Efficiënt beveiligings-management

Werken onder beveiligingsarchitectuur

Dr. ir. P.L. Overbeek RE en drs. E.P. Rutkens

Werken onder beveiligingsarchitectuur kan, mits met verstand toegepast, een bijdrage leveren aan het snel en flexibel reageren op veranderende klantbehoeften en bedrijfsdoelen. Door het werken onder beveiligings-architectuur procesmatig in te richten kunnen bovendien positieve kosteneffecten worden gerealiseerd. In een tijd van snelle technologische ontwikkelingen, een markt die voortdurend in beweging is en veranderende wet- en regelgeving is een beveiligingsarchitectuur een belangrijk hulpmiddel om beveiligingsmanagement effectief en efficiënt in te richten. In dit artikel worden de contouren geschetst van een pragmatische aanpak om de voordelen van een beveiligingsarchitectuur te realiseren.

Inleiding

Denkt u zich eens in dat u een auto heeft met dertien verschillende sleutels. Eén voor het licht, één voor de claxon, één voor de rem, ... Onvoorstelbaar? Toch is dat precies hoe we vandaag de dag onze beveiliging hebben 'opgelost': per applicatie eigen beveiligingsoplossingen. De 'business' heeft daar last van. Beveiliging wordt dan een last in de ontwikkeling van nieuwe diensten. Ook voor het beheer is dit een last vanwege de enorme en nog steeds toenemende complexiteit.

Daar komt bij dat de eisen aan flexibiliteit van de IT-systemen, en dus aan de beveiliging, toenemen. Immers, veel organisaties zijn aan het kantelen van product- of service- naar een klantgerichte benadering, zijn bezig met shared service centers, of zijn simpelweg aan het onderzoeken waar het goedkoper kan met gelijkblijvende kwaliteit. Dat vraagt om een aanpassing van de informatiearchitectuur en de daaruit volgende architectuur voor de technische infrastructuur.

Nu laten de kosten voor informatiebeveiliging zich moeilijk kwantificeren. Toch is evident dat er keuzen zijn in de inrichting van de beveiliging die sterke invloed hebben op die kosten of op de kwaliteit van de beveiliging. In het verleden ontwikkelde zich de informatiebeveiliging binnen een organisatie echter zelden aan de hand van bewuste keuzen, maar doorgaans op ad-hocbasis, en veelal reactief naar aanleiding van een (te) laat onderkende behoefte aan beveiliging. De meeste organisaties zitten nu met een lappendeken aan beveiligingsproducten die maar matig samenhangen met de rest van de (IT-) omgeving, en die veelal een grote beheerinspanning vragen. Zo is het niet ongebruikelijk dat autorisaties op tientallen plaatsen worden bijgehouden, en dat voor de identificatie van gebruikers diverse registraties en middelen worden gebruikt.

In de beveiligingsarchitectuur worden de keuzen voor de inrichting van de informatiebeveiliging expliciet gemaakt. De voordelen van het werken onder een beveiligingsarchitectuur zijn evident. Zo'n architectuur leidt tot een consistente, samenhangende en toekomstvaste verzameling beveiligingsfuncties en bijbehorende technische beveiligingsmaatregelen die een optimale bijdrage leveren aan de doelstellingen van een organisatie. Doelen van een architectuur zijn richting te geven aan toekomstige organisatie-inrichting, investeringen en migratiemogelijkheden. Ook beoogt een architectuur de complexiteit hanteerbaar te maken door het aanbieden van structuur in beveiligingsfunctionaliteit. Een architectuur geeft daarmee richting voor de toekomst: de koers als een punt op de horizon. In de praktijk worden de voordelen van 'werken onder architectuur' niet altijd ten volle gerealiseerd. Bijvoorbeeld wanneer de architectuur een doel op zich wordt, waarbij de impact op de organisatie en de complexiteit worden onderschat. Het omgekeerde wordt dan bereikt: een inflexibele en kostenverhogende beveiligingsarchitectuur die de beveiliging zwakker maakt.

In dit artikel worden de contouren van een pragmatische aanpak geschetst om de voordelen van een beveiligingsarchitectuur te realiseren.

Beveiligingsarchitectuur – principes

Voor het opzetten van een beveiligingsarchitectuur bestaat een aantal ontwerpcriteria of beveiligingsprincipes. Een aantal hiervan is al in het begin van de jaren zeventig van de vorige eeuw beschreven ([Salt75]). Ook in de Trusted Computer System Security Evaluation Criteria (TCSEC, beter bekend als het Orange Book) en zo'n dertig jaar later in de Common Criteria for IT Security Evaluation worden deze principes gehanteerd. Dat zijn:

1. Isolatie
Dit houdt in dat hardware en software die relevant zijn voor de beveiliging – de 'Trusted Computing Base' of TCB – altijd zo klein en compact mogelijk gehouden moeten worden. Hoe groter de TCB, hoe moeilijker het zal zijn om te verifiëren of de beveiliging van de TCB voldoende gewaarborgd is. Dit principe wordt onder meer toegepast in reference monitors, security kernels en firewalls.

2. Veilige defaults
Toegang mag alleen door het systeem worden verleend na expliciete permissie; alles wat niet expliciet is toegestaan, is verboden.

3. Volledigheid
Elke vorm van toegang mag pas plaatsvinden na autorisatie door het systeem. Gebruikers en processen dienen zich daartoe altijd eerst te legitimeren.

4. Open ontwerp
Een goede beveiligingsarchitectuur is niet gebaseerd op het geheimhouden van de gebruikte interne mechanismen ('security by obscurity'), maar gaat juist uit van een open ontwerp. Bij een gesloten ontwerp bestaat het risico dat de werking van interne mechanismen op den duur toch aan het licht komt, bijvoorbeeld door het toepassen van 'reverse engineering' en het uitlekken van ontwerpdocumenten. Het voordeel van een open ontwerp is dat het intensiever kan worden getest en eenvoudiger kan worden verbeterd. De Europese overheden hebben momenteel een uitgesproken belangstelling voor open systemen.

5. Functiescheiding
Kritische functies in het systeem moeten zodanig worden gesplitst dat de onderscheiden deelfuncties aan verschillende functionarissen worden toegewezen. Gevoelige handelingen mogen alleen door meerdere functionarissen tegelijk worden uitgevoerd (het vierogenprincipe).

6. Beperking
Het systeem moet zo opgezet zijn dat gebruikers en processen niet meer functies mogen uitvoeren dan strikt noodzakelijk is. Dit principe staat ook bekend onder de namen 'least privilege' en 'need to know'.

7. Compartimenten
Het systeem moet bestaan uit verschillende compartimenten, segmenten of modules, zodat een mogelijk veiligheidsprobleem tot het specifieke compartiment, etc. beperkt blijft. De koppelingen tussen de compartimenten moeten omwille van de controleerbaarheid zo slank mogelijk worden gehouden. Hierdoor neemt de robuustheid en daarmee ook de veiligheid van het systeem toe.

8. Ergonomie
Het systeem moet zo ontworpen zijn dat de kans op menselijke fouten zo klein mogelijk is. Een voorbeeld hiervan is het aanbieden van een intuïtieve, consistente en mensvriendelijke gebruikersinterface.

Daarnaast is het volgende criterium van belang:

9. Redundantie
De beveiligingsarchitectuur moet bestaan uit een combinatie van maatregelen, zodat de beveiliging niet afhankelijk is van één enkele maatregel.

Omdat we bij informatiebeveiliging niet alleen te maken hebben met onopzettelijke bedreigingen, maar ook met tegenstanders die beveiligingsmaatregelen willens en wetens proberen te omzeilen, kan dit criterium nog verder worden aangescherpt door eisen te stellen aan de diversiteit van de getroffen beveiligingsmaatregelen:

10. Diversiteit
De beveiligingsarchitectuur moet bestaan uit meerdere maatregelen die wezenlijk van elkaar verschillen, zodat het doorbreken van één beveiligingsmaatregel niet automatisch leidt tot de val van het gehele systeem.

11. Transparantie en beheersbaarheid
De getroffen beveiliging en de werking van de maatregelen dienen zodanig inzichtelijk te zijn dat de status van de beveiliging goed is te volgen, en dat bijsturing efficiënt en effectief kan worden uitgevoerd.

Deze beveiligingsprincipes zijn overigens allerminst specifiek voor informatie of ICT en worden al sinds mensenheugenis toegepast.

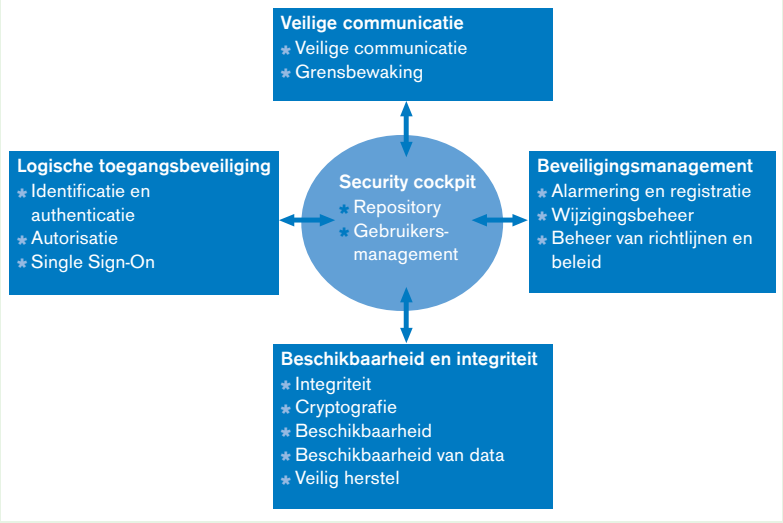
Beveiligingsarchitectuur – services

Bovengenoemde principes worden geïmplementeerd in beveiligingsservices, ook genoemd functies. Deze beveiligingsarchitectuur beschrijft de services die worden aangeboden aan de applicaties en IT-infrastructuur in het algemeen.

Hierna worden de bouwstenen van de architectuur beschreven (zie figuur 1).

Repository
Om de beveiliging van de objecten die binnen de architectuur vallen te kunnen onderhouden, worden alle gegevens met betrekking tot de beveiliging door middel van een centrale service opgeslagen en onderhouden. Deze dataverzameling wordt de repository genoemd. Typische elementen van de repository zijn: domaingegevens, gebruikersgegevens en -rollen, die op de systemen uitgevoerd mogen worden, maar ook gegevens van richtlijnen en policies, die onder andere betrekking hebben op de beveiliging en gegevens van de fysieke elementen die binnen de architectuur vallen. De bedoeling is dat via de repository enkelvoudige administratie van gegevens mogelijk wordt.

Figuur 1. Beveiligingsservices.



Gebruikersmanagement
Het beheer van gebruikersgegevens is één gemeenschappelijke service. Deze service maakt gebruik van en wijzigt gegevens over gebruikers in de repository.

Identificatie en authenticatie
Identificatie en authenticatie van gebruikers, applicaties, servers en andere intelligente componenten in de ICT-omgeving vormen een integraal deel van het beveiligingsraamwerk. Voor de service is er daarbij geen noodzakelijk onderscheid tussen authenticatie van, bijvoorbeeld, eigen medewerkers of van klanten of van beheerders. Het gaat om de I&A-service die met een bepaalde kwaliteit, of zekerheid, moet worden geboden. Die gewenste kwaliteit kan gebaseerd zijn op een analyse van de risico's. De I&A-service maakt gebruik van informatie uit de repository.

Autorisatie
Aan gebruikers kunnen verschillende privileges worden verleend, afhankelijk van de rol/functie van de gebruiker. Een gebruiker kan zowel een persoon als een automatisch proces zijn. De privileges worden opgeslagen in de repository, hetgeen definitie en administratie vereenvoudigt. Er is een sterke relatie met de I&A-service.

Single Sign-On
Een Single Sign-On-service zorgt ervoor dat de omgeving voor de gebruiker transparanter wordt. Een gebruiker hoeft maar één keer langs de I&A-service. Hij hoeft bijvoorbeeld maar één keer in te loggen. Afhankelijk van de autorisatie krijgt deze gebruiker door de Single Sign On-service ogenschijnlijk direct toegang tot de platforms, applicaties en andere componenten waar hij rechten toe heeft. Een gebruiker kan een persoon zijn, maar ook een applicatie of een andere component. De SSO-service maakt gebruik van de repository en de I&A-service.

Veilige communicatie
Wanneer informatie of applicaties buiten hun fysiek beschermde omgeving worden gebracht, ontstaan doorgaans risico's die om aanvullende maatregelen vragen teneinde ongewenste toegang tijdens het transport te voorkomen of te kunnen ontdekken. Deze service, die een vorm van toegangsbeheersing biedt, wordt veilige communicatie genoemd omdat juist tijdens communicatie risico's bestaan.

Grensbewaking
De eigen infrastructuur wordt in compartimenten verdeeld, waarbij overdracht tussen de compartimenten alleen beheerst plaats kan vinden. De bekendste vorm van compartimentering is die in netwerken. Denk daarbij aan bridges, firewalls, intrusion detection en application gateways. Een andere vorm is compartimentering in applicaties, zodanig dat informatie alleen voor specifieke (bedrijfs)toepassingen beschikbaar is, en voor andere juist niet. Zo hoeft de financiële administratie van uw ziekenhuis geen toegang te hebben tot uw medische gegevens. Deze techniek wordt dan ook tevens gebruikt ter ondersteuning van privacy.

Alarmering en registratie
Alarmering en registratie vindt niet alleen plaats op de grenzen, maar ook binnen de infrastructuur. Deze service biedt ook alarmering bij andere bijzondere gebeurtenissen, en registratie van activiteiten vindt plaats conform de richtlijnen.

Wijzigingsbeheer
Om de integriteit van de infrastructuur te kunnen waarborgen is het gewenst dat wijzigingen alleen op een beheerste manier totstandkomen. In het beheer wordt daarom vaak gewerkt op basis van (ITIL) Change Management (wijzigingsbeheer). Zodra alle acceptatie- en testprocedures zijn doorlopen, kan een wijziging in productie worden genomen. Wijzigingsbeheer zorgt ervoor dat de integriteitskenmerken van het gewijzigde object bekend zijn, en dat het object wordt opgenomen als geautoriseerde component in de repository.

Beheer van richtlijnen en beleid
Alle regels die voor de gehele infrastructuur gelden, worden door deze service bewaard en bewaakt.

Integriteit
Deze service bewaakt de integriteit van de componenten en informatie. Dat kan bijvoorbeeld door echtheidskenmerken te berekenen en deze veilig te laten bewaren in de repository.

Grensbewaking leidt tot een beheerste overdracht tussen de compartimenten.

Cryptografie
Op tal van momenten in de informatieverwerking en plaatsen in de IT-infrastructuur is er behoefte aan de inzet van cryptografie. Bijvoorbeeld om de integriteit van informatie te bewaken, om de identiteit van de bijbehorende eigenaar vast te stellen (authenticiteit dus), om informatie tijdens transport te beveiligen (vertrouwelijkheid, privacy) en ook om de beschikbaarheid te bewaken door een sessie cryptografisch af te schermen.

Beschikbaarheid
Deze service bewaakt of de prestaties nog voldoen aan de eisen en of componenten nog (voldoende) functioneren. Deze service leent zich bij uitstek om performancecriteria en drempelwaarden op te stellen zodat bij een overschrijding of storing al acties ondernomen kunnen worden om echte problemen te voorkomen. Zodra de prestaties onder een zekere waarde komen, of zodra een storing wordt gedetecteerd, kan deze service alternatieve resources inschakelen.

Beschikbaarheid van data
De beschikbaarheid van gegevens is de kern van alle informatiesystemen. Deze service beperkt het maximale gegevensverlies in geval van calamiteiten, en biedt de mogelijkheid om terug te gaan naar een stabiele situatie door activiteiten 'terug te kunnen spoelen'. Het maken van een back-up is een traditioneel voorbeeld, maar

Beveiligingsfunctie	Voorbeeld beveiligingsmechanisme
Identificatie en authenticatie	* Password schemes * Biometric approaches * Token-based authentication (e.g. smartcards) * Kerberos
Autorisatie	* Role-based access controls * Access control lists * SESAME * Closed user groups (e.g. ISDN, Frame Relay)
Veilige communicatie	* Firewalls * Screening routers * Virtual private networks (VPN)
Integriteit	* Anti-virus mechanisms * Active content management * Code signing (e.g. Java signing or ActiveX authenticode) * Message authentication codes (MAC)
Cryptografie	* SSL
Beschikbaarheid	* Redundant disk storage (e.g. RAID) * Backup mechanisms * Resilient components * Redundant components (e.g. dual power supplies) * Uninterruptible power supplies (UPS)
Grensbewaking	* (Switches) virtual LAN's * Routing control mechanisms * Firewalls * Gateways
Alarmering en registratie	* Audit trail collection * Audit trail analysis * Clock synchronisation * Intrusion detection

Tabel 1. Voorbeelden van beveiligingsfuncties en mogelijke beveiligingsmechanismen.

tegenwoordig is het niet ongebruikelijk om data parallel weg te schrijven naar verschillende locaties.

Veilig herstel
Deze service zorgt voor het weer operationeel maken van een systeem, op een gecontroleerde en veilige wijze. Juist tijdens de opstartfase blijken systemen kwetsbaar, niet alleen voor ongeautoriseerde toegang, maar ook wordt de beschikbaarheid van het systeem sterk beïnvloed door de wijze van opstarten.

Technische beveiligingsarchitectuur

De beveiligingsarchitectuur voorziet ook in de beschrijving van de samenhang tussen de verschillende beveiligingsservices en mechanismen, de gebruikte standaarden en interfaces, en de wijze waarop deze geïmplementeerd dienen te worden.

Beveiligingsservices worden via een selectie van beveiligingsmechanismen geïmplementeerd. Beveiligingsmechanismen zijn in feite technische beveiligingsmaatregelen. In tabel 1 worden voorbeelden gegevens van beveiligingsfuncties met daarbij voorbeelden van mogelijke beveiligingsmechanismen.

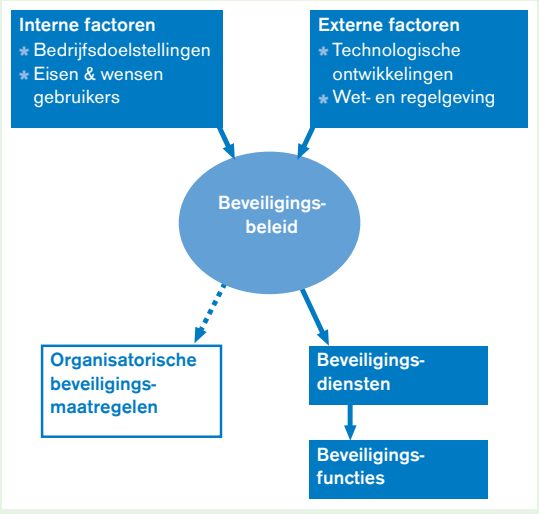
Een beveiligingsarchitectuur is geen doel op zichzelf, maar een middel om gestructureerd en op efficiënte en flexibele wijze de minimaal noodzakelijke beveiligingsfuncties (services) en maatregelen (mechanismen) te bepalen. Ten aanzien van een beveiligingsarchitectuur geldt dat de beveiligingseisen, zoals impliciet of expliciet vastgelegd in het beveiligingsbeleid, leidend zijn. Direct of indirect zijn diverse interne en externe factoren van invloed op een beveiligingsarchitectuur. Schematisch wordt het voorgaande in figuur 2 weergegeven.

Bij het opzetten van een beveiligingsarchitectuur kunnen de volgende modellen behulpzaam zijn:
* Zachman toegepast voor beveiligingsarchitecturen (www.zifa.com/);
* Open Group XDSF (www.opengroup.org/).

Pragmatische aanpak voor een beveiligingsarchitectuur

Op basis van praktijkervaringen hebben wij een aanpak ontwikkeld waarmee op eenvoudige en pragmatische wijze een start kan worden gemaakt met het werken onder beveiligingsarchitectuur. De aanpak bestaat uit de volgende stappen:

1. Classificeren en groeperen van informatiesystemen
Met behulp van een impactanalyse worden informatiesystemen (en diensten) geclassificeerd en gegroepeerd. Dit kan bijvoorbeeld worden gedaan met behulp van de impactanalyse uit SPRINT. SPRINT is een methode voor risicoanalyse die is ontwikkeld door het Information Security Forum. Tijdens de impactanalyse wordt per systeem/dienst een inschatting gemaakt – de impact – van het niet beschikbaar (B), integer (I) of vertrouwelijk (V) zijn van informatie. Ofwel, er wordt een zogenaamde BIV-classificatie toegekend. Op basis van de BIV-classificatie (in het Engels CIA) en de aard van de systemen (bijvoorbeeld internet, intranet of extranet) kunnen de informatiesystemen vervolgens gegroepeerd worden naar verschillende beveiligingsniveaus en/of verschillende domeinen.



Figuur 2. Relatie tussen beveiligingsbeleid en beveiligingsarchitectuur.

2. Bepalen gewenste situatie
Bij het bepalen van de gewenste situatie dient rekening te worden gehouden met de bedrijfsdoelstellingen. Indirect betekent dit dat relevante bedreigingen en kwetsbaarheden medebepalend zijn voor de te kiezen beveiligingsservices en mechanismen. Het spreekt voor zich dat het beveiligingsbeleid de kaders voor de beveiligingsservices en mechanismen stelt. Hiernaast is het van belang om rekening te houden met de eisen/wensen van gebruikers, technologische ontwikkelingen en wet- en regelgeving (bijvoorbeeld Wet bescherming persoonsgegevens).

In deze stap worden eerst (a.) de generieke beveiligingsservices per domein (over alle applicaties heen) bepaald en vervolgens (b.) de specifieke beveiligingsmechanismen.

Bij het bepalen van de gewenste situatie is het van belang de samenhang en integratie van de verschillende beveiligingsservices en mechanismen te bewaken.

3. Vaststellen huidige situatie
Tijdens deze stap wordt per systeem/dienst de huidige situatie (o.a. reeds geïmplementeerde beveiligingsservices en mechanismen) in kaart gebracht.

4. Evaluatie en transitie
Uitgaande van de huidige situatie zal moeten worden aangegeven op welke wijze en op welk moment de gewenste situatie bereikt moet worden. Op basis van de beschikbare financiële middelen, de vanuit de organisatie te betrekken expertise en de gewenste doorlooptijd wordt in een plan van aanpak een transitieschema opgesteld.

Het verdient aanbeveling het werken onder beveiligingsarchitectuur procesmatig in te richten (zie figuur 3).

Ten slotte is het van belang dat aan de volgende randvoorwaarden wordt voldaan:
* De organisatie heeft een (impliciet of expliciet) beveiligingsbeleid.
* Bij het management is voldoende draagvlak voor de beveiligingsarchitectuur (nut, noodzaak, kosten).
* Er is voldoende gebruikersbetrokkenheid.

Profile	Nature of assets	Assets	Confidentiality	Integrity	Availability
SEC 0	Public Internet	Internet websites	Low	Low	Low
SEC 1	Company Confidential	Various applications	Medium	Medium	Medium
SEC 2	Restricted	Various applications	Medium	High	High
SEC 3	Adressee only	Various applications	High	High	High
SEC 4	Client systems	Client systems	High	Medium	Medium
SEC 5	File and print service	File and print services	Medium	Medium	High
SEC 6	E-mail	Groupwise	Medium	High	High

Tabel 2. Classificatie en groepering van informatiesystemen.

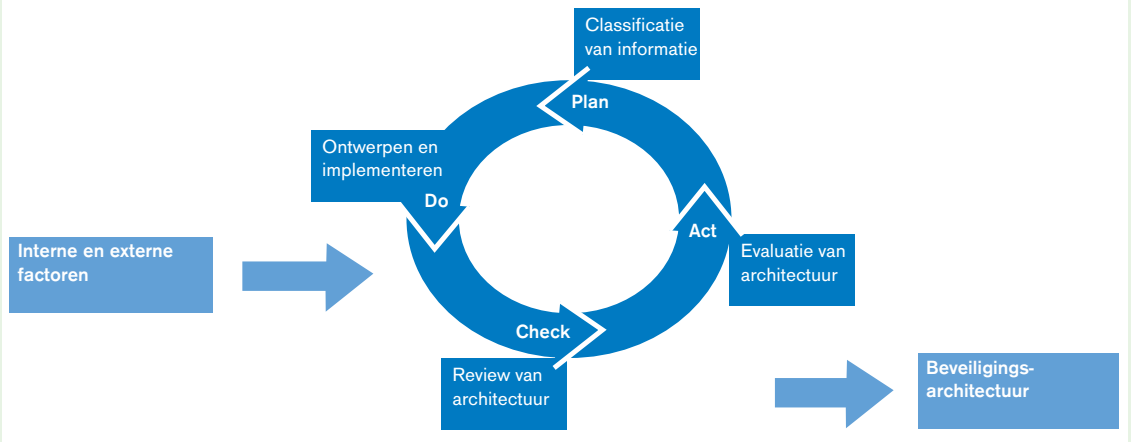
Voordelen van een beveiligingsarchitectuur

De voordelen van het werken onder beveiligingsarchitectuur zijn in het algemeen:
* Het vermindert de ontwikkel- en implementatietijd van beveiligingsmaatregelen.
* Het vergroot de effectiviteit en consistentie van beveiligingsmaatregelen.
* Het vergroot de flexibiliteit van de organisatie bij veranderende omstandigheden.
* Het definieert gestandaardiseerde interfaces.

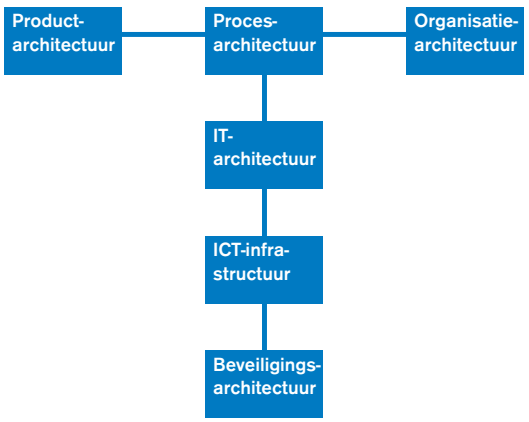
Samenvattend kunnen we zeggen dat het werken onder beveiligingsarchitectuur leidt tot positieve kosteneffecten en een positieve bijdrage aan het realiseren van de doelstellingen van een organisatie.

Aandachtspunten

Het werken onder beveiligingsarchitectuur betekent niet automatisch dat de in de vorige paragraaf genoemde voordelen zonder meer behaald worden. Het is van belang dat organisaties zich bewust zijn van de volgende aandachtspunten:
* Een beveiligingsarchitectuur is geen doel op zich.
* Een slechte architectuur vermindert de flexibiliteit, verhoogt de kosten en maakt de beveiliging zwakker.
* Bewaak de relatie met andere architecturen (zie figuur 4). Elke architectuur maakt gebruik van eigen concepten, methoden en technieken. Als de architecturen onvoldoende zijn geïntegreerd, worden de gevolgen van veranderingen binnen de ene architectuur niet zichtbaar in de andere.
* Zorg ervoor dat het beveiligingsniveau tijdens de transitieperiode gehandhaafd blijft.



Figuur 3. Architectuurproces.



Figuur 4. Relatie beveiligingsarchitectuur met andere architecturen.

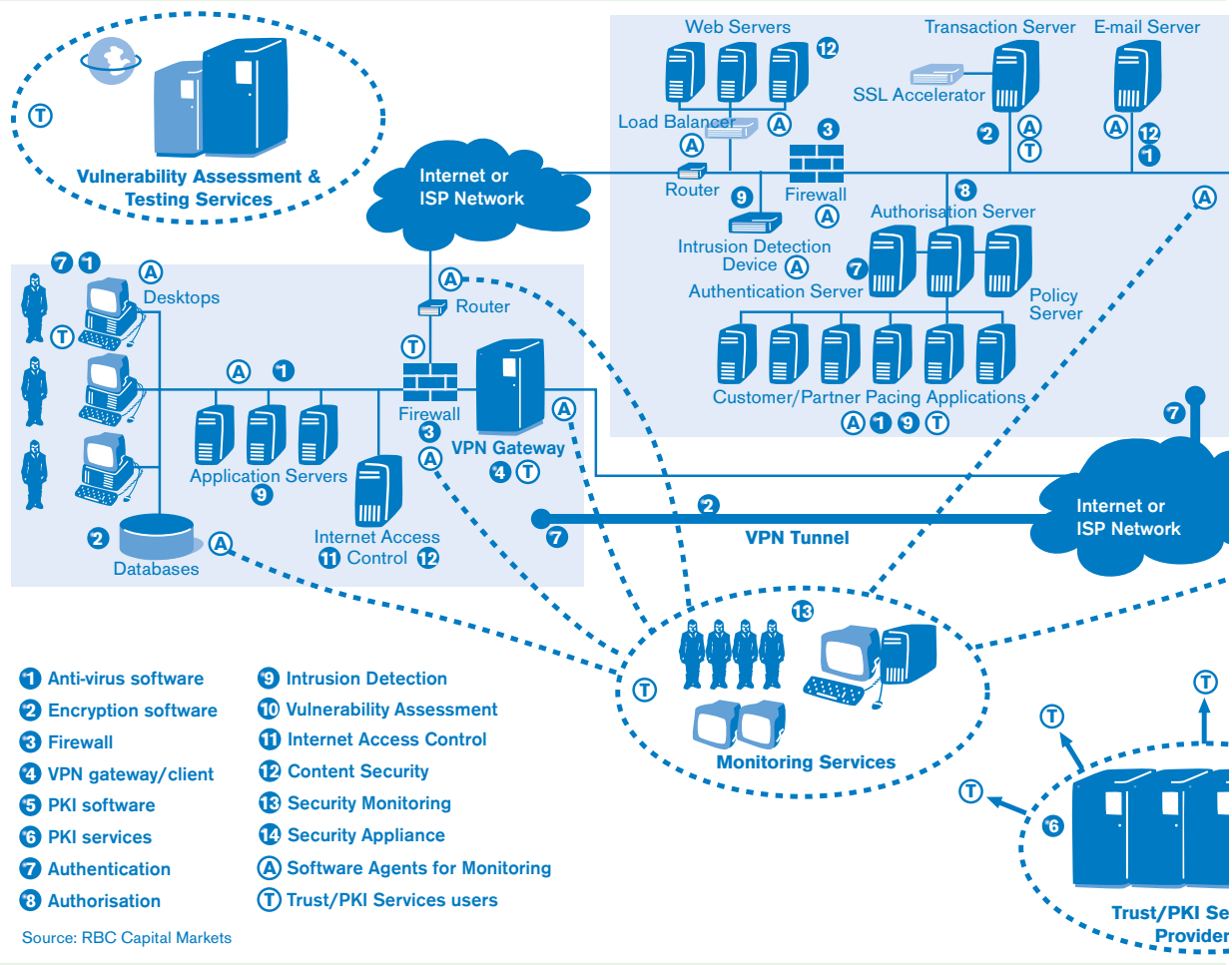
Conclusie

Een servicegerichte beveiligingsarchitectuur, die aansluit bij de behoeften van 'de business', geeft houvast. Essentieel is dat beveiliging als verzameling services in de algemene IT-infrastructuur wordt aangeboden. Na implementatie van deze services hoeft u of uw klant bijvoorbeeld nog maar eenmaal in te loggen, worden autorisaties enkelvoudig geadministreerd, en kunnen alle applicaties gebruikmaken van dezelfde set beveiligingsfuncties. Voor uw business betekent dit: 'klantvriendelijke beveiliging, die snel te realiseren is, tegen lagere kosten'.

De services in de security-architectuur bestaan uit de functies zelf, een besturingsgedeelte en een beheergedeelte. De fysieke realisatie kan gedistribueerd zijn, maar de service manifesteert zich en is beheersbaar als één geheel.

Een architectuur wordt doorgaans stapsgewijs ingevoerd. In de eerste fase worden bijvoorbeeld een single point of administration (enkelvoudig beheer van gebruikers), Single Sign-On en een autorisatieservice geïntroduceerd. De directe winst voor de business is: lagere kosten door vereenvoudiging van het beheer, en gebruiksgemak voor klanten en personeel door vereenvoudiging van het autorisatieproces en het 'inloggen'.

Werken onder beveiligingsarchitectuur kan, mits met verstand toegepast, een bijdrage leveren aan het snel en flexibel reageren op zich wijzigende klantbehoeften en bedrijfsdoelen. Door het werken onder beveiligingsarchitectuur procesmatig in te richten kunnen bovendien



positieve kosteneffecten worden gerealiseerd. In een tijd van snelle technologische ontwikkelingen, een markt die voortdurend in beweging is en veranderende wet- en regelgeving is een beveiligingsarchitectuur een belangrijk hulpmiddel om beveiligingsmanagement effectief en efficiënt in te richten.

Literatuur/Referenties

Dit artikel is geïnspireerd door onze klanten en de volgende bronnen:

http://archimate.telin.nl/

[IBM95]
IBM redbook, *Enterprise-wide security architecture and solution presentation guide*, november 1995.

[ISF00]
Information Security Forum, *Security Architecture* (workshop report), maart 2000.

[ISO]
ISO 7498-2 *Open Systems Interconnection – Security Architecture.*

[ISO]
ISO 15408 *Common Criteria for Information Technology Security Evaluation.*

[Nola00]
Nolan, Norton & Co, *Architectuur als managementinstrument*, Ten Hagen & Stam, 2000.

[Over99]
P.L. Overbeek en W.H.M. Sipman, *Informatiebeveiliging*, Tutein Nolthenius, 1999.

[Over00]
P.L. Overbeek, E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder controle*, Pearson Education, Financial Times/Prentice Hall imprint, 2000.

[Perd01]
M. Perdeck, *Kritieke succesfactoren voor het werken onder architectuur*, A&I, nr. 3, 2001.

[Salt75]
J.H. Saltzer and M.D. Schroeder, *The Protection of Information in Computer Systems*, Proceedings of the IEEE, Vol. 63, No. 9, 1975.

[TCSE85]
TCSEC, *Trusted Computer Systems Evaluation Criteria* (TCSEC), US DoD, 5200.28-STD, 1985.

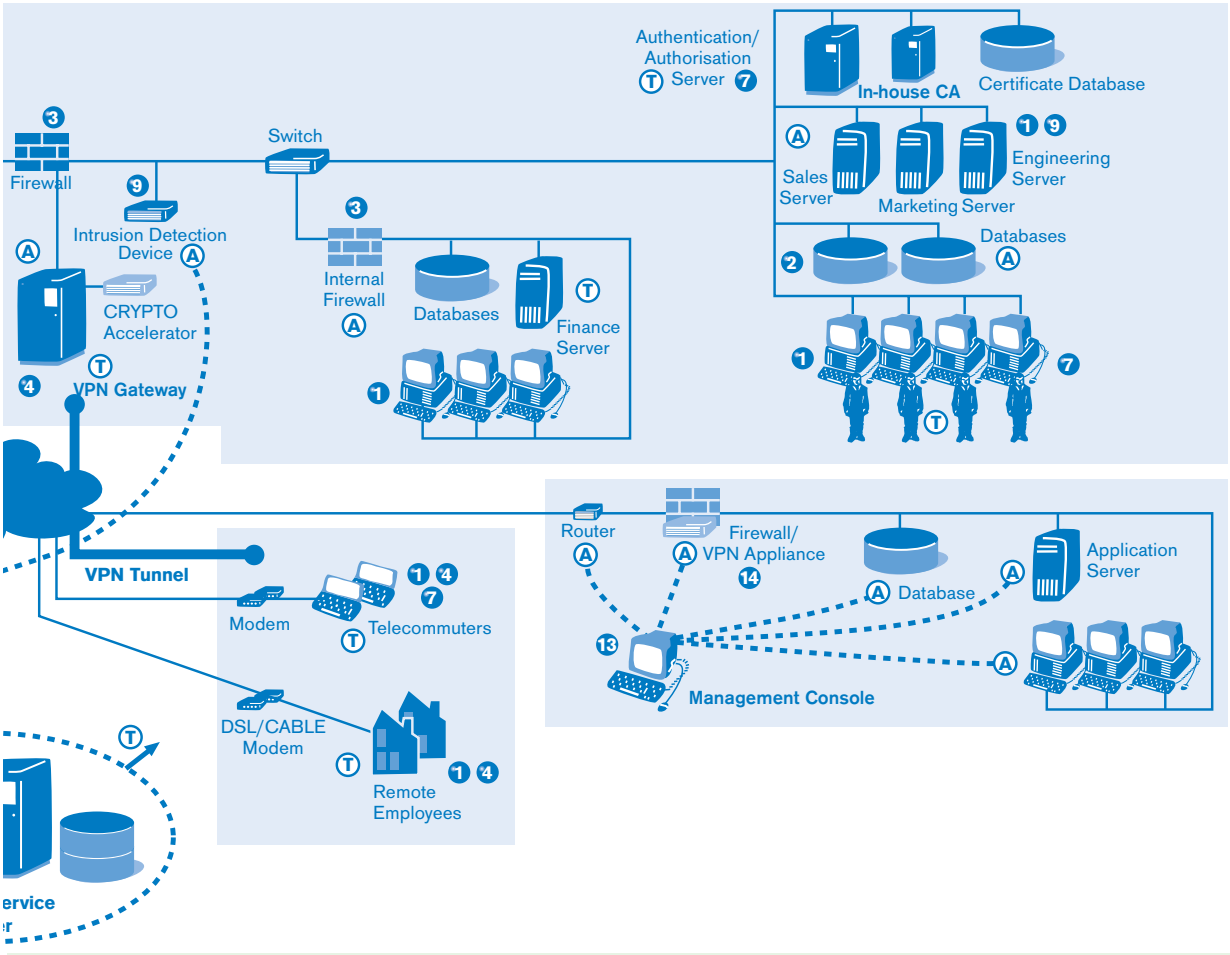
[Viss02/3]
N. Visser en R. Kuiper, drieluik *Beveiliging en architectuur*, Informatiebeveiliging nr. 7 en 8, 2002 en nr. 1, 2003.

Dr. ir. P.L. Overbeek RE is director bij KPMG Information Risk Management en medeverantwoordelijk voor de dienstverlening van KPMG met betrekking tot Information Security Management. Hij is nauw betrokken bij de Code voor Informatiebeveiliging en één van de auteurs van de ITIL-module Security Management.

overbeek.paul@kpmg.nl

Drs. E.P. Rutkens is werkzaam als consultant bij KPMG Information Risk Management. Hij houdt zich bezig met de dienstverlening van KPMG met betrekking tot Information Security. Verder is hij betrokken bij de ontwikkeling van producten op dit gebied, waaronder beveiligingsarchitecturen en risicoanalyse.

rutkens.erik@kpmg.nl



Figuur 5. Typische infrastructuur.