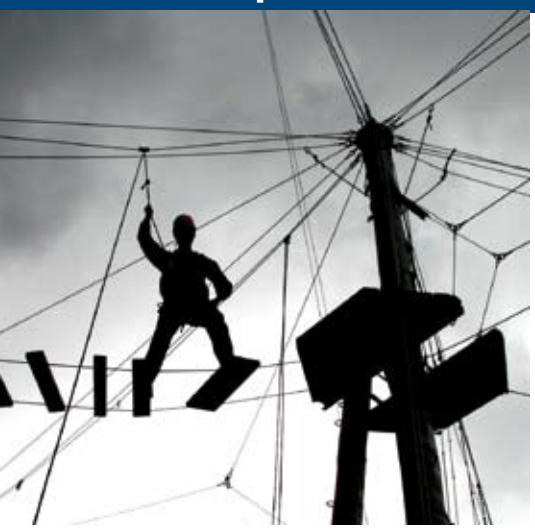


Informatie-beveiliging versus SaaS

Drs. W.S. Chung
is manager bij KPMG Advisory in Amstelveen en is specialist op het gebied van nieuwe architectuurmodellen waaronder SaaS en SOA (Service Oriented Architecture). Daarnaast heeft hij samen met collega ir. R. Heil en KPMG Sustainability de Green/Sustainable IT services binnen KPMG Nederland opgezet. Hij is een veelgevraagde spreker op congressen en seminars.

chung.mike@kpmg.nl

Drs. Mike Chung

Bedrijfssoftware over het internet wordt steeds populairder. Vrijwel alle grote softwareleveranciers en IT-integrators bieden steeds uitgebreidere en professionelere onlinediensten aan onder de noemer SaaS. Maar ook hier gaan kansen vergezeld met gevaren. Met name op het gebied van informatiebeveiliging biedt SaaS de nodige uitdagingen die nochtans zijn onderbelicht. Hoog tijd voor de kritische IT-auditor om weerwoord te geven aan dit fenomeen.

Inleiding

Software-as-a-Service (SaaS) heeft zich de laatste jaren gestaag ontwikkeld van een eenvoudig 'software-over-het-internet'-concept tot een volwaardig sourcingmodel voor uitgebreide, bedrijfsbrede softwarediensten. Hoewel het oorspronkelijke ASP-model (Application Service Provider) uit de jaren negentig mede door zijn beperkte reikwijdte van diensten en gebrekkige integratie nooit kon bogen op enig commercieel succes, is SaaS anno 2008 één van de snelst groeiende ICT-modellen. Alleen al in Nederland nemen meer dan duizend organisaties softwarediensten af via het internet volgens het principe van SaaS, waarbij de groei voor zowel het MKB als voor beursgenoteerde ondernemingen meer dan twintig procent per jaar bedraagt (bron: ASP-forum Nederland). Onderzoeksbureau Gartner voorspelt dat ruim tien miljoen bedrijven binnen tien jaar zullen overstappen op SaaS ([Desio7]); ook IDC en Burton verwachten dat lokaal geïnstalleerde 'on-premise' software binnen afzienbare tijd wordt verdrongen door 'on-demand' SaaS-oplossingen ([Maiwo7]).

Nu de inmiddels gevestigde SaaS-pioniers, waarvan Salesforce.com de bekendste is, hun dienstenportfolio gestaag uitbreiden, storten vrijwel alle grote softwarebedrijven zich in het 'ver-SaaSen' van hun pakketten. Microsoft, IBM en Oracle bieden, al dan niet in samenwerking met andere softwarebedrijven en IT-integrators, steeds meer SaaS-oplossingen aan voor complete bedrijfsprocessen. Andere grote spelers zoals SAP, BEA en Software AG investeren in middlewareproducten die toekomstige on-demand diensten zullen faciliteren.

Terwijl het succes van SaaS geen grenzen lijkt te kennen dringt slechts langzaam het besef door dat SaaS met al zijn voordelen ook serieuze uitdagingen kent op het vlak van informatiebeveiliging. Zoals zo vaak bij nieuwe IT-modellen blijkt informatiebeveiliging ook bij SaaS een sluitpost van de begroting. Dit artikel zal als tegenwicht voor de euforie

rond SaaS nader ingaan op de specifieke risico's van SaaS betreffende de informatiebeveiliging vanuit het perspectief van de afnemer (klant). Alvorens de risico's in kaart zijn gebracht, zullen de baten van SaaS worden beschreven zodat we aan het eind van het verhaal een balans kunnen opmaken.

Wat is SaaS? 'On-premise' versus 'On-demand'

Het principe van on-demand software waaronder SaaS luidt dat het *bezit* en *eigenaarschap* van software wordt gescheiden van het *gebruik*. De software blijft bij on-demand oplossingen eigendom van de leverancier; de afnemer betaalt dus alleen voor het gebruik van de software en heeft geen lokale installatie van de software, dit in tegenstelling tot het traditionele 'on-premise' model. SaaS voorziet bovendien dat de bedrijfsdata die door de software wordt gebruikt eveneens wordt opgeslagen bij de leverancier. De afnemer heeft dus met SaaS geen lokale servers meer nodig; een pc met toegang tot het internet is voldoende (zie figuur 1).

Zo bezien verschilt SaaS niet fundamenteel van het aloude ASP-concept. Het uitgangspunt van beide modellen is immers het aanbieden en gebruiken van software over het internet. Echter, waar de ASP doorgaans beperkte dienstverlening leverde van één applicatie voor één enkel proces, omvatten SaaS-oplossingen meerdere applicaties of zelfs volledige, geïntegreerde software suites voor meerdere bedrijfsprocessen. In principe kan SaaS de volledige kantoorautomatisering omvatten waarbij alle standaardfunctionaliteiten zoals tekstverwerking, spreadsheets en e-mail als webdienst kunnen worden aangeboden. Gmail, Google Documenten en Microsoft Online Services (Exchange Online, SharePoint Online) zijn enkele bekende voorbeelden hiervan; steeds meer open source-varianten komen tevens beschikbaar zoals Ulteo Online Desktop.

Architectuur van SaaS

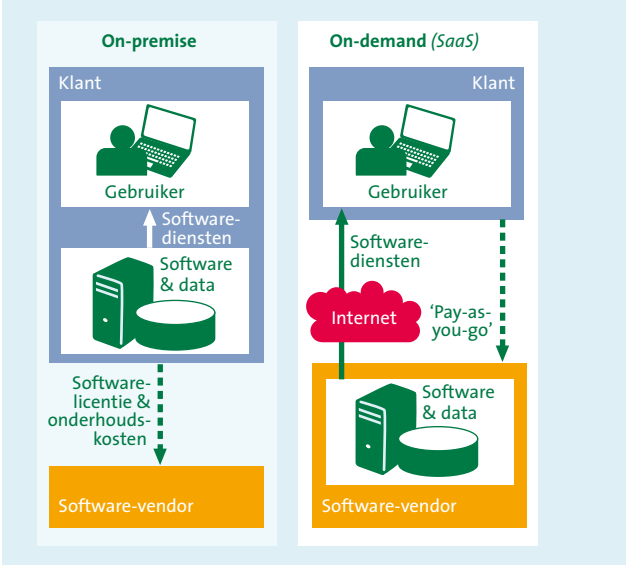
Logische architectuur

SaaS kent meerdere logische architectuurmodellen, maar de basis van SaaS vormt de 'multi-tenant'-architectuur. Bij het 'multi-tenant'-model zijn de IT-componenten opgebouwd om meerdere afnemers ('tenants') te bedienen (zie figuur 2). Dit is de eenvoudigste SaaS-architectuur.

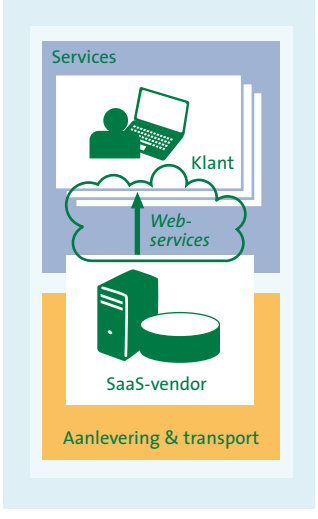
De leverancier (SaaS-vendor) heeft alle software en bedrijfsdata van de afnemers op een centrale locatie opgeslagen. Via gescheiden kanalen kunnen de afnemers de gewenste softwarefunctionaliteit en bedrijfsdata gebruiken. De SaaS-vendor zorgt hierbij voor het correct aanleveren en transporteren van de diensten, waarop de klant in staat wordt gesteld deze diensten als webdiensten af te nemen. De vroegere ASP-diensten werkten doorgaans volgens dit model.

Aangezien de kans klein is dat één leverancier in staat is alle bedrijfssoftware aan te bieden, zijn veel ondernemingen genoodzaakt om van meerdere SaaS-vendors diensten af te nemen voor een volledige applicatieportfolio. Dit vindt dan plaats volgens het 'multi-vendor'-model (zie figuur 3).

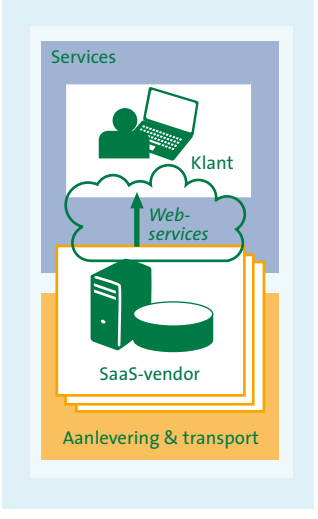
De afnemer heeft zijn bedrijfsdata verspreid over meerdere SaaS-vendors en locaties. Via al dan niet geïntegreerde kanalen neemt de afnemer verschillende softwarediensten af.



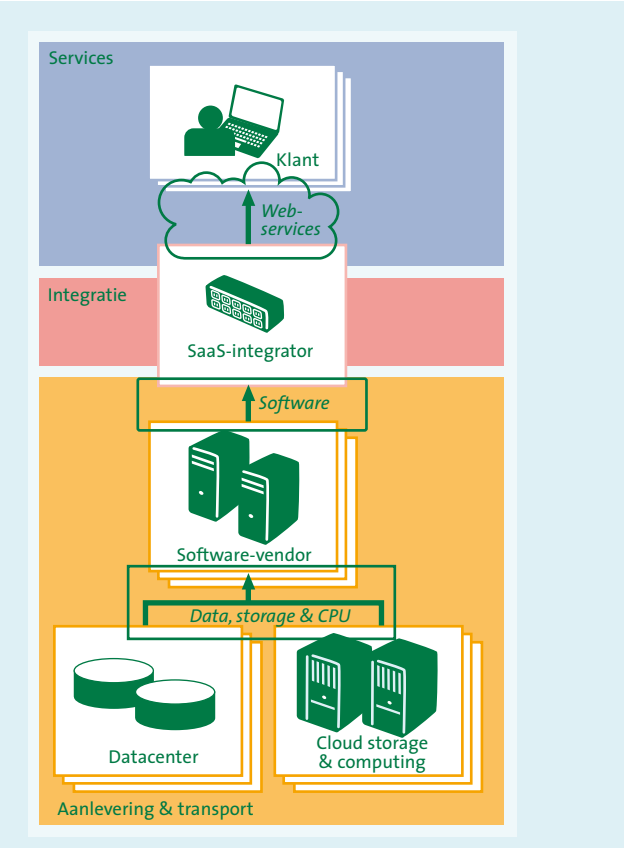
Figuur 1. **'On-premise' versus 'on-demand'.**



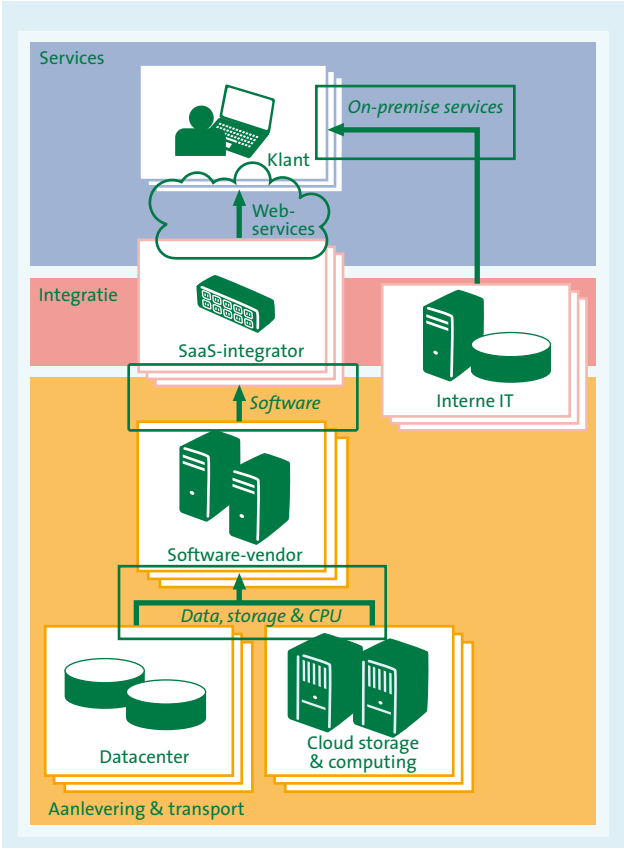
Figuur 2. **'Multi-tenant'-architectuur.**



Figuur 3. **'Multi-vendor'-architectuur.**



Figuur 4. **'Multi-instance'-architectuur.**



Figuur 5. **'Multi-integration'-architectuur.**

Steeds meer IT-integrators/resellers, grote softwarebedrijven en brancheorganisaties integreren diensten van verschillende partijen tot grotere SaaS-pakketten. Zij fungeren hierbij als SaaS-integrators – ook wel SaaS-aggregators of brokers genoemd – en vormen het contactpunt voor hun klanten. Soms hebben de partijen die de software leveren op hun beurt weer onderaannemers die specifieke diensten zoals dataopslag of CPU-power leveren. Dit wordt het 'multi-instance'-model genoemd (zie figuur 4).

Hoewel de afnemer één contactpunt heeft voor de SaaS-oplossing, namelijk de SaaS-integrator, worden de softwarefunctionaliteiten in feite door meerdere partijen geleverd. Ook de bedrijfsdata zijn verspreid over meerdere locaties waarbij de data niet noodzakelijkerwijs is opgeslagen bij de betreffende software-vendor. Steeds meer grote IT-bedrijven bieden tegenwoordig SaaS-diensten aan in de vorm van een 'multi-instance'-architectuur.

In de praktijk zullen grote, internationale ondernemingen evenwel door meerdere SaaS-integrators worden bediend. Bovendien zal een deel van de software, vanwege technische eisen of contractuele verplichtingen, alleen door lokale installaties te gebruiken zijn. Daarom zal een 'multi-integration'-architectuur voor die gevallen van toepassing zijn (zie figuur 5).

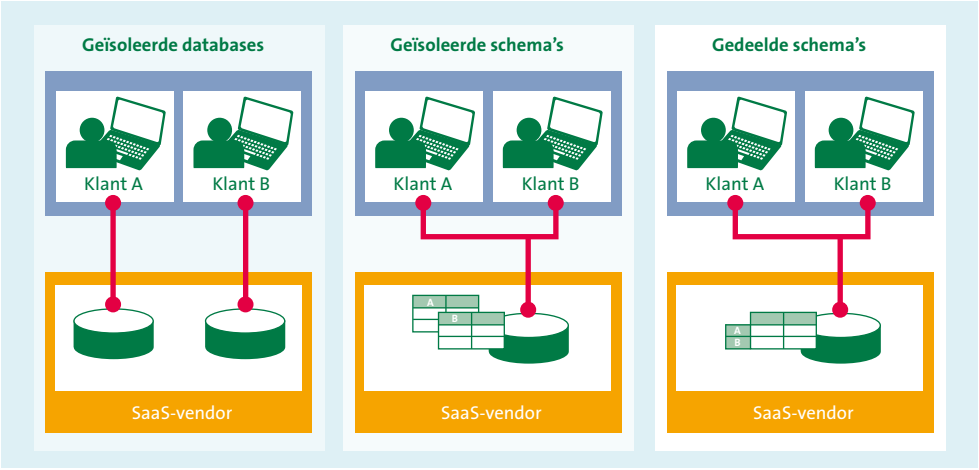
Bij dit model leveren meerdere SaaS-integrators met verschillende onderaannemers een deel van de softwarediensten aan. Een deel van de diensten blijft intern. De bedrijfsdata is derhalve verspreid over meerdere externe en interne locaties.

Data-architectuur

In principe wordt met gebruik van SaaS de data die hoort bij de software extern bij de SaaS-vendor opgeslagen en beheerd. Interne opslag is technisch mogelijk, maar veelal omslachtig in de praktijk. Het is als een lokale opslag van je e-mails met een Gmail-account.

Betreffende de architectuur van de externe opslag van data zijn voor SaaS de volgende drie modellen de meest voorkomende (zie ook figuur 6):

- *Geïsoleerde databases*, waarbij elke afnemer zijn eigen database bij de leverancier heeft. Andere klanten van de leverancier hebben geen toegang tot deze database.



Figuur 6. **Verschillende data-architecturen van SaaS.**

- *Geïsoleerde schema's*, waarbij de afnemers de database delen, maar ieder zijn eigen schema in de database heeft.
- *Gedeelde schema's*, waarbij de afnemers niet alleen de database, maar ook de schema's delen. De klant heeft zijn eigen klant-ID in de database.

Succes van SaaS

Het succes van SaaS hangt samen met het feit dat de bestaande toepassingen waarbij IT-diensten intern worden aangeboden, tegen steeds meer integratie- en beveiligingsproblemen aanlopen terwijl de kosten nauwelijks meer in de hand te houden zijn. Outsourcing en offshoring hebben de problematiek slechts ten dele opgelost en de beloofde kostenbesparing bleek in de praktijk zelden haalbaar. SaaS biedt in dit perspectief dé ideale oplossing: de hele IT inclusief alle hard- en software kan de deur uit, het beheer wordt opgeheven, alle benodigde softwarediensten worden afgenomen via het internet en de kosten zijn transparant en relatief eenvoudig te beheersen.

Naast de kostenfactor kent SaaS het theoretisch voordeel dat de onderneming zich echt kan richten op haar kerntaken zonder te worden gehinderd of geremd door de interne IT-afdeling. Bovendien is de verwachting dat de SaaS-vendor door het verkregen schaalvoordeel beter in staat zal zijn de nieuwste technologieën en beheerprocessen toe te passen teneinde de efficiëntie en effectiviteit van de dienstverlening te verhogen.

Kostenbesparing

Operationele IT-kosten kunnen met SaaS significant worden verlaagd aangezien SaaS geen grootschalige, kostbare en risicovolle implementaties van bedrijfssoftware kent aan de kant van de afnemer – alle installaties staan immers op de servers van de leverancier. Daarbij komen ook alle beheerkosten om de diensten continu beschikbaar te stellen voor de rekening van de leverancier. Bovendien kan er flink worden bespaard op hardware en de kostbare benodigdheden zoals serverruimten, koelinstallaties en elektriciteit aangezien SaaS nauwelijks (server) hardware behoeft aan de kant van de afnemer. Het enige wat de afnemer nodig heeft is een pc met (veilige) toegang tot het internet.

SaaS kent ook het voordeel dat softwareontwikkeling en -aanpassing grotendeels uit het zicht van de afnemer blijft. Idealiter levert de klant alleen de specificaties en eisen aan waarna de SaaS-vendor de vernieuwingen/veranderingen doorvoert op zijn eigen IT-omgeving. De enige verplichtingen van de afnemer zijn functionele tests en acceptatie. Hinderlijke updates op pc's behoren daarmee tot het verleden.

Lagere kosten voor softwaregebruik kunnen tot stand komen doordat er niet meer wordt gewerkt met vaste licentiekosten bij aanschaf gevolgd door jaarlijkse gebruikskosten, die meestal tien tot vijftien procent van de aanschafprijs bedragen. Bij SaaS wordt namelijk alleen het gebruik van de software in rekening gebracht aangezien de software in het bezit blijft van de SaaS-vendor. Gebruiksabonnementen zijn nog steeds de regel al raakt 'pay-as-you-go' de laatste jaren in zwang, waarbij de klant betaalt per keer dat de softwaredienst wordt aangeroepen. Het voordeel van 'pay-as-you-go' is dat er alleen wordt betaald voor software die daadwerkelijk wordt gebruikt en onnodige licentiekosten worden voorkomen. Zie tabel 1 voor een vergelijking.

Wel moet worden opgemerkt dat ofschoon de initiële kosten van SaaS aanmerkelijk lager zijn dan bij on-premise software, de kosten van SaaS door de hele software life cycle constant blijven terwijl de kosten bij lokale installaties geleidelijk zullen

afnemen. Kostenbesparing met SaaS is dus sterk afhankelijk van de duur van de software life cycle. Hoe langer een software wordt gebruikt, hoe lager het relatieve voordeel van SaaS is ten opzichte van on-premise software ([Dubeo7]).

Businessfocus

Theoretisch gezien is het gebruik van elektronische data bij SaaS transparant, eenvoudig te automatiseren en schaalbaar. Het gebruik van data kan simpel worden bijgehouden aan de hand van gecentraliseerde monitoring en logging aan de kant van de leverancier. Iteratieve, manuele taken kunnen eveneens centraal worden geautomatiseerd door middel van job scheduling. Bovendien heeft de afnemer met SaaS de mogelijkheid om het datagebruik uit te breiden of te verminderen zonder aanschaf of afschrijving van databases, hardware en ruimte.

Kortere implementaties van softwarediensten en veranderingen met minimale onderbrekingen alsook een eenduidige toegang tot de applicaties – namelijk via het internet – zorgen voor hogere productiviteit en tevredenheid bij de eindgebruikers. In plaats van verschillende applicatie-interfaces heeft SaaS namelijk maar één front-end: de webbrowser.

Geavanceerde technologie

Minimale opslag van lokale data en centraal geïnstalleerde software kunnen leiden tot een aanzienlijke verbetering van de informatiebeveiliging. De data kan door de SaaS-vendor centraal worden beveiligd met inzet van de meest geavanceerde technologieën waarbij de datastromen en sessies real-time worden gemonitord. Bovendien zijn ook uitwijkmogelijkheden en noodvoorzieningen bij de vendor geregeld. De afnemer profiteert op deze manier van de hoge(re) beveiligingsniveaus met gecentraliseerde expertise en ervaring bij de leverancier ([Dubeo7]).

	On-premise	On-demand *(SaaS)*
Ontwikkeling	• Ontwikkeling (deels) door interne IT-afdeling	• Door externe software-vendors
Aanschaf	• Eenmalig	• Geen aanschafkosten
Installatie	• Lokale installatie door interne IT-afdeling	• Door leverancier
Hardware	• Lokaal	• Van leverancier
Beheer	• Door interne IT-afdeling	• Door leverancier
Gebruik	• 10-15% van aanschafkosten per jaar	• Periodiek of 'Pay-as-you-go'

Tabel 1. **Kostenmatrix van on-premise versus SaaS.**

'State-of-the-art' technologieën kunnen ook worden toegepast aan de kant van de SaaS-vendor. Te denken valt aan energiebesparende datacenters, virtualisatie, cloud storage en ESB-technologieën (Enterprise Service Bus). Veelal zijn deze technologieën te duur voor kleinere ondernemingen, terwijl de SaaS-vendor door zijn schaalgrootte de benodigde investeringen wel kan doen.

Beveiligingsrisico's van SaaS

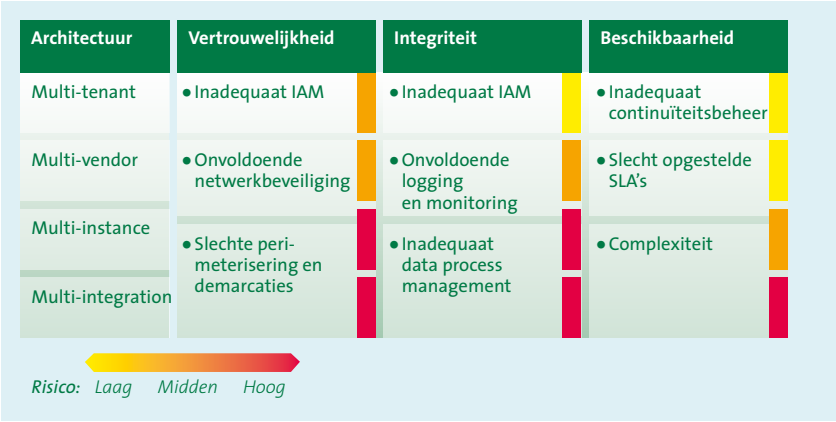
De voornaamste beveiligingsrisico's van SaaS zijn terug te voeren op drie risicogebieden van SaaS:
- de externe opslag en verwerking van data;
- de afhankelijkheid van het (publieke) internet; en
- de complexiteit van diensten en integratie.

Externe opslag van data

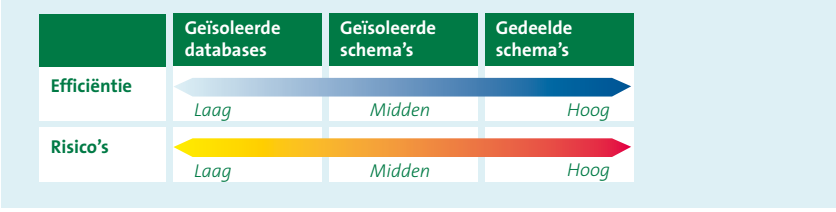
De opslag en verwerking van bedrijfsdata bij de SaaS-vendor betekent in de eerste plaats dat de potentieel zeer gevoelige en waardevolle data buiten de gecontroleerde zone of de 'interne perimeter' van de afnemer wordt geplaatst, soms zelfs buiten de landsgrenzen. De data staat dus op een plek die niet door interne beveiligingsmaatregelen kan worden beschermd. Ten tweede staat de data bij een leverancier die meerdere klanten bedient en in principe één beveiligingsstrategie hanteert voor data met verschillende eigenaren.

De grootste risico's van externe opslag zijn derhalve:
- verlies van bedrijfsdata als gevolg van incompetente operationele IT-afdelingen van de leverancier of onderaannemers zoals gebrekkige en/of falende back-ups, dataopslag, redundantie en slecht datamanagement;
- misbruik of diefstal van bedrijfsdata als gevolg van onvoldoende beveiligingsmaatregelen inclusief Identity & Access Management, zoals:
  - misbruik/diefstal van bedrijfsdata door het personeel van de leverancier of onderaannemers;
  - misbruik/diefstal van bedrijfsdata door ongeautoriseerde externe partijen zoals andere afnemers, criminelen of hackers;
  - misbruik/diefstal van bedrijfsdata door interne medewerkers als gevolg van gebrekkige functiescheidingen;
- inbreuk op vertrouwelijkheid van bedrijfsdata door fouten in de beveiliging en/of gebrekkige demarcaties (scheidingen) tussen verschillende afnemers;
- non-compliance en andere audit-findings als gevolg van slechte auditabiliteit;
- non-compliance als gevolg van gebrekkige functiescheidingen;

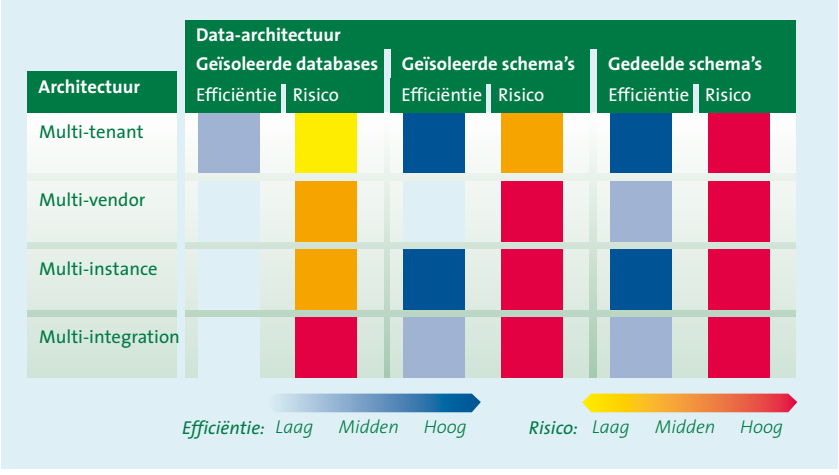
- ongecontroleerd dataverkeer als gevolg van slechte scheidingen van data tussen verschillende SaaS-afnemers en tussen de leverancier en onderaannemers;
- privacy issues als gevolg van onvoldoende assurance om vertrouwelijke en/of persoonsgegevens te beschermen;
- non-repudiation issues als gevolg van onvoldoende authenticatie- en verificatiemechanismen;
- juridische issues indien de data buiten de landsgrenzen komen.



Tabel 2. **Veelvoorkomende gebreken en risiconiveaus per architectuurmodel.**



Tabel 3. **Efficiëntie en risico's van verschillende architecturen.**



Tabel 4. **Efficiëntie en risico's van data-architecturen.**

De genoemde risico's zijn evenwel sterk afhankelijk van de SaaS-architectuur en de data-architectuur tussen de afnemer en de leverancier. Wat betreft de SaaS-architectuur zijn het aantal verschillende leveranciers en de complexiteit de belangrijkste factoren. Meer leveranciers betekent meer interfaces tussen de afnemer en de SaaS-vendors waardoor de kans op gebreken toeneemt. Daarnaast zal een eenvoudige 'multi-tenant'-architectuur doorgaans beter te controleren zijn en derhalve minder risico's met zich meebrengen dan een complexe 'multi-integration'-architectuur (zie tabel 2).

Wat betreft de data-architectuur zijn de relatief dure maar veiliger geïsoleerde databases minder riskant dan de goedkopere modellen waarbij de database of zelfs de schema's worden gedeeld. Ook hierbij gaat de regel op dat hogere efficiëntie ten koste gaat van informatiebeveiliging (zie tabel 3).

Als de besproken SaaS-architecturen en data-architecturen betreffende de efficiëntie en risico's worden gemapped krijgen we de matrix in tabel 4.

Afhankelijkheid van het internet

De continuïteit en beschikbaarheid van SaaS steunt voor een belangrijk deel op de beschikbaarheid en performance van het (publieke) internet. Deze afhankelijkheid kan ertoe leiden dat een storing of defect aan het internet de hele bedrijfsvoering stillegt. Recente storingen op het internet zoals die bij het webknooppunt AMS-IX en de beruchte kabelbreuk in de Middellandse Zee hadden tot gevolg dat bedrijven die afhankelijk waren van on-demand software in enkele gevallen dagenlang geen productie konden draaien. Er bestaan weliswaar technische mogelijkheden om (korte) onderbrekingen in de connectie te overbruggen of om sessies periodiek te laten synchroniseren, maar een langdurige storing van het internet betekent geen software en, veel ernstiger, geen toegang tot de bedrijfsdata!

Een bijkomend punt is dat niemand het internet 'bezit' waardoor het buitengewoon moeilijk is om verantwoordelijke/aansprakelijke partijen aan te wijzen in geval van storingen.

De grotere fysieke afstand tussen de gebruiker en de IT-afdeling over het internet is nadelig voor de performance. Vaste bandbreedtes zijn

meestal wel te regelen, maar ook dan is de afnemer afhankelijk van de vele knooppunten op het internet en de snelheid van het netwerk bij de leverancier.

Daarnaast is het (publieke) internet het domein van iedereen inclusief degenen met kwade bedoelingen. Niet alleen het onderscheppen of omleiden van het dataverkeer is relatief eenvoudig, de gebruikte protocollen zijn in veel gevallen slecht beveiligd. Denial of Service-aanvallen, data ransoming en malware-installaties zijn niet exclusief voorbehouden aan on-demand diensten, maar de constante dienstverlening met de bijbehorende data over het internet vergroot wel het risico op aanvallen en misbruik vanuit het internet aanzienlijk ([Zanto7]). Ook de actuele problematiek van zwakheden in de DNS-structuur is mogelijk van invloed op SaaS aangezien de SaaS-gebruikers door criminelen eenvoudig kunnen worden omgeleid naar clandestiene websites. Eventuele zwakheden in de wereldwijde architectuur van het internet kunnen derhalve verregaande gevolgen hebben voor online diensten, zeker als patches laat worden uitgebracht of niet worden geïnstalleerd.

Bedreiging	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen internetverbinding	Laag	Laag	Hoog
Geografische beperkingen	Laag	Laag	Midden
Storingen op internet	Midden	Midden	Hoog
Onderschepping dataverkeer	Hoog	Hoog	Midden
Denial of Service	Laag	Laag	Hoog
Data ransoming	Hoog	Hoog	Laag
Malware-installaties	Hoog	Hoog	Midden
Zwakheden internetarchitectuur	Hoog	Hoog	Hoog

Risico: Laag Midden Hoog

Tabel 5. **Bedreigingen van het internet.**

Dit in ogenschouw nemend, kunnen de volgende beveiligingsrisico's worden geïdentificeerd:

- discontinuïteit/onbereikbaarheid van diensten en data in geval dat er geen verbinding is tot het internet;
- slechte beschikbaarheid van softwarediensten als gevolg van storingen op het internet;
- slechte beschikbaarheid van softwarediensten over het internet als gevolg van geografische beperkingen;
- verlies van data als gevolg van storingen op het internet;
- verlies/misbruik/diefstal van data als gevolg van inadequate (netwerk)beveiliging;
- verlies/misbruik/diefstal van data als gevolg van zwakheden in de architectuur van het internet.

Complexiteit van diensten en integratie

Integratie met bestaande, interne IT-diensten evenals tussen verschillende SaaS-vendors en integrators kan grote integratieproblemen met zich meebrengen en de complexiteit vergroten.

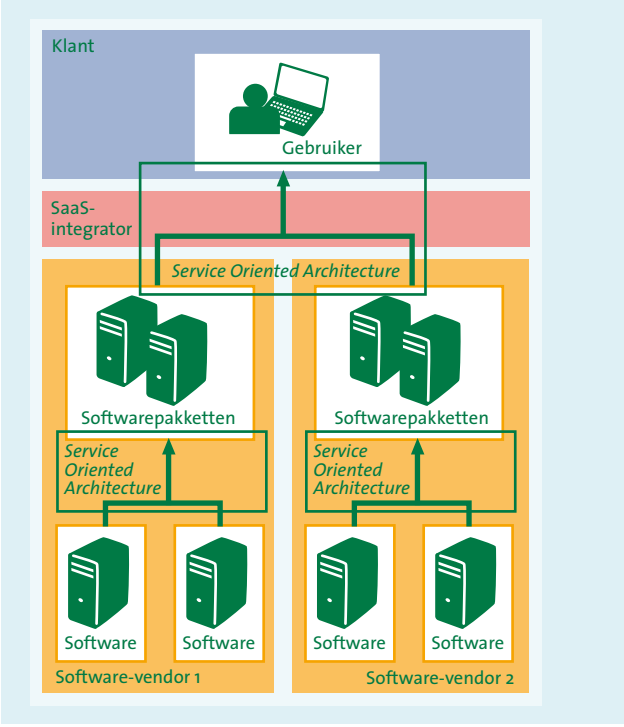
Deze complexiteit geldt ook voor de beveiligingsmechanismen en -strategieën. Niet alleen zal er sprake zijn van meerdere oplossingen waarvoor geldt dat de keten net zo sterk is als de zwakste schakel, de integratie van beveiliging leidt vaak tot compatibiliteitsissues en onduidelijke verantwoordelijkheden.

SaaS-vendors hebben meestal hun eigen methoden om het dataverkeer en data te beveiligen welke vooralsnog niet zijn gebonden aan algemeen geaccepteerde normen. Hierdoor is integratie zowel voor de integrator als voor de afnemer bij een 'multi-integration'-architectuur een complicerende factor.

Open standaarden inzake informatiebeveiliging worden steeds vaker toegepast, maar deze standaarden zijn nog lang niet uitgekristalliseerd. Integratie tussen verschillende softwarepakketten binnen SaaS en tussen verschillende leveranciers komt steeds vaker conform de principes van SOA (Service Oriented Architecture) tot stand. Hierbij worden de verschillende diensten (services) aan elkaar gekoppeld en aangeboden via een ESB (Enterprise Service Bus) (zie figuur 7). Helaas is het beveiligingsmodel voor SOA nog net zo onvolwassen als dat van SaaS en kent het model grote beveiligingsrisico's met name op het gebied van authenticatie en autorisatie ([Chuno7]).

Aangaande de complexiteit kunnen derhalve de volgende risico's worden geïdentificeerd:

- verlies of verzwakking van beveiligingsmechanismen als gevolg van beperkingen in de integratie tussen verschillende SaaS-oplossingen en/of tussen de nieuwe SaaS-oplossing en de bestaande IT-omgeving;
- slechte aansluiting van de gestandaardiseerde beveiligingsprocessen van de integrator op de bedrijfsspecifieke processen van de afnemer;
- complexiteit van de IT-omgeving als gevolg van vele en/of aangepaste interfaces, connecties, koppelingen en (meta) directories:
  - moeilijkheden bij het uitvoeren van security changes;
  - complexe root-cause analyses bij beveiligingsincidenten;



Figuur 7. **SaaS op basis van SOA.**

- beveiligingslekken als gevolg van deze complexiteit en de daarmee samenhangende demarcaties van verantwoordelijkheden inzake informatiebeveiliging.

Mitigerende maatregelen

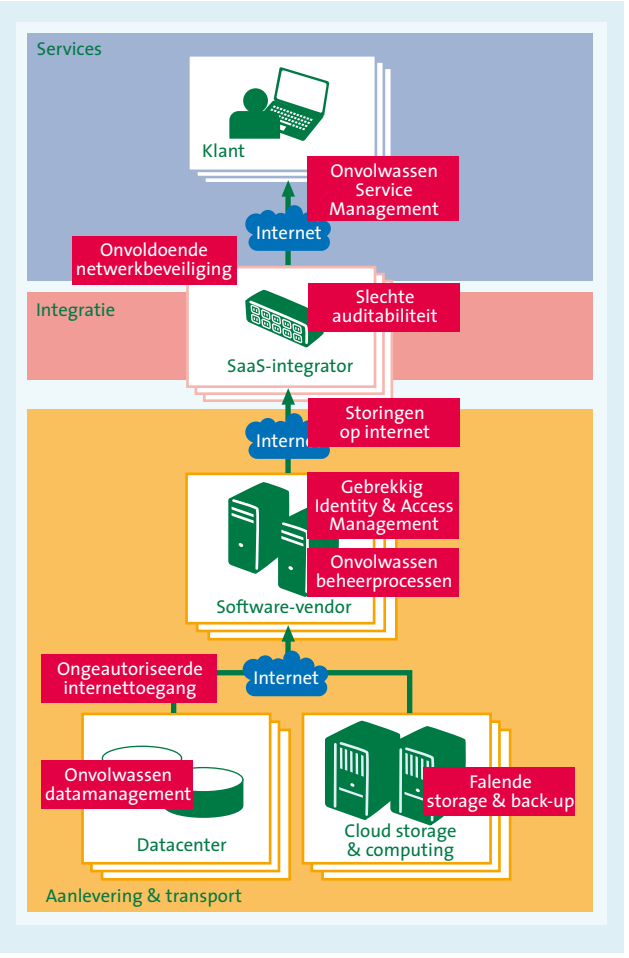
Externe opslag van data

Om de risico's inzake vertrouwelijkheid en integriteit van data te kunnen mitigeren dient te allen tijde duidelijk te zijn waar de data zich bevindt, wie de data beheert en hoe de datastromen precies lopen. Het in kaart brengen van deze informatie blijkt in de praktijk een zeer ingewikkelde onderneming voor de afnemers én de vendors. In veel gevallen weten de leveranciers zelf nauwelijks hoe het dataverkeer loopt tussen hen en hun onderaannemers ([Thoo07]). Bovendien moet een dergelijk overzicht voortdurend worden bijgewerkt waarbij de vraag rijst wie het eigenaarschap moet nemen op dit overzicht, de service manager aan de kant van de afnemer of de SaaS-vendor(s)?

In ieder geval vergen de volgende drie zaken de hoogste aandacht van de afnemer opdat de vertrouwelijkheid en integriteit van bedrijfsdata is gewaarborgd:

- Eisen en standaarden inzake bedrijfsdata (data policy) dienen voor de gehele dataketen in en buiten de organisatie te gelden. De SaaS-vendor/integrator dient zich te committeren aan deze eisen en standaarden evenals zijn onderaannemers.
- Verantwoordelijkheden en aansprakelijkheden dienen duidelijk te worden gedefinieerd en belegd. Hierbij moeten alle actoren van de dataketen betrokken worden.
- Er dienen periodieke controles plaats te vinden om het beveiligingsniveau te beoordelen voor de gehele dataketen.

De belangrijkste bedrijfsdata zou in ieder geval altijd bereikbaar moeten zijn voor de afnemer. Kopie van deze data zou dan lokaal opgeslagen moeten worden waarmee eigenlijk één van de uitgangspunten en voordelen van SaaS, namelijk dat alle data bij de externe leverancier wordt opgeslagen, teniet wordt gedaan. Bovendien zal dit het netwerkverkeer negatief beïnvloeden. Duidelijke criteria ten aanzien van de waarde van de bedrijfsdata waarbij een klein deel van de data lokaal wordt bewaard, is derhalve een goed uitgangspunt.



Figuur 8. **Potentiële kwetsbaarheden van SaaS in de praktijk.**

Beveiliging dient over de gehele dataketen aan de eisen van de afnemer te voldoen. Ook hierbij is de vraag relevant of de leverancier moet voldoen aan de (verschillende) eisen en standaarden van de afnemers of zelf de eisen en standaarden moet voorleggen die acceptabel zijn voor alle afnemers.

Voor de handhaving van functiescheidingen en gecontroleerde autorisaties is een goed ingericht Identity & Access Management (IAM) van essentieel belang. Ook hierbij is de vraag waar de verantwoordelijkheden liggen en wie het beheer van de IAM-tooling op zich moet nemen, de afnemer of de leverancier? IAM aan de kant van de afnemer heeft als voordeel dat de onderneming zelf 'in control' blijft over toegang tot haar data, maar zal vanwege de veelheid aan software agents en connectoren op zijn systemen in de praktijk onwerkbaar zijn voor de SaaS-vendor die meerdere klanten moet bedienen. IAM aan de kant van de vendor heeft als voordeel dat vanaf één centraal punt alle toegang wordt geregeld voor meerdere afnemers, maar deze oplossing zal hoogstwaarschijnlijk niet voldoen aan alle klanteisen ([Csero8]).

Afhankelijkheid van het internet

Storingen op het internet zijn helaas te onvoorspelbaar voor wat betreft de impact en duur om goede preventieve maatregelen daartegen te treffen. Het is daarom verstandiger om met de leverancier duidelijke afspraken te maken over verantwoordelijkheden en taken in geval van storingen. Het is voor de leverancier van belang dat alle mogelijke knelpunten en beperkingen in kaart worden gebracht opdat bij storingen de juiste repressieve maatregelen in werking treden.

In ieder geval dient de afnemer zich te verzekeren van voldoende beveiligde webbrowsers en verbindingen; werknemers mogen alleen gebruikmaken van de SaaS-diensten vanaf beveiligde en gecontroleerde pc's over beveiligde netwerken.

Complexiteit van diensten en integratie

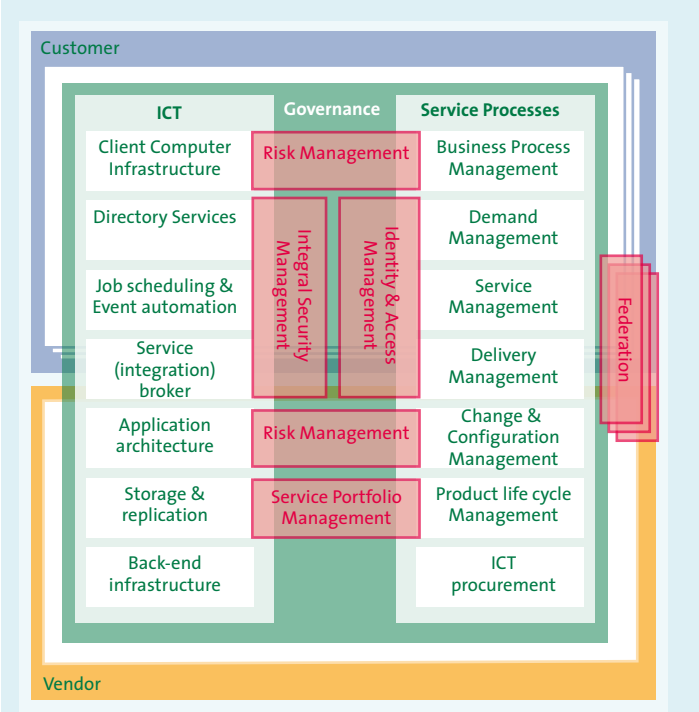
Om de complexiteit van de IT-omgeving niet te vergroten met SaaS kan de afnemer een SaaS-oplossing kiezen die voldoet aan de volgende eisen:
- eenvoudige integratie met de bestaande IT-omgeving;
- gebaseerd op open standaarden;
- transparante architectuur; en
- hoog volwassenheidsniveau van IT-beheer en governance,

en indien mogelijk aansluitend op de processen van de afnemer.

In gevallen dat er niet kan worden voldaan aan deze eisen dient de afnemer in ieder geval een goed overzicht te hebben van de complexiteit, de risico's en de perimeters. Ook dient de SaaS-omgeving periodiek te worden gecontroleerd op beveiligingsrisico's.

Goed opgestelde SLA's over informatiebeveiliging zijn eveneens een voorwaarde. Voor de security officer of de betreffende service manager van de afnemer geldt dat richting de leverancier duidelijke afspraken worden gemaakt over onder meer:
- standaarden en policies;
- beveiligingseisen;
- securityprocessen en -procedures inclusief de taken en verantwoordelijkheden;
- IAM;
- datamanagement;
- continuïteit en uitwijk;
- logging, monitoring en auditing.

De volledige aansprakelijkheid leggen bij de SaaS-integrator voor wat betreft de taken en verantwoordelijkheden van zijn onderaannemers kan het werk bij de afnemer vereenvoudigen, maar daarmee worden de risico's niet gedekt. Proces- en governancemodellen die deze leemte in IT Service Management dekken, hebben vooralsnog hun nut niet bewezen. De praktijk leert in ieder geval dat 'klassieke' best practices zoals ITIL v2 en Cobit lang niet alle beveiligingsaspecten van SaaS omvatten ([Turno3]).



Figuur 9. **KPMG's referentiemodel voor SaaS.**

Mitigatie	Type maatregel	Risicogebied
Volledig geïmplementeerd Identity & Access Management	Preventief, detectief	Externe dataopslag, complexiteit
Data policy over gehele dataketen	Preventief, correctief, repressief	Externe dataopslag
Business Continuity Management met nadruk op beschikking/toegang bedrijfsdata	Correctief, repressief	Externe dataopslag, afhankelijkheid internet
Inzicht in complexiteit, inclusief risicotaxatie en perimeterisering	Preventief	Complexiteit
Periodieke audits en security assessments	Preventief, detectief	Externe dataopslag, afhankelijkheid internet, complexiteit
Voldoende beveiligde verbinding tot diensten	Preventief, detectief	Externe dataopslag, afhankelijkheid internet
Goed opgestelde SLA's	Preventief, correctief, repressief	Externe dataopslag, afhankelijkheid internet, complexiteit
Logging & Monitoring	Preventief, detectief	Externe dataopslag, afhankelijkheid internet, complexiteit

Tabel 6. **Mitigerende maatregelen.**

Als uitgangspunt voor procesinrichting kan evenwel het SaaS-referentiemodel van KPMG worden gebruikt (zie figuur 9). Dit model geeft de verantwoordelijkheden van de afnemer, de leverancier alsook de gezamenlijke verantwoordelijkheden weer. Voorts biedt dit model een indicatie van welke processen kunnen worden uitbesteed, maar ook welke beslist binnen de eigen organisatie moeten worden gehouden ([Chuno8]).

Als we nu de belangrijkste mitigerende maatregelen afzetten tegen de belangrijkste risicogebieden krijgen we de matrix in tabel 6.

Conclusie

Waar kansen zich voordoen ontstaan ook risico's. SaaS biedt grote kansen voor organisaties die streven naar betere kostenbeheersing, sterkere businessfocus en schaalbare IT-diensten. Het aantal leveranciers en mogelijkheden is inmiddels groot genoeg om een heel softwareportfolio van de onderneming als SaaS af te nemen. De praktijk leert echter dat SaaS in zijn stormachtige ontwikkeling ook de nodige beveiligingsrisico's met zich heeft meegebracht die de verwachte baten teniet kunnen doen.

Externe dataopslag, sterke afhankelijkheid van het internet en complexiteit van diensten en integratie zijn de voornaamste risicogebieden van SaaS, waartegen met bestaande kennis en middelen voldoende te bewapenen valt. Het is dan wel van belang dat de relevante risico's voor de gehele dataketen van de dienst in kaart worden gebracht. Juist dit punt blijkt in de praktijk bij veel afnemende organisaties én SaaS-vendors onvoldoende onder controle te zijn.

Terwijl de softwarediensten en operationele activiteiten verplaatst kunnen worden naar de SaaS-vendor, zal SaaS in principe niet het risiconiveau van de afnemer verlagen. Om optimaal te kunnen profiteren van SaaS is het derhalve essentieel om de juiste mitigerende maatregelen te treffen alvorens er wordt overgegaan tot implementatie van dit veelbelovende model.

Literatuur

[Cardo05] Rui Cardoso and Mário Freire, *Security Vulnerabilities and Exposures in Internet Systems and Services*, Universidade de Beira Interior, Idea Group Inc., 2005.

[Chuno7] Mike Chung, *De beveiligingsproblematiek rond Service Oriented Architecture*, Banking & Finance, november 2007.

[Chuno8] Mike Chung, *Software-as-a-Service. Opportunities and Risks of SaaS*, KPMG ITA ISC, mei 2008.

[Cser08] Andras Cser and Jonathan Penn, *Identity Management Market Forecast: 2007 to 2014*, Forrester, februari 2008.

[Desio7] Roberto Desisto and Raymond Paquet, *Learn the Economic Advantages of a Pure SaaS Vendor*, Gartner Research, oktober 2007.

[Dubeo7] Abhijit Dubey and Dilip Wagle, *Delivering Software as a Service*, McKinsey Quarterly, mei 2007.

[Isfdo5] *Disappearance of the Network Boundary*, Information Security Forum, ISF Digest 2005.

[Maiwo7] Eric Maiwald, *SaaS for Collaboration and Content: A Smart Move or an Invitation to Disaster?*, Burton Group, 2007.

[Thooo7] Eric Thoo, *Safeguarding Information When Using SaaS*, Gartner Research, november 2007.

[Turno3] Mark Turner, David Budgen and Pearl Brereton, *Turning Software into a Service*, IEEE Computer Society, 2003.

[Zanto7] Arjen van Zanten en Ronald Heil, *Het ICT-Netwerk. Waar ligt de grens?*, Compact 2007/2.