GÖTEBORGS UNIVERSITET

MoInteknologi för företag

Förväntningar och riskmedvetenhet

Cloud Computing for businesses

Expectations and risk awareness

Martin Hanson
Martin Magnusson

Kandidatuppsats iInformatik

Rapport nr. 2011:017
ISSN: 1651-4769

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2011

Förord

Denna kandidatuppsats är ett avslutande moment i vår utbildning där vi skall använda oss av de kunskaper vi samlat på oss under utbildningen för att undersöka ett område som är intressant för oss och för den akademiska världen. Vi har valt det högaktuella ämnet molnteknologi, med inriktning på hur småföretag uppfattar moln, vad de hoppas kunna få ut av dem och vad de är oroliga för. Vi vill tacka vår handledare Ted Saarikko och våra kontakter på Teamster, Hans Hallberg och Thomas Lydhig.

Abstrakt

Företag är ständigt på jakt efter teknologier som kan minska deras kostnader, inte minst för informationsteknologier. Molnet har de senaste åren utmålats som en trendig kostnadsbesparare och nyttohöjare. Denna uppsats innehåller en undersökning om hur små till medelstora företag uppfattar risker och möjligheter med molnteknologi samt hur dessa relaterar till verkligheten. Vi ska med hjälp av intervjuer och ett grundläggande teoriarbete försöka bringa klarhet i många av de frågor som finns kring molnet. Resultatet skall kunna vara ett stöd för företag som vill flytta ut delar av sin verksamhet men inte i nuläget har kunskap om detta.

Nyckelord: Moln, mindre företag, säkerhetsrisker, lagstiftning, SaaS

Summary

Businesses are constantly in search of technologies that can cut their expenses, not least IT expenses.In the last few years, cloud computing has become the latest trend both for its cost efficiency and for added value. This thesis contains research about how small to medium sized businesses perceive risks and possibilities with cloud technology and how these perceived risks relate to real world risks and possibilities. With the use of interviews and base in theories, we try to shed light on many of the issues surrounding cloud computing. The resulting thesis can be a support for businesses who wish to move parts of their organization into the cloud computing realm, but lack the sufficient knowledge about this.

Keywords: Cloud computing, small business, security risks, legality, SaaS

Innehållsförteckning

1. Inledning

1.1. Moln

Det råder ingen tvekan om att molntjänster är bland de hetaste ämnena i IT-världen just nu. För att fastslå detta kan man besöka mediehuset idg:s startsida, där figurerar ordet 'moln' just nu 17 gånger.[1] Skulle man behöva mer än så för att övertygas räknar marknadsanalytikerna Gartner med en årlig tillväxt på över 20% för molntjänster fram till 2014, vilket kommer leda till en marknad värd närmare 150 miljarder dollar:

"The forecast shows that the worldwide cloud services market will be worth $68.3 billion by the end of 2010, and that by 2014 the market will grow to be worth $148.8 billion. This represents a compound annual growth rate of 20.5%." [2]

Oenighet råder däremot kring vad molntekniken egentligen innebär[3,4,5] och hur företag på bästa sätt bör dra nytta av molnet. Företag har svårt att veta vilka fördelar molnet kan ge dem, och om molnet överhuvudtaget är något för dem. En ytterligare aspekt där kunskap behövs är säkerhet. Teknik som molnteknologier, där ett företag tar hand om ett annat företags data i olika utsträckning, ställer nya krav på säkerhetstänkande från både leverantörer och kunder. Därtill kommer en rad legala aspekter, dels nationella lagar, t.ex. personuppgiftslagen, men även internationella lagar. EU kan t.ex. sätta stopp för att flytta persondata ut ur EU, och USA:s omfattande terrorlagar skulle kunna göra att man löper en risk ifall man råkar ligga i samma moln som en annan verksamhet som skulle kunna dra USA:s myndigheters ögon till sig. Samtidigt har beslutsfattare i företag ofta bildat sina uppfattningar mycket på populärvetenskap och vi vill undersöka huruvida dessa stämmer överens med vad molnet verkligen är och kan ge.

En studie som Marknadsanalytikerna IDC gjorde 2008där de frågade IT-chefer om deras inställningar till och förväntningar på molntjänster[6] tangerar denna uppsats ämne.Vi är docknyfikna på vad personer på ett svenskt företag har för åsikter, och ifall de 3 år som gått, när molnteknik fått mogna och placera sig i människors medvetande har förändrat inställningen till molnet.

[1] www.idg.se hämtat 2011-05-19
[2] Gartner: Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014, 2010-06-02
[3] www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality_1.html hämtat 2011-05-19
[4] www.windowsitpro.com/article/cloud-computing2/cloud-computing-confusion hämtat 2011-05-19
[5] www.networkworld.com/news/2009/072909-cloud-confusion.htmlhämtat 2011-05-19
[6] http://blogs.idc.com/ie/?p=210hämtat 2011-05-25

1.2. Syfte

Syftet med vår uppsats är att svara på om företags förväntningar och farhågor angående molnteknologi motsvaras i verkligheten. Förhoppningsvis kommer man också efter att ha läst uppsatsen ha en klarare bild av vad molnteknik innebär samt vilka aspekter man behöver tänka på som företagare när man överväger att flytta dit. Vi kommer att avgränsa våra undersökningar till molnteknik med inriktning på e-post. Till vår hjälp kommer vi använda artiklar och uppsatser i ämnet, samt intervjuer med nyckelpersoner från ett företag.

1.3. Frågeställning

Vi har definierat två frågeställningar, när vi svarar på dessa är vi främst fokuserade på e-post i molnet, men mycket av våra resonemang kommer ändå vara allmängiltiga.

Hur förhåller sig ett företags förväntningar på en molnmigration till de möjligheter molnleverantörer kan erbjuda?

Hur förhåller sig ett företags farhågor kring molnet med avseende på lagar och säkerhet till verkliga risker?

1.4. Disposition

Efter det här inledande avsnittet kommer vi beskriva samt motivera de metoder vi har valt för att utföra undersökningarna vi vill göra för att bygga vår uppsats kring. Sedan följer ett avsnitt där vi presenterar en tidigare undersökning av attityder. Efter det kommer en teoridel. I denna beskriver vi mer ingående vad moln är, samt exemplifierar några lösningar som kan vara aktuella för ett företag som vill flytta sin e-post. Därefter går vi in på säkerhetsaspekter och lagar som är viktiga när man lägger verksamhet i molnet. Sedan följer en del där vi presenterar det resultat vi fått av våra intervjuer. Efter detta diskuterar och analyserar vi våra resultat och ger en sammanfattning av vad vi kommit fram till, samt vad vi tycker är viktigast att tänka på.

2. Metod

Vårt arbete börjar med en litteraturstudie, för att vi vill sätta oss in i alla de aspekter kring molnet vi är osäkra på, samt för att kunna skapa bra intervjufrågor för vår undersökning. Som stöd till att skapa en korrekt och givande uppbyggnad av våra intervjuer kommer vi att använda boken “Forskningsmetodikens grunder” av Patel och Davidson.

2.1. Litteratursökning

För att lära oss mer om molnet har vi samlat in en mängd olika artiklar och andra typer av information, i huvudsak från vad Patel och Davidson (2003) kallar för sekundärkällor, d.v.s. inte förstahandsskildringar, utan beskrivningar och sammanställningar av olika slag. Vi har använt oss av Göteborgs universitet och Lunds universitets databaser för att finna relevanta artiklar och uppsatser, och utifrån det har vi även kunnat identifiera källor som ofta refereras till och söka upp dem genom att använda Google Scholar, Googles söktjänst för vetenskapliga publikationer. Vi har använt oss av sökord som; ”molntjänster”,”cloud computing”, ”cloud computing risks”och ”cloud computing privacy”. Bara på Google Scholar gav ”cloud computing” 390000 träffar. Vi har inte använt oss av några böcker i ämnet, då det finns ganska få och det ofta är enklare att hitta bra och framförallt aktuell forskning via Internet. Vi har även i viss mån använt oss av populärvetenskapliga artiklar, som inte ger så mycket fakta, men skapar en bra överblick och dessutom ger en känsla för just begreppsosäkerheten kring molnteknik. Eftersom molnteknik är ett område under snabb utveckling har vi favoriserat nyare artiklar över äldre.

2.2. Tidigare studie

Vi har även en studie av IDC angående inställningar och tankar kring molnet att tillgå, där de frågat 244 IT-professionella hur de ser på molntjänster och vad de prioriterar när de utvärderar molnleverantörer. Denna undersökningen är dock 3 år gammal, vilket är en evighet med avseende på molnområdets nuvarande utvecklingstakt. Vi vet heller inte hur deras urval ser ut och om det är applicerbart på svenska förhållanden. Därför finner vi det viktigt att komplettera med vår studie av ett svenskt företag.

2.3. Teamster AB

För att få denna kompletterande bild har vi kontakt med ett företag som heter Teamster AB. Teamster är ett göteborgsbaserat industriautomationsföretag med 50-talet anställda. Man arbetar mot olika typer av tillverkningsindustri, med Volvo som största kund. Teamster har två kontor på Hisingen i Göteborg, där man i nuläget hanterar sina egna lösningar för både e-post och backup. Dessa lösningar börjar bli gamla och en uppdatering av systemen närmar sig sakta men säkert. Eftersom man även planerar skära ner på sin interna IT-personal vill man utvärdera om skulle löna sig att flytta dessa viktiga funktioner till en molnlösning, samt få kunskap om de andra aspekter som är viktiga att tänka på, såsom säkerhet och möjlighet att i ett senare skede kunna byta leverantör eller gå tillbaks till intern drift. Genom att en av

uppsatsförfattarna arbetar på Teamster och fick en förfrågan om att skaffa ett beslutsstöd kring detta var vägen öppen för oss att i sin tur använda oss av Teamster som underlag för våra undersökningar.

2.3.1. Intervjupersoner

På Teamster finns två personer som har det yttersta ansvaret för IT-beslut, och vi fick tillgång till båda dessa. Vi ansåg inte att någon annan på Teamster var relevant för undersökningens syfte. VD:n har möjligen farhågor angående säkerhetsaspekter, men i slutändan är det dessa två personer som är både beslutande och drivande i IT-frågor. Dessa personer är:

Hans Hallberg, Teknikchef på Teamster. arbetat i 23 år på företaget. Elektroingenjör.

Thomas Lydhig, Robotautomationschef med 19 år på företaget. Automationsingenjör.

2.3.2. Intervjuer

Vi utförde våra två intervjuer i Teamsters lokaler på Hisingen i Göteborg. De gick till så att vi satt ned med papper, penna samt inspelningsutrustning och ställde ett fåtal frågor med avsikt att låta våra respondenter tala så fritt som möjligt, men med möjligheter för oss att leda in dem på de exempel vi var intresserade av. Detta har förstås den nackdelen att det finns en risk att man lägger ord i munnen på respondenten, men när vi endast hade ett par intervjuobjekt behövde vi få deras synpunkter på det som vi identifierat som de viktigaste frågorna. Våra intervjuobjekt var lite olika pratsamma, vilket ledde till att en intervju klockade in på strax över 15 minuter och den andra på närmare 30 minuter.

2.4. Intervjumetodik

För att få en bild av vad ett företag prioriterar, vad de förväntar sig av molnet, vilka säkerhetsaspekter de tycker är viktiga utför vi ett par intervjuer med nyckelpersoner på ett litet företag. Eftersom vi vill få en bild av hur vårt exempelföretag uppfattar moln och sig själva i förhållande till molnet, använder utför vi kvalitativa interjuer[7]. Vi ställer således öppna frågor med låg grad av strukturering[8].

2.4.1. Syftet med Intervjuerna

Som tidigare nämnt, det vi vill är att få en uppfattning om hur ett företag prioriterar och värderar olika säkerhetsaspekter, hur de tror att deras verksamhet påverkas av att använda molnet samt hur medvetna de är om de lagar som gäller. Vi har med hjälp av vår litteraturstudie identifierat de områden vi tror är av störst vikt och använder detta som underlag för intervjufrågorna, men vi kommer även ställa frågor av en mer öppen art för att intervjupersonerna skall kunna ge oss de infallsvinklar vi som IT-studenter kanske missar av olika anledningar. Vi ställer också frågor som rör företagets syn på sin egen kompetens och sina möjligheter att hantera fallgropar som kan uppstå till följd av molnmigreringen.

[7]Patel & Davidson (2003)
[8]Patel & Davidson (2003)

2.4.2. Analys

Enligt Patel och Davidson består forskarens arbete i att relatera teori och verklighet till varandra[9]. Vi kommer att samla ihop teoretisk data ur litteratur och artiklar och sen jämföra med den empiri vi får från våra kvalitativa intervjuer. När man gör kvalitativa bearbetningar finns enligt Patel och Davidson ingen universell metod, utan det är upp till var och en att hitta en metod som leder fram till en bra text.[10] Vår metod kommer gå ut på att vi tar datan ur våra intervjuer och strukturerar upp den efter likheter och avvikelser mellan intervjuobjektens uppfattningar och jämför med den tidigare studien och ställer det mot vad våra teoristudier har gett oss för uppfattningar.

2.4.3. Metodkritik

Eftersom vi endast använder oss av ett företag i våra undersökningar är förstås reliabiliteten förhållandevis låg i vår empiri, det kan mycket väl vara så att det företag vi har haft kontakt med av någon anledning inte är representativt för företag i samma storlek. Det är också ett problem att vi har stora kunskaper i ämnet när vi utför intervjuerna, något som gör att vi kan vara färgade och omedvetet leda in respondenter på de spår vi själva identifierat. Ett sätt att få bättre data hade varit att komplettera med en enkät som skickades ut till ett bredare underlag. Tyvärr fanns inte tiden att både hinna sätta sig in i teorin, skapa intervjuer och dessutom göra en enkätundersökning.

[9]Patel & Davidson (2003)
[10]Patel & Davidson (2003)

3. Tidigare undersökning

Marknadsanalytikerna International Data Corporation (IDC) utförde 2008 en undersökning där de frågade 244 IT-chefer om deras inställning till molnet och deras förväntningar på molnleverantörer.[11] Deras svar rankade fördelarna med moln/on-demand-modellen enligt följande:

Easy/fast to deploy:	63,9%
Pay only for what you use:	61,5%
Less in-house IT staff, costs:	57,0%

Tabell1: Rate the benefits commonly ascribed to the cloud/on-demand model (källa: http://blogs.idc.com/ie/?p=210)

Som synes i *Tabell1*är förväntningarna spridda, med enkelheten i konfiguration och möjligheten att bara betala för det man använder som vanligast nämnnda fördelar.

IDC bad även respondenterna att bedöma riskerna/utmaningarna med moln-modellen.

Security:	74,6%
Performance	63,1%
Availability	63,1%

Tabell2: Rate the challenges/issues ascribed to the cloud/on-demand model (källa: http://blogs.idc.com/ie/?p=210)

Säkerhet är enligt*Tabell2*den i särklass vanligaste utmaningen, med prestanda och tillgänglighet följande. Att säkerheten ligger högt förvånar inte efter de olika faktorer vi har stött på som skulle kunna påverka.

En annan fråga IDC ställde som är intressant för vår uppsats var vilka attribut som var viktigast vid val av leverantör.

Offer competitive pricing:	83,2%
Offers performance-level assurances/SLAs	81,1%
Understanding of my business and industry	68,0%
Can move cloud offerings back on-premise	67,2%

Tabell3: Importance of IT cloud service supplier attributes (källa: http://blogs.idc.com/ie/?p=210)

Som väntat är priset vanligen den viktigaste faktorn när ett företag beslutar om investeringar. Tittar man i *Tabell3*ser man dock att tillgänglighet inte ligger långt efter.

[11]http://blogs.idc.com/ie/?p=210

4. Teori

4.1. Vad är Molnet?

Till att börja med vill vi med denna uppsats försöka att bringa lite klarhet i vad molnet egentligen är. Knorr ochGrumanskriver:

"As a metaphor for the Internet, 'the cloud' is a familiar cliché, but when combined with 'computing,' the meaning gets bigger and fuzzier. Some analysts and vendors define cloud computing narrowly as an updated version of utility computing: basically virtual servers available over the Internet. Others go very broad, arguing anything you consume outside the firewall is 'in the cloud', including conventional outsourcing."[12]

De identifierar alltså två definitioner, en snävare, där cloud computing bara är virtuella servrar, och en väldigt vid, där allt utanför den egna brandväggen är moln.

US National Institute for Standards and Technology definierarmolnet:

"A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[13]

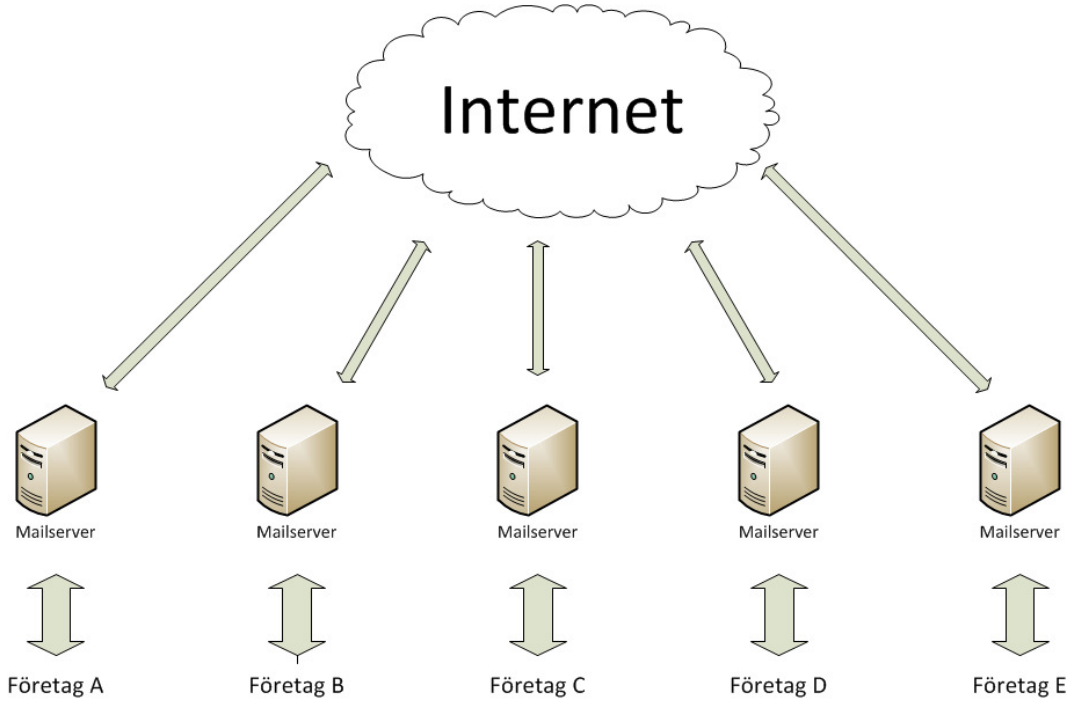
Denna definition ligger någonstans emellan Knorr och Grumans definitioner, den belyser dessutom på ett bra sätt en av molntjänsters styrkor, som är den enkla skalbarheten. Som citaten ovan visar, och som tidigare nämnts, råder en del förvirring kring begreppet moln. För denna uppsats, och med vår avgränsning, är det NIST:s definition som passar bäst.

Sammankopplat med molnteknologi är begreppet "as a Service", som syftar till att utgångspunkten är att man köper en *tjänst* av en leverantör, man bryr sig inte om hur tjänsten utformas på leverantörens sida (den finns i ett "moln" ur vilket man hämtar det man behöver), istället kan man helt fokusera på vad tjänsten utför. Man brukar tala om 3 huvudkategorier när det gäller "as a Service". **PaaS** eller Platform as a Service innebär att en molnleverantör tillhandahåller en mjukvaruplatform som användarens mjukvara körs på. Ett exempel är Google Apps engine[14]. **IaaS**, Infrastructure as a Service, innebär att en molnleverantör tillhandahåller dataresurser som till exempel lagring i molnet där användaren sedan placerar sin mjukvara. Till exempel SimpleDB[15]. **SaaS** i sin tur är när applikationer tillhandahålles och levereras via en webbläsare, såsom t.ex. Google Docs och Gmail[16].

[12]www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 hämtat 2011-05-16
[13]Auty et al (2010), s.659
[14]Auty et al (2010)
[15]Auty et al (2010)
[16]Auty et al (2010)

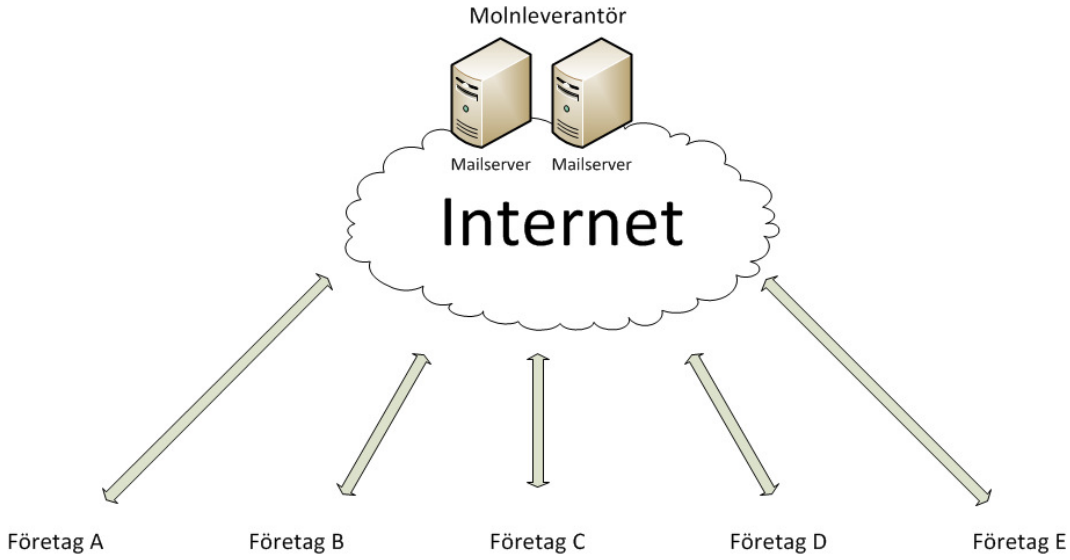
4.1.1. Molnmodellens resurseffektivisering

För att visa hur molnteknologi effektiviserar resursanvändning har vi gjort två figurer. *Figur 1* visar hur fem separata företag traditionellt skulle sätta upp sina epostlösningar, där de alla behöver sätta upp sin egen server och koppla den mot Internet.



Figur 1: traditionell utformning (Källa: egen figur)

I *Figur 2* beskrivs istället hur motsvarande behov tillgodoses av en molnleverantör.



Figur 2: molnlösning (Källa: egen figur)

Eftersom företagen tidigare troligen endast använde en fraktion av sina respektive servrars kapacitet vardera kommer molnleverantören kanske bara behöva ha två servrar för att tillgodose sina kunders behov.

4.2. Molnaktörer

Det finns en hel del olika varianter av molntjänster för företag, vi har valt att fokusera på jättarna, Microsoft och Google. Microsoft därför att det är den lösning vårt företag är bekanta med idag, och Google för att de är en stor och ansedd aktör med en aggressiv prissättning. När det gäller Microsoftlösningar är det antingen olika mindre bolag som driftar dessa, via Hosted Exchange, eller Microsofts nya molntjänst som fortfarande är i Beta-stadiet, Office 365. Den utlovade driftsäkerheten hos de olika aktörerna är såpass hög att, så länge de håller vad de lovar, är det egentligen ingen större fråga. Google lovar 99,9%[17] och en siffra som nämnts av en Hosted Exchange-leverantör var 99,8%[18]. Microsoft utlovar likt Google 99,9%[19] för Office 365.

4.2.1. Hosted Exchange

Microsoft Exchange är den vanligaste lösningen för e-post med 65% av marknaden[20], och den lösning vårt exempelföretag använder sig av idag. Hosted Exchange innebär att man helt enkelt hyr kapacitet ur ett företags Exchangemoln istället för att drifta en egen server. Bland fördelarna med att använda sig av Exchange är deras väl utvecklade integration med marknadsledande[21] kontorsmjukvaran Microsoft Office Suite..

4.2.2. Google Apps for Business

Google är förstås en jättelik spelare på molnmarknaden. Som de själva uttrycker det:

"Cloud computing is in Google's DNA"[22]

Alla Googles tjänster är mer eller mindre molnbaserade, och de har en användarbas som få kan konkurrera med. Det är svårt att hitta definitiva siffror, men Gmail sades i februari 2010 ha 170 miljoner användare[23] och Googles söktjänst uppskattas serva 2 miljarder sökningar dagligen (2008)[24]. (Yahoo! Mail säger sig vara störst med sina 270 miljoner användare, men alla dessa siffror bör tas med en nypa salt.) Detta innebär att Googles moln är enormt, och skalbarheten för användare och kunder för de flesta syften är obegränsad. Dessutom erbjuder Google Apps for Business en rad molnbaserade kollaborationsverktyg som ger ett avsevärt mervärde jämfört med en Hosted Exchange-lösning, exempelvis Google Docs, Google Calendar och Google Groups.

[17] www.google.com/apps/intl/sv/business/features.html hämtat 2011-05-19
[18] www.cygrids.com/Hosting/Software-as-a-Service/Hosted-Exchange-2010/ hämtat 2011-05-19
[19] www.microsoft.com/en-us/office365/online-software.aspx hämtat 2011-05-10
[20] Ferris Research (2008) (http://www.ferris.com/?p=318858)
[21] www.webmasterpro.de/portal/news/2010/02/05/international-openoffice-market-shares.html
[22] www.google.com/apps/intl/en-GB/business/cloud.html
[23] www.numberof.net/number-of-gmail-users/hämtat 2011-05-12
[24] www.mathewingram.com/work/2008/09/05/how-many-searches-has-google-done/ hämtat 2011-05-12

4.2.3. Office 365

Istället för Hosted Exchange kan man välja att vänta på Microsofts konkurrent till Google Apps, som ännu är på betastadiet men förväntas lanseras under året. I denna ingår en mail-lösning motsvarande Hosted Exchange. Dessutom ingår i vissa planer Office Web Apps, d.v.s. Office-paket på webben (likt Google Docs), samt Sharepointfunktionalitet[25] (Sharepoint är ett verktyg för att dela dokument och samarbeta).

[25] www.microsoft.com/en-us/office365/small-business/about.aspx

5. Säkerhet

Molntjänster är ett aktuellt ämne inom IT med många positiva omdömen. Men det finns en aspekt av molntekniken som kastar en skugga på det positiva med molntjänster, nämligen säkerheten. Det finns en utbredd osäkerhet bland företag när det gäller att lämna ut viktig data till en molnleverantör. I maj 2010 utförde Bloomberg-businessweek.com en undersökning bland mindre företag om deras inställning till molntjänster. 75% av de 65 respondenterna svarade att säkerheten är det största orosmolnet om man vill använda sig av molntjänster. I en annan undersökning gjord av Gartner frågade man chefer på olika företagsdatacenter vad det främsta skälet är till att man inte flyttar till molnet, 85% svarade då ”säkerheten” [26].

Säkerheten och säkerhetsrisker är ett väldigt brett område men samtidigt en väldigt viktigt aspekt när man överväger att flytta till molnet. Följande avsnitt ämnar ta upp en del av de risker som finns och vad som kan göras för att minimera dessa och därmed förtydliga vad ett företag behöver veta om de vill flytta till molnet.

Säkerheten i molnet är viktig eftersom informationen i molnet inte får spridas till obehöriga personer eller företag. Skulle ett företags affärsdata eller företagshemligheter spridas till obehöriga kan det få stora negativa konsekvenser[27]. Molnet står dock många gånger inför samma risker som andra IT-system. Den stora skillnaden är att information och data flyttas till en tredjepart vilket skapar nya risker[28].Enligt den amerikanska federala lagen FISMA (Federal Information Security Management Act of 2002)[29] finns det tre stycken säkerhetsmål för information och informationssystem; sekretess, integritet och tillgänglighet.Listan på säkerhetsrisker kan göras väldigt lång, för att nämna några exempel[3031]:

Mänskliga faktorer

- En anställd hos molnleverantören kan medvetet ändra eller skada en kunds data i molnet.
- Krypteringsnycklar kan gå förlorade och hamna hos en obehörig tredje part.

Tekniska faktorer

- Tillgången till molntjänster sker många gånger via webbläsaren, svagheter i själva webbläsaren kan därför utnyttjas för komma åt information i molnet.
- Överbelastning av molntjänsten kan leda till otillräcklig åtkomst eller ingen åtkomst alls av molnet.
- Undermålig kryptering kan leda till att data riskerar att hamna hos en obehörig part när information skickas mellan molnet och företaget.

[26]Conway (2011)
[27]Saripalli& Walters (2010)
[28]Zhang et al (2010)
[29]Saripalli& Walters (2010)
[30]Saripalli& Walters (2010)
[31]Auty et al (2010)

Ett moln kan antingen klassificieras som ett privat moln, ett publikt moln eller som en hybrid en kombination av privat och publikt moln. Privata moln har fördelen att det finns inom företagets gränser och kan då dra fördel av redan existerande säkerhetsrutiner. Men fördelen som ett publikt moln erbjuder finns inte, nämligen att flytta företagsdata till en molnleverantör utanför företaget och att då företaget slipper sköta detta. Men när ett moln blir publikt uppstår säkerhetsrisker[32]. När ett företag outsourcar till molnet blir det svårare att vidhålla dataintegriteten och tillgängligheten till datan. Utmaningen är idag att datan alltid ska vara tillgänglig samtidigt som den är skyddad.

Det finns olika typer av säkerhetsrisker och det finns idag olika modeller och ramverk för att bedömma riskerna och vad eventuella konsekvenser kan bli om säkerheten brister. Microsofts STRIDE-modell (**S**poofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege)[34] är en av de mer populära modellerna för att bedöma riskerna[35]. STRIDE-modellen är dock i första hand framtagen för "traditionella" IT-system.

Cloud Security Alliance har tagit fram tolv stycken nyckelområden för molnet som måste fungera både ur en stratetgisk synpunkt och sett till säkerhetsaspekter för att uppnå bästa möjliga molnmiljö[36]. Olika områden blir viktigare än andra beroende på vilken "molntyp" som används (SaaS, IaaS, PaaS). Eftersom vi inriktat oss på SaaS är till exempel applikationssäkerhet väldigt viktigt[37]. Exempel på ett antal områden är följande:

- **Styrning och riskhantering**
  Berör en organisations förmåga att styra och kontrollera de risker som uppstår vid användandet av molnet.
- **Överensstämmelse och revision**
  Beskriver hur en organisation bör göra återkommande revisioner för att se hur användandet av molnet påverkar och överenstämmer med organisationens verksamhet. Till exempel att molnets säkerhetspolicy stämmer överens med organisationens säkerhetspolicy.
- **Informationshantering**
  Hur själva hanteringen av datan i molnet fungerar. Vem som får tillgången till den, vem som ansvarar för den, vem som ansvarar för att skydda datans integritet etc.
- **Juridik**
  De juridiska problem som kan uppstå vid användandet av molnet till exempel integritetslagar.
- **Flyttbarhet och interoperabilitet**
  Möjligheterna att flytta data mellan olika molnleverantörer eller att flytta tillbaka datan "in-house".

[32]Auty et al (2010)
[34]msdn.microsoft.com/sv-se/library/ee823878(v=cs.20).aspxhämtat 2011-05-09
[35]Saripalli& Walters (2010)
[36]Cloud Security Alliance (2009)
[37]Zhang et al (2010)

- **Applikationssäkerhet**
  Handlar om att de applikationer som körs eller utvecklas i molnet måste ha en hög säkerhet.

Cloud Security Alliances guide finns att läsa i sin helhet på cloudsecurityalliance.org.

5.1. Krav på molnleverantören

Det är mycket viktigt att veta om en molnleverantör har en uppsatt plan för att identifiera säkerhetsrisker och hur man skyddar sig mot dessa. I ett avtal med en molnleverantör bör det ingå en plan för hur denne hanterar risker och hur man arbetare för att minimera riskerna[38]. Problemet är idag att många molnleverantörer har avtal som inte kan påverkas och accepteras inte avtalet blir det ingen affär. Detta beror delvis på att det skulle vara väldigt tidskrävande för en molnleverantör att specialanpassa varje avtal för varje enskild kund.Det är därför svårt för en organisation att påverka avtalet och anpassa det efter just deras behov. Det är även svårt för en organisation att undersöka en molnleverantörs tillgänglighet och säkerhet och därmed veta om det uppfyller organisationens krav[39].

I första hand bör en molnleverantör ha identifieratsina viktigaste nyckelområden och därefter gjort en riskanalys. En riskanalys består av att identifiera hot från skadlig mjukvara och crackers och deras möjligheter att använda sig av svagheter i till exempel infrastrukturen eller i applikationer för att komma åt information. I en riskanalys ingår även att identifiera sårbarheten. Både ur ett tekniskt perspektiv för att hitta svagheter i molnet men även organisatoriska svagheter[40]. För att nämna ett exempel; har molnleverantören rutiner för att plocka bort en före detta anställds inloggningsuppgifter? Har de inte det finns risken att han/hon får tillgång till molnet och plockar ut eller ändrar information[41].

I en riskanalys ingår även att bedöma riskerna utifrån hur sannolikt det är att det inträffar. Och vad konsekvenserna kan bli om en svaghet i molnet skulle utnyttjas av en obehörig part[42].

Etablerade och bedömda risker måste åtgärdas för att reducera riskerna till en acceptabel nivå för att skydda molnmiljön och datan som molnet innehåller. Områden där riskerna måste minimeras är till exempel[43][44]:

5.1.1. Mänskliga faktorer

- Införa säkerhetsrutiner som regelbundet uppdateras
- Övervaka riskerna, kan nya risker dyka upp om ändringar görs i molnet?

[38] Zhang et al (2010)
[39] Saripalli & Walters (2010)
[40] Zhang et al (2010)
[41] Zhang et al (2010)
[42] Zhang et al (2010)
[43] Saripalli & Walters (2010)
[44] Zhang et al (2010)

- Se till att personalen har kompetensen och medvetenheten att sköta en molntjänst.

5.1.2. Tekniska faktorer

- Bygga och underhålla en säker infrastruktur för molnet.
- Höga krav på Identifiering och åtkomstkontroll.
  Identifiering är viktig av flera anledningar bland annat därför att organisationer och användare ska få tillgång till rätt information och service. Om ett företag skulle få tillgång till ett konkurrerande företags affärsdata skulle det kunna få mycket allvarliga konsekvenser. Men identifiering är även viktigt ur molnleverantörens synvinkel för att de ska kunna fakturera rätt kund för den tjänst de använder.
- Övervakning av molnetför att hitta svagheter och försök till intrång i molnet. Att övervaka ett moln är dock inte helt problemfritt eftersom molnet består av flera olika delar som kräver olika typer av övervakning.
- Kryptering är en mycket viktig faktor när det gäller att skydda skydda datan i molnet. Även kommunikationen mellan molnet och användaren är beroende av säker kryptering för att skyddas mot att obehöriga kan läsa av den. Hur pass skyddad datan är när den ligger i molnet är dock ett ämne som är under ständig debatt. I dagsläget gäller två grundläggande principer, antingen lagrar ett företag bara data som inte utgör någon säkerhetsrisk om den hamnar hos en obehörig part. Eller så krypteras datan innan den skickas till molnet och dekrypteras inte förrän den är tillbaka på företag igen. Detta för att öka skyddet av datan ytterligare för när datan väl ligger i molnet har ett företag ingen möjlighet att påverka säkerheten.

Det bör även påpekas att ovanstående åtgärder som presenterats för att minimera risker även kan användas av ett företag eller organisation som ska flytta till molnet. Svag säkerhet från användarens sida kan också utgöra en säkerhetsrisk som kan utnyttjas för att komma åt information i ett moln[45].

6. Lagstiftning

Det finns lagstiftning som kan påverka molnet och molntjänster. Det finns lagstiftning som reglerar hur data får flyttas mellan länder och då framförallt data som berör personuppgifter. Men även lagstiftning som reglerar huruvida myndigheter kan få tillgång till den data som finns i molnet. Följande avsnitt ämnar att ta upp ett antal lagar som kan påverka molnet och användandet av molnet.

När det kommer till molnet och lagstiftning pratar man om två typer av moln; inrikesmoln och moln som sträcker sig över nationsgränser. Har en molnleverantör hela sin verksamhet inom ett land lyder molnleverantören under en lagstiftning och behöver således bara följa den gällande lagstiftningen. Däremot när en

[45]Zhang et al (2010)

molnleverantörs verksamhet sträcker sig över nationsgränser kan det uppstå problem[46]. När det gäller hur data som berör personuppgifter får flyttas mellan länder regleras det till exempel av Personuppgiftslagen (PuL)[47] i Sverige och av Dataskyddsdirektivet[48] inom EU. Problemet är att en molnleverantör ofta har sina datacenters utspridda på olika geografiska platser och därmed är det väldigt svårt för en användare att veta var deras data befinner sig rent fysisk som i sin tur kan innebär att användaren bryter mot gällande lagstiftning[49]. Molnleverantörer som Microsoft har kommit med krav på att till exempel Dataskyddsdirektivet måste uppdateras. Dataskyddsdirektivet infördes 1995 när datan sällan flyttades och blir därför ett problem för molntjänster eftersom data ofta förflyttas inom molnet[50]. Det finns även lagstiftning när det gäller olika myndigheters rätt att läsa av internettrafik och vad som lagras i databaser för att bland annat motverka terrorism. USA PATRIOT Act[51], FRA-lagen[52] och Datalagringsdirektivet[53] är några exempel på sådana lagstiftningar. Datalagringsdirektivet är dock en lag som riktar in sig på individer och är mer intressant när det gäller användandet av molnet för privatpersoner. USA PATRIOT Act är en väldigt omdebatterad lag även i molnsammanhang eftersom den ger amerikanska myndigheter stora möjligheter att ta del av en molnleverantörs data.

6.1. Dataskyddsdirektivet

Dataskyddsdirektivet antogs av Europeiska unionen 1995 i syfte att skydda enskilda personers integritet vid behandling av personuppgifter. I Sverige uppfylls direktivet genom Personuppgiftslagen (PuL). Tanken med Dataskyddsdirektivet är även att underlätta reglerna för att tillåta ett fritt flöde av personuppgifter inom EU. Det innebär inte att personuppgifter ska få spridas fritt utan att det inte ska spela någon roll i vilket land personuppgifterna lagras[54].

[46]Svantesson & Clarke (2010)
[47]www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/ hämtat 2011-04-28
[48]Direktiv 95/46/EG
[49]Svantesson & Clarke (2010)
[50]computersweden.idg.se/2.2683/1.289658/microsoft-kraver-eu-lag-for-moln hämtat 2011-05-16
[51]Gellman (2009)
[52]Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet
[53]Direktiv 95/46/EG
[54]Direktiv 95/46/EG

6.2. Personuppgiftslagen (PuL)

Personuppgiftslagen (PuL) trädde i kraft 1998 och skapades för att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas. Personuppgiftslagen bygger på gemensamma regler som har beslutats inom EU det så kallade dataskyddsdirektivet. Det innebär även att andra EU-länder har liknande lagstiftning. Personuppgiftslagens syfte är som sagt att skydda den personliga integriteten dock finns det många undantag, ett är till exempel för journalistiska ändamål. Utgångspunkten i Personuppgiftslagen är dock att den enskilde själv ska avgöra om personuppgifter om honom eller henne får behandlas[55]. Lagen gäller för personuppgiftsansvariga som är etablerade i Sverige. Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter[56].

Vid användandet av molntjänster och molnteknik kan det uppstå problem eftersom det inte alltid är helt klart var informationen som flyttats till molnet fysiskt befinner sig. En molnleverantör kan använda sig av flera leverantörer som i sin tur använder sig av leverantörer i flera led.Ur en teknisk synpunkt kan det också vara svårt att veta var information lagras eftersom molnleverantörens servrar kan vara spridda på flera olika ställen. Information kan därför flyttas mellan olika geografiska områden något som personuppgiftslagen inte tillåter om landet i fråga inte uppfyller kraven för lagring av personuppgifter[57]. Molnet är idag ett så pass aktuellt ämne att Datainspektionen har tagit fram en guide för vad en personuppgiftsansvarig behöver tänka på om ett företag vill flytta till molnet. Datainspektionens guide[58]nämner till exempelatt om ett företag väljer att flytta till molnet är det fortfarande den personuppgiftsansvarige på företaget som har ansvar för behandlingen av personuppgifter. Därför ska den som anlitar en molnleverantör för sin behandling av personuppgifter upprätta ett skriftligt personuppgiftsbiträdesavtal med instruktioner till molnleverantören. Personuppgiftsbiträdesavtalet ska bland annat innehålla instruktioner om att molnleverantören är skyldig att vidta tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Vidare bör den personuppgiftsansvarige undersöka säkerheten hos molnleverantören och till exempel titta på autentisering, behörighetskontroll och kommunikationssäkerhet. Som tidigare nämnt är det inte tillåtet enligt PuL att överföra personuppgifter till ett land som inte uppfyller kraven på skydd av personuppgifter en så kallad “adekvat skyddsnivå”. Det är även den personuppgiftsansvariges skyldighet att ta reda på om en överföring av personuppgifter till ett tredje land är tillåtet.

6.3. FRA-lagen

FRA-laget antogs av Sveriges riksdag den 18 juni 2008 och trädde i kraft 1 januari 2009. Syftet med lagen är att reglera på vilket sätt Försvarets radioanstalt (FRA) får ta del av kommunikation i kabel som passerar Sveriges gränser det vill säga telefon-

[55]www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/hämtat 2011-04-28
[56]www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/hämtat 2011-04-28
[57]www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster-/hämtat 2011-04-28
[58]www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster-/hämtat 2011-04-28

och internettrafik för att skydda Sverige mot till exempel terrorism. Signalspaningen bedrivs genom att internet- och teleoperatörerna måste göra tele- och datatrafiken tillgänglig för FRA. Trafiken filtreras sedan med olika sökbegrepp som bland annat reagerar på olika ord och språk. FRA har också rätt att ta del av trafikdata det vill säga vem som kommunicerar med vem, när, var etc[59].

6.4. USA PATRIOT Act

”Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001” mer känd som ”USA PATRIOT Act” är en samling lagändringar som antogs av USA:s kongress efter terrordåden den 11 september 2001 i syfte att skydda USA mot framtida terroristattacker[60]. Lagen innebär bland annat att amerikanska myndigheter och framförallt FBI (Federal Bureau of Investigation) kan kräva att ett företag lämnar ut affärsdata till dem dock inte utan ett domstolsbeslut. Lagen gäller även molnleverantörer och skulle molnleverantören ha sina servrar i USA finns risken att molnleverantörens kunders affärsdata hamnar hos amerikanska myndigheter[61].

[59]http://www.dn.se/nyheter/politik/snabbguide-vad-handlar-fra-lagen-om hämtat 2011-04-28
[60]http://www.fincen.govhämtat 2011-04-28
[61]Gellman (2009)

7. Empiri

7.1.1. Motivation och förväntningar

Vi ställde en fråga angående Teamsters anledningar till att vilja undersöka om de kan flytta delar av sin IT-verksamhet till molnet. Båda respondenterna var eniga om att *ekonomi* och *driftsäkerhet* var de två största drivkrafterna. TL tog även upp kollaborationsverktyg som en bonus han såg som en motiverande faktor och något man skulle komma att behöva. Att kunna dela med sig av filer och kalendrar till externa parter var också det en fråga som TL såg som viktig för framtiden.

"Driftsäkerheten hoppas vi att den kan bli bättre"

- HH om förhoppningar inför en molnflytt

"Vi behöver göra mer... Köra i samma dokument, samtidigt och redigera. [...] Filareor tillsammans med kunder."

- TL om kollaborationsverktyg

7.1.2. Hinder för att flytta till molnet

Enligt de båda respondenterna skulle ekonomin kunna vara det som hindraren flytt till molnet. TL tyckte det var det enda att oroa sig över, medan HH även nämnde säkerheten som ett potentiellt hinder.

"[om vi] lätt kunde se att det skulle vara billigare att lägga det på nätet än den kostnaden vi har för det idag så skulle inte jag tveka en millisekund att lägga ut det [...] om det är en stor leverantör"

-TL ser ekonomin som enda reella hinder

"Det är både ekonomi och säkerhet."

- HH svarar kort och koncist på frågan.

7.1.3. Säkerhetsrisker

När vi ställde en fråga om vilka säkerhetsrisker man oroades över fick vi inte lika entydiga svar. HH uttryckte oro för datasäkerheten och att information kommer på avvägar. Hans kände även en oro över att ett annat företag (molnleverantören) kan läsa av informationen. TL däremot kände ingen större oro över datasäkerheten eftersom Teamster inte krypterar sin e-post-trafik idag och därför ser han ingen större skillnad. Dessutom är informationen i e-post enligt Thomas inte så pass kritisk. TL var däremot mer orolig över risken att inte kunna byta molnleverantör och att data fastnar hos en molnleverantör (inlåsning).

"[Det är en] obehaglig känsla naturligtvis, finns det möjlighet att se nånting för andra företag, så, då finns ju alltid möjligheten att information läcker ut som inte skall göra"

- HH om risker med att ha data hos ett annat företag.

7.1.4. Juridiska frågor

När det gällde hur olika lagstiftningar påverkar Teamster såg ingen av respondenterna detta som något problem. Den data Teamster använder är inte av intresse för främmande makter, och de är för små och obetydliga för att väcka något intresse. I övrigt räknar man med att det inte är några problem att följa de riktlinjer som är aktuella.

”Nae, det e mindre obehag av det tror jag, än annan typ av åtkomst, från nyfikna anställda hos driftpersonal, den som driftar molnet”

- HH är inte oroad över juridiska risker

7.1.5. Övriga molntjänster

Respondenterna tyckte båda att backup i molnet var något man inte ännu är redo för, men angav lite olika anledningar. HH menade att han inte trodde att prestandan på en sådan tjänst skulle vara tillräcklig, medan TL snarare var orolig över osäkerheten i att inte ha kontrollen på sina egna backuper, ifall något skull hända med företaget man köpte tjänsten av. Däremot nämnde HH Officepaket som molntjänst som möjlighet, och TL var som tidigare nämnt intresserad av de kollaborativa funktionerna som finns i t.ex. Google Apps.

”Prestandamässigt så är jag väl tveksam till backup då, det är ett frågetecken för min del. Jag tycker det är svårt att få prestanda internt på det lokala nätverket, då undrar man hur är detom man skall köra en molntjänst då?”

- HH har frågetecken kring prestanda

“Kärnan, att man kunna dela filer på ett bra sätt via Internet, det är för mig det viktigaste med molnet”

- TL om tjänster som Dropbox

7.1.6. Inlåsning

Vi lyfte också frågan om återflytt eller migrering till en annan leverantör när man inte är nöjd.

”Det är alltid en kostnad om man skall byta och flytta information på det sättet.”

- HH ser problemet med att flytta tillbaka sin data som något man får lösa med resurser.

”Vi har iallafall ställt frågan, det kan jag ju säga, vi har varit ganska tydliga med det från början när vi har pratat om molntjänster, så har flytten vart en sån fråga. Så det e ju första grejen, att man ändå har tänkte på det, den möjligheten.”

[...]

”Vi har ju ställt frågan till exjobbarna!”

- TL menar att det är något man är medveten om och att man hoppas få kunskapen.

8. Diskussion

Vår studie visar att de främsta skälen till att flytta till molnet är ekonomi och driftsäkerhet. Teamster hade även förhoppningar om att kunna använda sig av kollaborationsverktyg för att lättare kunna samarbeta med externa parter i framtiden. Molntjänster har potentialen att bli billigare eftersom molnleverantören tar över resurserna. Ett företag som använder molntjänster kan minska på IT-personalen och behöver inte själva ha servrar på företaget för att hantera till exempel e-post. Detta innebär att resurser kan frigöras till andra ändamål. Företag har dock olika förutsättningar och det går därför inte att generellt säga att alla tjänar på att använda sig av molnet utan varje enskilt företag måste noga utvärdera om molntjänster faktiskt kommer minska deras kostnader.

De molnleverantörer vi har nämnt utlovar idag en driftsäkerhet på väldigt nära 100%. Förutsatt att molnleverantörerna håller vad de lovar kommer förväntningar och krav på hög driftsäkerhet att kunna uppfyllas. I slutändan är det dock upp till varje enskilt företag att bedöma huruvida de litar på molnleverantörernas driftsäkerhet. Önskemålet om att kunna använda kollaborationsverktyg för att underlätta samarbete med externa parter är en förväntning som framförallt Google kan uppfylla i dagsläget. Vår undersökning visade bland annat att möjligheten att dela med sig av kalendrar till externa parter var ett önskemål vilket idag är möjligt genom till exempel Google Calendar.

När det gäller farhågor med molnet visade vår studie att respondenterna på Teamster hade funderat kring detta. Datasäkerheten, oro över att andra personer kan läsa av informationen och risk för inlåsning hos molnleverantören beskrev respondenterna som potentiella farhågor. Farhågor som absolut är realistiska vilket vår litteraturstudie visar. Undermålig kryptering kan påverka datasäkerheten vilket kan leda till att en obehörig part kan läsa av informationen och opålitlig personal hos molnleverantören som medvetet ändrar eller förstör data för att nämna två exempel på risker för företag som har data i molnet. Det är tydligt att det finns risker med molntjänster precis som våra respondenter hävdade. Riskerna är inget som helt går att undvika och det bästa sättet att hantera riskerna är att ha en djup och bred kunskap om molnet. En tydlig plan för att hantera riskerna helt enkelt, både hos kunden och molnleverantören vilket vår litteraturstudie talar om. I våra intervjuer kom det fram att Teamster idag inte har kompetensen för att hantera en molntjänst men att de får skaffa kompetensen om det behövs. En högre kompetens gör att ett företag bättre kan utnyttja fördelarna och bedöma och hantera riskerna med molntjänster.

Respondenterna uttryckte ingen oro för lagstiftning som eventuellt kan påverka molnet. Dels för att de inte har något att dölja för myndigheter och dels för att informationen i deras e-post inte innehåller känsliga personuppgifter. Det är upp till varje enskilt företag att avgöra huruvida gällande lagstiftning kan påverka deras användande av molnet. Ytterst handlar det om vilket typ information som ett företag väljer att lägga ut i molnet.

Sammanfattningsvis finns det fördelar med att migrera till molnet men att det även finns risker och lagstiftning som kan påverka användandet av molntjänster. Det är

upp till varje företag att väga fördelar mot nackdelar vilket underlättas med en bra kompetens och utifrån det avgöra om molntjänster är en tjänst som kan ha en positiv påverkan på företaget.

Jämför vi våra resultat med den tidigare undersökning vi presenterade inledningsvis ser vi stora likheter. Dock med en skillnad; i IDCs undersökning när de frågade om fördelarna med moln hamnade ”lätt att implementera” på första plats och ekonomi först på tredje plats. Våra respondenter nämnde inte ”lätt att implementera” över huvud taget. Detta tillskriver vi den ökade mognad molnet genomgått de senaste 3 åren, vilket gör att man förutsätter att implementering fortlöper smidigt. När det gäller utmaningar och risker med molntjänster har vi likvärdiga svar. Båda i IDCs undersökning och i vår är säkerheten den största utmaningen. Intressant är att våra respondenter inte oroades över lagstiftning och IDCs undersökning finns det inte med. Vi drar därför slutsatsen att lagstiftning generellt inte är en oroande faktor vid en migrering till molnet. Trots att det idag kan vara svårt att kombinera lagstiftning som rör personuppgifter med molntjänster. Vid val av leverantör var priset den viktigaste faktorn enligt IDC precis som våra respondenter också hävdade att främsta skälet för en flytt är ekonomin.

Det är tydligt att det behövs mer forskning kring säkerheten och framförallt mer konkreta bevis kring hur säkerheten kring molnet fungerar. Molnleverantörerna borde framförallt vara intresserade av detta för att dämpa oron och därmed locka till sig fler kunder. Men forskningen behövs även för att kunna minimera nuvarande säkerhetsrisker ytterligare. Vidare borde det bedrivas forskning kring hur lagstiftning som påverkar personuppgifter ska anpassas för molnet. För precis som en del molnleverantörer hävdar är sådan lagstiftning omodern sett ur ett IT-perspektiv och idag svår att kombinera med molntjänster. Det måste dock påpekas att skyddet av den personliga integriteten är viktig, att hitta en lösning som både underlättar för molntjänster och fortfarande skyddar personuppgifter är en svår utmaning.

9. Slutsats

Vår uppsats har visat att ett företag som vill migrera till molnet förväntar sig att det ska bli billigare och att man förväntar sig en hög driftsäkerhet. Molnleverantörer och molntjänster har idag potentialen att minska kostnaderna för ett företag eftersom resurskostnader i form av IT-personal och servrar förflyttas till molnleverantören. Det är dock viktigt att komma ihåg att företag har olika förutsättningar och därför måste varje företag själva räkna på om det blir billigare med molntjänster. Det går alltså inte att säga att alla företag tjänar på molnet.I dagsläget har de molnleverantörer vi nämnt en driftsäkerhet på nära 100% enligt dem själva och det är upp till varje företag att avgöra om man litar på att en molnleverantör har en tillräckligt hög driftsäkerhet för deras behov. Vi drar slutsatsen att molntjänster motsvarar de förväntningar våra studier identifierat.

Vår uppsats har även visat att företags farhågor kring molnet främst handlar om säkerhetsrisker. Till exempel datasäkerhet, inlåsning (att det är svårt att flytta data från en molnleverantör) och även en oro för att andra personer ska läsa av informationen i molnet. Lagstiftning som kan påverka användandet av molnet är dock inget som oroar. Oron som finns kring säkerhet är befogad, det finns risker med molnet men de är hanterbara om det finns kompetens och medvetenhet på företaget för hur molnet ska hanteras. Lagstiftning kan även utgöra ett problem speciellt om personuppgifter ska lagras i molnet och det är upp till varje företag att känna till gällande lagstiftning och hur den ska appliceras på molnet. Vår slutsats är att företag har en ganska bra uppfattning om vari riskerna ligger.

10. Referenser

Auty, M., Creese, S., Goldsmith, M., och Hopkins, P., Inadequacies of Current Risk Controls for the Cloud, 2nd *IEEE International Conference on Computer and Information Technology (2010): 659-666*

Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 (2009)*

Conway, G. *Introduction to Cloud Computing (2011),* Innovation Value Institute

Davidson, B.och Patel, R., *Forskningsmetodikens grunder,* 3:e upplagan, Lund: Studentlitteratur AB, 2003

Gartner,*Forecast:Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014,*(2010)

Gartner, *Exploit the Differing Business Models of Google and Microsoft for Cloud Office, E-Mail and Collaboration Services*(2010)

Gellman, R., Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, *World Privacy Forum (2009)*

Saripalli, P. och Walters, B., QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security, *IEEE 3rd International Conference on Cloud computing (2010): 280-288*

Svantesson, D., Clarke, R., Privacy and consumer risks in cloud computing, *Computer Law & Security Review 26 (2010)*: 391-397.

Zhang, X., Wuwong, N., Li, H. och Zhang, X., Information Security Risk Management Framework for the Cloud Computing Environments, *IEEE 10th International Conference on Computer and Information Technology (2010):* 1328-1334