ,(2002), *Enterprise Architecture Maturity*, META Group Recorded Interview.

(Campbell & de Vries, 2009)
Architectuuraudit: de toegevoegde waarde David Campbell en Arjan de Vries, namens de werkgroep architectuuraudit van de Rijksauditdienst, 2009, www.rad.nl.

(Greefhorst et al., 2003)
Danny Greefhorst, Henk Koning en Hans van Vliet, (2003), *De dimensies in architectuurbeschrijvingen*, Informatie.

(Hendriks & Oosterhaven, 2006)
Hendriks, C. M. & Oosterhaven, J. A., (2006), *ICT Bibliotheek: Wendbaarheid door Architectuur*, Landelijk Architectuur Congres 2006, Sdu Uitgevers, Den Haag.

(IEEE, 2000)
The Institute of Electrical and Electronics Engineers, (2000), *IEEE Standard 1471-2000: IEEE recommended practice for architecture description of software-intensive systems*, ISBN: 0 7381 2518 0.

(Jochem et al., 2005)
GvIB Expert Brief, (2005), *Security Principes: Informatiebeveiliging op de managementagenda*, Genootschap van Informatie Beveiligers.

(Maes, 2007)
Maes, R. , (2007), *An Integrative Perspective on Information Management*, PrimaVera Working Paper, Universiteit van Amsterdam.

(Paauwe, 2006)
Paauwe, M., (2006), *Dragon 1*, voorpublicatie.

(Rijsenbrij, 2005)
Daan Rijsenbrij. (2005), *Architectuur in de digitale wereld. Syllabus: Inleiding in de Digitale Architectuur.*

(Tapscott & Caston, 1993)
Tapscott, D., & D. Caston, (1993), *Paradigm Shift – The New Promise of Information Technology*. McGraw-Hill.

(The Open Group, 2002)
The Open Group ,(2002), *The Open Group Architectural Framework*. Version 8.

(Van der Raadt, 2004)
Raadt, B. van der, Soetendal, J., Perdeck, M. & Vliet, H. van ,(2004), *Polyphony in Architecture*, Proceedings 26th International Conference on Software Engineering (ICSE 2004), Edinburg, May 2004.

(Vos, 2009)
Fijtse Vos, (2009), *Architectuur voor de auditor: een zege of een nachtmerrie?*, XR editie 3.

(Wagter, 2001)
Wagter, R., et al. ,(2001), *DYA: snelheid en samenhang in business en ICT-Architecture.* Tutein Nolthenius.

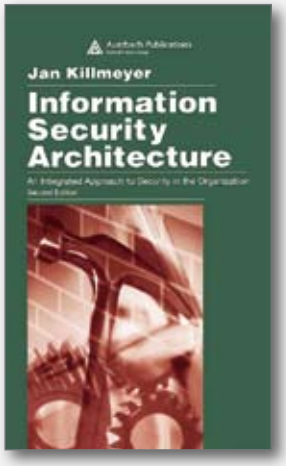
(Zachman, 1987)
Zachman, J.A., (1987), *A Framework for Information Systems Architecture.* IBM Systems Journal 26, No. 3.

Bronnen

- De GvIB Expert Brief (zie Jochem et al., 2005), zie www.pvib.nl/bibliotheek
- Waarom architectuur? Burke, op www.enterprisearchitectuur.net
- www.opensecurityarchitecture.org (zie ook artikel André Koot)
- www.sabsa-institute.org
- www.gartner.com

InZicht

Over deze rubriek > InZicht geeft een overzicht van recent verschenen en te verschijnen boeken en whitepapers in binnen- en buitenland, geselecteerd door de redactie. Onze bronnen voor de toelichting bestaan uit persberichten en internet, niet gegarandeerd onafhankelijke informatie. Actualiteit staat bij de inhoud van deze rubriek voorop.



Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition
Auteur: Jan Killmeyer
ISBN: 9780849315497
Uitgever: Auerbach Publications
Druk: 1e druk, september 2000
Vorm: paperback, 424 blz

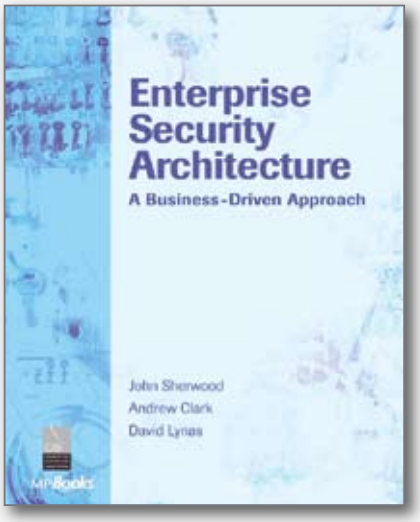
By providing clear and organized methods, this text incorporates the knowledge developed during the past decade that has pushed the information security lifecycle from infancy to a more mature, understandable, and manageable state.

Security Architecture: Design Deployment and Operations
Auteur: Christopher M. King, Curtis E. Dalton, T. Ertem Osmanoglu
ISBN: 9780072133851
Uitgever: McGraw-Hill/Osborne
Druk: 1e druk, juli 2001
Vorm: paperback, 481 blz

New from the official RSA Press, this expert resource explains how to design and deploy security successfully across your enterprise and keep unauthorized users out of your network. You'll get full coverage of VPN's and intrusion detection systems, plus real-world case studies.

Building an Effective Information Security Policy Architecture
Auteur: Sandy Bacik
ISBN: 9781420059052
Uitgever: Auerbach Publications
Druk: 1e druk, mei 2008
Vorm: paperback, 368 blz

Through the use of questionnaires, interviews, and assessments, Building an Effective Security Policy Architecture demonstrates how to evaluate an organization's culture and its ability to meet various security standards and requirements. The author provides practical guidance for building, writing, and implementing policy architecture that is designed to specifically fit within that culture. Recognizing that the effectiveness of a policy is dependent on cooperation and compliance, the author also demonstrates how to communicate that policy and provides advice on how to gain support. Samples of effective policy architecture are included.



SABSA – Enterprise Security Architecture, John Sherwood e.a.
Auteur: John Sherwood, Andrew Clark, David Lynas
ISBN: 1-57820-318-x
Uitgever: CMP Books
Druk: 1e druk, november 2005
Vorm: paperback, 608 blz

Destined to be a classic work on the topic, Enterprise Security Architecture fills a real void in the knowledge base of our industry. In a comprehensive, detailed treatment, Sherwood, Clark and Lynas rightly emphasize the business approach and show how Security is too important to be left in the hands of just one department or employee - it's a concern of an entire enterprise. Enterprise Security Architecture shows that having a comprehensive plan requires more than the purchase of security software - it requires a framework for developing and maintaining a system that is proactive.

Een interview met Alexander Baas, CIO SNS Bank

‘Weten wat het is om met je voeten in de klei te staan’

Auteur: Lex Borger > Lex Borger is Principal Consultant Information Security bij Domus Technica en redacteur van dit blad. Hij is bereikbaar via lex.borger@domustechnica.com.

Lex: “Het is al weer ruim een jaar geleden dat je CIO van het jaar werd. Hoe kijk je daar nu op terug? Hoe heeft het jou en SNS Bank veranderd?”

Alexander: “Het is mooi als je zoveel support krijgt voor je werk. Die support komt van je eigen collega’s en je wordt gezien als partij die goed omgaat met automatisering. Het maakt je als werkgever aantrekkelijk. Wij willen IT in eigen hand hebben en dat is dus een mooie spin-off naar de markt. De jury gaf aan dat we een goede visie en skills hebben en dat onze architectuur een goede combinatie van de theorie en de praktijk is.”

Lex: “Als we kijken naar drie activiteitsdomeinen binnen IT: uitvoering (het bestaande goed uitvoeren) - verandering (nieuwe elementen introduceren) - architectuur (een weg uitstippelen waarlangs dat loopt), dan zijn er natuurlijke spanningen tussen die domeinen. Kijk je als CIO ook zo tegen IT aan? En zo niet, hoe dan wel? Hoe ga je om met die spanningen tussen de activiteitsdomeinen? Is er een optimale verdeling?”

Alexander: “Wij maken verschil tussen exploitatie, ontwikkeling en architectuur, en daarnaast onderkennen we ook relatiebeheer. Al deze diensten staan op gelijk niveau en worden afgespiegeld in het management team. Er is een duidelijke taakverdeling. Architectuur is verantwoordelijk dat er goede richtlijnen en technologiekeuzes zijn, de andere bedrijfsdelen zijn verantwoordelijk dat ze deze juist implementeren.”

“Architectuur gaat over kennis en kunde. De architecten besteden veel tijd aan het landen hiervan binnen de bedrijfsonderdelen. Hierbij worden mechanismen gebruikt zoals train-de-trainer. Ook worden architecten vooraf ingeschakeld om te adviseren en te helpen. Uiteindelijk zijn alle partijen tevreden over de samenwerking. Architectuur en informatiebeveiliging hebben op papier veel macht, maar dat reikt niet tot aan de implementatie. Het is dus belangrijk dat ze backing krijgen van mij, en dat krijgen ze onvoorwaardelijk.”

“Spanningen los ik op door het managementteam in evenwicht te houden. Dit is niet vanzelfsprekend en het vergt wederzijds respect van alle partijen. Respect verdien je door ook inhoudelijk te kunnen sparren. Je moet dus weten wat het is om met je voeten in de klei te staan. Praktijkervaring uit het verleden is hierbij onontbeerlijk. Aan een ivoren toren heb je niets. We doen veel aan job rotation om deze praktijkervaring invulling te geven. Om te kunnen groeien is het nodig dat medewerkers niet alleen met hun eigen vak bezig zijn geweest. Ik zie veel bedrijven hiermee worstelen.”

Lex: “Hoe kijk je tegen informatiebeveiliging en architectuur aan? Beschouw je security architectuur apart? Of is het geïntegreerd in andere architecturen? Waar verwacht je dat een (security) architectuur voor SNS Bank een antwoord op gaat geven?”

Alexander: “Informatiebeveiliging hebben we geplaatst als staforganisatie, architectuur is een lijnafdeling. Architectuur moet op haar beurt dus werken conform de richtlijnen van informatiebeveiliging, procesmatig is dit ingebed in hun manier van werken volgens DYA (Dynamische Architectuur, http://www.dya.info - red.). Ze worden hier net zoals andere bedrijfsdelen op gecontroleerd door IB. Architectuur maakt jaarlijks het MAIS plan: het Meerjarenplan Architectuur Infrastructuur en Systeemontwikkeling. Dit is een praktische vertaling van de architectuur blauwdrukken en bevat verschillende hoofdstukken die de verschillende invalshoeken belichten. Een hiervan is informatiebeveiliging. De resultaten zijn in de hele architectuur weerspiegeld. De top-down analyse van de noodzaak voor informatiebeveiliging is belangrijk, daarna wordt het simpelweg een uitvoeringscyclus (plan-do-check-act).”

Lex: “Zijn de spanningen (zie boven) vergelijkbaar of anders als je specifiek naar security kijkt? Zijn er voor wat betreft security ook spanningen omdat security als non-functionals in verandertrajecten gezien wordt. In hoeverre zijn de aspecten risicomanagement, time-to-market en

gebruikersvriendelijkheid bij SNS Bank nu in samenhang en in de overwegingen samen gebracht?"

Alexander: "Binnen SNS bepaalt de business wat er gebeurd en IT bepaalt hoe het gebeurt. Onder het hoe valt ook een veilige implementatie waarbij met alle aspecten van BIV rekening wordt gehouden. Als de business hier in de specificaties onvoldoende rekening mee heeft gehouden, zal IT hierop wijzen. Business blijft altijd verantwoordelijk, maar kan natuurlijk wel steunen op IT dat ze voor grote risico's wordt behoed. Wij geven dit vorm middels een PSA (Project Start Architectuur)."
"Binnen SNS is er een grote transitie gaande van een kantorennetwerk naar dienstverlening over het internet. Dat kan alleen als de directie zich verantwoordelijk voelt voor de informatiebeveiliging. Vervolgens zijn er proceseigenaren en systeemeigenaren aangesteld, die de primaire verantwoordelijkheid hebben vanuit de business. Wat hierbij helpt is dat groep-audit dit duidelijk zo neerlegt. Audit-issues worden duidelijk bij de systeemeigenaar neergelegd, met een afschrift naar mij. Het is cruciaal dat het op die manier werkt."

Lex: "Hoe werkt security architectuur in de praktijk samen met de andere bedrijfsonderdelen (business, beleids-afdeling, informatievoorzienings-behoefte) binnen de SNS Bank en SNS Reaal? Wat zijn hierbij de succes-factoren?"

Alexander: "Zoals gezegd werken we met PSA's. Hier staan duidelijke eisen in.
Als hier uiteindelijk van afgeweken moet worden, wordt er een management letter naar de opdrachtgever geschreven met een uitleg van de afwijking en het tijdvak van het herstel hiervan. Daarnaast helpt het MAIS-plan alles in lijn te houden met de ontwikkelingen die gaande zijn. Hierdoor blijf je bij met alle ontwikkelingen."

Lex: "Hoe blijft de security architectuur actueel? Er zijn recentelijk toch enkele omgevingsfactoren geweest die de wereld van een bankier danig veranderd hebben, zoals outsourcing, phishing, georganiseerde cybercrime, de opkomst van social networking..."

Alexander: "Alle architectuurdocumenten, ook op het gebied van informatie-beveiliging, hebben een eeuwigdurende planning voor revisie. Ieder document komt minimaal een keer in de drie jaar aan de beurt. Bij de behandeling van revisies komen ook de nieuwe bedreigingen naar boven. Een van de architectuurdocumenten beschrijft expliciet de bedreigingen waar we onze infrastructuur tegen willen beveiligen. Als het nodig is, wordt dit document voortijdig bijgewerkt."

Lex: "Hoe kijk je tegen security en architectuurmodellen aan? Nieuwe modellen als TOGAF 9 en SABSA zijn in opkomst. ISO/IEC introduceert een heel scala aan informatiebeveiligingsnormen - de 27000 serie. CobiT wordt steeds vaker gerefereerd. Houd je je daar als CIO mee bezig? Zo ja, hoe?"

Alexander: "Uitgangspunt is dat we binnen IT voordat we iets nieuws doen goed in de markt kijken wat er beschikbaar is.
We maken volop gebruik van best practices die beschikbaar zijn, intern en extern.
We hebben CMM ingevoerd, we zijn nu op level 3. We hebben ITIL ingevoerd, we gebruiken ISO 20.000 als normenkader voor de controle op opzet, bestaan en werking.
Heel IT is gecertificeerd volgens BS7799 wat nu ISO27.001/2 heet. Ik zie TOGAF als een praktisch referentiemodel. Ik kijk primair niet naar referentiemodellen, maar naar de best practices. Deze blik levert keuzes voor referentiemodellen op.
We gebruiken DYA omdat we dit als best practice gekozen hebben. Groep-audit gebruikt CobiT om deze reden."

Lex: "Stel dat je vanuit een greenfield situatie als CIO een nieuwe SNS Bank zou mogen opzetten. Welke plaats zou je security en architectuur geven?" Wat zou je uit de huidige organisatie in dat geval absoluut niet willen kwijtraken?

Alexander: "Ik ben in de gelegenheid geweest om de IT- afdeling vorm te geven, dus greenfield of niet, ik zou het nog steeds zo doen zoals ik het nu doe.
De sleutel van het succes binnen IT is het hebben van kundige mensen, die dicht op de uitvoering zitten en die verantwoordelijkheid nemen voor wat ze doen. Binnen IT is zowel informatie-beveiliging als architectuur een logische activiteit geworden, dicht tegen de businessactiviteiten aan. Wat binnen IT gerealiseerd is willen we ook bedrijfsbreed neerzetten. We hebben vorig jaar een Regie organisatie neergezet die de business en enterprise architectuur activiteiten uitvoeren, voor een belangrijk deel bezet door ex-IT architecten die dus breder zijn gaan opereren. IT architectuur sluit hierop aan als een linking pin. Dit zal echter niet betekenen dat IT niet zijn eigen architectuurclub zou houden. Deze blijft nodig om onze eigen afhankelijkheden goed te kunnen invullen."
"Met informatiebeveiliging en business continuity is het nog niet zo ver. Dat komt nog wel, de werking vanuit IT voor het hele bedrijf is prima. Om hier ook de business in the lead te brengen moeten er nog wat stappen gezet worden."

Lex: "Waarvan lig je wakker als het gaat om informatiebeveiliging en architectuur? Wat wordt door security architectuur (modellen, raamwerken...) nog helemaal niet aangepakt?"

Alexander: "Het bankieren heeft vorig jaar een deuk in het vertrouwen opgelopen, dat is duidelijk. Het is belangrijk dat we hier goede lering uit trekken. We willen steeds meer zaken via het internet laten lopen om het centraal meer in de hand te hebben.
We hebben hier nu een voorsprong in.
Hoe houden we die? Iedereen begrijpt dat je 'netjes' met geld moet omgaan - dat bewaar je niet in de openheid, maar je stopt het juist in een veilige kluis.
De 'sense of urgency' met betrekking tot cybercrime wordt in de maatschappij nog niet op dezelfde manier gevoeld. Ik wil er graag aan bijdragen dat dit wel goed ingevuld wordt."

Open Security Architecture: een open source architectuur

Auteur: André Koot > André Koot is informatiemanager bij Univé-VGZ-IZA-Trias. Hij is ook hoofdredacteur van dit blad. Hij is bereikbaar via a.koot@unive.nl.

Als je op zoek bent naar iets over Security Architectuur kom je al snel terecht op de site van Open Security Architecture (OSA). En dat is dan ook meteen een site waar je even kunt rondhangen.

OSA is een initiatief van enkele idealisten op het gebied van het delen van kennis rond beveiligingsarchitecturen. En wat ons betreft is dat helemaal niet verkeerd. Vooral omdat deze mensen het ons mogelijk maken de kennis hieromtrent gewoon in dit blad te plaatsen: we gebruiken dezelfde vrije licentievorm, de Creative Commons licentie. Dat betekent dat we in ieder geval vrijelijk mogen putten uit de bron.

OSA project

Open Security Architecture is een doorlopend project dat gericht is op het faciliteren van bedrijven in het opstellen van een eigen security architectuur. De missie van het project luidt: 'OSA distills the know-how of the security architecture community and provides readily usable patterns for your application. OSA shall be a free framework that is developed and owned by the community'.

OSA is een bijzonder project, want met enige goede wil zou je het als een gemeenschappelijk open source-achtig project kunnen beschouwen. De organisatie achter OSA is niet strak geregeld, iedereen die mee wil doen, staat het vrij om een bijdrage te leveren in de vorm van een patroon of een model. De afzonderlijke bijdragen worden in een peer review werkwijze gepubliceerd. Iedereen die een bijdrage levert, plaatst die ter review op het forum, waarna medegebruikers daar aanvullingen of verbeteringen op kunnen voorstellen. Zoals bij elk gemeenschaps-project zijn er een paar grote leveranciers en is er een onbekend aantal afnemers.

OSA hanteert een strak Open Standaarden model. Om elke vorm van discussie rond licenties te vermijden, wordt niet alleen gebruik gemaakt van de Creative Commons licentie, maar worden alle afbeeldingen gepubliceerd in SVG-bestandsformaat, de open standaard voor vectorafbeeldingen.

Ook maakt OSA zo veel mogelijk gebruik van andere standaarden zoals de NIST 800-53 set, die als basis geldt voor de beheersmaatregelen die binnen OSA binnen de architectuur worden gepositioneerd. Daarnaast wordt ook gerefereerd aan standaarden als CobiT en de ISO 17799. OSA heeft binnen de architectuur kruisverwijzingen naar deze standaarden opgenomen.

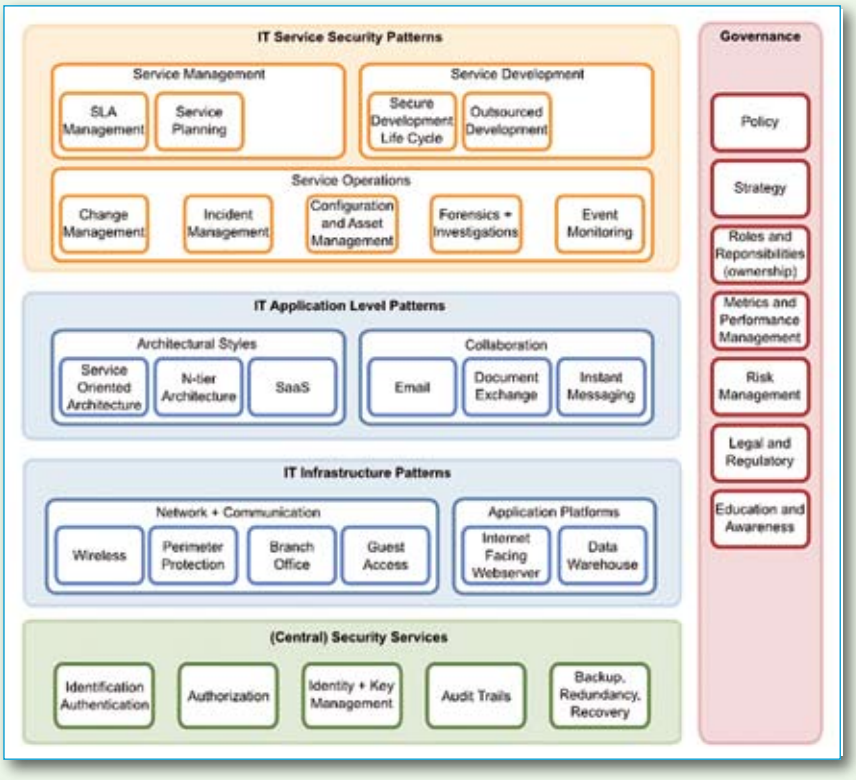
OSA componenten

OSA bevat een bibliotheek waarin patterns (patronen), Controls (beheersmaatregelen), Threats (bedreigingen), Icons (picto-grammen) en Pattern Templates (patroonsjablonen) zijn opgenomen. Daarnaast identificeert OSA Actors, ofwel de functionarissen die een specifieke rol spelen in het beveiligingsproces.

Patronen

Een patroon wordt binnen OSA gedefinieerd als een architecturele oplossing voor een probleem. Het is de bedoeling dat op termijn de patronen voor Industry Verticals geclusterd worden aangeboden, denk aan uitgewerkte security architecturen voor een branches als banken of logistieke organisaties.

De patronen zijn geclusterd in het Pattern Landscape.



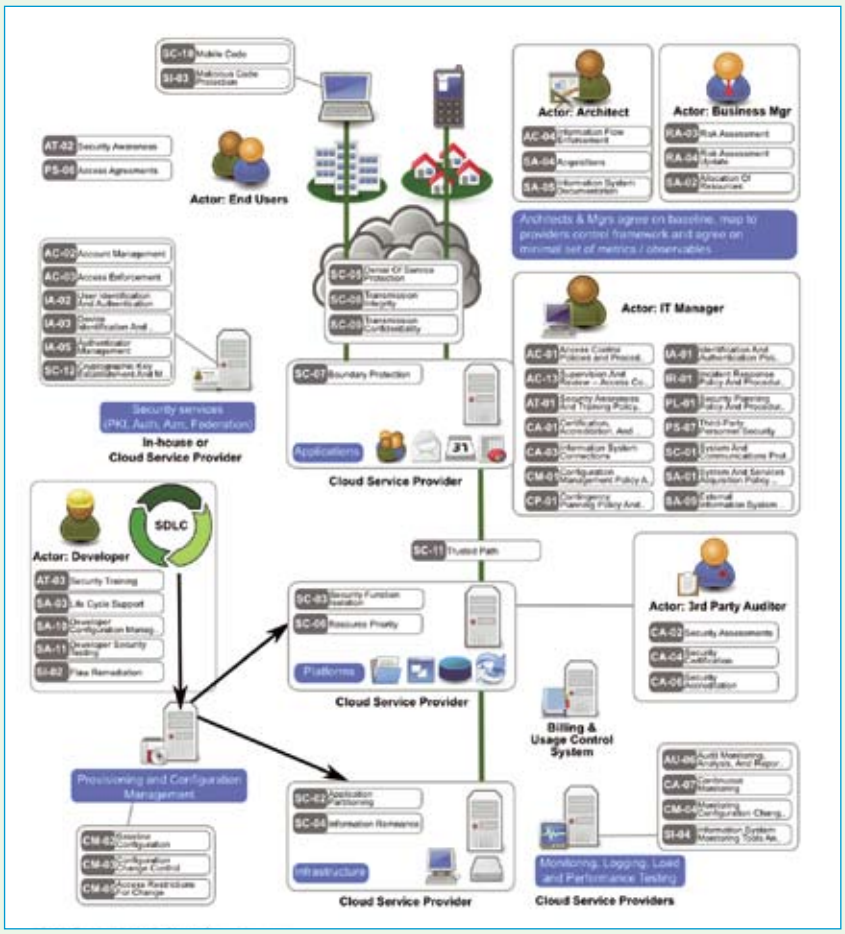
Afbeelding 1: OSA Pattern Landscape

De patronen bevatten oplossingen voor beveiligingsproblemen. Op dit moment zijn de volgende patronen beschikbaar:

Cloud Computing
Generic
Identity Management
Privacy Mobile Device
Public Web Server
SOA Internal Service Usage
SOA Publication and Location
Wireless- Using a public hotspot to access a private network
Wireless: Using a managed access point to access private network

Als een voorbeeld van een pattern pakken we gewoon de eerste, namelijk het pattern voor Cloud Computing: zie Afbeelding 2.

Dit patroon is al meteen een flinke. Het bestaat uit een groot aantal componenten, actoren en controls. Linksboven in de plaat staat bijvoorbeeld control SC-18, Mobile Code. Die ziet er als volgt uit:



Afbeelding 2: OSA pattern for Cloud Comp

SC-18 Mobile Code

Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.

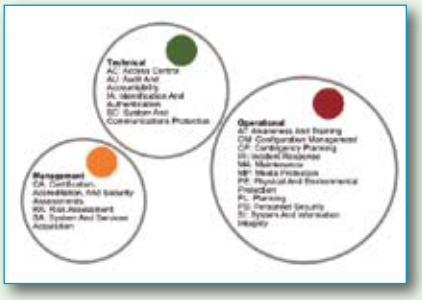
Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code.

Control Enhancements: (0) None.
Baseline: LOW Not Selected MOD SC-18 HIGH SC-18
Family: System And Communications Protection
Class: Technical
ISO 17799 mapping: 10.4.1, 10.4.2
COBIT 4.1 mapping: DS5.9 managed access point to access private network

In deze control beschrijving staat de beheerdoelstelling zelf, een uitvoerige beschrijving van de risico's, aanvullende maatregelen ((0) None), de vast te stellen Baseline (geldig of niet), de categorie (Family) en klasse (technisch) en de mapping op ISO 1799 en CobiT 4.1.

Naast de specifieke patronen zijn er ook twee modules beschreven, namelijk de module Client en de module Server. Deze beschrijvingen zijn als generieke patronen te beschouwen en bevatten een opsomming van beheersmaatregelen die voor client en server van toepassing zijn.

De controls
Zoals gezegd refereert OSA aan de beheersmaatregelen zoals die in NIST 800-53 worden gedefinieerd. Die maatregelen zijn onderverdeeld in maatregelen op het gebied van techniek, beheer en exploitatie. De naamgeving van de beheersmaatregelen is dan ook afkomstig van NIST.



Afbeelding 3: NIST Controls

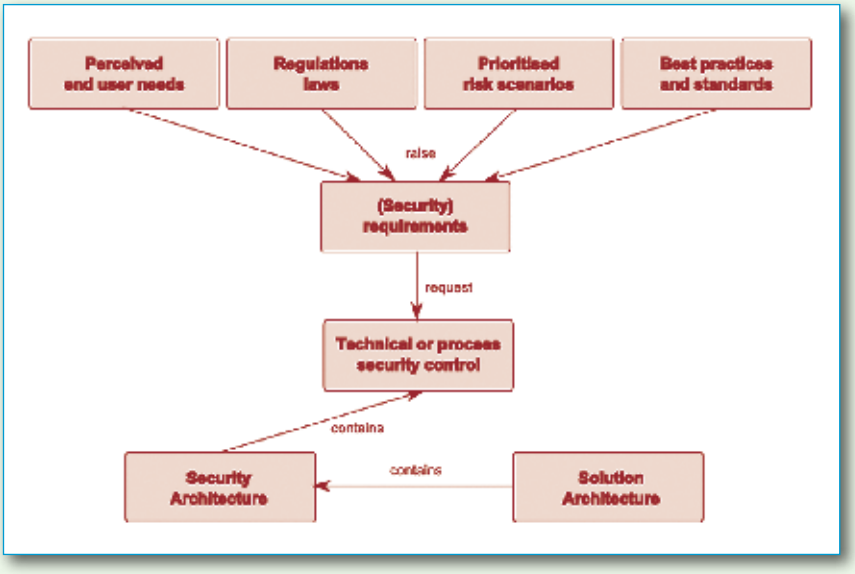
Scope van OSA

Inmiddels zijn verschillende begrippen de revue gepasseerd.

- Patroon
- Control
- Actor. Dit begrip is nog niet voldoende ingevuld. Hiervoor wordt momenteel nagedacht over het aansluiten bij het rolbegrip uit Owasp of uit ITIL v3.

OSA voegt aan de bekende begrippen in ieder geval een grafische interface toe, zodat de samenhang ook visueel vormgegeven wordt.

OSA richt zich met name op IT Security. Handig is in dit verband de mapping van NIST op CobiT en ISO17799 die op de site te vinden is.
Dat betekent niet dat de functionele kant van informatievoorziening buiten beschouwing blijft. Zo worden diverse controls beschreven die invloed moeten hebben op de bedrijfsvoering zelf. OSA hanteert het volgende model om te komen tot de functionele eisen die leiden tot de security architectuur:



Afbeelding 4: OSA Functional requirements

In deze figuur is te zien dat de requirements feitelijk allemaal uit de business optiek ontstaan.

Architectuur

Voldoet OSA aan de definities van een architectuur? Ja. Maar dat is niet zonder meer een goed antwoord. Zoals al elders vermeld is het begrip architectuur niet echt eenduidig te beschrijven. Als je het begrip Samenhang als een kernbegrip hanteert, dan is het antwoord in ieder geval 'ja'.
OSA maakt het mogelijk om beveiligingsrisico's en maatregelen in samenhang te beschouwen en daarmee kan het als uitgangspunt en als toetsingskader worden gehanteerd. Maar het OSA is nog niet klaar, het is vermoedelijk nog niet helemaal evenwichtig.

Mogelijkheden

OSA heeft nogal wat informatie en je mag er (binnen de CC licentie) vrijelijk uit putten. Als je het op de keper beschouwt, heb je in no-time een hele security architectuur bij elkaar gesprokkeld. Kies je patronen en controls, een paar teksten vertalen en klaar is kees. Maar er zit meer in. Het biedt natuurlijk de mogelijkheid om binnen de gemeenschap te komen tot een standaard architectuur die ook als toetsingskader bruikbaar is. Hoe groter de gemeenschap, hoe groter de kans ook dat het framework breed gedragen als een standaard toegepast kan worden.

Conclusie

OSA is niet klaar. OSA bevat geen uitgewerkte toolkit, geen uitgewerkte processen, onvoldoende patronen en maatregelen. OSA hanteert ook niet alle standaard architectuurbegrippen zoals Principe en Rationale. De naamgeving wijkt af (al is de inhoud wellicht wel te herkennen). Dat maakt het op dit moment misschien lastig om OSA te integreren in andere frameworks zoals SABSA, TOGAF, IAF, noem maar op. Misschien is OSA eerder te zien als een operationeel, dan als een tactisch framework. Misschien moet het nog verder groeien, zowel in concept als in implementatie.

Er is op dit moment nog geen bedreigingen catalogus. De belangrijkste reden voor het ontbreken hiervan is misschien ook wel de licentievorm. Bekende overzichten (denk aan BITS) zijn niet vrij toegankelijk en mogen daarom niet worden gebruikt. Om die reden is OSA niet meteen als input te gebruiken voor CRAMM-achtige analyses. OSA gebruik je vooral voor de top down, 'principle' gebaseerde benadering.

Vanuit het PvIB zouden we het OSA initiatief misschien moeten ondersteunen. Niet alleen omdat we dezelfde licentievorm hanteren (lekker makkelijk), maar ook omdat we binnen de vereniging met het expert brief initiatief feitelijk een soortgelijk proces doormaken: het door experts van verschillende pluimage samenwerken aan het laten ontstaan van kennis en het ontsluiten van die kennis, alles om bij te dragen aan een hoger niveau van beveiliging. Ook Ibpedia.nl lijkt heel veel op OSA. Me dunkt dat beide sites elkaar zouden moeten kennen.

Bronnen

OSA Website:
http://www.opensecurityarchitecture.org
NIST 800-53:
http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

Beveiligingsarchitectuur in Jericho-stijl

Auteur: Aaldert Hofman > Aaldert Hofman CISA werkt bij Capgemini onder andere in de rol van security architect en werkt voornamelijk binnen Financial Services. In de afgelopen jaren heeft hij zich verdiept in nieuwe technologieën als mashups en de impact daarvan op security. Hij is bereikbaar via Aaldert.Hofman@capgemini.com.

Het wordt hoog tijd dat we eens wat verder komen dan de obligate introductie tot Jericho en de Jericho Principes. Wat betekent Jericho in de praktijk van een bedrijf? Dit artikel gaat in op hoe je van een perimeter model (P-model) naar een deperimeterized model (DP-model[1]) komt en welke van de Jericho principes daar direct invloed op hebben. Hoe ziet zo'n DP-model er uit en hoe definieer je dat? De rol van classificatie wordt toegelicht. Welke principes liggen hieraan ten grondslag en welke principes zijn het gevolg van het nieuwe model? Kennis van Jericho, van architectuur en natuurlijk van informatie-beveiliging verwachten we als voorkennis.

Jericho-principes voor een DP-model

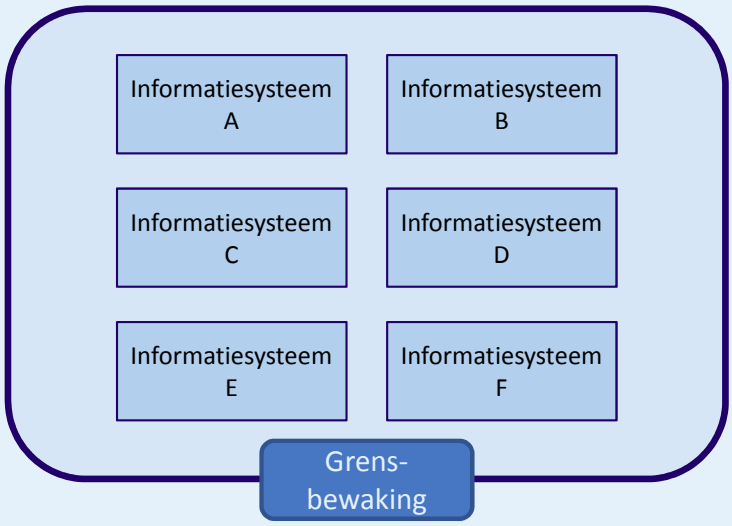
Het Jericho Forum (www.JerichoForum.org) is een internationale kennisgroep is op het gebied van IT-beveiliging , opgericht om nieuwe oplossingen te ontwikkelen die nodig zijn voor de beveiliging van IT-systemen in de open wereld. Het Forum stelt dat de traditionele benadering waarbij het afdoende is dat een firewall de grenzen van het netwerk bewaakt niet langer op gaat. Het traditionele onderscheid tussen 'jouw' en 'ons' netwerk verdwijnt.
Het Jericho Forum noemt deze ontwikkeling 'de-perimeterization' (ontgrenzing).

Het Jericho Forum definieerde de 11 Jericho Commandments (Jericho-principes). Deze kunnen worden gezien als de ontwerpprincipes die de meest essentiële requirements omvatten voor IT-beveiliging in een wereld zonder grenzen. De aan-bevelingen dienen als referentiekader waaraan concepten, oplossingen, standaarden en systemen kunnen worden getoetst.
In het kader van dit artikel zijn vooral drie van de 11 Jericho principes van belang. Zijn de overige Jericho principes dan niet meer nodig of zijn ze minder belangrijk? Nee, dat is de verkeerde conclusie. Puur voor de scope van dit artikel ligt de focus op de principes 1 en 6. Voor een volledig overzicht verwijs ik naar de site van het Jericho Forum.

Jericho Principe 1 – P en DP model

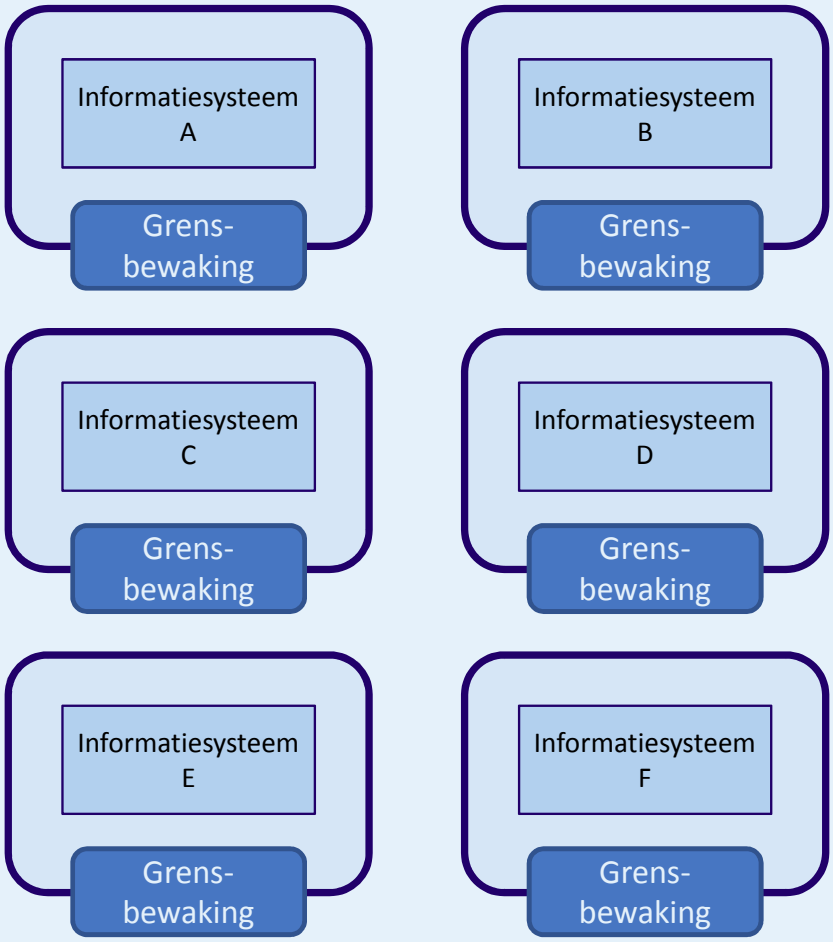
De letterlijke tekst van Jericho Principe 1 luidt: *'The scope and level of protection should be specific and appropriate to the asset at risk'*.
Deze eerste aanbeveling omvat de basisbeginselen van een visie op een bestaan zonder grenzen. De bedrijfsvoering vereist dat informatiebeveiliging een flexibele bedrijfsvoering mogelijk maakt en tegelijkertijd kosteneffectief is. Terwijl aan de ene kant de firewall op de grens van het bedrijfsnetwerk een basisniveau aan beveiliging blijft bieden, moeten de individuele systemen en data (assets) in staat zijn om zichzelf te beschermen.

Daarbij moeten we bedenken dat een asset beter is te beschermen naarmate de bescherming dichter op het asset wordt geboden.
Om nog maar weer eens het grootste misverstand rondom Jericho uit de wereld te helpen: Jericho schrijft beslist niet voor dat de traditionele firewall moet verdwijnen! Duidelijk wordt aangegeven dat de traditionele firewall aan de buitengrens van een organisatie kan blijven, maar niet langer toereikend is als enige maatregel. Individuele systemen, diensten en zelfs gegevens dienen aanvullende maatregelen te treffen en zo mogelijk zichzelf te beschermen.



Figuur 1 - Traditioneel P-model

[1] In navolging van het Jericho Forum zelf in het Jericho Position Paper over Cloud Cube Model, hanteer ik de afkorting P-model, respectievelijk DP-model voor een Perimeter Model cq een Deperimeterized Model.



Figuur 2 - Volledig DP-model

In het traditionele P-model met een generieke grensbewaking, meestal bestaande uit (een systeem van) firewalls, worden alle informatiesystemen op dezelfde manier beschermd. Besef daarbij wel dat de afzonderlijke informatiesystemen normaal gesproken ook nog beschermd zijn door bijvoorbeeld specifieke autorisaties of functiescheiding.

In de praktijk manifesteert een traditioneel P-model zich meestal als een rekencentrum, waarbij een intern en een extern netwerk wordt onderscheiden. De grens tussen intern en extern netwerk wordt zwaar bewaakt, maar eenmaal op het interne netwerk wordt er geen of weinig onderscheid gemaakt tussen de informatiesystemen.

Nemen we nu Jericho Principe 1 ter harte, dan moet de scope en het niveau van beveiliging specifiek en toepasbaar zijn voor het specifieke informatiesysteem dat we moeten beveiligen. Dat zou leiden tot het DP-model uit figuur 2. Waarschijnlijk bekruipt u hetzelfde intuïtieve gevoel als bij mij: kan dat nou niet handiger? Ja, maar daarvoor hebben we een ander Jericho principe nodig.

Jericho Principe 6 - Een geclassificeerd DP-model

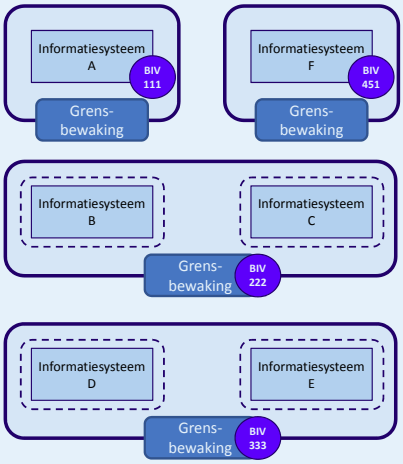
De letterlijke tekst van Jericho Principe 2 luidt: 'All people, processes, technology must have declared and transparent levels of trust for any transaction to take place'. Dit Jericho-principe geeft aan dat in deze context 'trust' uitgelegd moet worden als het tot stand brengen van wederzijds begrip bij de betrokken contractuele partijen in een transactie, inclusief de verplichtingen die dit voor deze partijen met zich meebrengt. Dit lijkt een wollige zin, maar dat blijkt mee te vallen zoals ik later in dit artikel zal laten zien.

Verder geeft dit principe aan dat een vertrouwensmodel zowel de mensen en organisaties, als ook de apparatuur en infrastructuur moet omvatten. Het vertrouwensniveau kan verschillen naar locatie, transactie, rol en het risico in de transactie.

Jericho Principe 6 heeft als doel om modellen en technologieën inter-operabel te maken om heldere en transparante niveaus van vertrouwen te realiseren. Dat is mooi, maar dat kan ook een enorme hoeveelheid werk met zich meebrengen om alle mensen, processen en technologie te voorzien van een bekend en transparant niveau van vertrouwen. Het is veel handiger om aan te sluiten bij een vertrouwd mechanisme, namelijk classificatie. Ik neem aan dat er al een classificatieschema in de organisatie wordt toepast. Voor de eenvoud laat ik de discussie of je nu processen, informatiesystemen of servers moet classificeren even voor wat het is.
Evenmin ga ik in op het opstellen van een goed classificatieschema.

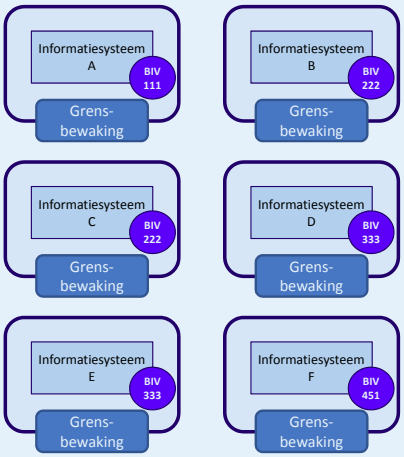
Voor dit artikel is mijn aanname dat er een goed gedefinieerd classificatieschema is met een oplopende classificatie van 1 tot en met 5 voor elk van de aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid. Dit schema is bekend en transparant zowel binnen als buiten de organisatie. Bovendien is voor elk informatiesysteem de BIV-classificatie bepaald en bekend, zoals in figuur 3 aangegeven. Daarmee zijn we al een heel eind op de goede weg om Jericho Principe 6 toe te passen in de praktijk.

De volgende stap ligt voor de hand: het definiëren van domeinen waarin



Figuur 3 - Volledig DP-model met classificatie

informatiesystemen met dezelfde classificatie ondergebracht worden. Vervolgens laten we de afzonderlijke grensbewaking voor die informatiesystemen vervangen door de grensbewaking van het domein (figuur 4).



Figuur 4 - Geclassificeerd DP-model

Merk op dat een geclassificeerd DP-model waarin alle informatiesystemen dezelfde classificatie hebben in feite overeenkomt met het P-model. In die situatie adviseer ik om het toegepaste classificatieschema of de uitgevoerde classificatie nog eens goed te evalueren.
Merk bovendien op dat een belangrijke reductie in complexiteit ontstaat omdat ik in dit voorbeeld de classificatie per informatiesysteem heb genomen. Strikt volgens Jericho Principe 6 is dit te grof en dient de classificatie per proces of per transactie (of per service) uitgevoerd te worden. In dat geval neemt de complexiteit enorm toe.
Wellicht is het u opgevallen dat het vertrouwensniveau van personen tot nu toe buiten beschouwing is gebleven. Daarover in de volgende paragraaf meer.

Een Multi Level Trust Model

Jericho Principe 6 vraagt ook voor personen een Trust Model met meerdere niveaus. Ik verwijs graag naar mijn publicatie over dat Multi Level Trust Model in Informatie[2] of naar de presentaties van de auteurs bij de RSA Conference of de Open Group conference. Enkele aspecten uit die publicatie zijn ook nu van belang.

In het kort: bij het definiëren van zo'n model worden drie stappen doorlopen.

In stap 1 wordt vastgesteld welke niveaus van betrouwbaarheid voor personen worden onderkend, inclusief naam en definitie.
In stap 2 wordt vervolgens vastgesteld welke transities tussen de niveaus mogelijk zijn. In stap 3 ten slotte worden de transitiecriteria bepaald, inclusief de meetbare criteria die per transitie aangeven onder welke condities een transitie wordt uitgevoerd. De volgende alinea's behandelen deze stappen in meer detail.

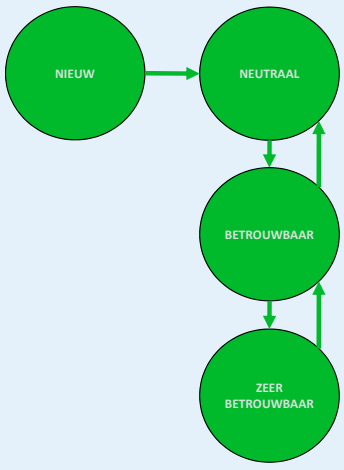
In stap 1 dienen twee belangrijke vragen zich aan: hoeveel niveaus onderkennen we en welke zijn dat dan? Als we kijken naar de normale gang van zaken binnen een organisatie met medewerkers, ligt het eerste niveau voor de hand. Een organisatie weet immers niets over een nieuwe medewerker en elke medewerker krijgt het voordeel van de twijfel. Een nieuwe medewerker krijgt een neutrale, blanco status, namelijk die van 'nieuw'. Zodra de eerste werkdag een feit is, krijgt de medewerker kleur. Hij of zij begint met een geloofwaardigheid van nul en brengt daar verandering in door betrouwbaar te handelen. Het werk wordt uitgevoerd. Dat is conform de verwachting en de medewerker krijgt het niveau 'betrouwbaar'.

Het kiezen van de naam van het niveau is belangrijk. De status 'nieuw' impliceert dat men daar nooit meer naar terug kan. Want wat er ook gebeurt, het is positief of negatief en de medewerker wordt nooit meer een nieuweling. Ter aanvulling definiëren we het niveau 'neutraal' voor de reguliere medewerkers die zich niet bijzonder positief of negatief onderscheiden.

Op basis van een normale gang van zaken ontstaat zo al snel een model met drie niveaus van vertrouwen: nieuw, neutraal, betrouwbaar. Dit basismodel is breed toepasbaar en organisaties kunnen het naar wens aanpassen. Het belonen van loyale medewerkers kan een reden zijn om een extra niveau te definiëren: zeer betrouwbaar.

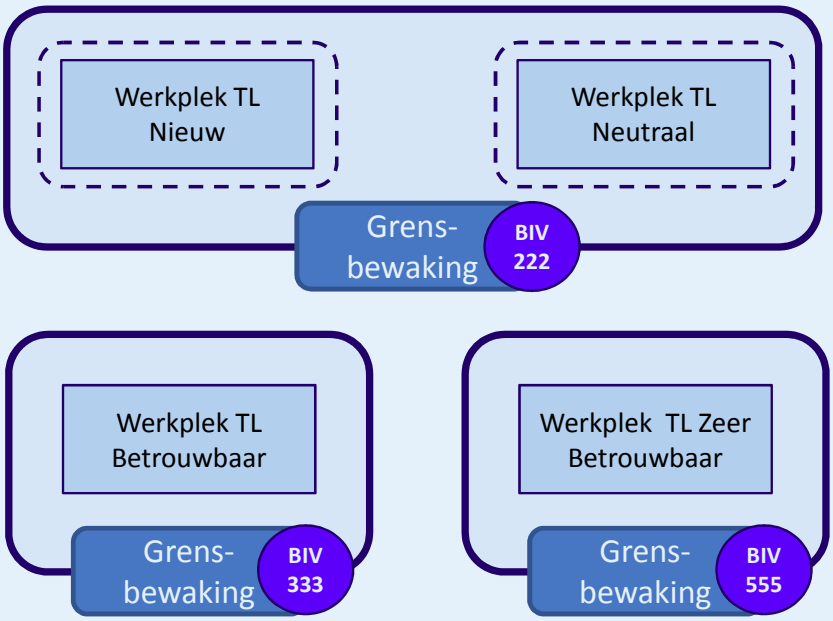
Het definiëren en benoemen van de niveaus alleen is niet voldoende. Welke overgangen tussen deze niveaus zijn mogelijk? Daarvoor dient in stap 2 het toestandsdiagram met mogelijke transities gedefinieerd te worden.
Bij het maken van het toestandsdiagram spelen interessante vragen. Wanneer verliest de medewerker de status 'betrouwbaar' en naar welke status gaat die dan? Naar 'neutraal' of direct door naar 'zwarte lijst' of 'onbetrouwbaar'? Leggen we bij een medewerker die een keer een foutje maakt gelijk een zware straf op door de status te veranderen? Door dergelijke vragen te beantwoorden en in kaart te brengen ontstaat het toestandsdiagram met mogelijke overgangen.

Na het vaststellen van het toestandsdiagram is het model bijna compleet. De niveaus zijn onderkend en de toegestane transities eveneens. Maar onder welke voorwaarden welke overgang wordt uitgevoerd, is nog niet vastgesteld. Dat is stap 3.
De criteria die definiëren welke transities mogelijk zijn, moeten specifiek en meetbaar zijn, want anders is het niet mogelijk om het betrouwbaarheidsniveau automatisch vast te stellen.
Voor een voorbeelduitwerking van een Multi Level Trust Model verwijs ik u graag naar de eerder genoemde publicatie en naar het Trust Framework zoals dat binnen de Open Group ontwikkeld wordt. Voor dit artikel is het voldoende om als resultaat van het gedefinieerde model aan te nemen dat we voor medewerkers vier niveaus van vertrouwen onderkennen: nieuw, neutraal, betrouwbaar en zeer betrouwbaar (figuur 5).



Figuur 5 - Multi Level Trust Model voor medewerkers

[2] 'Waar baseert u dat vertrouwen op?', door John Sluiter en Aaldert Hofman, Informatie, mei 2008



Figuur 6 - DP-domeinen voor werkplek per Trust Level

De status 'niet te vertrouwen' komt niet voor in het model, omdat die medewerkers niet meer bij de organisatie werken.

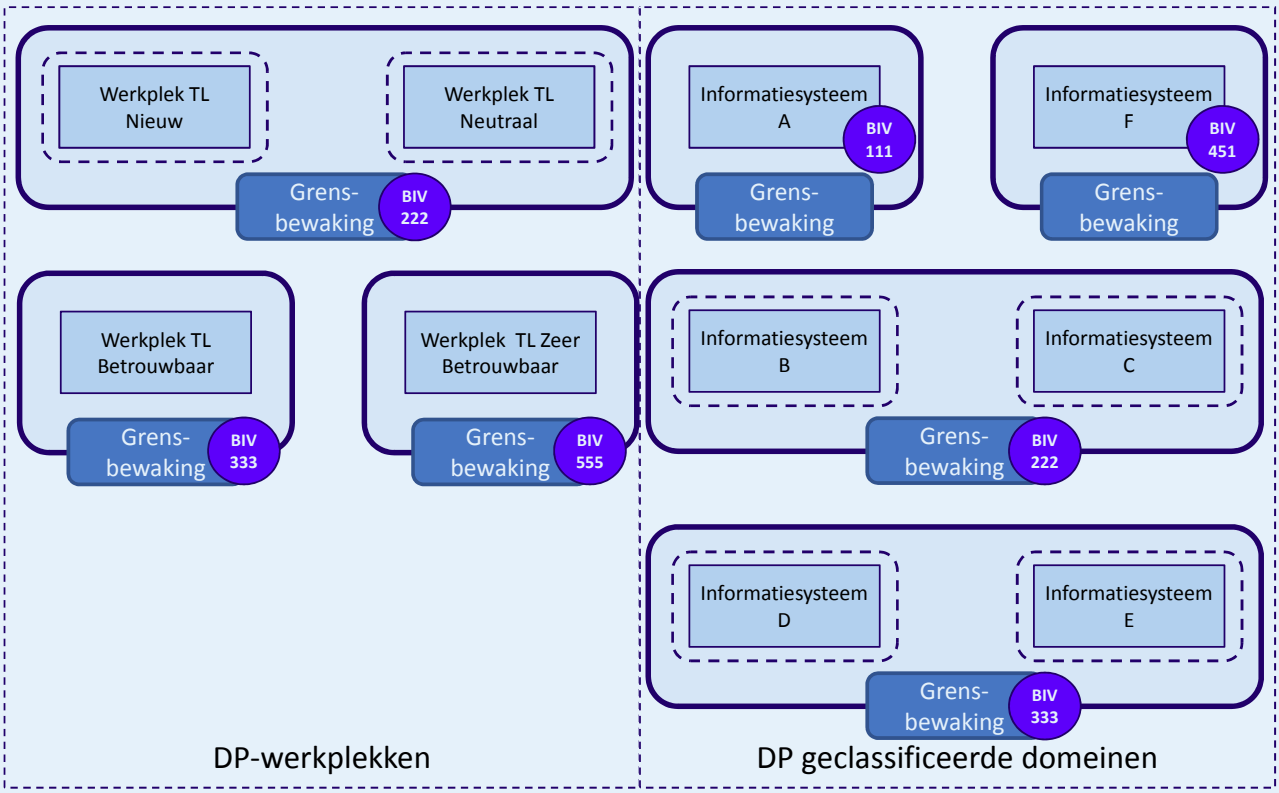
DP-model en Trust Levels gecombineerd

Het laatste stapje dat we moeten zetten om Jericho Principe 6 zo volledig mogelijk invulling te geven, is het combineren van het DP-model en de Trust Levels. Dat doen we door een tabel te definiëren waarin voor elk Trust Level aangegeven staat welke geclassificeerde DP-domeinen (en daarmee de informatiesystemen in dat DP-domein) zij mogen gebruiken.

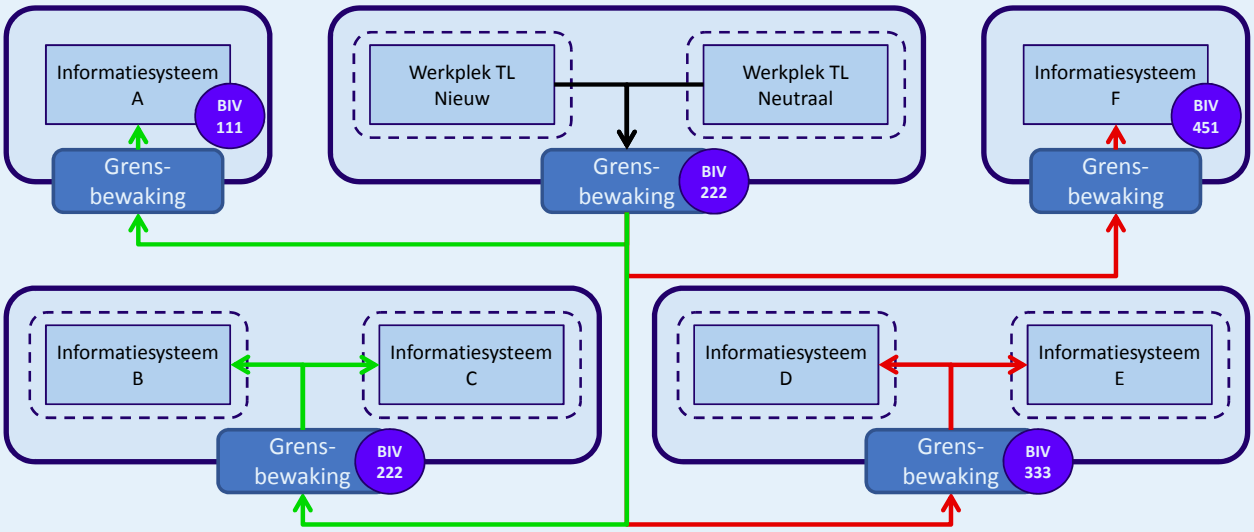
Let wel, hiermee wordt niet gesteld dat daarmee ook autorisatie wordt gegeven tot gebruik van alle functionaliteit van al die informatiesystemen! Zoals eerder al aangegeven, de autorisaties per informatiesysteem zijn aanvullend ten opzichte van de DP-domeinen.

Trust Level	Mag DP-domeinen gebruiken met
Nieuw	Classificatie 222 of lager
Neutraal	Classificatie 222 of lager
Betrouwbaar	Classificatie 333 of lager
Zeer betrouwbaar	Classificatie 555 of lager

Ook in de Jericho-stijl architectuur geldt nog steeds dat beveiliging over de hele keten verzorgd moet worden, dus dat is tot en met de werkplek van de medewerker. Onafhankelijk van de soort werkplek, de locatie of de randapparatuur die gebruikt wordt. Dat impliceert dat we in het DP-model ook enkele domeinen op moeten nemen voor de werkplekken van de medewerkers (figuur 6).



Figuur 7 - Het totale DP-model



Figuur 8 - Interactiemodel vanuit Trust Level Nieuw of Neutraal

Daarmee komt het totale DP-model er als volgt uit te zien (figuur 7), waarbij we in totaal zeven verschillende domeinen onderkennen. Drie domeinen voor de werkplekomgevingen van de medewerkers en vier geclassificeerde domeinen voor de informatiesystemen.
In de werkelijkheid van veel organisaties zal dit model te simpel blijken, bijvoorbeeld omdat:

- Naast de medewerkers zijn er meer actoren met werkplekken te onderkennen, zoals daar zijn: klanten en potentiële klanten, business partners als intermediairs, toeleveranciers of afnemers, dienstverleners waaraan een deel van de IT of zelfs hele bedrijfsprocessen zijn uitbesteed. De diversiteit en complexiteit in werkplekomgevingen wordt enorm.
- In theorie kan er voor elke mogelijke BIV-combinatie een apart domein gedefinieerd worden. Bij vijf verschillende classificatieniveaus leidt dit tot maximaal 5 * 5 * 5 = 125 verschillende domeinen. Dat is in de praktijk niet werkbaar en in de praktijk zullen ook lang niet alle combinaties voorkomen. Maar het aantal van vier verschillende geclassificeerde domeinen uit dit artikel is wel aan de lage kant.

Tot nu toe is in dit model niet in kaart gebracht welke communicatie tussen welke domeinen nu wel of niet toegestaan is. De bron daarvoor is de eerder gedefinieerde tabel. In een DP-model met deze werkomgevingen zijn de consequenties voor wat betreft de informatiebeveiliging en de interacties tussen deze werkomgevingen:

- Interactie tussen logische werkomgevingen die hetzelfde BIV-niveau leveren vereist geen specifieke additionele beveiligingsmaatregelen anders dan de reguliere bescherming van de interactie (en die reguliere bescherming biedt beveiliging tot het gespecificeerde niveau).
- Interactie tussen logische werkomgevingen die niet hetzelfde BIV-niveau leveren, vereist wel degelijk additionele beveiligingsmaatregelen om de interactie veilig te doen zijn.

Als voorbeeld toont figuur 8 het interactiemodel gezien vanuit de werkplekomgevingen met Trust Level Nieuw of Neutraal.

Jericho Principe 7 - Samenwerking met anderen

Nog even een woord over Jericho Principe 7, dat stelt dat betrouwbaarheidsniveaus nu veelal eenzijdig worden bepaald, omdat er meestal geen mogelijkheid is tot wederzijdse vaststelling van dit niveau. Het Jericho Forum zoekt naar juist wel naar wederzijds vast te stellen betrouwbaarheidniveaus. Dat is nodig zowel bij communicatie tussen gebruikers en services als tussen services onderling.

Op zich zal samenwerking met anderen niet hoeven te leiden tot aanpassing van het DP-model. Immers, het is juist een DP-model omdat we in een wereldwijd met elkaar verbonden wereld leven. Juist door het afschaffen van de grenzen, of meer correct gezegd het opnieuw definiëren of inrichten van de grenzen, wordt de samenwerking met andere partijen eenvoudiger.

Waar in de samenwerking wel nadrukkelijk aandacht aan moet worden besteed, is aan de gedefinieerde Trust Levels en aan de inzichtelijkheid en transparantie van de classificatie. Want alleen in dat geval kan wederzijds het niveau van vertrouwen goed vastgesteld worden.

Concluderend

Het definiëren van een Jericho-stijl security architectuur is goed mogelijk. Het Perimeter-model is met behulp van classificatie van de informatiesystemen en met behulp van Trust Levels voor de medewerkers goed om te zetten naar een De-Perimeter-model. In deze worden met name de Jericho Principes 1 en 6 toegepast.

Functionarissen in de Informatiebeveiliging

Auteur: Tom Bakker > Tom is lid van de redactieraad van Informatiebeveiliging en te bereiken via tom_bakker@deltalloyd.nl

Voor de aftrap voor de reeks Functies in de Informatiebeveiliging in de praktijk heeft Tom Bakker Ronald van Erven, Information Risk Officer bij de Grafische Bedrijfs Fondsen (GBF) geïnterviewd. In dit themanummer over Architectuur zal nader worden ingegaan op de functies Business Information Security Architect (BISA) en Information Security Architect (ISA).

Wat heb je zoal gedaan in de informatie beveiliging en wat doe je nu?
"Ik werk sinds 1994 in informatie-beveiliging. Ik ben begonnen als network/ system specialist en in de periode 2000-2008 ben ik IT security officer en IT security manager bij Versatel en Translink geweest. Tegenwoordig heb ik een modernere naam voor information security officer (ISO), namelijk information risk officer bij GBF op de afdeling Risk & Compliance Management. In de wandel-gangen heet het nog steeds ISO, misschien wel omdat IRO niet klinkt.
Maar what's in a name? Belangrijkste is leuk en uitdagend werk in het vakgebied. Iets dat ik eigenlijk niet als werk zie, maar een uit de hand gegroeide hobby. Het leukste is de hoeveelheid creatieve mensen die je tegenkomt. Mensen die er alles aan doen om richtlijnen, beleid, beheer en architecturen proberen te omzeilen."

Hoe kijk je aan tegen architectuur en security in het bijzonder?
"De trend die ik bij mijn werkgevers inzet is dat security en dus het 'security architectuur-denken' een nutsvoorziening is en dat het security-denken onderdeel moet zijn bij de ICT en business architecten. Een dedicated ISA is in elk geval bij de bedrijven waar ik werk geen optie. Het is meer een rol die iemand die zich architect noemt automatisch moet nemen en hij wordt getoetst door of de IAD of door de ISO/IRO (information security officer/ information risk officer)."

Informatie Beveiliging of ICT Security als nutsvoorziening. Net als dat je de kraan open doet en veilig drinkwater krijgt, moet de organisatie (lees: de eindgebruiker) op veilige ICT en informatie kunnen vertrouwen zonder de exacte eisen en infrastructuur te kennen. De eindgebruiker van het drinkwater weet globaal wat regels en eisen over drinkwater zijn en kan erop vertrouwen dat ze het kunnen gebruiken, tot men instructies krijgt over dat het niet veilig is en dat men bijvoorbeeld het water moet koken. Ditzelfde geldt voor ICT en ICT-beveiliging. De organisatie moet globaal van de hoed en de rand weten en de ICT-fabriek zorgt ervoor dat de ICT veilig is. Dit houdt in dat informatiebeveiliging in de genen van ICT-ers moet zitten en dat elke manager in die ICT-fabriek aan (information) risk management moet doen. De security specialist (IRO/IRM/ ISO) heeft dan een faciliterende rol en moet mensen bijstaan met oplossingen en scherp zijn op risico's die over het hoofd worden gezien. Een soort tweede- of derdelijns-beveiligings schil.

Welke rol heb jij met betrekking tot security architectuur?
"Wat opvalt is dat veel mensen zich tegenwoordig security architect noemen, maar zich slechts op de techniek richten. Een architect of iemand die het security architect-denken in zich heeft doet meer. Kortom; ik heb wat als ISA (want dat is een deelrol van mij) maar ik probeer altijd die informatiebeveiligingsarchitectuur kennis zoveel mogelijk bij de ICT en business architecten in te brengen. En tot op heden lukt dat aardig."

Kennen jullie een BISA en/of een ISA bij GBF?
"De BISA functie bestaat niet als zodanig, maar de taken worden wel uitgevoerd door business architecten en proces architecten. De ISA functie heet bij ons ICT Architect. Maar ook dit is een verzamelnaam voor netwerk, software/database of systeem architect. De ISO heeft een faciliterende werking en helpt het architectenteam. Het is een doel van de ISO om het kennisniveau qua beveiliging in het architectenteam op peil te brengen en te houden. Maar in de praktijk blijkt dat de businessarchitecten een goed zicht hebben op de informatie in hun bedrijfsprocessen en de waarde van die informatie in relatie tot de CIA begrippen vanuit informatiebeveiliging. Maar de business- en proces architecten kunnen ook goed inschatten waar men controle of beveiligingmaatregelen zou willen nemen en als dit een ICT maatregel is dan komt men bij de ICT architecten. En in samenspraak maken zij een technische-, procedurele- of bewustmakingsmaatregel."

Op welke plek binnen in organisatie hoort een security architect thuis?
"Het in de PvIB studie (functies in de informatiebeveiliging) geschetste principeplaatje van een organisatie vind ik teveel schijven en hokjes en zeker niet slagvaardig. Wij hanteren onderstaand schema.

Het werkt als volgt: je hebt drie omgevingen: Controleren en Richting geven, Bouwen en Operationaliseren en Onderhoud en Beheer."

"Bij controleren en richting geven wordt aan risico management en compliance management gedaan en geeft men richtlijnen t.b.v. informatiebeveiliging. Rapporterend aan de manager Risk & Compliance."

"Bij Onderhoud en Beheer zorgt men ervoor dat de huidige ICT omgeving probleemloos loopt. Indien er een nieuwe functionaliteit bij komt, dan stellen zij aansluit- of acceptatiecriteria op. Rapporterend aan de ICT operations manager."

"Bij Bouw en Operationalisering vertaalt men alle (acceptatie) eisen en richtlijnen in business- en ondersteunende ICT architecturen en bewaakt men deze blauwdrukken, inclusief de gestelde eisen vanuit het bedrijfbeleid, ICT beleid, risico & compliance management en de acceptatiecriteria vanuit beheer. Het is in deze groep die, naast de innovatie en bewaking van de architecturen, ook de beleidsdocumenten in beheer heeft en deze operationaliseert. Voordeel is dat de business en ICT architecten veelal betrokken zijn bij beleidsvorming. Maar het voordeel wordt nog groter als zij het beleid en hun architecturen mogen operationaliseren. Zo blijven de architecten een gevoel met de 'werkelijke' wereld en bedrijfsvoering houden.
De architecten hebben als direct leidinggevende een manager Innovatie en Ontwikkeling met een functionele sturing vanuit het business management. En innovatie houdt niet in continu nieuwe technologieën naar binnen halen, maar ook continu verbeteren en 'fine-tunen' om zo de beste efficiëntie en effectiviteit te krijgen in de processen en ondersteunende ICT."

"Vervolgens is het richtlijnen geven aan de ICT architecten. Zij ontwerpen en bouwen. Daarna wordt er getest en worden de acceptatiecriteria gecontroleerd, waarna de ICT architectuur in beheer kan worden genomen. Door steeds weer te meten en te rapporteren door de service manager en aan de hand van een jaarlijks good-control-program (audit programma, incl. technische audits) uit te voeren door de ISO, kan de organisatie continu verbeteren."

Wat vind je van de competenties en het opleidingsniveau?
"Zowel de business architect, proces architect of ICT architect zitten op HBO niveau, dan wel Master, en zijn in elk geval lid van het PvIB. Certificeringen zijn niet nodig, maar helpen wel en hebben puur tot doel dat vakgenoten dezelfde taal spreken en elkaar via een professioneel netwerk snel kunnen vinden."

"Belangrijkste is ervaring. Je kunt niet van de hogeschool of universiteit komen en je gelijk architect noemen. Je mist de ervaring. Degenen die de investering doen en eerst in de operatie gaan werken, hebben het beste gevoel voor de business en het vakgebied. Degenen die dan na vijf jaar de sprong naar 'bouwen en operationaliseren' maken, zijn vaak de beste architecten, pragmatisch ingestelde bouwers met een goede helikopterview over het hele speelveld van de architecten. Globaal hanteer ik onderstaande tabel met een eigen invulling op de competenties.

Interviewkandidaten
Voelt u zich na het lezen van dit interview geroepen om ook geïnterviewd te worden over uw mening over of ervaring met Functies in de Informatiebeveiliging? Meldt u zich dan aan als interviewkandidaat bij Tom Bakker. Hij is bereikbaar via Tom_Bakker@deltalloyd.nl.

	WO – HBO – MBO	Certificaten	Ervaring in jaren	Competenties (uit de PvIB functie in IB rapport)
Controleren	HBO+; RE;	CISA of CISSP	5>	- Integriteit - Omgevingsbewustzijn - Organisatiesensitiviteit - Overtuigingskracht - Stressbestendigheid - Visie - Analytisch vermogen - Doorzettingsvermogen - Voortgangsbewaking
Focus op ICT Architecten	HBO+;	CISSP; product certificaten	5>	- Integriteit - Omgevingsbewustzijn - Organisatiesensitiviteit - Overtuigingskracht - Visie - Analytisch vermogen - Creativiteit - Initiatief - Samenwerken
Beheerders	MBO/HBO;	willen leren! (voor certificaten + CISSP)	starters	- Doorzettingsvermogen - Leiderschap - Integriteit - Analytisch vermogen - Kwaliteitsgerichtheid - Leervermogen - Resultaatgerichtheid - Samenwerken - Voortgangsbewaking

Architectuurprincipes versus projectmatig opportunisme

Auteur: Lex Borger > Lex Borger is Principal Consultant Information Security bij Domus Technica en redacteur van dit blad. Hij is bereikbaar via lex.borger@domustechnica.com.

Een terugkerend thema in mijn werkzaamheden als beveiligingsexpert is dat ik geconfronteerd word met het spanningsveld tussen de principiële aanpak van architecten en de opportunistische insteek van projectmedewerkers. Architecten kunnen zich aardig ingraven in hun principes die gevolgd moeten worden en projecten hebben maar een beperkte tijd en middelen tot beschikking om een resultaat te bereiken. Het opvolgen van de architectuurprincipes heeft soms tot gevolg dat een project meer kosten moet maken. Ik denk dat beveiligers vaker dan anderen hiermee te maken krijgen, doordat beveiliging vereist dat er met een andere insteek naar de materie gekeken wordt. Hoe moeten we omgaan met dit spanningsveld? Ik heb daar wat gedachten over, die ik in dit artikel opgeschreven heb.

Bijvoorbeeld: stel dat bij de realisatie van een nieuwe applicatie ook een geheel nieuw multi-factor authenticatiesysteem gebouwd moet worden. Strategisch gezien is dit een keuze die zinvol is, het project zal dit graag opnemen binnen de scope van het project, zolang ze er de ruimte voor krijgen. Vervolgens komt er druk te staan op het project – het moet eerder klaar, of de selectie van het authenticatiesysteem duurt wat langer doordat de leverancier wat meer beloofd heeft dan waargemaakt kan worden, of bij invulling blijkt dat het kostenplaatje niet meer past. Elke verstoring lijkt gelijk te leiden tot de discussie 'moet het project nu de last dragen van de implementatie van een dienst omdat het de eerste gebruiker van de dienst is?'

Dit lijkt vaak een moeilijk te overbruggen tegenstelling: de principiële aanpak en de opportunistische weg zijn tegenpolen van elkaar, die nooit tot elkaar kunnen komen. Of toch wel? Wat als we het niet meer als een strijd zien, maar als een spel? Door uit de overlevingsmodus te komen en het geheel als spel te zien, kunnen we ook het speelveld en de spelregels tot ons laten doordringen. Uiteindelijk zijn we met zijn allen bezig een succes te realiseren voor één organisatie, die ons daarvoor beloont. Vergelijk dit eens met verschillende voetbalclubs als Ajax en Feyenoord, die dit jaar met goede spelers niet in staat zijn geweest een toppositie te realiseren en ze lieten AZ met de roem en glorie wegkomen. Waar zit het verschil? In de voetbalwereld is het eenvoudig: de trainer heeft het gedaan.

Ook de politiek zit vol met principiële ego's en opportunisten. In deze wereld worden de verschillen vaak levensgroot uitvergroot en is de wil tot samenwerken ver te zoeken, vooral rond verkiezingstijd.

Cooperation, Wbs 70, via Flickr

Toch waren de meest succesvolle kabinetten gestoeld op een goede, intrinsieke samenwerking. We kunnen uit de politiek in ieder geval leren wat we ***niet*** willen:

- Exclusief gelijk willen krijgen – terwijl beide partijen beiden gelijk kunnen hebben.
- Vanuit een machtspositie iets opleggen – als het tij keert wordt er eerst veel energie gestoken in het ongedaan maken van het 'onterecht' opgelegde.
- Alles helemaal uitpraten totdat er een universele consensus is – polderen heeft zijn nut, maar tot op een bepaald niveau. Er moet wat gebeuren. Er mag verschil van inzicht overblijven, maar er mag geen verlamming optreden.

Het wereldje van architecten en projecten zit vol met politici. Er is in het wereldje echter geen eenvoudige equivalent van de voetbaltrainer. Het is niet de projectleider of de programmamanager, ook niet de architect of zijn management. Al deze partijen zijn in feite spelers. Deze spelers zouden elkaar de ruimte voor andere standpunten moeten gunnen en hun eigen rol (of dat nu die van principieel of van opportunist is) vanuit dat gevoel van ruimte kunnen spelen. De rol van het middenmanagement lijkt het meest op die van de trainer. Zij overzien zowel de ontwikkeling van projecten, als de dagelijkse uitvoering. Zij zitten in stuurgroepen van projecten en hebben belang bij een beheersbare uitvoering.
De vraag is: kunnen zij zich verheffen boven het opportunisme dat leidt tot een onbeheersbare uitvoering of de principiële blokkade tegen ongewenste veranderingen? Oftewel; kunnen zij de nodige ruimte en het respect geven aan beide partijen zodat de discussies op de werkvloer gaan over het verbeteren van de bedrijfsvoering in plaats van over het gelijk van de een of de ander?
Uiteindelijk horen we allen dankbaar te zijn voor de inbreng van de ander – door de dialoog aan te gaan met je tegenpool, ben je bewuster van je eigen opstelling. In plaats van de energie te steken in het expliciet maken van de tegenstelling kunnen we ons dan ineens richten op een samenwerking. De dialoog maakt uiteindelijk dat beide partijen in de discussie naar de argumenten van de ander moeten luisteren, ze begrijpen en op hun waarde schatten. Als gevolg kunnen beide partijen hun argumenten beter formuleren. Het is eigenlijk heel menselijk: ga uit van het goede in ieders standpunt, weeg het op waarde en behandel het met respect.

Even terug naar het voorbeeld van het authenticatiesysteem. Door opnieuw te bekijken of en waarom het systeem nodig is, kunnen we de strategie en projectuitvoering zinnig bijstellen. De noodzaak kan al opgeschreven zijn bij de architectuur-documentatie, anders moet dat alsnog achterhaald worden.

Het is helemaal niet taboe om af te wijken van je principes, als je weet dat het principieel beoogde doel nog steeds bereikt wordt. Het dient wel een win-win situatie voor beide partijen. Drie belangrijke afwegingen die naar mijn mening bij iedere bijstelling gemaakt moeten worden zijn:

- **Kan het eenvoudiger?** Architectuur is gemaakt zonder specifieke situaties in ogenschouw te nemen. Het kan zijn dat de vertaling van de architectuur in de context van een project nieuwe inzichten oplevert die in de architectuur verwerkt kunnen worden als aanpassingen, in plaats van onevenredig grote inspanningen te eisen van een project. *Als een authenticatiesysteem gekoppeld moet worden met bronsystemen en doelsystemen kan er een strakgeleide, onbespreekbare koppeling opgelegd worden vanuit architectuur of er kan in het licht van architectuur gekeken worden naar de beoogde werking van het systeem vanuit het oogpunt van de leverancier. In mijn ervaring levert deze dialoog vaak een stabielere infrastructuur op, dan blindelings de architectuurprincipes te volgen alsof het dogma's zijn. Door af te wijken van de beoogde werking van de leverancier verhoog je de implementatiekosten en het bijbehorende risico. De transitie naar nieuwe versies kan ook problematischer verlopen.*

- **Zal het systeem echt gebruikt worden?** Vaak genoeg leveren de compromissen die bereikt worden bij een scopebijstelling van een project helemaal geen werkbare situatie meer op.

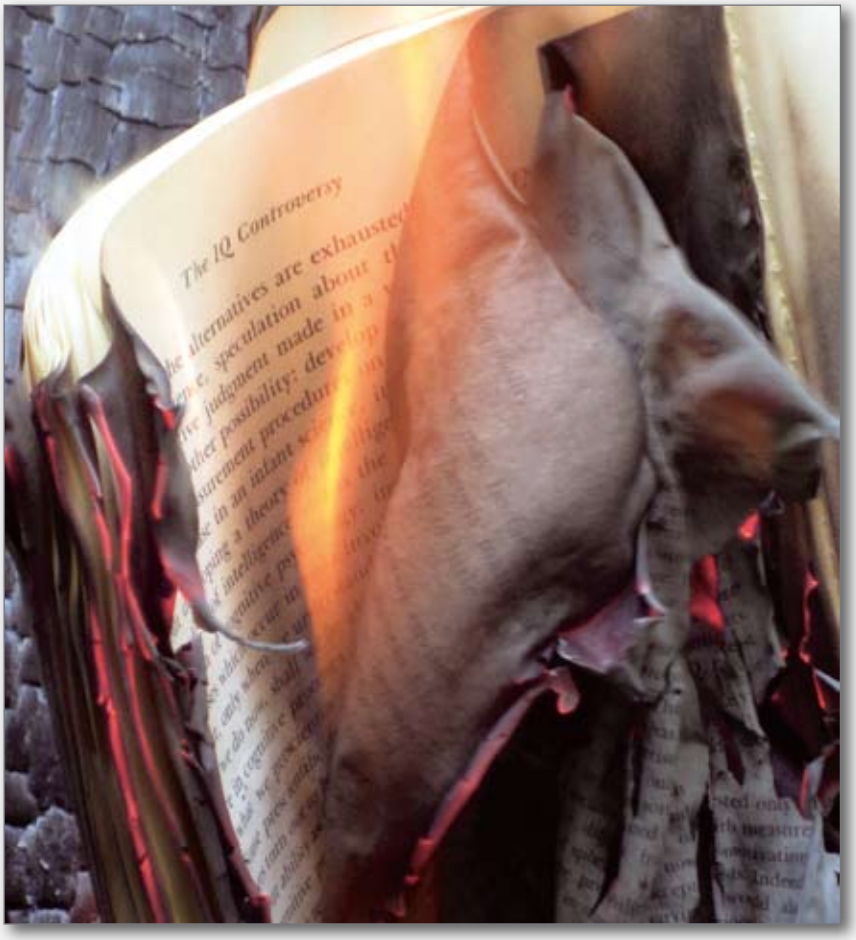
Opposition, *Abhi*, via Flickr

Als een authenticatiesysteem bijvoorbeeld niet meer voor alle gebruikers geldt, maar alleen voor externe gebruikers, die op dat moment al een werkbaar alternatief hebben. Terugzoekend blijkt dat het authenticatiesysteem tot doel had juist een universeel authenticatiesysteem te leveren. Het compromis is geen win voor architectuur en geen win voor het project. Beter is het dus om het project te ontslaan van de verplichting het authenticatiesysteem te realiseren door het buiten scope te plaatsen.

- **Is er niet een geheel ander alternatief?** Architectuur geeft ons de weg naar een visie. Soms zijn bepaalde wegen nog niet goed in kaart gebracht, soms blijken wegen anders te lopen dan verwacht. De korte geschiedenis van de automatisering heeft ons dit al meermalen geleerd. Ik illustreer dit met twee trends, die veelbelovend waren, maar die belofte niet waargemaakt hebben.

Fat-client computing

De PC bracht de computer op het bureau in de tachtiger jaren en het werd de vanzelfsprekende plaats waar verwerking werd gedaan. In de integratie met de backoffice systemen werd dit ook doorgezet. De fat client was geboren. Zelfs de internet browser hebben we kunnen omtoveren tot een fat client. De laatste jaren krijgen we steeds meer door dat het beheren en beveiligen hiervan te moeilijk en tijdrovend is en gaan we terug naar thin client oplossingen. In feite hebben we met zijn allen moeten constateren dat de mainframe terminal nog niet zo'n slecht concept is. Alle belangrijke verwerking vindt plaats in de veilige omgeving van het mainframe in het datacenter. Nu stoppen we fat-client computing weg in gevirtualiseerde desktops.



Controversy, Aprilzosia, via Flickr

De firewall

Netwerkbeveiliging werd in de negentiger jaren synoniem met een firewall. Vervolgens zagen we ook dat de firewall geïntegreerd werd in netwerkapparatuur; meer functionaliteit kreeg. Aan deze ontwikkeling leek geen eind in zicht te zijn. Elk beveiligingsprobleem kon principieel in de firewall opgelost worden. Het gebruik van encryptietunnel techniek gaat hier echter dwars tegenin. Een encryptietunnel realiseert een verbinding waar een firewall bij inspectie weinig over te weten kan komen.

Ik heb meegemaakt dat de eerste reactie van de architecten was: 'Encryptietunnels mogen niet!' Vervolgens bleek dat niet vol te houden, vooral SSL-tunnels werden gemeengoed en dienen ook duidelijk hun nut. Ineens hoeven er geen dure leased-lines meer ingezet te worden om veilig met derden te kunnen communiceren. Communicatie kan veilig over het grote, boze internet. Inmiddels heeft SSL zijn waarde als beveiligingsprotocol wel bewezen. Dus het standpunt 'geen encryptietunnels' levert op: architecten – win, projecten – lose. Men is er weer succesvol in geslaagd de inzet van een waardevol, nieuw mechanisme tegen te houden.

Maar dit houdt natuurlijk geen stand. De tweede reactie was dan ook: 'SSL mag, maar dan wel met onderbreking in de firewall'. Dit standpunt is naar mijn mening echt een lose-lose scenario voor zowel de architectuur als de implementatie. De veiligheid van de SSL-tunnel wordt structureel onderbroken op een plaats die veel kwetsbaarder is dan de PC op mijn bureau, namelijk op een server in de DMZ zone. Verder is het voor mij als eindgebruiker niet meer te controleren of de SSL-tunnel wel helemaal correct is opgebouwd. En helaas is deze controle nog steeds hard nodig, een man-in-the-middle aanval op mijn SSL-tunnel is gestructureerd en scriptmatig mogelijk, zonder de encryptie zelf te breken. Als illustratie hiervoor kunnen sslsniff en sslstrip dienen (zie links).

De weg van de firewall als primair mechanisme voor netwerkbeveiliging loopt dus dood. Dat realiseerde een groep van CISO's van gerenommeerde bedrijven zich ook. De bestaande principes rondom de firewall werkten niet meer. Als antwoord schreven ze een aantal principiële inzichten op ter de-perimetrisatie van het netwerk en richtten ze het Jericho Forum op (zie links). Ook hier zien we dus een succesvolle breuk met het gevestigde firewall dogma en het inzetten van een principieel nieuwe richting.

Conclusie

Ik weet zeker dat er velen zullen zijn die een andere kijk hebben op dit vlak. Geheel in lijn met wat ik hierboven heb opgeschreven, verwelkom ik die alternatieve inzichten. Architectuur is een discipline die niet meer weg te denken is uit een gezonde bedrijfsvoering. Architectuur is onlosmakelijk verbonden aan informatiebeveiliging, het is niet langer het exclusieve domein van de security expert. Architecten vormen geen kleine partij meer die vanuit de eeuwige oppositierol en hun eigen overtuiging dictaten roept. Het zijn professionals, die volwaardig mee zouden moeten spelen.

Wat ik met dit artikel aangeef, is dat wanneer het spel goed en eerlijk gespeeld wordt, er geen architectuurbeslissingen meer doorgedrukt hoeven te worden ten koste van projecten. Of omgekeerd: dat een project zegeviert en architectuur het onderspit delft. Ik pleit ervoor om niet dogmatisch achter architectuurprincipes aan te lopen, maar om ook pragmatisch met een project mee te denken, maar dan wel met de businesscase van het dogma in het achterhoofd.

URLs

Thin client (& fat client) - Wikipedia
http://en.wikipedia.org/wiki/Thin_client

- New Tricks For Defeating SSL In Practice – Moxie Marlinspike
http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf

- Jericho Forum - About: Vision-Mission
http://www.opengroup.org/jericho/about.htm

Toegang tot patiëntgegevens

Auteur: L.T. van der Krogt > Leon is werkzaam bij het UMCG voor de afdeling ICT Beleid. Vanuit wetgeving, landelijke ontwikkelingen en eisen vanuit de business werkt ICT Beleid aan een passende architectuur voor een veilig elektronisch patiënten dossier.

Het Universitair Medisch Centrum Groningen
Elke dag zijn er 1000 bedden in gebruik door patiënten die behandeld worden en er werken meer dan 9.000 mensen samen aan zorg, onderzoek, opleiding en onderwijs. Jaarlijks zijn er ruim 31.000 opnames, er komen er zo'n 32.000 patiënten op de Centrale Spoedopvang en er studeren ongeveer 3.400 studenten.

In dit artikel neem ik u graag mee in de discussie 'toegang tot patiëntgegevens'. Een actueel onderwerp dat tot verhitte discussies leidt. Vanuit verschillende belangen wordt gekeken naar dit probleem: de zorgverlener die gewoon het dossier wil inzien, de patiënt die inzage wil beperken en de zorgverzekeraar die graag wil weten waarvoor hij betaalt. En in de universitaire setting zijn er ook nog wat wensen, zoals de onderzoeker die allerlei dwarsdoorsneden wil kunnen maken van dossiers of de professor die zijn studenten graag inzicht geeft in de interessante patiënten die op dat moment in behandeling zijn. Kortom; de 'never ending story' begint hier!

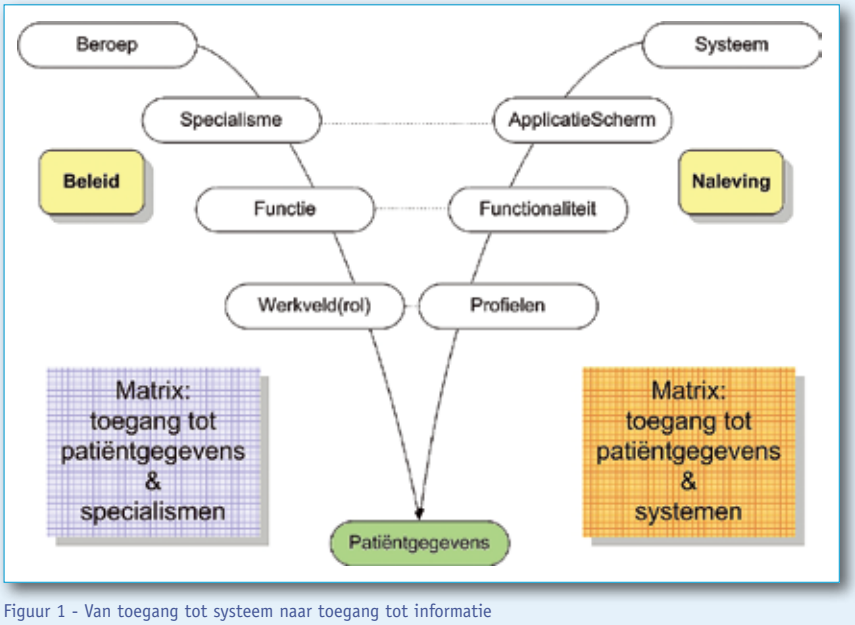
De echte ICT-er roept gelijk RBAC! Ooit wel eens gekeken naar RBAC? De literatuur die hierover te vinden is, doet je de moed in de schoenen zakken. Het starten van een discussie over role-based access control is dan ook een lang slepende, die meestal blijft hangen in de eerste letter: de rol. In de praktijk lopen we gruwelijk vast doordat traditioneel de autorisatie op systeemniveau geregeld wordt, soms op applicatieniveau, maar zelden op informatieniveau. De diversiteit van autorisatie is dan ook groot. Veelal zijn toegangsregistraties vastgelegd op de niveau's systeem of applicatie en niet op toegang tot informatie.

Na een aantal brainstormsessies met mensen uit de zorgbusiness zijn er toch genoeg punten op tafel gekomen om te starten met een architectuurontwerp. Ook zijn er een aantal belangrijke punten naar voren gekomen die opgelost moeten worden als het architectuurontwerp ten uitvoer wordt gebracht. Dit ontwerp is niet een alledaags ICT ontwerp, want het laat de techniek even voor wat het is. Het onderwerp is al ingewikkeld genoeg zonder ICT. Belangrijk is te constateren dat iedereen zijn eigen definities hanteert en deze hebben we dan ook geslecht door het eens te worden over de definities en vast te leggen als basis voor verdere discussie.

Over het doel zijn we het snel eens: optimale privacy met zo min mogelijk inspanning, die wel voldoet aan de wet. Concreet houdt dit in: de juiste toegang (identiteit) tot de juiste informatie (need to use) en het liefst nog op de juiste plaats (locatie) en het juiste moment (tijd).

Het waarom is duidelijk: we willen graag de privacy van onze patiënten respecteren en natuurlijk moeten we als zorginstelling voldoen aan de Wet Bescherming Persoonsgegevens (WBP), Wet op de Geneeskundige Behandel Overeenkomst (WGBO), Wet medisch-wetenschappelijk onderzoek met mensen (WMO), de Archiefwet 1995, etc. En straks ook de Wet op het Elektronisch Patiënten Dossier (EPD). Vanuit deze laatste wet moet, voor het aansluiten op het landelijke EPD, de toegang tot de informatie traceerbaar zijn. En voor de rest wil de business er geen last van hebben en is het vooral een niet leuk ICT feestje. Wat we nodig hebben is een duidelijk richtlijnen document: hoe om te gaan met toegang tot informatie. Dit moet voor zowel de business als de ICT begrijpelijk en bruikbaar zijn.

Ondanks de ontwikkelingen naar WEB2.0, waar de hiërarchie is losgelaten, zie je dat we toch graag vasthouden aan hiërarchie. Dat komt doordat organisatiestructuren,



Figuur 1 - Van toegang tot systeem naar toegang tot informatie

maar ook ICT systemen uitgaan van hiërarchie. Zo hebben we dus gekozen voor de persoon als hoogste object en het informatieattribuut als laagste. Dat de infrastructuur hiërarchisch is, houdt niet in dat je geen invulling kunt geven aan WEB2.0. Doordat de infrastructuur logisch wordt opgebouwd, kan er beter geautomatiseerd worden. Hierdoor kunnen autorisaties door de juiste business-verantwoordelijke via een zelfservice worden geregeld. De informatie wordt op basis van standaard profielen conform de wet aangeboden aan de business. Zo hoeft er alleen nagedacht te worden over de afwijkingen op de standaard en het risico dat de business hiermee loopt.

Met de organisatie en infrastructuur-hiërarchie zijn we gaan invullen en kwamen we tot het volgende model: een persoon heeft een beroep, heeft een specialisme, heeft een functie, heeft een rol(werkveld) en wil toegang tot informatie.

Als je kijkt naar de techniek zie je een-zelfde hiërarchie: de organisatie gebruikt een systeem, gebruikt een applicatie-scherm, gebruikt een functionaliteit, gebruikt een profiel dat toegang geeft tot informatie.

Hier zie je aan de linkerkant het beleid, de keus die we gemaakt hebben in de hiërarchie en aan de rechterkant de uit-voering zoals die in de infrastructuur herkend wordt. Opeens wordt het duidelijk waarom de huidige registraties van toegang tot systemen niet meer bruikbaar zijn. Het Excel werkblad waarop nu de persoon en de toegang tot een systeem wordt geregistreerd, zegt niets over de informatie die de persoon kan benaderen. Met de huidige toegangsregistraties is het achterhalen wie nu toegang heeft tot informatie voor een auditor een lastig en tijdrovend karwei.
In dit model gaan we uit van toegang tot informatie behorend bij de rol. Kijkend naar de WBP en WGBO weten we welke informatieattributen wel of niet toe-gankelijk mogen zijn voor bepaalde rollen. Hierdoor zijn we in staat standaard profielen te maken en te koppelen aan rollen. Zo ontstaat dus een basis van wettelijke profielen.

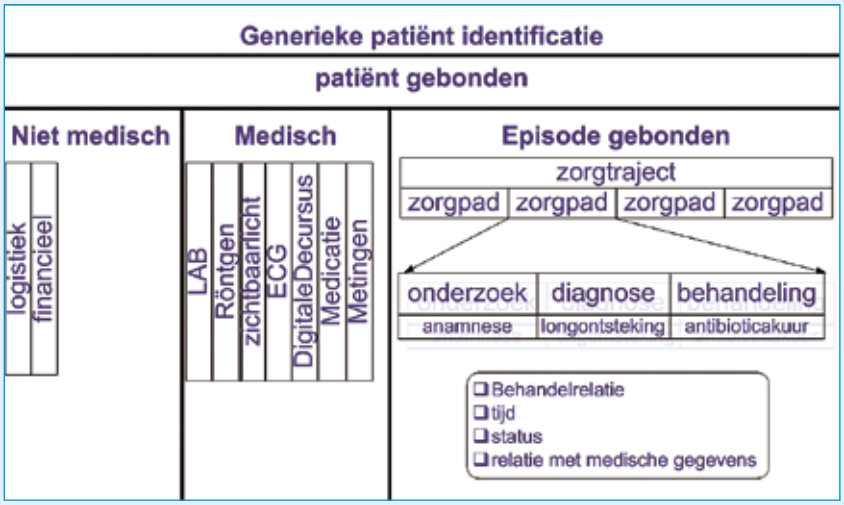
Een abstract medisch dossier

Alleen al over de indeling van het medisch dossier kan een boek geschreven worden! Om de toegang specifiek te maken, moet de informatie worden gecategoriseerd. Ook hiervoor hanteren we een model om de complexiteit te verminderen. Voor de architectuur is de inhoud niet echt van belang, maar is het belangrijk om te onderkennen dat informatiecategorieën nodig zijn om de toegang op categorie-niveau te kunnen bepalen.
De meeste categorieën zijn logisch en rechtlijnig te gebruiken. Anders is het met episodegebonden informatie. Kijken we naar de WGBO dan zien we dat een zorgverlener alleen toegang tot een dossier mag hebben als deze een behandelrelatie heeft met de patiënt voor het ziektebeeld waarvoor de behandeling is aangevraagd: de episode. Breekt een psychiatrisch patiënt zijn been, dan mag de arts die het been herstelt, geen toegang hebben tot het psychiatrisch dossier. In het traditionele papieren dossier is dat niet ingewikkeld, dit papieren dossier bevind zich op de afdeling psychiatrie en is alleen toegankelijk voor zorgverleners op die afdeling.

Het zorgtraject is opgebouwd uit diverse zorgpaden en een zorgpad bestaat weer uit verschillende processtappen. Binnen deze processtappen wordt weer medische en niet medische informatie vastgelegd en gebruikt.

Domeinen en doelgroepen

Dat de zorg niet eenvoudig is, wisten we al maar in een universitair ziekenhuis heb je te maken met meerdere domeinen waar per domein verschillende regels gelden. Zo onderkennen we de domeinen: zorg, onderzoek, onderwijs & opleiding en ondersteunend. Het lastige is dat binnen deze domeinen meerdere doelgroepen actief kunnen zijn, zoals de zorgverlener, de patiënt, de zorgconsument en de medewerker. En allemaal gebruiken ze een deel van het dossier. De facilitaire dienst die de maaltijd bereidt en bij de patiënt bezorgt, moet weten wat de patiënt eet en waar deze verblijft. De facilitaire dienst heeft niets te maken met de medische gegevens. De onderzoeker die graag dwarsdoorsneden van dossiers wil maken, mag niet bij de persoonsgegevens.
En professor die 's middags zijn zaalrondes doet, mag 's avonds in de collegezaal niet de persoonsgegevens van de patiënt tonen. Zeker deze laatste doelgroep maakt het lastig om een goed werkbaar architectuur-ontwerp te maken.



Figuur 2 - Abstracte indeling patiëntdossier

- ❑ Is een geldig identiteit getoetst?
- ❑ Is een behandelrelatie aanwezig?
- ❑ Is identiteit onderzoeker of student? => alleen anonieme informatie
- ❑ Is de informatie afgeschermd met een autorisatieprofiel? (bezwaarprocedure landelijke EPD)
- ❑ Is de patiënt een VIP?
- ❑ Identiteit = patient < 12 jaar: zie aanvullings- of correctie en vernietigingsverzoek
- ❑ Identiteit = patient 12-16 jaar: zie aanvullings- of correctie en vernietigingsverzoek
- ❑ Identiteit = patient > 16 jaar: zie aanvullings- of correctie en vernietigingsverzoek
- ❑ Identiteit = wettelijk vertegenwoordiger: zie aanvullings- of correctie en vernietigingsverzoek
- ❑ Is de houdbaarheidsdatum van de gevraagde info nog geldig?

Figuur 3 - Controleregels voor toegang

Rol gebaseerde toepassingen

Een ontwerp maak je niet alleen voor toegangsbeveiliging, je kunt er veel meer mee. Zo kan bij het aanmelden worden vastgesteld welke rol er aan hangt en kan een voor die rol standaard schermopbouw worden getoond. Ook kan een voorselectie van informatie worden gedefinieerd op bijvoorbeeld het specialisme. Zo krijgt een internist meer generieke informatie te zien, terwijl in hetzelfde hoofdscherm een chirurg meer detailinformatie krijgt van dezelfde patiënt.

De functie kan gebruikt worden om een mandaat vast te leggen. Zo kan een arts een arts in opleiding bepaalde patiënten toewijzen, zodat de arts in opleiding onder supervisie van de arts dossiers kan inzien om een consult voor te bereiden.

Aandachtspunten

Het gebruik van rollen, functie, specialisme en beroepen kan voor meerdere doelen gebruikt worden:

- Vaststellen authenticiteit (vertrouwen)
- Autorisatie (toegang)
- Schermen (lay-out)
- Informatie (inhoud)
- Mandaat (in opdracht van)
- Single Sign-on (gebruikers gemak)
- Decentraal Rolbeheer (manager bepaald wat een rol kan)

Vaststellen van de authenticiteit

Binnen de zorg mag de identiteit van een persoon niet meer vastgesteld worden aan de hand van een gebruikersnaam en wachtwoord. Dit is immers niet herleidbaar tot de natuurlijke persoon. Zelfs het kijken in een medisch dossier moet tot op de persoon herleidbaar zijn. Hiervoor zijn sterke identificatiemiddelen en een identificatieproces noodzakelijk. En moet bijvoorbeeld het eigen personeelssysteem, het UZI-register, DigiD als vertrouwde identiteitleverancier worden onderkend.

Aandachtspunten

1 Zorg dat de instantie die de identiteit levert als vertrouwd wordt onderkend.
2 Zorg voor een koppeling tussen infrastructuur en het personeelssysteem.
3 Zorg dat niet-medewerkers ook in het personeelssysteem geregistreerd kunnen worden.

Voorwaardelijk toegang

Natuurlijk krijg je niet zomaar toegang tot patiëntinformatie. Er zijn nog een aantal barrières waar je doorheen moet. Neem bijvoorbeeld de behandelrelatie die vanuit de WGBO verplicht is. Heb je geen behandelrelatie met de patiënt, dan krijg je geen toegang anders dan via de noodprocedure. Ook de toegang via de noodprocedure is vastgelegd in de WGBO. De WBP voegt nog wat regels toe voor de bescherming van de patiënt (link 1). En als je als patiënt je eigen gegevens wilt inzien, moeten we de leeftijd controleren. Ben je jonger dan 12 jaar, dan mag inzage alleen met toestemming van je wettelijke vertegenwoordiger. Op je 12de mag je zelf wel aanvullen maar niet corrigeren, dat mag de wettelijke vertegenwoordiger dan weer wel. Ben je tussen de 12 en 16 jaar, dan heb je zelf toegang en mag de wettelijke vertegenwoordiger niet zonder meer informatie aanvullen. Ben je ouder dan 16 jaar, dan mag je zelf het dossier inzien, aanvullen en corrigeren. De wettelijke vertegenwoordiger is dan de toegang ontzegd.

Het landelijke EPD doet de laatste duit in het zakje. Een patiënt kan bezwaar maken tegen inzage in het dossier op zorgverlenerniveau of dossierniveau bij het opvragen vanuit andere zorginstellingen. Dezelfde regel geldt ook intern.

Nog een belangrijke regel die te maken heeft met de vernietigingsplicht: de houdbaarheidsdatum van de opgevraagde informatie. Ook hier wordt vaak opgemerkt dat dit overbodig is, als de informatie vernietigd is, kun je het niet meer opvragen. In theorie klopt dit, maar praktisch gezien kun je dossiers niet volledig vernietigen omdat deze vele malen op back-upmedia staan. Het kan dus voorkomen dat een patiënt een opdracht tot vernietiging geeft. Als patiënt wil je hier niet een jaar op wachten tot het dossier ook uit de back-ups verdwenen is. Ook hebben we te maken met de archiefwet die vereist dat medische dossiers onveranderbaar opgeslagen worden (zie link 2). De digitale archiefmedia die we inzetten als archief zijn natuurlijk zo gebouwd dat er niets meer vernietigd kan worden.

Aandachtspunten

1 Zorg dat identificatie van zowel de zorgverlener als de patiënt altijd eenduidig zijn (UZI & BSN).
2 Er moet een mandaatregeling zijn om de wettelijke vertegenwoordigers toegang te verlenen tot de informatie van de (pleeg) kinderen.
3 Een koppeling met het Landelijk EPD is nodig voor het invoegen van de eventuele bezwaren.
4 Het vernietigen van een dossier in ieder geval regelen door deze niet te tonen aan de aanvrager.

Informatiecategorieën

De informatie moet gecategoriseerd worden om de toegang tot die informatie goed te kunnen regelen. Dit kan door profielen te definiëren waarmee de toegang tot deze specifieke informatie geregeld wordt of beter, vooraf de informatie classificeren zodat bij het benaderen van de informatie het juiste profiel gekozen wordt.
Informatie moet geclassificeerd worden volgens WBP en WGBO. Niet iedere zorgverlener hoeft het huisadres van de patiënt te zien. Ook de keuken die de maaltijd bereidt voor de patiënt hoeft alleen maar het dieet, de afleverlocatie en de aflevertijd tijd te weten.
Vanuit de WBP is het niet toegestaan om bijzondere persoonsgegevens vast te leggen (zie link 3). Er ontstaan een aantal hoofd-categorieën zoals: persoonsgegevens, niet-medische gegevens, bijzondere persoonsgegevens, medische gegevens, episodegebonden gegevens en specialismegebonden gegevens. Steeds weer hebben we de discussie waarom we een categorie bijzondere persoonsgegevens hebben als we deze gegevens toch niet mogen vastleggen. Bij het categoriseren van nieuwe gegevens is het van belang dat deze attributen niet per ongeluk onder een andere categorie gezet kunnen worden.
Er zijn medische onderzoeken waarbij de afkomst van een bepaald ras van belang is. Dit mag alleen geregistreerd worden met ontheffing van College Bescherming Persoonsgegevens (CBP).
Wat het lastig maakt, is dat er weer uitzonderingen komen op de categorieën. Zo zal vanuit de Wet op het EPD zal straks bepaald worden dat allergie ook zichtbaar moet zijn in de professionele samenvatting (zie link 4) zodat er in de keuken of bij voorbereiding van de operatiekamer ook rekening gehouden kan worden met bepaalde allergieën.
Dit pleit niet voor het aanpassen van de basiscategorieën maar om uitbreiding daarvan naar bijvoorbeeld views op bepaalde informatiesets. Zo zal een categorie 'professionele samenvatting' een verzameling wettelijk verplichte velden uit andere categorieën moeten regelen.

De praktijk van beroepen, functies en specialismen

In de brainstormsessie kwam naar voren dat beroep, functie en specialisme door elkaar gebruikt worden in diverse, niet gekoppelde systemen. Medewerkers worden aangenomen in een bepaalde functie, gekoppeld aan een salarisschaal. In de loop van de carrière wordt de functie anders ingevuld of krijgen ze een andere functie met behoud van de vorige door een vangnetconstructie. Ook worden specialismen als functie geregistreerd. Er is dus veel vervuiling van de functietabel van het HR systeem. Ook in de elektronische telefoongids worden de drie niveaus door elkaar gebruikt. En dat terwijl er voor de zorg wettelijke beroepen geregistreerd zijn (zie link 5) en de UMC's een de facto standaard voor functies heeft.
De Functiewaardering voor Academische Ziekenhuizen (FUWAVAZ) bevat de basis voor de functies in de academische zorg. Helaas heeft deze niet een relatie met de beroepen in de zorg die vanuit de wet zijn geregeld. Deze moet dus zelf aangebracht worden.

Aandachtspunten

1 Gebruik WBP, WGBO en andere brancheafhankelijke wetten als basis voor de classificatie.
2 Zorg dat er één bron van beroepen, functies en specialismen benoemd is.
3 Zorg dat diverse registraties zoals telefoongids, personeelssysteem en gebruikersregistraties dezelfde naamgeving en niveaus hebben.
4 Zorg voor een aliastabel voor functies om vangnetconstructies in tact te laten.
5 Een persoon kan meerdere beroepen uitoefenen, meerdere specialismen en rollen hebben.
6 UZI-pas bevat niet alleen de persoonsidentificatie, maar ook het beroep en het specialisme.

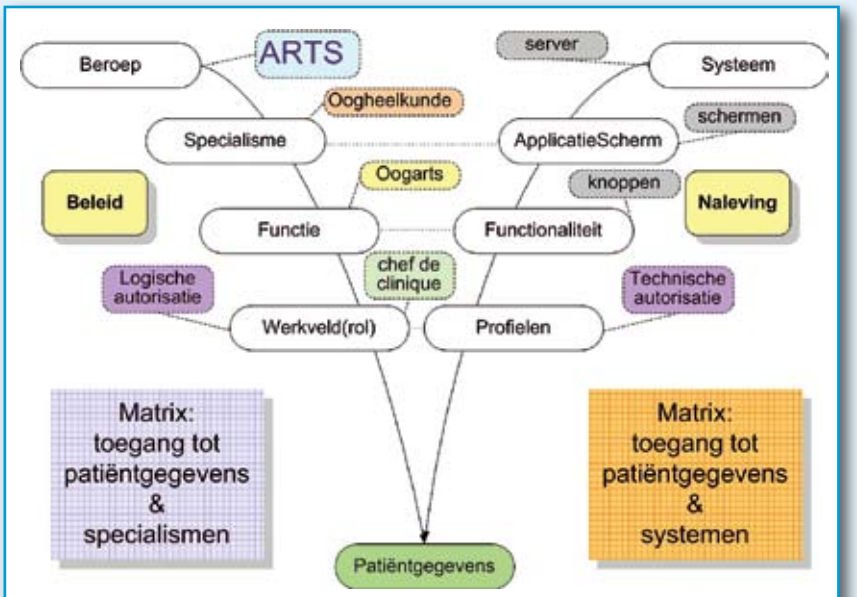
Figuur 4 - UZI-pas bevat ook het beroep en het specialisme

Architectuur vertaald naar infrastructuur

Er zijn heel veel standaarden gedefinieerd en de overheid komt ook nog eens met allerlei middelen die kosteloos beschikbaar worden gesteld. Zo is er de PKI-Overheid die regelt dat ambtenaren en zorgverleners kunnen gebruikmaken van een Public Key Infrastructure (PKI). Voor de zorg is dat in de vorm van een Unieke Zorgverlener Pas (UZI). DigiD kan zorgen voor een identificatie van de burgers en later dus ook van de patiënten. DigiD in combinatie met SMS geeft al mogelijkheden om patiëntgegevens aan de patiënt te tonen. Met het BSN dat bij het aanmelden via DigiD beschikbaar komt, kan via de BSN service de identiteit vastgesteld worden.

De UZI-pas levert een aantal attributen die bruikbaar zijn in het ontwerp. Zo wordt voor zorgverleners niet alleen een uniek nummer op de pas vermeld, maar ook het beroep en specialisme. Zorgverleners met meerdere specialismen hebben dus meerdere passen. Hierdoor ontstaat een Single Sign-on omgeving per pas. Deze passen zijn ook nog eens op te vragen in een landelijk register voor beroepen in de zorg, zodat we van zorgverleners met meerdere specialismen de andere specialismen en passen kunnen opvragen. Ook bezit de pas op naam een digitaal certificaat voor de digitale handtekening. Deze handtekening staat gelijk aan de wettelijke geavanceerde digitale handtekening die de gewone handtekening op papier kan vervangen.

DigiD levert bij het inloggen het Burger Service Nummer (BSN) waarmee we via de webservice BSN de bijbehorende naam, adres en woonplaats gegevens kunnen toetsen. Ook kan de geboortedatum worden achterhaald die nodig is voor het vaststellen van de leeftijd, zodat een dertienjarige niet direct toegang krijgt tot zijn dossier, maar pas als de wettelijk



Figuur 5 - Van architectuur naar infrastructuur

In het architectuurplaatje zijn rollen en profielen elkaars evenknie, net als functies en functionaliteit en specialisme en applicatiescherm. Belangrijk bij de uitwerking naar techniek is het gebruik van administrative groups (AG) en physical groups (PG). Elk platform heeft eigen benaming voor groepen, maar in dit artikel houden we het op AG en PG.

AG's zijn groepen mensen, afdelingen, etc. PG's vertegenwoordigen toegang tot de daadwerkelijke informatie. Bijvoorbeeld een oogarts is dus lid van de AG-beroep arts, de AG-specialisme Oogheelkunde en de AG-functie Oogarts en een AG-rol algemeen. Een profiel waarin de toegang geregeld wordt, is een PG. Deze wordt gekoppeld aan het hoogst gemeenschappelijke toegang. Is de toegang tot de informatieset X voor alle artsen hetzelfde, dan kan de PG-X gekoppeld worden aan de AG-beroep arts. Is een dataset alleen specifiek bedoeld voor de oogartsen, dan wordt de informatieset Y met een PG-Y gekoppeld aan AG-specialisme Oogheelkunde.

vertegenwoordiger zich ook aanmeldt.
De informatieclassificatie zorgt er voor dat alleen de gegevens opgevraagd worden die passen bij het beveiligingsniveau van DigiD met SMS.
Door de toegang vooraf te bepalen aan de hand van de WGBO en WBP kan een standaard set compliancy profielen worden gedefinieerd. Zodra iemand met goede argumenten een afwijkende toegang wil hebben, kan dit geregeld worden in een nieuw herkenbare profiel. Hierdoor ontstaat een rapporteerbaar model voor handhaving. Periodiek kunnen de afwijkingen naar de verantwoordelijke afdeling worden gerapporteerd. Zij zijn immers verantwoordelijk voor de juiste toegang. Ook vanuit de auditor ontstaat een wenselijke situatie. Naar wettelijk vastgestelde profielen hoeft maar één keer gekeken te worden. Deze moeten verder onveranderd blijven.

Een belangrijk stukje architectuur zijn de toegangsregels. Het aanbrengen van deze regels in bestaande applicaties is praktisch niet haalbaar. Zeker in de zorg zijn applicaties veelal gebaseerd op oude technologie. Hiervoor kan het beste een toegangsportaal gebouwd worden op basis van services. De controle van BSN wordt ook al via een service aangeboden en zo kunnen de toegangsregels ook via een Patiënt Bezwaar Service geregeld worden. Het zou mooi zijn als het huidige bezwaarprocedure, nu nog een papieren tijger, ook als service wordt aangeboden vanuit het Landelijke EPD.

Meerdere rollen

In een zorgbedrijf kan een persoon in meerdere domeinen actief zijn. Dat houdt in dat een persoon verschillende toegangen moeten hebben. Dit is een praktisch probleem waar we pragmatisch mee moeten omgaan. Voorlopig hebben we de verschillende domeinen op pasniveau gescheiden. Logt iemand in met DigiD dan is het een burger of patiënt. Logt dezelfde persoon in met een UZI-pas, dan heeft deze de rol zorgverlener. Inloggen met een medewerkerpas is een ondersteunende rol.

Binnen het zorgdomein kun je naast zorgverlener ook nog eens onderzoeker en opleider zijn. Om deze rollen praktisch vorm te geven kan dit als volgt worden vormgegeven: de professor meldt zich aan met de UZI-pas en kan vervolgens in het scherm zelf zijn rol kiezen. Standaard staat deze tijdens werktijd op 'arts' en buiten werktijd op 'onderzoek' of 'onderwijs'.

Aandachtspunten

1 Naast de identiteit wordt via een pas ook de rol vastgesteld.
2 Het wisselen van een rol in een systeem moet voor de gebruiker makkelijk zijn, anders gaat deze met de verkeerde rol aan het werk en kunnen onbevoegden privacygevoelige gegevens inzien.

Tijdafhankelijke rol

Als de architectuur volledig in de infrastructuur verankerd is, kan overwogen worden om een losse koppeling te maken naar het roosterpakket zodat de rol ook tijdsafhankelijk wordt. Hierdoor kunnen voorkeursinstellingen vanuit het rooster worden aangepast of zelfs worden afgedwongen. Als een zorgverlener volgens het rooster werkt, hoeft deze buiten roostertijden geen toegang meer tot patiëntendossiers te hebben.

Plaatsafhankelijke rol

Steeds meer techniek komt beschikbaar waarmee ook de plaats van de identiteit bepaald kan worden. Is de rol architectuur eenmaal in gebruik, dan is ook een uitbreiding naar locatie afhankelijke toegang niet ingewikkeld toe te voegen.

Content afhankelijke identificatie

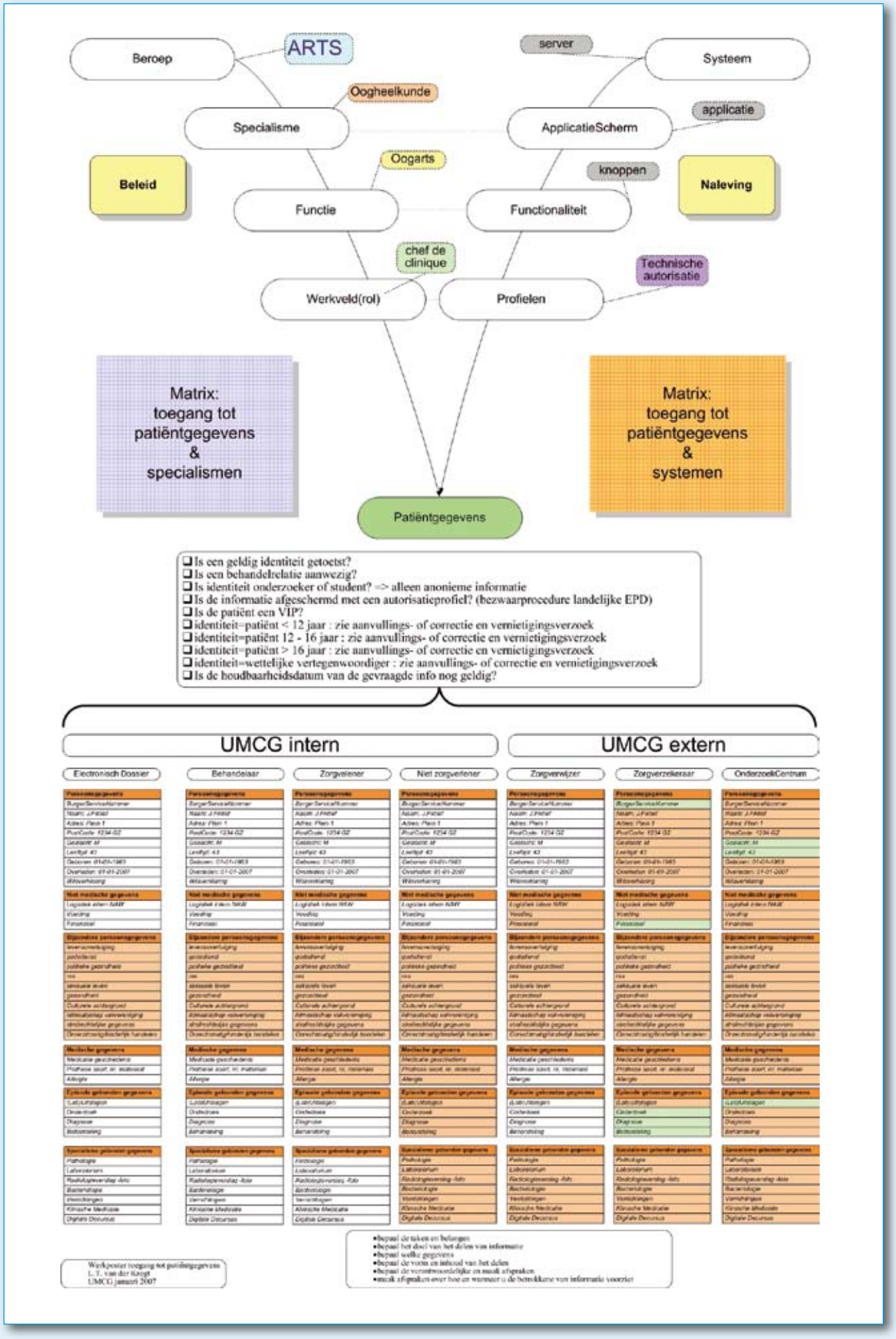
Uiteindelijk willen we naar een identificatie op het moment dat de informatie erom vraagt. Zo hoeft een gebruiker zich niet te identificeren zolang deze publieke informatie op vraagt. Zodra de gebruiker informatie opvraagt waarvoor identificatie noodzakelijk is, zal de gebruiker de keus worden gesteld in te loggen met een bijpassend identificatiemiddel.
De informatieattributen zijn immers geclassificeerd. Voorlopig is het nog niet zover dat attributen van metagegevens worden voorzien, maar het concept is er klaar voor.

Links

1 Regels bescherming patiënt
http://www.cbpweb.nl/downloads_overig/tabel_aanvullings_correctieverzoek_VA.pdf
2 Eisen opslag medische dossier
http://knmg.artsennet.nl/web/file?uuid=22307fcb-51ab-4d95-bd45-8e9a35cfce16&owner=5a314179-999d-489a-ab9f-645780c60bf9
3 Regels vastleggen bijzondere gegevens
http://www.justitie.nl/images/Handleiding%20voor%20verwerkers%20persoonsgegevens_tcm34-3940.pdf
4 Richtlijn gegevensuitwisseling
http://www.nictiz.nl/uploaded/FILES/Spoedeisende%20hulp/Richtlijn%20gegevensuitwisseling%20HA-AMB-SEH%20definitief%20v2.pdf
5 Wet BIG
http://www.ribiz.nl/diplomaenwerk/wetenregelgeving/wetbig/

URLs

1 http://tiny.cc/CbpAanvullingCorrectie
2 http://tiny.cc/WGBO_deel3
3 http://tiny.cc/WBP_handleiding
4 http://tiny.cc/NICTIZ_ProfessioneleSamenvatting
5 http://tiny.cc/RIBIZ_beroepenInDeZorg



Figuur 6 - De praatplaat toegang tot patiëntgegevens

Risico Management in SABSA

Het SABSA® Model

Samenvatting door Lex Borger > Lex Borger is Principal Consultant Information Security bij Domus Technica en redacteur van dit blad. Hij is bereikbaar via lex.borger@domustechnica.com.

SABSA is een sterk opkomend raamwerk om een security architectuur te beschrijven. Er is één standaardwerk om kennis te nemen van SABSA en dat is het boek dat door John Sherwood, Andrew Clark en David Lynas zelf geschreven is: Enterprise Security Architecture: A Business-Driven Approach, uitgegeven bij CMP Books in 2005. Alle referenties in deze samenvatting verwijzen dan ook naar dit boek, tenzij anders vermeld.
Het is een omvangrijk boek, bijna 600 pagina's. In deze samenvatting kijk ik naar de plaats van risico management in het SABSA raamwerk, wat in mijn ervaring een zwak punt is in security architectuur raamwerken die ik in het verleden gezien heb.

Op de eigen website (www.sabsa-institute.org) wordt SABSA omschreven als: 'een bewezen raamwerk en methodologie voor Enterprise Security Architecture en Enterprise Security Service Management. SABSA verzekert dat de bedrijfsbehoeften volledig gedekt worden en beveiligingsdiensten worden ontworpen, opgeleverd en beheerd als een integraal onderdeel van de bedrijfsbeheer- en ICT-beheer infrastructuur'.

Kernwoorden hierin zijn raamwerk, methodologie, waarborgen (Engels: assure), volledig en integraal. SABSA omvat dan ook ruim alle aspecten die je in een Security Architectuur zou mogen verwachten. SABSA is gebaseerd op het Zachman-raamwerk, met kleine aanpassingen. De zes basislagen van Zachman worden in SABSA net even anders weergeven, zoals in het SABSA-model (Figure 3-1, pagina 34) en het ontwikkelproces heeft als basis een plan-do-check-act cyclus, waarbij de namen van de stappen aangepast zijn (Figure 7-2, pagina 113). De reden die voor de

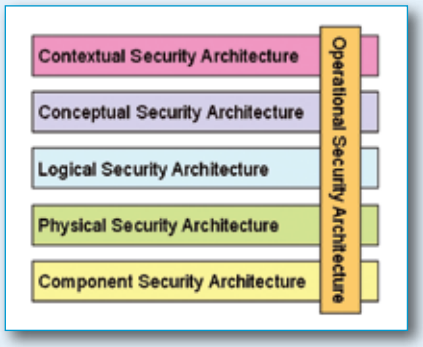


Figure 3-1: The SABSA® Model for Security Architecture Development

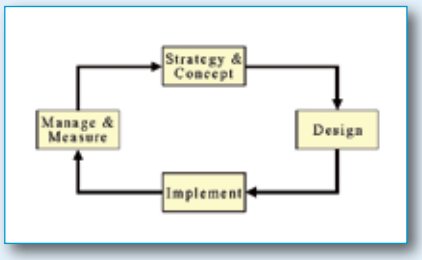


Figure 7-2: The SABSA® Lifecycle

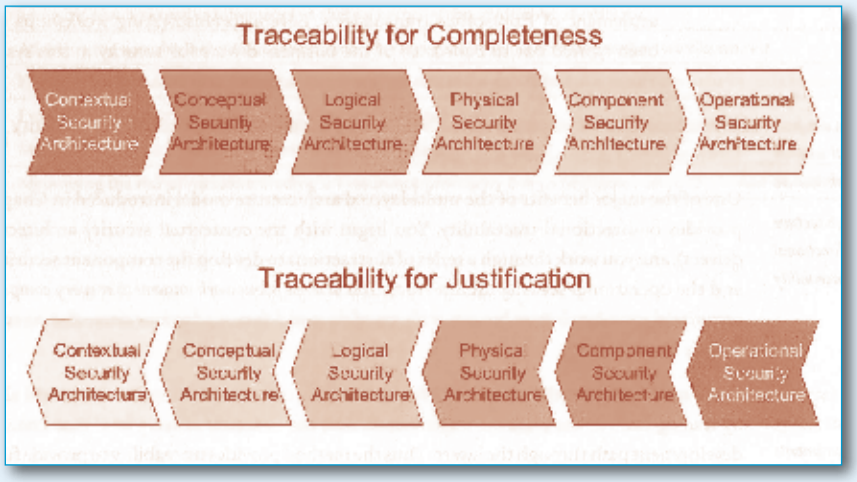


Figure 6-3: Two-Way Traceability

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Management	Business Process Model	Business Organisation & Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies & Architectural Layering	Security Equity Model & Trust Framework	Security Domain Model	Security Related Lifetimes & Deadlines

Figure 7-6: The Contextual and Conceptual Rows of the SABSA® Matrix

kanteling van de operationele laag wordt gegeven, is dat de operationele laag betekenis heeft in alle andere lagen. Nogal een zwak argument, dit wordt namelijk ook geïllustreerd door de traceerbaarheid (Figure 6-3, pagina 88).

Risico management is een gebied dat binnen SABSA op een plaats ingedeeld is en op verschillende plaatsen aangehaald wordt. Het is ingedeeld in de contextuele laag onder motivatie (Figure 7-6, pagina 115).

Business Risk Model

SABSA bevat een gedetailleerd proces voor de ontwikkeling van een security architectuur, dat ook aangeeft welke informatie waar wordt geproduceerd en waar wordt gebruikt (Figure 7-4 en 7-5, pagina 114). In dit proces worden de bedrijfsrisico's bepaald na een bedrijfsmodel en verschillende eisen. SABSA noemt dit deel van het proces de SABSA Risk Assessment Method, bestaande uit vijf stappen (pagina 205-208):

1. Bedrijfsmodel
   Beschrijf de drijfveren (drivers) en middelen (assets) van het bedrijf in het bedrijfsmodel. Het bedrijfsmodel wordt beschreven in bedrijfskenmerken (business attributes) (Figure 6-4, pagina 88).

2. Dreigingsanalyse
   Vanuit een vaste database met dreigingen (Table 9-1 t/m 9-7, pagina 191-205) en de impact die dat heeft op het bedrijf wordt het bedrijfsrisicomodel samengesteld. Er is een raamwerk om het draaiboek van het verloop van dreigingen te modelleren (Figure 9-2, pagina 202).

3. Impactanalyse
   De impact komt weer vanuit het bedrijfsmodel. Dit levert de bedrijfsrisico analyse deel 1.

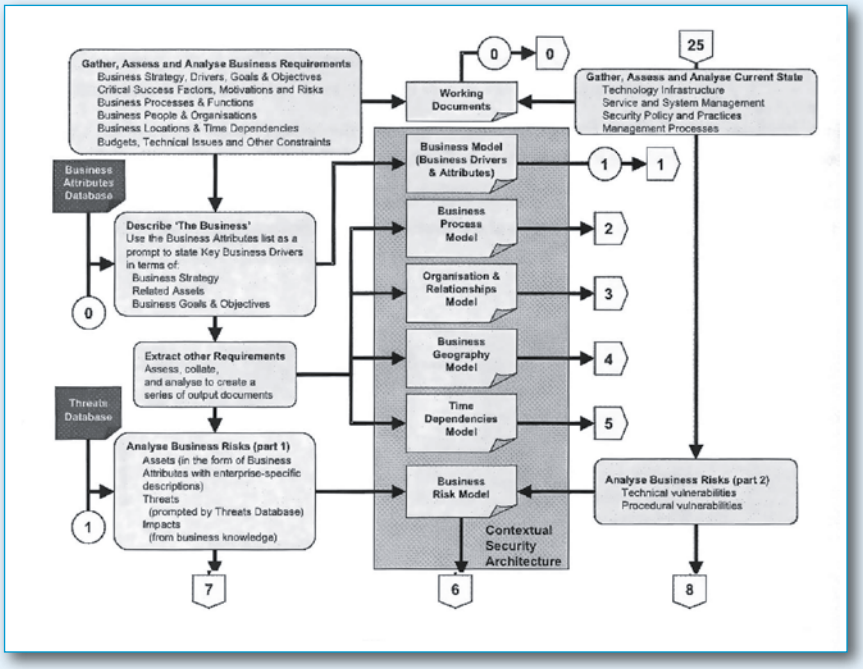


Figure 7-4: Developing the Contextual Security Architecture

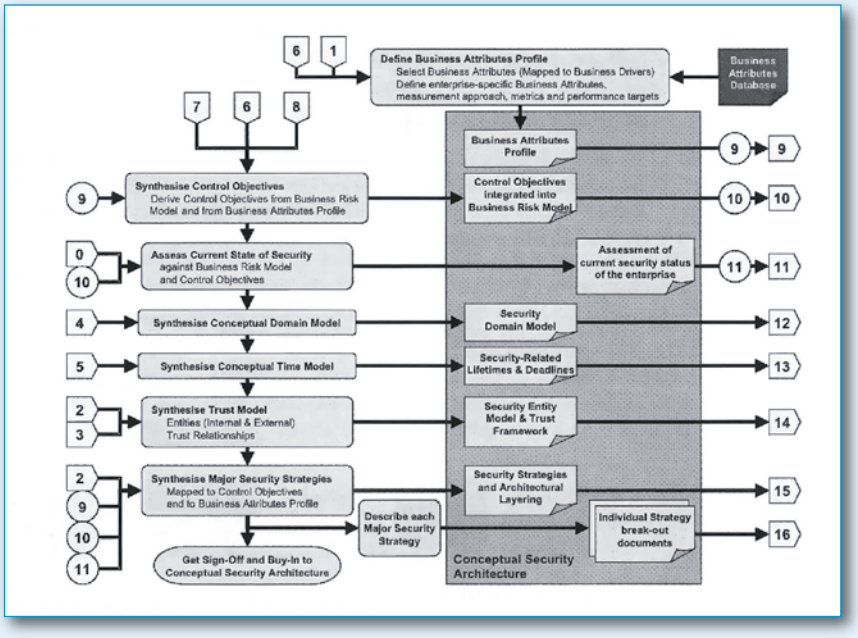


Figure 7-5: Developing the Conceptual Security Architecture

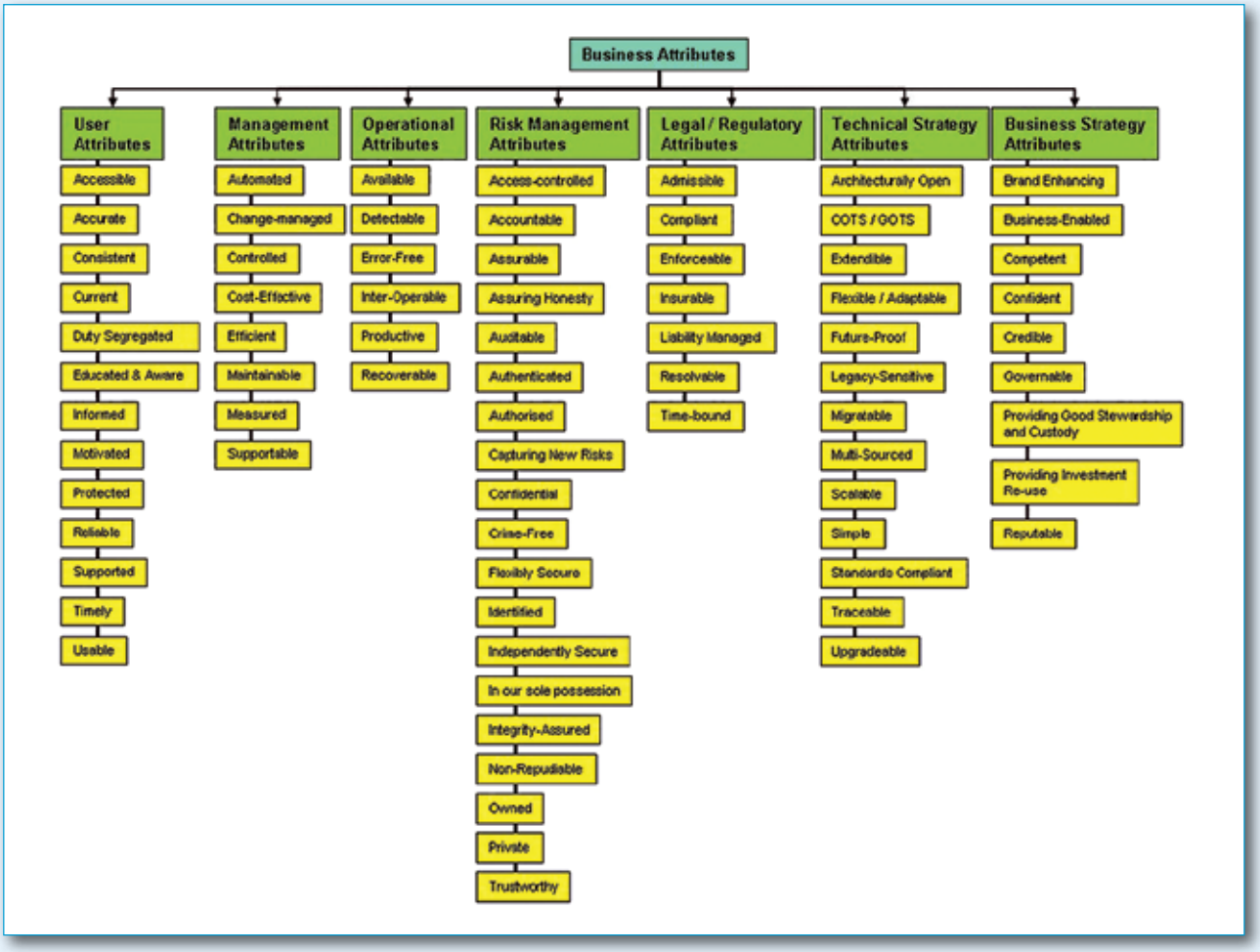


Figure 6-4: Taxonomy of Business Attributes

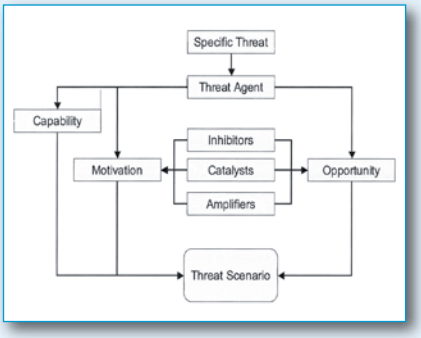


Figure 9-2: Framework for a Threat Scenario

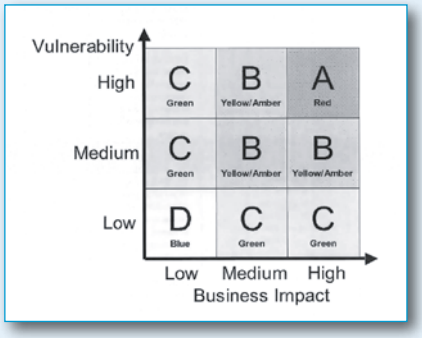


Figure 9-3: Mapping Risk Categorie to Impact and Vulnerability

4. Kwetsbaarheidanalyse
   Deze analyse voegt aan het bedrijfsrisicomodel de kwetsbaarheden toe, wat de bedrijfsrisico analyse deel 2 levert.

5. Risico categorisatie
   De twee analyses worden gecombineerd en in een risico categorie ingedeeld (Figure 9-3, pagina 208).

Beheersdoelen

Als volgende stap worden uit het business risk model de beheersdoelen (control objectives) afgeleid. Hiermee is de overgang van de contextuele laag naar de conceptuele laag gemaakt. Dit heeft vervolgens niets meer met risicomanagement te maken, behalve dat in de kwetsbaarheidanalyse de effecten van de beheersdoelen wordt meegenomen als terugkoppeling.

Conclusie

Risico management heeft een zeer duidelijke plaats in het SABSA raamwerk. De invulling van het raamwerk zelf is duidelijk afhankelijk van de risico analyse. Er wordt een gestructureerde methode beschreven die uitgaat van de drijfveren en middelen van het bedrijf. Hiermee valt SABSA niet in een valkuil zoals alleen de ICT middelen in het bedrijf te beschouwen of uit te gaan van een standaard checklist. De risico analyse zelf bevat de stappen die je van zo'n analyse mag verwachten, waarbij de verschillende stappen goed en duidelijk uit elkaar getrokken zijn. Hiermee heeft het resultaat van de analyse een duidelijke traceerbaarheid terug naar de uitgangspunten.

compromis

Het voorjaar is goed begonnen en ik lig ik in mijn hangmat te luisteren naar de vogeltjes die in mijn tuin zich te goed doen aan alles wat er gedurende de winter is komen te liggen. Met de ogen half dicht geknepen, kijk ik naar mijn huis dat nodig weer eens een schoonmaakbeurt nodig heeft, maar mijn aandacht gaat nog meer naar het raampje in de gevel.

Mijn huis is van het conventionele type, zoals dat vaak door kinderen wordt getekend: voordeur, puntdak, schoorsteen met rook eruit en een paar bomen erbij. Vijftien jaar geleden bedacht ik samen met mijn vrouw dat als we een huis wilden (laten) bouwen dat we er dan niet te lang mee moesten wachten en al snel kocht ik bij ons in de gemeente een stukje grond. Bij de overdracht van de grond kreeg ik van de gemeente een dik pak papier waarop alle bouwvoorschriften stonden en ik kwam er al snel achter dat ik wel verstand heb van IT, maar minder van bouwen van huizen. Dus ik ben maar eens op zoek gegaan naar een architect die mij kon helpen mijn reine stukje grond te voorzien van ons droomhuis.

De twee gevels waren al snel getekend en de eisen van vier slaapkamers, een ruime leefomgeving en een zeer ruime zolder waar ik mijn werk- en studeerkamer wilde hebben, stonden al snel op de bouwtekening. Avonden achter elkaar zaten mijn vrouw en ik gebogen over de tekeningen, inmiddels versie elf. We waren er bijna uit, ik had nog één probleem en dat was met mijn werk- en studeerkamer. Ik wilde namelijk niet alleen ramen in de schuine wanden, maar ook een bescheiden raam in de gevel van de woning. Zowel de voor- als de achtergevel moesten in de nok van de gevel een driehoekig raam hebben, waardoor het licht op de zolder perfect zou zijn. Op mijn verzoek ging de architect met versie twaalf aan de gang en toen deze tekeningen op de deurmat ploften, bleek wederom dat alles goed was, behalve dan dat de driehoekige raampjes ontbraken. Geërgerd belde ik de architect (laten we hem Jan noemen) die mij aangaf dat ik niet blij zou zijn met de kosten die de twee raampjes met zich mee zouden brengen. Jan noemde een bedrag en daar werd ik inderdaad niet blij van.

Ik nodigde Jan bij ons thuis uit om tijdens een goed glas wijn de dreigende impasse te bespreken. Na twee flessen wijn kon Jan mij nog steeds niet uitleggen waarom de prijs, van de in mijn ogen zeer kleine wens, zo hoog moest zijn. Ik wil u graag de uitleg van Jan besparen, maar na nog een flesje Kaapse Pracht kwam het hoge woord er uit. Meneer Jan vond het niet passen binnen zijn concept. Na een paar wijntjes word ik altijd zeer gevat en ik riep tegen Jan dat het ook niet in zijn concept moest passen, maar in mijn huis. Jan zette zijn glas neer en zei dat het dan wel mijn huis was, maar ook zijn ontwerp en dat was leidend. Ik mompelde nog dat het eigenlijk te gek was voor woorden dat ik niet mocht bepalen hoe mijn eigen huis eruit ging zien. U begrijpt, de investering van drie goede flessen wijn had zijn rendement niet opgebracht en de onderhandelingen zaten muurvast.

Na veel verbaal vuurwerk is het uiteindelijk toch goed gekomen en hebben we een compromis bereikt. De voorgevel van mijn huis bleef ongemoeid en de achtergevel is voorzien van mijn hartenwens. Toen de woning eenmaal door ons bewoond werd, zat ik tevreden op mijn zolder te werken toen ik achter in de tuin een bekende verschijning zag. Jan liep er rond. Ik zocht hem op en ik heb hem een rondleiding door het huis gegeven. Tot slot bekeken we mijn werk- en studeerkamer. Bewonderend keek hij naar mijn bureau en het inmiddels beruchte raam. Hij zei niets, maar ik kon het niet laten en ik vroeg aan hem of hij het mooi vond. Weer zei hij zei niets en ik gaf hem aan dat ik als eigenaar van de woning bijzonder tevreden was met mijn raampje. Zwijgend liep hij de zoldertrap af. Ik zweeg dit keer ook, maar bedacht dat het helemaal terecht was dat ik nu genoot van mijn raam.

Rillend word ik wakker. Ik rol uit mijn hangmat, jammer dat het in april tegen de avond al zo snel kouder wordt. Terwijl ik terugloop naar het huis kan ik de neiging niet onderdrukken om nog even naar boven te kijken. Glimlachend loop ik de keuken in.

Groeten,
Berry

NIEUW!

SOPHOS
secured.

Sophos Endpoint Security

Nu ook volledige disk encryptie, removable storage encryptie en Windows-based pre-boot authenticatie!

Kijk voor meer informatie op www.crypsys.nl of bel (0183) 62 44 44.

CRYPSYS Data Security B.V. - Benelux Distributeur van Sophos
Edisonweg 4 - 4207 HG Gorinchem - Postbus 542 4200 AM Gorinchem
T (0183) 62 44 44 - F (0183) 62 28 48 - E sales@crypsys.nl

CRYPSYS
data security