2012•2013
FACULTEIT BEDRIJFSECONOMISCHE WETENSCHAPPEN
master in de toegepaste economische wetenschappen:
handelsingenieur in de beleidsinformatica

Masterproef

Continue monitoring als audittool bij cloud computing

Promotor :
Prof. dr. Roger MERCKEN

Kristof Huysmans

Masterproef voorgedragen tot het bekomen van de graad van master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica

universiteit hasselt
KNOWLEDGE IN ACTION

Universiteit Hasselt | Campus Hasselt | Martelarenlaan 42 | BE-3500 Hasselt
Universiteit Hasselt | Campus Diepenbeek | Agoralaan Gebouw D | BE-3590 Diepenbeek

universiteit hasselt
KNOWLEDGE IN ACTION

2012•2013
FACULTEIT BEDRIJFSECONOMISCHE WETENSCHAPPEN
master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica

Masterproef

Continue monitoring als audittool bij cloud computing

Promotor :
Prof. dr. Roger MERCKEN

Kristof Huysmans

Masterproef voorgedragen tot het bekomen van de graad van master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica

universiteit hasselt
KNOWLEDGE IN ACTION

1 Voorwoord

De voorbije jaren waren opwindende tijden op het gebied van het gebruik van informatiesystemen binnen de bedrijfscontext. Meer en meer wordt de eigen infrastructuur uitbesteed. Als afstuderend handelsingenieur in de beleidsinformatica lijkt het mij zeer boeiend en meeslepend om mij in dit domein verder te verdiepen. De combinatie van mijn kennis van bedrijfskunde samen met kennis van courante informatiesysteeminfrastructuren, die ik tijdens mijn opleiding heb opgedaan, maakt cloud computing zeer passend voor mijn onderzoek. Cloud computing is immers een relatief nieuwe benadering die opportuun kan zijn voor elk bedrijf. Kennis omtrent de werking van een bedrijf is dus noodzakelijk, vermits we ons hier specifiek richten op de bedrijfsbenadering van cloud computing. Kennis omtrent informaticastructuren is ook onmisbaar, vermits het hier gaat om het outsourcen van de reeds bestaande informaticastructuren.

Cloud computing is de term die gebruikt wordt bij een vorm van uitbesteden van informatiesystemen aan derde partijen. Cloud computing providers zijn veelal erg gespecialiseerd en hebben de nodige mankracht ter beschikking om deze service te kunnen bieden. Ze bieden deze service op flexibele manieren aan zodat er in principe enkel betaald moet worden voor wat er werkelijk wordt verbruikt.

In deze masterproef stel ik een continu auditmodel op waarmee de risico's, die inherent zijn aan cloud computing, ingedekt worden. Allereerst zal ik een schets geven van het domein cloud computing. Hierna zal ik de voordelen van cloud computing benoemen. Bij cloud computing zijn er echter ook nadelen. Vanuit de nadelen en voordelen bij cloud computing komen risico's voort. Een aangepast continu auditmodel is erop gericht om deze risico's in te dekken. Aan de hand van een kwalitatieve studie zal ik toetsen of het mogelijk is dit auditmodel te implementeren in de realiteit.

Ik bedank mijn ouders en mijn broer voor de steun tijdens het maken van deze masterthesis. Ik bedank ten slotte Prof. Dr. Roger Mercken voor de verdere informatie en richtlijnen tijdens diverse contactmomenten.

2 Samenvatting

Cloud computing wordt gedefinieerd als een pay-per-use, je betaalt enkel wat je gebruikt, service die over het Internet de bestaande informatietechnologiemogelijkheden uitbreidt. De term cloud staat voor het feit dat men niet moet weten wat er precies in de cloud gebeurt, het is voldoende dat de consument zich aan de cloud aansluit en zo kan de consument van de cloud service genieten.

Cloud computing heeft vele voordelen, maar ook bepaalde nadelen. De drie belangrijkste voordelen zijn: investeringsvoordelen/kostenvoordelen, flexibiliteit, toegangsvoordelen tot de markt. De drie belangrijkste nadelen zijn eventuele problemen bij: toegang van de provider tot de data, continue werking, lock-in.

Bij het gebruik van cloud computing treden er verschillende risico's op. Bedrijven moeten bij het gebruik van cloud computing rekening houden met deze risico's. Voor particulieren is dit minder het geval.

Algemene risico's kunnen allereerst ingedekt worden door de cloud gebruiker. Het management moet een geheel overzicht hebben van de cloud, de risico's moeten bekend zijn bij de managers, het management moet weten wie de cloud gebruikt, het management moet het risico in de cloud monitoren, het management moet controle houden wat er in de cloud opgeslaan wordt. De technische staf moet de nieuwste, laatste best practices van cloud computing steeds opvolgen, de technische staf moet nagaan of de cloud met wetten en zogenaamde policies overeenstemt. De technische staf en het zakenpersoneel moeten alle noodzakelijke kennis hebben van de cloud.

Algemene risico's kunnen daarnaast ingedekt worden door de cloud gebruiker en de cloud provider aan de hand van een vertrouwensmodel. Het vertrouwen zal de kosten van onderhandelingen verlagen en de mogelijkheid tot conflict verlagen. Er zijn vijf eigenschappen die gecontroleerd moeten worden alvorens er vertrouwen in de cloud kan zijn: aanpasbaarheid, robuustheid, schaalbaarheid, beschikbaarheid, betrouwbaarheid. Privacy en beveiliging zijn de ondersteunende principes van deze 5 eigenschappen. Privacy risico en beveiligingsrisico bespreek ik verder. Wanneer de 5 eigenschappen worden afgesproken dan wordt er een contract opgesteld. Hier treedt het consumentenrisico bij het opstellen van het contract op, dit bespreek ik ook verder.

Allereerst zijn er verschillende privacy risico's. Deze privacy risico's kunnen ingedekt worden door wetgeving. In de US stelt de privacywetgeving echter niet veel voor. In US is privacy een goed dat te koop is. De US Supreme Court heeft nog altijd niet onderkend dat informatie privacy één van de fundamentele rechten is. In EU is privacy echter een grondrecht. Europa heeft de striktste privacywetgeving ter wereld. Spanje, Italië en Duitsland zijn nog strenger. Een Amerikaans bedrijf kan zich wel Safe Harbor compliant verklaren aan de strengere Europese Data Protection Directive. Dit wil zeggen dat het voldoet aan de strengere Europese regelgeving. Het lijkt te tenderen naar een internationaal

verdrag. Het samenwerken van de verschillende landen zal zeker niet slecht zijn, maar of het gaat lukken dat is een andere vraag. Naast de wetgeving dekt de privacy policy ook de privacy risico's in. Wanneer er met gevoelige data gewerkt wordt, moet er via policies bepaald worden wie er toegang tot de data krijgt en hoe met die data wordt omgegaan. Dit mag niet een loutere ad hoc regeling zijn. Er moet een echte policy hierover aanwezig zijn. Het is belangrijk dat de privacy policy goed bekeken wordt alvorens men voor een cloud service intekent. De privacy policy is, zoals bijvoorbeeld bij Google, meestal vaag opgesteld. Dit is meestal gedreven door een commercieel perspectief, maar ondermijnt de wettige privacy rechten van de individuele gebruiker. Wetten die deze privacy policies beter reguleren, moeten dus toegepast en geïmplementeerd worden.

Bij transborder clouds zijn er speciale privacy risico's. Hier speelt het feit of de wetten van het land waar de data naar getransfereerd wordt een voldoende mate van privacy garandeert die minstens even hoog is als het land van de gebruiker. Als indekking is hiervoor artikel 25 van de EU Directive 95/46 (data mag enkel getransfereerd worden naar een land als het voldoende mate van privacy kan garanderen). Er kan ook gewerkt worden met binding corporate rules (standaarden opleggen aan verschillende entiteiten in verschillende landen, die standaarden moeten in één land in Europa goedgekeurd worden).

Verder zijn er de beveiligingsrisico's. Er zijn verschillende beveiligingsrisico's. Deze beveiligingsrisico's kunnen ingedekt worden door: logs opslaan om de werking van de cloud transparant te maken, andere contextuele informatie bij het aanmelden toe te voegen, paswoorden niet te snel delen, encryptie, tokens (een reeks cijfers of karakters die niet te verzinnen zijn, iemand die een token heeft bewijst daarmee geldige toegang te hebben). De hoogste laag SaaS zal de meeste beveiliging krijgen en hoe meer men afdaalt in de lagen tot IaaS zal men meer beveiliging aan de eindgebruiker laten. Bij de opbouw kan men ook verschillende beveiligingsrisico's indekken: protectie van de fysieke faciliteiten (redundante stroom, redundante koeling, tweede back-up center, zuurstof verlaagt bij brand, cijferslot op racks, etc.), implementeren van voldoende scheiding tussen de virtuele clients, gegevens gemakkelijk kunnen overdragen naar een andere cloud provider door bijvoorbeeld standaard API's. Bij de operationele werking kan men ook verschillende beveiligingsrisico's indekken: verzekeren van de business continuïteit door regelmatige inspectie van de infrastructuur van de cloud provider, een systeem waarbij indringers snel ontdekt worden (firewalls, etc.), gebruikers op de hoogte brengen van een veiligheidsincident en noodplan opstarten, noodzakelijk om te weten wat de redenen van het beveiligingsincident waren (root cause analyse), bottlenecks bij het overdragen van grote hoeveelheden data moet vermeden worden door bijvoorbeeld het overbrengen van disks. Er blijven echter steeds menselijke factoren mee betrokken, je kunt niet altijd alles technisch indekken.

In contracten gebeurt het wel eens dat cloud providers bevoordeeld worden ten nadele van cloud gebruikers. Dit is het consumentenrisico bij het opstellen van

het contract. Het zijn toetredingscontracten waarbij de cloud gebruikers veelal onwetend met een aantal benadelende voorwaarden instemmen. Bij public cloud spelen deze risico's een grotere rol, bij private cloud een minder grotere rol omdat men hier over meerdere dingen in het contract kan onderhandelen dan bij public cloud. Om een gebalanceerde rechtvaardigheid te garanderen tussen cloud provider en cloud gebruiker hanteert de wet enkele beperkingen op dergelijke contracten: verplichte informatie over het product en/of provider, omstandigheden van het vormen van het contract, etc. Er blijven echter benadelingen meespelen. De wetgeving moet hiervoor beter toegepast en verbeterd worden om de benadeling zo veel mogelijk te verminderen.

Er moet gekeken worden bij de audit of er voldaan wordt aan de desbetreffende wetgeving en of de aangegeven additionele indekkingen voldaan zijn. Door middel van continue monitoring kan men zich ervan verzekeren dat de indekkingen gedaan worden.

3 Inhoudsopgave

4 Lijst van afkortingen

AES: Advanced Encryption Standard
API: Application programming interface
BDMA: Belgian Direct Marketing Assocation
BTW: Belasting over de toegevoegde waarde
CaaS: Communication as a Service
CPU: Central processing unit
CEO: Chief Executive Officer
CRM: Customer Relationship Management
ERP: Enterprise Resource Planning
EU: Europese Unie
EVRM: Europees Verdrag voor de Rechten van de Mens
FOD: Federale Overheidsdienst
GB: Gigabyte
HIPAA: Health Insurance Portability and Accountability Act
HTTPS: HyperText Transfer Protocol Secure
IaaS: Infrastructure as a Service
ICT: Informatie- en communicatietechnologie
I/O: Input/output
IP: Internet Protocol
IT: Informatietechnologie
ISMS : Information Security Management System
ISO: International Organisation for Standardization
KMO: Kleine en Middelgrote Onderneming
NaaS: Network as a Service
NDA: Non-Disclosure Agreement
NV: Naamloze Vennootschap
PaaS: Platform as a Service
SaaS: Software as a Service
SAS: Statement on Auditing Standards
SLA: Service Level Agreement
UK: United Kingdom
UPS: Uninterruptible Power Supply
US: United States (of America)
USB: Universal Serial Bus
VN: Verenigde Naties
VPN: Virtual Private Network

5 Continue monitoring als audittool bij cloud computing

5.1 Hoofdstuk 1: Inleiding en probleemstelling

Ondernemingen gebruikten grote mainframes in de jaren ’60, minicomputers kwamen erbij in de jaren ’70 en personal computers in de jaren ’80. De laatste jaren groeit het gebruik van smart phones en andere mobiele toestellen. De ontwikkeling van cloud computing is nu één van de meest recentste fenomenen (Jena & Mahanti, 2011). Uiteraard heeft die evolutie een grote invloed op risico’s, controle en auditing. Voor dit onderzoek kozen wij voor een een combinatie van literatuuronderzoek met een aantal interviews met bevoorrechte getuigen uit de wereld van aanbieders van cloud computing oplossingen, gebruikers, consultants, advocaten en durfkapitaalverschaffers. Daarnaast werd er een bezoek gebracht aan een vakbeurs over IT-security en een datacenter van Belgacom in Brussel.

De personen, die ik geïnterviewd heb, zijn het unaniem eens dat cloud computing een belangrijke en blijvende component is.

Tom Aerts (LRM) (2012) vermeldt dat ze heel wat nieuwe innovatieve projecten rond cloud computing zien langskomen. Het is een nieuwe trend.

Mark Lens (Eurosys – IT-solutions) (2012) merkt op dat er een enorme shift aan het gebeuren is naar de cloud toe. Cloud is een modewoord.

Laurens Dauwe (Stibbe) (2012) merkt op dat ze de laatste drie jaren meer en meer vragen krijgen over cloud computing. Hij merkt ook op dat cloud computing een nieuwe trend is die echt wel belangrijk is. Maar je moet de trend ook niet overschatten.

Erik R. Van Zuuren (Vakbeurs IT security) (2013) merkt op dat meer en meer organisaties zich willen verbinden met cloud online services.

Met cloud computing wordt ‘computing’ gezien als een utility zoals water, elektriciteit, gas en telefonie (Cheng & Lai, 2012).

5.1.1 Incentives om te komen tot cloud computing

De laatste jaren zijn er verschillende krachtige veranderingen opgetreden die een invloed hebben op het gebruik van informatiesystemen binnen zowel de private als de bedrijfscontext, waarbij de eigen infrastructuur meer en meer wordt uitbesteed (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2010):

- De eenheidskost van computerbewerkingen wordt steeds lager. Dit komt doordat opslagcapaciteit steeds goedkoper wordt en computers steeds sneller berekeningen kunnen uitvoeren (Marston et al., 2010). De zogenaamde ‘wet van Moore’ suggereert dat het computervermogen immers elke 18 tot 24 maanden zal verdubbelen (O’Brien & Marakas,

2008). Tot nu toe is deze voorspelling telkens uitgekomen. Doordat de eenheidskost van computerbewerkingen blijft dalen, wordt het uitvoeren van computerbewerkingen meer en meer als een commodity beschouwd (Marston et al., 2010). Een commodity is een basisproduct dat gewoon vervangbaar is door een ander product van hetzelfde type en waarvan de prijs onderhevig is aan de wetten van vraag en aanbod. Daarnaast komen er steeds meer spelers op deze cloud computing markt. Er zijn dus veel spelers die hetzelfde product aanbieden op een prijssensitieve markt. Er is dus als het ware perfecte competitie (Durkee, 2010). Er werd enkel gekeken naar de prijs. Dit was bij cloud 1.0. Bij cloud 2.0 gaat men de cloud services veelal een beetje differentiëren doordat ze willen voldoen aan bepaalde betrouwbaarheidsmaatstaven, kwaliteitsmaatstaven, etc. die ze inwilligen met bepaalde SLA's (Durkee, 2010).

- Het managen van de hele infrastructuur van informatiesystemen binnen het eigen bedrijf wordt steeds complexer (Marston et al., 2010).

- Investeringen in informatietechnologie worden het grootste deel van de tijd niet helemaal ten volle gebruikt (Marston et al., 2010).

- Het opkomen van het Internet (O'Brien & Marakas, 2008).

- De draadloze bereikbaarheid met een veelheid aan apparatuur (PC's, tablets, smartphones, smartwatches,…).

- Het digitale universum van informatie is aan het exploderen. Ondanks de revolutionaire toename van goedkope opslagcapaciteit is er geen plaats genoeg op lokale servers om alles op te slaan (Barrasso & Wallace, 2012).

5.1.2 Definities van cloud computing

Cloud computing wordt gedefinieerd als iedere abonnementsgerelateerde of pay-per-use, je betaalt enkel wat je gebruikt, service die in real time over het Internet de bestaande informatietechnologiemogelijkheden uitbreidt (Knorr & Gruman, 2011). Pieter Delbeke (Zentrick) (2013) merkt op dat je je architectuur en software ook moet aanpassen aan de structuur van de cloud. De term cloud staat voor het feit dat men niet moet weten wat er precies in de cloud gebeurt, het is voldoende dat de consument zich aan de cloud aansluit en zo kan de consument van de nodige service genieten (Panko & Panko, 2011). Raf De Backer (Ferranti) (2013) bevestigt dat de technologie in de cloud de consument niet meer interesseert. Enkel belangrijk is dat de consument zich aan de cloud kan aansluiten. Bij cloud 1.0 werd de service veelal enkel als commodity verkocht en keek men veelal enkel naar de prijs. Een cloud service was heel prijsgevoelig. Bij cloud 2.0 wordt er echter steeds meer rekening gehouden met de up-time en betrouwbaarheid, waar bij cloud 1.0 enkel naar de prijs gekeken werd (Durkee, 2010). Vandaag de dag is er veel meer 2.0 waarbij men meer kijkt naar de betrouwbaarheid en het hele plaatje dan wel enkel naar de prijs. De

continue operabiliteit van het pay-per-use model kan gegarandeerd worden door een SLA (Service Level Agreement). Dit stelt diverse streefdoelen die de operabiliteit van een cloud computing provider minimaal moet halen (Ismail, 2011). Deze SLA houdt rekening met de risico's en hoe de provider deze risico's voor de consument indekt. Om te weten of de gewenste service echter daadwerkelijk gehaald wordt en de risico's ingedekt worden en de SLA dus overeenkomt, moet er echter aan continue auditing gedaan worden. Hierbij worden de risico's duidelijk, hoe deze risico's ingedekt worden en of deze indekkingen echt gebeuren.

Raf De Backer (Ferranti) (2013) bevestigt dat cloud een service is waarbij iemand anders met de IT-gerelateerde zaken bezig is en de risico's hierbij uitlegt en afdekt en dat jij jezelf bezig kan houden met de core business kant van het verhaal.

Bedrijven vragen aan cloud providers typisch 4 negens aan up-time (99,99 %), dit zijn 52 minuten dat de server niet beschikbaar is per jaar. Elke additionele negen verdubbelt de kost van de service. Omdat de kost van beschikbaarheid zeer fel vergroot als de 100 % grens bereikt wordt, beschouwen velen de 5 negens (99,999 %) en erboven als onbereikbaar en onbetaalbaar (Durkee, 2010).

Waar vroeger een eigen server in privaat bezit van het desbetreffende bedrijf werd gebruikt tot verwerking en opslag van gegevens, wordt dit vandaag de dag meer en meer uitbesteed (Marston et al., 2010). Een gedeelte van de infrastructuur dat vroeger eigen bezit was, wordt uitbesteed aan een derde partij (Roes, 2008). Deze derde partij is veelal veel gespecialiseerder en heeft de nodige mankracht ter beschikking om deze uitbestede service aan te bieden (Panko & Panko, 2011). Deze kan de benodigde opslagmogelijkheden en mogelijkheden tot verwerking van gegevens veel flexibeler aanbieden.

Een andere ruimere definitie van cloud computing stelt vier voorwaarden. Een eerste voorwaarde is dat de service geleverd wordt over een telecommunicatienetwerk. Een tweede voorwaarde is dat de gebruikers kunnen vertrouwen op de service om hun data te verwerken of te raadplegen. Een derde voorwaarde is dat de data onder wettige controle van de gebruiker staan. Een laatste voorwaarde is dat sommige resources waarop de service draait gevirtualiseerd kunnen worden (Ismail, 2011).

Uit de interviews blijkt dat de term cloud computing niet altijd eenduidig gebruikt wordt.

Peter Dedrij (Microsoft) (2013) merkt op dat cloud computing een heel ruim begrip is en dat vandaag de dag er veel gegoocheld wordt met dit begrip zonder dat de betekenis ervan duidelijk is.

Pieter Delbeke (Zentrick) (2013) bevestigt dat er vandaag de dag heel veel gebruik wordt gemaakt van de term cloud in een foutieve zin. Er worden heel

veel dingen verstaan onder cloud dit totaal niet cloud zijn. Een echte cloud provider doet veel meer dan enkele virtuele servers aanbieden.

Erik R. Van Zuuren (Vakbeurs IT security) (2013) bevestigt dat bij de cloud veelal iedere keer het verkeerde vocabularium gebruikt wordt en het in een foutieve zin gebruikt wordt.

Raf De Backer (Ferranti) (2013) bevestigt dat cloud nog altijd een buzz-woord is. Iedereen gebruikt op dit moment wel het woord cloud.

Mark Lens (Eurosys – IT-solutions) (2012) vermeldt dat in het verleden bedrijven hun systemen klassiek on-premise hadden staan, dit is aan het veranderen. Er is meer evolutie naar cloud-gebaseerde oplossingen. Klassieke systemen on-premise waren gekenmerkt met heel wat problemen met klanten die mailgerelateerd ofwel back-up gerelateerd waren ofwel een combinatie van de twee. Bij Eurosys werd in de eerste fase mail overgebracht naar de cloud, wat niet veel kost. Voor Google kost het veertig euro per jaar voor een volledige mailbox van een gebruiker in de cloud te zetten met vijfentwintig Gb opslagcapaciteit. Op een jaar tijd zijn ongeveer 250 bedrijven en zo een 6000/7000 gebruikers naar de cloud overgebracht met hun mail. In de tweede fase werd heel het faxverhaal overgebracht naar een cloud omgeving. Ze stellen applicaties van een andere cloud provider voor aan de klant en ze verdelen applicaties. Ze bouwen daar bovenop eigen add-ons, maar hebben zelf geen cloud applicaties die ze op die manier ter beschikking gaan stellen.

Mark lens (Eurosys – IT-solutions) (2012) haalt aan dat je heel specifiek moet gaan kijken welke applicatie zich ertoe leent om in de cloud te worden opgenomen.

Gartner, een onderzoeks- en adviesbureau in de informaticatechnologie-sector, stelt dat organisaties meer en meer aan het overschakelen zijn van hardware binnen het eigen bedrijf naar pay-per-use cloud service modellen (Han, 2010).

De term cloud computing werd in brede kring populair in 2006 door de service EC2 (Amazon Elastic Compute Cloud) van Amazon (Abbadi & Martin, 2011). Het is een web service dat schaalbare computercapaciteit in de cloud aanbiedt (website Amazon EC2, 2013). Door cloud computing kan het bedrijf zich nu richten op zijn meer kritische doelen (core competences) (Ros, 2012). Pieter Delbeke (Zentrick) (2013) bevestigt de rol van de Amazon cloud services. Dit is de Amazon waarbij je ook boeken en andere producten online kunt kopen. Zij hadden veel servers draaien om hun online verkoop te regelen. Op piekmomenten hadden zij enorm veel capaciteit nodig. Ze zijn begonnen om het overschot aan capaciteit in rustiger tijden te verkopen als cloud services. Amazon biedt een heel ruim pakket aan cloud diensten aan waarin SaaS een belangrijke rol vervult.

Cloud computing is een grote markt. Forrester Research schat dat de cloud computing markt 185 miljard euro waard zal zijn in 2020. Dat is een verhoging

van 154 miljard euro in 10 jaar. De uitgave aan materiaal voor zowel de publieke als private cloud zal aan 56 miljard euro geraken in 2015 (Barrasso & Wallace, 2012).

Pieter Delbeke (Zentrick) (2013) stelt als voorbeeld van een cloud Amazon. Je gaat naar Amazon en je duidt aan hoeveel virtuele machines je wilt hebben. Je zegt hoe snel je die machines wilt laten draaien en hoeveel capacteit die moeten hebben. Amazon start die servers op en monitort de servers zodat die stabiel draaien. Als die niet stabiel draaien, dan krijg je een e-mail. Al die dingen gebeuren volautomatisch. Het verder specifiek configureren en monitoren gebeurt allemaal door Amazon en daar moet de eindgebruiker zich niets van aantrekken.

5.1.3 Technologieën die cloud computing ondersteunen

De evolutie naar volwaardige cloud computing modellen is volop aan de gang. Verschillende hoofdtechnologieën zijn daarbij belangrijk:

- Virtualisatie abstraheert de koppeling tussen hardware en het operating systeem (Rimal & Choi, 2012). De logische resources worden gescheiden van de onderliggende fysieke resources om flexibiliteit te verbeteren, kosten te drukken en dus waarde aan de business toe te voegen. De fysieke karakteristieken van het platform worden verborgen. In de plaats daarvan wordt er een abstract virtueel platform voorgesteld, dat zich gedraagt als een onafhankelijk systeem en op aanvraag kan aangepast of geconfigureerd worden. Het eigenlijke fysieke platform zal zo beter gebruikt worden doordat er meerdere virtuele platforms mogelijk zijn op één bepaald fysiek platform. Virtualisatie kan gevonden worden onder de vorm van netwerk, hardware en applicatie (Rimal & Choi, 2012). Waar virtualisatie een aantal beveiligingsproblemen introduceert, geeft het ook antwoord op heel wat beveiligingsvragen. De sensors kunnen de CPU activiteit meten, I/O patronen, en geheugenbeheer. Gebaseerd op modellen van vroeger gedrag kunnen verdachte activiteiten gespot worden (Anthes, 2010).
  Kristof Janssens (Jordens Datacenter) (2012) merkt op dat Jordens Datacenter virtuele VM-ware machines gebruikt.

- Multitenancy. Hierbij is het mogelijk dat één instantie van een applicatiesoftware meerdere clients bereikt. Dat laat wederom toe dat de resources beter gebruikt zullen worden. Specifieke softwarelicenties voor cloud computing kunnen hiervoor gebruikt worden (Armbrust et al., 2010).

- Web services (Rimal & Choi, 2011). Dit zijn software systemen die gemaakt zijn om interoperabiliteit tussen machines te verwezenlijken. Hiervoor maken ze gebruik van gestandaardiseerde interfaces die toelaten dat de communicatie door diverse machines begrepen wordt (Rimal & Choi, 2011).

- Grid computing, dit is het aan elkaar koppelen van computers om ze samen te laten werken (Rimal & Choi, 2011).

- Utility computing, dit is het samenvoegen van computing resources als een gemonitorde service (Rimal & Choi, 2011).

- Distributed computing, dit is een techniek waarbij computertaken niet door één computer worden uitgevoerd, maar door een gedistribueerd netwerk (Rimal & Choi, 2011).

- Web 2.0, dat zich focust op interoperabiliteit tussen gebruikers, en web 3.0, dat zich focust op interactiviteit (Rimal & Choi, 2011).

- 'Ubiquitous' één host en die is toegankelijk van overal, op elk moment (Rimal & Choi, 2011).

5.1.4 Service modellen van cloud computing

Het meest bekende model is SaaS oftewel Software as a Service. Hier werken de applicaties op aanvraag in de cloud, waardoor er geen nood meer is om de applicaties te installeren op de client computer (Marston et al., 2010). Organisaties die SaaS gebruiken, hebben toegang tot deze service via een 'thin client': de webbrowser (Garrison, Kim, & Wakefield, 2012). Voorbeelden van SaaS zijn applicaties zoals Salesfore en Netsuite (Durkee, 2010). Speciale types van SaaS zijn desktop as a service, test environment as a service. SaaS zorgt ervoor dat applicaties niet meer lokaal moeten opgeslagen worden (Mohammed, 2011).

Kristof Janssens (Jordens Datacenter) (2012) en Mark Lens (Cegeka) (2012) merken op dat zij vooral SaaS aanbieden.

Een ander model is PaaS oftewel Platform as a Service. Hier wordt een platform ter beschikking gesteld waarop diverse applicaties op gemaakt kunnen worden (Garrison et al., 2012). De kost en complexiteit van het kopen of managen van de onderliggende hardware wordt hier vermeden (Garrison et al., 2012). Het voordeel van PaaS is dat de ontwikkelaar een gehele productieomgeving kan kopen (Durkee, 2010). Een aantal voorbeelden zijn Microsoft's Azure Service Platform, Salesfore Force.com of Google App Engine (Marston et al., 2010).

Raf De Backer (Ferranti) (2013) haalt aan dat ze tevens PaaS aanbieden.

Het laatste model is IaaS oftewel Infrastructure as a Service. Hierbij worden de opslag- en computerbewerkingscapaciteiten als een service aangeboden (Garrison et al., 2012). Een aantal voorbeelden zijn Amazon's S3 opslag service en EC2 computing platform, Rackspace Cloud Servers of Joyent (Marston et al., 2010).

Tom Palmaers (Cegeka) (2012) merkt op dat ze IaaS aanbieden. De applicatielaag en het beheer ervan (SaaS) die doen ze voor sommige klanten maar is eigenlijk zeer beperkt. Het is niet echt dat we de applicatie als een service aanbieden, dat is eerder bij de klant.

Mark Lens (Eurosys – IT-solutions) (2012) merkt op dat zij IaaS aanbieden.

Raf De Backer (Ferranti) (2013) merkt op dat ze vooral IaaS aanbieden.

De Internationale Telecommunicatie Unie noemt in 2012 ook nog NaaS en CaaS als mogelijke service modellen voor cloud computing.

NaaS oftewel Network as a Service is een categorie van cloud services waarbij aan de cloud user de mogelijkheid wordt geboden netwerkconnectiviteitservices te gebruiken. Hiermee wordt bijvoorbeeld bedoeld: een flexibele VPN verbinding, bandbreedte op aanvraag, etc. Dit is de definitie volgens de Internationale Telecommunicatie Unie (2012).

CaaS oftewel Communication as a Service is een categorie van cloud services waarbij aan de cloud user de mogelijkheid wordt geboden real-time communicatie- en samenwerkingservices te gebruiken. Hiermee wordt bijvoorbeeld bedoeld: voice over IP, instant messaging, video conferencing, etc. Dit is de definitie volgens de Internationale Telecommunicatie Unie (2012).

In de praktijk kunnen deze vijf modellen op verschillende wijzen geïmplementeerd worden.

5.1.5 Implementatiewijzen van cloud computing

De modellen kunnen als public-, private-, community- of hybrid cloud ingezet worden.

Public cloud wordt gekarakteriseerd als een cloud service die raadpleegbaar is door derde partijen, het publiek, via het Internet (Armbrust et al., 2010). Google Apps is een bekend voorbeeld hiervan (Marston et al., 2010).

Private Cloud wordt gemanaged binnen de eigen organisatie. Bij dit soort van cloud is er een grotere controle over de desbetreffende infrastructuur. Niet het publiek, maar een selecte organisatie kan ervan gebruik maken. Deze cloud service is wel nog groot genoeg om van de voordelen bij cloud computing gebruik te maken (Armbrust et al., 2010). Een voorbeeld hiervan is Government Cloud door Google (Marston et al., 2010). Kostenbesparingen bij een private cloud zullen eerder gelimiteerd zijn (Garrison et al., 2012).

Kristof Janssens (Jordens Datacenter) (2012) merkt op dat zij private cloud diensten aanbieden.

Tom Palmaers (Cegeka) (2012) merkt op dat Cegeka voornamelijk private cloud diensten levert.

Community cloud wordt gecontroleerd en gemanaged door een groep van organisaties die een gemeenschappelijke interesse hebben. Deze gemeenschappelijke interesse kunnen specifieke beveiligingsbehoeften zijn of een gemeenschappelijke missie inhouden. Een voorbeeld hiervan is de United States federal government, deze is één van de grootste gebruikers van een community cloud (Rimal & Choi, 2011).

Tenslotte bestaat er hybrid cloud. Dit is een combinatie van een public en een private cloud. Gewoonlijk wordt niet-kritische informatie op een public cloud gezet, terwijl de kritische informatie en services op een private cloud gezet worden die onder controle van de organisatie staat (Rimal & Choi, 2011).

Peter Dedrij (Microsoft) (2013) bevestigt dat er verschillende mogelijke implementatiewijzen van cloud computing zijn. Ofwel ga je naar een soort private cloud. Een stukje cloud dat voor u voorzien is. Ofwel ga je naar een public cloud provider en daar zijn er enkele waarvan Microsoft ook ééntje is, daar ga je naar nog grotere schaalvoordelen. Je kan daarnaast ook een combinatie maken van verschillende implementatiewijzen. Bepaalde stukken data hou je on-site. Je gaat bepaalde dingen naar een lokale host/private cloud hosten en minder kritische data naar een public cloud outsourcen. Het is belangrijk dat deze hybride systemen goed geïntegreerd worden.

Tom Aerts (LRM) (2012) bevestigt het bestaan van hybrid cloud en merkt op dat overheden veel meer met privégegevens bezig zijn. Confidentiële gegevens (zoals bijvoorbeeld patiëntgegevens, btw en taksen) als je dergelijke dingen cloud based gaat maken daar is potentieel een zeer groot gevaar. Bij overheden en banken wordt de data heel fel afgeschermd. Eer dat je dat soort gegevens cloud based gaat maken dat kan wel nog even duren.

5.1.6 Probleemstelling

Bij het gebruik van cloud computing treden er verschillende risico's op.

In deze masterproef ga ik onderzoeken welke risico's er zijn en hoe deze risico's het best ingedekt worden zodat aan het SLA (Service Level Agreement) kan voldaan zijn. Vermits bestaande auditmanieren niet voldoende zijn voor cloud computing stel ik zo een eigen auditkader op dat gebruikt kan worden voor cloud computing.

Ik stel vanuit de wetenschappelijke literatuur een auditkader op en aan de hand van structurele diepte-interviews kijk ik of het auditkader in de realiteit geïmplementeerd kan worden.

5.1.7 Methodologie

Diverse bevoorrechte getuigen, zowel cloud users als cloud providers, werden geïnterviewd. Aan de hand van een kwalitatieve data analyse toetsen we of het vertrouwensmodel in de realiteit al reeds gedeeltelijk gebruikt wordt en/of het realistisch is dit model in de praktijk in uitvoering te brengen. Indien ik

kwantitatieve data zou gaan verzamelen zou ik enquêtes moeten gaan afnemen. Vermits de respons op dit soort enquêtes zeer laag is, kies ik voor een kwalitatief onderzoek. Aan de hand van structurele diepte-interviews met bevoorrechte getuigen verkrijg ik accurate kwalitatieve data. Mijn onderzoeksgebied blijft binnen België. Vermits ik enkel interviews afneem binnen België zal het praktijkonderzoek vooral hierop gericht zijn. Een internationaal onderzoek zal het niet zijn, ik spits mij toe op Belgische aanbieders van cloud computing oplossingen, gebruikers, consultants, advocaten en durfkapitaalverschaffers.

Ik zal eerst trachten toestemming te krijgen van de desbetreffende geïnterviewde om het gesprek op te nemen zodat ik later gemakkelijk het gesprek opnieuw kan afspelen. Indien deze echter geen toestemming geeft, neem ik enkel notities en zal zo dan aan kwalitatieve dataverzameling doen (Sekaran & Bougie, 2009). Ik gebruik structurele interviews omdat ik via de literatuur al de aandachtspunten te weten gekomen ben wat ik precies kan vragen. Via deze structurele interviews zal ik de kwalitatieve data ook makkelijker kunnen gaan coderen (Sekaran & Bougie, 2009).

Na ieder gesprek zal ik vragen of de geïnterviewde nog referenties kan geven. Aan de hand van deze referenties zal ik met nog meer personen rond mijn onderzoeksdomein in contact komen. Ik zal proberen een zo gevarieerd mogelijke waaier aan geïnterviewden te krijgen, dit om een eenzijdig beeld te vermijden. Waar het niet zal lukken de beste variatie te krijgen, zal ik proberen dit te benaderen.

Bij het afnemen van interviews is het belangrijk dat de bias, dit zijn errors of onnauwkeurigheid bij het verzamelen van data, zo klein mogelijk is. Bias kan geïntroduceerd worden door de interviewer, geïnterviewde of de situatie (Sekaran & Bougie, 2009). Ik zal zorgvuldig naar de geïnterviewde luisteren, vertrouwen opbouwen, de vragen herhalen of verduidelijken waar nodig, neutrale kledij aandoen en een neutrale locatie trachten te kiezen (sommige personen voelen zich niet op het gemak als ze geïnterviewd worden op de werkplaats). Dit allemaal om bias te minimaliseren.

Ik zal bij het interviewen de volgende tips in het achterhoofd houden: trachten geen vooroordelen te hebben, aangenaam te zijn, eerst algemene vragen en dan pas specifieke vragen te stellen (de zogenaamde funneling technique), proberen zonder bias vragen te stellen (bijvoorbeeld niet: ‘Het werk dat je doet moet wel heel saai zijn. Wat zijn precies je ervaringen met dit werk?’), verheldering waar nodig geven, de respondent door onzekerheden helpen als hij niet in staat is zijn mening verbaal te maken (Sekaran & Bougie, 2009).

De interviews zullen face-to-face verlopen. Voordeel hiervan is dat de vragen kunnen aangepast worden. Een ander voordeel is dat, indien noodzakelijk, non-verbale tekens kunnen opgevangen worden. Nadeel is de geografische verplaatsingen die noodzakelijk zijn (Sekaran & Bougie, 2010). Een verdere verplaatsing is voor mij echter niet zo erg. Een substantieel nadeel is het feit dat

respondenten niet anoniem worden behandeld als ze face-to-face tegenover de interviewer zitten (Sekaran & Bougie, 2009).

Deze kwalitatieve data ga ik daarna coderen. Dit is het verminderen, opnieuw ordenen en integreren van de data om een theorie te vormen (Sekaran & Bougie, 2009). De bedoeling is als het ware betekenisvolle conclusies te kunnen vormen over de data. Via codes en categorieën van codes (bijvoorbeeld welke categorie van risico is het, is het een indekking van risico, etc.) zal ik de tekst tot betekenisvolle kleinere stukken kunnen representeren (Sekaran & Bougie, 2009). Ik zal niet telkens nieuwe codes en categorieën moeten aanmaken. Doordat ik reeds een theoretisch model heb opgesteld kan ik daar mijn codes en categorieën op gaan baseren. Als het nodig is kunnen gedurende het meer en meer afleggen van diepte-interviews codes en categorieën veranderd of verfijnd worden als er nieuwe codes of categorieën blijken op te duiken (Sekaran & Bougie, 2009). Wat in het vet is uitgedrukt zijn hoofdpunten en de belangrijkste punten/codes uit het interview. Deze uitdrukkingen in bolt breng ik over op mijn literatuurstudie. Ik ga zo kijken of het realistisch zou zijn om het opgestelde auditkader in de realiteit te implementeren.

Uiteindelijk moeten er uit deze kwalitatieve data analyse conclusies getrokken worden. Aan de hand van de vooropgestelde data voorstellingen en codes en categorieën kunnen we ons theoretisch model waar nodig bijschaven en komen zo tot een reëel model dat in de realiteit als continu auditmodel kan gebruikt worden (Sekaran & Bougie, 2009). Deze bevindingen heb ik geïmplementeerd in bovenstaande literatuurstudie.

Betrouwbaarheid en validiteit moeten echter nog geverifieerd worden (Sekaran & Bougie, 2009). Categorie betrouwbaarheid zorgt ervoor dat onze categorieën op een zelfde manier worden geïnterpreteerd zodat er overeenkomst is welk item van de populatie in een bepaalde categorie hoort of niet hoort (Sekaran & Bougie, 2009). Er moet rekening mee gehouden worden de categoriebeschrijving niet te simpel te maken en te generaliseerbaar te maken. Maar een goed gevormde, niet te algemene, definitie van de categorie zal een goede categorie betrouwbaarheid ten goede komen (Sekaran & Bougie, 2009). Via de literatuurstudie hebben we al bepaalde categorieën opgesteld. We gaan ook de validiteit van deze studie verzekeren (Sekaran & Bougie, 2009). We gaan eerst kijken naar de frequentie van bepaalde events. Infrequente voorkomingen worden uitgefilterd. Zo zal er vermeden worden dat er te veel aandacht gaat naar een kleine frequentie van voorkomingen (Sekaran & Bougie, 2009). Er zal ook vermeden worden dat infrequente voorkomingen die de theorie toch ondersteunen, worden geselecteerd. Infrequente voorkomingen gaan we er als het ware uitfilteren. Tenslotte kan validiteit bereikt worden door de representativiteit van de cases ten op zichte van de populatie te verzekeren en door de toevoeging van cases die de theorie tegenspreken (Sekaran & Bougie, 2009). Ik heb hiervoor getracht een zo representatief en volledig beeld van geïnterviewden te krijgen. Ik heb diverse gebruikers, consultants, advocaten en

durfkapitaalverschaffers geïnterviewd om een zo volledig mogelijk beeld te krijgen.

Tenslotte zullen we via triangulation ervoor zorgen dat we meer vertrouwen kunnen hebben in onze resultaten. We gaan hier data triangulation toepassen. We gaan data verzamelen van verschillende soorten en/of op verschillende tijdperiodes (Sekaran & Bougie, 2009). In dit geval gaan we bij verschillende cloud computing providers interviews afnemen en we gaan deze interviews op een ander tijdsmoment afnemen.

Triangulation zorgt er ten slotte voor dat we nog meer vertrouwen kunnen hebben in onze resultaten.

Daarnaast moeten echter ook nog een aantal ethische regels bij het verzamelen van gegevens in acht houden. Allereerst zal ik verzekeren dat de verzamelde informatie strikt confidentieel gehouden zal worden (Sekaran & Bougie, 2009). Zo zal de privacy van de desbetreffende geïnterviewde of het desbetreffende bedrijf niet in het gedrang komen. De bedoeling van het interview zal ik in het begin duidelijk maken zodat er geen misverstand bestaat over de context van het interview (Sekaran & Bougie, 2009). Ik zal vermijden om te persoonlijke vragen te stellen, namelijk mogelijke vragen die te veel aan de persoonlijke privacy van de persoon in kwestie schenden (Sekaran & Bougie, 2009). Ik zal geen misinterpretaties of ruis in het rapporteren van de data brengen (Sekaran & Bougie, 2009).

Ik zal uiteindelijk kunnen concluderen of het zelf opgestelde continue auditmodel om de diverse risico’s bij cloud computing in te dekken geschikt is voor eventuele verdere reële implementaties.

5.2 Hoofdstuk 2: Voor- en nadelen van cloud computing

Laurens Dauwe (Stibbe) (2012) haalt aan dat cloud computing vele voordelen heeft. Het heeft echter ook bepaalde nadelen. Maar als hij het globaal bekijkt, moet hij toegeven dat de nadelen niet opwegen ten op zichte van de voordelen.

5.2.1 Voordelen van cloud computing

De voordelen van cloud computing worden hier besproken in volgorde van belangrijkheid.

Investeringsvoordelen/ kostenvoordelen

- Het verlaagt de kost voor kleinere bedrijven om op de markt te verschijnen omdat het voor een kleiner bedrijf nu ook mogelijk is dure intensieve analytische bewerkingen te gaan uitvoeren (Marston et al., 2010).
- Door het combineren van verschillende infrastructuren op dezelfde locatie zijn er schaalvoordelen mogelijk. Er worden personeel en financiële middelen bespaard. Hierdoor kunnen lagere tarieven gehanteerd worden (Han, 2010) (Durkee, 2010).
- Cloud providers kunnen services onder de kosten van kleine of middelgrote data providers aanbieden en toch nog een goede winst maken (Armbrust et al., 2010).

De meeste geïnterviewden bevestigen dat cloud computing goedkoper is.

Kristof Janssens (Jordens Datacenter) (2012) stelt dat cloud computing goedkoper is voor de eindgebruiker en het een lagere investeringskost geeft.

Tom Aerts (LRM) (2012) meent dat cloud computing veel efficiënter is en dus heel wat kostenvoordelen met zich meebrengt.

Tom Palmaers (Cegeka) (2012) benadrukt dat cloud computing kostenbesparingen met zich meebrengt doordat je werkt met heel wat shared platformen. Dit kan leiden tot substantiële kostenbesparingen.

Laurens Dauwe (Stibbe) (2012) bevestigt dat kostenbesparingen een heel groot voordeel ervan zijn.

Perter Dedrij (Microsoft) (2013) haalt aan dat je het best kan bekijken naar analogie wat er gebeurt met water. Vroeger had ieder huis zijn eigen waterput en het kostte veel geld om een waterput te boren. Diegene die er zelf geen konden boren gingen lokaal in hun dorp aan de pomp water halen. Met cloud computing is eigenlijk hetzelfde verhaal aan het gebeuren. In plaats van dat iedereen zijn eigen server racks gaat installeren, zijn er bepaalde bedrijven en organisaties waaronder Microsoft deze infrastructuur gaan opzetten om die basis ter beschikking te stellen die kostefficiënter is.

Jos Ectors (Vakbeurs IT security) (2013) merkt op dat personeelskosten verminderd worden bij de cloud.

Erik R. Van Zuuren (2013) merkt echter op dat cloud services niet altijd kostenbesparend zijn doordat ze beveiligingsmaatregelen, flexibiliteit, etc. integreren. Cloud services geven meer opties, waarvoor betaald moet worden.

Mark Lens (Eurosys – IT-solutions) (2012) stelt zelfs dat cloud over het algemeen iets duurder is dan klassieke applicaties die eerst on-premise waren. Maar het geeft je grotere flexibiliteit.

Ook Raf De Backer (Ferranti) (2013) merkt op dat de cloud niet noodzakelijk altijd goedkoper is.

Flexibiliteit

- Het is makkelijker voor bedrijven om hun services te laten groeien. De services zijn immers makkelijker schaalbaar (Han, 2010). Er is minder nood aan het op voorhand plannen van capaciteit omdat het zo gemakkelijk schaalbaar is (Han, 2010) (Durkee, 2010).
- Elasticiteit is het echte gouden ei van cloud computing en maakt het concept cloud computing revolutionair (Owens, 2010).
- Er moet enkel betaald worden voor wat men gebruikt. Het zogenaamde pay-per use model (Durkee, 2010).
- Configuratie kan al op een standaard worden ingesteld zodat de desbetreffende klant zo minimaal mogelijk aan configuratiewerk moet doen (Marston et al., 2010).
- Er is de mogelijkheid om heel grote of kleine hoeveelheden data op te slaan of te verwerken (Han, 2010).
- In het geval van Amazon, zelfs als pay-as-you-go duurder zou zijn als zelf de hardware aankopen, dan nog zal het pay-as-you-go model beter zijn. Omdat het mogelijk is op een makkelijke manier nieuwe capaciteit bij te krijgen of te veel capaciteit terug te geven (Armbrust et al., 2010).

Ook dit argument wordt door de meeste geïnterviewden onderschreven.

Tom Aerts (LRM) (2012) bevestigt dat cloud computing veel meer flexibiliteit toelaat.

Tom Palmaers (Cegeka) (2012) stelt dat het belangrijkste voordeel is de makkelijke manier om dingen te schalen. Je kan heel makkelijk en snel capaciteit gaan uitbreiden waar nodig is.

Mark Lens (Eurosys – IT-solutions) (2012) benadrukt dat de cloud enorm schaalbaar is. Als je vandaag honderd mensen moet bijzetten op een mailbox dan is dat op een goed uur gebeurd. Je moet niet zelf investeren in infrastructuur. Je betaalt enkel voor het gebruik. Heb je een maand minder mensen, moet je minder betalen.

Laurens Dauwe (Stibbe) (2012) argumenteert dat vroeger al de gegevens in-house werden opgeslagen. Er was altijd een welbepaalde infrastructuurkost. Ze

hadden een server nodig. Je hebt je datalijnen naar die servers, die heb je moeten betalen. Daarnaast heb je ook maintenance, management van die servers, dat heeft ook een kostprijs. Je moet er mensen opzetten. Daarnaast moet je ook rekening houden dat op die servers software draait. Je hebt een licentiekost. Als je echter naar een cloud provider gaat die zegt gewoon dit is mijn oplossing en you just 'pay-as-you-go'. Als je bijvoorbeeld een user-based licence hebt en je hebt duizend mensen die ervan gebruik maken, dan neem je gewoon duizend user-based licences. Tijdens de economische crisis moeten er driehonderd ontslagen worden. In een traditioneel systeem betekent dat: je hebt een contract van vijf jaar voor duizend licenties. Dan moet je die duizend licenties blijven betalen. Heel veel cloud providers zeggen echter, kijk geen probleem, dan pak je gewoon nog maar zevenhonderd licenties. Dus kan je als het ware je kost flexibeler managen.

Peter Dedrij (Microsoft) (2013) bevestigt en haalt aan dat bij een public cloud de schaalvoordelen nog groter zijn. Hij haalt verder aan dat met cloud het supereenvoudig is om een nieuwe mailbox aan te maken. Dat is twee seconden werk. Het kan door een niet IT-persoon gedaan worden. Je kunt je nieuwe medewerker bij wijze van spreken binnen de tien minuten een nieuwe mailbox geven.

Raf De Backer (Ferranti) (2013) stelt dat je bij cloud computing een compleet model hebt dat schaalbaar is. Als klein bedrijf zou het kostelijk zijn om schaalbaarheid zelf te introduceren. Maar je kan als klein bedrijf wel gebruik maken van de schaalbaarheid van een grote cloud provider.

Ook Pieter Delbeke (Zentrick) (2013) benadrukt dat cloud computing een perfect schaalbare oplossing geeft. Je moet geen eigen hardware investeringen doen. Je betaalt effectief voor wat je gebruikt. In een klassiek systeem zou je na het uitvoeren van een zwaar project services hebben die voor niets staan te draaien. Bij cloud computing kunnen deze kosten vermeden worden, je betaalt enkel wat je gebruikt.

Jos Ectors (Vakbeurs IT security) (2013) bevestigt dat cloud computing schaalbaarheid aanbiedt. Hij haalt echter aan dat er bij HP ook interne systemen kunnen aangekocht worden die de schaalbaarheid kunnen nabootsen.

Toegangsvoordelen tot de markt

- De obstakels tot innovatie worden verlaagd. Het wordt immers makkelijker verschillende informatietechnologieën op een gemakkelijkere manier aan te spreken (Marston et al., 2010).
- Het is mogelijk nieuwe applicaties en services te creëren die voordien niet mogelijk waren (Marston et al., 2010). We denken hierbij aan zogenaamde Mashups waarbij de data of functionaliteit van twee externe bronnen worden gecombineerd tot een nieuwe applicatie. Een voorbeeld van een Mashup is om geografische data te combineren met data van vastgoed.

Hierdoor ontstaat een nieuwe web service die oorspronkelijk door geen van beide sources aangeboden was (Marston et al., 2010).
- Vermits verwerking en opslag in de cloud gebeurt, kunnen gebruikers met minder krachtige toestellen toch de cloud raadplegen en gebruiken. Voorbeelden van toestellen zijn: minder krachtige computers, smartphones, etc. (Cheng & Lai, 2012).

Peter Dedrij (Microsoft) (2013) bevestigt. Voor kleinere bedrijven vandaag is een infrastructuur mogelijk die vroeger enkel weggelegd was voor heel grote bedrijven.

Hoge toegankelijkheid

- De servers zijn verbonden via Internet wat toelaat dat makkelijk data via Internet verstuurd kan worden (Durkee, 2010).
- De data kan door toegang via Internet makkelijk op allerlei plaatsen geraadpleegd worden (Hastings, 2009).

Laurens Dauwe (Stibbe) (2012) bevestigt dat de hoge toegankelijkheid van de data een groot voordeel is. Vroeger moesten gebruikers via het netwerk gaan om gegevens uit een database te halen. Nu is dat heel eenvoudig. Ze loggen heel eenvoudig via hun device in. Zelfs bijvoorbeeld een Ipad. Ze checken eventjes, hebben dan de gegevens en het is gedaan. Daar is een gigantisch voordeel voor veel van die bedrijven.

Core competences

- Het bedrijf kan, door het outsourcen van de desbetreffende IT-infrastructuur, zich meer richten op zijn core competences waarin het beter is gespecialiseerd en concurrentieel voordeel kan halen. In IT is het bedrijf veelal niet gespecialiseerd (behoort niet tot de core competences), het is het best dit dan ook te outsourcen via cloud computing (Garrison et al., 2012) (Han, 2010).

Ook dit argument wordt door de meeste geïnterviewden onderschreven.

Peter Dedrij (Microsoft) (2013) meent dat bedrijven aan de hand van cloud computing zich meer kunnen concentreren op hun core business.

Raf De Backer (Ferranti) (2013) bevestigt dat doordat iemand anders zich bezig houdt met de IT-gerelateerde zaken, het bedrijf zelf zich kan bezighouden met de business kant van het verhaal.

Pieter Delbeke (Zentrick) (2013) geeft als voorbeeld dat het configureren en monitoren allemaal door Amazon gebeurt. Daar moet Zentrick zich niets van aantrekken.

Erik R. Van Zuuren (Vakbeurs IT security) (2013) benadrukt dat het bedrijf zich nu kan richten op de core competences en zich niet moet bezighouden met de IT-infrastructuur waar het veelal geen concurrentieel voordeel uit kan halen.

Jos Ectors (Vakbeurs IT security) (2013) bevestigt dat je IT moet kopen, niet produceren als je hier zelf geen conurrentieel voordeel uithaalt.

Beveiliging

- De software zal niet zonder toestemming gekopieerd worden. De software bevindt zich immers op de servers van de cloud provider en het zal dus quasi onmogelijk zijn om deze software te kopiëren (Cheng & Lai, 2012).
- Data wordt opgeslagen in datacenters die zich duizenden kilometers verder bevinden. Als deze on-premise zouden geplaatst zijn, zou niet dezelfde beveiliging kunnen gegarandeerd worden (Han, 2010).
- Wanneer lokaal gegevens verloren gaan dan kunnen deze toch nog in de cloud aanwezig zijn, dit is een grote beveiligingstroef (Hastings, 2009).

Ook dit argument wordt ondersteund.

Kristof Janssens (Jordens Datacenter) (2012) bevestigt dat cloud computing meer up-time geeft door meer beveiligingsmaatregelen.

Mark Lens (Eurosys – IT-solutions) (2012) benadrukt dat er een enorme bedrijfszekerheid is op het gebied van mail.

Peter Dedrij (Microsoft) (2013) bevestigt dat cloud computing de basis ter beschikking stelt die ook alle nodige beveiliging geeft.

Raf De Backer (Ferranti) (2013) stelt dat security een voordeel bij cloud computing kan betekenen.

Up-to-date

- De cloud provider kan er zeker van zijn dat de gebruiker altijd de meest recente versie van de software gebruikt. Namelijk diegene die gehost wordt op de server van de cloud provider (Cheng & Lai, 2012).

Profielen

- Aan de hand van gesofisticeerde data mining algoritmen kunnen profielen van gebruikers opgesteld worden en deze kunnen dan aan de hand van dit profiel gepersonaliseerde advertenties krijgen (Cheng & Lai, 2012).

De mogelijkheid van de cloud user (het bedrijf) om de services van de verkoper van cloud services te integreren en ervan gebruik te maken binnen het eigen bedrijf, maken of van cloud computing en zijn bijbehorende voordelen genoten kan worden (Garrison et al., 2012). Er zijn echter ook nog nadelen bij het gebruik van cloud computing die verder nog besproken worden.

Deze voordelen kunnen voor de specifieke cloud user (het bedrijf) een concurrentieel voordeel opleveren wanneer een cloud service op een eigen wijze gebruikt wordt. Als iedereen dezelfde cloud services gebruikt kan het lijken dat er geen concurrentieel voordeel met cloud services behaald kan worden. Nochtans zullen er nog wel degelijk verschillen blijven bestaan in de wijze waarop ze die gebruiken en kan zo een concurrentieel voordeel ontstaan (Garrison et al., 2012).

Zoals hierboven aangehaald heeft cloud computing duidelijk een aantal voordelen waardoor het interessant kan zijn om cloud computing te gaan gebruiken. Bij het gebruik van cloud computing zijn er echter ook een aantal belangrijke nadelen die niet over het hoofd mogen gezien worden.

5.2.2 Nadelen van cloud computing

De nadelen van cloud computing worden hier besproken in volgorde van belangrijkheid.

Toegang van providers tot de data

- Cloud service providers hebben toegang tot de data die op de cloud is gezet (Cheng & Lai, 2012).

Continue werking

- De cloud computing provider kan niet beloven dat de desbetreffende applicatie 100 procent van de tijd zal werken. Voor zeer kritieke applicaties kan dit onvoldoende zijn (Marston et al., 2010).
- De cloud computing provider kan failliet gaan of er gewoon mee stoppen (Han, 2010) (Armbrust et al., 2010).

Mark Lens (Eurosys – IT-solutions) (2012) merkt op dat een nadeel kan zijn dat bedrijven zomaar plots kunnen verdwijnen.

Gevaar voor lock-in

- Het gevaar bestaat dat er een zogenaamde lock-in gevormd wordt. Je zit gevangen bij één bepaalde cloud provider zonder dat je kan vragen dat je data overgedragen wordt naar een andere cloud provider (Armbrust et al., 2010). Om deze lock-in te voorkomen zijn er al diverse groepen ontwikkeld om te komen tot standaarden die het makkelijker maken om over te schakelen naar andere cloud computing providers. ISO, the International Organisation of Standardisation, en the Open Web Foundation zijn twee groepen die zich bezighouden met het opstellen van deze standaarden (Marston et al., 2010).
- Om niet onderhevig te zijn aan perfecte competitie worden cloud gebruikers veelal in langetermijnverbintenissen aan het bedrijf gehouden. Deze lock-in kan een gevaar voor de cloud gebruiker betekenen, doordat

het minder evident wordt om over te stappen naar een andere cloud provider (Durkee, 2010).

Gevaren van het Internet

- Clouds bevinden zich op het Internet. Alle gevaren (fraude, hackers) die gepaard gaan met het Internet kunnen dus optreden (Cheng & Lai, 2012).

Peter Dedrij (Microsoft) (2013) bevestigt en haalt aan dat je met een Internetdienst zit. Nadeel kan zijn dat je geen Internet hebt. We gaan ervan uit dat netwerk overal en altijd ter beschikking is. Als dat niet ter beschikking is, zit je met een probleem. Over het algemeen is de connectiviteit echter goed.

Pieter Delbeke (Zentrick) (2013) bevestigt dat een nadeel kan zijn dat je geen Internetverbinding hebt. Als alles in de cloud staat dan zit je met je vingers te draaien en kan je de desbetreffende services niet raadplegen, wanneer de Internetverbinding niet werkt.

Geen fysieke quarantaine

- Sensitieve data wordt niet meer gescheiden door fysieke quarantaine. Dit komt doordat er veel aan virtualisatie wordt gedaan (Cheng & Lai, 2012).

Kristof Janssens (Cegeka) (2012) bevestigt dit. Er is namelijk het shared gegeven. Het is één grote wolk. Als er dus een technisch incident is in die wolk dan heeft dat heel snel impact op meerdere klanten. In het verleden met de klassieke infrastructuur had iedere klant zijn eigen omgeving. Als er één omgeving met een technisch probleem zat, bleef dat beperkt tot die klant. Wanneer nu één fysieke component het begeeft, heeft dat weerslag op een heel aantal virtuele clients.

Fysieke locatie

- Het is meestal niet mogelijk om te bepalen op welke fysieke locatie de data nu precies verwerkt of opgeslagen wordt (Durkee, 2010).

Data overdracht bottlenecks

- Het overdragen van grote delen data kan op de netwerklijnen te veel data zetten om op de gewone snelheid over te dragen. Vertraging van deze lijnen is een gevolg (Han, 2010).

Kristof Janssens (Jordens Datacenter) (2012) bevestigt dit en haalt aan dat het het belangrijk is dat er een redundante lijn moet geïmplementeerd worden naar de cloud provider toe. Als er graafwerken gebeuren en de fysieke datalijn wordt beschadigd, is het belangrijk dat er tenminste nog een redundante lijn is die in werking kan treden.

Mark Lens (Eurosys – IT-solutions) (2012) bevestigt dat een groot nadeel is als de Internetlijn uitligt dan heb je ook geen beschikbaarheid. Vandaag de dag in

België is de kans dat Internetlijnen uitliggen echter zeer laag. Je hebt ook mogelijk nog een andere oplossing. Je kan gaan via een andere operator. Je kan gaan via een Proximus of Mobistar kaartje. Er zijn wel wat alternatieven voor.

Jasper Geraerts (Vakbeurs IT security) (2013) bevestigt dat een nadeel is dat er bottlenecks bij het overdragen van grote delen data naar de cloud kunnnen optreden.

Jobs zijn bedreigd

- Er zijn jobs binnen het eigen IT-departement die door de aanschaf van cloud computing bedreigd zullen worden (Marston et al., 2010) Vooral bij grote bedrijven met een reeds sterk ontwikkeld IT-departement zal de overgang naar cloud computing moeilijker zijn.

Uit deze voor- en nadelen kunnen we diverse risico's afleiden. Deze risico's moeten ingedekt worden om als bedrijf op een veilige manier van cloud computing gebruik te kunnen maken. De huidige auditnormen om cloud risico's in te dekken zijn veelal onvoldoende.

In deze masterproef zal ik een nieuw auditkader ontwikkelen die de risico's bij cloud computing benoemt en maatregelen om deze in te dekken voorstelt.

5.3 Hoofdstuk 3: Risico's van cloud computing en vertrouwensmodel

Het is evident dat particuliere gebruikers meer en meer privacy risico's en beveiligingsrisico's willen ondergaan voor eenvoud en prijs. De particulier zelf is bereid verschillende risico's te nemen. Tom Aerts (LRM) (2012) bevestigt dat mensen veel meer open staan als vroeger voor data die men in de cloud opslaat.

Bavo Vandenheuvel (Vakbeurs IT security) (Vakbeurs IT security) (2013) haalt echter aan dat het belangrijk blijft als particulier dat je controle houdt over het spoor dat je achterlaat op Internet. Alles wat je op Internet achterlaat kan immers tegen je gebruikt worden. Oplossing zou zijn om met pseudoniemen te werken. Voorbeelden hiervan zijn: Google Street view vragen om je huis wazig te maken, een online proxy te gebruiken, etc. Particulieren doen dit echter niet en zijn zo bereid meer privacy- en beveiligingsrisico's te lopen. Als er echter met gegevens van bedrijven (heel kritische gegevens) gewerkt wordt dan moet er veel meer rekening met deze mogelijke risico's worden gehouden (Mohammed, 2010). Een bedrijf zal voor zijn heel kritische data niet zomaar bereid zijn om grote risico's te nemen. Het is een heel ander verhaal als je zelf je eigen gevoelige informatie op een cloud zet dan als een bedrijf jouw informatie op een cloud zet. In het tweede geval moet er veel meer rekening gehouden worden met de risico's (Mohammed, 2010).

Kristof Janssens (Jordens Datacenter) (2012) bevestigt dat niet alle bedrijven vandaag de dag klaar zijn om cloud computing te gaan gebruiken. In grote bedrijven blijven ze vandaag de dag veelal hybride. Men kan nog niet alles op de cloud zetten vandaag de dag.

Jos Ectors (Vakbeurs IT security) (2013) stelt dat er een evolutie, maar geen revolutie naar de cloud moet gebeuren. De geschiedenis heeft immers reeds getoond dat revoluties heel wat problemen met zich meebrengen. Een voorzichtige overstap met hybride systemen is wenselijk.

Mark Lens (Eurosys – IT-solutions) (2012) bevestigt en haalt aan dat niet zomaar alles naar de cloud gebracht mag worden. Je moet goed opletten per applicatie om naar de cloud te brengen.

Raf De Backer (Ferranti) (2013) benadrukt dat bijvoorbeeld de bankensector heel wat klantengegevens lokaal hebben staan.

Pieter Delbeke (Zentrick) (2013) poneert dat alle mogelijke contracten nog steeds lokaal bewaard worden.

Erik R. Van Zuuren (Vakbeurs IT security) (2013) haalt aan dat je niet zomaar alle data in de cloud mag gooien, je moet goed opletten met gevoelige, kritische data. Deze mag niet zomaar overgebracht worden. Het is ook belangrijk om te weten wat er precies met de back-ups gebeurt.

Mark Lens (Eurosys – IT-solutions) (2012) merkt verder ook op dat bedrijven goed moeten opletten met welke partijen ze in zee gaan om de applicaties in de

cloud te gaan onderbrengen. De cloud is maar zo bedrijfszeker als het bedrijf dat erachter staat. De cloud wordt veel meer anoniem. Je weet niet meer welke mensen er achter de producten zitten. Dat is toch wel een punt waar op gelet moet worden. De risico's moeten dus goed onderzocht worden en er moet bepaald worden hoe deze risico's ingedekt worden. De normen voor het indekken van risico's van grote bedrijven zoals bv. Google zijn meestal veel groter.

Kristof Janssens (Jordens Datacenter) (2012) merkt echter op dat er bijvoorbeeld in Limburg weinig spelers zijn die een echte cloud hebben gebouwd. Een groot werkpunt van de cloud is security en stabiliteit van het systeem. Niemand in Limburg wil echt het risico lopen om een cloud te gaan opzetten. Het zijn serieuze investeringen die moeten gedaan worden. In Antwerpen heb je nog ClearMedia die met cloud computing bezig is. Maar in Limburg zijn er weinig bedrijven die ermee bezig zijn om het aan te bieden.

Laurens Dauwe (Stibbe) (2012) haalt aan: de meeste vragen die we ontvangen handelen over de risico's bij cloud computing. Hij vermeldt drie soorten risico's: privacy risico's, beveiligingsrisico's en contractrisico's. Dit is de indeling die ik gemaakt heb om de risico's in deze masterproef in te delen.

5.3.1 Indekken algemene risico's door cloud gebruiker

Management

- Allereerst moet het management een overzicht hebben over de gehele cloud (Bublitz, 2010). Het is zeer belangrijk dat bedrijven zich een begrip vormen van de cloud provider alvorens ze data aan de desbetreffende cloud service overhandigen (Bublitz, 2010). Tom Aerts (LRM) (2012) bevestigt en merkt op dat ze moeten weten dat het even safe is als een normale storage. Kristof Janssens (Jordens Datacenter) (2012) merkt op dat het meestal de managers zijn die komen en die zeggen wat ze precies nodig hebben. Dat zijn meestal de managers waarmee we rond de tafel zitten. Peter Dedrij (Microsoft) (2013) bevestigt dat het managementteam moet betrokken worden bij de discussie voor het implementeren van cloud toepassingen omdat het fundamenteel is voor het bedrijf.

- De risico's in de cloud moeten bekend zijn bij de managers (Vohradsky, 2012). Men moet contracten screenen op het bevatten van maatregelen m.b.t verschillende risico's (Bublitz, 2010). Peter Dedrij (Microsoft) (2013) bevestigt dit en haalt aan dat je goed moet kijken naar de privacy risico's. Wie heeft access tot de data, waarvoor mag het gebruikt worden.

- Het management moet weten wie de cloud aan het gebruiken is. Juiste beveiligingsmaatregelen moeten geïmplementeerd worden voor ieder mogelijk gebruik van de cloud (Vohradsky, 2012). Er moet een meeting zijn met de cloud provider om die beveiligingsstrategieën te bespreken (Gold, 2012). Raf De Backer (Ferranti) (2013) bevestigt dat het belangrijk is dat je via een active directory kan managen wie toegang krijgt.

- Het management moet het risico in de cloud monitoren. Alle cloud gebaseerde technologie moet transparante en snelle rapporten van informatierisico's garanderen. Deze moeten gegarandeerd worden door goed gedocumenteerde en gecommuniceerde monitoring (Vohradsky, 2012). Eén van de hoofdelementen van het managen van cloud providers is continue montoring. Het is belangrijk een eerste selectie te maken van de cloud provider, maar bedrijven moeten niet vergeten om de cloud provider te herevalueren op een regelmatige basis. Als een cloud provider's financiële situatie verslechtert, moet dat zo snel mogelijk geweten worden. Als er voor een audit gefaald wordt, moet dit zo snel mogelijk geweten worden (Bublitz, 2010).

- Het management moet autoriseren wat in de cloud gestoken wordt (Vohradsky, 2012). Een protocol moet worden opgestart om te controleren tot het juist behandelen van informatie binnen de organisatie en informatie die verspreid wordt buiten de organisatie (Gold, 2012). Er moet ook bepaald worden wat soort van gevoelige informatie er in de cloud gestoken mag worden (Gold, 2012). Tom Aerts (LRM) (2012) bevestigt dit en merkt op dat ieder bedrijf moet weten wat er in de cloud gestoken wordt en wat er met de gegevens gebeurt. Kristof Janssens (Jordens Datacenter) (2012) merkt op wat er in de cloud gestoken wordt dat dit de eigen verantwoordelijkheid van de klant is. Tom Palmaers (Cegeka) (2012) merkt op dat het er een beetje vanaf hangt. Er zijn een aantal klanten die heel hun infrastructuur outsourcen naar Cegeka. Voor die klanten weten we wat er in de cloud zit. Maar we hebben ook een hosting afdeling die een aantal andere IT-bedrijven als klant hebben die op zich ook data van hun klanten erop gaan zetten en daarbij weten we vaak niet wat er op die systemen zit. Laurens Dauwe (Stibbe) (2012) merkt op dat bij veel cloud providers die PaaS leveren die gaan ook wel weten welk type van data er kan ingepompt worden in hun systeem. Natuurlijk bij Amazon ECM die puur infrastructuurdiensten levert, wat er daar precies berekend wordt is hun zaak niet. Het enige wat zij zullen doen, is dat ze niet zouden aangesproken worden voor de content die geprocessed wordt op hun systeem. Ze zeggen dat je het niet mag gebruiken voor illegale doeleinden. Wat dat er concreet in hun systeem draait dat interesseert die mensen niet meer. Bij PaaS is het meer van belang om te weten wat voor soort data er binnen komt. Anders geldt het principe 'garbage in, garbage out'. Jij als klant moet ervoor zorgen dat die data in het juiste formaat bij mij binnenkomt. Bij IaaS is dat minder van belang. Peter Dedrij (Microsoft) (2013) haalt aan dat het geregeld wordt in contracten wat er in de cloud gestoken mag worden. Bij Youtube mag je bijvoorbeeld niet zomaar aanstootgevend materiaal posten. Raf De Backer (Ferranti) (2013) bevestigt dat als ze zelf van een cloud gebruik maken, het belangrijk is om te weten welke data erin wordt gestockeerd. Hij merkt echter op dat als zij

zelf cloud provider zijn het niet belangrijk is om te weten wat erin wordt gestopt. Pieter Delbeke (Zentrick) (2013) merkt op dat de eindgebruiker niet echt weet wat er nu in de cloud draait. Dit is echter niet nodig omdat er nauwelijks met gevoelige data gewerkt wordt.

Technische staf

- De nieuwste, laatste, best practices van ontwikkeling en infrastructuur van de cloud moeten steeds opgevolgd worden om de nieuwe optredende risico's in te dekken (Vohradsky, 2012).

- Er moet nagegaan worden of het cloud gebeuren overeenstemt met wetten en bepaalde policies (Vohradsky, 2012). Zo moeten cloud users via contracten een zekerheid hebben dat de contracten het toelaten de cloud provider te vervolgen bij beveiligingsissues (Bubiltz, 2010). Kristof Janssens (Jordens Datacenter) (2012) merkt op dat ze de richtlijnen en wetgevingen over de cloud uitleggen in hun contracten.

Technische staf en zakenpersoneel

- Zowel het zakenpersoneel als het technologisch personeel moet de juiste skills hebben om de cloud mogelijk te maken. Waar het niet mogelijk is deze skills intern te hebben, is het noodzakelijk deze extern te verwerven (Vohradsky, 2012). Tom Aerts (LRM) (2012) merkt op dat het technisch personeel de juiste skills moet hebben om met de cloud te kunnen handelen.

Variaties van dit model bestaan er in de verschillende modellen van cloud computing (SaaS, PaaS of IaaS) en in de verschillende implementatiewijzen (public, community, private of hybride). Een business in de cloud moet zich bewust zijn van de variaties (Vohradsky, 2012).

5.3.2 Indekken algemene risico's door cloud gebruiker en cloud provider aan de hand van vertrouwensmodel

Organisaties kunnen concurrentieel voordeel creëren door superieure relaties met cloud providers te creëren. Door het zuiver gebruiken van de technologie van cloud providers kan geen blijvend concurrentieel voordeel gehaald worden. Opgebouwde relaties zijn wel een vorm van concurrentieel voordeel. Het gerelateerd vertrouwen zal de kosten van onderhandelingen verlagen en de mogelijkheid van conflict verlagen. Een gebrek aan vertrouwen zal hogere achterdocht met zich meebrengen wat effectieve uitwisseling van informatie zal tegenwerken (Garrison et al., 2012).

Erik R. Van Zuuren (Vakbeurs IT security) (2013) bevestigt dat er een vertrouwensmodel moet opgesteld worden om de service provider te vertrouwen. Vroeger met interne systemen was dit veelal automatisch het geval dat het te vertrouwen was.

Een vertrouwensmodel waarbij er meer vertrouwen in de cloud provider kan gesteld worden is dus wenselijk, dit helpt ook om algemene risico's in te dekken. Een vertrouwensmodel helpt:

- In het zichtbaar maken van componenten die moeten vertrouwd worden of worden geacht vertrouwd te worden in de cloud (Abbadi & Martin, 2011);
- In het opstellen van diverse betrouwbare metingen die het mogelijk maken een vergelijking van de componenten te maken tussen cloud providers (Abbadi & Martin, 2011);
- Om de betrouwbaarheid van de componenten van de cloud provider in het algemeen te garanderen (Abbadi & Martin, 2011).

Met andere woorden betekent vertrouwen in de cloud, dat de cloud service zijn job doet zoals verwacht (Abbadi & Martin, 2011).

Het invoeren van vertrouwen in de cloud is één van de hoofddoelen van het door de EU gesponsorde TClouds (Trustworty clouds) project. Het maken van vertrouwensmodellen in de cloud is een complex probleem om aan te pakken, dat veel samenwerking tussen de industrie en academische wereld vereist (Abbadi & Martin, 2011) (Abbadi, 2011). Hier ga ik me richten op de vijf hoofdeigenschappen die moeten voldaan zijn om vertrouwen in de cloud te hebben.

Het vertrouwen in de cloud hangt volgens hen af van vijf eigenschappen: aanpasbaarheid, robuustheid, schaalbaarheid, beschikbaarheid en betrouwbaarheid (Abbadi & Martin, 2011) (Abbadi, 2011).

Deze vijf eigenschappen kunnen gemeten worden en zo kan het vertrouwen in de cloud gesteld worden. Afhankelijk van het gewenste service level dat gevraagd is kan de juiste cloud gekozen worden en kan men er dan vertrouwen in hebben (Abbadi, 2011).

Ik geef hier globale beschrijvingen van deze eigenschappen. Ik blijf echter bij dit vertrouwensmodel van vijf eigenschappen omdat via de vijf eigenschappen een goed globaal beeld van de cloud weergeven. Op dit vertrouwensmodel van vijf eigenschappen bouw ik verder met eigen onderzoek.

Het aanpassingsvermogen betekent dat de cloud provider efficiënt en snel reageert om de infrastructuur of applicaties aan te passen (Abbadi & Martin, 2011). Voorbeelden van veranderingen waaraan de cloud provider zich moet aanpassen: hardware falingen, veranderingen in de noden van de gebruiker, security incidenten, etc.

Robuustheid of weerstand is de mogelijkheid van het systeem om toch zijn features te behouden hoewel er subsystemen en componenten kunnen falen. Systemen met hoge weerstand hebben een design nodig die bv. gebruik maakt van redundante componenten. Verdere voorbeelden hiervan zijn: als een proces

faalt, moet het systeem redundante services opstarten die de gefaalde services ondersteunen, er moet een back-up van de data zijn (Abbadi & Martin, 2011).

Schaalbaarheid is de mogelijkheid om de resources te verhogen of te verlagen, gebaseerd op de vraag die ernaar is, zonder de prestaties te verlagen of sommige functies te doen stoppen en zonder de privacy of security noden van de gebruiker aan te tasten (Abbadi & Martin, 2011).

Beschikbaarheid van een service representeert de relatieve tijd dat een service met al zijn functies te gebruiken is (Abbadi & Martin, 2011). De beste manier om zeer hoge beschikbaarheid te hebben is het gebruiken van meerdere cloud computing providers (Armbrust et al., 2010). Een andere mogelijkheid om beschikbaarheid te garanderen is dat bij een overbelaste resource de gebruiker wordt doorverwezen naar een resource die niet overbelast is. Wanneer de overbelaste resource niet meer overbelast is, kan er weer naar deze resource verwezen worden (Abbadi & Martin, 2011).

Betrouwbaarheid refereert naar de mate van succes waarin een service functioneert, de mate waarin de service correcte resultaten levert en geen dataverlies oplevert (Abbadi & Martin, 2011). Hoge betrouwbaarheid helpt in het ondersteunen van hoge robuustheid of weerstand. Dit helpt op zijn beurt weer tot hogere beschikbaarheid (Abbadi & Martin, 2011).

Met beveiliging en privacy moet rekening gehouden worden, ze komen voor doorheen de vorige eigenschappen en vormen het punt van onderzoek voor deze masterproef (Abbadi & Martin, 2011).

Bij robuustheid moet bijvoorbeeld een nieuw geïmplementeerde resource rekening houden dat het dezelfde security en privacy noden hanteert als de initiële resource. Bij schaalbaarheid moeten bijvoorbeeld de bijkomende resources ook rekening houden dat het dezelfde security en privacy noden hanteert als de initiële resources. Bij beschikbaarheid is het bijvoorbeeld belangrijk dat er beveiligde communicatiekanalen gehanteerd worden. (Beveiliging en privacy zijn ook twee topcis die zeer veel voorkomen in de opvolgende modellen van Tclouds)

Allereerst worden de privacy risico's besproken en de methoden om deze het beste in te dekken.

5.3.2.1 Privacy risico's

Individuen hebben ten op zichte van cloud providers een nadelige positie en hebben daarom nood aan een heldere wetgeving voor protectie van informatie privacy op het Internet (Cheng & Lai, 2012).

De service provider heeft toegang tot de data en zou die data kunnen gebruiken voor verschillende doeleinden, die niet altijd zouden kunnen stroken met de wil van de cloud user (Ryan, 2011).

Het probleem van privacy risico's is in het algemeen bekend. Cloud computing vergroot dit probleem, doordat cloud services het toelaten data van veel meer instanties tegelijk te verzamelen. Dit vergroot de opportuniteiten voor misbruik van de data door de cloud provider (Ryan, 2011).

Laurens Dauwe (Stibbe) (2012) haalt aan dat privacy een heel belangrijk risico is. Als er naar de risico's gekeken wordt zijn de privacy risico's de belangrijkste volgens Laurens Dauwe (Stibbe) (2012).

Peter Dedrij (Microsoft) (2013) bevestigt dat het privacy risico een belangrijk risico is. We leggen al onze eieren in de mand van een grote wereldwijde IT-speler. Wat gaat die er mee doen. Vanuit privé-standpunt laat de thuisgebruiker al veel langer gegevens achter bij een grote wereldwijde IT-speler. Mensen die Gmail, Hotmail, Skype, etc. gebruiken. Die services zijn er al tien tot vijftien jaar. Dat zijn eigenlijk ook niet meer en niet minder dan cloud producten. Daar stelt men de vraag niet. Maar als het gaat over een bedrijfscontext stelt men zich er wel vragen bij. Je moet goed kijken naar de business plannen van de leverancier die erachter zit. Daarvan is de gebruiker zich niet altijd bewust. Alles wat je bijvoorbeeld opslaat bij Google, daarvan heeft Google het recht op data. Bij Microsoft is dat niet het geval. Microsoft komt niet aan de data. In geval van Google sta je je rechten van de data af aan Google. Je staat de rechten af aan Facebook. Je staat de rechten op je foto's af aan Flickr. De privacy policy, waar verder in de tekst nog over wordt uitgewijd, moet goed bekeken worden.

Cloud computing kan de volgende privacy risico's inhouden:

- De data worden blootgelegd waar blootlegging niet gepast is (Svantesson & Clarke, 2010). Tom Palmaers (Cegeka) (2012) bevestigt dit. Het grootste privacy risico is dat de gegevens zouden uitlekken.
  Er bestaat daarnaast de American Patriot Act. Dat houdt concreet in dat in de US Law enforcement agencies gerechtigd zijn om zichzelf toegang te verschaffen tot infrastructuur die zich in de US bevindt. Zij kunnen die gegevens opvragen. Zeker voor cloud service providers, die bewaren de gegevens van hun klanten en soms zijn dat wel heel interessante gegevens. Welbepaalde financiële data wordt gestored op servers, soms in de US. Als de US based authorities daar toegang tot krijgen kan het een serieus risico inhouden voor onze klanten. Dat is iets wat we steeds proberen te vermijden. Dat is iets wat je in de praktijk moet proberen af te dekken, contractueel (Dauwe, 2012). Het is te verwachten dat aanvragen van de overheid voor de toegang tot data opgeslagen in de cloud vermeerderen in de toekomst. De mogelijkheid dat buitenlandse overheden informatie opvragen is een risico dat niet enkel door contractuele indekkingen kan gegarandeerd worden. Het is best om alternatieven te bedenken voor data waar het een onacceptabel risico zou vormen als ze in de handen van de Amerikaanse overheid zou komen (Hoboken, Arnbrak, & Eijk, 2012). Raf De Backer (Ferranti) (2013) bevestigt het bestaan van het risico van de US Patriot Act. Alle data die

over Blackberry gaat, staan ofwel in een datacenter in de UK ofwel in een datacenter in de US. Als het in de US staat, kan de overheid hier gemakkelijk aan via de US Patriot Act.

- Wat zijn de precieze omstandigheden waaronder data geraadpleegd en gewijzigd kunnen worden (Svantesson & Clarke, 2010)? Laurens Dauwe (Stibbe) (2012) merkt op dat Google bij Google Docs en Gmail half aan het filteren waren zonder toestemming van de gebruikers en op basis daarvan aan target advertising deden. Dat is uiteraard niet toegelaten onder privacy recht. Je moet gegevens altijd verwerken voor een welbepaald doel. Als je zegt: ik doe het voor het ter beschikking stellen van cloud diensten voor jou, dan conflicteert dat met het doel voor target advertising. Bavo Vandenheuvel (Vakbeurs IT security) (Vakbeurs IT security) (2013) bevestigt dat Google aan filtering doet zonder dat de gebruikers dit echt weten. Raf De Backer (Ferranti) (2013) bevestigt dat de omstandigheden waaronder data geraadpleegd en gewijzigd kan worden een privacy risico is wat kan optreden.
- Wat is de precieze duurtijd dat de data opgeslagen blijven (Svantesson & Clarke, 2010)? Persoonlijke informatie die opgeslagen blijft nadat ze zogezegd al verwijderd zou zijn is een mogelijk risico. Raf De Backer (Ferranti) (2013) bevestigt dat het een mogelijk privacy risico is dat data te lang wordt opgeslagen terwijl die eigenlijk verwijderd zou moeten zijn.
- Wordt de klant voldoende geïnformeerd over deze privacy risico's (Svantesson & Clarke, 2010)? Dit kan gebeuren via een privacy policy.

Laurens Dauwe (Stibbe) (2012) haalt aan dat er te weinig kennis is van de klanten over de privacy risico's.

5.3.2.1.1 Indekken privacy risico's door wetgeving

Mark Lens (Eurosys – IT-solutions) (2012) haalt aan dat privacywetgeving zeker een wetgeving is waar men rekening mee moet houden.

In de US zijn er verschillende wetten die kunnen gebruikt worden bij de protectie van privacy in cyberspace. Eén punt van privacy van informatie kan onder verschillende wetten tegelijkertijd vallen. De Privacy Act van 1974 regelt het overheidsgebruik van persoonlijke informatie. Tom Palmaers (Cegeka) (2012) bevestigt het bestaan van deze wet. Laurens Dauwe (Stibbe) (2012) merkt op dat hij hiermee soms in aanraking mee komt. Hij zegt ook dat deze niet veel voorstelt. De E-Government Act vereist dat een agent van de overheid privacy impact assessments moet uit voeren om de impact van informatietechnologie op de informatie privacy te kunnen inschatten (Cheng & Lai, 2012). Tom Palmaers (Cegeka) (2012) zegt dat hij met deze wet niet bekend is, dit geldt ook voor Laurens Dauwe (Stibbe) (2012). De US-overheidsinstanties worden niet enkel door deze twee federale wetten gereguleerd, maar ook door de Health Insurance Portability and Accountability Act oftewel HIPAA van 1996. HIPAA zorgt voor de bescherming van individuele medische informatie privacy (Cheng & Lai, 2012).

Tom Palmaers (Cegeka) (2012) bevestigt het bestaan van deze wet. Laurens Dauwe (Stibbe) (2012) zegt dat hij geen ervaring heeft met deze wet.

De privacywetgeving stelt in het algemeen in de US echter niet veel voor (Dauwe, 2012). Het concept van privacy is totaal anders. In de US is privacy een goed dat te koop is. In de US trekken mensen het zich echt niet aan. Laurens Dauwe (Stibbe) (2012) merkt op dat hij een klant heeft gehad die een heel grote aanbieder van zoekdiensten is die een major privacy risico heeft gehad. Het eerste wat ze zeiden was dat privacy niet zo belangrijk was. Tot op het moment dat de privacy commissie besloot bij hen binnen te vallen in de Belgische vestiging. Er werd ook een strafklacht ingediend. In de US moet je altijd je kwartaalresultaten neerleggen. Daarin moet je echter ook opnemen dat er een strafklacht werd ingediend tegen uw onderneming. Als daarnaast ook nog het openbaar ministerie serieus moeilijk begint te doen zodat ze strafrechtelijk veroordeeld kunnen worden dan schiet iedereen wakker en is het alle hens aan dek om te zorgen dat dat privacy risico ingedekt wordt. Privacy is anders voor hun echter niet zo belangrijk. Ze gebruiken het als het hun uitkomt. Als het hun niet uitkomt dan is het een onbelangrijk risico. In Europa is privacy een grondrecht. Dat is ook gewaarborgd door artikel 8 van de Europese wet van de rechten van de mens. Dat is het artikel dat stelt dat iedereen het recht heeft op bescherming van zijn privé-leven, zijn gezinsleven en zijn correspondentie. Dat is het algemeen kader eigenlijk, grondrechtelijk gezien. Het is meer dan alleen bescherming van privacy bij het betrekken van computers. Het is ruimer. Dat is een grondrecht. Mark Lens (Eurosys – IT-solutions) (2012) bevestigt dit en haalt aan dat ze in Amerika veel minder streng zijn over de privacywetgeving dan in Europa. Tom Palmaers (Cegeka) (2012) bevestigt dit ook en zegt dat de Amerikaanse privacywetgeving eigenlijk een lachertje is. Europa heeft de striktste privacywetgeving ter wereld. Raf De Backer (Ferranti) (2013) bevestigt dat de privacywetgeving van de US niet afgestemd is met de strengere regelgeving van Europa.

Binnen Europa zijn er dan nog verschillen te zien. Je hebt de Europese richtlijn en ieder land moet die implementeren in zijn eigen privacywet. Maar er zijn landen die ervoor gekozen hebben om verder te gaan dan de Europese wetgeving. Spanje en Italië bijvoorbeeld zijn gekend om hun strenge privacywetgeving, die zijn nog strenger dan de algemene Europese richtlijn (Palmaers, 2012). Duitsland is ook veel strenger (Dauwe, 2012). De meeste wetgeving waar Cegeka mee geconfronteerd wordt is de Belgische privacywetgeving. Wat daar heel dikwijls te zien valt, is dat heel veel bedrijven er niet van op de hoogte zijn of niet goed volgen. Cegeka zelf moet klanten veelal op de hoogte brengen van de desbetreffende privacywetgeving.

Om voor Amerikaanse bedrijven een hogere privacywetgeving tegenover Europese regelgeving te garanderen bestaat er de Safe Harbor wet die stelt dat een Amerikaans cloud provider moet overeenstemmen met de EU Data Protection Directive voor hogere bescherming van de privacy. Als een

Amerikaans bedrijf dan Safe Harbor compliant kan worden verklaard aan de Europese regelgeving zullen Europese bedrijven hun gegevens in een Amerikaans bedrijf kunnen opslaan met toch de strenge Europese regelgeving (Dauwe, 2012). Tom Palmaers (Cegeka) (2012) bevestigt dit. Safe Harbor compliant is voor Europese bedrijven die hun data in Amerika verwerken een agreement dat wordt opgesteld zodat de Amerikaanse organisatie voldoet aan de Europese vereisten. Raf De Backer (Ferranti) (2013) haalt aan dat hij niet bekend is met de Safe Harbor wet.

In de EU is de belangrijkste regel van informatie privacy richtlijn 95/46/EC (Data Protection Directive). Artikel 8 van deze richtlijn stelt dat persoonlijke data die de etnische herkomst, politieke opinies, religieuze of filosofische waarden, lidmaatschap van een vakbond, gezondheid of geslacht bevat, moeten beschermd worden met slechts enkele uitzonderingen hierop (Cheng & Lai, 2012). Tom Palmaers (Cegeka) (2012) bevestigt het belang van de richtlijn 95/46 van de Europese Unie bij het reguleren van cloud providers en merkt op dat de Belgische wetgeving hierop gebaseerd is. Richtlijn 2002/58/EC over privacy en elektronische communicatie stelt dat de mededeling van een beveiligingslek noodzakelijk is voor providers van publieke elektronische communicatienetwerken en services zoals telefonieoperatoren, mobiele telefonie providers, internetproviders, en andere providers van elektronische communicatie services die aangeboden worden aan het publiek in plaats van privaat (Cheng & Lai, 2012). Laurens Dauwe (Stibbe) (2012) merkt op dat dit de e-privacy directive is. Deze is echter niet zo belangrijk als de Data Protection Directive (95/46/EC). Richtlijn 2002/58/EC: elk lek moet gerapporteerd worden aan de autoriteiten en als het een individu rechtstreeks betreft, dan moet dat individu gewaarschuwd worden. Tom Palmaers (Cegeka) bevestigt dat deze wet meespeelt bij de regulering van cloud providers. Uit deze maatregelen kunnen we opmaken dat informatie privacy beter beveiligd wordt in de EU. Hij merkt verder op dat 'The notification act' het Amerikaanse equivalent is van 2002/58/EC. Die stelt ook dat als er een lek is dat dit gemeld moet worden aan de persoon van wie gegevens bootgesteld worden. Raf De Backer (Ferranti) (2013) haalt aan dat hij niet vertrouwd is met het bestaan van de Europese richtlijn 95/46 of de Europese richtlijn 2002/58.

Pieter Delbeke (Zentrick) (2013) vermoedt dat de wetgeving niet snel genoeg kan bijbenen met de evolutie van de technologie. Er is een voorstel op komst om bovenop de algemene principes die in richtlijn 95/46/EC zijn beschreven, een update te brengen aan de digitale omgeving. Ook om de administratie te vereenvoudigen en de rechten van het individu, de verantwoordelijkheid van de controllers en de processors van persoonlijke data en de krachten van de toeziende nationale autoriteiten te versterken. Dit kan gelezen worden in de 'Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"' (2012). Dit document kreeg ik bij mijn interview van IT-advocaat Laurens Dauwe. Eén van de voorstellen die op tafel liggen is om specifieke clausules,

specifieke contractuele voorwaarden, op te leggen voor het gebruik van cloud computing. Er wordt in gezegd dat het bestaande systeem niet is opgewassen tegen nieuwe trends zoals cloud computing. Het is een poging tot. Ik durf niet zo ver te gaan dat het zal gereguleerd worden. Maar als ik eerlijk ben, denk ik wel dat er na verloop van tijd na x-aantal jaar een regulering van cloud computing zal komen (Dauwe, 2012). Omdat er te grote onduidelijkheid is. Een Belgische grootbank wil in zee gaan met Microsoft, Microsoft 365. Ze zijn privacy compliant, maar het is nergens de facto geattesteerd. Het is nooit de facto bevestigd door een privacy commissie. Meer en meer gaan cloud providers aan de privacy commissies in de verschillende landen vragen of ze privacy compliant zijn. De stap van de EU Data Protection Supervisor is een stap in de goede richting voor rechtszekerheid te bieden voor klanten die naar de cloud willen migreren.

Peter Dedrij (Microsoft) (2013) bevestigt dat Europa een heel aantal nieuwe richtlijnen aan het formuleren is om heel het data privacy gebeuren te reguleren. Hierbij begint men vooral de access te reguleren. Vroeger had men regels over waar moet de data gaan staan. Eigenlijk is de juistere vraag die men stelt, wie heeft er access tot mijn data.

Mark Lens (Eurosys – IT-solutions) (2012) haalt aan dat er een Europese wetgeving is die er aankomt specifiek voor cloud computing. Hij haalt ook aan dat we allemaal toch een beetje bevreesd zijn van wat er allemaal gedaan wordt met de data die iedereen in de cloud heeft staan. Het digitale spoor dat je achterlaat als je gaat surfen. Daar kunnen ze kenmerken aan koppelen dat het niet mooi is om te zien. Dat is toch wel even opletten.

Mark Lens (Eurosys – IT-solutions) (2012) haalt aan dat er ook als maar meer data wordt gecapteerd. Google heeft met auto's rondgereden om streetview te maken. Zo komen nu ook met een spel uit. Dan kan je live in de straten gaan spelen. Vanuit je android telefoon kun je gewoon door de kaart wandelen en dan kun je opdrachten uitvoeren. Een spel dat je live zelf aan het spelen bent. Alles wat je doet wordt opgeslagen: uw wandelpaden, etc. Heel grote bedrijven Apple, Microsoft, Google, Facebook capteren enorm veel data op dit moment. Dat daar een betere regelgeving voor komt daar is Mark Lens (Eurosys – IT-solutions) (2012) een groot voorstander voor.

In België valt de regeling van privacy onder de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten op zichte van de verwerking van persoonsgegevens. Deze wet regelt de bescherming tegen het ongeoorloofd opnemen, gebruiken en verspreiden van persoonsgegevens via databasebestanden (Lambrecht, 2000). Een eerste beperking van deze wet is dat de houder van een bestand enkel gegevens mag inzamelen en verwerken voor duidelijk omschreven wettelijke doeleinden. Ten tweede wordt er een bijzondere categorie gecreëerd van gegevens die als dusdanig persoonlijk worden beschouwd dat ze enkel mogen geregistreerd worden als zo door wetten en uitvoeringsbesluiten bepaald zijn. Ten derde moet de persoon over wie de

gegevens verzameld wordt op de hoogte worden gebracht van identiteit en adres van de houder van het bestand, de wijze waarop de betreffende gegevens zullen worden gebruikt en van zijn recht op toegang en verbetering van de gegevens. Ten slotte moet iedere geautomatiseerde verwerking aangegeven worden bij de commissie ter bescherming van de persoonlijke levenssfeer die een register bijhoudt van alle geautomatiseerde verwerkingen (Lambrecht, 2000).

Bavo Vandenheuvel (Vakbeurs IT security) (Vakbeurs IT security) (2013) haalt een paar instanties aan die bevoegd zijn voor privacy in België. Dit zijn de Privacycommissie, de FOD Economie, de BDMA, e-cops, etc.

Laurens Dauwe (Stibbe) (2012) stelt dat in de privacywet ook staat dat je de verplichting hebt de security te garanderen van persoonsgegevens.

Mark Lens (Eurosys – IT-solutions) (2012) merkt op dat men in Nederland er al een stukje verder in is in het beschermen van de privacy van de consument op het Internet. Er moet eerst toegelaten worden om cookies te accepteren vooraleer dat deze gebruikt kunnen worden. In België is men er echter ook verder mee naar het evolueren. Cookies kunnen immers een spoor achterlaten op de PC waarmee men alles kan gaan monitoren wat je op het Internet doet. Men kan alles beginnen traceren aan de hand van de cookies die je achterlaat. Gewoon zeggen dat alle cookies weg moeten, dat is ook niet mogelijk. Als je soms bepaalde log-ingegevens achterlaat wil je immers dat die automatisch opgeslagen worden. Pieter Delbeke (Zentrick) (2013) bevestigt dat Europa er mee begonnen is met te melden dat je niet zomaar cookies meer mag gebruiken om te tracken. Wat je moet doen is een notificatie tonen op je website. Aan de kant van Zentrick zouden ze niet liever zien dat ze de eindgebruikers getracked zien. Maar ze moeten hierbij opletten dat ze geen privacyregels schenden.

Op 24 oktober 1995 vaardigde het Europees Parlement de richtlijn 95/46 uit. Deze richtlijn streefde ernaar om de regels over de bescherming van persoonsgegevens gelijk te stellen in de hele Europese Unie. De richtlijn 95/46 van de EU voorziet een termijn van drie jaar binnen dewelke de lidstaten haar dienen omgezet te hebben in hun interne wetgeving. Concreet betekent dit dat de richtlijn op 25 oktober 1998 had moeten omgezet worden in de Belgische richtlijn (Lambrecht, 2000). Op de site van de Belgische Privacy Commissie (2012) kan gelezen worden dat op 11 december 1998 de Belgische privacywet werd aangepast voor overeenstemming met Europese richtlijn 95/46. De tweede wijziging die er gebeurde was nodig om de evolutie van onze geïnformatiseerde maatschappij te volgen. Met de Wet van 26 februari 2003 werden het statuut, de samenstelling en de bevoegdheden van de privacycommissie aangepast en werden de sectorale comités opgericht.

Het verschillend behandelen van informatie privacy tussen de EU en de US heeft te maken met het feit dat in US de Supreme Court nog altijd niet onderkend heeft dat informatie privacy één van de fundamentele rechten is (Cheng & Lai, 2012). In de EU is deze onderkenning wel gebeurd. Daarnaast wordt er gezegd

in EU dat de verwittiging van een beveiligingslek als een preventieve maatregel moet geregeld worden. Wat betreft de verwittiging van het verzamelen van informatie is het beter om de US maatregelen te implementeren diegene die meer flexibel zijn om de verschillende interesses in de protectie van informatie privacy te balanceren (Cheng & Lai, 2012).

De toepassing van de desbetreffende informatie privacywetgeving onder de verschillende wetgeving is dus verschillend. De uiteindelijke oplossing zal zijn dat er een internationaal verdrag hieromtrent komt (Schiller, 2011). Tom Aerts (LRM) (2012) bevestigt dit en ziet een meer uniforme wetgeving over heel de wereld evolueren. Kristof Janssens (Jordens Datacenter) (2012) denkt ook dat het meer en meer evolueert naar een internationaal verdrag. De verschillen tussen landen zijn echter nog groot. Het samenwerken van de verschillende landen zal zeker niet slecht zijn, maar of het gaat lukken dat is een andere vraag. De belangen zijn eigenlijk nog verschillend. Ook Mark Lens (Eurosys – IT-solutions) (2012) meent dat er een internationaal verdrag over komt. Hij denkt dat het niet verkeerd is dat er een nieuwere internationale wetgeving komt voor de bescherming van de privacy. Laurens Dauwe (Stibbe) (2012) merkt op dat de standaarden die in Europa gelden, waarschijnlijk zullen gelden als standaarden globaal. Omdat Europa zeer streng is. De cloud providers gaan zich in de toekomst aanpassen aan de Europese regelgeving. Raf De Backer (Ferranti) (2013) vreest echter dat de privacy wetgeving, zoals wij ze in Europa kennen, relatief strikt, wel eens afgebouwd zou kunnen worden.

5.3.2.1.2 Indekken privacy risico door privacy policy

Om de privacy risico's in te dekken met een privacy policy die normaal overeenstemt met de desbetreffende privacywetgeving, nemen we Google Docs als voorbeeld (Svantesson & Clarke, 2010).

Het is belangrijk dat er alvorens data op een andere server gezet wordt naar de privacy policy gekeken wordt (Hastings, 2009).

Wanneer er met gevoelige data gewerkt wordt, moet er via policies bepaald worden wie er toegang tot de data krijgt en hoe met die data wordt omgegaan, dit mag niet een loutere ad hoc regeling zijn. Er moet een echte policy hierover aanwezig zijn (Ryan, 2011).

Peter Dedrij (Microsoft) (2013) bevestigt en haalt aan dat of het nu gaat om een Gmail account, een Hotmail account, een CRM of Google Docs, en zo verder, je ondertekent altijd iets. Meeste bedrijven kijken niet wat hierin staat omdat het gratis is. Maar ze zouden de privacy policy beter moeten controleren alvorens ze de desbetreffende gratis service gaan gebruiken.

Pieter Delbeke (Zentrick) (2013) merkt op dat hun privacy policy is verwerkt en opgesteld door een advocaat.

Op de webpagina iCloud: overzicht van iCloud beveiliging- en –privacy (2013) staat te lezen dat Apple in heel haar bedrijf een verbintenis tot het beschermen

van uw privacy heeft. In de privacy policy staat beschreven hoe je gegevens verzameld, gebruikt, vrijgegeven, overgedragen en bewaard worden. Apple houdt zich niet alleen aan haar privacybeleid maar heeft ook iCloud-functies ontworpen rekening houdend met uw privacy: u moet 'zoek mijn iPhone, iPad en iPod touch' inschakelen in de iOS-instellingen voordat de locatie van uw apparaat kan worden bepaald, u moet zoek mijn Mac inschakelen in systeemvoorkeuren van OS X voordat de locatie van uw Mac kan worden bepaald, etc.

Google specifieert dat het de informatie voor allerhande doeleinden kan gebruiken. Het blijft echter vaag omschreven.

"We use the information we collect from all of our services **to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users**". Te lezen in de privacy policy Google 27 juli 2012

De data van consumenten kan in Google's bezit blijven zelfs nadat de consument de data gedeletet heeft. Het blijft echter vaag omschreven. Er wordt niet gespecifieerd hoe lang het maximum op de servers mag blijven.

"We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we **may not immediately delete residual copies from our active servers and may not remove information from our backup systems.**" Te lezen in de privacy policy Google 27 juli 2012

Google kan de gegevens op een server buiten het land waarin je de service gebruikt zetten. Het blijft echter vaag omschreven, je weet niet precies in welk land de data terecht zal komen.

"We **may process your personal information on a server located outside the country where you live**." Te lezen in de privacy policy Google 27 juli 2012

De analyse van Google's Privacy Policy toont dat de gebruiker slechts een gelimiteerd begrip krijgt van hoe zijn of haar persoonlijke informatie echt gebruikt wordt door Google. Dit is meestal gedreven door het commercieel perspectief, maar ondermijnt de wettige privacy rechten van de individuele gebruiker (Svantesson & Clarke, 2010). Wetten die deze privacy policy beter reguleren, moeten dus beter toegepast en geïmplementeerd worden.

Gebruikers zijn veelal niet goed op de hoogte gebracht van de privacy risico's bij cloud computing (Mohammed, 2011). De privacy policy van Google Docs is hier een bewijs van.

Tom Aerts (LRM) (2012) bevestigt dat cloud computing een vaag begrip blijft. De privacy policies zijn niet goed beschreven. Betere wetten zouden hiervoor moeten geïmplementeerd worden.

Kristof Janssens (Jordens Datacenter) (2012) haalt aan dat je heel vaak NDA's, non-disclosure agreements, tegenkomt. Hiermee wordt de privacy beschermd. Dit kan men vergelijken met een Privacy Policy. Vanaf het moment dat je iets bij

Amazon of Google zet dan is het niet meer jouw eigendom. Vanaf het moment dat iets bij Jordens datacenter staat, mag niemand in de box komen kijken.

Nu wordt er verder gegaan met het indekken van de transborder privacy risico's.

5.3.2.2 Privacy risico's bij transborder clouds

Transborder clouds hebben naast de bovenstaande privacy risico's nog volgend additioneel privacy risico (Svantesson & Clarke, 2010):

- Garanderen de wetten van het land naar waar de data getransfereerd wordt voor de desbetreffende cloud provider voldoende mate van privacy die minstens even hoog is als het land van de gebruiker (Svantesson & Clarke, 2010)?

Pieter Delbeke (Zentrick) (2013) bevestigt dat het voor een internationaal bedrijf allemaal nog iets complexer is omdat je niet alleen de privacywetgeving van België moet respecteren maar ook die van andere landen waarmee je zaken doet. De bescherming van de privacy in dit land moet minstens even hoog zijn als de bescherming van de privacy in het land van de gebruiker, zie de indekking hier verder beschreven.

Laurens Dauwe (Stibbe) (2012) merkt daarnaast op dat bepaalde landen het niet toelaten dat bijvoorbeeld hun overheidsgegevens gehost worden buiten hun eigen territorium. In Nederland is dat zo en in Duitsland is dat ook zo. Cloud providers moeten daar rekening mee houden.

5.3.2.2.1 Indekken privacy risico's bij transborder clouds

Om transborder privacy risico's voor clouds in te dekken is er de wet Artikel 25 van de EU Directive 95/46. Deze stelt dat een cloud provider enkel data mag transfereren naar een ander land, om daar verwerkt te worden, als dit land een voldoende mate van protectie van privacy kan garanderen (Svantesson & Clarke, 2010).

Als een klant in een Europees land bijvoorbeeld Google Docs zou implementeren dan zou deze klant moeten weten in welk land precies de data zou opgeslagen of verwerkt worden. Alleen wanneer het land bekend is, kan immers gecontroleerd worden of dit land voldoende protectie biedt. Zo wordt er dan voldaan aan het bovenstaande Artikel 25 (Svantesson & Clarke, 2010).

De makkelijkste oplossing blijkt om producten op de markt te brengen die geografisch op dezelfde plek geplaatst zijn. Zo moet er niet iedere keer over contracten met eventueel verschillende landen onderhandeld worden. Bij het voorbeeld van Google Docs moet het dus mogelijk zijn voor een Europees bedrijf om hun data enkel op servers binnen de Europese Unie op te slaan (Svantesson & Clarke, 2010).

Om dit artikel te vermijden hebben cloud providers zelfs de intentie om data niet onder een bepaalde wetgeving te laten vallen, maar in de plaats daarvan hun

data op zee op te slaan. Zo zullen ze onder geen enkele wetgeving vallen en dit artikel niet moeten toepassen (Svantesson & Clarke, 2010).

Amazon Web Services zorgt er steeds voor dat de lokale infrastructuur aangepast is aan het land waarin de desbetreffende wetgeving toegepast is. Gebruikers kunnen daarnaast ook kiezen in welk land ze hun data plaatsen (Marston et al., 2010).

Het is veelal moeilijk precies te weten waar de data opgeslagen wordt, omdat veelal meerdere servers in meerdere datacenters naar buiten komen als één gemeenschappelijke resource (Mohammed, 2010).

Laurens Dauwe (Stibbe) (2012) merkt op dat er ook binding corporate rules kunnen worden toegepast. Stel dat je een heel grote onderneming bent en je moet je gegevens transfereren naar je verschillende vestigingen. Het zijn vestigingen in India, in Marokko dan moet je ook het gepaste beschermingsniveau bieden en dan kan je op het niveau van de hele groep binding corporate rules opleggen. Dat betekent standaarden opleggen aan elke entiteit van de groep. Die standaarden moeten in één land in Europa ook goedgekeurd worden. In België worden die goedgekeurd door middel van een Koninklijk Besluit. Als je met verschillende entiteiten in verschillende landen werkt, dan zie je dat er op gebied van regelgeving inconsistenties zullen verschijnen. Dan heb je een probleem. Als je met verschillende entiteiten in verschillende landen werkt, dan ga je best voor binding corporate rules. Elke entiteit van de groep moet zich akkoord verklaren met die specifieke regels en dan ben je ook in één keer afgedekt. Ander alternatief is model clauses. Dit zijn standaard contractuele clausules die worden opgelegd door de Europese Commissie. Als je dat wil toepassen op je groep, dat wil zeggen dat je met elke entiteit van je groep zo een contract moet afsluiten. Dat is echter een vrij omvangrijk werk.

Naast privacy die doorheen de eigenschappen van het vertrouwensmodel voorkomt, komt ook beveiliging voor.

5.3.2.3 Beveiligingsrisico's

Laurens Dauwe (Stibbe) (2012) haalt aan dat beveiliging een heel belangrijk risico is. Hij haalt aan dat dit heel vaak wordt onderschat.

Gebruikers worden veelal niet goed op de hoogte gebracht van de verschillende mogelijke beveiligingsrisico's bij cloud computing (Mohammed, 2010).

De Cloud Security Alliance (CSA) heeft een artikel gepubliceerd waarin zes belangrijke beveiligingsrisico's in een cloud omgeving beschreven werden:

1) Onbeveiligde interfaces en APIs (insecure interfaces and APIs) (Che & Duan, 2011). Mark Lens (Eurosys – IT-solutions) merkt op dat klanten van cloud producten een browserinterface kunnen gaan gebruiken. Deze

interface kan niet goed beveiligd zijn. Raf De Backer (Ferranti) (2013) bevestigt tevens dat onbeveiligde interfaces een mogelijk beveiligingsrisico vormt.
2) Kwaadwillige indringers (malicious insiders) (Che & Duan, 2011). Tom Aerts (LRM) (2012) bevestigt dat het risicovol is dat je gehackt wordt. Tom Palmaers (Cegeka) (2012) bevestigt dat het risicovol is dat hackinggroepen de cloud hacken omdat de cloud typisch internetfacing is. Mark Lens (Eurosys – IT-solutions) bevestigt het risico van hacking. Hij haalt het geval van Sony aan dat gehackt is geweest met zijn gameconsoles. Hij merkt op dat individuele hackings veel meer gebeuren als die die in de cloud gebeuren. Omdat bij de cloud er een veel grotere security en veel grotere manpower achter zit.
3) Gemeenschappelijke technologie problemen (shared technology issues) (Che & Duan, 2011). Tom Palmaers (Cegeka) (2012) bevestigt dit. Als er een technisch incident is in de wolk dan heeft dat heel snel impact op meerdere klanten. In het verleden met de klassieke infrastructuur had iedere klant zijn eigen omgeving. Als er één omgeving met een technisch probleem zat, bleef dat beperkt tot die klant. Maar als vandaag de dag met cloud computing sommige onderliggende componenten het begeven dan heeft dat zijn weerslag op een heel aantal klanten. Als er bij de onderliggende virtuele structuur een probleem zit, zit dat probleem onmiddellijk gespreid bij een heel aantal klanten. Bij het klassieke was het top op het fysisch niveau gescheiden.
4) Dataverlies of lekken (data loss or leakages) (Che & Duan, 2011): vb. In maart 2009 ervaarde Google Docs service een datalek. Documenten die niet bedoeld waren om gedeeld te worden werden gedeeld door een fout van Google. Google schatte dat er enkel 5 procent van de documenten waren getroffen, maar dit is een groot cijfer als je het totaal aantal documenten bij Google Docs in rekening neemt (Bublitz, 2010). Laurens Dauwe (Stibbe) (2012) merkt op dat als je de security van persoonsgegevens niet voldoende gegarandeerd hebt en je hebt een data breach, dan heb je een serieus probleem. Dan heb je op strafrechtelijk niveau een probleem, omdat jij als verantwoordelijke wettelijk aansprakelijk bent. Maar je hebt ook een burgerrechtelijke aansprakelijkheid, dat betekent dat het openbaar ministerie tegen ons een claim kan indienen. De virtuele burgers, de klanten, zeggen dat hun dossier nu geweten is over heel België, die kunnen een schadeclaim indienen. Bavo Vandenheuvel (Vakbeurs IT security) (2013) haalt aan dat bij de NMBS onlangs van 1,4 miljoen reizigers hun persoonlijke data was gelekt. Dit is natuurlijk een groot probleem.
5) Account of service kaping (account or service hijacking) (Che & Duan, 2011). Dit is het risico dat een bestaand account door een malafide gebruiker kan gekaapt worden om de malafide gebruiker te bevoordelen ten kostte van de echte gebruiker of cloud provider. Pieter Delbeke (Zentrick) (2013) bevestigt dat dit een mogelijk beveiligingsrisico is. Als

hun master paswoord of hun account bij Amazon gekaapt wordt dan hebben zij een heel groot probleem natuurlijk.
6) Onbekend risicoprofiel (unknown risk profile) (Che & Duan, 2011). Het gebrek aan kennis van de beveiligingsmaatregelen van de cloud provider kan aanleiding geven tot het intekenen van services die te weinig beveiliging zouden hebben dan noodzakelijk.

Gartner, een globaal IT onderzoek en analysebedrijf, heeft tevens zes belangrijke beveiligingsrisico's samengevat:

1) Bevoorrechte gebruikerstoegang (privileged user access) (Che & Duan, 2011). Tom Aerts (LRM) (2012) bevestigt dit en merkt op dat je steeds wel een menselijke factor erbij betrokken hebt. Ik ga bijvoorbeeld op verlof en geef mijn paswoord door aan iemand anders. Maar als je het te streng gaat maken dat iedere keer dat je permissie moet vragen als je iets doet, dat werkt ook niet.
2) Voldoen aan wetten en reguleringen omtrent beveiliging (regulatory compliance) (Che & Duan, 2011). Dit kan ISO/SAS 70, Up-time institute, etc. zijn.
3) Data locatie (data location) (Che & Duan, 2011). Risico waar je data zich precies bevindt en hoe deze dan is beveiligd.
4) Data enkel beschikbaar voor desbetreffende gebruiker (data segregation). Risico bestaat erin dat een gebruiker de data van een bepaalde andere gebruiker kan raadplegen (Che & Duan, 2011) Raf De Backer (Ferranti) (2013) bevestigt dat je ook via de active directory kan gaan bepalen waar iemand aan mag en waar iemand niet aan mag. Die instellingen kan je gaan afstemmen op de cloud provider zodat je zelf controle hebt.
5) Herstellingsrisico (recovery) (Che & Duan, 2011). Tom Palmaers (Cegeka) (2012) merkt op dat er een root cause analyse zal gedaan worden. Die gaat na hoe het incident is kunnen gebeuren en dan kunnen er collectieve maatregelen genomen worden om ervoor te zorgen dat het incident of dergelijke incidenten zich in de toekomst niet meer kunnen voordoen. Risico voor herstel kan hier optreden.
6) Lange termijn effectiviteit (long-term viability) (Che & Duan, 2011). Zal de cloud provider ook op lange termijn dezelfde servicelevels of beveiliging kunnen hanteren?

Nu gaan we naar de beveiligingsrisico's kijken specifiek vanuit het standpunt van de gebruiker en cloud provider.

5.3.2.3.1 Beveiligingsrisico's bij cloud gebruikers

De beveiligingsrisico's waarmee specifiek cloud gebruikers mee geconfronteerd worden zijn:

1) Tijd dat de service niet bereikbaar is, wat niet helemaal vermeden kan worden (Che & Duan, 2011). Tom Aerts (LRM) (2012) merkt op dat het

niet bereiken van de service niet enkel kan afhangen van de service zelf, maar ook van de internetverbinding die niet goed werkt. Kristof Janssens (Jordens Datacenter) (2012) bevestigt dit en haalt aan dat het belangrijk is dat er een redundante lijn moet geïmplementeerd worden naar de cloud provider toe. Als er graafwerken gebeuren en de lijn wordt beschadigd, dat er tenminste nog een redundante lijn is die in werking kan treden. Peter Dedrij (Microsoft) (2013) bevestigt en haalt aan dat het kan zijn dat je geen netwerkverbinding met het Internet hebt. Over het algemeen is de connectiviteit echter zeer goed. Maar je hoort inderdaad wel eens problemen. Telenet is recent voor een tijdje uitgevallen (3 februari 2013). Pieter Delbeke (Zentrick) (2013) bevestigt dat een nadeel kan zijn dat je geen Internetverbinding hebt. Als alles in de cloud staat dan zit je met je vingers te draaien en kan je de desbetreffende services niet raadplegen, wanneer de Internetverbinding niet werkt. Erik R. Van Zuuren (Vakbeurs IT security) (2013) bevestigt dat het belangrijk is dat er redundante lijnen zijn zodat er steeds van de service genoten kan worden als bepaalde lijnen uitliggen.

2) Mogelijke lekken van commerciële geheimen (Che & Duan, 2011). Dit is een beveiligingsrisico wat ook door de privacywetgeving gedwongen wordt om in te dekken.
3) Hoe handelen met de geprivileerde status van de cloud service provider (Che & Duan, 2011). Dit is een beveiligingsrisico wat ook door de privacywetgeving gedwongen wordt om in te dekken.

5.3.2.3.2 Beveiligingsrisico's bij cloud providers

De beveiligingsrisico's waarmee specifiek cloud providers mee geconfronteerd worden zijn:

1) Hoe de werking op lange termijn van de cloud garanderen en fouten bij die werking te minimaliseren (Che & Duan, 2011).
2) Hoe te vechten tegen een talrijk en agressief netwerk van hackers (Che & Duan, 2011). Hoe te vechten tegen denial of service/distributed denial of service aanvallen, waarbij een netwerk aan geïnfecteerde computers de cloud provider opvragen en door vele aanvragen de cloud provider offline krijgen (Owens, 2009). Tom Aerts (LRM) (2012) bevestigt dat het risicovol is dat je gehackt wordt. Pieter Delbeke (Zentrick) (2013) bevestigt bij een man-in-the-middle attack het verkeer van een bepaalde gebruiker kan worden afgetapt tot de cloud provider en zo wordt onbeveiligde informatie vrijgegeven. Een typische man-in-the-middle is dat ze ertussen zitten en een ander bedrag en rekeningnummer invullen.
3) De reputatie van de cloud provider kan in gevaar zijn als zijn cloud service voor illegale doeleinden gebruikt wordt (Armbrust et al., 2010).

5.3.2.3.3 Indekken van beveiligingsrisico's

Nu volgen enkele indekkingen van beveiligingsrisico's:

1) Cloud providers zouden voor gebruikers management en onderhoud van de cloud meer transparant en makkelijker moeten maken. Dit houdt in dat er logs moeten opgeslagen worden en deze logs voor gebruikers toegankelijk te maken. Het monitoren van de logs door de gebruiker kan bijvoorbeeld door middel van een online interface (Adesanya, 2012). Erik R. Van Zuuren (Vakbeurs IT security) (2013) bevestigt dat het belangrijk is om te vragen naar logs om die te kunnen inspecteren.
2) Zwakke toegangsbeveiliging vormt een mogelijk risico omdat hoog sensitieve informatie vandaag de dag meestal enkel maar een simpel paswoord vereisen. Andere contextuele informatie zoals de locatie van de gebruiker worden meestal niet in rekening gehouden. Sterkere paswoorden dienen geïmplementeerd te worden (Adesanya, 2012). Op de website iCloud: overzicht van iCloud- beveiliging en –privacy (2013) valt te lezen dat wanneer u een Apple ID aanmaakt voor het gebruik van ICloud, uw wachtwoord minstens 8 tekens, een cijfer, een hoofdletter en een kleine letter bevatten. Een sterk wachtwoord gebruiken is het belangrijkste wat u kunt doen om uw gegevens veilig te houden. Erik R. Van Zuuren (Vakbeurs IT security) (2013) haalt aan dat er gebruik kan worden gemaakt van de elektronische identiteitskaart om een strengere toegangscontrole te vormen. Om bijvoorbeeld tax-on-web te raadplegen wordt gebruik gemaakt van de strenge controle met eID's.
3) Ineffectief management van geprivileerde gebruikers vormt een volgend mogelijk risico. Het delen van administratorpaswoorden dat te snel gebeurt, kan voor ongepaste toegang zorgen in de cloud. Niet te snel delen van adminstratorpaswoorden is een must (Adesanya, 2012). Tom Aerts (LRM) (2012) bevestigt dit en merkt op dat je steeds wel een menselijke factor erbij betrokken hebt. Ik ga bijvoorbeeld op verlof en geef mijn paswoord door aan iemand anders. Maar als je het te streng gaat maken dat iedere keer dat je permissie moet vragen als je iets doet, dat werkt ook niet. Tom Palmaers (Cegeka) (2012) merkt op dat er wordt gewerkt met toegangssystemen. Binnen Cegeka krijg je enkel toegang tot die systemen die nodig zijn om je job te kunnen uitoefenen. Het is niet dat heel het bedrijf aan de gegevens kan. In het verleden was het ook zo dat wachtwoorden per klantenteams beheerd worden. Dit willen ze nu centraal gaan aanpakken om de nodige controle te zetten op generieke administratoraccounts. Dit is een voorbeeld van een goed mogelijk management van een aanmeldsysteem voor een cloud service.
4) Informatiebeveiliging bestaat uit het beveiligen van de echte inhoud van een informatiemedium en het controleren van de toegang tot dit medium (Ros, 2012).
    a. Het eerste kan beveiligd worden door encryptie en andere manieren om ervoor te zorgen dat de informatie niet kan gelezen, gewijzigd of vernietigd kan worden (Ryan, 2010). Encryptie kan wel een moeilijk

en kostelijk proces betekenen, hierover moet gewaakt worden (Anthes, 2010). Tom Aerts (LRM) (2012) bevestigt dit en merkt op dat bij encryptie nog altijd een aantal obstakels mee betrokken zijn. In de toekomst zou dit meer en meer mogelijk worden. Kristof Janssens (Jordens Datacenter) (2012) merkt op dat er standaard encryptie op de storage staat. Tom Palmaers (Cegeka) (2012) zegt dat er encryptie zowel is op netwerkniveau (transportniveau) als op storageniveau (opslag van gegevens). Mark Lens (Eurosys – IT-solutions) (2012) merkt op dat de verbindingen gebeuren aan de hand van de geëncrypteerde standaard https. Er wordt ook gebruik gemaakt van een VPN-verbinding voor een punt tot punt verbinding waarmee de applicaties kunnen geraadpleegd worden. Een VPN-tunnel is geëncrypteerd. Raf De Backer (Ferranti) (2013) bevestigt dat ze VPN-verbindingen gebruiken om data over het Internet te versturen. Pieter Delbeke (Zentrick) (2013) bevestigt dat hun paswoorden zwaar geëncrypteerd zijn. Op de webpagina iCloud: overzicht van iCloud beveiliging- en –privacy (2013) staat te lezen dat iCloud je gegevens beveiligt door deze te coderen bij het verzenden via Internet, deze in de server te bewaken in een gecodeerde structuur en veilige tokens gebruikt voor identiteitscontrole. Dit betekent dat je gegevens beveiligd zijn tegen onbevoegde toegang wanneer ze worden overgezet naar uw apparaten en wanneer ze worden bewaard in de cloud. ICloud gebruikt een AES-codering van minstens 128 bits (hetzelfde veiligheidsniveau als bij de grootste financiële instellingen) en biedt nooit coderingssleutels aan derde partijen.

b. Ten tweede moet toegangsbeveiliging strikt zijn maar in geval van noodgevallen kan er meer toegang aan die bepaalde personen gegeven worden (Ros, 2012). Het is beter om voor het veranderen van verschillende rollen op voorhand na te denken dan in het midden van de chaos (Ros, 2012). Laurens Dauwe (Stibbe) (2012) bevestigt dat het belangrijk is hoe de toegang tot de gegevens gebeurt. Mark Lens (Eurosys – IT-solutions) (2012) merkt op dat er gebruik wordt gemaakt van tokens. Tokens zijn een reeks cijfers of karakters die niet zomaar te verzinnen zijn. Deze kunnen gegenereerd worden via een apparaatje. Iemand die in het bezit is van een token kan het dus niet verzonnen hebben en bewijst daarmee de geldige toegang te hebben. Het hoogste niveau is het afschermen met tokens. Op de webpagina iCloud: overzicht van iCloud beveiliging- en –privacy (2013) staat te lezen dat wanneer je iCloud-voorzieningen gebruikt via ingebouwde apps van Apple, gebeurt de identiteitscontrole met een veilige token.

De verschillende belangrijkste lagen van een cloud zijn reeds besproken (IaaS, PaaS, SaaS), nu worden de beveiligingsrisico’s in de verschillende lagen besproken.

5.3.2.3.4 Indekken beveiligingsrisico's in de verschillende lagen

IaaS is de laagste laag en hier zijn slechts minimale beveiligingsmaatregelen door de cloud provider, enkel om de infrastructuur zelf te beveiligen. PaaS geeft een platform waar de desbetreffende gebruiker zelf zijn applicaties op kan maken. Hier zijn al meer beveiligingsmaatregelen, maar deze zijn niet compleet. Gebruikers hebben zelf nog de mogelijkheid tot implementeren van additionele beveiliging. Bij SaaS daarentegen is de gehele beveiliging overgelaten aan de cloud provider en heeft de gebruiker geen inspraak (Che & Duan, 2011).

Tom Aerts (LRM) (2012) bevestigt dit en merkt verder op dat er ook verschillende prijzen zijn om het in te dekken.

Kristof Janssens (Jordens Datacenter) (2012) bevestigt dat er een verschillend beveiligingsrisico is per laag.

Tom Palmaers (Cegeka) (2012) merkt op dat in het contract naar de klant altijd duidelijk gesteld is wie welke verantwoordelijkheid heeft. Als bijvoorbeeld bij een applicatie het beheer daarvan bij de verantwoordelijkheid van de klant ligt dan ligt het beveiligingsstuk ook bij de klant.

Laurens Dauwe (Stibbe) (2012) bevestigt dit en merkt op dat als je infrastructuur aanbiedt, dan is de verantwoordelijkheid van aanbieder enkel beperkt tot de infrastructuur. Dat betekent dus als je IaaS aanbiedt, dan moet je zorgen voor quasi enkel fysieke beveiligingsmaatregelen. Je gaat access controles in je datacenter implementeren, bijvoorbeeld badging. Alleen maar specifieke mensen mogen bijvoorbeeld toegang hebben tot je servers. Je gaat geen vulnerability assessments of penetration tests moeten doen op puur IaaS. Dat zijn zaken die je eigenlijk meer op applicatief niveau doet. Hoe hoger je in de lagen gaat, hoe zwaarder de beveiligingsvereisten worden, ook in juridisch niveau is hier een onderscheid.

Om beveiligingsrisico's in te dekken zijn er verschillende strategieën die gebruikt kunnen worden om deze in te dekken bij de opbouw en operationele werking (Che & Duan, 2011).

5.3.2.3.5 Indekken van beveiligingsrisico's bij de opbouw

Allereerst zijn er de zogenaamde strategieën bij de opbouw (Che & Duan, 2011):

1) De traditionele beveiligingsmechanismen (protectie van fysieke faciliteiten) (Che & Duan, 2011). Er moet een tweede back-up center zijn (Hastings, 2009). Tom Aerts (2012) bevestigt dit en zegt dat data moet gebackupt zijn op een locatie die verder als 20 of 30 km ligt, zodat je de back-ups altijd ter beschikking hebt. Zodat als er morgen een bom valt op je datacenter, dat je altijd je gegevens ter beschikking hebt. Kristof Janssens (Datacenter Jordens) (2012) haalt aan dat het datacenter een tier 3 niveau van beveiliging heeft. Dit is hoog naar Belgische normen. Ze hebben redundante stroomaansluitingen, telefonie daar zijn acht aansluitingen voor, overal zijn camera's aangebracht, toegangscontrole

wordt beheerd door een badgesysteem (alle bewegingen van alle personen worden geregistreerd), etc. Deze tier-normen zijn Amerikaanse normen. De Europese gemeenschap is echter ook bezig met het opstellen van nieuwe regels, die gaan later nog in werking treden. Er wordt vandaag gesproken over het Amerikaanse uptime instituut: tier 1, 2, 3 en 4. Europees is er nog geen dergelijk instituut. Tom Palmaers (Cegeka) (2012) bevestigt dat ze met twee datacenters werken. Ze hebben één datacenter in Hasselt en één datacenter in Leuven. Als er een zwaar incident gebeurt op een component in Hasselt dan kunnen de systemen in Leuven het overnemen. Mark Lens (Eurosys – IT-solutions) (2012) bevestigt dat het datacenter in Brussel camerabewaking heeft. De zuurstof in de rekken wordt enorm verlaagd als er brand zou zijn zodat het zo weinig mogelijk zou kunnen uitdijnen. Er wordt op een speciale manier geblust zodat de apparatuur geen schade loopt. Er is ontdubbeling van de airco, ontdubbeling van de stroom. Als de stroom volledig uitvalt, kan het datacenter toch nog verder gaan op batterijen (UPS). Peter Dedrij (Microsoft) (2013) bevestigt dat ze multiple sites en meerdere connecties hebben. De fysische beveiliging van het datacenter is een vak apart. Het Microsoft datacenter in Dublin, dat is bijna alsof je bij NATO naar binnengaat qua beveiliging. Er mogen niet meer dan zoveel personen tegelijk binnen, je moet doorgeven op voorhand wie er binnenkomt, wat is de bedoeling van het bezoek. Er zijn heel strenge beveiligingsnormen. Maar dat moet ook wel anders kom je in de problemen terecht. Raf De Backer (Ferranti) (2013) bevestigt dat ze drie of vier datacenters hebben waarvan ze gebruik maken (multiple sites). Er wordt gebruik gemaakt van datacenters van Colt die voldoen aan de tier 4 norm. Pieter Delbeke (Zentrick) (2013) bevestigt dat in het datacenter dat ze gebruiken (van Amazon) niemand binnen kan in het datacenter en dat dat goed beveiligd is. Jasper Geraerts (Vakbeurs IT security) (2013) haalt aan dat er gedeeltelijke replica's met Arcserve gemaakt kunnen worden zodat er twee sites zijn, en er dus dubbele opslag is, wat veiliger is. Mark De Vriendt (2013) van het high density belgacom datacenter, waar ik een bezoek aan gebracht heb, haalde ook verschillende fysieke beveiligingsmaatregelen aan die toegepast worden in hun nieuwe high density datacenter te Brussel. Er wordt aan badging gedaan om bepaalde kamers binnen te kunnen geraken. Er is camerabewaking. De stroom wordt gegarandeerd met een redundante dieselmotor (UPS) die ervoor zorgt dat als de stroom uitvalt het probleem na max. 3,5 seconde is opgelost. De koeling is dubbel uitgevoerd. Er is een cijferslot op de racks waar de servers inzitten. Het datacenter heeft een tier 3+ niveau van beveiliging. Dit betekent dat het datacenter een betrouwbaarheid van 99,99 % garandeert. Bij tier 3+ gaat het over de fysieke beveiligingsmaatregelen. Het voldoet ook aan de tia 942 norm. Dit is een internationale norm uitgegeven door een Amerikaanse instelling, de Telecommunications Infrastructure Association. Om de 4 jaar wordt hier een test op gedaan. Hier gaat het ook over de

fysieke beveiligingsmaatregelen van het datacenter. Als er brand is dan wordt er inert gas onder hoge druk in de serverroom gespoten om het zuurstofgehalte te verlagen zodat de brand stopt. Mogelijke personen in de serverroom worden dan gewaarschuwd via allerlei signalen om zo snel mogelijk zich uit de serverroom te begeven waar het zuurstofgehalte zich aan het verlagen is. De bewaking van het datacenter gebeurt door een erkende beveiligingsfirma (Securitas) die 24/24 7/7 aanwezig zijn. Er is ook 30 man continu aanwezig om het datacenter te beheren. Er zijn ook branddeuren die brand afweren indien er brand zou uitbreken. Er zijn drukknoppen om branden te melden. Er is ook inbraakdetectie.

2) Beoordeling van de veiligheid bij het gebruik van opbouw van virtualisatie (Che & Duan, 2011). Er is immers al gemeld dat het mogelijk was dat iemand van één virtuele client op een andere virtuele client kon overstappen die gemanaged werden door dezelfde onderliggende hypervisor (het programma dat de verschillende virtuele machines beheert) (Owens, 2010). Het implementeren van voldoende scheiding tussen de verschillende virtuele clients is een noodzaak (Owens, 2010). Mark Lens (Eurosys – IT-solutions) haalt aan dat ze de virtualisatie gaan testen.
3) Er kan omwille van diverse redenen (kosten, service die stopt, etc.) van cloud provider veranderd worden. Er moet rekening mee gehouden worden dat de gegevens overgedragen kunnen worden. Met dit risico moet rekening gehouden worden alvorens een cloud provider gekozen wordt (Armbrust et al., 2010). Een oplossing hiervoor kan zijn om standaard API's te gebruiken zodat data makkelijk naar andere cloud provider overgebracht kan worden (Armbrust et al., 2010). Dit zal niet zozeer een race introduceren naar de goedkoopste omdat, vandaag de dag, met cloud 2.0 er ook veel aandacht gaat naar de kwaliteit van de service (Armbrust et al., 2010). Kristof Janssens (Jordens Datacenter) (2012) bevestigt dat ze er heel flexibel in zijn. Data kan heel makkelijk overgebracht worden naar het Jordens Datacenter of data kan heel makkelijk overgebracht worden naar een ander datacenter. Er is een heel flexibele manier van werken. Tom Palmaers (Cegeka) (2012) bevestigt dat ze er heel flexibel in zijn. Bedrijven zetten hun data bij Cegeka en er worden altijd in contracten clausules afgesproken dat wanneer zij hun contract stopzetten dat ze hun data op een gemakkelijke manier terugkrijgen. Mark Lens (Eurosys – IT-solutions) (2012) haalt aan dat het kunnen overdragen van gegevens puur van de applicatie afhangt. Als je mail hebt van Google dan kan je je mailbox exporteren en inlezen in een andere applicatie. Salesforce is ook een heel gekende cloud applicatie. Daar kan je ook de zaken exporteren en inlezen. Laurens Dauwe (Stibbe) (2012) bevestigt dat er een goede regeling noodzakelijk is voor wat er gebeurt op het einde van het contract. Namelijk als je gegevens in de cloud zet dat je gegevens op het einde van het contract ook deftig teruggegeven worden, zodat je kan migreren naar een andere provider. Dat is altijd heel belangrijk, maar

wordt heel vaak over het hoofd gezien. Peter Dedrij (Microsoft) (2013) stelt dat er contracten zijn, die regelen hoe 'lock-in' vermeden kan worden en gegevens makkelijk overgedragen kunnen worden naar een andere cloud provider. In principe zijn cloud diensten generiek. Pieter Delbeke (Zentrick) (2013) bevestigt dat bij elke beslissing die ze in de architectuur nemen ook rekening mee gehouden wordt dat de applicaties ook moeten kunnen werken op een ander platform. De lagen die specifiek zijn voor Amazon die zijn mooi geabstraheerd en als zij ooit beslissen om naar een andere cloud provider te gaan, dan kan het platform binnen de paar dagen op een ander systeem draaien. Erik R. Van Zuuren (Vakbeurs IT security) (2013) bevestigt ten slotte ook dat een zogenaamde lock-in vermeden moet worden.

Nu de strategieën bij de opbouw zijn besproken, wordt er verdergegaan bij de strategieën bij de operationele werking om beveiligingsrisico's in te dekken.

5.3.2.3.6 Indekken van beveiligingsrisico's bij de operationele werking

Vervolgens zijn er de zogenaamde strategieën bij de gewone operationele werking:

1) Verzekeren van de business continuïteit. Regelmatige inspectie van de cloud provider van zijn cloud infrastructuur is hier een must (Che & Duan, 2011). Gijsbert Wiesenekker (Vakbeurs IT security) (2013) haalt aan dat via Nimsoft gemakkelijk aan infrastructuur monitoring gedaan kan worden. Via een functioneel dashboard kan dan informatie over de status van de infrastructuur opgevraagd worden. Tom Palmaers (Cegeka) 2012 bevestigt dat er aan een soort vulnerability management gebeurt waarmee op regelmatige basis systemen en vooral de systemen die aan het Internet gekoppeld zijn, controleren of daar veiligheidslekken in aanwezig zijn. Laurens Dauwe (Stibbe) (2012) haalt aan dat er meestal additionele penetration tests of vulnerability assessments gedaan moeten worden. Erik R. Van Zuuren (Vakbeurs IT security) (2013) haalt ook aan dat er gebruik moet gemaakt worden van ethische hackers die testen of het systeem nog goed beveiligd is.
2) Een cloud is een zeer groot netwerksysteem dat zeer kwetsbaar is voor aanvallen. Een systeem waarbij indringers snel ontdekt kunnen worden, moet geïmplementeerd worden (Che & Duan, 2011). Kristof Janssens (Jordens Datacenter) (2012) haalt aan dat ze werken met een redundant firewall. Eens dat het datacenter contact heeft met het Internet dan is deze ingesteld. Hierop gebeurt monitoring waar het verkeer doorgaat. Er gebeurt antivirusfiltering, spamfiltering alvorens de data nog maar aan de switchen kan. Tom Palmaers (Cegeka) (2012) merkt op dat er monitoring aanwezig is om de mensen die toegang hebben ook voor controles te zetten dat hun toegang niet misbruikt wordt. Mark Lens (Eurosys – IT-solutions) merkt op dat ze firewalls gebruiken.

3) Wanneer zich een beveiligingsincident heeft voorgedaan, moeten allereerst de gebruikers op de hoogte gebracht worden. Verder moeten cloud service providers een noodplan (disaster recovery, cloud service backup, etc.) opstarten, alvorens te reageren op het desbetreffende beveiligingsincident (Che & Duan, 2011). Tom Aerts (2012) merkt op dat meestal de gebruiker als eerste erachter komt dat er een incident gebeurd is. Kristof Janssens (Jordens Datacenter) (2012) bevestigt dit en zegt dat als er een inbraak wordt vastgesteld dan wordt de alarmcentrale verwittigd, die geeft het door aan de politie en de brandweer. Sommige medewerkers krijgen een alarm. Is er een probleem met de koeling of stroom dan krijgen sommige medewerkers een alarm. Vanaf het moment dat er iets afwijkt van het normale krijgen sommige medewerkers en de alarmcentrale een bericht. Tom Palmaers (Cegeka) (2012) merkt op dat ze een security incident process hebben. Als er een incident gemeld wordt dan triggert dat eigenlijk een heel proces. Er wordt gekeken hoe het incident verholpen kan worden. Peter Dedrij (Microsoft) (2013) bevestigt dat ze een disaster-recovery scenario hebben.
4) Om te voorkomen dat hetzelfde beveiligingsincident nog eens zou kunnen voorkomen, is het noodzakelijk te achterhalen welke de redenen van het beveiligingsincident waren. Auditing kan hierbij helpen bij het onderzoeken naar de echte oorzaken (Che & Duan, 2011). Er moet een overeenkomst zijn en verplichtingen om beveiligingsincidenten aan het licht te brengen (Gold, 2012). Tom Palmaers (Cegeka) (2012) merkt op dat er een root cause analyse zal gedaan worden die nagaat hoe het incident is kunnen gebeuren en dan kunnen er collectieve maatregelen genomen worden om ervoor te zorgen dat het incident of dergelijke incidenten zich in de toekomst niet meer kunnen voordoen.
5) Bottlenecks bij het overdragen van grote hoeveelheden data moeten vermeden worden. Dit kan vermeden worden door het overbrengen van disks waarop de data staat. Jim Gray vond dat de goedkoopste manier om een grote hoeveelheid data te versturen het overbrengen van disks of zelfs gehele computers was. Vooral bij grote zoals grote belangrijke datasets, kan dit belangrijk zijn (Armbrust et al., 2010).

Raf De Backer (Ferranti) (2013) merkt echter op dat de beveiligingsindekkingen op technisch vlak heel dikwijls sterk afgedekt zijn. Firewalls, intrusion prevention systems, stukken virtualiseren. Er is echter nog steeds een menselijke factor die meestal voor tachtig procent van de beveiligingslekken voorstelt. Voorbeeld: de werknemer die werkt in een data centre, heeft nog altijd een USB-stickje bij en die heeft dat toevallig mee en die is niet encrypted en de geheimen komen op straat terecht.

De eigenschappen van het vertrouwensmodel moeten goed geregeld zijn middels contractuele voorwaarden. Dit brengt ons tot het consumentenrisico bij het opstellen van het contract.

5.3.2.4 Consumentenrisico's bij het opstellen van het contract

De consument die een bepaald cloud computing product gaat gebruiken moet bekend zijn met de diverse consumentrisico's. Het is belangrijk dat er geen onevenwicht bij het opstellen van het contract is en er niet ingetekend wordt voor dingen waar men niet mee bekend is (Svantesson & Clarke, 2010). Volgens Bublitz (2010) gebeurt het wel eens dat cloud providers in contracten bevoordeeld worden ten nadele van cloud gebruikers.

Laurens Dauwe (Stibbe) (2012) bevestigt dat veel cloud computing contracten eigenlijk niet zijn opgesteld zoals ze zouden moeten opgesteld zijn. Salesforce bijvoorbeeld hebben hun eigen contractuele voorwaarden die stipuleren dat enkel de wetgeving van de UK van toepassing is. Maar als je als consument moet gaan procederen in de UK, het gaat je heel veel geld kosten. In de praktijk is dat al een drempel om niet te gaan procederen. Anderzijds zie je dat er liability, aansprakelijkheidsclausules instaan. Waarbij de aansprakelijkheid wordt beperkt tot drie maanden servicing fees. Als dat drie maanden servicing fees zijn en je moet bijvoorbeeld tachtig euro per maand betalen. Dat is 240 euro voor damages voor schade als je al je gegevens kwijt bent. Als je als kleine zelfstandige je volledige boekhouding kwijt bent, dat kost wel veel meer dan die schamele 240 euro. Dan is er de mogelijkheid dat je zelf gaat onderhandelen. Maar je moet realistisch zijn. Ten op zichte van grotere spelers is het moeilijk tegen te vechten.

5.3.2.4.1 Indekken consumentenrisico's bij het opstellen van het contract

Zoals quasi ieder consumentenproduct op het Internet wordt het aanbod van consumenten cloud producten normaal enkel beheerd aan de hand van contracten die exclusief door de cloud providers, zonder input van de users, worden opgesteld (toetredingscontracten). Cloud providers hebben de intentie om zichzelf te bevoordelen hierin om bijvoorbeeld verplicht te mogen filteren, target advertising te doen. Cloud gebruikers worden zo meestal benadeeld doordat dit niet duidelijk in contracten goed wordt vermeld. Cloud gebruikers gaan veelal onwetend akkoord met benadelende voorwaarden. Om echter een gebalanceerde rechtvaardigheid te handhaven tussen de provider en de user hanteert de wet enkele beperkingen op dergelijke contracten (Svantesson & Clarke, 2010). Voorbeelden van dergelijke beperkingen zijn: verplichte informatie over het product en/of provider, omstandigheden van het vormen van het contract, etc.

Peter Dedrij (Microsoft) (2013) bevestigt en stelt dat in een cloud gebeuren het meestal te nemen of te laten is. Er wordt dikwijls gewerkt met standaardcontracten. Het is niet zo dat je kan gaan vragen om een specifiek lijntje in het contract aan te passen. Als je spreekt over public cloud kan over dat lijntje niet onderhandeld worden. Je kan wel leveranciers met elkaar gaan vergelijken, maar binnen één leverancier is het moeilijk voorwaarden te veranderen. Bijvoorbeeld als je water afneemt van een waterleverancier (bijvoorbeeld 'de Watergroep'), dan kan je niet met de desbetreffende

leverancier gaan onderhandelen met verschillende lijnen in het contract. Je kan bepaalde dingen wel veranderen, maar niet oneindig. Als je oneindig wil gaan veranderen, dan moet je overstappen op private cloud.

Een consument wordt geacht bekend te zijn met het specifieke cloud product. Wanneer we echter als voorbeeld weer Google Docs stellen, stellen we vast dat het vrij moeilijk is om van heel het product op de hoogte te komen. Alle documenten samen zijn zo een 7 pagina's lang en bevatten daarnaast nog linken naar ander bijkomende contractuele documenten. Zeer weinig consumenten zullen dus de nodige tijd vrijmaken om op de hoogte te komen van heel het product (Svantesson & Clarke, 2010).

Bavo Vandenheuvel (Vakbeurs IT security) (Vakbeurs IT security) (2013) bevestigt dat mensen veelal niet van het volledige contract op de hoogte zijn en veelal onwetend instemmen.

Na het nader onderzoeken van deze diverse documenten kwamen Svantesson & Clarke tot enkele interessante conclusies. Een eerste conclusie is dat een consument niet alleen akkoord moet gaan met specifieke termen die enkel en alleen bepaald zijn door Google, maar dat deze zonder waarschuwing door Google veranderd kunnen worden. Google mag m.a.w. zonder waarschuwing zijn services veranderen of stopzetten (Svantesson & Clarke, 2010). Wanneer een gebruiker de services van Google gebruikt, wordt dit al gezien als een aanvaarding van de termen in heel het contract. Daarnaast kan de consument de toegang tot zijn account verboden worden. Consumenten zijn niet toegelaten om hun services te gebruiken als ze niet tot een legale leeftijd behoren om een contract met Google af te sluiten. Google heeft daarnaast het recht om advertenties te tonen, gebaseerd op de informatie die bij hun services gestockeerd zijn (Svantesson & Clarke, 2010).

Het is duidelijk dat gebruikers van Google Docs, veelal onwetend, akkoord gaan met een reeks voorwaarden die grote gevolgen hebben (Svantesson & Clarke, 2010). Wanneer ik zelf voor de eerste keer Google Docs ging gebruiken moest ik enkel inloggen met mijn Gmail e-mailadres. Na het inloggen kon ik onmiddellijk de service gebruiken zonder dat ik nog bijkomende schermen met voorwaarden kreeg. Om helemaal op de hoogte van het product te komen moet men echter door veel webpagina's klikken. Veel gebruikers doen deze moeite niet en gaan veelal onwetend akkoord met deze service.

Deze voorwaarden zijn daarenboven niet altijd even wettig. De wetgeving moet hier dus beter toegepast en verbeterd worden om een sluitend model tot indekking van deze consumentenrisico's bij het opstellen van het contract te krijgen (Svantesson & Clarke, 2010), zodat gebruikers niet onwetend intekenen in voorwaarden die serieuze consequenties kunnen hebben en waarvan de legaliteit van sommige voorwaarden te bediscussiëren valt.

Raf De Backer (Ferranti) (2013) bevestigt dat de grote public providers altijd gaan proberen iets toe te laten in het contract zodat ze iets kunnen doen, dat is natuurlijk hun grote marktwaarde.

Laurens Dauwe (Stibbe) (2012) merkt op dat er ook een duidelijke security policy om de beveiligingsrisico's in te dekken moet toegevoegd worden aan het contract.

Kristof Janssens (Jordens Datacenter) (2012) merkt echter op dat bij hun bij het opstellen van een cloud computing contract dat de voorwaarden allemaal mooi zijn opgeschreven zonder de consument te willen beliegen. De consument is van alle facetten op de hoogte gebracht.

5.3.2.5 Besluit risico's en vertrouwensmodel

Heeft het vertrouwensmodel eigenschappen die realistisch zijn om voldoende vertrouwen in de cloud te hebben en de risico's van de cloud in te dekken?

Tom Aerts (LRM) (2012) bevestigt dat schaalbaarheid een eigenschap is waar cloud providers aan moeten voldoen. Met beveiliging en privacy moet volgens hem ook rekening gehouden worden. Hij haalt ook aan dat er een tweede datacenter aanwezig moet zijn voor back-up: betrouwbaarheid, aanpassingsvermogen, beschikbaarheid, robuustheid en weerstand zijn dus eigenschappen die ondersteund moeten worden. Alle eigenschappen worden dus bevestigd door hem.

Kristof Janssens (Jordens Datacenter) (2012) merkt op dat er een redundante lijn naast de gewone lijn naar de cloud provider moet zijn, redundante stroomaansluitingen, telefonie daar zijn acht aansluitingen voor, redundant firewall. De eigenschappen betrouwbaarheid, aanpassingsvermogen, beschikbaarheid, robuustheid en weerstand zijn dus eigenschappen die ondersteund moeten worden. Met beveiliging en privacy wordt rekening gehouden door de klanten op te delen in boxen. Jordens datacenter kan niet kijken in de box en data blijft volledig gescheiden van data van andere klanten. Over schaalbaarheid wordt hier niet gesproken.

Aan de hand van dit vertrouwensmodel zullen de cloud services meer en meer transparant worden en zal het niveau van vertrouwen verhogen. Een resultaat hiervan zal zijn dat de inburgering van cloud computing zal verhogen en we een nieuwe tijd van computing zullen binnenstappen (Mohammed, 2011).

Hoewel cloud computing reeds een groot fenomeen is, blijft de echte opkomst een beetje beperkt door de risico's (Che & Duan, 2011). Deze risico's kunnen onder meer door het vertrouwensmodel ingedekt worden.

De sleutel tot een succesvolle verdere inburgering van cloud computing is ervoor zorgen dat de privacy risico's, beveiligingsrisico's en consumentenrisico's bij het

opstellen van het contract ingedekt zijn. Dit werd vermeld door Laurens Dauwe (2012) en dit is tevens de indeling die ik gehanteerd heb in mijn masterproef. Gedurende de andere interviews zijn er geen categorieën verschenen die anders dan deze zijn. Er kan gesteld worden dat alle risico's van cloud computing besproken zijn. Indien men de privacy risico's, beveiligingsrisico's en consumentenrisico's bij het opstellen van het contract niet adequaat zou indekken dan zal cloud computing bij eilanden blijven en niet zijn volle potentieel bereiken (Mohammed, 2011). Naast deze drie risico's die onderdeel zijn van het vertrouwensmodel zijn er ook indekkingen van algemene risico's door cloud gebruikers. Deze zijn ondergedeeld in indekkingen die door management gedaan worden, indekkingen die door technisch personeel gedaan worden, en indekkingen die door technisch en zakenpersoneel gedaan worden. Tesamen vormt het een volledig geheel van risico's en indekkingen die vertaald kunnen worden in een continu auditmodel.

5.4 Hoofdstuk 4: Continu auditmodel

Hieronder volgt eerst een korte beschrijving over auditing en dan een schematische vorm van het continu auditmodel.

5.4.1 Auditing gedefinieerd

Auditing wordt gedefinieerd als het objectief verzamelen en evalueren van bewijs betreffende stellingen van economische acties en gebeurtenissen om de gelijkenis tussen deze stellingen en vooropgelegde criteria (bijvoorbeeld een SLA, oftewel Service Level Agreement) te vergelijken en de resultaten te communiceren naar de geïnteresseerde gebruikers (Rittenberg & Schwieger, 2004).

De Raad van Bestuur huurt het management om de organisatie draaiende te houden. Dit management bereidt de financiële overzichten voor die voorgelegd worden aan derde partijen. Auditors zullen deze financiële overzichten auditen en hun audit opinies aan deze derde partijen doorgeven (Rittenberg & Schwieger, 2004).

Hierbij moet wel een kanttekening gemaakt worden dat een audit enkel waarde toevoegt als de auditor expertise heeft in het evalueren van bewijs omtrent de financiële overzichten en de economische stellingen die in deze financiële statements verwerkt zijn. De auditor moet daarnaast ook onafhankelijk zijn van het management en derde partijen en dus een objectieve opinie te geven van de financiële resultaten (Rittenberg & Schwieger, 2004).

Auditing houdt in:

1) Het proces om bewijzen te verzamelen om stellingen te bewijzen (Rittenberg & Schwieger, 2004);
2) Het audit proces is systematisch (Rittenberg & Schwieger, 2004);
3) De auditor is onafhankelijk van de entiteit die geaudit wordt (Rittenberg & Schwieger, 2004).

Kristof Janssens (Jordens Datacenter) (2012) merkt op dat er ook al reeds bestaande auditmanieren zijn om een cloud provider te auditen. SAS 70 is een Amerikaanse audit standaard oftewel ISO 27001 als Europese standaard. SAS 70 staat voor Statement on Auditing Standards en garandeert dat een service organisatie zijn controlemiddelen en controleactiviteiten worden gecontroleerd door een onafhankelijke auditfirma (hoofdwebsite SAS 70, 2013). Tom Palmaers (Cegeka) (2012) merkt verder op dat het de ambitie is van Cegeka om zich te gaan certifiëren volgens de ISO 27001 norm. Het certifiëren aan de ISO-normen is een manier om aan te tonen dat een onafhankelijke instantie is komen kijken dat alles volgens hun normen gebeuren en dan heb je daar een certificaat van (hoofdwebsite ISO, 2013). Enkel de ISO 27001 is de norm uit de reeks waarop je je kunt laten certifiëren (hoofdwebsite ISO, 2013). Veel mensen denken dat hierin gestipuleerd staat wie en op welke wijze er aan beveiliging gedaan wordt. Ze citeren echter alleen maar de principes en het proces dat je moet voorzien.

Mark Lens (Eurosys – IT-solutions) (2012) merkt op dat ISO echter niets zegt over de kwaliteit van het product echter enkel over hoe het proces om iets te maken moet geïmplementeerd zijn. Als je je wil certifiëren moet je als bedrijf een ISMS maken (hoofdwebsite ISO, 2013). ISMS staat voor Information Security Management System (hoofdwebsite ISO, 2013), dat is eigenlijk je beheersysteem van informatiebeveiliging (Palmaers, 2012). Als je je als bedrijf wil certifiëren moet je aantonen dat je ISMS hebt uitgedacht. Dan ga je die ISMS moeten implementeren in de organisatie, je moet die gaan meten, je moet jaarlijks een review doen en zijn er verbeteracties mogelijk. Dan moet je aan de hand van die verbeteracties opnieuw verbeteringen toevoegen. Je krijgt een model van continue verbetering. Je moet aan een auditor aantonen dat je die fasen volgt om ISO 27001 gecertificeerd te geraken (Palmaers, 2012). Dit gaat echter enkel over het proces en niet specifiek over de beveiliging. Je kan een bedrijf hebben dat een zeer sterke beveiliging heeft en je kan een ander bedrijf hebben dat eigenlijk een zeer lichte beveiliging heeft en die kunnen allebei ISO 27001 gecertificeerd zijn. Met dat certificaat kan je het niveau van beveiliging niet gaan afleiden. Je kan enkel afleiden dat je op een procesmatige manier omgaat met die informatie (Palmaers, 2012). Mark Lens (Euorsys – IT-solutions) (2012) merkt op dat om ISO te implementeren heel wat werk kost en het geen een sinecure is. Het is daarnaast geen garantie dat als je ISO gecertificeerd bent dat je goede producten aflevert. De ISO 27002 standaard is daarnaast een soort van hulpmiddel om ISO 27001 te gaan implementeren (hoofdwebsite ISO, 2013). Je kan dat zien als een soort kookboek met een hele hoop controles in: dit zijn mogelijke maatregelen die je kan nemen op het gebied van beheer van wachtwoorden, op het niveau van fysieke beveiliging en dergelijke meer. Maar je moet je er niet aan houden. Het betreft eerder een overzicht van richtlijnen die je als inspiratie kan gebruiken om controles te gaan definiëren (Palmaers, 2012). Laurens Dauwe (Stibbe) (2012) haalt ook aan dat ze vaak een referentie naar ISO-normen zien. Bijvoorbeeld ISO 27001. Maar een ISO-norm is heel algemeen, heel vaag. Die norm schrijft voor dat je operational security measures, organisational security measures en physical security measures moet opleggen. Als je echter over heel gevoelige gegevens spreekt, wordt er echter veelal geëist dat er wat meer wordt gedaan dan zuiver ISO 27001. Die ISO-normen zijn al veel ouder als de cloud. Het is echter niet specifiek voor cloud computing gemaakt (een nieuw continue auditmodel voor cloud computing stel ik in deze masterproef zelf op). Raf De Backer (Ferranti) (2013) merkt op dat ze nog bezig zijn om te voldoen aan de ISO 27000 norm. Aan de ISO 9001 norm voldoen ze reeds. Pieter Delbeke (Zentrick) (2013) merkt op dat je ISO gecertificeerd moet zijn om te werken voor de overheid. Ook sommige bedrijven vereisen dat je ISO gecertificeerd bent. Zentrick heeft echter nog nooit de vraag gehad van klanten om ISO gecertificeerd te zijn. Het kost ook veel geld om te voldoen aan een ISO-norm. Het is echter niet voldoende om enkel aan de ISO-norm te voldoen. Vandaar het continu audit kader.

Hier specifiek bij cloud computing wordt er een continu auditkader ontwikkeld. Nu gaan we verder met het definiëren van continue auditing.

5.4.2 Continue auditing

De bedoeling van continue auditing is om auditing dichter bij het operationele proces te brengen en weg van het traditionele terugkijkend eens-per-jaar van de financiële resultaten (Alles, Kogan, & Vasarhelyi, 2008).

Continue auditing is een methodologie die onafhankelijke auditors de mogelijkheid geeft om een geschreven verzekering over een bepaald onderwerp te geven, waarover het management verantwoordelijk is, op basis van rapporten die quasi tegelijkertijd of een korte periode nadat de gebeurtenissen gepasseerd zijn (Alles et al., 2008).

In plaats van te rapporteren na de feiten, wordt er als het ware aan continue rapportering gedaan. We gaan een continu auditmodel opstellen waarmee we een audit op cloud computing kunnen gaan toepassen.

Wanneer ik dit model opstel moet er wel rekening mee gehouden worden dat bij continue monitoring de nood voor het verdedigen van de extra investeringen verhoogt. Hierdoor zal de mogelijkheid tot niet investeren namelijk het 'status quo effect' interessanter lijken, hier is immers minder verdediging voor nodig, en zal dus eerder gekozen worden dan extra investeren in een risicovoller project (Hunaton & Mauldin, 2010). Hoewel extra investeren toch meer overeen zou stemmen met het lange termijn succes, wordt dus niet investeren gekozen.

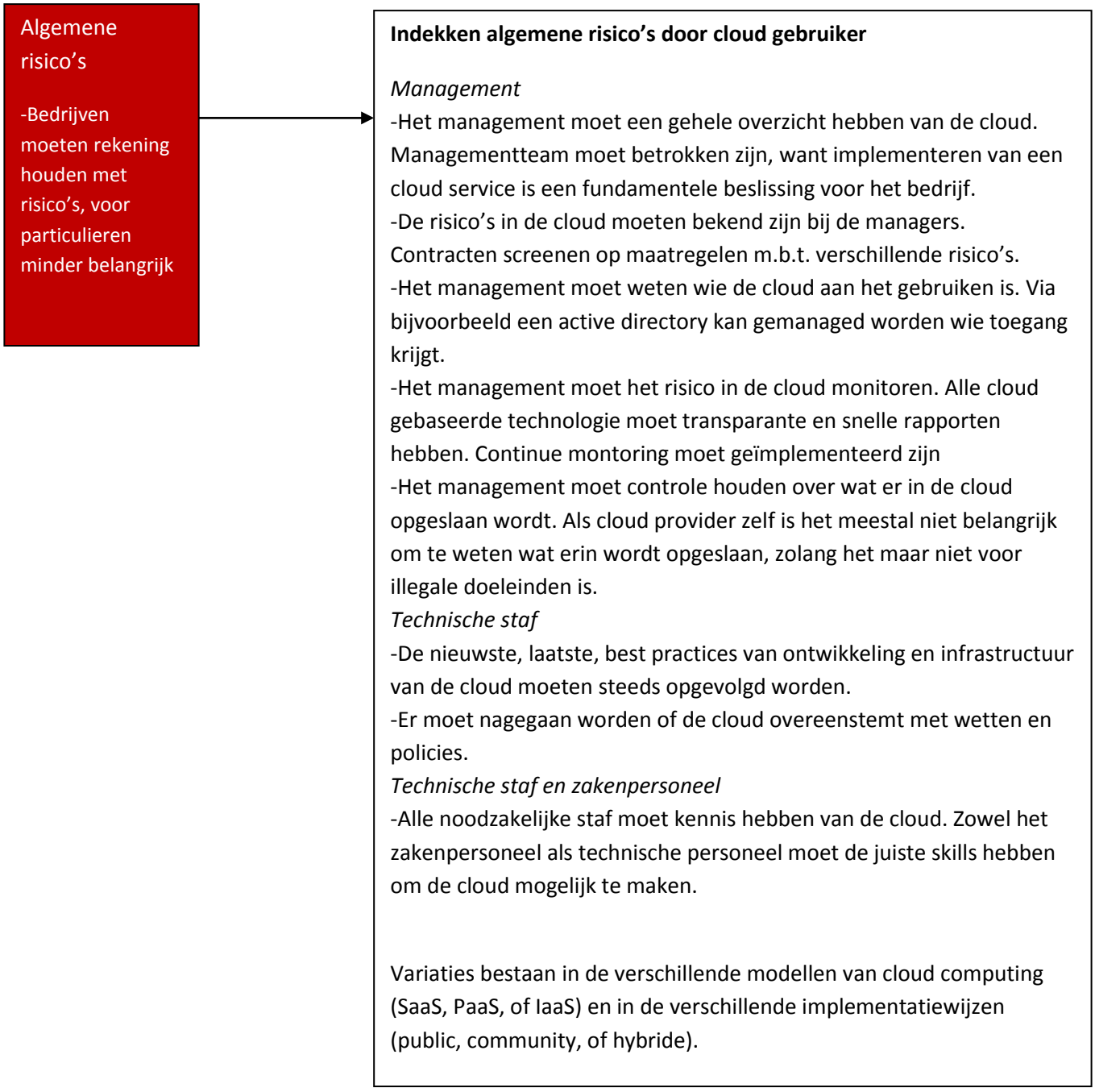
Dit effect dient steeds in het achterhoofd gehouden te worden bij het opstellen van het aangepast continue auditmodel voor cloud computing.

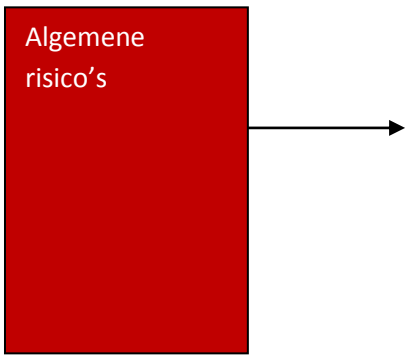
5.4.3 Schematische vorm continu auditmodel

We hebben nagegaan of het auditmodel dat reeds is opgesteld in de praktijk al zijn toepassing heeft gevonden of dat het mogelijk is dit auditmodel in de praktijk te gaan implementeren. Namelijk welke risico's, die reeds benoemd zijn, het meest frequent voorkomen en welke indekkingen van risico's het meest frequent voorkomen en welke eventuele wetten er worden toegepast.

Ik heb de bevindingen uit de interviews reeds geïmplementeerd in de bovenstaande literatuurstudie. Hierdoor zijn we al op de hoogte gebracht of het voor de specifieke puntjes het mogelijk en realistisch was te veronderstellen dat ze in de realiteit gelden.

Hieronder volgt een schematische vorm van het continu auditmodel.





Indekken algemene risico's door cloud gebruiker en cloud provider aan de hand van vertrouwensmodel

Geen concurrentieel voordeel te verkrijgen door louter technologie. Maar wel door het vertrouwen in de cloud provider. Het gerelateerde vertrouwen zal de kosten van onderhandelingen verlagen en de mogelijkheid tot conflict verlagen. (vroeger met interne systemen was het veelal automatisch het geval dat het te vertrouwen was).

Vertrouwensmodel voor het indekken van de algemene risico's. Vertrouwen in de cloud betekent dat een cloud zijn job doet als verwacht.

5 eigenschappen van het vertrouwensmodel:

1) Aanpasbaarheid: snel en efficiënt reageert om zijn infrastructuur aan te passen wanneer dit nodig is. (hardware falingen, veranderingen in de noden gebruiker)
2) Robuustheid: De mogelijkheid van het systeem om toch zijn features te behouden hoewel er subsystemen en componenten falen
3) Schaalbaarheid: De mogelijkheid om resources te verhogen of verlagen
4) Beschikbaarheid: De relatieve tijd dat een service met al zijn functies te gebruiken is
5) Betrouwbaarheid: De mate van succes waarin een service functioneert, de mate waarin de service correcte resultaten levert en geen dataverlies oplevert

=> Privacy en beveiliging zijn de ondersteunende principes van deze 5 eigenschappen. Deze moeten in orde zijn om de 5 eigenschappen te kunnen garanderen. Met het **privacy risico en beveiligingsrisico** moet dus rekening gehouden worden
=> Wanneer de 5 eigenschappen worden afgesproken dan wordt er een contract opgesteld. Hier treedt **het consumentenrisico bij het opstellen van het contract** op.

Deze drie risico's en de indekkingen ga ik verder bespreken.

Privacy risico's

-De service provider heeft toegang tot de data en zou die data kunnen gebruiken voor verschillende doeleinden, die niet altijd stroken met de wil van de cloud user.

-Cloud computing vergroot de opportuniteiten voor misbruik van de data door de cloud provider. Cloud services verzamelen immers data van veel meer instanties tegelijk.

-Een zeer belangrijk risico dat niet onderschat mag worden. Voor bedrijven met gevoelige informatie zeer belangrijk.

Verschillende privacy risico's:

1) Data wordt blootgelegd waar niet gepast. Hierbij denken we aan de US patriot Act waarbij de Amerikaanse overheid vrij kan kijken in de data van een datacenter als het vermoedt dat er criminele of terroristische activiteiten achter zitten.
2) Wat zijn de precieze omstandigheden waaronder data geraadpleegd en gewijzigd kan worden? Google Docs en Gmail was data half aan het filteren en zei niet expliciet dat het aan het filteren was voor target advertising.
3) Wat is de precieze duurtijd dat data opgeslagen blijft? Persoonlijke data die blijft opgeslagen nadat het zogezegd verwijderd zou zijn is een mogelijk risico.
4) Wordt de klant voldoende geïnformeerd over deze privacy risico's? Dit kan via de privacy policy.

Indekken privacy risico's door wetgeving

US: Privacy Act 1974, E-government Act (een agent van de overheid moet privacy impact assessments uitvoeren om de impact van informatietechnologie op de informatie privacy te kunnen inschattten, minder bekend), HIPAA (bescherming van de individuele medische informatie privacy), The notification act (Amerikaanse equivalent van 2002/58/EC)

EU: Data Protection Directive dit is richtlijn 95/46/EC, e-privacy directive dit is richtlijn 2002/58/EC (mededeling van een beveiligingslek is noodzakelijk), voorstel op komst om een update te brengen van 96/46/EC aan de nieuwe digitale omgeving (veel voorstanders om deze update te implementeren)

België: Wet van 8 december 1992 (bescherming van de persoonlijke levenssfeer ten op zichte van de verwerking van persoonsgegevens), instanties die bevoegd zijn voor privacy: Privacycommissie, FOD Economie, BDMA, e-cops, etc.

Indekken privacy risico's door wetgeving

In de US stelt de privacywetgeving echter niet veel voor. In US is privacy een goed dat te koop is. Privacy is voor hun niet belangrijk, ze gebruiken het als het hun uitkomt. In de US heeft het Supreme Court nog altijd niet onderkend dat informatie privacy één van de fundamentele rechten is. Als het hun niet uitkomt is het een onbelangrijk risico. In EU is privacy echter een grondrecht. Dit is gewaarborgd door artikel 8 van de Europese wet van de rechten van de mens. Europa heeft de striktste privacywetgeving ter wereld. Spanje, Italië en Duistland zijn nog strenger. Een Amerikaans bedrijf kan zich wel Safe Harbor compliant verklaren aan de strengere Europese Data Protection Directive. Dit wil zeggen dat het voldoet aan de strengere Europese regelgeving.

Evolutie lijkt erop dat men meer en meer evolueert naar een internationaal verdrag. De verschillen tussen de landen zijn echter nog groot. Het samensmelten van de verschillende landen zal zeker niet slecht zijn, maar of het gaat lukken dat is een andere vraag.

Indekken privacy risico's door privacy policy

-Wanneer er met gevoelige data gewerkt wordt, moet er via policies bepaald worden wie er toegang tot de data krijgt en hoe met die data wordt omgegaan, dit mag niet een loutere ad hoc regeling zijn. Er moet een echte policy hierover aanwezig zijn
-Het is belangrijk alvorens er data op een andere server gezet wordt naar de privacy policy wordt gekeken. Meestal wordt dit niet goed bekeken.
-Daarnaast is de privacy policy meestal vaag opgesteld. De gebruiker krijgt bij Google slechts een gelimiteerd, vaag, begrip van hoe zijn of haar persoonlijke informatie wordt gebruikt bij Google. Dit is meestal gedreven door het commercieel perspectief, maar ondermijnt de wettige privacy rechten van de individuele gebruiker. Wetten die deze privacy policies beter reguleren, moeten dus toegepast en geïmplementeerd worden.

Privacy risico's bij transborder clouds

-Garanderen de wetten van het land waar de data naar getransfereerd wordt voor de desbetreffende cloud provider voldoende mate van privacy die minstens even hoog is als het land van de gebruiker?

(bepaalde landen laten het zelfs niet toe dat overheidsgegevens gehost worden buiten hun eigen territorium)

Indekken privacy risico's bij transborder clouds

EU: Artikel 25 van de EU Directive 95/46 (data mag enkel getransfereerd worden naar een ander land, als dit land een voldoende mate van protectie van privacy kan garanderen), er kan ook gewerkt worden met binding corporate rules (standaarden opleggen aan verschillende entiteiten in verschillende landen, die standaarden moeten in één land in Europa goedgekeurd worden)

-Gemakkelijkste manier om in te dekken, is data enkel op dezelfde geografische plaats onderbrengen. Zo moet er niet iedere keer over contracten met verschillende landen onderhandeld worden.
-Zelfs op zee onderbrengen lijkt een oplossing. Zo zullen ze onder geen enkele wetgeving vallen.

Beveiligingsrisico's

-Een heel belangrijk risico, wordt vaak onderschat. Gebruikers worden veelal niet goed op de hoogte gebracht van de verschillende beveiligingsrisico's bij cloud computing.

CSA noemt 6 beveiligingsrisico's:

1) Onbeveiligde interfaces en APIs. Browserinterface houdt een risico in.
2) Kwaadwillige indringers. Het is risicovol dat je gehackt wordt. Sony is bijvoorbeeld gehackt geweest met zijn gameconsoles.
3) Gemeenschappelijke technologieproblemen bij virtualisatie. Als er een technisch incident is op de onderliggende infrastructuur heeft dat effect op heel wat virtuele clients
4) Data verlies of lekken. In maart 2009 ervaarde Google Docs service een data lek. 5 procent van de documenten werd gedeeld waar dit niet de bedoeling was. Als je de security van persoonsgegevens niet goed garandeert kan het openbaar ministerie een klacht tegen je indienen. Bij de NMBS was onlangs van 1,4 miljoen van de reizigers hun persoonlijke data gelekt.
5) Account of service kaping. Als het account gekaapt wordt door malafide gebruikers.
6) Onbekend risicoprofiel. Het gebrek aan kennis van de beveiligingsmaatregelen van de cloud provider kan aanleiding geven tot het intekenen van services die te weinig beveiliging hebben als noodzakelijk.

Gartner noemt 6 beveiligingsrisico's:

1) Bevoorrechte gebruikerstoegang. Als administratorpaswoorden bijvoorbeeld te snel gedeeld worden.
2) Voldoen aan wetten en reguleringen omtrent beveiliging. Dit kan ISO/SAS 70, up-time institute, etc. zijn.
3) Data locatie. Risico waar je data zich bevindt en hoe deze dan is beveiligd.
4) Data enkel beschikbaar voor desbtreffende gebruiker. Via een active directory kan je gaan bepalen wie aan bepaalde data mag en wie niet.
5) Herstellingsrisico. Risico voor herstel van aantastingen van de cloud service.
6) Lange termijn effectiviteit. Zal de cloud provider dezelfde servicelevels of beveiliging kunnen garanderen.

Beveiligingsriscio's bij cloud gebruikers

1) Tijd dat de service niet bereikbaar is. Dit kan ook afhangen van de Internetverbinding die niet goed werkt. Telenet is bijvoorbeeld recent voor een tijdje uitgevallen. Een redundant lijn naar de cloud provider toe is een oplossing.
2) Mogelijke lekken van commerciële geheimen. Dit is een beveiligingsrisico wat ook door de privacywetgeving gedwongen wordt om in te dekken.
3) Hoe handelen met de geprivileerde status van de cloud provider. Dit is een beveiligingsrisico wat ook door de privacywetgeving gedwongen wordt om in te dekken.

Beveiligingsrisico's bij cloud providers

1) Hoe de werking van de cloud garanderen en fouten bij die werking te minimaliseren.
2) Hoe te vechten tegen een talrijk en agressief netwerk van hackers.
3) De reputatie van de cloud provider kan in gevaar zijn als zijn cloud service voor illegale doeleinden gebruikt wordt.

Indekken beveiligingsrisico's

1) Cloud providers zouden het voor gebruikers management en onderhoud meer transparant en makkelijk moeten maken. Dit houdt in dat er logs moeten opgeslagen worden en deze logs voor de gebruikers toegankelijk moet maken.
2) Andere contextuele informatie zoals de locatie van de gebruiker zou moeten worden toegevoegd bij het aanmelden van de gebruiker. Sterkere paswoorden moeten geïmplementeerd worden. Elektronische identiteitskaarten als aanmeldmethode zijn hier een voorbeeld van.
3) Ineffectief management van geprivileerde gebruikers moet vermeden worden. Paswoorden mogen niet te snel gedeeld worden.
4) Het beveiligen van de inhoud van het informatiemedium (met encryptie) en het controleren van de toegang tot het medium (met bijvoorbeeld tokens).
   Encryptie: Https, VPN, AES codering
   Tokens: een reeks cijfers of karakters die niet zomaar te verzinnen is. Deze kunnen gegenereerd worden via een apparaatje. Iemand die in het bezit is van een token kan het dus niet verzonnen hebben en bewijst daarmee de token te hebben.

Indekken beveiligingsrisico in de verschillende lagen

IaaS is de laagste laag en hier zijn slechts minimale beveiligingsmaatregelen door de cloud provider. Enkel om de infrastructuur zelf te beveiligen. PaaS geeft een platform waar de desbetreffende gebruiker zelf zijn applicaties op kan maken. Hier zijn al meer beveiligingsmaatregelen, maar deze is niet compleet. Gebruikers hebben zelf nog de mogelijkheid tot implementeren van additionele beveiliging. Bij SaaS daarentegen is de gehele beveiliging overgelaten aan de cloud provider en heeft de gebruiker geen inspraak

Indekken van beveiligingsrisico's bij de opbouw

1) De traditionele beveiligingsmechanismen (protectie van fysieke faciliteiten). Er moet een tweede back-up center zijn, redundante telefoonaansluitingen, redundante stroom, camera's, badgesysteem, zuurstof in de rekken verlagen bij brand, op een speciale manier geblust zodat de apparatuur geen schade oploopt, redundante koeling, toegangsbeveiliging, cijferslot op de racks waar de servers inzitten, bewaking door veiligheidsagenten, branddeuren, inbraakdetectie.
   De zogenaamde tier-normen zijn hier van toepassing: tier 1, 2, 3 en 4. Deze zijn geregeld door het Amerikaanse up-time instituut. Europees is er nog geen dergelijk instituut.
   Tia 942 norm kan ook van toepassing zijn. Dit is een internationale norm uitgegeven door het Amerikaanse Telecommunications Infrastructure Association.
2) Beoordeling van de veiligheid bij het gebruik van virtualisatie. Het implementeren van voldoende scheiding tussen de virtuele clients is noodzakelijk zodat het niet gemakkelijk is om zomaar van de ene virtuele client op de andere te gaan. Vermits ze hetzelfde onderliggende fysieke platform hebben is hiervoor immers een verhoogd risico op.
3) Gegevens moeten makkelijk naar een andere cloud provider overgedragen kunnen worden, een zogenaamde lock-in moet vermeden worden. Een oplossing kan zijn om standaard API's te gebruiken zodat data gemakkelijk naar een andere cloud provider overgebracht kan worden. Beveiliging tegen een vaste cloud provider wordt hierdoor geïmplementeerd.

Indekken beveiligingsrisico's bij de operationele werking

1) Verzekeren van de business continuïteit. Regelmatige inspectie van de infrastructuur van de cloud provider is hier een must. Via Nimsoft kan gemakkelijk aan monitoring van de infrastructuur gedaan worden. Vulnerability assessments kunnen ook toegepast worden. Ethische hackers kunnen ook ingeschakeld worden.
2) Een systeem waarbij indringers snel ontdekt kunnen worden, moet geïmplementeerd worden (firewalls, controles zodat toegang niet misbruikt wordt).
3) Gebruikers op de hoogte brengen van een beveiligingsincident en een noodplan opstarten om te reageren op het beveiligingsincident (alarmcentrale verwittigen, brandweer en politie worden verwittigd, sommige medewerkers krijgen een alarm).
4) Noodzakelijk om te weten wat de redenen van het beveiligingsincident waren (root cause analyse).
5) Bottlenecks bij het overdragen van grote hoeveelheid data moeten vermeden worden. Dit kan vermeden worden door het overbrengen van disks waarop de data staat. Beveiliging tegen bottlenecks wordt hierdoor geïmplementeerd.

Je kan echter niet alle beveiligingsrisico's indekken. Op technisch vlak zijn ze heel dikwijls heel sterk afgedekt. Er is echter nog steeds een menselijke factor die veel beveiligingslekken voorstelt. De persoon die werkt heeft nog altijd een USB-stickje bij en die heeft dat toevallig mee en die is niet encrypted en de geheimen komen op straat terecht.

Consumentenrisico's bij het opstellen van het contract

-In contracten gebeurt het wel eens dat cloud providers bevoordeeld worden ten nadele van cloud gebruikers.
-Veel cloud computing contracten zijn niet opgesteld zoals ze zouden moeten zijn. De contracten zijn onevenwichtig ten op zichte van de cloud provider.
-De contracten zijn meestal zogezegde toetredingscontracten die enkel door de cloud provider zijn opgesteld zonder input van de cloud gebruiker.
-Cloud gebrukers aan veelal onwetend akkoord met benadeelde voorwaarden zonder dat ze dit weten.
-Bij public cloud spelen deze risico's een grotere rol, bij private cloud een minder grotere rol omdat men hier over meerdere dingen in het contract kan onderhandelen dan bij public cloud

Indekken consumentenrisico's bij het opstellen van het contract

-Om een gebalanceerde rechtvaardigheid te garanderen tussen cloud provider en cloud gebruiker hanteert de wet enkele beperkingen op dergelijke contracten: verplichte informatie over het product en/of provider, omstandigheden van het vormen van het contract, etc.

-Er blijven echter benadelingen meespelen

-De wetgeving moet beter toegepast en verbeterd worden om een sluitend model van de consumentenrisico's bij het opstellen van het contract te krijgen.

Er moet gekeken worden bij de audit of er voldaan wordt aan de desbetreffende wetgeving en of de aangegeven additionele indekkingen voldaan zijn. Zo kan er zeker van gemaakt worden dat de risico's zijn ingedekt. Door middel van continue monitoring kan zeker gemaakt worden dat de indekkingen gedaan word

6 Bijlagen

Nu ga ik dieper in op het uitvoeren van de structurele diepte-interviews met bevoorrechte getuigen. Ik pas mijn vragen aan, aan de functie die de desbetreffende geïnterviewde uitoefent. Een cloud provider zal immers andere dingen weten dan een cloud user en omgekeerd. Deze vragen hebben tot doel te kunnen stellen in hoeverre het reeds opgesteld model in de realiteit kan geïmplementeerd worden.

6.1 Hoofd van de divisie ICT & Media investments LRM – Tom Aerts

Als eerste contactpersoon heb ik Tom Aerts (LRM NV, de investeringsmaatschappij voor Limburg). Hij is verantwoordelijk voor de divisie ICT & Media Investments bij LRM. LRM is een investeringsmaatschappij in Limburg en investeert in Limburgse bedrijven. De divisie ICT & Media Investments investeert in beloftevolle spelers in de Limburgse ICT Sector. De portefeuille ICT & Media bedraagt ongeveer 15 bedrijven.

Hierna volgt een transcriptie van dit interview. Het interview duurde 41 minuten en 40 seconden en werd gehouden in de gebouwen van LRM te Hasselt op 25 oktober 2012. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor beide partijen. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Hoe komt u in aanraking met cloud computing?

We zien heel veel **innovatieve projecten** passeren met betrekking tot ICT & Media. Die nieuwe innovatieve projecten zijn de laatste tijd meer en meer **cloud-based**. Het is een **nieuwe trend**.

Wat zijn volgens u de belangrijkste voordelen van cloud computing?

Efficiëntie en het is veel **flexibeler**. Door flexibiliteit kan je veel efficiënter data storen.

Wat zijn volgens u de belangrijkste nadelen van cloud computing?

Cloud computing kent nog altijd de perceptie onveilig te zijn. Het blijft een **vaag begrip**. Je merkt dat bij de **niet-ICT bedrijven het een zeer vaag begrip blijft**. Ik ga dat ergens stockeren, wie kan het zien, wie kan eraan? Het blijft altijd intrinsiek de perceptie hebben, dat wanneer data in de cloud zit, dan kan **iedereen dat zien**.

Is er een onevenwicht tussen provider en gebruiker bij het opstellen van een cloud computing contract?

Zoals bij elk contract ga je voor een **gezond evenwicht tussen de twee partijen**.

Welke beveiligingsrisico's voor consumenten treden er op?

De tijd dat de service bereikbaar is, is **niet noodzakelijk een beveiligingsrisico**. Het **kan zijn dat je internetverbinding niet goed werkt**.

Mensen staan veel meer open als vroeger alles wat gemonitord wordt via Facebook of Google. Vroeger was alles wat je ingaf op het web al een inbreuk op de privacy. Nu **evolueert de maatschappij veel meer: naar opener zijn**. Op sociale media worden zeer veel persoonlijke data geüpload. Puur voor particulieren waarbij die **mentaliteitswijziging bezig is.**

Welke beveiligingsrisico's voor providers treden er op?

Dat je **gehackt wordt**, dat je **beveiliging niet optimaal is**. De data die de klant bij je stored dat die gehackt wordt.

Welke beveiligingsrisico's voor overheden treden er op?

Overheden zijn nog **veel meer met privégegevens bezig. Als je fiscale gegevens (v.b. BTW) 'cloud- based' gaat maken,** daar zit je met zeer veel privégegevens. **Potentieel zeer zwaar gevaar**. Als belastingsaangifte of bankrekening online beschikbaar is, zou niet fijn zijn. De liability is er veel groter. Bij overheden en banken wordt het **heel zwaar afgeschermd**. Het zal nog wel even duren vooraleer je dat cloud based gaat maken.

Hoe kunt u deze beveiligingsrisico's indekken?

Paswoorden en administratorrechten daar stel ik vast dat die **heel snel worden doorgegeven onder collega's**. Ik ga op verlof en ik **geef bijvoorbeeld mijn code door**. Je zit altijd met een menselijke factor. Maar als je telkens administratorrechten zo gaat beperken of streng maken dat je iedere keer moet opgebeld worden als je het minste moet doen dat werkt ook niet. Zolang bij de beveiliging een **menselijke factor tussenzit ga je altijd een risico hebben.**

Encrypteren wordt gedaan, maar er zijn **technisch nog altijd een aantal obstakels**. Iets wat **naar de toekomst meer en meer kan**.

Hoe dekt u beveiligingsrisico's in de verschillende lagen in?

Ja, **verschillend per laag (PaaS, IaaS, SaaS)**. Er zijn ook **verschillen in prijs om in te dekken**. Bij verschillende datacenters kan je hogere beveiliging vragen. Bij sommigen zijn de eisen naar beveiliging veel hoger als bij andere services.

Hoe denkt u over virtualisatie?

Met **virtuele servers heb je altijd één tussenpartij er extra bij. Hoe meer partijen ertussen zitten, hoe meer risico.**

Hoe dekt u beveiligingsrisico's bij de operationele werking in?

Je hebt bedrijven die cloud computing diensten aanbieden. Het verzekeren dat die servers aangeboden blijven. Data **moeten gebackupt zijn op een locatie die verder als 20 of 30 km ligt**. Dat zijn diensten die vaak gevraagd worden in offertes. De data moeten op verschillende plaatsen opgeslagen worden. Zodat je de back-ups altijd beschikbaar hebt. **Valt daar morgen een bom, dan is de data nog altijd ter beschikking**.

Meestal komt eerst de gebruiker van de server erachter dat er een hack is gebeurd.

Auditing kan nooit genoeg doen. Je **kunt 100 dingen testen maar dat één incident kan net bij situatie 101 zich voordoen**. Je kunt heel wat testen en uitsluiten maar **je bent nooit 100 procent zeker**.

Wat moet het management/kaderpersoneel weten van de cloud?

Ze moeten **garanderen dat het even safe is als een normale storage**.

Moet er geweten worden wat er in de cloud gestoken wordt en wie er iets in de cloud steekt?

Ja, ieder bedrijf moet weten **wat er in de cloud wordt gestoken en wat er met de gegevens gebeurt**.

Het **technisch personeel moet de juiste skills hebben** om met de cloud te kunnen handelen.

Beveiliging van de cloud zelf bouwen of kopen kan beide. Als je koopt van een specialist dan ben je echter safe.

Hoe ziet u de wetgeving over heel de wereld evolueren?

Meer en meer uniforme wetgeving over de **hele wereld**.

Hebt u nog verdere opmerkingen?

Cloud computing is een **nieuwe hype**, het is een **nieuwe trend**. Alles is meer en meer **cloud gebaseerd. Beveiliging is key** in dat soort diensten. Je krijgt **nooit iets risicoloos**. Veiligheid moet je inbouwen. **Maar je krijgt altijd risico's**.

6.2 Jordens Datacenter NV – Kristof Janssens

Als tweede contactpersoon heb ik Kristof Janssens. Deze is werknemer bij Jordens Datacenter NV. Dit bedrijf verhuurt datacenterruimte en voorziet in de groeiende behoefte van bedrijven en instellingen om web- en Internetinfrastructuur extern te huisvesten. Het bedrijf houdt ten zeerste rekening met het milieu oftewel green technology. De eerste module van het datacenter is sinds september 2011 operationeel. De planning is om op termijn 12 autonome modules met een vloeroppervlakte van telkens 250 m^2 te bouwen.

Het datacenter ligt op het industrieterrein Tongeren Oost te Tongeren vlak bij de snelweg E313. Het bedrijf levert private cloud diensten.

Hierna volgt een transcriptie van dit interview. Het interview duurde 30 minuten en 39 seconden en werd gedaan in de gebouwen van Jordens Datacenter NV te 13 november 2012. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor beide partijen. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Hoe komt u in aanraking met cloud computing?

Zelf zijn we **cloud provider sinds 1 november**. We waren voordien wel een datacenter. Wij hebben de beslissing genomen om cloud computing te gaan installeren. Dat is **gebaseerd op een aantal VM-ware machines met een shared storage** die uiteindelijk cloud diensten kan leveren naar klanten.

Wat zijn volgens u de belangrijkste voordelen van cloud computing?

Hangt van bedrijf tot bedrijf af. **Niet alle bedrijven zijn er vandaag klaar voor**. Voor een **KMO** zijn de voordelen: **het is goedkoper voor de eindgebruiker; het geeft meer redundancy; het geeft meer uptime; lage investeringskost**. In de **grote bedrijven** blijven ze meestal als **hybride** oplossing. Men kan nog **niet alles van cloud computing laten afhangen** vandaag de dag.

Wat zijn volgens u de belangrijkste nadelen van cloud computing?

Het grootste nadeel dat heel wat bedrijven vandaag tegenhoudt is dat je eigenlijk **een redundante lijn** moet hebben aan de kant waarmee de cloud user op de cloud provider aansluit. Stel: er zijn graafwerken van aannemers of dergelijke in de straat. Als je dan geen **degelijke redundant lijn** liggen hebt of geen lijn hebt die over verschillende wegen loopt, dan lig je **onmiddellijk buiten dienst** als er iets met die ene lijn gebeurt. Dat is een heel groot nadeel aan de cloud. Verder zie ik vandaag de dag niet zo zeer nadelen aan het gebruik van de cloud.

Welke privacy risico's zijn er bij het gebruik van de cloud? Welke wetten zijn er om deze in te dekken?

In tegenstelling tot concurrenten **delen we klanten op in de vorm van boxen**. Niet enkel **op het niveau van servers ook op het niveau van storage**. De ene klant kan niet aan de andere klant op storage niveau maar ook niet wat betreft netwerk. Dat **blijft allemaal volledig gescheiden**. Er bestaan ISO normen die bepalen hoe we met data betreffende klanten omgaan. **ISO 27001 en ISO 27002** die **opleggen hoe er moet omgegaan worden met gegevens van klanten**. Wat je ook heel vaak tegenkomt is dat er **NDA's, non-disclosure agreements**, moeten getekend worden. **Waarmee de protectie van de**

privacy wordt gegarandeerd. Zodat wanneer een rechtzaak geopend wordt, dat je als eindgebruiker iets hebt om je op te staven. Er is automatisch aan diverse regelgeving voldaan doordat het opgedeeld is in boxen.

Er valt een groot verschil te maken tussen de cloud die wij hier hebben de cloud van **Google of Amazon**. Op het moment dat je iets bij Dropbox of Amazon zet dan is het **niet meer jouw eigendom**. Vanaf het moment dat iets bij **Jordens staat mag niemand er in de box komen kijken**. Amazon en Dropbox kijken er wel in. Daar zit juridisch het grote verschil.

Is er een onevenwicht tussen provider en gebruiker bij het opstellen van een cloud computing contract?

Dat is allemaal letterlijk mooi neergeschreven in de contracten, **zonder de consument te willen beliegen**. En de consument is van alle facetten op de hoogte gebracht.

Welke beveiligingsrisico's voor providers treden er op?

Er zijn twee facetten in. De **beveiliging van het datacenter zelf en daarnaast hebben we ook de cloud**. Het datacenter op zich heeft **tier 3 niveau**. Op zich is dat vrij hoog naar Belgische normen. Wij hebben **redundante stroomaansluitingen. Voor telefonie hebben wij acht aansluitingen**. **Overal zijn camera's aangebracht**, binnen en buiten het gebouw. **Toegangscontrole wordt beheerd door een badgesysteem**: als je van de één zaal naar de ander zaal gaat, moet je je met je badge je registreren anders kan je niet binnengaan. Om uw eigen rek open te doen heb je zelfs die badge nodig en alles wordt geregistreerd. **Dus in principe zijn alle bewegingen van personen geregistreerd**. Er gaan nog een aantal stappen bijkomen volgend jaar maar daar zitten we nu al goed.

Op cloud niveau werken we met een **redundant firewall**. Eens dat het datacenter met het internet contact heeft is deze ingesteld. Hierop gebeurt **monitoring waar het verkeer doorgaat**. Er gebeurt een antivirusfiltering, spamfiltering. Alvorens het nog maar aan de switchen, ESX'en of VMware client kan.

Worden de beveiligingsrisico's door wetten gereguleerd?

Via **Amerikaanse normen (tier 1, 2, 3, 4)**. De **Europese gemeenschap is ook bezig met het opstellen van nieuwe regels**. Op het eind van de maand zullen deze in werking treden.

Doen jullie aan encryptie?

Er staat **standaard encryptie op de storage** die voorzien is.

Wat doen jullie SaaS, PaaS of IaaS? Zijn er verschillende beveiligingsrisico's voor die verschillende lagen?

Vooral SaaS. Ja, er is een verschillend beveiligingsrisico.

Kunnen gegevens makkelijk overgedragen worden zodat lock-in vermeden wordt?

We zijn er heel flexibel in. **Data kan heel makkelijk naar ons datacenter overgebracht worden of data kan heel makkelijk naar een ander datacenter overgebracht worden**. Een heel flexibele manier van werken.

Moet er geweten worden welke gegevens er in de cloud gestoken worden?

Er staat letterlijk in het contract **dat de eigen klant verantwoordelijk is**. Daar hebben **we geen zaken mee met wat de klant precies in de cloud steekt**.

Hoe ziet u de wetgeving over de hele wereld evolueren?

Ik denk dat het meer en meer **evolueert naar een internationaal verdrag**. Ik denk dat dat zeker niet slecht is. Cloud is niet landgebonden. **De verschillen tussen landen zijn echter nog groot**. Het samensmelten van de verschillende landen zal zeker niet slecht zijn, **maar of het gaat lukken dat is een andere vraag**. De belangen tussen de verschillende landen zijn eigenlijk verschillend.

Heeft u nog suggesties omtrent de wetten die jullie moeten naleven?

Daar is Europa nog volop mee bezig om dat allemaal neer te schrijven. De meesten zijn (niet-bindende) **richtlijnen**. Iedereen spreekt vandaag de dag over het **Amerikaanse uptime institute: tier 1, 2, 3 en 4**. Europees is er nog geen dergelijk instituut. Er is nog wat werk om het Europees te regelen. Het is economisch en geografisch quasi onmogelijk om bijvoorbeeld een tier 4 datacenter te implementeren in België. Een **tier 4 datacenter mag bijvoorbeeld niet op 100 km van een vliegveld liggen, in België is dat quasi onmogelijk te bereiken**. In Amsterdam liggen het grootst aantal datacenters van Europa, die liggen allemaal rond Schiphol. Aan tier 4 is dus niet voldaan.

Er is nog werk aan de wetgeving van cloud en data.

SAS 70 is **een Amerikaanse audit standaard** oftewel **ISO 27001** voor te auditen.

Beter om technologisch in te dekken dan **zuiver alleen met wetteksten** in te dekken. Bij **technologisch moet het nog gekraakt worden**.

Wat moet het management, technisch personeel weten van de eindklant?

Het zijn meestal **de managers die komen en die hun benodigheden uiten.** Dat zijn meestal **de managers waarmee we rond de tafel zitten**. We leggen uit hoe de security in elkaar zit, hoe het datacenter in elkaar zit en de richtlijnen en wetgevingen daaromtrent.

Is er ook een procedure als er een beveiligingsincident is?

Als er een inbraak **wordt vastgesteld dan wordt de alarmcentrale verwittigd** die geeft het door aan de politie en de brandweer. Is er een **probleem met de koeling of stroom krijgen sommige medewerkers een alarm**. Vanaf het moment dat er iets afwijkt van het normale **krijgen sommige medewerkers en de alarmcentrale een bericht**.

Hebt u nog verdere opmerkingen?

Ik was onlangs op een netwerkevent van VOKA omtrent ICT. **Er waren ongeveer 80 mensen aanwezig, alle ICT-bedrijven van Limburg**, en ik stelde de vraag: 'Wie heeft er al een cloud gebouwd?'. Er zijn maar twee in Limburg die een cloud gebouwd hebben. **Buiten Jordens en Cegeka niemand**. Een **groot werkpunt van de cloud is de security en de stabiliteit van het systeem**. Niemand wil echt het risico lopen om een cloud te gaan opzetten. Het **zijn serieuze investeringen die moeten gedaan worden**. In Antwerpen heb je nog ClearMedia die met cloud computing bezig is. Maar in **Limburg zijn er weinig bedrijven die ermee bezig zijn om het aan te bieden**.

6.3 Security officer Cegeka – Tom Palmaers

Als derde contactpersoon heb ik Tom Palmaers. Tom Palmaers is sinds 2011 security officer bij Cegeka. Cegeka behoort tot de top van ICT-leveranciers in de Benelux. Het bedrijf levert kwalitatieve ICT-oplossingen die klanten helpen om hun businessdoelstellingen te realiseren. ICT kan een strategisch voordeel bieden. Cegeka zorgt ervoor dat business en ICT permanent in lijn blijven. Cegeka bestaat sinds 1988.

Hierna volgt een transcriptie van dit interview. Het interview duurde 27 minuten en 53 seconden en vond plaats in de hoofdgebouwen van Cegeka te Hasselt op 21 november 2012. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor beide partijen. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Wat moet u precies doen als security officer?

Mijn job houdt eigenlijk in dat ik het **security beleid binnen de organisatie** bepaal.

Hoe komt u in aanraking met cloud computing?

Als bedrijf levert Cegeka cloud diensten aan de klanten. Wij leveren voornamelijk **private cloud** diensten, waarbij klanten ruimte in ons datacenter hebben.

Wat zijn volgens u de belangrijkste voordelen van cloud computing?

Voor onze klanten vooral de **makkelijke manier om dingen te schalen**. Je kan heel makkelijk capaciteit gaan uitbreiden waar nodig is. Ook

kostenbesparingen omdat je heel wat werkt met shared platformen. Dit kan leiden tot kostenbesparing.

Wat zijn volgens u de belangrijkste nadelen van cloud computing?

Het feit dat in de cloud alle systemen bij elkaar staan. Er is namelijk het shared gegeven. Het is één grote wolk. Als er dus een **technisch incident** is in die wolk dan heeft dat **heel snel impact op meerdere klanten**. In het verleden met de klassieke infrastructuur had iedere klant zijn eigen omgeving. Als er één omgeving met een technisch probleem zat, bleef dat beperkt tot die klant. Als vandaag de dag sommige componenten van cloud computing-infrastructuur het begeven heeft, dan heeft dat zijn **weerslag op een heel aantal klanten**. Als er bij de onderliggende virtuele structuur een probleem zit, zit dat probleem onmiddellijk verspreid bij een heel aantal klanten. Bij het klassieke systeem zonder virtualisatie was het tot op het fysisch niveau gescheiden.

Welke privacy risico's zijn er bij het gebruik van cloud computing?

Het grootste privacy risico bij cloud computing is **verlies van persoonlijke gegevens**. De kans dat die **gegevens zouden uitlekken**. Daar zijn natuurlijk privacywetgevingen die erin meespelen.

Welke wetten zijn er om deze privacy risico's in te dekken?

Onder andere **richtlijn 95/46** van de Europese unie speelt hier mee. Dat is een Europese richtlijn waarop de Belgische wetgeving op gebaseerd is.

> *Speelt **richtlijn 2002/58/EC** hier ook mee?*
>
> Ja die heeft hier ook een aandeel in.
>
> *Bent u ook met de Amerikaanse wetgeving hieromtrent vertrouwd?*
>
> Ook een beetje. **The breach Notification Act** die de Amerikaanse equivalent van 2002/58/EC is. Die stelt ook dat als er een lek is dat dit gemeld moet worden aan de getroffen persoon.

*Speelt de **safe harbor agreement** ook een rol qua wetgeving?*

Ja, die ken ik. Die ken ik vanuit het verleden. Met Cegeka zelf komen we er echter niet echt mee in aanraking, omdat we niet echt Amerikaanse bedrijven als klant hebben. Maar safe harbor agreement is voor Europese bedrijven waarvan hun data in Amerika verwerkt worden, een soort agreement is dat opgesteld wordt **zodat de Amerikaanse organisatie voldoet aan de Europese vereisten**.

*Bent u bekend met **EU Directive 95/46 Artikel 25**? (hierna volgde een beschrijving van dit artikel)*

Ja dit herken ik. Dit wordt toegepast.

Welke beveiligingsrisico's treden er op?

De voornaamste risico's die wij zien vandaag zijn geënt op drie pijlers: vertrouwelijkheid van informatie, integriteit van informatie en beschikbaarheid van informatie. De risico's die ik zie, zijn geënt op die drie pijlers. Ten eerste de **vertrouwelijkheid van informatie** namelijk de kans dat de informatie kan uitlekken, dit is het **privacy aspect**. Ten tweede de **integriteit van informatie**, namelijk dat iemand die informatie kan gaan wijzigen zonder dat Cegeka er controle over heeft. **Beschikbaarheid** is, zoals ik daarstraks al zei, risicovol omdat we werken **met virtualisatie**. Heel wat systemen kunnen tegelijk uitvallen als er één enkel incident in de onderliggende virtualisatie gebeurt.

Hoe worden deze beveiligingsrisico's ingedekt?

De risico's met betrekking tot vertrouwelijkheid wordt gewerkt met **toegangscontrolesystemen**. Binnen Cegeka krijg je enkel toegang tot de systemen die nodig zijn om je job te kunnen uitoefenen. Ook de engineering teams die die systemen beheren, zijn een beperkte groep mensen per klant. Het is **niet dat heel het bedrijf aan die gegevens kan**, **het is beperkt per klant**. Meestal zijn er maar maximaal twintig mensen die toegang hebben tot zo een klantenomgeving. Voor zeer kritische klanten zoals banken is de toegang zelfs nog meer beperkt gezien nog minder mensen toegang verkrijgen tot bancaire systemen. Anderzijds is er **monitoring aanwezig om de mensen die dan toegang hebben om daar ook nog de nodige controles te voorzien zodat de toegang niet misbruikt wordt**. Monitoring wordt ook gebruikt om misbruik van een account tegen te gaan. Stel dat iemand zijn accountgegevens verliest of die gegevens lekken uit. Het systeem moet dan zo opgezet worden dat niet iemand anders daar misbruik van kan maken. We voorzien een aantal controlemechanismen. Alsook specifiek voor beveiliging naar systemen toe doen we hier intern aan **vulnerability management** waarop we op regelmatige basis systemen en vooral de systemen die aan Internet gekoppeld zijn, controleren of daar **veiligheidslekken in aanwezig zijn**. Dat is naar vertrouwelijkheid toe. Naar integriteit toe worden meestal op databankniveau controles voorzien. Niet standaard, gebeurt eerder op vraag van de klant. Naar beschikbaarheid toe om die risico' af te dekken werken we met **twee datacenters.** We hebben een **datacenter hier in Hasselt één in Leuven**. Kritische systemen waarbij het nodig is dat die 24 uur en 7 dagen op 7 beschikbaar zijn, worden ontdubbeld door een kopie in Leuven. Zodat als er een zwaar incident gebeurt op een component in Hasselt dan kunnen de systemen in Leuven dat overnemen.

Wat biedt u aan IaaS, PaaS of SaaS?

Je kan stellen dat **wij IaaS aanbieden**. De applicatielaag en beheer ervan (SaaS) die doen we ook voor sommige klanten maar eigenlijk zeer beperkt. Het is niet echt dat we de applicatie als een service gaan aanbieden, dat is eerder bij de klant.

In het contract naar de klant **is altijd duidelijk gesteld wie welke verantwoordelijkheid heeft**. Als bijvoorbeeld bij een applicatie als het beheer daarvan bij de verantwoordelijkheid van de klant ligt dan ligt het beveiligingsstuk ook bij de klant.

Kunnen gegevens makkelijk overgedragen worden naar een andere cloud provider?

Bedrijven zetten hun data bij ons en in contracten worden altijd **clausules** voorzien. Wanneer zij hun contract hier stopzetten **dat zij hun data op een gemakkelijke manier terugkrijgen.**

Hoe ziet u de wetgeving over heel de wereld evolueren?

Er gaat **meer en meer belang komen naar het privacy aspect**. Ik denk dat de **privacywetgevingen van vandaag ook niet echt rekening houden met de cloud aspecten**. Als je puur de wetgeving bekijkt dan zegt de wetgeving bijvoorbeeld dat informatie onderhevig is aan de privacywetgeving in het land waar het zich bevindt. Als je met public cloud diensten werkt **dan weet je niet in welk land de data zich bevindt. Ik denk dat er wel nog wat verbetering naar de wetgeving mogelijk is.**

Is er een procedure bij een beveiligingsincident?

We hebben een **security incident process**. Waarbij wanneer een incident gemeld wordt, dat triggert dan een proces. Nu zal ik het even in grote lijnen schetsen. Ieder incident krijgt een oordeel dat afhangt van de initiële impact van het incident. Bleef het beperkt tot één klant, heeft het dataverlies tot gevolg gehad, is het gerelateerd aan iets publiek (hacking). Aan de hand daarvan zal het proces geïnitieerd worden waarbij de focus ligt op de containment. Namelijk hoe kan ik het incident verhelpen. Als er bijvoorbeeld een bepaalde machine gehackt wordt, zal die uit het netwerk gehaald worden. De nodige acties zullen gedaan worden om de machine terug als normaal op te richten. Daarna gebeurt er een root cause analyse die nagaat hoe het incident is kunnen gebeuren en kunnen er collectieve maatregelen genomen worden om ervoor te zorgen dat het incident of dergelijke incidenten zich in de toekomst niet meer kunnen voordoen.

Moet er geweten worden wat er in de cloud gestoken wordt?

Ja en neen. **Het hangt er een beetje vanaf**. We hebben een aantal klanten die heel hun infrastructuur outsourcen naar Cegeka. Voor die klanten weten we wat er in hun private cloud zit. Maar we hebben ook een hosting afdeling die een aantal andere IT-bedrijven als klant hebben die op zich ook data van hun klanten erop gaat zetten en **daarbij weten we vaak niet wat er op die systemen zit**.

Het te snel delen van administratorpaswoorden komt dat ook voor bij u?

Ja. In het verleden was het zo dat wachtwoorden per klantenteams beheerd werden. Dat willen we **nu centraal gaan aanpakken**. **Om de nodige controle**

te zetten op generieke administratoraccounts. Dat is ook wel heel belangrijk.

Gebeurt er ook encryptie?

Dat is eigenlijk ook weer heel klantspecifiek. Je hebt klanten die dat niet vereisen, je hebt klanten die dat wel vereisen. Dat kan op alle niveaus voorzien worden. **Zowel op netwerkniveau (transportniveau) als op storageniveau (opslag van gegevens)**.

Met welke Amerikaanse wetgevingen bent u nog bekend?

Privacy Act van 1974 US zegt mij wel iets. **HIPAA** dat is voor healthcare, daar ben ik ook mee bekend. E-Government Act US zegt mij niets. American Recovery and Reinvestment act zegt mij niets. Stored communication act zegt mij niets. Wij komen **niet veel in aanraking met Amerikaanse bedrijven**. Dat is niet relevant voor ons. De Europese wetgeving is al complex genoeg.

Is de wetgeving in Europa strenger als Amerika?

Zeker! De **Amerikaanse privacywetgeving is eigenlijk een lachertje**. **Europa heeft de striktste privacywetgeving ter wereld**. In Europa zijn er nog verschillen. Je hebt de Europese directive en ieder land moet dat dan implementeren in zijn eigen privacywet. Maar er zijn landen die ervoor gekozen hebben om verder te gaan dan de Europese wetgeving. Zoals bijvoorbeeld **Spanje en Italië die zijn gekend om hun zeer strenge privacywetgeving, die zijn nog strenger als de algemene Europese directive**.

De wetgeving waarmee wij vooral worden geconfronteerd is de Belgische privacywetgeving. Wat we daar dikwijls nog bij zien, is dat heel veel bedrijven er niet van op de hoogte zijn of niet goed volgen. Wij moeten klanten veelal op de hoogte brengen van de desbetreffende privacywetgeving.

Bent u bekend met ISO-norm 27001?

Je hebt de **ISO 27000 serie**. Bij Cegeka proberen we ook die richtlijnen te volgen. We zijn nog niet gecertificeerd volgens die normen maar dat is wel onze ambitie om in de loop van volgend jaar te behalen.

Het certificeren aan de ISO-normen is een manier om aan te tonen dat een **onafhankelijke instantie ons is komen auditen en hier een certificaat voor aflevert**. Enkel de **27001** is diegene uit de reeks van standaarden die je kan certifiëren. Dat is **eigenlijk een heel dun document**. Veel mensen denken dat daar instaat van jij moet je beveiliging zo doen maar dat is eigenlijk niet waar. Ze zeggen eigenlijk alleen maar de principes en het proces dat je moet voorzien is belangrijk voor je certificatie. Als je je wil certificeren volgens de ISO-norm moet je als bedrijf een **ISMS** maken. ISMS staat voor **Information Security Management System** dat is eigenlijk je beheersysteem van informatiebeveiliging. Als je je als bedrijf wil certificeren moet je aantonen dat je

die **ISMS uitgedacht hebt**, dat ISMS is gebaseerd op een risico-analyse. Dat je eerst gaat kijken naar risico's en dat je aan de hand daarvan gaat kijken welke beheersmaatregelen je hebt ingesteld. Dan ga je die ISMS moeten implementeren in de organisatie. Vervolgens moet je die gaan meten. Namelijk wordt dat ISMS nageleefd, kent iedereen dat en dergelijke meer. Verder moet je jaarlijks een review doen, namelijk zijn er verbeteracties mogelijk. Aan de hand van die verbeteracties moeten opnieuw verbeteringen toegevoegd worden. **Je krijgt een model van continue verbetering**. Je moet aan een **auditor aantonen dat je die fasen volgt om ISO 27001 gecertificeerd te geraken**. **Maar zoals je al hoort gaat dat over dat proces en niet over de beveiliging**. Je kan een bedrijf hebben dat een zeer sterke beveiliging heeft en je kan een ander bedrijf hebben dat eigenlijk een zeer lichte beveiliging heeft en die kunnen allebei ISO 27001 gecertificeerd zijn. **Met dat certificaat kan je het niveau van beveiliging niet gaan afleiden. Je kan enkel afleiden dat je op een procesmatige manier omgaat met die informatie.**

De ISO 27002 standaard is een soort van hulpmiddel om ISO 27001 te gaan implementeren. Dat kan je zien als een **soort van kookboek** met veel controles in: 'dit zijn mogelijke maatregelen die je kan nemen op het gebied van beheer van wachtwoorden, op het niveau van fysieke beveiliging en dergelijke meer'. Maar je moet je er niet aan houden. Dat zijn eerder een soort van richtlijnen die je als inspiratie kan gebruiken om controles te gaan definiëren. Die **ISO-normen zijn al veel ouder als de cloud**. **De ISO-normen zijn niet gemaakt specifiek richting cloud computing.** ***(een nieuw continue auditmodel voor cloud computing stel ik in deze masterproef zelf op)***.

ISO 27002 dat is een hele bundel. Dat gaat over hoe je risico assessments kunt doen; hoe het security policy moet uitzien; hoe je security moet gaan organiseren binnen uw bedrijf, namelijk welke rollen je er voor moet hebben, je gaat het als bedrijf moeten gaan definiëren; het beheer van je assets; stukje over human resources; fysieke beveiliging van datacenters; communicatie, back-ups nemen; toegangscontrole; continuïteit. **Die dingen ga je echter niet in de wetgeving gaan terugvinden.**

Hebt u nog verdere opmerkingen?

De risico's van cloud zijn **typisch het feit dat het Internet facing is**. Heel hoop risico's vanuit al die hackinggroepen en bewegingen en dergelijke meer.

Hebt u nog referenties binnen de sector?

Tot nu toe niet.

6.4 CEO Eurosys – IT Solutions – Mark Lens

Als vierde contactpersoon heb ik Mark Lens. Mark Lens is de CEO van Eurosys – IT solutions. Als particulier en bedrijf kan u terecht bij Eurosys – IT solutions groep voor al de desbetreffende IT-noden van A tot Z. De groep bestaat uit 8 Limburgse winkels, de Eurosys Business Centers te Houthalen en Halle en het

softwarebedrijf IT Solutions. 'Een totaalservice aanbieden', zo luidt het uitgangspunt voor de gehele Eurosys – IT solutions groep.

Hierna volgt een transcriptie van dit interview. Het interview duurde 30 minuten en 14 seconden en vond plaats in de hoofdgebouwen van Eurosys te Houthalen op 30 november 2012. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor beide partijen. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Hoe komt u in aanraking met cloud computing?

Veel bedrijven hadden in het **verleden** hun systemen klassiek **on-premise** in het eigen bedrijf staan. We zijn **anderhalf jaar geleden** gestart **om migratie naar cloud te doen**. Eén van de gemakkelijkste manieren om naar cloud te emigereren is de mail. De mail is een **commodity**. Je hebt er een aantal spelers op. Je hebt Microsoft die in de cloud zit, je hebt Google die in de cloud zit. We hebben een heel deel bedrijven omgezet naar **Google Mail** toe. Bij **on-premise was het gekenmerkt met heel wat problemen** met klanten die mailgerelateerd ofwel back-up gerelateerd waren ofwel een combinatie van de twee. Als de Internetlijn uitlag konden ze niet meer werken en er **was een hoge onzekerheid binnen bedrijven**. De eerste fase die we gedaan hadden was de mail overbrengen naar de cloud. Dat is goedkoop, dat is **commodity**, dat kost niet veel. Voor Google kost dat veertig euro per jaar voor een volledige mailbox van een gebruiker in de cloud te zetten met vijfentwintig Gb opslagcapaciteit. Klanten kunnen op een heel eenvoudige manier overgaan naar de cloud. Ze kunnen **nog altijd hun outlook blijven gebruiken** als ze dat willen of ze kunnen de **browserinterface gaan gebruiken**. We hebben op een jaar tijd op dit moment ongeveer 250 bedrijven overgezet en zo een 6000/7000 gebruikers naar de cloud overgebracht met hun mail. Dat is één stap die je kan doen. De tweede stap die we heel eenvoudig gedaan hebben het afgelopen jaar naar cloud brengen is het **faxverhaal**. Op een eenvoudige manier wordt een nummer gekoppeld met de cloud waarbij je een fax ontvangt op een **cloud-achtige omgeving**. De fax wordt afgeleverd naar de beeldbox naar de mensen toe in PDF-formaat. Dat was een tweede stap die wij gedaan hebben. Nu zijn we met fase drie bezig.

Wij **bieden** als het ware **een applicatie van een andere cloud provider aan** aan de klant. Wij **verdelen applicaties**. Wij bouwen daar bovenop eigen add-ons. Maar we hebben zelf geen eigen cloud applicaties die wij op die manier gaan ter beschikking stellen.

Wat zijn de belangrijkste voordelen van cloud computing?

Heel belangrijk voordeel is dat het zaken zijn die **commodity** zijn waar je **geen zorgen meer voor hebt** die geoutsourced worden. Mail die altijd blijft werken. Er is een **enorme bedrijfszekerheid** op het gebied van mail. De cloud is enorm

scalable. Als je vandaag honderd mensen moet bijzetten op een mailbox op een goed uur is dat goed en wel gebeurd. Je **moet niet zelf investeren in infrastructuur**. Je betaalt enkel voor het gebruik. Heb je een maand minder mensen, moet je minder betalen.

Wat zijn de belangrijkste nadelen van cloud computing?

Cloud is een soort modewoord geworden. Maar als we vandaag applicaties in de cloud gaan beheren, moeten we goed **opletten met welke partijen we in zee gaan om de applicaties in de cloud te gaan onderbrengen**. Als die partijen allemaal zelf het beheer gaan doen, wie zegt dat die even stabiel en even goed gaan zijn. Bij Google weet iedereen dat het goed gaat blijven werken. **Er zit immers een heel groot bedrijf achter.**

Je moet heel specifiek gaan kijken welke **applicatie er zich toe leent** om in de cloud te worden opgenomen. Welke applicatie is **genoeg gescaled**, welke applicatie geeft **voldoende veiligheid**. Als je aan al die parameters voldoet dan zouden wij adviseren om met die applicatie naar de cloud te gaan en dan het kostenplaatsje in het oog houden. Als het er niet aan voldoet moet je er zeker niet aan beginnen. **Niet alles zomaar naar de cloud brengen**. **Goed opletten per applicatie** om naar de cloud te brengen.

Een ander groot nadeel aan de cloud is dat er heel wat applicaties in de cloud zijn waarvan je niet meer weet welke partij erachter zit. Is dat een bedrijf met honderd werknemers, duizend werknemers of is dat een bedrijf met ene man en een paardenkop. Hoe veilig zijn die applicaties dan en hoe bedrijfszeker zijn die applicaties. **Het is maar bedrijfszeker als het bedrijf dat erachter staat**. De cloud wordt veel meer **anoniem**. Je **weet niet meer welke mensen er achter de producten zitten**. Dat is toch wel een punt waar op gelet moet worden.

Een volgend groot nadeel aan de cloud is als de **Internetlijn uitligt dan heb je ook geen beschikbaarheid**. Vandaag de dag in België is de kans dat Internetlijnen uitliggen zeer laag. Je hebt ook mogelijk een andere oplossing. Je kan gaan via een andere operator. Je kan gaan via je Proximus of Mobistar kaartje. Er zijn wel wat alternatieven voor. Maar dat moet je wel in het achterhoofd houden. Cloud is over het algemeen **wel iets duurder** om klassieke applicaties die eerst on-premise waren in de cloud te gaan zetten. Dat prijskaartje is iets duurder, maar dat **geeft je een grotere flexibiliteit**.

Welke privacy risico's zijn er bij het gebruik van cloud computing?

Dat hangt af van de applicatie waarmee je in zee gaat. Bij Google Mail is het zodanig afgeschermd. Er zijn verschillende labels die aantonen wat security levels ze hebben. Bij Google heb je daar weinig risico's mee. Maar als je andere applicaties van andere bedrijven gaat installeren, is het wel belangrijk dat je van die bedrijven weet van **welke level van security, welke SLA ze hebben, aan welke normen voldoen ze. Die normen kan je opvragen. Er zijn allerhande regels voor**.

Welke beveiligingsrisico's treden er op?

Komt eigenlijk een beetje op het zelfde neer. Het heeft **te maken met de desbetreffende applicatie**. De mensen die de desbetreffende applicatie maken, die bepalen het risicoprofiel van de applicatie. Je moet heel goed afstemmen welke labels en welke veiligheid ze hebben. Ook een groot risico zijn de mensen zelf. Als je in de cloud zit, is het makkelijker om zaken te gaan delen en om zaken te mee te nemen. Het maakt het gemakkelijker om informatie te verspreiden op een heel korte termijn. Er moet zeker een goede policy in de onderneming opgesteld worden **hoe je het gaat afschermen**.

Het is belangrijk dat je met **goede bedrijven samenwerkt**, zeker voor bedrijfskritische data.

De **normen die grote bedrijven hanteren zijn veelal veel groter**.

Sony is vroeger gehackt geweest met zijn gameconsole. Als je zou weten welke individuele hackings er gebeuren, die zijn veel groter als die die in de cloud gebeuren. Omdat bij de **cloud** er een **veel grotere security en veel grotere manpower achter zit**. Hacking kan natuurlijk altijd gebeuren.

Wordt er rekening mee gehouden dat gegevens makkelijk naar een andere cloud kunnen overgedragen worden?

Dat hangt **puur van de applicatie af**. Als je je mail hebt van **Google** dan kan je je **mailbox exporteren en inlezen ergens anders** in een andere applicatie. **Salesforce** is **ook** een heel gekende cloud applicatie. Daar kan je ook de zaken exporteren en inlezen.

Moet u zich aan bepaalde wetgeving houden? Hanteert u ISO-normen?

Privacywetgeving is zeker een wetgeving waar men rekening mee moet houden. Bij Facebook en Google moet je zelf echter aanduiden dat ze alle gegevens mogen gebruiken. In welke mate is er dan nog privacy? Er is wel **Europese wetgeving die er aankomt**. We zijn toch wel allemaal een beetje bevreesd van wat er allemaal gedaan wordt met de data die iedereen in de cloud heeft staan. Het digitale spoor dat je achterlaat als je gaat surfen. Daar kunnen ze kenmerken aan koppelen dat het niet mooi is om te zien. Dat is toch wel even opletten.

Welke laag biedt u aan IaaS, PaaS of SaaS?

We bieden SaaS aan. We doen ook IaaS. Daar draait een Microsoft, Citrix omgeving op en VM-ware virtualisatie die **al de nodige afscherming hebben**. We werken met wereldspelers en die hebben die afscherming ter beschikking. Wat doen we met de cloud: we gaan de mensen **testen op virtualisatie**, **testen op streaming**, we bouwen **private networks** dat meerdere kantoren met elkaar verbonden worden en afgescheiden op het Internet zodat ze een

privaat netwerk hebben, we gebruiken **firewalls**, de verbindingen gebeuren via **https**.

Hoe ziet u de wetgeving over heel de wereld evolueren?

Ik denk dat er nood is aan **een internationaal verdrag**. Ik denk dat het niet verkeerd is dat er een nieuwere internationale wetgeving komt voor de bescherming van de **privacy**. Als mensen ergens iets op Internet achterlaten moet er betere bescherming komen. **Ik verwacht dat die wetgevingen zullen evolueren.** Europa is nu bezig met de wetgeving, Nederland is er al een stukje verder in. Dat men eerst moet toelaten om cookies te accepteren voor dat deze gebruikt mogen worden. In België is men er ook verder naar aan het evolueren. Cookies kunnen een spoor achterlaten op de PC waarmee men alles kan gaan monitoren wat je op het Internet doet. Men kan alles beginnen traceren aan de hand van de cookies die je achterlaat. Het statement 'alle cookies moeten weg', dat is niet mogelijk. Als je soms bepaalde log-ingegevens achterlaat wil je immers dat die automatisch opgeslagen worden.

In Amerika **zijn ze veel minder streng over de privacywetgeving dan in Europa**. Ik denk dat het **goed is als men er strenger in wordt**. Ik denk dat ze ermee bezig zijn om de privacy beter te beschermen van de gebruikers.

Er wordt ook als maar meer en meer data gecapteerd. Google heeft met die auto's allemaal rondgereden om streetview te maken. Ze komen nu ook met een spel uit. Dan kan je live in de straten gaan spelen. Vanuit je Android telefoon kun je gewoon door de kaart wandelen en dan kun je opdrachten uitvoeren. Een spel dat je live zelf aan het spelen bent. Alles wat je doet wordt wel opgeslagen, uw wandelpaden, etc. Heel grote bedrijven Apple, Microsoft, Google, Facebook capteren **enorm veel data op dit moment. Dat daar een betere regelgeving voor komt daar ben ik een groot voorstander voor**.

Wij **ontwikkelen zelf geen cloud applicaties,** daarom moeten we ons niet **houden aan ISO 27001/27002 houden**. ISO zegt echter niets over de kwaliteit van het product echter enkel over hoe het proces om iets te maken moet geïmplementeerd zijn. Om ISO te implementeren daar is echter heel wat werk aan en dat is geen sinecure. **Het is echter geen garantie dat als je ISO gecertificeerd bent, dat je goede producten aflevert**. Wij bouwen echter niet tot die laatste layer niveau om daarvoor ISO gecertificeerd te moeten zijn.

Doen jullie aan encryptie?

Encryptie gebeurt automatisch via het **https- protocol**. Alle klanten die extern iets toegankelijk willen maken, gebruiken encryptie.

Hebben jullie ook een datacenter?

We hebben hier een **datacenter in Houthalen en een datacenter in Brussel**. Het datacenter in **Brussel is cloud** gerelateerd.

Hoe wordt het datacenter in Brussel beveiligd?

Er is **camerabewaking, zuurstof wordt enorm verlaagd** in de rekken voor als er brand zou zijn zodat het zo weinig mogelijk zou kunnen uitdijnen. Er wordt op **een speciale manier geblust** zodat de apparatuur geen schade loopt, **ontdubbeling van airco**, **ontdubbeling van stroom**, als de stroom volledig uitvalt dan kan het datacenter toch nog verder gaan op batterijen.

Er zijn echter ook **cloud applicaties die niet via ons datacenter werken maar via een derde partij**. Wij **verdelen bijvoorbeeld Google applicaties**. Google voldoet aan die desbetreffende normen. Wij verdelen zowel applicaties van bijvoorbeeld derden, bijvoorbeeld Google, als eigen applicaties.

We stellen een **VPN verbinding** voor, dit is een punt tot punt verbinding, waarmee de applicaties kunnen geraadpleegd worden. Een **VPN-tunnel** is beveiligd en geëncrypteerd. Als er van buitenaf toegang moet verkregen worden, wordt er met Citrix gewerkt, dit werkt met **https**. Er kan ook nog met een verdere authenticatie gewerkt worden en dit zijn **tokens**. Tokens zijn een reeks cijfers of karakters die niet zomaar te verzinnen zijn. Iemand die in het bezit is van token kan het dus niet verzonnen hebben en bewijst daarmee het token te hebben. Het hoogste niveau is het afschermen met tokens.

Heeft u nog verdere opmerkingen?

Er is een **enorme shift aan het gebeuren naar cloud toe**. Cloud is een modewoord. We moeten opletten ons niet te laten meeleiden door modewoorden en tendensen. Want dan nemen mensen soms verkeerde beslissingen. **Niet zomaar stellen om alles in de cloud te gaan injecteren**, dat zou een totaal verkeerde beslissing zijn. Er moet echt gekeken worden naar wat het bedrijf gebruikt, wat het bedrijf nodig heeft. Er zijn heel veel applicaties die interessant zijn voor de cloud maar ook heel wat applicaties die niet interessant zijn voor de cloud.

Zaken die **commodity** zijn die moet men **gewoon overzetten op de cloud**, bijvoorbeeld mail. Iemand die vandaag mail nog lokaal zet, die verklaar ik gek. Er zijn mensen die hier veel gespecialiseerder in zijn. Fax is nog zoiets. **Zet zoiets gewoon in de cloud**. Bepaalde sales tools kan men in de cloud gaan zetten. CRM zet zoiets in de cloud. Commodity zeker omschakelen naar cloud.

Heeft u nog referenties binnen de sector?

Combell en **Adapti**. Daarnaast ook Jordens, **Jordens** is op zich een goed datacenter maar kan niet de snelheid garanderen die we nodig hebben op het gebied van datalijnen. Ons datacenter van Brussel kan ons veel betere datalijnen garanderen. **Cegeka** is nog een andere referentie. Cegeka kan echter ook niet de goede kwaliteit zoals ons datacenter van Brussel garanderen. Het voldoet niet aan dezelfde normering als in Brussel gehanteerd wordt.

6.5 IT & Telecommunicatieadvocaat Stibbe – Laurens Dauwe

Als vijfde contactpersoon heb ik dhr. Laurens Dauwe. Laurens Dauwe is sinds 2008 IT & Telecommunications advocaat bij Stibbe. Stibbe is een advocatenbureau dat gevestigd is in Brussel en zich richt op de internationale commerciële praktijk. In 2010 werd Stibbe verkozen tot 'Benelux Law Firm of the Year' tijdens de PLC Which Lawyer Awards. In 2011 werd Stibbe opnieuw verkozen tot 'Benelux Law Firm of the Year', ditmaal echter door The Lawyer European Awards. Stibbe is een 'full service' advocatenkantoor dat bestaat uit een groep specialisten die in teamverband een gepersonaliseerde dienstverlening aanbiedt. De wensen van elke cliënt zijn verschillend, daarom worden er ad hoc teams samengesteld om op maat gemaakte oplossingen uit te dokteren. Het bedrijf werd opgericht in 1911.

Hierna volgt een transcriptie van dit interview. Het interview duurde 46 minuten en 11 seconden en vond plaats in de gebouwen van Stibbe te Brussel op 6 december 2012. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor de geïnterviewde. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Hoe komt u in aanraking met cloud computing?

Ik ben **IT-advocaat**. Wij treden heel vaak op **voor klanten**, grote bedrijven. Meestal zijn dat klanten van **cloud services,** soms zijn dit ook **cloud providers**. We kennen dus **beide kanten van het spectrum**. Zeker **de laatste drie jaar krijgen we meer en meer vragen over cloud computing**. De meeste vragen zijn, als we aan de klantzijde zitten, **de risico's**. **Privacy is een heel belangrijk risico**. **Security is ook een heel belangrijk risico**. En dan operationeel gezien: als je de gegevens in de cloud zet, moet je natuurlijk ook een regeling treffen aangaande de toegang tot mijn gegevens en **wat gebeurt er op het einde van het contract?** Namelijk als je gegevens in de cloud zet dat je je gegevens op het einde van het contract ook terugkrijgt, zodat **je kan migreren naar een andere provider**. Dat is altijd heel belangrijk, maar wordt heel vaak over het hoofd gezien. Dat zijn zo een beetje de **main aspects of de main risks** die we tegenkomen. Wat dat je ook ziet, in de financiële sector bijvoorbeeld, ik heb vorige week de vraag gehad van een Belgische grootbank die gebruik wil maken van de Microsoft 365 services. De eerste vraag die ze hebben**, is het privacy compliant?** Tweede vraag die ze hebben: **wat omtrent de security?** En een ander punt en dat is ook heel belangrijk is, zeker als je met US-based suppliers werkt, **wat zijn de rechten van de US government?** Je weet bijvoorbeeld de **American Patriot Act**. Dat houdt concreet in dat in de **US Law enforcement agencies gerechtigd zijn om zichzelf toegang te verschaffen** tot infrastructuur die zich in de US bevindt. Zij kunnen die gegevens de facto opvragen. Zeker voor cloud service providers, die bewaren de gegevens van hun klanten en soms zijn dat wel heel interessante gegevens. Welbepaalde financiële data wordt gestored op servers, soms in de US. Als **de**

US based authorities daar toegang tot krijgen kan het **een serieus risico** inhouden voor onze klanten. Dat is iets wat we ten allen tijde proberen te vermijden. Dat is iets wat je in de **praktijk moet proberen af te dekken, contractueel.**

Wat zijn de belangrijkste voordelen van cloud computing?

Cloud computing heeft immens veel voordelen. Het heeft echter ook bepaalde nadelen. Maar als ik het globaal bekijk, moet ik toegeven dat **de nadelen niet opwegen ten op zichte van de voordelen**. Vroeger was het zo dat bedrijven alles in-house opsloegen. Ze sloegen al hun gegevens in-house op maar ze hadden wel een welbepaalde infrastructuurkost. Zij hadden capaciteit nodig, ze hadden servers nodig bijvoorbeeld. Server, oké, dat kost u een x-aantal duizend euro. Je hebt je datalijnen naar die servers, die heb je moeten betalen. Daarnaast heb je je maintenance, management van die servers, dat heeft ook een kostprijs. Je moet er mensen opzetten. Daarnaast moet je ook rekening houden dat op die servers software draait. Je hebt ook een licentiekost. Vroeger dumpte je jouw Oracle software op je eigen server. Je hebt een ERP-systeem bijvoorbeeld. Dat kost gigantisch veel geld. Je moet dat daarnaast allemaal kunnen managen. Als je naar een cloud service provider gaat die zegt gewoon dit is mijn oplossing en **you just pay-as-you-go**. Als je bijvoorbeeld een user-based licence hebt en je hebt duizend mensen die ervan gebruik maken, fine, dan neem je gewoon duizend user-based licences. Nu tijdens de economische crisis moeten er driehonderd ontslaan worden. In een traditioneel systeem betekent dat, je hebt een contract van vijf jaar voor duizend licenties. Dan moet je duizend licenties blijven betalen. Heel veel cloud provider zeggen, **kijk geen probleem, je ontslaat er driehonderd.** Dan pak je gewoon nog maar zevenhonderd licenties. Dus je kan als het ware je kost beter managen. Het **grootste voordeel is kostefficiëntie**. Dat is een heel belangrijk voordeel en er zijn heel wat klanten die zich dat nu ook beginnen te realiseren. Ook **availability van de data**, availability in de zin van **een gecentraliseerd systeem**. Vroeger moesten ze via het netwerk gaan om gegevens uit een database te halen. Nu is dat heel eenvoudig. **Ze loggen heel eenvoudig via hun device in.** Zelfs bijvoorbeeld met een ipad of whatever. Ze checken even, ze hebben de gegevens en het is gedaan. **Daar is een gigantisch groot voordeel** voor veel van die bedrijven en het is ook in veel bedrijven de **main driver om over te gaan op cloud computing.**

Welke risico's zijn er bij cloud computing?

In **hoofdzaak privacy risico's**. De **Belgische privacywetgeving**, privacy is eigenlijk Europees gereguleerd, die bepaalt dat indien u uw gegevens exporteert naar een land dat **geen adequate level of protection geeft dan moet je daar bepaalde maatregelen voor nemen**. Je hebt **in Europa een geharmoniseerd geheel** dat alle Europese landen en alle aanbieders in Europa die moeten **compliant zijn met de EU Data Protection Directive** en de lokale nationale reglementering. De **US biedt in principe niet het gepaste**

beschermingsniveau. Omdat er in het verleden een probleem is geweest, heeft men in de de Chamber of Commerce van de US het principe van '**Safe Harbor' gecreëerd**. Dit betekent dat bedrijven die een passend **beschermingsniveau bieden dat equivalent is aan dat van de EU** een **Safe Harbor compliant** verklaring krijgen. Dat betekent dus als je Safe Harbor compliant bent dan kan je als Europees bedrijf uw cloudgegevens opslaan in de US. Dus **privacy is één belangrijk risico**, je moet dat zeker managen. Er zijn andere modaliteiten buiten Safe Harbor, maar dat is specifiek voor de US. Andere modaliteiten zijn **binding corporate rules**. Ik weet niet of je dat in de praktijk al gehoord hebt. Wij hebben een binding corporate rules systeem toegepast voor British Petrol, BP. Stel dat je **een heel grote onderneming bent en je moet je gegevens transfereren naar de verschillende vestigingen**. Het zijn vestigingen in India, in Marokko dan moet je ook het gepaste beschermingsniveau bieden en dan kan je op het niveau van de hele groep **binding corporate rules opleggen**. Dat **betekent standaarden opleggen aan elke entiteit van de groep**. Die standaarden moeten **in één land in Europa ook geapproved worden**. In **België worden die geapproved door middel van een Koninklijk Besluit**. Natuurlijk dat is ook één van de problemen met cloud computing. Je hebt cloud services, je hebt er in de US. Je hebt ook aanbieders die 'following the sun' toepassen. Dat betekent dat ze serversystemen hebben staan in Bangalore, India. Ze hebben systemen staan in de US. Hun gegevens wordt een stuk opgeslaan in de US, een stuk opgeslaan in Bangalore bijvoorbeeld. Nu, je ziet al de verschillende landen, dat is een probleem. Als je **met verschillende entiteiten moet werken**, dan ga je best voor **binding corporate rules**. Elke entiteit van de groep moet zich akkoord verklaren met die specifieke regels en dan ben je ook in één keer afgedekt. **Ander alternatief is modal clauses**. Dit zijn **standaard contractuele clausules die worden opgelegd door de Europese Commissie**. Als je dat wil **toepassen op je groep**, dat wil zeggen dat je met elke entiteit van je groep zo een contract moet afsluiten. **Dat is een vrij omvangrijk werk.** Globaal genomen is privacy dus een substantieel risico. Een **tweede risico betreft securit,** dit **wordt heel vaak onderschat**. Hetgeen we vaak zien in contracten, is dat de supplier bepaalde security measures gaat implementeren. Hij zegt bijvoorbeeld van kijk ik ga een **adequate level van security waarborgen.** Ook de privacywetgeving vraagt ook om een zeker adequaat security level. Vaak wordt dat niet duidelijk gespecifieerd. **Wat is adequate security nu juist?** Mijn interpretatie van adequate security zal hoogstwaarschijnlijk verschillend zijn dan die van u. We stellen ook een toenemende referentie naar ISO-normen vast. Bijvoorbeeld ISO 27001. Maar een ISO-norm dat is leuk, maar een ISO-norm blijft een ISO-norm. **Dat is heel algemeen, heel vaag**. Die zeggen je moet operational security measures, organisational security measures en physical security measures opleggen. Dat kan gaan van het opleggen van access control door middel van badges. Dat kan organisational door bepaalde procedures op te leggen intern in de organisatie. Maar er is heel veel verwarring over. Als je echt **over heel gevoelige gegevens spreekt** die worden opgeslagen in een cloud, die toegankelijk is via een

webinterface, wat ik dan toch vaak vraag als ik aan de klantzijde sta, is **dat er toch wel wat meer wordt gedaan dan een referentie naar ISO 27001**. Dan kan het zijn dat ik vraag of regelmatig **penetration tests**, **vulnerability assessments** worden gedaan. Dat ze ook een duidelijke security policy toevoegen aan het contract. Dat zijn van die zaken die ik qua security toch vaak opvraag en dat moet ook regelmatig gerapporteerd worden. In de privacywet staat ook dat je **de verplichting hebt de security te garanderen van persoonsgegevens**. Stel nu dat je dat niet doet en je hebt een data breach dan heb je een serieus probleem. Dan heb je op **strafrechtelijk niveau een probleem**. Omdat jij als verantwoordelijke wettelijk aansprakelijk bent. Als wij als Stibbe gegevens op de cloud zetten en die cloud provider verliest die gegevens dan hebben wij een strafrechtelijke aansprakelijkheid, ook een **burgerrechtelijke aansprakelijkheid**. Dat betekent dat het openbaar ministerie tegen ons een claim kan indienen. En dat de virtuele burgers, onze klanten bijvoorbeeld, zeggen dat mijn dossier nu gekend is over heel België, die kunnen ook tegen ons een claim indienen. **Dat is een serieus risico dat je moet indekken door adequate measures of security te implementeren** in de organisatie. Natuurlijk andere risico's die we tegenkomen in de praktijk, juridisch gezien, is dat **veel cloud computing contracten eigenlijk niet zijn opgesteld zoals ze zijn moeten opgesteld**. Bijvoorbeeld Salesforce die hebben hun **eigen contractuele voorwaarden** die stipuleren uit dat enkel de wetgeving van de UK van toepassing is. Maar als consument is het moeilijk om te gaan procederen. Als je in de UK moet gaan procederen. Veel geluk, het gaat heel veel geld kosten. In de **praktijk is dat al een drempel om niet te gaan procederen**. Anderzijds zie je dat er liability, aansprakelijkheidsclausules instaan. Waarbij de **aansprakelijkheid wordt beperkt tot drie maanden servicing fees**. Als dat drie maanden servicing fees zijn en je moet bijvoorbeeld tachtig euro per maand betalen. Dat is 240 euro voor damages voor schade als je al je gegevens kwijt bent. Als je als kleine zelfstandige je volledige boekhouding kwijt bent, dat kost wel veel meer als die schamele 240 euro. Dan is er de mogelijkheid dat je zelf gaat onderhandelen. Maar je moet realistisch zijn. **Ten op zichte van grotere spelers is het moeilijk tegen te procederen.** Het **contract is een major risk**, **security is een major risk en privacy is een major risk**. Dat zijn **globaal genomen de drie belangrijkste risico's** die ik in de praktijk zie.

Hoe ziet u de wetgeving over heel de wereld evolueren?

Dat is moeilijk om twee redenen. Het zou de bedoeling zijn te gaan stemmen, gedurende het thans plaatsvindende congres in Dubai, om het **Internet te gaan reguleren door de VN**. Nu, je weet sowieso dat **dat niet gaat gebeuren**. **Internetregulering is gigantisch moeilijk**. In Europa globaal genomen bijvoorbeeld cloud reguleren dat lijkt mij in de praktijk ook heel moeilijk. Hoe zal cloud in de praktijk gereguleerd worden. Het **zal gereguleerd worden door diegene die de hoogste standaarden legt**. Qua cloud computing denk ik dat cloud providers de standaarden gaan opleggen en daar zijn ze trouwens ook mee

bezig **om de standaarden die in Europa gelden om die wereldwijd te implementeren**. Waarom? Europa is heel streng en je ziet het ook vanuit de klanten. Als er geen privacy compliance is dan gaan klanten gewoon niet naar de cloud migreren. **De cloud providers gaan zich in de toekomst aanpassen aan de Europese regelgeving**. De Europese **regelgeving qua privacy is momenteel heel vaag**. Nu, ik heb toevallig, en je mag het gerust hebben, er is een bijdrage geweest van Peter Hustings van de EU **Data Protection Supervisor over de verdere regulering van de cloud**. Eén van de voorstellen die op tafel liggen is om **specifieke clausules**, specifieke contractuele voorwaarden, **op te leggen voor het gebruik van cloud computing**. Waarom is dat? Ik heb gezegd privacy is een major risk, security is een major risk en consumer protection is een major risk. Vanuit Europa zien ze dat ook. In die context zeggen ze dat **het bestaande model niet altijd opgewassen is tegen nieuwe trends, zoals bijvoorbeeld cloud computing**. In die context zijn ze aan het **proberen om cloud computing te reguleren**. **Het is een poging tot**. Ik durf niet zo ver te gaan dat het zal gereguleerd worden. Ik denk eerlijk gezegd wel dat er na verloop van tijd **na x-aantal jaar een regulering van cloud computing zal komen**. Waarom? Omdat er te grote onduidelijkheid is. Een Belgische grootbank wil in zee gaan met Microsoft, Microsoft 365. Microsoft bijvoorbeeld heeft al problemen gehad. Ze zijn privacy compliant, maar het is nergens de facto geattesteerd. Het is nooit de facto bevestigd door een privacy commissie. Die banken zeggen van kijk als wij geen garantie, geen duidelijkheid hebben dat het **effectief privacy compliant is**, dan willen wij er niet mee in zee gaan. Wat zijn die grote cloud providers nu aan het doen? Die zijn naar onder meer privacy commisions in verschillende landen aan het vragen van **kijk dit is onze oplossing, voldoet dat aan uw vereisten in zake privacy?** Ik denk dat dat een **goede trend is en ook rechtzekerheid biedt voor de klanten die naar de cloud willen migreren**. Anders als je er niet honderd ten honderd zeker van bent, heb je een probleem als er iets voordoet ben jij als eerste aansprakelijk ten op zichte van je klanten. In die context vind ik dat wel een goede trend. Het lijkt me **nuttig vanuit Europa om duidelijke krijtlijnen uit te zetten waaraan cloud services moeten voldoen**. De **stap van de EU Data Protection Supervisor ik denk dat dat een stap in de goede richting is om duidelijkheid mee te scheppen.**

Is er een verschillend beveiligingsrisico voor de verschillende lagen? IaaS, PaaS, SaaS?

Dat is een heel interessante vraag. Dat is **een vraag die ik al regelmatig heb gekregen**. Stel nu dat je bijvoorbeeld alleen maar **infrastructuur aanbiedt**. Daar is **uw verantwoordelijkheid van aanbieder enkel beperkt tot de infrastructuur**. Als je service levert en je doet puur service management betekent van ik kijk is de CPU niet aan het vollopen met opdrachten. Moet ik een scriptje schrijven voor back-ups bijvoorbeeld? Dat kan je **doen maar je aansprakelijkheid is beperkt tot die specifieke laag**. Dat betekent dus ook als je puur IaaS zou leveren, dan moet je zorgen dat je beveiligingsmaatregelen

van toepassing zijn, **maar dat zijn dan meer fysieke beveiligingsmaatregelen**. Je gaat access controls in je datacenter implementeren, bijvoorbeeld badging. Alleen maar specifieke mensen mogen bijvoorbeeld toegang hebben tot je servers. Afscheiden tot een kooi. Fysieke scheiding van servers. **Uw level van security gaat anders zijn**. Je gaat geen vulnerability assessments of penetration tests moeten doen op puur IaaS. Dat zijn zaken die eigenlijk meer op applicatief niveau doet. **Hoe hoger je eigenlijk in uw laag gaat, hoe zwaarder de beveiligingsvereisten worden**. Uw **verplichtingen gaan veel ruimer zijn**, uw aansprakelijkheid gaat ook veel ruimer zijn. Dat is logisch natuurlijk. Het verschilt echt wel in de diensten die je aanlevert. Er is ook een onderscheiding op het juridisch niveau.

Moet er geweten worden wat er in de cloud gestoken wordt?

Veel cloud providers die **PaaS** leveren die **gaan ook wel weten welk type van data er kan ingepompt worden in hun systeem**. Natuurlijk als je bij wijze van spreke een Amazon ECM bent die **dan puur infrastructuurdiensten levert**. Die hebben een cluster van verschillende servers. Kijk je hebt een opdracht, pomp die opdracht maar in mijn systeem. **Wat dat er precies berekend wordt is hun zaak niet**. **Het enige wat zij zullen doen, is dat ze niet zouden aangesproken worden voor de content die wordt geprocessed op hun systeem. Dan gaan ze zeggen, je mag het niet gebruiken voor illegale doeleinden. Je mag er geen IP infringements en dergelijke meer mee doen**. **Wat dat er concreet in hun systeem draait dat interesseert die mensen niet meer**. Natuurlijk als je een Salesforce bent en je hebt een bepaald platform bijvoorbeeld dan ga je natuurlijk moeten zien welke types van gegevens binnenkomen in het systeem. Ik heb bijvoorbeeld een klant die **levert fleet management services**. Dat betekent dus voor heel grote bedrijven die een vloot van auto's hebben, zij kennen voordelen van alle aard toe aan hun werknemers. Bijvoorbeeld een auto, een tankkaart en dergelijke meer. Er bestaat cloud software waarmee je die voordelen berekent. Natuurlijk, cloud software dat is een engine. Dit is puur een applicatie waarin data ingepompt wordt. Het voordeel en dergelijke meer wordt dan berekend door die software en dan krijgt men een output. Tuurlijk wat gaat die cloud provider zeggen in ons geval. Hij gaat eerst zeggen **ik wil weten wat voor soort data er binnen komt**. Jij als klant moet wel zorgen dat die data in het juiste formaat bij mij binnenkomt. Want als dat in het **verkeerde formaat binnenkomt** dan **geldt het principe garbage in garabage out**. De cloud provider heeft geen aansprakelijkheid voor de data die eruit komt en die erin gaat. In die context **is het belangrijk om te weten van welke data erin gaat**. Maar dat hangt er natuurlijk af van het soort platform dat je aanbiedt. **PaaS hier is dat van belang. IaaS hier is het iets minder van belang.**

Is de privacywetgeving in Amerika minder streng als in Europa?

Ik heb heel veel **US based clients**. Bij hun **privacy is van 'what is the concern'. Het eerste wat die zeggen is 'privacy that's not an issue'**. Voor

hen is dat geen issue omdat **het concept van privacy totaal anders is**. Bij hun is **privacy een goed dat te koop is**. Bij ons in Europa is privacy een grondrecht. Dat is ook gewaarborgd door **Artikel 8 van de Europese wet van de rechten van de mens.** Dat is een grondrecht. Natuurlijk de perceptie is er totaal anders in. Zelf binnen Europa is de perceptie totaal anders. De perceptie van privacy in Duitsland is bijvoorbeeld anders dan de perceptie van privacy in België. **Duitsland is veel strenger**. In de **US trekken mensen het zich echt niet aan**. Ik heb een klant gehad die een heel grote aanbieder van zoekdiensten is, die hebben een major privacy risk gehad. Echt een serieus privacy risk. Het eerst wat die zeiden **privacy dat is toch geen issue**. Tot op het moment dat de **privacy commissie besloot bij hen binnen te vallen in de Belgische vestiging**. Toen werd er een strafklacht ingediend**. Toen begonnen alle belletjes plots te rinkelen**. Waarom is dat? Je moet het eens indenken. In de US als US based company, je bent beursgenoteerd en je moet altijd je kwartaalresultaten neerleggen. Maar **daarin moet je ook opnemen dat er een strafklacht werd ingediend tegen uw onderneming**. Plus het punt is in België heb je zoiets van dubbele aansprakelijkheid. Soms kan het zijn dat je de bestuurders van een onderneming aansprakelijk kan stellen. Jongens, in België is het openbaar ministerie serieus moeilijk aan het doen dus het kan wel eens zijn dat we strafrechtelijk veroordeeld worden. Zeker op het moment als ze dat realiseren **schiet iedereen wakker en is het alle hens aan dek om te zorgen dat dat privacy risico ingedekt wordt**. Privacy is voor **hen geen major issue**. Ze **gebruiken het als het hun uitkomt**. Als het **hun niet uitkomt dan is het minor risk**. Ik heb twee weken geleden nog hetzelfde meegemaakt op een Amerikaans bedrijf waar ze ook iets zeiden van een **minor risk**. Er was fraude gepleegd in een Belgische vestiging en ze wouden al hun gegevens van werknemers controleren. Ze wouden eraan beginnen. **Tot op het moment dat ze op de hoogte gebracht werden van privacy. Initieel liggen ze er echt niet van wakker.**

Komt u de volgende wetten tegen?

Privacy Act US komen wij soms tegen, maar stelt niet veel voor. E-government act ook niet. **HIPAA, ja die kom ik wel tegen.** American recovery and reinvestment act kom ik niet tegen. **Artikel 8 95/46, ja dat is de Data Protection Directive**. Dat is eigenlijk het kader voor verwerking van persoonsgegevens in Europa. Als het gaat over verwerking van persoonsgegevens is dat eigenlijk de belangrijkste richtlijn. Je hebt **ook de E-privacy Directive**. Deze directive, op een Europees niveau, is de **meest gebruikte directive bij telecommunicatie**. Maar deze is niet zo belangrijk als de Data Protection Directive. De E-privacy directive **regelt bijvoorbeeld het gebruik van cookies**. Dat is recent ook gewijzigd geweest. Globaal genomen, is dat echt het kader. Dan heb je **Artikel 8 EVRM** (**Europees verdrag van de rechten van de mens)**. Dat is het artikel dat stelt dat iedereen het recht heeft op bescherming van zijn privé-leven, zijn gezinsleven en zijn correspondentie. Dat is het algemene kader eigenlijk, grondrechtelijk gezien. Het is meer dan

alleen bescherming van privacy bij het betrekken van computers. Het is ruimer. **Richtlijn 2002/58 kom ik ook vaak tegen. Dat is de E-privacy directive waar ik net over sprak**. Die is van toepassing op aanbieders van elektronische communicatie diensten. In principe als je het heel restrictief interpreteert, zo moet het eigenlijk ook geïnterpreteerd worden, is het zo dat die verplichting van toepassing is op **telecomoperatoren**. Omdat die privacy directive kadert binnen de zogenaamde telecom-package. Dus een telecomoperator als die een breach heeft op zijn netwerk dan moet die dat melden aan BPT, de regulator voor telecom. Vooral in België heb je een beetje een misvatting over het toepassingsgebied van die bepaling. Die verplichting van een **data breach notification of security breach notification** die wordt ook opgelegd in de **nieuwe privacy verordering welke de Europese wetgeving 95/46 gaat wijzigen**, vervangen, maar die is nog niet in werking getreden. Er is nog geen volledig akkoord over. Maar de **data breach notification zal een van de belangrijkste verplichtingen worden** onder de **nieuwe verordering**. Dat betekent dus als uw cloud provider een security leak of een data leak vaststelt dan moet hij dat notifiëren aan de privacy autoriteiten en als er een user impact is dan moet hij dat ook aan het publiek notifiëren.

Heeft u nog verdere opmerkingen?

Ik denk dat **cloud computing een nieuwe trend is** die **echt wel belangrijk is**. Maar je moet de **trend ook niet overschatten**. Cloud computing heeft een **zekere maturiteit**. Maar het **staat nog niet honderd ten honderd op punt**. Er is **nog te veel misvatting over bepaalde aspecten van cloud computing**. Te **weinig kennis** van klanten **over privacy**. Ook te weinig kennis van risico's die het met zich mee brengt. Het geeft zeker heel grote voordelen. **Cost-savings** is een heel groot voordeel ervan. **Flexibiliteit** is ook een heel groot voordeel ervan. Maar als je de keuze moet maken hierover, tussen de voordelen en de nadelen dan moet je ook **echt wel rekening houden met de nadelen en de bijhorende risico's**. Je moet ook echt zien **qua security, qua privacy**. Je moet ook zien **dat je nooit in een lock-in terechtkomt**. Als je niet betaalt, kan je provider de access afsluiten en kan het zijn **dat je zo geen toegang meer hebt tot je data**. Dat leidt tot discontinuïteit van de onderneming. Dat zijn zaken waar je echt voor moet zorgen en echt rekening mee moet houden. Specifiek voor cloud providers in de public sector kan dat ook een probleempunt zijn. **Bepaalde landen laten bijvoorbeeld niet toe dat overheidsgegevens worden gehost binnen hun eigen territorium**. In Nederland is dat een issue, in Duitsland is dat een issue. Cloud providers moeten daar rekening mee houden. Een laatste punt is dat **cloud providers uw gegevens gebruiken voor andere doeleinden**. Google is daar een voorbeeld van. Die hebben in het verleden een issue gehad met name omdat zij op hun Google Docs en Gmail de **content half aan het filteren waren zonder toestemming van de gebruikers**. En dat ze op basis daarvan aan target advertising deden. Dat is uiteraard **niet toegelaten onder privacy recht**. Je moet gegevens altijd **verwerken voor een welbepaald doeleinde**. Als je zegt ik doe het voor het ter beschikking van

cloud diensten voor jouw, dan **conflicteert dat met het doel voor target advertising**. Je hebt een onderscheid **tussen de echt mature providers**. Microsoft is een voorbeeld daarvan. Salesforce is daar ook een voorbeeld van. Maar je hebt ook **kleinere providers die niet goed weten waar ze mee bezig zijn en die toch nog wat moeten groeien.**

Hebt u nog enkele referenties binnen de sector?

Ik zal die per mail nog verder doorsturen. Ik heb zowel aan supplier zijde kennissen als aan de user kant. De supplier zijde die gaan elkaar wel veelal tegenspreken.

6.6 Directeur Microsoft Innovation Center Vlaanderen VZW – Peter Dedrij

Als zesde contactpersoon interviewde ik Peter Dedrij. Peter Dedrij is sinds maart 2012 directeur van het Microsoft Innovation Center Vlaanderen VZW. Deze VZW heeft als doel om de ontwikkeling van de regio Vlaanderen te stimuleren op het vlak van informatie- en communicatietechnologie (ICT) bij prioriteit in het domein van de welzijns- en zorgsector.

Hierna volgt een transcriptie van dit interview. Het interview duurde 29 minuten en 31 seconden en werd uitgevoerd in de gebouwen van het Microsoft Innovation Center Vlaanderen VZW te Genk op 11 februari 2013. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor beide partijen. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Hoe komt u in aanraking met cloud computing?

Enerzijds omdat wij een **leverancier** zijn van oplossingen die voor een stuk gebaseerd zijn op **cloud computing**. Cloud computing is **echter een heel ruim begrip** en vandaag wordt er veel gegoocheld met dit begrip zonder dat de betekenis ervan duidelijk is. Eigenlijk deden bedrijven een **soort van cloud computing al veel langer**. Als je data outsourcet van een datacenter, al staat dat datacenter in België, dit is reeds een vorm van cloud computing. Er zijn inderdaad **verschillende mogelijkheden**. Ofwel ga je naar een soort **private cloud**. Een stukje cloud dat voor u voorzien is. Ofwel ga je naar een **public cloud** provider en daar zijn er enkele van waarvan Microsoft ook één is. Hier ga je kunnen genieten van **nog grotere schaalvoordelen**. Het wordt als het ware een hostingplatform dat voor de hele wereld wordt opengezet. Daar heb je verschillende nuances in. Je kan perfect een **combinatie maken** van de verschillende implementatiewijzen. Bepaalde stukken data hou je on-site. Je gaat bepaalde dingen naar een lokale host/private cloud hosten en andere minder kritische data naar een public cloud outsourcen. Ik denk dat het vandaag de dag vooral een 'en-en'-verhaal is. Voor kleinere bedrijven is het veelal eenvoudiger alles naar een public cloud te brengen. **Grotere bedrijven** gaan echter **een stuk van de data bij zich houden**, **andere minder kritische data** gaat dan

naar een public cloud worden geoutsourced. Zo kan er gebruik gemaakt worden van de specifieke voordelen van de verschillende vormen die er zijn. Natuurlijk rijst de vraag **hoe je al die data met elkaar gaat moeten integreren**, opdat het een stukje transparanter wordt. Dat het **als het ware één geheel wordt waarmee je kan werken**, dat is één van de grote uitdagingen vandaag de dag. Het is belangrijk dat je juist weet waarover het gaat. Cloud computing is een **heel breed begrip**. Daarom **moet je goed kijken of het gaat over private, public of hybride systemen**.

Wat zijn volgens u de belangrijkste voordelen van cloud computing?

Eigenlijk kan je dat het best gaan analyseren, naar analogie wat er gebeurt met water. Vroeger had ieder huis zijn eigen waterput en dat kostte een hoop geld om een waterput te gaan boren, dus diegene die er zelf geen konden boren gingen lokaal in hun dorp aan de pomp water halen. Eigenlijk is het hetzelfde verhaal met cloud computing. In plaats van dat iedereen zijn eigen serverracks gaat installeren, zijn er **bepaalde bedrijven en organisaties,** waaronder Microsoft die **infrastructuur gaan opzetten** om die **basis die ter beschikking wordt gesteld** om die heel **kostefficiënt** met alle beveiligingen en alles er op en eraan ter beschikking te stellen van de wereld als je het zo wil noemen. Hierdoor kan een **bedrijf** zich **meer bezighouden met zijn specifieke business** en moet het zich niet meer bezighouden met het feit of die server nu draait of niet, hoe zit het met mijn security, disaster en recovery scenario's en zo verder. Zodat een bedrijf zich **kan gaan bezighouden met wat er echt toe doet voor het bedrijf**. Hoe IT de business kan enablen eerder dan de vraag of mijn infrastructuur draait en de investeringen die daar mee te maken hebben. Tweede bijkomend punt is natuurlijk dat als je zelf een datacenter uitbaat dat je zelf volledig voor de kosten moet gaan opdraaien, of je dat datacenter nu volledig gebruikt 100 % of je gebruikt dat 20 %. Dikwijls zie je in datacenters in bedrijven dat er maar **bepaalde gedeeltes gebruikt worden**. Je kan dus onmogelijk gaan schalen. Stel, je hebt een marketingcampagne en je voorziet daarvoor een website waar ineens heel veel verkeer op die website komt, dan moet je server daarop voorzien zijn. Als je naar een public cloud gaat outsourcen dan zie je dat **dat eenvoudiger mee kan schalen met de behoefte**. Heb je weinig nodig, betaal je weinig. Heb je veel nodig of immens veel nodig, **die cloud schaalt mee met je behoefte**. Je **factuur schaalt mee met de behoefte** wat een voordeel is voor het bedrijf. Wat je ook ziet is dat vooral voor **kleinere bedrijven** vandaag **een infrastructuur mogelijk** is die vroeger enkel weggelegd was voor heel grote bedrijven. Als je spreekt over SaaS. Vandaag kan een bedrijf van twee, drie personen perfect kiezen om een CRM-systeem te implementeren. Denk aan Microsoft CRM, **de kosten die erachter zitten zijn perfect verantwoordbaar**. Terwijl als je dit gaat doen in een traditioneel model is die kost misschien niet verantwoordbaar. Je moet servers installeren, je moet applicaties aankopen. Je zit daar met een pay-per-license model. Terwijl in een cloud zit je in een **pay-per-use model**. Het is veel **flexibeler** om hiermee om te gaan. Bijkomend iets wat ik er nog aan kan toevoegen, voornamelijk voor die

kleinere bedrijven is dat als je gaat kijken naar KMO's bijvoorbeeld en hun e-mailboxen en de applicaties die zij dagelijks gebruiken. Op dat moment, zie je vaak dat als er nieuwe medewerkers beginnen dat het even duurt vooraleer die mailboxen opgezet zijn. Typische problemen bij de IT-infrastructuur van een KMO die niet altijd de nodige IT-personen in dienst heeft, is dat ze vertrouwen op externe partijen die voor hun de IT willen doen. Met **cloud** kan je die problemen gaan oplossen. Het is **super eenvoudig** om een nieuwe mailbox aan te maken. Dat is slechts twee seconden werk. Het kan immers door een niet IT-persoon uitgevoerd worden. Je kunt je nieuwe medewerker bij wijze van spreken **binnen de tien minuten een nieuwe mailbox geven**. Je koopt een computer aan, je maakt die mailbox aan en het is klaar. Ook heel makkelijk aan te maken voor mensen die niets van IT kennen. Je gaat een **beetje abstractie maken van het technische**.

Wat zijn volgens u de belangrijkste nadelen van cloud computing?

Je zit met een **Internetdienst**, een **netwerkdienst**. Eén van de grote nadelen natuurlijk als je **geen netwerk hebt**. We gaan ervan uit dat netwerk overal en altijd ter beschikking is. **Als dat niet ter beschikking is, zit je met een probleem**. Dan kan je dus ook niet gaan werken. Als je volledig vertrouwt op cloud in de zin van webapplicaties en zo verder. Daar zijn ook weer oplossingen voor te vinden natuurlijk. Je kan bepaalde dingen lokaal houden. Dat is één nadeel. Zie ik dat als een groot nadeel voor de wereld waarin wij leven, neen. **Over het algemeen is die connectiviteit zeer goed**. Maar je hoort inderdaad wel eens problemen. Ik verwijs recent naar het **Telenet-verhaal**. Die zijn voor een **tijdje uitgevallen**. Voor een aantal bedrijven die 100 % afhankelijk zijn van de cloud, kan dat een uitdaging zijn. Wat zijn bijkomende nadelen? Heel het legale, **het privacy-aspect dat er bijhoort**. Waar men vandaag zo een beetje vragen bij stelt. We leggen **al onze eieren in de mand van een grote wereldwijde IT-speler**. Wat gaat die er meer doen en zo verder. Niet vergeten dat vanuit privé standpunt de **thuisgebruiker** dat al veel langer doet. Mensen die Gmail, Hotmail, Skype al die dingen gebruiken. Die services zijn er al tien tot vijftien jaar. Dat zijn ook eigenlijk niet meer en niet minder dan cloud producten. **Daar stelt men de vraag niet**. Maar als het gaat over **een bedrijfscontext** dan **stelt men zich er wel vragen bij**. Het is een beetje een dualiteit. Het is iets nieuw en dat moet nog zijn weg vinden natuurlijk. Heel veel bedrijven zijn al overgestapt naar cloud diensten. Het begint zijn weg te vinden.

Welke privacy risico's zijn er bij het gebruik van de cloud?

Daar staat men nog maar in zijn **kinderschoenen**. Ik weet dat **Europa een aantal nieuwe richtlijnen aan het formuleren is** om heel dat data privacy gebeuren te reguleren. Waarbij men vooral de **acces tot de data begint te regelen**. Vroeger had men regels over waar moet de data gaan staan. Eigenlijk is de vraag die men stelt, **wie heeft er acces tot mijn data**. Dat is de juiste vraag. Dat is een **juister verhaal** dan louter te weten waar staat de data. Het is **vooral belangrijk dat je reguleert wie er acces heeft**. Privacy is uiteraard

een heel belangrijk verhaal. Ook gelinkt aan richtlijnen zeker in België en in Europa. Die data mag het continent tussen aanhalingstekens niet verlaten. Je ziet dat er een enorme beweging op gang is om dat ook in vraag te gaan stellen omdat men vandaag meer en meer in globalere economie gaan leven. **Het is niet meer Europa waarin we leven. Maar Europa, Amerika, de wereld waarin we leven**. Mensen vinden net zo makkelijk een dienst in de VS als in Azië als in Europa. Je ziet ook heel **veel verschuivingen op dat vlak in privacywetgeving** gebeuren. Het blijft **een superbelangrijk punt in heel het cloud gebeuren**. Ik verwijs ook nog even naar de particuliere kant. Als je vandaag je foto's op een Flickr of andere diensten die er zijn, mails in een Gmail zet moet je goed **kijken naar de business plannen van de leverancier die erachter zit**. Daarvan is de gebruiker zich niet altijd van bewust. Is de leverancier een IT bedrijf, is die geïnteresseerd voor het aanleveren van IT diensten. Of is de leverancier een communicatie/databedrijf. Google is een information company. Microsoft is een software company. Dat is een groot verschil. **Google** stelt dat alles wat je bij ons doet, hebben wij **het recht op die data**. Bij **Microsoft is dat niet het geval**. Wij zijn een IT bedrijf en laten gebruikers betalen voor hun IT diensten. **Microsoft komt niet aan de data aan**. In het geval van **Google sta je de rechten op je data af**. Ik verwijs ook naar de recente persartikels van Facebook wat eigenlijk ook alweer een cloud service is. Je **staat de rechten van je foto's af aan Facebook**. Je **staat de rechten op je foto's af aan Flickr**. Dat wil zeggen dat op een moment dat het voor hun kan die gegevens kunnen en mogen gebruiken zonder dat jij daarvan op de hoogte wordt gebracht. De vraag is hoe weet ik wat er met mijn data gebeurt? Een **privacy policy moet goed bekeken worden**. **Wat onderteken ik eigenlijk?** Je ondertekent altijd iets. Of het nu gaat om een Gmail account of een Hotmail account, een CRM, Google Docs, en zo verder, je ondertekent altijd iets. Wat staat daar in? De meeste bedrijven liggen daar niet van wakker. Ze kijken enkel of het gratis is. **Het is misschien wel gratis, maar 'there is no such thing as a free lunch'. Op één of andere manier keert dat wel tegen je, er moet immers ergens inkomsten zijn.**

Is er een onevenwicht bij het opstellen van een contract tussen een cloud provider een een cloud user?

In een **cloud** gebeuren is het **meestal te nemen of te laten**. Er wordt dikwijls gewerkt met **standaardcontracten**. Het is een dienst die wordt aangeboden aan de wereld. Het is **niet** zo dat **je kan gaan stellen dat je niet akkoord bent met een bepaalde clausule.** Dan zit je eigenlijk automatisch in een **alternatief scenario zijnde een private cloud** daar **kan je over dat lijntje gaan onderhandelen**. Als je spreekt over public cloud, het woord zegt het zelf: publiek, dus voor iedereen hetzelfde. Je kan wel leveranciers tegenover elkaar gaan bekijken, maar binnen één leverancier is het moeilijk voorwaarden te veranderen. Bijvoorbeeld als je je water afneemt van een Vlaamse watermaatschappij. Dan kan je **niet met de desbetreffende leverancier gaan onderhandelen met deze lijnen in het contract ben ik niet akkoord**. Dan

moet je ofwel een alternatief gaan bekijken. Dat zijn de voorwaarden waaraan zij leveren. **Telenet** levert bijvoorbeeld ook een **publieke dienst** aan voor België. Bij cloud is dat niet anders. Als je specifieke voorwaarden zou leveren zou je geen publieke cloud meer zijn. Maar veeleer een private cloud, dat is een ander business model. Bij **Microsoft 365** is het ook zo, als je een contract aangaat zijn er **standaardvoorwaarden** die erin zitten. Je **kan bepaalde dingen wel veranderen, maar niet oneindig**. **Als je oneindig wil gaan veranderen, dan moet je overstappen naar een private cloud**. De mogelijkheden zijn beperkt waardoor de prijs ook gedrukt kan worden bij een public cloud. Voor grotere bedrijven zullen hybride oplossingen het beste zijn. Niet-kritische data op een public cloud en kritische data op een private cloud.

Welke beveiligingsrisico's treden er op bij het gebruik van de cloud?

Wij bij Microsoft hebben **wereldwijd een aantal datacenters die top beveiliging hebben**. Ik denk niet dat je in een lokaal datacenter een dergelijke mate van beveiliging kunt hebben als je alles in rekening brengt. Je spreekt hier over **disaster-recovery, multiple sites, meerdere connecties**. Je zit met je **software of databeveiliging op zich, connectiebeveiliging tot de data, en zo verder**. Dan heb je ook de **fysische beveiliging** van de datacenters. Dat is een **vak apart**. Ik heb vroeger een bezoek mogen brengen aan het **Microsoft datacenter in Dublin**. Dat is **bijna of je bij de NATO naar binnengaat qua beveiliging**. Er mogen niet meer dan **zoveel personen tegelijk binnen, je moet doorgeven op voorhand wie komt er binnen, wat is de bedoeling van het bezoek**. Er zijn **heel strenge beveiligingsnormen**, maar dat moet ook wel anders kom je in problemen terecht.

Wat moet het management over het gebruik van de cloud weten, welke skills moeten in organisatie beschikbaar zijn?

Ik denk dat bij cloud computing het er vooral op aankomt om te kijken naar een model. Wat is het model erachter. Je **moet niet meer licenties, servers gaan aankopen**. Het is een **strategische managementbeslissing om meer te evolueren naar operationele uitgaven bij cloud**, het zogenaamde **pay-per-use** verhaal. Hierdoor ga je ook een aantal besparingen kunnen gaan realiseren op de infrastructuur. Je koppelt de techniciteit van de infrastructuur als het ware los van het gebruik ervan. Ik denk wel dat dat een **managementbeslissing is**. Kijk eerst en vooral naar het financiële en strategisch verhaal. Ten tweede kijken we naar het **privacy verhaal**. Wat onderteken ik eigenlijk, wie heeft acces tot de data, waarvoor mag het gebruikt worden. Dat is op zich ook wel belangrijk. Inderdaad het scenario dat vooral in de particuliere wereld speelt, is dat ik al mijn rechten op de data afsta. Als je dit als bedrijf gaat doen, geeft dit de hele bedrijfsfilosofie bloot aan iedereen. Indien er gekozen wordt om **bepaalde data lokaal op te slaan en bepaalde data op een cloud, dan is dat ook een managementbeslissing**. Ik ben van mening dat het **managementteam moet betrokken worden bij deze discussie omdat het fundamenteel is voor het bedrijf**.

Hoe ziet u de wetgeving over heel de wereld evolueren?

Er zijn **heel veel wetgevende machten bezig met deze evolutie**. In Europa, België zie je een positieve trend met alles wat met cloud computing te maken heeft. Men **erkent de problematiek van cloud computing** versus de huidige wetgeving. Vandaag zie je vaak dat **de huidige wetgeving in niet alle gevallen toelaat dat cloud computing geïntroduceerd wordt**. Omwille van het feit dat je data misschien niet meer in België, in Europa, maar ergens ter wereld zit. Het maakt **niet meer uit waar je data zit, maar wel wie er acces toe heeft**. Men erkent zeker **dat het een trend is waarop men moet gaan inspelen**.

Moet er van de cloud provider kant geweten worden wat er in de cloud gestoken wordt?

Ik denk dat dit ook **geregeld wordt in contracten**. Ik denk dat men zegt dat bepaalde data niet mag gestored worden in bepaalde clouds, **dit is uiteraard leverancierafhankelijk**. Net zoals op **Youtube** mag je **geen aanstootgevende films publiceren**.

Kunnen gegevens makkelijk overgedragen worden op een andere cloud service om 'lock-in' te vermijden?

Als je gaat kijken naar SaaS, **hoe hoger dat je die ladder beklimt**, hoe **meer je een stukje afhankelijk wordt**. Maar **cloud diensten zijn in principe generiek**. Je kan perfect abstractie maken en stellen: ' wanneer heb ik een lock-in en wanneer niet'. Er zijn **natuurlijk ook contracten die dit regelen**.

Heeft u eventuele referenties binnen de sector?

Hier zal ik nog even over nadenken en u die doormailen indien ik er nog heb.

6.7 Solutions architect Ferranti Computer Systems – Raf De Backer

Als zevende contactpersoon heb ik Raf De Backer geïnterviewd. Raf De Backer is sinds augustus 2011 Solutions architect bij Ferranti Computer Systems. Ferranti Computer Systems was gesticht in 1976 in Antwerpen, België. De core business die Ferranti vertegenwoordigt, is business processen uit te tekenen en een automatiestrategie met laatste vernieuwingen aan klanten voor te leggen. Voordat Raf De Backer bij Ferranti werkte, werkte hij ook nog bij Argenta. Hij heeft een diploma Master Computer Sciences van de Universiteit Antwerpen.

Hierna volgt een transcriptie van dit interview. Het interview duurde 29 minuten en 40 seconden en werd uitgevoerd in de gebouwen van Ferranti te Antwerpen op 27 februari 2013. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor Raf De Backer. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Hoe komt u in aanraking met cloud computing?

We zijn een **service provider**. Dat wil zeggen dat wij zowel **private, public als hybrid cloud providen**. Als Ferranti geven we **dynamic datacenter oplossingen**. Iedere speler nu is niet meer geïnteresseerd in gewoon doosjes, maar in totaaloplossingen. Die oplossingen moeten voorzien worden van computer resources. **Wat eronder staat, interesseert hun meestal niet meer**. Oftewel gaan ze naar een **echte cloud provider, een Amazon of dergelijke**, of je gaat naar een eigen cloud waarbij je zegt, kijk ik weet dat het in **België of in Nederland staat** afhankelijk van wetgeving, of je gaat **een eigen on-premise cloud bouwen**. In die zin als integrator **leveren wij die drie verschillende mogelijkheden**.

Wat zijn de belangrijkste voordelen van cloud computing?

Cloud is natuurlijk **nog altijd een buzz-woord**. **Iedereen gebruikt op dit moment wel het woord cloud**. Bij cloud computing heb je een compleet model dat **schaalbaar** is. **Schaalbaarheid, security, flexibility zijn voordelen**. Het is **echter niet noodzakelijk goedkoper**. Iemand anders neemt de risico's voor jou, je krijgt alles in een voorspelbaar model. Je **dekt het aan de ene kant af in een contract**. Doordat het **schaalbaar is** kunnen ze een pak makkelijker omgaan met de risico's. Vooral voor een klein bedrijf als je heel veel on-site zou moeten gaan bouwen, je kan even goed zorgen voor een cloud computing model. In een **klein verhaal** zou het **kostelijk zijn om het schaalbaar te maken**. Als het bedrijf groot genoeg zou zijn, zou het mogelijk on-premise gebouwd kunnen worden en zo schaalbaarheid gehaald kunnen worden. Je kan langs de andere kant een **externe cloud leverancier**, zoals **Microsoft,** aanspreken en er alles gaan plaatsen. Voor mij is cloud een service dat **iemand anders met de IT-gerelateerde zaken bezig is** en **de risico's hierbij uitlegt en afdekt** en dat **jij zelf bezig kan zijn met de core business kant van het verhaal**.

Wat zijn de belangrijkste nadelen van cloud computing?

Er zijn **verschillende nadelen afhankelijk van in welke sector** dat je zit. Er bestaan **heel veel wetgevingen omtrent de utility sector** in **Nederland**. In de **bankensector** stellen ze dat **alle klantengegevens lokaal moeten blijven staan**, waarbij je ook garantie moet hebben dat het daar blijft staan. Dus als je zegt we gaan door met cloud en willen alles in de public cloud steken dan kan je natuurlijk **niet meer meegaan** of je moet gaan onderhandelen met één van die providers die een **lokale cloud** ergens gaat bouwen voor u met dezelfde kenmerken, met dezelfde kostprijzen. Dan zit je **op dat moment een beetje vast**, omdat zij dat ook niet speciaal voor jou gaan bouwen. **Een bedrijf als Ferranti zou dat wel voor u kunnen gaan bouwen**. Er zijn heel veel parameters, maar er moet goed nagedacht worden: wat heb ik effectief nodig? Grootste nadeel is eigenlijk die twee zaken combineren. **Je hebt on-site heel wat applicaties draaien, je hebt heel gemakkelijk dat je extra resources erbuiten nodig hebt**. Het **moet goed geconnecteerd zijn**, je moet zorgen dat je ernaartoe kan gaan. Stel dat je echt een ouderwetse applicatie hebt met verschillende lagen. Als die **verschillende lagen** op **verschillende cloud**

diensten geïnstalleerd zouden worden, **zouden er vertragingen kunnen optreden** die heel groot zijn.

Welke privacy risico's zijn er bij cloud computing?

De data **wordt te lang opgeslagen terwijl die eigenlijk verwijderd zou moeten zijn,** is inderdaad een risico dat optreedt. Wat zijn **de precieze omstandigheden dat de data geraadpleegd kan worden,** is een ander voorbeeld van privacy risico. Je hebt de grote spelers die ervoor kunnen zorgen dat je het goedkoper kan doen, ze zijn bezig met heel wat Europese datacenters te bouwen. Maar als je er **momenteel nog gebruik van maakt zit je met Amerikaanse datacenters**. In **Amerika** heb je echter de '**American Patriot Act'**. Deze stelt dat als wij als **overheid denken dat er een vermoeden is van terrorisme, dan kunnen ze erin**. Iphone, alles wat e-mail betrokken is en zo verder. Als het product Blackberry beschouwt, stel je vast dat ze gebruik maken van een compleet ander systeem. **Blackberry connecteert via een Blackberry server over de Blackberry datacenters** die **eigenlijk alle data bevatten**. Dat wil zeggen dat alle data die over Blackberry gaat ofwel in een datacenter **in de UK staat of in een datacenter in de US staat**. **Als het in de US staat, kan de overheid er makkelijk aan**. In principe kan de overheid dan alle gegevens raadplegen. Dat is een **stukje privacywetgeving van de US die niet afgestemd is met de strengere regelgeving van Europa**.

Welke privacywetgevingen zijn er?

Een **website moet bepaalde gegevens publiceren**. Als je een bedrijf bent, **moet je daarop vermelden op welke manier ze je kunnen contacteren** en **verplichten om je BTW-nummer erop te zetten**. Langs de andere kant, stel dat je nu eindgebruikers hebt. Zelfs uw eigen werknemers moeten in principe een **handtekening geven om hun foto te gebruiken binnen het eigen bedrijf**. Eigenlijk moet **elke individuele medewerker een handtekening gezet hebben of in zijn contract gezet hebben om te stellen of hun foto gebruikt mag worden**. Europese richtlijn 95/46 is mij niet bekend. Europese richtlijn 2002/58 is mij niet bekend. Safe Harbor principe is mij tevens niet bekend.

Worden privacy policies goed opgesteld?

Je kan via de **active directory gaan bepalen** waar **iemand aan mag en waar iemand niet aan mag**. Je gaat als het ware een **access list bepalen**. Die link van de active directory **kan je gaan afstemmen op de cloud provider zodat je zelf een stuk in controle bent**.

Welke beveiligingsrisico's treden er op?

Onbeveiligde interfaces is inderdaad hier een voorbeeld van. Eén van de grootste aspecten is altijd dat twee applicaties, die samenwerken, behoorlijk aan elkaar gekoppeld worden. Er zijn heel dikwijls zogenaamde **man-in-the-middle**

attacks. Verkeer van een bepaalde gebruiker wordt **afgetapt tot de cloud provider en zo wordt onbeveiligde informatie vrijgegeven**. **Bij banken worden hierdoor meestal extra beveiligingscodes ingebouwd**. Een typische **man-in-the-middle attack** is dat ze **ertussen zitten** en **een ander bedrag en rekeningnummer invullen**. Ze geven gewoon de challenge terug en jij vult de juiste nummers in. **Account of service kaping hoort hier ook bij**. Het grootste probleem op dit moment is **niet altijd de problematiek van systemen**. Als je gaat kijken naar waar gaat de data nu verloren of waar gaan geheimen nu verloren, komt er nu te veel informatie naar buiten. Daar zijn **meestal enkel menselijke factoren mee betrokken**. **Tachtig procent van de datalekken zijn menselijke factoren**. **De security aspecten op technisch vlak zijn heel dikwijls heel sterk afgedekt**. **Firewalls, intrusion prevention systems, stukken virtualiseren** zodat je er nog moelijker doorgeraakt. De **persoon die er werkt** heeft echter nog altijd **een USB-stick bij** en die heeft dat toevallig mee en **dat is niet encrypted en de geheimen komen op straat terecht**. **Die menselijke factor is eigenlijk het grootste risico**. Het **grootste percentage dataverlies dat er optreedt, heeft met medewerkers te maken en niet met de systemen**. Het **belangrijkste is dat de mensen weten waar ze mee bezig zijn**. Je hebt binnen contracten zogezegde **nda's (non-disclosure agreements).**

Is er een verschillend beveiligingsrico per laag (SaaS, PaaS, IaaS)?

Ferranti biedt **verschillende modellen** aan. Bij **SaaS hebben we momenteel een serivce in ontwikkeling**. Hetgeen wij uiteindelijk vooral aanbieden, is IaaS**. We bieden echter ook PaaS aan.**

Moet er geweten worden wie de cloud gebruikt en wat er in de cloud geïnjecteerd wordt?

Als ik moet refereren naar Ferranti, is dat wij onze visie erop kunnen geven, **maar is het bedrijf zelf dat beslist wat er op de cloud gezet wordt**. In die zin als wij ons als leverancier aan de kant van de tafel zetten dan **gaan wij zeggen kijk dit zijn de modaliteiten waarbinnen wij kunnen handelen**. Die modaliteiten zijn het feit dat **wij niet met de Patriot Act rekening moeten houden en dat wij een schaalbaar model kunnen aanbieden**. Als wij **zelf cloud provider zijn is hiet niet belangrijk om te weten wat erin gestoken is. Als wij zelf van een cloud gebruik maken, is het wel belangrijk om te weten wat erin wordt gestopt**.

Het belangrijkste is dat je aan de hand van de **active directory kan managen wie toegang krijgt, welke gegevens er gezien mogen worden, etc.**

Hoe ziet u de wetgeving over heel de wereld evolueren?

Uiteindelijk merk je sterk dat **Europa onder druk gezet wordt door Amerika om alles veel meer open te zetten**. Een goed voorbeeld vond twee jaar geleden plaats: het **SWIFT-netwerk.** Dit is het eigenlijke transactienetwerk

tussen alle banken wereldwijd, waar **Amerika meer inzicht in wou. Europa werd onder druk gezet om informatie vrij te geven**, **anders zouden ze hun eigen netwerk** bouwen. De nieuwe groeimarkten: **Brazilië, India en China** zijn **geen schoolvoorbeeld van privacy**. Ik heb de **vrees** dat de **privacywetgeving**, zoals wij ze in Europa kennen, relatief strikt, **wel eens afgebouwd zou kunnen worden**.

Voldoet u ook aan ISO-normen?

Ja, inderdaad. We **voldoen aan de 9001 norm** en we zijn **bezig met de ISO-norm 27000**.

Doen jullie ook aan encryptie?

Uiteraard. We g**ebruiken VPN-verbindingen om data over het Internet te versturen**.

Hoeveel datacenters hebben jullie?

Wij hebben **drie of vier datacenters** waar we gebruik van maken. We hebben geen eigen datacenter. We **maken gebruik van datacenters van Colt** die **voldoen aan de tier 4 norm**. Waar wij ons op **concentreren**, is het **aanbieden van de services** aan onze klanten en **niet zozeer het aanbieden van een datacenter, daar is Colt een veel sterkere partner als Ferranti**.

Is er een goed evenwicht bij het opstellen van het contract tussen cloud user en cloud provider?

Wij geven 'recht toe recht aan' **service agreements**. Ik denk dat we meestal **meer transparant zijn dan hetgeen wat de rest van de collega's aanbiedt**. De **grote public cloud providers gaan altijd iets erin proberen toe te laten dat ze met die dingen iets kunnen doen, dat is natuurlijk hun grote marktwaarde**.

Hebt u nog verdere opmerkingen?

Ik hoop dat ik u een beetje heb kunnen helpen.

6.8 Chief Technology Officer Zentrick – Pieter Delbeke

Als achtste contactpersoon heb ik Pieter Delbeke geïnterviewd. Pieter Delbeke is sinds augustus 2010 Chief Technology Officer (CTO) bij Zentrick. Zentrick is een jonge start-up die interactieve videostreaming levert. Naast oprichter van Zentrick is Pieter Delbeke ook oprichter van Insite Mees-Delbeke VOF. Hij heeft ook nog bij Recomatics NV en Bank J. Van Breda & Co gewerkt. Hij heeft van een opleiding aan de Katholieke Hogeschool Mechelen en Karel de Grote' Hogeschool Antwerpen genoten.

Hierna volgt een transcriptie van dit interview. Het interview duurde 29 minuten en 22 seconden en werd uitgevoerd in de gebouwen van Zentrick te Gent op 27

februari 2013. Het interview werd niet gehouden op een andere locatie vermits dit het beste uitkwam voor Pieter Delbeke. Een neutraal lokaal werd ons aangeboden. Hierdoor zal potentiële bias door de werklocatie geminimaliseerd zijn.

Hoe komt u in aanraking met cloud computing?

Wij waren **op zoek naar een heel schaalbare oplossing**. Als **start-up** heb je **niet zo gigantische budgetten** om op te kunnen starten. Het moest dus iets heel **flexibel** zijn. **Cloud computing** is dan eigenlijk perfect. Je moet **geen hardware investeringen doen**. Je **betaalt voor wat je effectief gebruikt**. In het begin als start-up heb je bijna geen verbruik. Dan betaal je eigenlijk als het ware bijna geen geld. Naarmate je meer klanten hebt, **schaalt uw systeem mee** en betaal je meer. Vandaar dat cloud voor ons het meest interessant was.

Wat zijn de belangrijkste voordelen van cloud computing?

Het **meeschalen is een zeer belangrijk voordeel**. **Zowel in het stijgen als in het dalen van de databehoefte**. Stel dat je een maand lang een heel zwaar project moet doen. Met een **paar muisklikken, kan je zo van meer service genieten**. Als dat project voorbij is kunnen we zo van minder service gebruik maken. **We betalen dan ook minder**. In een **klassiek systeem** zou je die service moeten aankopen en **na dat zwaar project zouden die voor niets staan te draaien**.

Wat zijn de belangrijkste nadelen van cloud computing?

Ik heb er **eigenlijk nog heel weinig nadelen aan ondervonden**. Misschien een nadeel is **als je als bedrijf geen Internet hebt**. **Als alles in de cloud staat, dan zit je met je vingers te draaien** en **kan je de desbetreffende services niet raadplegen**. Je moet je **architectuur en software ook aanpassen aan de structuur van de cloud. Er zijn dingen die je niet kunt doen in de cloud. Dan moet je daar wel rekening mee houden**.

Met welke privacy risico's komen jullie in aanraking?

Ik heb daar op voorhand al zo wat over zitten nadenken. **Qua privacy hebben wij heel weinig risico** omdat wij **nauwelijks persoonlijke data stockeren**. De gegevens die wij **bijhouden zijn een e-mailadres, een naam en facturatiegegevens**. Maar die facturatiegegevens zijn normaal data van bedrijven, die zijn ook publiek toegankelijk. **Paswoorden zijn zwaar geëncrypteerd dus dat is ook geen risico**. **Dan is het juist nog de username en e-mailadres, maar als dat zou uitlekken is het risico niet gigantisch**.

Weet u iets of deze privacy risico's door wetten worden ingedekt?

Wij **weten hier heel weinig van**. Ik denk dat **wij er te weinig van weten**. **Probleem** is nog **dat wij een internationaal bedrijf zijn**. Dat maakt het

allemaal **nog iets complexer** omdat je niet alleen de **privacywetgeving** van **België moet respecteren maar ook die van de andere landen** waarmee je zaken doet. Eigenlijk zouden we dat beter moeten uitzoeken. Maar als start-up is dat één van de dingen die je naar achter schuift. **Moesten we zo een bedrijf zijn zoals een Facebook of dergelijke iets dat heel veel clients gerelateerde data heeft, zouden we daar al meer tegen doen**. Maar **bij ons is dat niet zo belangrijk**. In onze 'terms of use' staat er wel een **privacy policy** en dergelijke zaken. Dat zit wel **verwerkt en is opgesteld door een advocaat**. Dat is wel in orde. Het gebeurt **niet dikwijls dat we de wetgeving uit het hoofd gebruiken**.

Is er een onevenwicht bij het opstellen van het contract tussen cloud provider en cloud user?

We hebben er **nooit echt bij stilgestaan en echt mee geconfronteerd mee geweest**. Van dat onevenwicht bij het opstellen van het contract, daar hebben wij **niet echt ervaring mee**.

Welke beveiligingsrisico's treden er op?

Bij ons is het datacenter Amazon. Die heeft bepaalde eisen. Je weet dat **niemand binnenkan in dat datacenter en dat dat goed beveiligd is**. **Account of service kaping is een beveiligingsrisico**. Als ons **master paswoord of ons account bij Amazon gekaapt wordt** dan hebben wij een **groot probleem natuurlijk**. Daar moet je je van bewust zijn.

Is er een verschillend beveiligingsrisico tussen de verschillende lagen?

Daar heb ik geen ervaring mee.

Wat gebruiken jullie eigenlijk SaaS, PaaS of IaaS?

Het is meer PaaS. Onze **databases en zo draaien meer als een SaaS**. Wij gebruiken heel intensief cloud platformen maar eigenlijk zijn wij met die termen heel weinig bezig.

Moet er ook rekening mee gehouden worden dat gegevens makkelijk naar een andere cloud provider kunnen overgedragen worden?

Elke beslissing die we nemen in onze architectuur **daar houden we ook rekening mee dat dat ook moet werken op een ander platform**. De lagen die specifiek zijn voor Amazon die zijn mooi geabstraheerd en als wij ooit beslissen om naar een andere cloud provider te gaan, **dan kan het platform binnen de paar dagen op een ander systeem draaien**.

Doen jullie ook aan encryptie?

Ja, **alle paswoorden en zo zijn geëncrypteerd**.

Moet er geweten worden aan de cloud user kant wat er in de cloud gestoken wordt?

Onze **eindgebruiker** die **weet niet echt wat dat er nu in de cloud draait**. Maar opnieuw er is **nauwelijks iets van privacy gevoelige data** dat we gebruiken. Alles van **contracten en zo dat wordt lokaal bij ons bewaard**.

Hoe ziet u de privacywetgeving over heel de wereld evolueren?

Dat **weet ik niet**. Omdat **wij niet zo met privacy gevoelige data werken**, is dat bij ons niet zo een issue. Heel het **cookie gebeuren,** het feit dat je users mag tracken. **Europa is daar eigenlijk mee begonnen met te zeggen van je mag eigenlijk niet zomaar cookies meer gebruiken om te gaan tracken**. Maar bijna alle websites doen dat. **Wat dat ge moet doen, is zo een notificatie tonen op je website**. Dat zijn wel dingen waarmee je moet rekening houden. **Aan onze kant willen we niet liever dat we de eindgebruikers getracked zien. Maar we moeten hiermee wel opletten dat we geen privacyregels schenden.**

Jullie gebruiken cloud diensten en jullie leveren cloud diensten?

Ja, wij **transfereren een PaaS naar een SaaS**.

Wat doen jullie nu eigenlijk precies?

Wij **maken video's interactief**. Stel je hebt een video waarin een product in gedemonstreerd wordt of mensen die rondlopen. Dan **kan je die mensen of producten gaan aanklikken**. Je kan er een **interactieve laag bovenleggen**. Zodanig dat als je gaat klikken op dat product of die mens dat je informatie gaat krijgen. Maar het gaat verder dan dat. **Je kunt 'social' dingen verwerken. Je kunt in feite gamefication erin toepassen**. Eigenlijk **alles wat je boven een video kunt inwerken, wat meerwaarde aan de video toont**. We gaan die video verrijken met acties die je kunt gaan doen. Op **Youtube heb je annotaties**, kaders die automatisch verschijnen op je video als je naar de video kijkt. Wij **hebben daar een verbeterde versie van**. Wij kunnen veel meer dan gewoon links naar externe video's leggen. Wij kunnen **ervoor zorgen dat al die externe informatie in de video zelf zit**. Wij hebben **ook bepaalde servers in andere landen staan**. Daar staan **kopieën van onze bestanden op**. Als men uit een bepaald land onze service opvraagt dan gaat het via die server in dat bepaald land. **Een soort van cache/proxy-achtig systeem**. **We gebruiken ook een databasesysteem**. Daarvoor is de cloud natuurlijk super. Als je zo een databasesysteem moet opzetten met je eigen servers, dan betaal je je blauw. Dan is het daarnaast ook niet schaalbaar. Nu **kan je instellen in slechts één veldje, welk gigabytes per seconde je wenst te hebben. Je kan in een seconde je capaciteit verdubbelen.**

Voldoen jullie ook aan ISO-normen?

Mijn **vorige werkgever die waren ISO-certified**. Ik weet dat je dat **nodig hebt om te werken voor de overheid**. **Sommige bedrijven vereisen ook dat je ISO certified bent**. Maar zelf heb ik daar zwaar mijn twijfels bij. Maar **wij hebben nog nooit de vraag gehad van klanten**. Het **kost ook veel geld om te voldoen aan een ISO-norm**. Men spreekt hier over **ISO 27000 en ISO 9000. ISO 27000 biedt weinig garanties vind ik**. Er worden **bij ons processen afgesproken maar die zijn niet gecertificeerd**.

Is de privacy policy niet te vaag opgesteld?

Ik weet dat dat **opgesteld is in samenspraak met een advocaat**. Dat **staat in de terms of use**. **Informatie** die **we vooral van klanten krijgen zijn IP-gegevens**. Als een eindgebruiker een filmpje bekijkt, krijgen wij in onze log-files **welk IP-adres dat was en dat kunnen we dan mappen op geografische data**. **Gegevens die in de interactieve video worden ingegeven die komen rechtstreeks bij de eindklant terecht**.

Heeft u nog verdere opmerkingen?

Ik denk dat er **heel veel gebruik wordt gemaakt van de term cloud in een foutieve zin**. Er worden **heel veel dingen verstaan onder cloud die totaal niet cloud zijn, in mijn ogen**. Een **echte cloud provider** doet **meer dan enkel virtuele servers aanbieden**. Je moet zelf nog **zorgen voor de schaalbaarheid die erachter zit**. **Schaalbaarheid is de kracht van cloud** vanuit mijn standpunt. Een cloud houdt bijvoorbeeld het volgende in: je gaat naar **Amazon** en je **duidt aan hoeveel virtuele machines je wil hebben**. Je zegt van ik wil dat die zo snel is, zoveel ruimte voorzien is om op te werken. **Amazon start die servers op, monitort die zodat die stabiel draaien**. Als die niet stabiel draaien dan krijg je een mail. Al die dingen gebeuren volautomatisch. Dit kan je dan **in plaats van honderduizenden euro's, laten draaien voor een paar euro's in de maand. Je betaalt enkel wat je gebruikt**. Het configureren, monitoren gebeurt allemaal door Amazon en daar moet de eindgebruiker zich niets van aantrekken. We moeten bijvoorbeeld ook **nooit wakker liggen dat we op een dag te weinig storage gaan hebben**. Ik denk dat **in die aangehaalde dingen de kracht zit van cloud**.

Ik vermoed dat de **overheid de wetgeving niet snel genoeg kan bijbenen met de evolutie van de technologie**. Het feit dat onze servers in Ierland staan, dus niet in België voor die servers **geldt de wetgeving van Ierland**. Dat heeft er allemaal wel impact op. Stelt dat **uw server in de US staat, dat kan impact hebben op uw wetgeving en privacy**. **Wij doen eigenlijk zo weinig privacy gevoelige dingen dat wij daar geen last van hebben**. Ik ken een bedrijf die **wel privacy gevoelige data handelt dat die daar wel mee bezig is waar de data en servers nu precies staan in de wereld**.

Als we over Amazon spreken, is dat **ook de Amazon die boeken en andere dingen online verkoopt**. Zij **doen ook echter aan cloud computing**. Zij

hadden heel veel servers draaien om hun online verkoop te regelen. Op piekmomenten hadden die heel veel capaciteit nodig en soms minder capaciteit nodig. Ze **zijn begonnen om de overschot aan capaciteit te verkopen als cloud services**. Amazon biedt een heel ruim pakket aan cloud diensten aan.

6.9 Vakbeurs en seminaries over IT security – Infosecurity.be

Tegenwoordig worden bedrijven bijna dagelijks geconfronteerd met allerlei vraagstukken op het gebied van IT-security. Vraagstukken waar de vakbeurs Infosecurity.be op inhaakt en waar u uw oplossingen kunt presenteren. Een absolute must voor elke ICT-professional.

Op 20 maart 2013 bracht ik een bezoek aan deze beurs in Brussel. Ik volgde verschillende seminaries vanuit mijn invalshoek: 'de risico's bij cloud computing'. Hieronder haal ik kort aan welke seminaries ik gevolgd heb en waarover ze gaan. Er volgt geen volledige transcriptie maar een korte schets. De belangrijkste conclusies van ieder seminarie zijn reeds verwerkt in deze masterproef.

Het eerste seminarie was getiteld: 'ARCserve: How to protect your data with one solution in any environment: physical, virtual and in the cloud.' Het ging over een stukje software waarmee het voor een systeembeheerder zeer gemakkelijk is om back-ups mee uit te voeren. Dit seminarie werd gegeven door Jasper Geraerts (Vakbeurs IT security) en duurde een half uur.

Het tweede seminarie dat ik volgde was getiteld: 'CA Nimsoft Monitor 'Monitor as you want from the datacenter to the cloud'. Het ging over het monitoren van de IT-infrastructuur zowel van de cloud als binnen het eigen bedrijf. Zo wordt er een functioneel dashboard opgesteld waarmee de infrastructuur real-time gemonitord kan worden. Dit bedrijf deed al 15 jaar aan monitoring. Dit seminarie werd gegeven door Gijsbert Wiesenekker (Vakbeurs IT security) en duurde een half uur.

Het derde seminarie dat ik volgde was getiteld: 'E-Identity, Trust and Security Challenges of online & cloud services bij een Vlaamse Overheid'. Het ging over de mogelijkheid om de elektronische identiteitskaart te gebruiken om strengere toegangsbeveiligingen te vormen. Verder ging het over de vertrouwens- en beveiligingsaspecten van cloud services. Dit seminarie werd gegeven door Erik R. Van Zuuren (Vakbeurs IT security) en duurde drie kwartier.

Het vierde seminarie dat ik volgde was getiteld: 'WARNING: YOUR IDENTITY IS AT RISK!'. Het ging over het feit dat je als gebruiker heel veel privacygevoelige informatie op het web achterlaat zonder dat je het als gebruiker goed en wel beseft. Dit seminarie focuste zich vooral op de particulier. Oplossingen hiervoor zou: pseudoniemen gebruiken, Google Street view vragen om je huis wazig te maken, een online proxy te gebruiken, etc. Er zijn ook al diverse instanties die zich met privacy bezighouden, zoals: de Privacycommissie, BDMA (Belgian Direct Marketing Assocation), e-cops, etc. Dit seminarie werd gegeven door Bavo Vandenheuvel (Vakbeurs IT security) en duurde drie kwartier.

Het vijfde en laatste seminarie dat ik volgde was getiteld: 'Feel obliged to move to the cloud? Today maybe not, tomorrow probably. Keep you ready just in case.' Het ging over het feit of je als bedrijf alles onmiddellijk zou moeten overbrengen op de cloud. De echte toekomst bestaat eerder in hybride oplossingen. De hype die vandaag leeft dat eigen IT dood is, is niet waar. HP haalt aan dat het eigen IT gebeuren nog belangrijk is. Er zijn bijvoorbeeld ook speciale harde schijven te koop waarmee de flexibiliteit van cloud providers kunnen worden gegenereerd. Men moet meer gaan voor een evolutie naar cloud toe dan een revolutie. Dit seminarie werd gegeven door Jos Ectors (Vakbeurs IT security) en duurde een half uur.

6.10 High density datacenter Belgacom te Brussel

Op 27 maart 2013 bracht ik een bezoek aan het nieuwe high density datacenter van Belgacom te Brussel. Hier kreeg ik een rondleiding door Mark De Vriendt. Op 1 februari 2013 opende Belgacom dit nieuw, groen datacenter in Brussel. Met het nieuwe datacenter zal het voor Belgacom mogelijk zijn aan de snelgroeiende vraag voor cloud and datacenter-services te voldoen. Het nieuwe datacenter is extreem energie-efficiënt en gebruikt duurzame infrastructuur voor de toevoer van stroom en koeling.

Mijn aandacht ging vooral uit naar de beveiligingsmaatregelen van dit datacenter. Er wordt aan badging gedaan om bepaalde kamers binnen te kunnen. Er is camerabewaking. De stroom wordt gegarandeerd met een redundante dieselmoter die ervoor zorgt dat als de stroom uitvalt het probleem na 3,5 seconde is opgelost. De koeling is dubbel uitgevoerd. Er is een cijferslot op de racks waar de servers inzitten. Het datacenter heeft een de ISO 27001 classificatie en een tier 3+ niveau van beveiliging. Dit betekent dat het datacenter een betrouwbaarheid van 99,99 % garandeert. Bij tier 3+ gaat het over de fysieke beveiligingsmaatregelen. Het voldoet ook aan de tia 942 norm. Dit is een internationale norm uitgegeven door een Amerikaanse instelling, de Telecommunications Infrastructure Association. Om de 4 jaar wordt hier een test op gedaan. Hier gaat het ook over de fysieke beveiligingsmaatregelen van het datacenter. Als er brand is dan wordt er inert gas onder hoge druk in de serverroom gespoten om het zuurstofgehalte te verlagen zodat de brand stopt. Mogelijke personen in de serverroom worden dan gewaarschuwd via allerlei signalen om zo snel mogelijk zich uit de serverroom te begeven waar het zuurstofgehalte zich aan het verlagen is. De bewaking van het datacenter gebeurt door Securitas die 24/24 7/7 aanwezig zijn. Er is ook 30 man continu aanwezig om het datacenter te beheren. Er zijn ook branddeuren die brand afweren indien er brand zou uitbreken. Er zijn drukknoppen om branden te melden. Er is ook inbraakdetectie.

De term high density staat voor het feit dat er veel kilowatt aan voeding per serverrack beschikbaar is, dit is meer dan in een gewoon datacenter het geval is. Op de racks staat er een teller die aangeven hoeveel elektriciteit er gebruikt wordt.

Het nieuwe high density datacenter te Brussel wordt ook gecatalogiseerd als een green datacenter. De koeling wordt verzorgd door middel van een speciaal kyotowiel en is redundant uitgevoerd. Aan de ene kant van het wiel neemt het warme datacenter lucht op die aan de andere kant voor de administratieve gedeeltes worden vrijgegeven. De koude buitenlucht koelt het wiel weer af, wat dan wordt vrijgegeven aan het datacenter gedeelte. Het wiel draait rond en zo is de cyclus volledig. Door deze manier van koeling is het energieconsumptieniveau verlaagd met meer dan 60 %.

6.11 Opvallende overeenstemmingen en verschillen tussen de interviews

Een eerste opvallende vaststelling is dat cloud providers de nadelen van cloud computing minimaliseren en vooral de voordelen benadrukken. Soms halen ze zelfs aan dat er helemaal geen nadelen bij het gebruik van cloud computing zijn, terwijl dit helemaal niet waar is. Een andere opvallende vaststelling is dat cloud providers over andere cloud providers vaak kritiek uitten. Terwijl als ik een interview had bij die desbetreffende cloud provider, waarover de kritiek ging, de feiten meestal niet naar buiten kwamen. De cloud providers vinden hunzelf veelal beter tegenover andere cloud providers. Dit blijkt uit de antwoorden van de interviews. Nog een opvallende vaststelling was dat sommige geïnterviewden meer gespecialiseerd waren in de technische kant en sommige geïnterviewden meer gespecialiseerd in de juridische kant. Na een aantal interviews werd dit meer en meer duidelijk. Uit de interviews kwamen over het algemeen meer gelijkenissen naar boven dan verschilpunten.

7 Lijst van geraadpleegde werken

Abbadi, I.M., & Martin A. (2011). Trust in the cloud [Elektronische versie]. *Information Security Technical Report, 16,* 108-114.

Abbadi, I.M. (2011). *Operational Trust in Clouds' Environment.* Opgevraagd op 19 april, 2013, via http://www.cin.ufpe.br/~redis/intranet/bibliography/middleware/abbadi-operational-2011.pdf

Ahmed, A. (2012). Meeting PCI DSS When Using a Cloud Service Provider. *ISACA, 5,* 24-30.

Alles, M.G., Kogan, A., & Vasarahelyi, M.A. (2008). Putting Continuous auditing Theory into Practice: Lessons from Two Pilot Implementations [Elektronische versie]. *Journal of Information Systems, 22,* 195-214.

Amazon Elastic Compute Cloud (Amazon EC2). (2013). Opgevraagd op 30 april, 2013, via http://aws.amazon.com/ec2/

Anthes, G. (2010). Security in the Cloud [Elektronische versie]. *Communications of the ACM, 53,* 16-18.

Armbrust, M., Fox, A., Griffith,R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M.(2010). A view on cloud computing [Elektronische versie]. *Communications of the ACM,53,* 50-58.

Barrasso, R., & Wallace, M. (2012). Cloud Storage – Bursting Through the Hype. *ISACA, 5,* 6-8.

Bublitz, E. (2010). Catching the Cloud: Managing Risk When Utilizing Cloud Computing [Elektronische versie]. *National Underwriter / P&C, 114,* 12-16.

Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing [Elektronische versie]. *Procedia Engineering, 23,* 586-593.

Cheng, F.-C., & Lai, W.-H.(2012). The Impact of Cloud Computing Technology on Legal infrastructure within Internet – Focusing on the Protection of Information Privacy [Elektronische versie]. *Procedia Engineering, 29,* 241-251.

Durkee, D. (2010). Why cloud computing will never be free [Elektronische versie]. *Communications of the ACM, 53,* 62-69.

Garrison, G., Kim, S., & Wakefield, R.L. (2012). Success Factors for Deploying Cloud Computing [Elektronische versie]. *Communications of the ACM, 55,* 62-68.

Hastings, R. (2009). Cloud Computing [Elektronische versie]. *Library Technology Reports, 45,* 10-12.

Hoboken, J.V.J., Arnrbak, A.M., & van Eijk, N.A.N.M. (2012). *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*. Opgevraagd op 30 december, 2012, via http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534

Hunton, J. E., Mauldin, E., & Wheeler, P. (2010). Continuous monitoring and the status quo effect [Elektronische versie]. *International Journal of Accounting Information Systems, 11,* 239-252.

Icloud: overzicht van iCloud-beveiliging en –privacy. (2013). Opgevraagd op 24 maart, 2013, via http://support.apple.com/kb/HT4865?viewlocale=nl_NL&locale=nl_NL

Ismail, N. (2011). Cursing the Cloud (or) Controlling the Cloud? [Elektronische versie]. *Computer Law & Security Review, 27,* 250 – 257.

ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (2012). Opgevraagd op 19 april, 2013, via http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891

ISO/IEC 27010:2012 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications (2012). Opgevraagd op 19 april, 2013, via http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42509

Jena, R.K., & Mahanti, P.K. (2011). Computing in the cloud: Concept and Trends [Elektronische versie]. *International Review on Computers & Software, 6,* 1-10.

King, N.J., & Raja, V.T. (2012) Protecting the privacy and security of sensitive customer datain the cloud [Elektronische versie]. *Computer law & security review, 28,* 308-319.

Lambrecht, D. (2000). De bescherming van de privacy in de Belgische wetgeving. Overzicht van de bestaande wetgeving en een blik vooruit naar de op handen zijnde veranderingen [Elektronische versie]. *Jura Falconis, 3,* 443-494.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2010). Cloud computing – The business perspective [Elektronische versie]. *Decision Support Systems, 5,* 176-189.

Mohammed, D. (2011). Security in cloud computing: An Analysis of Key Drivers and Constraints [Elektronische versie]. *Information Security Journal: A Global Perspective, 20,* 123-127

Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe" (2012). Opgevraagd op 30 december, 2012, via http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

Owens, D. (2010). Securing Elasticity in the Cloud [Elektronische versie]. *Communications of the ACM, 53,* 46-51.

Panko, R.R., & Panko, J.L. (2011). *Business Data Networks and Telecommunications.* US: Pearson Education, Inc.

Perloff, J.M. (2008). *Microeconomics Theory and Applications with Calculus.* US: Pearson Education, Inc.

Rimal, B.P., & Choi, E. (2012). A service-oriented taxonomical spectrum, cloudy challenges and opportunities of cloud computing [Elektronische versie]. *International Journal of Communication Systems, 25,* 796-819.

Rittenberg, L.E., & Schwieger, B.J. (2004). *Auditing. Concepts for a Changing Environment.* US: Thomson South-Western.

Ross, S.J. (2012). Is security a wall or a door?. *ISACA, 5,* 4-8.

Ryan, M. D. (2011). Cloud computing Privacy Concerns on Our Doorstep [Elektronische versie]. *Communications of the ACM, 54,* 36-38.

SAS 70 OVERVIEW (2013). Opgevraagd op 19 april, 2013, via http://sas70.com/sas70_overview.html

Schiller, K. (2011). Legislating the cloud [Elektronische versie]. *Information Today, 28,* 1-36.

Sekaran, U., & Bougie, R. (2009). *Research Methods for Business.* UK: John Wiley & Sons Ltd.

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing [Elektronische versie]. *Computer Law & Security review, 26,* 391-397.

Sun, D., Chang G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments [Elektronische versie]. *Procedia Engineering, 15,* 2852 – 2856.

Yan, H. (2010). On the Clouds: A New Way of Computing [Elektronische versie]. *Information Technology & Libraries, 29,* 87-92.

Vaohradsky, D. (2012). Cloud Risk – 10 Principles and a Framework for Assessment. *ISACA, 5,* 31- 41.

Zhu, Y., Hu, H., Ahn, G.-J., & Yau, S.S. (2012). Efficient audit service outsourcing for data integrity in clouds [Elektronische versie]. *Journal of Systems and Software, 85,* 1083-1095.

Auteursrechtelijke overeenkomst

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
Continue monitoring als audittool bij cloud computing

Richting: **master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica**
Jaar: **2013**

in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Niet tegenstaand deze toekenning van het auteursrecht aan de Universiteit Hasselt behoud ik als auteur het recht om de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij te reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

Ik bevestig dat de eindverhandeling mijn origineel werk is, en dat ik het recht heb om de rechten te verlenen die in deze overeenkomst worden beschreven. Ik verklaar tevens dat de eindverhandeling, naar mijn weten, het auteursrecht van anderen niet overtreedt.

Ik verklaar tevens dat ik voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen heb verkregen zodat ik deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal mij als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze overeenkomst.

Voor akkoord,

Huysmans, Kristof

Datum: **30/05/2013**