GvIB Expert Brief – December 2006
ISSN 1872-4876, Jaargang 2 – Nr. 4

December 2006

Security architectuur: Nieuwe hype voor specialisten of nuttig communicatiemiddel?

Henk Bel

Lucien Bongers

Lex Borger

Erno Duinhoven

Jo Koppes

Renato Kuiper

Tonne Mulder

Henny van de Pavert

Michel Ritskes

Kees Terlouw

Veel organisaties worstelen met de vertaling van het informatiebeveiligingsbeleid naar concrete maatregelen. Het beleid is vaak gedefinieerd in abstracte termen. Voor applicatie- of infrastructuurontwerpers is het lastig te bepalen welke beleidsuitspraken consequenties hebben voor hun verantwoordelijkheidsgebieden en op welke manier dit ingevuld dient te worden. Inzicht in de samenhang van beveiligingsmaatregelen ontbreekt.
Een security architectuur kan dit inzicht verschaffen en de complexiteit van mogelijke oplossingsrichtingen reduceren aan de hand van hanteerbare modellen en principes.
De expertgroep heeft getracht helder in kaart te brengen wat een security architectuur nu precies is en wanneer het zinvol is een security architectuur te ontwikkelen. Is het echt een nuttig communicatiemiddel of toch weer een hype?

Pagina

3 **DE ONDERZOEKSVRAGEN**
- Wat is een security architectuur, wat zijn de doelgroepen en wat is de relatie met andere architecturen?
- Waarom een security architectuur en wat is de business case?
- Wat staat er in en wat zijn kritieke succesfactoren?

3 **WAT IS EEN SECURITY ARCHITECTUUR?**
- Definitie en doelgroepen
- Wat is de relatie met andere architecturen?

6 **DE BUSINESS CASE**
- Een kwantitatieve en een kwalitatieve benadering
- Randvoorwaarden

9 **SCOPE EN INHOUD**
- Wat omvat een security architectuur?
- Nadere afbakening
- Welke architectuur modellen zijn bruikbaar als basis?

14 **CONCLUSIES EN VERVOLG**

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

2

INLEIDING EN SITUATIE SCHETS

Hebben organisaties naast een informatiebeveiligingsbeleid behoefte aan een security architectuur? Een vraag voor veel informatiebeveiligers maar ook voor architecten en managers. Om die vraag te kunnen beantwoorden hebben we behoefte aan een heldere omschrijving wat we bedoelen met een security architectuur. Wat is een security architectuur precies, wat is de toegevoegde waarde hiervan en wie heeft er belang bij?

De meeste organisaties ervaren een 'gat' tussen het beveiligingsbeleid en de praktische invulling hiervan in de praktijk. Vaak is er wel een beveiligingsbeleid aanwezig, maar de inhoud is niet direct toepasbaar voor architecten en ontwerpers. Het beleid beschrijft op hoog abstractieniveau welke doelen moeten worden bereikt, maar hoe dit gerealiseerd moet worden wordt niet aangegeven. De vertaalslag van beleid naar concrete praktische maatregelen is voor velen lastig te maken.
Dat heeft deels te maken met de verschillen in denken tussen beleidsmakers en de ontwerpers die specifieke oplossingen moeten uitwerken en realiseren. Ook zijn business en ICT omgevingen vaak zo complex dat het lastig is een goed inzicht te krijgen van de samenhang tussen alle security maatregelen in ICT en business omgevingen. Een helder inzicht ontbreekt. Resultaat is dat deeloplossingen niet optimaal op elkaar afgestemd zijn.
Technische of procedurele maatregelen voor een specifiek deelgebied worden dan maar geïmplementeerd op basis van 'best-practices', eisen van auditors, algemene richtlijnen van productleveranciers of normenkaders van beroepsverenigingen.
Of daarmee het beleid van de organisatie wordt gevolgd blijft onduidelijk. Een gedefinieerde beleidsdoelstelling effectief en efficiënt vertalen naar concrete maatregelen vraagt inzicht in de argumentatie achter de doelstelling en hoe dit past binnen de totale context van de organisatie. Zolang dit inzicht ontbreekt en risico's onvoldoende in kaart zijn gebracht blijft het lastig te bepalen waar en wanneer een doelstelling voldoende is gerealiseerd. Ook is het niet kosteneffectief om bij ieder deelsysteem of project het wiel opnieuw uit te vinden.
De vraag is in welke mate een security architectuur in deze situatie verbetering kan brengen.

Architectuur is het terrein waar de uitgangspunten, eisen van de belanghebbenden, de te hanteren basis principes, de structuur en de onderlinge samenhang van elementen inzichtelijk wordt weergegeven. Met het scheppen van inzicht en overzicht kan een architectuur voor een groot deel het 'gat' tussen beleidsmakers en ontwerpers overbruggen. Op gebied van security is deze behoefte nadrukkelijk aanwezig. Ook stelt het ontwerpers in staat daarmee grotendeels onafhankelijk van elkaar te werken. Architectuur dient veelal als communicatie-middel tussen verschillende partijen om overzicht en inzicht te krijgen van het geheel en om ieders belangen en plaats in het geheel op een begrijpelijke manier over te brengen.

Het ontwikkelen van een security architectuur vraagt echter om een gecoördineerde aanpak en vraagt investeringen die terugverdiend moeten worden. Voordat hierover een beslissing genomen kan worden moet eerst duidelijk zijn wat een security architectuur nu precies is, wat er in staat en met welke diepgang, wat het doel en de scope is, wie de belanghebbenden zijn, etc. En als je een security architectuur wilt ontwikkelen hoe doe je dat dan? Is er een business case te maken, zijn er basiscondities om een security architectuur zinvol te laten zijn en hoe pak je het vervolgens aan? En is een security architectuur voor iedere organisatie hetzelfde?

Deze expertbrief probeert op een aantal vragen antwoord te geven. De onderzoeksvragen die de expertgroep zichzelf gesteld heeft, staan hieronder genoemd. De vragen die de expertgroep niet heeft kunnen beantwoorden zullen in een vervolg sessie verder worden uitgewerkt.

DE ONDERZOEKSVRAGEN

De expertgroep heeft zich gebogen over de volgende vraagstelling:

- Wat is een security architectuur en wat is de relatie met andere architecturen zoals business, informatie, applicatie en infrastructuur architectuur?
- Waarom een security architectuur en wat is de business case? Is het hebben van een security architectuur belangrijk of is het gewoon een nieuwe hype?
- Voor wie heeft het welke toegevoegde waarde?
- Zijn er omstandigheden of condities die bepalen wanneer het ontwikkelen van een security architectuur wel of niet zinvol is?
- Welke aspecten en onderwerpen horen thuis in een security architectuur en met welke diepgang?
- Hoe ontwikkel je een security architectuur en welke basis architectuur modellen kunnen hiervoor gebruikt worden? Wat zijn hun sterke en zwakke kanten?
- Hoe borg je dat een security architectuur wordt ingevoerd en onderhouden en dat ze effectief wordt gebruikt?

De expertgroep heeft zich vooraf gerealiseerd dat het onwaarschijnlijk is dat al deze vragen in één expertsessie beantwoord konden worden. Uiteindelijk wil zij door vervolgactiviteiten wel graag een antwoord op al deze vragen.

WAT IS EEN SECURITY ARCHITECTUUR?

Er bestaan verschillende definities van wat architectuur is. Zo kunnen ook verschillende definities gegeven worden van wat een security architectuur is. De expertgroep heeft gekozen voor een definitie in eenvoudige en begrijpelijke taal. Het overbrengen van de essentie wordt belangrijker geacht dan het 100% wetenschappelijk correct en volledig weergeven.

> Een Security Architectuur is een voorschrijvend document dat door middel van een set samenhangende modellen en principes efficiënt en flexibel richting geeft aan de invulling van het informatiebeveiligingsbeleid van een organisatie.

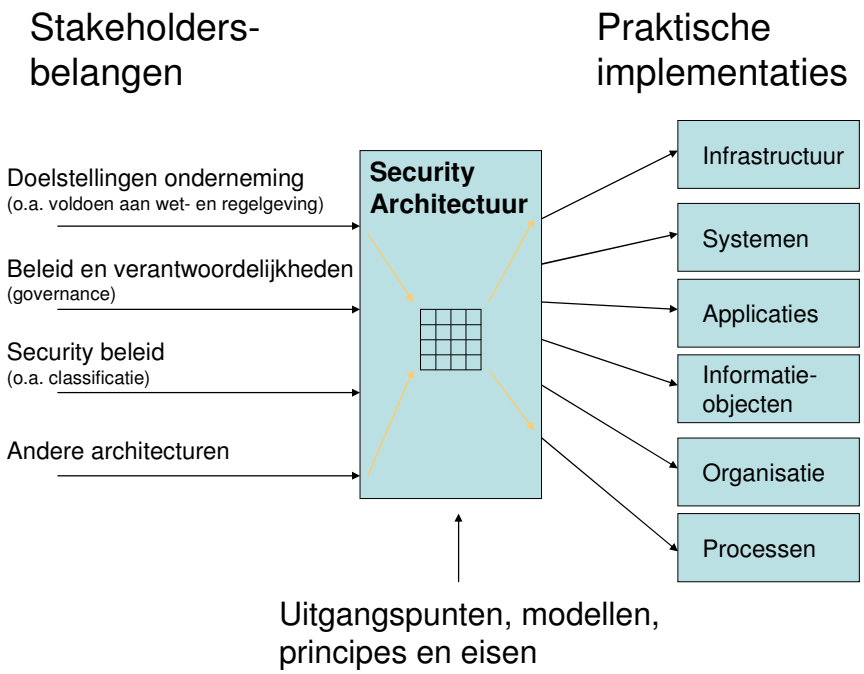
Anders gezegd:
Een security architectuur bestaat uit een transparant en samenhangend overzicht van modellen, principes, uitgangspunten en condities waarmee een concretere invulling wordt gegeven aan het informatiebeveiligingsbeleid meestal zonder in specifieke oplossingstermen te spreken. Een security architectuur reduceert een complex probleem tot te bevatten modellen, principes en deelproblemen, veelal aan de hand van de bekende wat, waar, wanneer, hoe, waarmee en door wie vragen. De modellen en principes geven aan waar je welk type maatregelen neemt, wanneer de principes van toepassing zijn en hoe ze samenhangen met andere principes.

De scope van een security architectuur ligt niet vast en kan sterk afhankelijk zijn van het doel of het probleem dat een organisatie daarmee wil oplossen. Ligt de focus primair op vertrouwelijkheid en integriteit of wordt beschikbaarheid ook meegenomen? Beveiliging van zeer geheime militaire informatie kan voor een defensie organisatie relevant zijn maar voor een industriële omgeving totaal niet. En de ene organisatie kan zich beperken tot algemene

richtlijnen met ruime vrijheid om dit in the vullen, terwijl een andere de keuze van maatregelen in veel meer detail wil vastleggen.
In veel gevallen ligt de focus op een verbijzondering van die eisen uit het informatie-beveiligingsbeleid die op een of andere manier in de ICT omgeving of de bijbehorende organisatie en processen geïmplementeerd moeten worden.
Security belangen vanuit de business en wet- en regelgeving vormen de belangrijkste input voor de beveiligingsarchitectuur, maar ook niet security gerelateerde belangen vanuit algemene ICT architectuur kunnen van grote invloed zijn op een security architectuur.

Doelgroepen

In feite is een security architectuur een hulpmiddel om de beveiligingsbelangen van de stakeholders op een gestructureerde en samenhangende manier te communiceren naar de partijen die er praktische invulling aan moeten geven. Maar ook kan het de communicatie en het inzicht tussen stakeholders onderling verbeteren.
Om als communicatiemiddel te kunnen dienen is het belangrijk dat begrippen eenduidig en helder gedefinieerd zijn voor de verschillende doelgroepen. De samenhang van begrippen geeft context aan de gebruikers van de architectuur.
Figuur 1 geeft nog eens grafisch weer hoe de belangen van verschillende stakeholders worden samengebracht, vertaald naar principes en zodanig geclusterd dat ze een bruikbare input vormen voor architecten en ontwerpers van verschillende aspectgebieden.



Figuur 1 De positie van een security architectuur

Belangrijk is om de stakeholders en gebruikers (doelgroepen) van een architectuur goed te onderscheiden. Stakeholders zijn diegenen die hun (business) belangen in de architectuur verwerkt willen hebben en doorgaans voor de financiering zorgen, terwijl de gebruikers de architectuur moeten gebruiken om er iets mee te realiseren. Stakeholders kunnen indirect ook weer gebruikers zijn.

De belangrijkste doelgroepen zijn:

Primaire doelgroepen	
(ICT) Architecten	zij hebben de security principes nodig om de juiste bouwstenen op de juiste plaats te kunnen definiëren met high-level security eisen.
Ontwerpers	zij hebben de security principes nodig om bouwstenen en services te ontwerpen volgens deze principes in de context van de security architectuur
Security specialisten	zij gebruiken de architectuur om de organisatie consistent te adviseren over security eisen waar services en systemen aan moeten voldoen.
Secundaire doelgroepen zijn onder andere	
Business managers	zij financieren de beveiliging, stellen de eisen en kunnen uit de architectuur op hoofdlijnen opmaken hoe hun business informatie wordt beveiligd. Door gestructureerd te werken volgens een security architectuur kunnen zij beter verantwoorden dat zij stelselmatig werken aan een goede bescherming van bedrijfsinformatie en informatieverwerkende systemen.
Auditors	zij kunnen de architectuur gebruiken als toetsingsinstrument tijdens hun controles.

Afhankelijk van de organisatie kunnen mogelijk nog andere specifieke doelgroepen worden onderkend, zoals externe toezichthouders.
Belangrijk is om een security architectuur zodanig te structureren en te verwoorden dat het voor elke doelgroep toegankelijk en begrijpelijk is. Dit kan bijvoorbeeld door het creëren van views voor de verschillende stakeholders / doelgroepen.

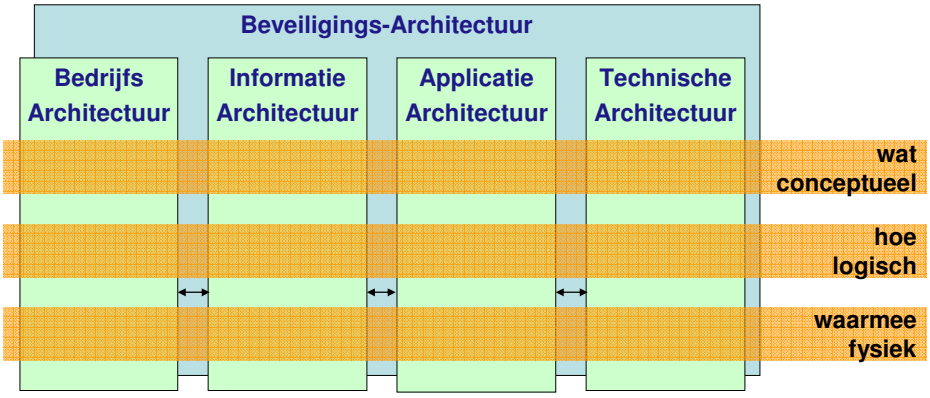
Security architectuur in relatie tot andere architecturen

Is een security architectuur een aparte architectuur in een apart document naast andere architecturen? Dat kan, maar hoeft niet. In essentie is het een view op onderliggende business, informatie, applicatie en technische architecturen. Security aspecten kunnen in een apart document worden weergegeven, maar ze kunnen ook in elk van de onderliggende architecturen zijn beschreven. Ook de exacte invulling en opdeling in architectuurdomeinen of de volledige invulling hiervan is niet van essentieel belang. Wel is belangrijk dat het geheel aansluit waardoor de traceerbaarheid van uitgangspunten en eisen naar maatregelen gewaarborgd wordt.

In figuur 2 is dit grafisch weergegeven.

6

Beveiligings-Architectuur in relatie tot andere architecturen



Figuur 2 Relatie met andere architecturen

Voordeel van het vastleggen van een security architectuur als aparte architectuur is dat het overzicht en de samenhang tussen alle uitgangspunten, modellen, principe, keuzes en maatregelen beter naar voren komt.

DE BUSINESS CASE

Op basis van welke criteria kan een organisatie beslissen of het een security architectuur wil ontwikkelen? Zijn er kenmerkende condities en randvoorwaarden te onderkennen die dit bepalen?

Algemene voordelen van werken onder architectuur zijn complexiteitsbeheersing, kostenbesparing en creëren van uniformiteit/standaardisatie. Deze voordelen gelden onverminderd voor een security-architectuur. De vraag is echter of de voordelen van het werken onder architectuur groot genoeg zijn om de investeringen te rechtvaardigen. En hoe bepaal je dat dan?

De kwantitatieve benadering

De kosten van het ontwikkelen van een security architectuur zijn redelijk goed in te schatten, de baten echter veel minder goed. Bij baten kan gedacht worden aan kostenbesparing door bijvoorbeeld:

- Minder vaak opnieuw ‘het wiel uit te vinden’ in requirements-specificatie trajecten. Toepassing van de richtlijnen van een security architectuur kan veel tijdwinst opleveren in projecten.
- Eenmalige inrichting en goed hergebruik van generieke bouwstenen. Hierdoor kan de omvang en complexiteit van individuele projecten worden gereduceerd.

- Sneller en met minder inspanning realiseren van nieuwe diensten. Flexibiliteit en time-to-market van nieuwe producten en diensten wordt steeds belangrijker en kan businessvoordelen opleveren.
- Beperking van kapitaalvernietiging door onevenwichtige en incompatibele maatregelen. Een onbalans van maatregelen kan veel kosten tot gevolg hebben en toch onvoldoende veiligheid bieden.
- Realiseren van een meer uniform en beter aantoonbaar niveau van beveiliging.

Veel baten zijn echter verborgen baten, die lastig zichtbaar te maken zijn. Verder is een handicap dat er binnen het vakgebied informatiebeveiliging bijna geen kengetallen beschikbaar zijn die aangeven in welke mate kostenbesparing kwantitatief gerealiseerd kunnen worden. Daarnaast zijn de kosten van specifieke security maatregelen in ICT omgevingen en processen vaak niet inzichtelijk, waardoor ook de besparingen hierop lastig in kaart te brengen zijn.

De beschikbaarheid van betrouwbare uitgangsgegevens voor een business case is mede afhankelijk van het maturity level van een organisatie. Immers naarmate een organisatie zijn processen beter beheerst zullen er meer gedetailleerde en betrouwbare meetgegevens beschikbaar zijn over kosten en mogelijke besparingen.
Als een organisatie voortdurend kosten maakt voor ad-hoc oplossingen om beveiligingsproblemen het hoofd te bieden, zou zij moeten overwegen of een investering in een security architectuur zichzelf niet snel terugverdient.

Op basis van genoemde besparingen kan ook geconcludeerd worden dat het werken met een security architectuur voordelen heeft voor de organisatie als geheel, maar niet per definitie voor ieder individueel project of systeem.
Daarom mag een security architectuur ook geen vrijblijvend karakter hebben. Zonder een mate van dwang zullen de beoogde voordelen van het werken onder architectuur niet of beperkt worden gehaald. Het is belangrijk dit goed te communiceren naar alle doelgroepen. Het hogere management moet dit ook ondersteunen.

De kwalitatieve benadering
De praktijk leert dat beslissingen over het ontwikkelen van een security architectuur zelden op basis van zuiver economische argumenten worden genomen. Veel belangrijker is het of er een invloedrijke stakeholder aanwezig is met een duidelijke visie en overtuiging dat het werken onder architectuur belangrijk is.
Deze overtuiging kan gebaseerd zijn op eerder ervaringen of goede adviezen, maar kan ook eenvoudig ingegeven zijn door het feit dat branchegenoten het ook doen of omdat het een nieuwe trend is waarbij men niet wil achterblijven.
Ook de visie dat de organisatie veiliger wordt door het kiezen van een gestructureerde aanpak kan een belangrijke motivator zijn.

Een organisatie met een laag volwassenheidsniveau heeft vaak weinig historische gegevens beschikbaar over project kosten en dus is daar de aanwezigheid van een invloedrijke stakeholder vrijwel altijd doorslaggevend bij een beslissing tot het ontwikkelen van een security architectuur.
In meer volwassen organisaties kan een stakeholder een kosten/baten analyse gebruiken om zijn reeds bestaande overtuiging verder te onderbouwen.

Geconcludeerd kan worden dat het hebben van een invloedrijke stakeholder met een heldere visie en overtuiging alsmede het aanwezig zijn van een algemene architectuur aanpak voor ICT belangrijker is dan het hebben van sluitende ROI berekeningen.

Een security architectuur is zelden de eerste architectuur die een organisatie ontwikkelt. Als de trend om volgens architectuur principes te werken al is ingezet, zal een beslissing om ook een security architectuur te ontwikkelen makkelijker worden genomen.
Specifiek op het terrein van security is de behoefte aan 'vertaling' van business behoeften en beleid naar concrete maatregelen groter dan bij functionele specificaties. De reden is dat security veelal als een niet-functioneel kwaliteitsaspect wordt gezien waarvan de kennis bij velen onvoldoende is. Business managers vinden het vaak ook lastig om hun security eisen en wensen concreet te maken en om aan te geven welke wet- en regelgeving van belang is. Deze behoefte aan 'vertaling van beleid' is in veel gevallen nog niet onderkend door stakeholders, die vaak ook de budgethouders zijn. Daarnaast is het voor business managers vaak onvoldoende inzichtelijk wat security bijdraagt aan hun resultaat en worden ze er niet op afgerekend.

De voordelen van het hebben van een security architectuur zijn afhankelijk van de complexiteit en overzichtelijkheid van de ICT omgeving. Naar mate deze omgeving complexer is zal er meer behoefte zijn aan reductie van complexiteit. Of in geval van een sterk gedistribueerde omgeving, waarbij het overzicht moeilijk te krijgen is, is het erkennen van duidelijke principes en condities belangrijker dan in een simpele omgeving.

Randvoorwaarden
In figuur 1 staat een aantal bronnen genoemd die de uitgangspunten moeten leveren voor de security architectuur. De beschikbaarheid van de informatie uit deze bronnen vormt een belangrijke voorwaarde voor het kunnen neerzetten van een goede security architectuur. Als doelstellingen en verantwoordelijkheden niet duidelijk zijn, is het moeilijk een zinvolle security architectuur te ontwikkelen.

- De doelstellingen van de organisatie moeten duidelijk zijn evenals het risicoprofiel dat de organisatie kiest. De mate van beveiliging moet immers in overeenstemming zijn met de waarde van de informatie en risico's die de organisatie wil en mag nemen. Dit risicoprofiel wordt enerzijds bepaald door het businessmodel van de organisatie en anderzijds door de dreigingen en de wet- en regelgeving voor de branche waarin een organisatie opereert. Soms is het lastig een eenduidig risicoprofiel vast te stellen omdat verschillende divisies van een organisatie uiteenlopende belangen kunnen hebben en in verschillende marktsegmenten opereren.
- De organisatie moet een heldere governance structuur hebben met duidelijk belegde verantwoordelijkheden. De diepgang waarmee een security architectuur ingevuld kan worden, kan bijvoorbeeld sterk beïnvloed worden door de vrijheid die decentrale organisatieonderdelen hebben om onafhankelijke keuzes te maken.
- De organisatie moet een security beleid hebben waarin de uitgangspunten voor informatiebeveiliging helder zijn vastgelegd. Classificatie van informatie is daarin een essentieel element om security eisen te kunnen differentiëren per classificatiegroep. De kosten van de te nemen maatregelen en de lasten van eventuele extra maatregelen moeten immers afgestemd zijn op de potentiële business risico's die per classificatiegroep gelopen worden.

Classificaties zijn vaak gebaseerd zijn op gangbare vertrouwelijkheidniveaus, zoals publiek, uitsluitend voor intern gebruik, confidentieel en geheim, maar kunnen ook speciale kenmerken betreffen, zoals medisch geheim. Daarnaast kunnen voor integriteit en beschikbaarheid classificaties gedefinieerd zijn.

- Basisprincipes vanuit andere architecturen, zoals een algemene ICT architectuur, kunnen mede bepalen welke risico's relevant zijn. Een organisatie waarin veel medewerkers voorzien worden van laptops en verwijderbare media, zoals USB-sticks of CD's, om daarmee flexibiliteit en mobiliteit te realiseren, loopt andere risico's dan een organisatie waar de medewerkers uitsluitend 'domme' terminals ter beschikking hebben.

Groeimodel
Als een organisatie weinig ervaring heeft met werken onder architectuur of in een security architectuur niet te veel wil investeren kan gekozen worden om initieel een 'lean and mean' basis architectuur neer te zetten zonder veel diepgang. Alleen al het neerzetten van de belangrijkste basis principes kan een organisatie een flink stuk in de goede richting helpen. In een latere fase kan de architectuur verder worden uitgediept of kunnen specifieke aspecten worden toegevoegd.
Om van een security architectuur te kunnen spreken moet wel voldaan worden aan basiskwaliteiteisen. De kwaliteit van een security architectuur kan beoordeeld worden aan de mate dat het voldoet aan de volgende aspecten: een architectuur moet een totaal overzicht bieden, moet transparant en evenwichtig zijn en de samenhang helder aangeven.

SCOPE EN INHOUD

Als besloten wordt tot het ontwikkelen van een security architectuur rijst de vraag wat er wel en wat er niet in zou behoren te staan. Anders gezegd, wat wordt de scope en de inhoud?
En is er een eenduidig lijstje welke aspecten minimaal in een security architectuur behoren en welke 'nice-to-have' zijn? Zijn er kritieke succesfactoren die een security architectuur wel of niet tot een nuttig instrument maken?

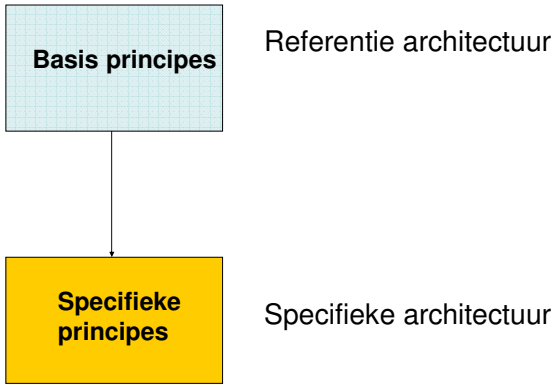
Scope

De scope van een security architectuur is een van de eerste aspecten die vastgesteld moeten worden. Dit kan worden bepaald aan de hand van verschillende vragen:

- Welke aspecten van security neem je wel of niet mee? Gaat het alleen over vertrouwelijkheid of moeten ook integriteit en beschikbaarheid worden meegenomen?
- Moet fysieke security compleet worden meegenomen of alleen die zaken die direct gerelateerd zijn aan informatievoorziening?
- Hoe complex is de omgeving waarvoor de security principes moeten worden vastgesteld en welke detail niveau is gewenst? Kies je er bijvoorbeeld voor op een hoog abstractie niveau te blijven en alleen basis principes vast te leggen, waarbij delen van de organisatie veel ruimte krijgen om dit verder in te vullen (referentie-architectuur) of ga je voor een meer specifieke architectuur?

  Bij een grote multinational met sterk verschillende divisies kan bijvoorbeeld gekozen worden alleen te beschrijven hoe de divisies met elkaar gekoppeld moeten worden en

op welke wijze er gecommuniceerd mag worden zonder vast te stellen hoe de divisies dit binnen de eigen geledingen moeten regelen. De divisies moeten dan binnen de principes van de referentiearchitectuur zelf een meer divisie-specifieke invulling van de security architectuur maken.
In figuur 3 is dit nog een weergegeven.



Figuur 3 Architectuur op verschillende niveaus

- Voor welke doelgroepen is de architectuur? Is het voldoende tot en met de logische architectuur te gaan of is het wenselijk om ook voor de fysieke laag keuzes voor te schrijven. Ontwerpers hebben vaak behoefte de architectuur 'zo concreet mogelijk' te laten zijn.
- Moet alleen een blauwdruk van de gewenste (SOLL) situatie worden beschreven of moet rekening worden gehouden met een transitie vanuit de huidige (IST) situatie nar de gewenste (SOLL) situatie?

Wat omvat een security architectuur?

Er bestaan verschillende modellen voor het beschrijven van architecturen, zoals het Zachmann model, het TOGAF model van de Open Group of het Integrated Architecture Framework.
Security-specifieke modellen zijn het SABSA model, wat eigenlijk een security verbijzondering is van het Zachmann model, en de Enterprise Security Architecture van het Network Applications Consortium. Beiden bevatten ook procesmodellen om te komen tot een security architectuur en om deze te onderhouden.

Hoewel security architectuur modellen verschillen, hebben ze allemaal een zekere gelaagdheid. Zoals al eerder is aangegeven is het niet van essentieel belang hoe de verschillende gerelateerde architecturen precies zijn beschreven of afgebakend.

Belangrijk is wel in elk geval 4 lagen te onderscheiden:

- een business (context) laag,
- een conceptuele laag
- een logische laag en
- een fysieke laag

De business laag
De business laag beschrijft de basis aannames, uitgangspunten en overtuigingen die afgeleid zijn van de organisatiemissie, waarden en normen en governance principes van de organisatie. Daarnaast beschrijft het op hoofdlijnen de organisatie specifieke business principes, business opportunities, compliance-eisen, de geldende wet- en regelgeving en bedreigingen die voor de specifieke business onderkend worden. Dreigingen variëren vaak sterk afhankelijk van de locatie of zone waar informatie verwerkt wordt, de aard van de business en de waarde van de informatie. Daarom is het verstandig dreigingen specifiek te maken voor bepaalde omgevingen en voor de verschillende soorten business processen die een organisatie heeft.

De inhoud van de business laag heeft een sterke relatie met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid wordt immers als uitgangspunt overgenomen in de security architectuur.
Het is essentieel om een goede scheidslijn te trekken tussen wat in het beleid moet staan en wat in de architectuur. Verantwoordelijkheden en de vereiste controls dienen in het beleid te worden vastgelegd. De security architectuur geeft een gestructureerde invulling van het beleid. Indien tijdens het opstellen van de security architectuur blijkt dat beleidsuitspraken ontbreken, waardoor geen goede invulling kan worden gemaakt in de architectuur, dan is het beter deze beleidsuitspraken niet in de architectuur vast te leggen, maar alsnog aan het informatiebeveiligingsbeleid toe te voegen. Het vaststellen van beleid is immers geen bevoegdheid van de architect.

De conceptuele laag
Op basis van de in het beleid gedefinieerde informatie en waardeobject classificatie beschrijft deze laag modellen en concepten met informatiestructuren, -stromen en –objecten. Per classificatie moeten de security principes en beveiligingsnormen voor deze informatie worden aangegeven.
Een adequate classificatie en een duidelijk onderscheid in niveau van maatregelen per classificatie is een essentieel element van een security architectuur. Immers niet alle informatie en alle objecten hoeven op dezelfde manier beveiligd te worden. De mate van bescherming is afhankelijk van de vereiste niveaus van vertrouwelijkheid, integriteit en beschikbaarheid. Met het classificeren van informatie vindt op hoofdlijnen een eerste schifting plaats van de maatregelen die nodig zijn voor adequate beveiliging.

De logische laag
Binnen de architectuur beschrijft de logische laag op een gestructureerde manier de controls die nodig zijn voor verschillende aspectgebieden. Aangegeven moet worden welke controls nodig zijn, waar welke controls ingezet moeten worden, onder welke condities, wie verantwoordelijk is voor beheer van de controls etc. Het is wenselijk de security controls daarbij te groeperen naar aspectgebieden.
Voorbeelden van deze gebieden zijn:

- Identificatie en authenticatie (hoe stel je vast wie iemand is).
- Autorisatie (wat mag iemand doen en hoe wordt dit op hoofdlijnen beheerd).
- Encryptie (wanneer en waar moet versleuteling van informatie plaatsvinden).
- Isolatie (welke zones of deelsystemen worden onderscheiden en welke controles moeten plaatsvinden op de koppelvlakken).
- Beheer (welke zaken moeten centraal en welke decentraal geregeld worden)
- Logging en monitoring (wat registreren en hoe deze informatie nuttig gebruiken).

De logische laag specificeert nog niet welke technische middelen nodig zijn, maar wel waar ze functioneel en kwalitatief aan moeten voldoen. Zo kan beschreven worden wanneer sterke authenticatie nodig is, waarbij zowel kennis als een vorm van bezit wordt vereist, en wanneer zwakke authenticatie voldoende is, waarbij alleen kennis wordt vereist. Met welke technische middelen sterke authenticatie moet worden gerealiseerd wordt hierbij niet vastgelegd. Dit is iets voor de fysieke laag.
Bij al deze zaken moeten ook de eisen ten aanzien van gebruikersgemak worden meegewogen en welke maatregelen redelijkerwijze van een klant of partner worden mogen verwacht. Belangrijk is om de samenhang van principes en maatregelen helder aan te geven, zodat duidelijk wordt hoe het geheel de gewenste beveiliging biedt.

Op basis van dit overzicht kunnen gebruikers van de architectuur bepalen welke aspecten binnen hun verantwoordelijksgebied moeten worden ingevuld en welke aspecten door andere deelgebieden ingevuld zouden moeten zijn. Een goede afbakening van verantwoordelijkheidsgebieden is daarbij uiteraard voorwaarde.

Veel security architecturen gaan niet verder dan de logische laag omdat het functioneel beschrijven van security controls vaak voldoende is als input voor het opstellen van requirements. Dit geldt zowel voor interne projecten als ook voor extern te verwerven systemen of services. In het laatste geval is een functionele beschrijving met aansluitvoorwaarden van de security functies in een RFI of RFP meestal voldoende. De keuze voor fysieke implementatie kan dan worden overgelaten aan de leverancier.

Het is mogelijk binnen de logische laag nader onderscheid te maken tussen applicaties en infrastructuren. Echter met de toenemende ‘middleware’ is deze scheidslijn steeds moeilijker te trekken.

De fysieke laag
Soms zijn er redenen om ook de implementatie van logische functies specifieker te definiëren uit oogpunt van bijvoorbeeld kostenbesparing door standaardisatie of vereiste interoperabiliteit. Zo kan het zijn dat een organisatie een speciale keuze van sterke authenticatie consequent wil doorvoeren of specifiek vereist dat uitsluitend bepaalde goedgekeurde versleutelalgoritmes gebruikt moeten worden. Dit zijn zaken die in de fysieke laag beschreven kunnen worden. Risico van te veel diepgang en detail in een security architectuur is dat het als een bureaucratische hindernis ervaren kan worden en niet als nuttig hulpmiddel. Naar mate een architectuur gedetailleerder en omvangrijker is, wordt de kans groter dan gebruikers niet de tijd hebben of de motivatie hebben de belangrijke aspecten hiervan tot zich te nemen.
Ook dienen veranderingen in technologische mogelijkheden dan regelmatig bekeken te worden op hun impact voor de security architectuur.

Nadere afbakening

Is risicoanalyse onderdeel van de security architectuur?
Risicoanalyse is een proces dat op verschillende plaatsen in ontwikkeltrajecten en operationele processen plaatsvindt. Voorafgaand aan het opstellen van een security architectuur is het wenselijk op hoofdlijnen het dreigingenprofiel voor de organisatie vast te stellen. De architectuur moet aangeven op welke wijze processen en systemen beschermd moeten worden tegen deze dreigingen. Principes moeten zoveel mogelijk worden vastgelegd in termen van stabiliteit van processen en systemen (tegengaan van storingen) en niet in

termen van maatregelen tegen specifieke dreigingen. Dreigingen veranderen sneller dan de updatecyclus van een architectuur (doorgaans 3 tot 5 jaar) en de architectuur moet ook beveiliging bieden tegen nieuwe dreigingen.

Een belangrijke reden om met classificaties te werken is dat niet elke keer complete risicoanalyses gedaan hoeven te worden. Bij het uitwerken van de maatregelen per classificatie zijn de risico's op hoofdlijnen al impliciet meegenomen.
Bij een implementatietraject kan het wel nodig zijn nadere risicoanalyses uit te voeren om bijvoorbeeld de meest geschikte fysieke implementatie van een logische functie te bepalen. De architectuur biedt voornamelijk een set van principes en maatregelen die nader ingevuld moeten worden.

Geconcludeerd kan worden dat risico analyse op hoofdlijnen nodig is om een security architectuur te definiëren, maar dat het uitvoeren van een risicoanalyse voor een specifieke situatie geen onderdeel van een security architectuur. Het hebben van een security architectuur kan een risicoanalyse wel vereenvoudigen.

Wanneer is een security architectuur goed genoeg?
Zoals in dit artikel al eerder is aangegeven is de invulling van een security architectuur sterk afhankelijk van het doel, de doelgroep en de scope van de architectuur.
Voor goede acceptatie is het belangrijk is dat de security architectuur bruikbaar is voor de doelgroepen. Definities moeten eenduidig zijn en de woordkeuze moet aansluiten bij de behoefte van de doelgroepen. Voor elke doelgroep moet er een 'view' zijn.
Verder moet de architectuur voldoen aan de eerder genoemde kwaliteitseisen.
De omvang en diepgang van een architectuur is sterk afhankelijk van de complexiteit van de business en (ICT) omgeving en de behoefte bij de doelgroepen aan reductie van de complexiteit tot hanteerbare modellen en principes.

Verantwoording van principes en traceerbaarheid vanuit het informatiebeveiligingsbeleid zijn belangrijk voor het inzicht van de gebruiker in het geheel van de security architectuur. Overigens is niet iedere gebruiker hierin in gelijke mate geïnteresseerd. Een ontwerper die voor een applicatieontwerp simpelweg de security maatregelen moet implementeren zal vaak minder geïnteresseerd zijn in het waarom en de verantwoording van de principes dan een architect die de samenhang van security principes met andere architectuurprincipes moet begrijpen om de specifieke keuzes te kunnen maken.

Kun je een security architectuur maken zonder de andere architecturen te kennen?
In theorie kan men wel een security architectuur opstellen zonder de onderliggende business, informatie, applicatie en technische architectuur en het risicoprofiel te kennen, alleen dat is niet kosteneffectief en leidt tot overbodig werk. Er moeten dan al snel te veel principes worden beschreven omdat over veel mogelijke scenario's iets vastgelegd moet worden. Daarmee kan de security architectuur erg omvangrijk worden en minder toegankelijk voor degenen die er mee moeten werken.

Daarmee is eigenlijk ook gelijk de vraag beantwoord of het mogelijk is een generieke 'blueprint' van een security architectuur te maken die voor een grote variatie aan organisaties toepasbaar is. Liever niet dus!

Wel is het mogelijk een 'aanbod' architectuur te maken, zonder de business en informatielagen precies te kennen. Door aannames te doen of uit te gaan van basis modellen

betreffende deze lagen is het mogelijk een infrastructuurgerichte architectuur te maken. Dit kan een nuttige keuze zijn voor grote multinationals met businessunits die in sterk verschillende markten opereren. Traceren van maatregelen vanuit de businesseisen is dan niet mogelijk waardoor het onzeker blijft of de architectuur voldoende houvast biedt.

Welke architectuur modellen zijn bruikbaar?

Hierboven zijn al verschillende architectuur modellen genoemd, die elk hun eigen voor- en nadelen hebben.
Een goed model is van belang om op een gestructureerde manier de benodigde elementen van een security architectuur te identificeren. Het is echter ook mogelijk elementen van verschillende modellen te gebruiken.
De expertgroep heeft nog geen uitgesproken mening kunnen vormen van de voor- en nadelen van de genoemde modellen en welk model in welke situatie het best toepasbaar is.

CONCLUSIES EN VERVOLG

De expertgroep is er in geslaagd om antwoorden te vinden op een groot deel van de gestelde vragen.
Een definitie van security architectuur is gegeven en de inhoud is op hoofdlijnen beschreven. Ook is aangegeven wat belangrijk is om te komen tot een besluit om een security architectuur te gaan ontwikkelen. Op basis van enkel een harde business case met kosten en baten zal zit besluit niet snel genomen worden. Belangrijker is invloedrijke stakeholders te vinden met visie voor werken onder architectuur.

Een algemene conclusie is dat een security architectuur nuttig is als communicatiemiddel en bijdraagt aan een beter inzicht in de security requirements voor onderdelen van de ICT omgeving en de organisatie. Tevens kan een security architectuur een beter zicht geven op de balans en consistentie van de informatiebeveiliging van de gehele organisatie en kan het bijdragen om flexibeler en sneller nieuwe (business) services op te zetten.
De mate waarin deze voordelen tot uiting komen is afhankelijk van diverse factoren, waar onder de complexiteit van de ICT omgeving (en dus de behoefte aan reductie hiervan), de business risico's, de dynamiek van een organisatie, etc.

Kritieke succesfactoren voor het ontwikkelen van een security architectuur zijn het hebben van beleid en een classificatiesysteem voor beveiliging, bruikbaarheid voor de doelgroepen en de beleving dat met een security architectuur de complexiteit wordt gereduceerd en een betere beveiliging kan worden gerealiseerd.
Het opstellen van een generiek bruikbare 'blueprint' van een security architectuur lijkt niet praktisch haalbaar. Security architecturen kunnen heel verschillend worden ingevuld afhankelijk van doel en scope.

De vragen hoe je een security architectuur ontwikkelt en hoe je borgt dat een security architectuur effectief en consequent wordt gebruikt zijn nog onvoldoende beantwoord.
De expertgroep zal deze vragen in een vervolg sessie proberen te beantwoorden. De expertgroep is erg benieuwd naar de toegevoegde waarde van deze expertbrief voor u en ontvangt graag commentaar.
U kunt uw reacties sturen naar expertbrief@gvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

LITERATUURLIJST

Voor het tot stand brengen van deze expertbrief heeft de werkgroep de volgende literatuur geraadpleegd:

Aaldert Hofman, *Inbouwen in plaats van aanbouwen, Informatie mei 2004*

Win Sonnemans en Renato Kuiper, *Beveiligingsarchitectuur ICT, Openbare orde en veiligheid. ITSMF seminar 14 september 2005, www.itsmf.nl*

Network Application Consortium, Enterprise Security Architecture, A Framework and Template for Policy-Driven Security , 2004, http://www.netapps.org

Lucien Bongers, *Security binnen enterprise architecture. Radboud Universiteit Nijmegen, 10 februari 2006.*

John Sherwood, Andrew Clark, David Lynas, *Enterprise Security Architecture,, A Business-Driven Approach, 2005. Uitgeverij CMPBooks, ISBN 1-57820-318-X*

John Sherwood, Enterprise Security Architecture, SABSA, September 2003. www.sherwoodassociates.co.uk

Henny van de Pavert, *Security architecture Rabo groep. ISF O&G Chapter meeting 23 mei 2005.*

Renato Kuiper, *Architecten debat, 21 juni 2006, PI/GvIB themamiddag. www.pi4ib.nl*

Nico Visser en Renato Kuiper, *Artikelen serie Beveiliging bouwen onder architectuur. Informatiebeveiliging nummer 7,8-2002 en nummer 1van 2003, ww.gvib.nl*

Leo van Koppen, *Ontwikkeling van een security architectuur voor de Haagse School.MSIT thesis* TIAS Business School Eindhoven, 2005.

Network Applications Consortium, *Enterprise Security Architecture, a framework and template for policy-driven security, 2004*

Open Group, *The Open Group Architecture Framework (TOGAF)*

Sherwood Associated Limited, *SABSA (Sherwood Applied Business Security Architecture)*

16

APPENDIX GEBRUIKTE LICENTIEVORM

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

Deze pagina ziet er op het moment van schrijven als volgt uit:

creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

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

Onder de volgende voorwaarden:

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

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

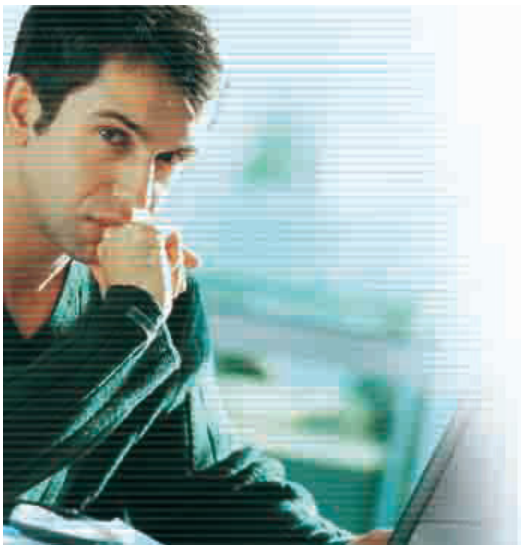
- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

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

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

Vrijwaring

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



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

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

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

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

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

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