LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Krav för säkra molntjänster

Kandidatuppsats, 15 högskolepoäng, SYSK01 och SYSK03 i informatik

Framlagd: 2011-06-08

Författare: Linn Bjärvall
Martin Ståhl

Handledare: Anders Svensson

Examinatorer: Agneta Olerup
Markus Lathinen

Abstrakt

Titel: Krav för säkra molntjänster

Författare: Linn Bjärvall
Martin Ståhl

Utgivare: Institutionen för informatik

Handledare: Anders Svensson

Examinatorer: Agneta Olerup
Markus Lathinen

Publiceringsår: VT 2011

Uppsatstyp: Kandidatuppsats 15Hp

Språk: Svenska

Nyckelord Cloud Computing, Molntjänster, Informationssäkerhet, Risker, Krav

Abstrakt:

För att uppnå större kostnadskontroll på sina IT tjänster och samtidigt ha möjlighet att vara konkurrenskraftigt inom sin bransch väljer fler och fler företag idag att använda sig av molntjänster. Molntjänster kan ses som en form av tjänster som levereras över internet. Dock finns det många frågetecken runt säkerheten, vilket gör att många företag har svårt att förlita sig helt på molntjänster. För att som kund våga ta steget och använda sig av en molntjänst är det därför av stor vikt att veta vilka krav som behöver uppfyllas för att molntjänsten skall anses som säker utifrån ett informationssäkerhetsperspektiv. Syftet med vår studie är att identifiera de säkerhetskrav som kunder har på informationssäkerhet på privata och publika molntjänster samt utforma en kravlista för detsamma. I uppsatsens litteraturgenomgång lyfter vi exempelvis fram riskerna med molntjänster, de olika typerna av molntjänster samt olika avtal som finns mellan kunder och leverantörer. Litteraturstudier samt intervjuer med såväl kunder som leverantörer av molntjänster har gett oss ett underlag för att kunna ta fram en övergripande kravlista. Studiens resultat visade att det finns en mängd krav på säkerhet som behöver uppfyllas för att kunden skall känna sig trygg och att de kraven varierar beroende på molntjänstens arkitektur. Kravlistan ger även läsaren en överblick över de skillnader i krav som finns mellan de respektive typerna av molntjänster. Eftersom den största osäkerheten för kunden vad gäller molntjänster handlar om att kunden inte har någon fysisk kontroll av sina servrar, är de krav som kunder värderar högst att känna trygghet och tillit till leverantören. För att göra det krävs att de avtal som skrivs med leverantören är välspecificerade.

Förord

Vi vill framföra ett stort tack till alla företag och personer som tagit sig tid och bidragit med mycket kunskap för att genomföra studien. Ett särskilt tack vill vi rikta till Mia Madsen, Emely Jonasson och Fredrik Stolpe, som hjälpt oss att ta fram kontaktuppgifter till intressanta och relevanta informanter.

Vi vill även tacka vår handledare Anders Svensson, som varit ett stort stöd för oss under arbetets gång och bidragit med konstruktiv kritik samt värdefulla kommentarer.

Linn & Martin

Innehållsförteckning

Figurförteckning

Tabellförteckning

1 Inledning

1.1 Bakgrund

Det senaste året har mycket i IT världen handlat om det så kallade molnet och molntjänster. Cloud Computing representerar ett mer specifikt sätt att använda datorn där dynamiska skalbara resurser tillhandahålls som tjänster genom Internetteknologin. (Somashekar, 2010)

Beskrivning av Cloud:*”Cloud is a metahaphor for a network of computing resourses accessible publically or privately over the Internet or Intranet*”. Det är med andra ord en abstraktion av den komplicerade infrastrukturen som döljs för slutanvändaren. (Somashekar, 2010 s.4)

Molntjänster är applikationer som levereras som tjänster över Internet och det som även utmärker dem är att hårdvaran är skiljd från köparen och att inga direkta investeringar krävs från denne. Istället för att ta hand om driften av egna system och servrar körs allt via Internet. Den dynamiska kapaciteten hos molntjänster gör att den kan höjas respektive sänkas efter behov. Molntjänster förmodas innebära kostnadseffektivitet och flexibilitet, men ställer också höga krav på säkerhetsmedvetande. (Forsén, 2010)

Företagen börjar alltmer se över möjligheten att använda molntjänster istället för att behöva investera i hård- respektive mjukvara samt programlicenser. Företagen ser många fördelar med molntjänster i form av ökad effektivitet samt möjlighet att spara pengar på sin IT - verksamhet. Dock återstår många frågetecken runt de säkerhetsfrågor som blir aktuella vid en övergång till en molntjänst. Även om molnet skapar nya möjligheter krävs det ett nytt säkerhetstänk när företagen inte längre har fysisk kontroll över sina servrar. Behov av åtkomst och sekretess styr ofta vilken typ av molntjänst man väljer. (Forsén, 2010)

Företags allmänt ökade intresse för Cloud Computing grundas på att de vill minska sina IT-kostnader samtidigt som man vill öka sin kapacitet. (ENISA, 2009) Med molntjänster avses processorkraft, lagringsutrymme och applikationer som finns på servrar i en eller flera datorhallar som kunden får åtkomst till via internet. Att använda molntjänster kan ses som en form av outsourcing. Det som skiljer molntjänster från outsourcing är att användarna har mindre kontroll över sin information i molnet. Vid traditionell outsourcing vet köparen var tjänsten utförs. Oavsett om tjänsten driftas hos köparen eller leverantören finns en fysisk plats identifierad. När det gäller molntjänster levereras de normalt från stora datacenter som teoretiskt sett kan vara placerade var som helst i världen. (Forsén, 2010)

På 60- talet förespådde datorpionjären John McCarthy att beräkningar av olika slag i framtiden skulle kunna organiseras som en allmän tillgång. Cloud Computing är förverkligandet av detta som just underlättar leveransen av olika typer av beräkningar på begäran, vilket kan jämföras med leverans av elektricitet. Cloud Computing är i sig inget nytt koncept. Grid Computing, On demand Computing och Utility Computing är föregångarna till konceptet Cloud Computing. De löser alla tre problemen med att organisera datorkraft som en gemensam lättillgänglig resurs. Det som skiljer Cloud Computing från Grid Computing är främst att användarna i Grid Computing först måste dela med sig av egna resurser innan de får tillgång till en större pool med delade resurser. I Cloud Computing betalar användarna endast för datortjänsterna. (Wei & Blake, 2010)

Cloud computing är utvecklingen av de senaste 15 årens trend mot en industrialisering av IT. Cloud computing har blivit möjligt genom den pågående standardiseringen av underliggande tekniker som virtualisering, SOA samt Web 2.0. (Somashekar, 2010)

År 2006 började företaget Amazon erbjuda molntjänster som benämndes som Elastic Computing Cloud. Ett par år senare, år 2008, startade även företag som Google, Google Apps samt Microsoft Azure Plattform med molnplattformar. (Wei & Blake, 2010)

1.2 Problemdiskussion

Den generella uppfattningen är, som nämnts ovan, att molntjänsterna bidrar med en hög effektivitet och flexibilitet för företaget, men att det trots det fortfarande är få företag som förlitar sig helt på molntjänster. De allra flesta är dock övertygade om att man inom fyra år kommer att ha upphandlat ett flertal molntjänster. Med andra ord pekar allt på att effektiviteten som krävs för ett konkurrenskraftigt företag med kostnadskontroll finns i molnet bara vi kan känna oss trygga med säkerheten och ha kontroll på det vi lägger ut. (Glaad, 2011)

Datorvärlden utvecklas mot Cloud Computing, där program och tjänster sköts över internet i stället för lokalt på användarens dator. När individen har all information på sin egen dator innebär det också full kontroll jämfört med Cloud Computing, där service och dataförvaring sköts av säljaren och kunden är omedveten om var informationen finns lagrad. Logiskt sett har kunden med andra ord ingen kontroll över hur data behandlas även om säljaren lämnar vissa garantier i ett säkerhetsavtal, Service Level Agreement (SLA). (Jensen et al., 2009)

Enligt en enkätundersökning som amerikanska CIO genomfört bland 173 företagsledare visade det sig att så mycket som 45 procent tyckte att det största orosmomentet med Cloud Computing var just säkerheten. (Rosengren, 2008)

Som konstaterats ovan innebär molntjänster stora frågetecken kring säkerheten. För att kunna införa molntjänster med ett bra resultat krävs ett högt säkerhetsmedvetande i organisationen. Många företag vill ta steget, men vågar inte på grund av oro för vad det skulle kunna innebära för den del av företagets information som det skulle bli aktuellt för. Vi har vid litteraturgenomgången funnit att det finns dokumenterade risker och svårigheter inom

molntjänsternas föregångare outsourcing, som förmodligen har flera likheter med riskerna med molntjänster. De gemensamma och specifika säkerhetsriskerna avser den *förlorade kontrollen över data* samt att *konfidentialiteten, integriteten* och *tillgängligheten* hotas. (Forsén, 2010)

Utifrån det finner vi det intressant att studera vilka krav som behöver uppfyllas för att en molntjänst skall anses som säker för kunden. Det leder oss vidare till vår forskningsfråga.

- *Vilka säkerhetskrav behöver kunder ställa på molntjänster för att känna sig säkra?*

  I vår uppsats avser vi med säker molntjänst att den uppfyller de tre främsta säkerhetsmålen inom informationssäkerhet såsom konfidentialitet, integritet och tillgänglighet.

1.3 Syfte

Huvudsyftet med studien och efterföljande analys är att identifiera de krav på informationssäkerhet som behöver uppfyllas för molntjänster skall vara säkra för kunden. Ytterligare ett syfte är att utforma och tillhandahålla en enkel och övergripande kravlista för detsamma. Tanken med kravlistan är att den skall kunna användas som en form av mall för kunder vid införande av molntjänster. För att kunna genomföra det har vi fördjupat oss i lämplig litteratur och tidigare forskning inom ämnet. Uppsatsen och kravlistan riktar sig framförallt till mindre företag som saknar teknisk kompetens inom verksamheten, men som dock vill försäkra sig om en säker användning av molntjänster.

1.4 Avgränsningar

Studien avgränsas till privata och publika molntjänster men kommer inte att omfatta skillander i krav på de olika leveransmodellerna: Software as a Service (SaaS), Platform as a Service (PaaS) samt Infrastructure as a Service(IaaS). Säkerhetskraven belyses utifrån konfidentialitet, integritet och tillgänglighet. Studien omfattar även de lagar och avtal som gäller för molntjänster.

2 Litteraturgenomgång

För att kunna identifiera de eventuella riskerna med molntjänster behöver kunder göra någon form av riskanalys. Tidigare studier med molntjänster visar att det finns många risker med outsourcing som har likheter med de som förekommer vid molntjänster, därav att vår litteraturgenomgång innehåller även dessa. Konfidentialitet, integritet samt tillgänglighet är tre hörnstenar för generell informationssäkerhet som gäller även för molntjänster. För att få en uppfattning om molntjänsters uppbyggnad och därmed vilka risker som generellt förekommer för en molntjänst beskrivs de tre olika leveransmodellerna av molntjänster, dock kommer vi inte gå närmare in på dem i studien. Molntjänster kan också delas in i tre typer: privata, publika samt hybrida molntjänsten, som är avgörande för hur säkerheten ser ut för molntjänster. Infrastrukturens säkerhetsnivåer på molntjänster ses ofta som en helhet, dock har vi i vår studie valt att dela upp dem i tre nivåer för att kraven på molntjänster lättare skall kunna identifieras. Olika säkerhetsstandarder för kunder kan underlätta när de väljer molntjänst även om det inte är avgörande. Avtal mellan kunden och leverantören samt lagar gäller alltid när parterna inte är överrens och hur ser de ut för att kunden skall känna sig säker?

2.1 Riskanalys

Med risk menas att en slumpmässig händelse negativt påverkar möjligheten att nå ett uppställt mål. En risk är summan av sannolikheterna för att en skadehändelse ska bli verklighet och de konsekvenser händelsen kan få. (Hamilton, 1996) En teknisk risk i ett IT-system är en funktion av sannolikheten för att några hot kommer att attackera, eller utnyttja en viss sårbarhet i ett IT-system relaterat till konsekvenserna för attacken. (Covert & Nielsen, 2005) Det finns en skillnad mellan risk och hot. Vi har ständigt ett antal potentiella risker i vår omgivning, men det är endast ett fåtal av dem som utgör ett hot. Ett exempel på det är om man går på trottoaren. Då utgör bilarna på vägen en risk, men det blir först ett hot när vi korsar vägen. Av alla risker som finns är det därför hoten som vi bör gardera oss mot. (Hamilton, 1996)

Människor reagerar på risker utifrån hur de själv upplever dem och inte utifrån riskers siffermässiga värde. Risker som hänger samman med ny okänd teknik överdrivs ofta samtidigt som äldre välkända risker ofta underskattas. Exempelvis är människor mer benägna att acceptera risken för en bilolycka än ett haveri i ett kärnkraftverk, trots att antalet dödsoffer i trafiken överstiger de i kärnkraftsolyckor. (Hamilton, 1996)

Att utföra en riskanalys innebär att man kartlägger det aktuella företagets riskmiljö. Målsättningen vid en sådan är att få fram trovärdig information om hot och risker och skapa förutsättningar för att skydd och säkerhet blir fullständiga. (Covert & Nielsen, 2005)

Det finns två sätt för att beräkna risken för ett IT system: kvalitativ riskanalys samt kvantitativ riskanalys. Varje metod har sina styrkor och svagheter och används för olika ändamål. (Covert & Nielsen, 2005) Det är svårt att göra någon lättöverskådlig modell för hur alla riskanalyser ser ut. Riskanalyser brukar delas in efter grad av mätbarhet. För att identifiera specifika risker används kvalitativa metoder. Syftet med dem är främst att ge beskrivningar av olika händelser vid olika förutsättningar. När en kvalitativ riskanalys används värderas riskerna efter erfarenheter och anges då ofta som en siffra. (Magnusson, 1999) En kvantitativ riskanalys används när man är i behov av en mätbar uppskattning av frekvensen för olika hot. (Hamilton, 1996)

Utifrån de kvalitativa samt kvantitativa riskanalyserna har det utvecklats ytterligare metoder, som kan kombineras med de grundläggande metoderna. Exempel på ett antal grundläggande metoder för att utföra en riskanalys är exempelvis *checklistor*, *delphi - teknik* samt *förväntad skadekostnadsanalys*. Checklistor innebär att man ställer frågor från ett frågeformulär om risker, sårbarhet och skadeexponeringar och utgör en kontroll av en fastställd säkerhetsnivå. Delphi-teknik är en form av ”brainstorming” som utförs av någon kompetent grupp inom verksamheten. Gruppen väljer ut de risker och förhållanden som ska granskas. Metoden som benämns som förväntad skadekostnadsanalys är en form av kvantitativ riskanalysmetod. (Hamilton, 1996)

2.2 Risker vid outsourcing av IT

Det är av stor betydelse att informera sin outsourcingleverantör om vikten av att behandla konfidentiell information på ett visst sätt, precis som om det skulle informeras om det internt. (Augustson & Sten, 1999)

Företag som överväger outsourcing bör vara försiktiga och inte underskatta de säkerhetsrisker som är förknippade med överföring av skyddade uppgifter eller personuppgifter och bör klart förstå alla följder av sådana överföringar. Betydande säkerhetsrisker kan inkludera att obehöriga får tillgång till data eller att data förloras på grund av att fysiska anläggningar inte är tillräckligt säkra. Information lämnas ut olämpligt på grund av otillräcklig kontroll av personal som i extrema fall kan leda till utpressning och bedrägeri. (Lesk et al., 2005)

Ett outsourcingavtal varar normalt 5-10 år. Under en sådan period kommer organisationen ställas inför stora verksamhetsförändringar i takt med att kunders behov förändras, teknisk utveckling, politiska förändringar eller förändrad lagstiftning. Det finns inget outsourcingkontrakt som kan förutse de här förändringarna för alla sorters händelser. Organisationer är starkt beroende av sina IT-tjänster. Det medför olika risker, exempelvis om leverantören blir ekonomiskt instabil eller i värsta fall går i konkurs. (Sparrow, 2003) Leverantören kan även bli uppköpt av ett annat företag med ett annorlunda och ovälkommet förhållningssätt. Servicenivån kan falla till oacceptabelt låg nivå som en följd av interna problem inom tjänsteleverantören vilket även drabbar kunderna. (Sparrow, 2003) När en organisation har lagt ut ett antal av sina IT-funktioner hanteras de inte längre som tidigare av anställda specialister på företaget. Därför måste företaget försäkra sig om att

tjänsteleverantören utnyttjar tekniken effektivt. Trots att företaget saknar specialister som de tidigare hade, måste de ändå utveckla sin IT-strategi. Förlusten av teknisk expertis genom outsourcing kan bidra till att organisationen blir sårbar vad beträffar dålig service och höga priser. (Sparrow, 2003)

I en outsourcingrelationen har leverantören tillgång till information och andra tillgångar som organisationen normalt skulle betrakta som konfidentiella. Det finns inga möjligheter för kunder att behålla hemligheter för tjänstleverantören i outsourcingsammanhang. Det medför bland annat en ökad risk för missbruk av konfidentiell information, exempelvis om intern e-post och redovisningsdata får behandlas av tjänstleverantören. Även strategiska verktyg som ger en konkurrenskraftig fördel kan användas och underhållas av leverantören. Det bidrar även till ökade svårigheter att skydda andras sekretess, exempelvis tillgång till anställdas filer samt kunddata. (Sparrow, 2003)

Osäkerheten handlar främst om förlorad kontroll över säkerhet om leverantören överför behandlingen av informationen till en ny plats. Hur ska det övervakas? Vem kommer att få tillgång till informationen? Tjänstleverantören kanske använder platsen för flera kunder och hur kan det då garanteras att en konkurrent inte får tillgång till obehörig information? (Sparrow, 2003)

När en extern leverantör tar över ansvaret för produktionen av varan eller tjänsten som outsourcingen omfattar har förtag inte samma kontroll längre. Det är viktigt att bedöma risken som den förlorade kontrollen medför och som beror på vilken kontroll man hade över IT verksamheten i utgångsläget. Hur allvarlig kontrollförlusten blir beror också på tjänstens karaktär och utformningen av outsourcingen. Om outsourcingen endast omfattar stödfunktioner är inte kontrollfunktionen lika stor. Om däremot outsourcingen omfattar affärskritiska system kan förlusten av system vara allvarligare. En kortsiktig leverantörsstörning kan bottna i tekniska orsaker som att leverantörens system går ner. Långsiktiga leveransstörningar kan uppstå om leverantören hamnar i finansiella problem. Risken för långsiktiga störningar hanterar man genom att välja en finansiellt stabil partner med god utvecklingspotential. En kortsiktig leveransstörning hanteras genom att man skriver ett välgenomtänkt Service Level Agreement (SLA) som reglerar tillgänglighet, svarstider och konsekvenser vid uppkomna störningar i leveranserna. (Augustson & Sten, 1999)

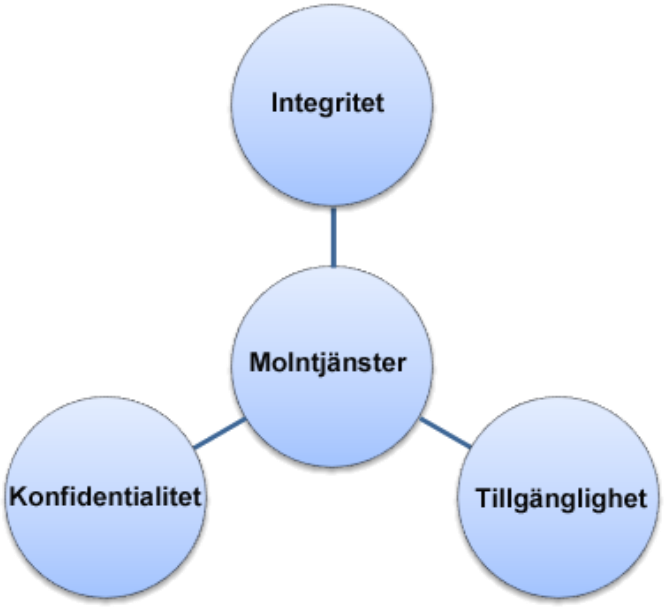
De risker som främst förekommer vad gäller outsourcing är således:

- Obehöriga får tillgång till data
- Data förloras på grund av att fysiska anläggningar inte är tillräckligt säkra
- Otillräcklig kontroll av personal
- Leverantör som går i konkurs
- Missbruk av konfidentiell information

Ovanstående risker har många likheter med de risker som finns med molntjänster.

2.3 Generell informationssäkerhet

Enligt (figur 2.1) finns det tre grundläggande principer för informationssäkerhet: Confidentiality, Integrity och Availability (CIA) som vi framöver kommer att använda den svenska översättningen av, det vill säga; konfidentialitet, integritet och tillgänglighet. Det är de tre hörnstenar som definierar en organisations säkerhetsnivå. Alla informationssäkerhetskontroller, skydd, hot, sårbarheter samt säkerhetsprocesser kan mätas i förhållande till dessa teorier. (Krutz & Russel, 2010) Som framgår av (figur 2.1) är det de tre säkerhetsaspekterna: integritet, konfidentialitet samt tillgänglighet som vi kommer fokusera på i studien.



Figur 2.1: Informationssäkerhet och molntjänster (Bjärvall & Ståhl, 2011)

2.3.1 *Konfidentialitet*

Begreppet konfidentialitet innebär förhindrandet av avsiktligt eller icke avsiktligt obehörigt röjande av informationsinnehållet. (Krutz & Russel, 2010)

Säkerhetskravet för konfidentialitet garanterar att användardata som finns i molntjänster inte kan nås av en obehörig part utan endast kan nås genom en korrekt krypteringsteknik. (Almulla & Yeun, 2010) I molntjänstsammanhang spelar konfidentialiteten en viktig roll, särskilt för att behålla kontrollen över organisationers data som ligger över flera distribuerade databaser. Det är nödvändigt när man använder en publik molntjänst på grund av dess form och tillgänglighet. För att kunna garantera konfidentialiteten av användarnas profiler samt skydda deras data från tillträde krävs att man har olika informationssäkerhetsprotokoll på olika lager av molnprogram. (Ramgovind et al., 2010)

Information kan försvinna på flera olika sätt, exempelvis genom ett avsiktligt borttagande av privat organisationsinformation eller genom missbruk av nätverksrättigheter. De tre element som används för att försäkra konfidentialiteten i telekommunikation är

nätverkssäkerhetsprotokoll, nätverksautentieringstjänster och datakrypteringstjänster. (Krutz & Russel, 2010)

2.3.2 *Integritet*

Integritet för informationssäkerhet bör inte förväxlas med personlig integritet utan avser att garantin för att det meddelande som mottagits är detsamma som det som skickats och att meddelandet varken oavsiktligt eller avsiktligt förändrats. Om datas integritet uppfylls korrekt garanteras att meddelandet som mottagits är samma som det som skickats och att meddelandet varken oavsiktligt eller avsiktligt har förändrats. (Krutz & Russel, 2010) Integritetsförlust kan uppstå genom en avsiktlig attack som görs för att förändra informationen eller som sker oavsiktligt av en tekniker. Integritetskonceptet inkluderar också konceptet oavvislighet. De element som används för att försäkra sig om integriteten innefattar brandväggstjänster, kommunikationssäkerhetshantering och intrångsskyddstjänster. (Krutz & Russel, 2010) Användare av molntjänster bör således inte bara oroa sig för sekretessen av data som lagras som molntjänst utan även om datas integritet. I huvudsak finns det två sätt som ger integritet dels genom att använda Message Authentication Code (MAC) dels genom digitala signaturer. MAC är en kort bit information som används för att autentisera ett meddelande och en digital signatur är ett matematiskt system som man kan användas för att visa att ett digitalt meddelande eller dokument är äkta (Almulla & Yeun, 2010).

2.3.3 *Tillgänglighet*

För att upprätthålla tillgängligheten av data används olika tekniker för att undvika eller motverka hot som påverkar tillgängligheten av tjänsten eller data. Exempel på hot som riktar sig mot tillgänglighet kan vara Denial Of Service (DoS) attacker. En DoS attack är således ett försök att göra en datorresurs otillgänglig för tilltänkta användare (Almulla & Yeun, 2010). Tillgänglighet är ett av de mest kritiska informationssäkerhetskraven för molntjänster när den efterfrågas av auktoriserade användare, eftersom det ofta är en avgörande beslutsfaktor när man väljer mellan dels leveransmodell och dels typer av molntjänster. Service Level Agreement (SLA) är det viktigaste dokumentet som belyser oron vad gäller tillgängligheten på molntjänster samt resurserna som finns mellan kund och leverantör. (Ramgovind et al., 2010)

Begreppet tillgänglighet refererar till de faktorer som skapar tillförlitlighet och stabilitet i nätverk och system. I begreppet ingår en försäkran om att det finns en förbindelse som är tillgänglig när så önskas och som tillåter behöriga användare att komma åt systemen och nätverket. Några element som används för att försäkra sig om tillgängligheten är exempelvis feltoleransen vad gäller tillgängligheten av data som backup eller dubbletter av disksystem, acceptabla inloggningar och prestandan på processer som utförs samt tillförlitlighet och synkade säkerhetsprocesser och nätverkssäkerhetsmekanismer. (Krutz & Russel, 2010)

2.4 Leveransmodeller för molntjänster

Arkitekturen för molntjänster kan kategoriseras in i tre typer av leveransmodeller; mjukvara, plattform och infrastruktur. Leveransmodellerna är oberoende av vilken typ av molntjänst som används. (Ramgovind et al., 2010)

2.4.1 *Software as a Service (SaaS)*

Traditionell försäljning av mjukvara innebär att kunden installerar mjukvaran på sin egen hårdvara mot en licenskostnad. Kunden ansvarar själv för installationer av uppdateringar. (Mather et al., 2009) I molnet behöver användaren inte köpa programvaran utan hyr i den i stället. Betalningen baseras på hur mycket programvaran används och kan byggas ut efter behov (Almulla & Yeun, 2010) (Ramgovind et al., 2010) (Mather et al., 2009) och är åtkomlig för användaren direkt genom Internet via webbläsaren (Ramgovind et al., 2010). Kunden behöver heller inte någon speciell hårdvara även om det kan behövs modifieringar i företagets brandväggar för att applikationen ska fungera smidigt (Mather et al., 2009). Den fysiska bakomliggande infrastrukturen delas mellan flera användare men logiken är unik för varje användare (Almulla & Yeun, 2010). Eftersom programvaran nås via webbläsare över Internet är webbläsarens säkerhet av största vikt.

> *"Software offered by a third party provider, available on demand, usually via the Internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, etc)." (ENISA, 2009 s.15)*

Fördelarna med SaaS är att företag kan outsourca lagring samt hantering av applikationer till en tredje part, vilket minskar kostnaderna för licenser, servrar och personal som hade fått hantera det internt. Underhållningen utav SaaS applikationer sköts av leverantören. (Mather et al., 2009)

Den viktigaste skillnaden mellan traditionell mjukvara och SaaS är antalet användare som applikationen stödjer. Traditionell mjukvara är begränsad eftersom kunder köper en mjukvara som de installerar på en server. Servern kör enbart den specifika applikationen och då endast för den enskilda kundgruppen. SaaS-modellen däremot har stöd för flera användare. Det betyder att den bakomliggande infrastrukturen delas mellan flera användare medan logiken är unik för varje användare. Infrastrukturen i SaaS maximerar fördelningen av resurserna för varje användare, dock säkrar den ändå olika data som tillhör en viss kund. Ett exempel är när en användare på ett företag hanterar kundinformation via ett SaaS Customer Relationship Management (CRM). Då kan applikationsinstansen som användaren är uppkopplad till anpassa sig till användare från flera hundra andra företag, där alla är totalt okända för de andra användarna. (Mather et al., 2009) (Julisch & Hall, 2010)

2.4.2 *Platform as a Service (PaaS)*

Leveransmodellen Platform as a Service (PaaS) erbjuder en integrerad miljö för att utforma, utveckla, testa samt stödja en kundapplikation som utvecklats på det språk som plattformen stödjer (Mather et al., 2009). Plattformar består av både utvecklingsverktyg och en

utvecklingsmiljö. Kunderna till molntjänsterna använder utvecklingsverktygen för att programmera sina egna applikationer mot det gränssnitt som kunden har mot molntjänsten, Application Programming Interface (API) i utvecklingsmiljön. (Julisch & Hall, 2010)

> *"Allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine." (ENISA, 2009 s.15)*

PaaS är en variant av SaaS, som bygger på att utvecklingsmiljön är tillgänglig som en service. Utvecklarna använder sig av byggklossar, exempelvis fördefinierade kodblock från leverantören för att skapa sina egna applikationer. Här tillhandahålls en molnhostad virtuell utvecklingsplattform som kan nås via en webbläsare. (Mather et al., 2009) Plattformen kommer att befinnas sig i molnet och kommer att nås med hjälp av webbläsaren. (Almulla & Yeun, 2010)

Fördelen är att mjukvaruutvecklare kan bygga webbapplikationer utan att behöva installera utvecklingsverktygen för mjukvaror på sina egna datorer. Traditionella utvecklingsverktyg är menade för en enskild användare medan molnbaserade måste stödja flera användare. (Mather et al., 2009) PaaS är således en utvecklingsplattform där utvecklingsverktyget finns i molnet och är tillgängligt via webbläsaren. Platform as a Service fungerar likt Infrastructure as a Service, dock med skillnaden att den har en extra nivå av funktionalitet. (Ramgovind et al., 2010)

Plattformen kommer att befinnas sig i molnet och kommer att nås med hjälp av webbläsaren. (Almulla & Yeun, 2010)

Leverantören erbjuder en utvecklingsmiljö för applikationsutvecklare som utvecklar applikationer och erbjuder dem tjänster via leverantörsplattformen. Leverantören utvecklar vanligtvis verktyg och standarder för utveckling och kanaler för disposition och betalning. Leverantören får i sin tur betalning för levereringen av plattformen, servicen för försäljning av tjänsten samt disposition. Med tanke på den låga inträdeskostnaden möjliggör det en snabb spridning av mjukvaran och även en snabb väg för att hitta de etablerade kanalerna för att värva kunder. (Mather et al., 2009)

Kunden förvaltar och styr programvaran medan leverantören förvaltar och styr operativsystem och infrastruktur. Kunden ansvarar således ord för alla kontroller gällande programvaran medan leverantören är ansvarig för generella IT-kontroller. (Julisch & Hall, 2010)

2.4.3 *Infrastructure as a Service (IaaS)*

När det gäller den tredje varianten av leveransmodell för molntjänster Infrastructure as a service (IaaS) levererar leverantören hela infrastrukturen till en kund som denne kan köra sina program på. Infrastrukturen hanterar toppar och dalar av krav och lägger till ny kapacitet när kraven ökar. Betalningsmodellen grundar sig på datorkraften, diskutrymme med mera, som kunden använder. Det möjliggör för kunden att använda sig av exakt den mängd av infrastruktur som krävs för tillfälligt. (Mather et al., 2009) IaaS är en låg nivå av datorresurser

såsom exempelvis virtuella maskiner eller lagring som tillhandahålls över internet. (Julisch & Hall, 2010)

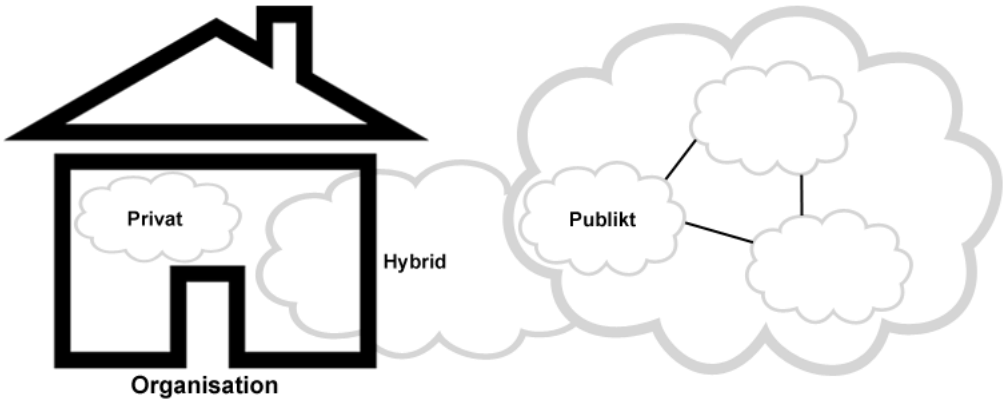
> *"Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud." (ENISA, 2009 s.15)*

Molntjänsten levereras i form av teknik, datacenter och IT-tjänster till kunden likt traditionell outsourcing fast till betydligt mindre arbete och lägre kostnader. Det huvudsakliga syftet är att skräddarsy en lösning till kunden baserat på dennes krav samt att leverera en hög skalbarhet som är tillgänglig via webbläsaren för kunden. (Almulla & Yeun, 2010)
Molntjänstleverantörers dedikerade resurser delas mellan de kunder som man har skrivit kontrakt med och de betalar i sin tur per användning. Fördelen är att behovet av enorma nyinvesteringar i datorhårdvara såsom servrar, nätverksutrustning och processorkraft minimeras. Fördelen med molntjänsten är att det också tillåts olika grader av finansiell och funktionell flexibilitet som inte finns inom företags egna datacenter eftersom datorresurser kan läggas till eller frigöras mycket snabbare och mer kostnadseffektivt Beslutsfattare måste dock vara medvetna om att driftskostnaden växlar från en periodisk fast kostnad till en rörlig driftskostnad. (Ramgovind et al., 2010)

I IaaS är det kunden som hanterar och kontrollerar mjukvaran som körs på leverantörens infrastruktur. I det ansvaret inkluderas samtliga av mjukvarans säkerhetskontroller inklusive uppdateringar, antivirusprogram samt accesskontroller av olika slag. (Julisch & Hall, 2010)

2.5 Typer av molntjänster

Kunderna till molntjänster måste besluta sig för vilken typ av molntjänst de vill ha. Det finns tre typer av molntjänster som erbjuds: publika moln, privata moln samt hybrida moln (Figur 2.3). När beslutsfattarna bestämmer sig för vilken typ av tjänst de vill distribuera bedöms skillnaderna mellan de olika typerna och valet av modell grundar sig på vad som är viktigt för just den organisationen. En leveransmodell kan presenteras för användarna som en eller flera typer av molntjänster. (Ramgovind et al., 2010)



Figur 2.2: Privata, hybrida och publika molntjänster (Bjärvall & Ståhl, 2011)

2.5.1 *Publika molntjänster*

Som framgår av figur 2.1 befinner sig informationen utanför den egna organisationen i publika molntjänster. Ett publikt moln ger användarna tillgång till molntjänster via webbläsaren och användaren betalar per enhet som används, ungefär som betalning för elektricitet. Fördelen är flexibiliteten för att tillgodose toppar i efterfrågan. (Ramgovind et al., 2010) I publika moln är säkerhetshanteringen överlämnad till en tredje part. Det ger kunden av publika molntjänster mindre kontroll och översikt av den fysiska säkerheten i jämförelse med privata moln. (Mather et al., 2009) (Ramgovind et al., 2010) För organisationer vars existens är beroende av att skydda kunddata, affärshemligheter, sekretessbelagda uppgifter eller patentskyddad information erbjuder publika moln inte tillräckligt skydd. (Hofmann & Woods, 2010)

2.5.2 *Privata molntjänster*

Privata molntjänster skiljer sig från publika molntjänster på det viset att nätverket, processerna samt lagringen av all data tillhör den enskilda organisationen och delas inte med andra organisationer (Figur 2.1), vilket kan liknas vid funktionerna i ett intranät. (Mather et al., 2009). Därför ansvarar kunden själv för molntjänsten, vilket underlättar anpassningen av säkerhet och lagkrav. Det ger även företaget mer kontroll över utveckling och användning (Mather et al., 2009) (Ramgovind et al., 2010). I privata moln tillhandahålls skalbara resurser och virtuella applikationer av molntjänstleverantörer. De aktuella resurserna och applikationerna sammanförs och är på så vis tillgängliga för användarna av molntjänsterna. Att utnyttja privata moln är således betydligt säkrare än att utnyttja de publika molntjänsterna, eftersom kunden har en bättre översikt av både den fysiska och personliga säkerheten. (Ramgovind et al., 2010) (Mather et al., 2009)

2.5.3 *Hybrida molntjänster*

Som framgår i figur 2.1 består en hybrid molntjänst av en kombination av en intern och extern molntjänst. Molntjänstleverantören tillhandahåller virtuella IT - lösningar genom att blanda både publika och privata molntjänster. (Ramgovind et al., 2010) (Mather et al., 2009). Med en hybrid molntjänst kan organisationen köra en del applikationer i det publika molnet och samtidigt köra applikationer med mer känslig data i ett privat moln. (Mather et al., 2009)

2.6 Infrastrukturens säkerhetsnivåer för molntjänster

Kapitel 2.6 bygger i huvudsak på Mather et al. Vi anser att det är relevant, eftersom teorin är av stor betydelse för den kravlista som studien resulterar i. Vid litteraturgenomgången har vi funnit att ett flertal artiklar inom ämnesområdet molntjänster och säkerhet refererar till författaren Mather et al. Vi använder den också för att ha möjlighet att utforma bättre frågor vid våra intervjuer samt för att förtydliga strukturen på de olika säkerhetskrav som vi belyser i vår studie.

Molntjänster kan baseras på en affärsmodell där resurser delas på nätverksnivå, värdnivå samt applikationsnivå. På varje respektive nivå är molntjänsterna skyldiga att uppfylla säkerhetskrav för att kunna bevara den grundläggande säkerheten. (Mather et al., 2009)

2.6.1 *Network Level*

Det är av stor vikt att skilja på publika och privata moln när man betraktar säkerheten i infrastrukturen. Det finns inga nya attacker, sårbarheter eller förändringar vad avser privata molntjänster och risker som är specifika för nätverkets struktur som de säkerhetsansvariga behöver ta med i beräkningarna. Oavsett om den nuvarande IT- arkitekturen förändras vid implementeringen av den privata molntjänsten kommer inte nätverksstukturen att förändras avsevärt. Om en organisation väljer att hyra en publik molntjänst kommer dock förändrade säkerhetskrav att kräva förändringar i nätverksstrukturen. Det är då viktigt att se över den befintliga nätverksstrukturen och hur den interagerar med molntjänstleverantörens nätverksstruktur. (Mather et al., 2009)

Några av riskfaktorerna som man bör ta i beaktande är att man måste försäkra sig om konfidentialiteten samt integriteten hos data som rör sig mellan organisationen och molntjänstleverantören. Vissa resurser och data som tidigare begränsats till ett privat nätverk utsätts nu för Internet och för ett offentligt delat nätverk som tillhör en tredjepartsleverantör. (Mather et al., 2009)

Man bör också ta hänsyn till accesskontroll det vill säga autentisering, befogenhet och granskning för samtliga resurser som används av molntjänstleverantören såsom verifiering till dataresurserna, befogenhet till dem samt kontroll och granskning av dem. (Mather et al., 2009)

Konfidentialitetsrisken minskar genom att använda kryptering, och genom att använda implementeringar som är krypteringsbekräftade för data som är i rörelse. Specifika digitala signaturer gör det svårare för någon att ändra data, vilket skyddar integriteten. Vid användning av publika molntjänster är det svårare att mildra tillgänglighetsproblem. Även om privata molntjänster inte delas med andra ökar risken för tillgänglighetsproblem på nätverksnivån. (Mather et al., 2009)

Vad beträffar den *förebyggande kontrollen* av säkerhet på nätverksnivån så finns det en mindre form av kontroll över tillgången till nätverket. Det stöds av leverantören genom exempelvis en brandvägg samt kryptering av data som överförs. Det finns också en detektiv kontroll som innebär att leverantören hanterar sammanslagningar av säkerhetsincidenter och hantering av dem i loggar. I den ingår även nätverksbaserade intrångsskydd. (Mather et al., 2009)

Det är av stor vikt att förstå att nätverksrisker existerar oavsett vilken leveransmodell man använder; Saas. Paas eller Iaas. (Mather et al., 2009)

Leverantören kommer att övervaka, bevara och samla information om brandväggar, detektering av intrång och skyddssystem samt dataflöde inom nätverket. (Almulla & Yeun, 2010)

Genom att använda kryptering kan verksamheten reducera riskerna med konfidentialiteten. Om verksamheten använder sig av digitala signaturer blir det betydligt svårare att sabotera data, vilket försäkrar datas integritet. Tillgänglighetsproblem däremot är betydligt svårare att lindra så länge organisationen inte använder en privat molntjänst, som ingår internt i din nätverksstruktur. Förebyggande skydd och kontroller på nätverksnivån, som skyddar accesskontrollen av nätverket, är främst brandväggar samt kryptering av data som är i rörelse exempelvis SSL och IP sec.

2.6.2 *Host Level*

När man analyserar säkerheten och bedömningen av risker måste leveransmodellerna SaaS, PaaS och IaaS samt utvecklingsmodeller tas i beaktande. Även om det inte finns några nya hot för värddatorer som är specifika för molntjänster finns det ett antal virtualiseringshot såsom att virtuella datorer försvinner, systemkonfigurationsdrift eller insiderhot som beror på svaga accesskontroller till den virtualiserade plattformen som finns i molntjänstmiljön. Med elasticiteten i molntjänster följer nya utmaningar ur ett säkerhetshanteringsperspektiv samt en virtualiserad platform som tillåter flera operationssystem att köra på en värddator samtidigt. Verksamhetsmodeller förutsätter snabba beslut och flytande instanser av den virtuella maskinen. Att hantera säkerheten är därför svårare, eftersom förändringstakten är betydligt högre än i ett traditionellt datacenter. Att molntjänsterna fungerar som den samlade kraften för tusentals datornoder kombinerat med den homogenitet av operativsystem som drivs av servrar betyder att hoten kan utbreda sig snabbt och lätt. Leverantörer brukar inte dela information som är relaterade till serverns plattform, operativsystem eller de processer som skall garantera säkerheten i värddatorn, eftersom hackers kan utbreda sin information då de försöker ta sig in i molntjänster. (Mather et al., 2009)

Vad gäller SaaS och PaaS är säkerheten på servern oklar för kunderna och ansvaret för denna ligger på leverantören. Leverantören måste försäkra sig om att lämpliga förebyggande och pågående kontroller görs. Det är dock kundens ansvar att få en lämplig nivå på säkerhetsgarantin med hänsyn till hur leverantören hanterar säkerheten på värdnivån. (Mather et al., 2009)

Både leverantörsmodellen PaaS och SaaS döljer operativsystemet för slutanvändarna i servern genom lagret som heter *Host abstraction layer*. Skillnaden mellan PaaS och SaaS är tillgängligheten till det nämnda lagret som servar användarna till applikationerna. I SaaS är inte det abstrakta lagret synligt för användarna utan enbart för utvecklarna samt den leverantörstekniska personalen. Detta är skillnaden från PaaS användare som ges indirekt tillträde till det host abstraction layer i form av ett gränssnitt som i sin tur interagerar med host abstraction layer. (Mather et al., 2009) Det är av största vikt att samla information om systemets loggfiler för att veta var och när program har loggats. (Almulla & Yeun, 2010)

Säkerheten kring värddatorn i molntjänster av typen SaaS och PaaS åligger leverantören. Kunder behöver inte skydda dig mot serverbaserade hot, vilket är en förmån ur både säkerhetshanteringssynpunkt och kostnadssynpunkt. Dock finns det alltid en risk för kunder med information som lagras i molntjänster. Det är kundens ansvar att få en försäkran om hur leverantören tar hand om informationen. (Mather et al., 2009)

Till skillnad från molntjänster i form av PaaS och SaaS, ansvarar IaaS kunden för att säkra värddatorn som tillhandahålls av molnet. Eftersom många IaaS-tjänster som är tillgängliga idag, använder virtualisering på värdlagret, kan säkerheten i Iaas kategoriseras som dels säkerheten på den virtualiserade mjukvaran dels säkerheten på den virtualiserade servern. Det är av stor vikt att lagret av mjukvaran som sitter mellan hårdvaran och den virtuella servern är säkert. I en publik IaaS har inte kunderna tillgång till detta lager av mjukvaran. Det är enbart leverantörerna som förvaltar det. Den virtuella instansen av ett operativsystem som tillförs ovanpå virtualiseringsskiktet är synlig för kunder från Internet. De förebyggande säkerhetsskydden på värdnivån är brandväggar, accesskontroll samt en stark autentisering. De säkerhetsskydd som finns, mot det som har varit, är också loggar precis som på nätverksnivån. (Mather et al., 2009)

2.6.3 *Application Level*

Att utforma och implementera applikationer som är tänkta för molnplattformar kräver att nuvarande säkerhetsprogram använder de standarder och praxis som finns. Säkerheten på applikationsnivå för molntjänster avser hela spektret från enskilda användare till e-handelsapplikationer som används av många användare. Webbapplikationer som exempelvis ledningssystem, diskussionsforum eller liknande används av både stora och små organisationer. De befintliga hoten utnyttjar välkända sårbarheter i applikationen som exempelvis SQL-injektioner, skadliga filutförande och andra sårbarheter som uppstår vid programfel eller konstruktionsfel. Hackare har både verktyg och kunskap för att kunna utnyttja sårbarheter för diverse olagliga verksamheter såsom finansiella bedrägerier eller att göra intrång i vissa rättigheter. Det vanligaste är att man använder en kombination av säkerhetskontroller och accesskontroller på nätverks- respektive hostlevel för att skydda webbapplikationer som utvecklas i en hårt kontrollerad miljö. Den inkluderar företagets intranät och privata moln som skyddar tjänsten från utomstående hackare. Det finns stora risker för att Webbapplikationer som byggs och utvecklas på en publik plattform kommer att utsättas för en hög risknivå, genom exempelvis attacker samt att de utnyttjas potentiellt av hackare för att stödja bedräglig och olaglig verksamhet. Dessutom måste man vara observant på DDoS - attacker som kan störa molntjänster under en längre tid. Dessa attacker har oftast sitt ursprung från datasystem som har dåliga rykten och är anslutna till Internet. (Mather et al., 2009)

Som kund av en molntjänst är du ansvarig för de säkerhetsprocedurer som skyddar din dators internetuppkoppling. Det betyder att mjukvaran på datorn måste skyddas med antivirus, brandväggar och säkerhetspatchar. Alla webbläsare utsätts för mjukvarornas sårbarheter som gör dem sårbara för slutanvändarnas säkerhetsattacker. För att få en säkerhet från början till slut i molntjänster är det viktigt att kunden upprätthåller en hög säkerhet i webbläsaren. Det

innebär att webbläsaren måste vara uppdaterad för att minska sårbarheterna kring den. (Mather et al., 2009)

Beroende på leverensmodell samt det avtal som finns mellan kund och leverantör ligger räckvidden av det säkerhetsmässiga ansvaret på både kund- och molntjänstleverantör. Det är av stor betydelse att veta vad som är ens ansvar. De säkerhetskontroller som behöver göras på applikationsnivån är identitetshantering samt åtkomstkontrollsbedömning via webbläsaren som också bör vara uppdaterad. (Mather et al., 2009). Det är även viktigt att man kontrollerar behörighet samt kontrollerar och övervakar ändpunkterna i molntjänsten så att man sätter in antivirus samt intrångsskydd. (Mather et al., 2009)

2.7 Säkerhetsrisker med molntjänster

Molntjänstleverantören förvaltar samt kontrollerar servrar, nätverk, brandväggar och de mänskliga resurserna. Om den fysiska säkerheten är låg spelar det ingen roll om nätet till servarna skyddas med kryptering och brandvägg. (Archer et al., 2010)

Uppgifter av känslig karaktär som behandlas utanför företaget medför alltid en risknivå. Eftersom företagets data är outsourcad och därmed inte finns på företaget längre finns det inte längre någon form av fysisk eller personlig kontroll på denna. De främsta riskerna säkerhetsmässigt med molntjänster är således att informationen skickas över Internet, hur informationen lagras hos leverantörerna och hur leverantören hanterar den lagrade informationen. Informationen om de administratörer som sköter uppgifter av olika slag runt molntjänsten är viktiga. Det är också av stor betydelse att leverantörerna tillhandahåller specifik information om de som administrerar tjänsten samt vad de har tillgång till för information. Kunderna till molntjänster är alltid ytterst ansvariga för säkerheten och integriteten av sin data även om den finns hos en tjänsteleverantör. Vid användandet av molntjänster vet man inte var data finns lagrad, om ens vilket land den förvaras i. I molntjänster förekommer datan i en delad miljö tillsammans med data från andra kunder. Ett sätt att skydda sin data i den delade miljön är genom kryptering, som dock inte ger en total säkerhet. En leverantör av en molntjänst bör tillhandahålla bevis för att krypteringssystem utformats och testats av erfarna specialister innan tjänsten levereras. (Kandukuri et al., 2009)

Även om vi inte vet vara data finns bör leverantören tala om för oss vad som kommer hända med data och tjänsten om någon form av katastrof skulle inträffa. Att undersöka olämplig eller olaglig verksamhet kan vara omöjligt vad gäller molntjänster. Det kan vara mycket svårt att utreda, eftersom loggning och data för flera samlokaliseras och också kan spridas över en ständig föränderlig uppsättning av datacenter och värdar. (Kandukuri et al., 2009)

Det finns ett antal risker med Cloud Computing som man inte kan bortse ifrån. Srinivasamurthy och Liu (2010) fäster stor vikt vid det som de anser vara de sju främsta riskerna med molntjänster. Att exempelvis *missbruka eller använda molntjänsterna på ett medvetet dåligt sätt* är ett stort hot. Det kan exempelvis röra sig om att någon använder sig av olika nät för att sprida skräppost eller någon form av sabotageprogram. För angripare är det

möjligt att i de offentliga molntjänsterna hitta sätt att ladda upp skadlig kod till tusentals datorer och genom det använda möjligheter i molnets infrastruktur till att attackera andra datorer. Föreslagna åtgärder för att minska de riskerna är att validera processer samt ha strängare regler för nyregistrering. Man bör samtidigt ha en ordentlig övervakning av kreditkortsbedrägerier samt en omfattande kontroll av kundnätstrafiken. (Srinivasamurthy & Liu, 2010)

En annan riskfaktor är *osäkra användargränssnitt*. Det avser de gränssnitt som kunden använder för att interagera med molntjänsterna. Det är av största vikt att de är säkra vad gäller autentisering, åtkomstkontroll och kryptering, särskilt när det finns en tredje part som börjar bygga på dem. För att minimera de säkerhetshoten är det viktigt att analysera säkerhetsmodellen av molnleverantörens gränssnitt samt se till att både en stark autentisering och en stark behörighetskontroll genomförs i samband med krypterad överföring. (Srinivasamurthy & Liu, 2010)

De *skadliga insiderhoten* är hot som ökar i betydelse. Många leverantörer av molntjänster vill inte avslöja hur de anställer folk, hur de beviljar dem åtkomst till data samt hur de övervakar dem. För att minska den här typen av brott kan man genomföra en heltäckande leverantörsbedömning och specificera krav på anställda i det juridiska kontraktet. Dessutom kan man kräva insyn i den övergripande informationssäkerheten. (Srinivasamurthy & Liu, 2010)

Med den delade teknologin följer också ett antal sårbarheter. *För att säkerställa att inte kunder är inne på varandras territorium* krävs att det finns en stark uppdelning och övervakning av data. Cloud Security Alliance (CSA) har föreslagit ett antal åtgärder för att minimera den här typen av hot, såsom att exempelvis införa Best Practices för installation och konfiguration. Ytterligare åtgärder de vill främja är en stark autentisering och åtkomstkontroll för administrativ åtkomst och verksamhet. (Srinivasamurthy & Liu, 2010)

Dataförlust är en annan typ av hot. Det kan uppstå om man inte har tagit backup, exempelvis genom förlust av den kodade nyckeln eller på grund av att någon har fått obehörig åtkomst. Det finns en stor oro för företagen, eftersom de inte vill förlora sitt rykte. De är också enligt lag skyldiga att hålla den säker. Föreslagna åtgärder mot hoten är att göra en stark åtkomstkontroll på API:erna samt att kryptera och skydda integriteten för all data som är i rörelse. Vidare behöver man analysera dataskyddet både på designsidan och körsidan Det är också viktigt att man i kontrakten noga specificerar de strategier som gäller för backup och lagring. (Srinivasamurthy & Liu, 2010)

Olika former av konto-, service-, samt trafikkapning är ytterligare hot som molnanvändare behöver vara medvetna om. Exempel på sådana hot är Man-in-the-middle attacker, phishing, spam och DoS-attacker. För att minska den här typen av hot skulle man kunna förbjuda användarna att dela autentiseringsuppgifter mellan konto och tjänster samt använda förebyggande övervakning för att upptäcka otillåtna aktiviteter. Det är också av stor vikt att man förstår och sätter sig in ordentligt i leverantörernas säkerhetspolicys samt SLA. (Srinivasamurthy & Liu, 2010)

Exempel på saker som alltid bör hållas i åtanke är koduppdateringar, säkerhetspraxis, sårbarhetsproblem samt olika typer av intrångsförsök. För att minska den här typen av hot är det viktigt att övervaka och varna om nödvändig information. (Srinivasamurthy & Liu, 2010)

2.8 Standarder som verktyg för molntjänsters säkerhet

Det finns ett antal standarder för informationssäkerhet som även gäller för kunder när de väljer en molntjänst.

2.8.1 *ISO/IEC 27001*

Standarder görs utifrån diskussioner med många berörda organisationer och grupper både nationellt och internationellt. International Organization for Standardization (ISO), är den största utvecklaren av standarder. (ISO27000, 2007)

Ett certifikat enligt ISO/IEC 27001 visar att ledningssystemet för informationssäkerhet har uppfyllt kraven enligt standarden för informationssäkerhet. I denna standard specificeras generella krav som skall uppfyllas för att policy, mål, processer och rutiner skall vara så effektiva som möjligt för att hantera risker och förbättra informationssäkerheten. Det finns även krav på övervakning och granskning av informationssäkerheten samt underhåll av den. Ett certifikat garanterar för nuvarande - och blivande kunder att organisationen har definierat och verkställt effektiva informationssäkerhetsprocesser. Det bidrar till att skapa en förtroendegivande relation. En certifieringsprocess ger samtidigt organisationen möjlighet att fokusera på att kontinuerligt förbättra sin informationssäkerhetsprocess. (Calder & Watkins, 2008)

2.8.2 *ITIL*

ITIL (Information Technology Infrastucture Library) är också en säkerhetshanteringsstandard som är relevant för säkerhetshantering av molntjänster. ITIL definierar ett integrerat processbaserat tillvägagångssätt för att hantera IT tjänster och kan användas för varje typ av IT miljö inklusive molntjänster. ITIL försäkrar om att det tas effektiva mätvärden för informationssäkerhet på såväl strategiska som taktiska sant operationella nivåer. (Mather et al., 2009)

2.9 Avtal och lagar

Vid användandet av en molntjänst står det oftast i användarvillkoren att leverantören avsäger sig allt ansvar. Även om data hålls av en leverantör bär kunden det yttersta ansvaret för säkerheten och integriteten av data (Kandukuri et al., 2009). I Google apps villkor för att använda tjänsten står det att Google kan avbryta tjänsten, ha låg kvalité och vara full av fel men Google tar inget ansvar gentemot kunden. Villkoren för tjänsten säger även att

användaren uttryckligen godkänner att Google och partners inte ansvarar gentemot användaren för någon form utav skada. (Google, 2011) Även Amazon skriver i sitt kundavtal att de inte har något ansvar gentemot kunden i fall obehöriga får åtkomst, använder eller raderar kunders information eller applikationer. (Amazon, 2011)

Enligt Augustson och Sten (1999) är IT-rätt ett relativt ungt fenomen med rättsregler som reglerar den kommersiella användningen utav informationsteknik. Typiska frågor som omfattas är rättsliga ärenden relaterade till datorer, programvara och digitalt lagrad information, även telekommunikation kan ingå i vissa fall. Oavsätt om man köper en bil, båt eller diskett är det i huvudsak samma regler som avgör. Anledningen är att de köp- och avtalsrättsliga principerna som styrt den svenska rättsutvecklingen i decennier även gäller det IT-rättsliga området. De grundläggande lagarna inom juridiken som berör IT-rätten är i första hand *avtalslagen*, *köplagen* och *upphovsrättslagen*. Utöver det tillkommer även ett antal speciallagar som exempelvis nya personuppgiftslagen, telelagstiftningen och i vissa fall kan även lagen om offentlig upphandling (LOU) och de konkurrensrättsliga reglerna. Utmärkande för IT-rätten är också förekomsten av övergripande EU-direktiv som bland annat berör det rättsliga skyddet för datorprogram, personuppgifter och databaser. EU-direktiven har förenats med den svenska lagstiftningen genom bland annat nya personuppgiftslagen och genom ändringar i upphovsrättslagen. (Augustson & Sten, 1999)

2.9.1 *Avtalslagen*

Enligt avtalslagen sker ett avtal i två led, det vill säga, när en anbudsgivare lämnar ett bud eller en offert och en mottagare accepterar anbudet. Avtalslagen innehåller även en katalog över ogiltighetsgrunder, det vill säga, en beskrivning av de situationer som kan leda till att ett avtal ogiltigförklaras helt och hållet, som om det aldrig ingåtts. De klassiska ogiltighetsgrunderna är svek, tvång, råntvång, utpressning som ogiltighetsförklaras med stöd av ogiltighetskatalogen i avtalslagen. (Augustson & Sten, 1999)

När ett avtal har anknytning till flera olika länder behöver man avgöra vilket lands lag som ska tillämpas på avtalet. Lagvalet bestäms av så kallade internationella privaträttsliga regler. Huvudregeln är att avtalsparterna själv har rätt att bestämma vilket lands lag som ska tillämpas på avtalsförhållandet. Om parterna inte har något överenskommet löser man frågan med hjälp av internationella överenskommelser eller konventioner. De två mest väsentliga konventionerna är Haagkonventionen och Romkonventionen. För båda konventionerna avser lagen det land där säljaren befinner sig när han tar emot beställningen. Vid konflikt mellan konventionerna har reglerna i Haagkonventionen företräde. De enda skillnaderna mellan konventionerna avser tillämpningsområdena, eftersom Haagkonventionen inte är tillämplig på konsumentköp medan Romkonventionen kan tillämpas på alla typer av köp. (Gerhard, 2008)

2.9.2 *Köplagen*

Köplagen från 1990 reglerar köp av all slags lös egendom mellan näringsidkare. Lös egendom definieras som allting som inte är fast egendom, det vill säga, varor, bilar, aktier med mera. Köplagen är dispositiv, vilket innebär att parterna har full frihet att avtala om andra regler än

köplagens. Köplagen fyller med andra ord ut de punkter där parterna inte kommer överens om något annat. Den dominerande uppfattningen är att köplagen är direkt tillämplig på köp av hårdvara och standardprogramvara. Vid specialutvecklade system är lagen inte prövad i domstol, men enligt Augustson och Sten (1999) faller även outsouring av IT-tjänster under köplagen. Köplagen innehåller regler om beställningsköp när ansvaret går över från säljare till köpare. Den behandlar också frågor om fel och dröjsmål samt vilka påföljder som då gäller. Vid dröjsmål och fel är den huvudsakliga påföljden prisavdrag, rättelse, skadestånd och hävning. (Augustson & Sten, 1999)

2.9.3 *Personuppgiftslagen*

Den nya personuppgiftslagen (PUL) som trädde i kraft i oktober 1998, ersätter den gamla datalagen. I den nya lagen har kravet på tillstånd för databaserade register tagits bort. I stället fokuserar den på individers integritetsskydd. Det är endast under förutsättning att personen lämnat sitt medgivande till bearbetning av personuppgifter som dess personuppgifter får behandlas. Enligt lagen definieras personuppgifter som alla uppgifter som kan hänföras till en levande fysisk person. Nya personuppgiftslagen är anpassad efter EU:s direktiv. Det innebär att personuppgifter får hanteras över länders gränser inom EU utan särskilt tillstånd. Dock krävs samtycke om personuppgifter lämnas ut till ett land utanför EU exempelvis USA. (Augustson & Sten, 1999)

2.9.4 *Service Level Agreement*

Molntjänster har som tidigare nämnts flera likheter med outsourcing, på det viset att en klient överför vårdnaden av delar av sitt informationssystem till en tjänsteleverantör. Tjänsteleverantören tar därefter ansvar för kundens informationssystem och driver den i enlighet med de avtalsvillkor som kunden och leverantören kommit överrens om. De avtalsvillkor som definierar samarbetet och relationen mellan outsourcingklienten och leverantörer kallas för Service Level Agreement (SLA). SLA är ett specialfall av ett avtal mellan kund och leverantör. (Julisch & Hall, 2010)

SLA är det enda juridiska dokumentet mellan leverantören och kunden av molntjänsten. En mycket viktig del i SLA är, *Definition of Services* som beskriver sättet som tjänsten skall levereras på. Informationen om molntjänsterna måste vara exakta och innehålla detaljerade specificeringar på vad som skall levereras. En del av SLA, *performance management*, handlar om att hantera och övervaka prestandan av tjänsten. Det är viktigt att varje molntjänst kan mätas och att resultaten analyseras och rapporteras. Riktlinjerna, målet och mätvärden som skall användas måste specificeras tydligt. Det är också av stor betydelse att tjänstens prestanda kan granskas och revideras regelbundet av parterna. Syftet med *problem management* är att reducera den negativa påverkan på incidenter och problem. Det är ett krav att det ska finnas en lämplig process för att ta hand om och lösa oplanerade incidenter. Det måste också finnas förebyggande aktiviteter för att reducera förekomsten av oplanerade incidenter. (Kandukuri et al., 2009)

Kundens uppgifter och ansvar handlar om att få kunden att förstå att denne också har ett ansvar i att stödja tjänstens leveransprocess. Normalt sett måste kunden exempelvis ordna tillgångar och resurser för leverantörens anställda. SLA omfattar servicekvalitet, ersättningar i form av fodringar, rättsmedel för överträdelser samt undantag för nöd eller skador som inte kan förutsägas. Säkerheten är av stor betydelse i alla SLA. I den kan till exempel ingå att leverantören måste respektera och följa beställarens säkerhetspolicy och rutiner. (Kandukuri et al., 2009)

Amazon EC2 Service Level Agreement

Amazon kallar sin molntjänst för EC2. De ansvarar inte för några faktorer utanför deras kontroll. De tar inte heller något ansvar för om något händer i molnet på grund av kunden själv, en tredje part eller någon utrustning som inte är deras egen. Enligt deras SLA utlovas att tjänsten skall vara tillgänglig 99,95% under 365 dagar om året. Däremot är det kundens ansvar att kontrolla och rapportera till Amazon om tjänsten inte är tillgänglig. I de fall där Amazon tar på sig skulden får kunden någon form av ersättning. (Amazon, 2008)

Windows Azure Service Level Agreement

Azure är en form av molntjänst från Microsoft som fungerar som en plattform, där kunder kan ha program och verktyg för att bygga egna applikationer. Microsoft definierar i sitt SLA vad de levererar samt vad som händer om de inte levererar det. Det finns också specificerat under vilka omständigheter de inte är ansvariga. Microsoft lägger ett stort ansvar på kunden, vilket innebär att en hel del av de potentiella fel som kan uppstå är kundens ansvar. Microsoft garanterar minst 99,95% tillgänglighet och om tjänsten inte skulle vara tillgänglig den utlovade upptiden har Microsoft i sitt SLA specificerat hur mycket de betalar kunden i ersättning för den förlorade tillgängligheten. (Microsoft, 2010)

Google Apps Service Level Agreement

Google Apps är en SaaS-tjänst från Google som inkluderar exempelvis mailtjänsten G-mail och kontorspaketet Docs som bland annat innehåller ordbehandlare och kalkylblad. Tjänsten finns tillgänglig som gratisversion med begränsat lagringsutrymme samt betalversion där Google erbjuder mer lagringsutrymme för en avgift. Google lovar att tjänsten är tillgänglig minst 99,9% av tiden i en kalendermånad. Skulle Google mot förmodan inte uppfylla de utlovade kraven till kunden erbjuds gratisdagar för kunden. Ett exempel på det är om tjänsten enbart är tillgänglig 95 % - 99 %. Då erbjuds kunden sju dagars tillgång till tjänsten utan extra kostnad. Dock är det kundens ansvar att meddela Google inom 30 dagar från det att tjänstens tillgänglighet varit begränsad, för att få ersättning i form av extradagar utan kostnad. Google tar inte på sig ansvaret för problem som uppstår utanför deras kontroll, inte heller om det gäller kundens egna fel eller om problemet orsakats av en tredje part. Det står även preciserat i deras SLA att de har planerade driftstopp och att man som kund då måste vara medveten om att tjänsten kommer att ligga nere under en tid. Den tiden ingår således inte i den utlovade upptiden. Vid planerade driftstopp meddelas kunden fem dagar innan. Driftstoppet överstiger inte tolv timmar per år. (Google, 2011)

2.10 Sammanfattning av litteraturgenomgången

Verksamheter bör alltid göra någon form av riskanalys för att identifiera de risker som finns med en ny teknik. Det gäller även för molntjänster. Outsourcing av IT är en föregångare till molntjänster, vilket gör att det har många likheter med molntjänster. Precis som vid molntjänster släpps ytterligare en part in kundens verksamhet. Dessutom är den tredje parten en extern leverantör, vilket gör att risken för att någon använder informationen i ett syfte som skadar kunden ökar, medvetet eller omedvetet. (Kandukuri et al., 2009)

Flera av riskerna som finns med outsourcing kommer således även att förekomma när en kund beslutar sig för en molntjänst. De tre begreppen konfidentialitet, integritet och tillgänglighet är de tre främsta säkerhetsmålen för generell informationssäkerhet, vilket betyder att det även är av stor betydelse för molntjänster. (Krutz & Russel, 2010) Vid kundens val av en molntjänst behöver denne även besluta sig för vilken leveransmodell som är aktuell för verksamheten. De olika leveransmodellerna innebär olika säkerhetsrisker och ansvar för kunden. (Ramgovind et al., 2010) Även typen av molntjänst påverkar säkerheten. En privat molntjänst förekommer endast inom den egna organisationen och är därmed också säkrare än en publik molntjänst som förekommer utanför organisationen. (Ramgovind et al., 2010) (Mather et al., 2009) (Hofmann & Woods, 2010)Vid val av molntjänst behöver kunden också beakta infrastrukturens säkerhetsnivåer, som även de är avgörande för hur säker en molntjänst är, även om de ofta brukar ses som en helhet. (Mather et al., 2009) För att kunna ta fram en kravlista innehållande de krav som kunder ställer på olika leveransmodeller samt typer av molntjänster, för att den skall anses som säker, behöver bör man först och främst känna till de främsta riskerna säkerhetsmässigt med molntjänster. Exempel på det är enligt våra litteraturstudier att informationen skickas över Internet, hur informationen lagras hos leverantörerna samt hur leverantören hanterar lagrade informationen. Även information om systemadministratörerna är av största vikt. (Kandukuri et al., 2009) Det finns även ett antal standarder som underlättar för kunder när de står inför valet av en molntjänst såsom; ISO 27001samt ITIL. (ISO27000, 2007) (Mather et al., 2009)Vid en eventuell tvist mellan kund och leverantör är det viktigt för kunder att veta vilka lagar och avtal som gäller för molntjänsten. Service Level Agreement (SLA) är ett specialfall av ett avtal mellan kund och leverantör och är det enda juridiska dokumentet som finns mellan kund och leverantör. (Kandukuri et al., 2009)

Utifrån litteraturgenomgången har det utkristalliseras tre perspektiv som är av stor betydelse för kunder vid valet av molntjänstleverantör ur ett säkerhetsperspektiv och som vi kommer fokusera på i vår studie:

- Informationssäkerhet
- Typ av molntjänst
- Avtal och lagar

Informationssäkerhet avser konfidentialitet, integritet samt tillgänglighet, vilket är de säkerhetsmål man strävar efter att uppfylla även för molntjänster oavsett vilken typ man som kund väljer, privat eller publik molntjänst. Innehållet samt utformningen av det avtal som

skrivs mellan kunden och leverantören är av största vikt och påverkar i högsta grad säkerhetsgraden av molntjänsten.

3 Metod och empirisk undersökning

I detta kapitel presenterar vi den metod och den ansats vi valt för att uppfylla syftet med vår studie. Vi diskuterar metoden och dess relevans för underökningen. Metoden har gett oss stöd i hur vi skall genomföra vår studie.

3.1 Angreppssätt

Metoden är ett arbetssätt för att samla in empiri om verkligheten. När man genomför en empirisk undersökning, oavsett metod, finns det alltid en risk för att de resultat som vi kommit fram till har skapats av undersökningen det vill säga en undersökningseffekt. (Jacobsen, 2002)

Vi utförde ett antal semistrukturerade öppna intervjuer då vi ansåg att de skulle vara mest lämpliga för att få tillgång till den data som skulle besvara vår forskningsfråga samt uppfylla syftet med studien.

Vi valde mellan fyra olika metoder med olika syfte för datainsamling; den individuella öppna intervjun, gruppintervjun, observation samt dokumentundersökning. Enligt Jacobsen (2002) lämpar det sig bäst med öppna intervjuer när få enheter skall undersökas. Det var också av stort intresse för oss att få information om den enskilde individens inställningar och uppfattningar samtidigt som vi var intresserade av hur informanten tolkar och utvärderar ett specifikt fenomen. Dessutom har man vid öppna intervjuer möjlighet att gå på djupet inom ämnesområdet för att få en bredare och djupare förståelse för förhållandet mellan undersökningsenheten och den kontext som undersökningsenheten ingår i. (Jacobsen, 2002) Ovanstående överväganden ligger således också till grund för valet av den kvalitativa ansatsen, eftersom den ger oss ett lämpligt underlag för vår forskningsfråga och samt kravlistan. För att få en högre giltighet på svaren i undersökningen samt en så heltäckande bild som möjligt intervjuade vi både kunder och leverantörer av molntjänster. För att få relevant underlag för att besvara såväl forskningsfrågan som syftet med vår studie ansåg vi att det var av stor vikt att våra informanter hade dels ett stort intresse av ämnesområdet dels erfarenhet.

3.2 Semistrukturerade intervjuer

Informanterna vi använt oss av i vår studie kommer från tre olika företag; A, B och C från såväl större som medelstora kund- respektive leveransföretag av molntjänster i Malmö, Lund

och Stockholm. Totalt har vi intervjuat sex intervjupersoner varav tre av dem tillhör kategorin kunder av molntjänster och tre tillhör kategorin leverantörer av molntjänster. För att få det mest lämpliga underlaget till vår studie använde vi oss av besöksintervjuer på företagen samt en telefonintervju. Den sistnämnda på grund av ett alltför långt avstånd till intervjupersonen. Jacobsen(2002) menar att besöksintervjun är den vanligaste metoden inom den kvalitativa ansatsen. En av fördelarna med besöksintervjuer är att det är enklare för två personer att få personlig kontakt när de sitter fysiskt mittemot varandra jämfört med telefonintervjuer, även om telefonintervjuer kan minska det som benämns som intervjuareffekt. Besöksintervjuer innebär också färre allvarliga hot mot tillförlitligheten än öppna intervjuer via telefon, eftersom intervjuaren inte har möjlighet att observera intervjupersonen. (Jacobsen, 2002)

Vid de semistrukturerade intervjuerna har vi haft en fast struktur på intervjuguiden, fast ordningsföljd på frågorna och i stort sett enbart öppna frågor. Intervjuguiden skickades ut till informanterna i förväg för att de skulle kunna förbereda sig och ha möjlighet att ge så djupgående svar som möjligt. Samtliga besöksintervjuer har utförts på informanternas arbetsplats med undantag för en av leverantörsintervjuerna, som utfördes över telefon.

För att underlätta sammanställningen av det empiriska materialet har samtliga intervjuer spelats in digitalt. Det medförde samtidigt att vi hade möjlighet att upprätthålla en mer naturlig samtalskontakt med informanten och underlättade även flytet i intervjun. (Jacobsen, 2002) Informanterna tillfrågades före intervjun om det var OK för deras del. Ett annat syfte med att spela in intervjun var att vi ville försäkra oss om att inte förlora värdefull information.

3.2.1 *Urval av företag och informanter*

För att ha möjlighet att uppnå syftet och besvara frågeställningen inom den tidsram som getts för studien gjordes ett urval av kundföretag respektive företag som levererar molntjänster.

Urvalet för vår undersökning är:

- Leverantörer av molntjänster, väletablerade leverantörer med stor erfarenhet men även leverantörer med mindre erfarenhet av att leverera molntjänster, alla i Malmö-Lundregionen med undantag för telefonintervjun med Stockholm.
- Företag som i dagsläget använder olika typer av molntjänster i Malmö- Lundregionen samt Stockholm.

	Företag A	**Företag B**	**Företag C**
Typ av företag	Medelstort internationellt företag, *kunder samt leverantörer* av molntjänster	Internationellt börsnoterat företag, *leverantörer* av molntjänster	Internationellt börsnoterat företag, *kunder* av molntjänster
Antal Informanter	2st kunder samt 2 st leverantörer	1 st leverantör	1 st kund
Ort	Malmö	Lund	Stockholm

Tabell 3.1: Översikt av intervjuade företag

Vi hade följande kriterier på våra informanter för både leverantörer och kunder:

- Informanten skulle ha god generell kunskap om företaget
- Informanten skulle helst vara informationssäkerhetsansvarig alternativt besitta stor kompetens inom informationssäkerhetsområdet i företaget.

3.2.2 *Design av intervjuguide och intervjufrågor*

Intervjuguiden bestod av två delar, en till kunder och en till leverantörer. Intervjuguiderna var snarlika med skillnaden att frågorna till leverantörer var utformad för att identifiera vilka riskera de tar hänsyn till när de levererar en molntjänst. Intervjuguiden till kunderna utformades efter vilka säkerhetskrav kunder tittar på innan de beslutar sig för en molntjänst. Anledningen till att vi valde att intervjua både kunder och leverantörer var att vi förmodade att leverantörer och kunder inte ser på samma aspekter vad det gäller säkerhet för molntjänster, vilket vi även fick bekräftat under den empiriska undersökningen.

Intervjuguiden till kunder (Bilaga 7) bestod av fem rubriker, tjugo huvudfrågor samt ett antal underfrågor. Intervjuguiden till leverantörer (Bilaga 3) bestod av fyra rubriker, femton huvudfrågor samt ett antal underfrågor. Anledningen till att antalet frågor inte var färre var att vi bedömde den mängden frågor vara relevanta för att ge oss tillräckligt underlag för att kunna besvara vår forskningsfråga samt uppfylla syftet med studien. Dock hade fler frågor tagit för lång tid och kanske avskräckt informanterna vad gäller tid och detaljnivå. Vid utformningen av frågorna var vår strävan att utforma dem så att de blev så övergripande, tydliga och konkreta som möjligt. Även den språkliga formuleringen av frågorna var noggrant genomtänkt för att göra dem lättförståliga samt för att inte ge utrymme för frågorna att kunna misstolkas. Båda intervjuguiderna kategoriserades utifrån inriktningen på frågorna. Syftet med att dela in frågorna i ett antal kategorier var att skapa struktur som underlättade dels själva intervjun och dels sammanställningen av svaren efter intervjuerna.

Kategoriseringen av våra frågor för kunder av molntjänster var:

- Inledande frågor
- Säkerhetsrisker med molntjänster
- Skillnader i säkerhetskrav på olika typer av molntjänster samt leveransmodeller
- Juridiska avtal mellan kunder och leverantörer
- Avslutande frågor

Kategoriseringen av våra frågor för leverantörer av molntjänster var:

- Inledande fråga
- Säkerhetsrisker med molntjänster
- Fysisk säkerhet
- Lagar och avtal mellan kunder och leverantörer av molntjänster

Intervjuguide leverantörer

Inledande fråga

Intervjuguiden till leverantörer började med en inledande fråga för att se ifall det fanns några säkerhetsskillnader mellan PaaS, SaaS och IaaS. Vi ville se om valet av leveransmodell påverkar svaren av resterande frågor med målet att kunna dra en slutsats att någon leveransmodell har större säkerhetsrisk än en annan.

Säkerhetsrisker med molntjänster

Eftersom vi vill analysera vilka krav som måste uppfyllas för säkra molntjänster vill vi få bekräftat att vi täckt in alla riskerna som vi har tagit upp i vår litteraturgenomgång. Håller företagen med om de riskerna vi uppfattat? Har de några risker som vi inte har tagit med i vår litteraturgenomgång? Enligt undersökningsmodellen finns det fler typer av molntjänster. Vid första intervjun med en av leverantörerna ville han att vi skulle förtydliga vad vi menade med privat molntjänst, eftersom han ansåg att uttrycket inte var gemensamt inom branschen. Efter intervjun la vi till det som en extra fråga i intervjuguiden för att se om leverantörers definition av en privat molntjänst överensstämmer med kunders definition. Säkerhetsaspekterna skiljer sig mycket mellan en privat och en publik molntjänst och det är därför viktigt att branschen har en gemensam syn på definitioner inom molntjänster.

Fysisk säkerhet

Fysisk säkerhet är en del av den generella informationssäkerheten och är av stor betydelse även om det inte rör sig om en molntjänst. Den fysiska platsen där data förvaras kan vara en säkerhetsrisk. Det är viktigt att det specificeras i avtalen mellan kund och leverantör så att kunden känner sig trygg. Som nämnts för outsourcing finns det också säkerhetsrisker som inkluderar att obehöriga får tillgång till data eller att data förloras på grund av att Vi vill med denna fråga undersöka om de fysiska anläggningar som kunden egentligen inte har kontroll över vid en molntjänst är tillräckligt säkra. Fysisk säkerhet ingår som en del i tillgängligheten av tjänsten, vilket i sin tur är en del av de tre perspektiv som vi har fokus på i svår studie Det är ett av de kraven som ställs på säkerheten. Vi vill undersöka hur pass stor tillgängligheten är för leverantören till kunders data och om det uppstår ett hot ifall leverantörer har tillgång till kunders data? Hur förhindras de risker som finns på leverantörssidan, har de exempelvis säkerhetskontroll av anställda innan anställning? och finns det någon form av behörighetskontroller för att upprätthålla informationssäkerheten i form av konfidentialitet, integritet och tillgänglighet?

Lagar och avtal

Alla frågorna i intervjuguiden berör avtal och lagar för att veta vad det är som gäller om tjänsten uppfyller det som är angivet. Har leverantörerna ett färdigt SLA som kunden godkänner eller är det något som båda parterna gemensamt kommer överens om och vad finns angivet för att kunden ska känna sig säker med molntjänsten?

Intervjuguide till kunder

Inledande fråga

Som molntjänstleverantör förväntas man ha stor kunskap om molntjänster men hur väl känner kunder till molntjänster och dess säkerhet? Som en inledande fråga ville vi veta hur stor kunskap kunderna vi intervjuade hade inom molntjänster eftersom det påverkar kvalitén på resterande svar. Vi ville också undersöka vilka faktorer som kunder främst beaktar när de skall börja med en molntjänst. Är det säkerhetsaspekten som är den viktigaste faktorn att beakta eller är det andra faktorer som är viktigare? Vi ville även undersöka om någon av våra informanter har haft några negativa erfarenheter av molntjänster. Det ville vi göra eftersom vi ville identifiera om kunder har upplevt några säkerhetsrisker med molntjänster. Syftet med de inledande frågorna var också att få en förståelse och inblick i hur företagets kunskap och erfarenhet om molntjänster var. Ett annat syfte vara att skapa förutsättningar för att informanten skulle känna sig trygg i intervjusituationen.

Säkerhetsrisker med molntjänster

Med denna fråga ville vi undersöka om kunder utför någon form av riskanalys innan de bestämmer sig för vilken information de vill lägga i en molntjänst samt vilka risker de ser som de största vad det gäller molntjänster?

Lagar och avtal

Med frågorna som behandlar lagar och avtal ville vi undersöka vad som finns angivet i avtalen mellan leverantören och kunden och även om det är något parterna gemensamt kommer överens om? Det finns flera företag som är certifierade med exempelvis ISO 27000 och vi ville studera om kunder der det som en garanti för att leverantören uppfyller en viss säkerhetsnivå? Vi ville också undersöka om kunder har kunskap om vad som gäller om inte leverantören håller sitt avtal, exempelvis vilket lands lagar det är som gäller eller om det finns försäkringar som kunder kan teckna om inte leverantören håller sin del av avtalet? Eftersom SLA är det enda juridiska dokumentet som finns mellan kunden och leverantören och dilemmat med molntjänster är att kunden inte har kontroll över sin data förstår vi att avtalen är av största vikt.

Avslutande frågor

Som avslutande frågor ville vi veta om kunderna anser att de har samma syn på säkerheten som leverantörerna av molntjänster eller om det finns skillnader i synsätt. Om kunder och leverantörer inte skulle ha samma syn på säkerheten skulle vi se det som ett dilemma och vad skulle de skillnaderna kunna grunda sig på? För att ha möjlighet att komplettera med frågor i efterhand till våra informanter frågade vi även dem om det var okej att vi återkom om vi undrade över någon fråga, vilket slutligen inte visade sig behövas.

Strukturen och kategoriseringen av frågorna grundar sig på den teori och forskning som vi fördjupat oss i och presenterat i litteraturgenomgången. Samtliga frågor är förankrade i de tre perspektiv som tas upp i sammanfattningen av litteraturgenomgången (rubrik 2.10).

Innan intervjutillfällena utförde vi testintervjuer för att säkerställa ordval och tydlighet av intervjufrågorna och även för att ha möjlighet att upptäcka brister och behov av eventuella följdfrågor. Ett annat syfte var att undvika att behöva komplettera intervjuerna i efterhand, vilket hade varit svårt att göra på grund av den begränsande tidsfaktorn. Den avslutande frågan i intervjuguiden handlade om möjligheten att återkomma med kompletterande frågor vid behov, vilket aldrig behövdes. Efter intervjun med den första informanten kände vi behovet av att utöka vår intervjuguide med ytterligare en fråga som vi bedömde som avgörande för att kunna göra en rättvisande analys och slutligen besvara syftet med vår studie. Frågan gällde ”*Hur definierar du en privat molntjänst”*? Före undersökningen förmodade vi att våra informanter hade samma synvinkel på denna definition. Dock fick vi bekräftat vid första intervjun att det förmodligen inte var så. Därför kompletterades vår intervjuguide med den frågan från och med den andra intervjun.

3.2.3 *Datainsamling*

För att genomföra vår undersökning har vi använt oss av totalt sex intervjuer varav tre av dem tillhör kategorin kunder av molntjänster och tre av dem är leverantörer av molntjänster. Intervjuerna har utförts på tre olika företag varav ett företag är både leverantör och kund av molntjänster. Fyra av informanterna kommer från företag A och de övriga två från vars ett företag. Vi har samlat in data genom intervjuer och därefter transkriberat, analyserat och tolkat vårt underökningsmaterial. Samtliga intervjuer har varit semistrukturerade och öppna. De har utförts på informanternas arbetsplats med undantag för en telefonintervju. På så vis har vi haft möjlighet att uppmuntra djupare diskussioner mellan frågorna.

3.2.4 *Genomförande av intervju*

Vi inledde intervjuerna med att berätta kort om oss själva, syftet med vår studie och hur informationen och resultaten från våra intervjuer skulle användas och behandlas. Detta för att skapa en form av tillit och även som en form av uppvärmning för båda parter innan själva intervjun startade. Intervjun inleddes med ett antal lättsammare frågor, där vi bad informanterna berätta öppet om sin roll och befattning i organisationen. Jacobsen (2002) menar att de första frågorna är av stor betydelse eftersom, de anger tonen i intervjun och att det därför är viktigt att vara speciellt uppmärksam på dem. Ett annat skäl till att börja med en ganska allmän fråga är att man inte vill inleda ett samtal med för invecklade frågor, eftersom samtalet då lätt kan låsa sig. (Jacobsen, 2002)

Vi frågade också inledningsvis om det var möjligt att spela in intervjun. Frågorna ställdes växelvis och i de fall det fanns behov ställdes ytterligare följdfrågor. Under tiden som intervjun fortskred fördes anteckningar av intervjupersonerna, dels i syfte att uppvisa intresse för informanten, dels för att vid analysfasen lättare sortera det empiriska materialet. Informanten erbjöds också att ta del av de resultat vi kommit fram till i vår undersökning. För att behålla såväl företagens som informanternas anonymitet och inte göra det möjligt för någon att identifiera dem i organisationen har vi valt att inte transkribera deras namn i uppsatsen. Vid presentationen av vår empiri refererar vi till dem som Företag A, B samt C samt informant 1,2,3 respektive 4 inom respektive företag.

3.2.5 *Analys av intervjumaterialet*

Eftersom informanterna inte hade så stor erfarenhet av de leveransmodellerna PaaS och IaaS har inte vår empiriska undersökning gett oss tillräckligt underlag för att kunna definiera skillnaderna i säkerhet mellan de olika leveransmodellerna av molntjänster som vi hade tänkt i vår undersökning från början. Detta medför att det i de båda intervjuguiderna finns separata frågor om de olika leveransmodellerna trots att det inte finns i frågeställningen samt slutsatsen. Därför har vi i sammanställningen av de säkerhetskrav vi funnit på molntjänster och som vi också presenterar i empiri- och analyskapitlet sammanställt molntjänster som en helhet.

Våra intervjuer har sammanställts utifrån de kategorier vi har använt oss av i de båda intervjuguiderna. Anledningen till att vi kategoriserade dem var att vi ville samla ihop data till grupper och genomföra en abstrahering av den. Vi ville få en form av struktur och samla ihop intervjusvaren på ett lättöverskådligt sätt för att kunna uppfylla vårt syfte och för att kunna besvara vår frågeställning. Jacobsen (2002) menar att ett av syftena med kategoriseringen är att förenkla komplicerad och detaljrik data och att hänföra materialet till en viss kategori utifrån vissa kriterier. I och med det kan vi också förhålla oss till ett fåtal kategorier och behöver inte hantera den totala datamängden. Kategoriseringen är också en förutsättning för att kunna jämföra de olika intervjumaterialen. (Jacobsen, 2002) Vi har då också möjlighet att jämföra de olika intervjuerna som behandlar samma ämne och belysa dem ur olika synvinklar.

3.3 Undersökningens kvalitet

Metoden är som tidigare nämnts vårt tillvägagångssätt när vi utför vår undersökning. Oavsett vilken typ av undersökning det rör sig om bör empirin uppfylla följande två krav enligt Jacobsen (2002):

- Empirin måste vara giltig och relevant (valid)
- Empirin måste vara tillförlitlig och trovärdig (reliabel)

Det betyder att vi vill ha ett resultat som mäter det vi är intresserade av och som vi kan lita på. För att uppfylla de två kraven måste studien genomföras på ett korrekt sätt.

Validiteten det vill säga giltigheten av undersökningen avser att belysa huruvida undersökningsmetoden faktiskt mäter de fenomen som vi faktiskt vill undersöka. (Jacobsen, 2002) Med utgångspunkt från det har vi utformat våra intervjuguider så att frågorna i dem är förankrade i vårt teoretiska ramverk (figur 2.4)för att uppfylla syftet med studien och därmed vara säkra på att de är lämpliga utgångspunkter för att besvara vår forskningsfråga. Då några av våra informanter inte har så stor erfarenhet av de olika typerna samt leveransmodellerna som finns av molntjänster medför det att vi inte kan generalisera resultaten. Däremot har två av våra informanter (informant 1, företag B) samt (informant 1, företag C) dels mycket höga befattningar och dels lång erfarenhet inom informationssäkerhetsområdet i sina respektive verksamheter, vilket gör att studiens validitet ändå kan anses som hög.

Vad avser undersökningens reliabilitet, det vill säga dess tillförlitlighet och trovärdighet avses att undersökningen går att lita på. Det innebär enligt Jacobsen (2002) att man i så fall kan förvänta sig ungefär samma resultat om man skulle genomföra exakt samma undersökning en gång till. Då vi har fördjupat oss i flera olika källor inom såväl den akademiska litteraturen som tidigare forskning och främst använt oss av primärkällor vid våra litteraturstudier har vi tagit detta i beaktande. En annan faktor som bidrog till att höja reliabiliteten i vår studie var att vi genomfört sex olika intervjuer med intervjupersoner dels från olika företag men också från olika befattningar inom förtagen för att få en så bred bild som möjligt av vårt problemområde. För att höja tillförlitligheten har vi också spelat in samtliga intervjuer elektroniskt. Genom det har vi försäkrat oss om att vi uppfattat informanternas svar rätt. För att försäkra oss om att vi uppfattat intervjusvaren rätt skickade vi det transkriberade materialet till våra respektive informanter för att de i efterhand skulle ha möjlighet att korrigera eventuella missförstånd eller dylikt.

3.4 Etik

Vår empiriska undersökningsprocess är planerad och utförd utifrån målet att tillgodose de tre grundkrav som Jacobsen (2002) rekommenderar det vill säga:

- Informerat samtycke
- Krav på privatliv
- Krav på att bli korrekt återgiven

Vad gäller informerat samtycke handlar det framförallt om att den som undersöks frivilligt skall delta i undersökningen samt bli informerad om vilka risker och vinster som finns med ett deltagande. (Jacobsen, 2002) För att beakta detta e-postade vi våra informanter innan vi ringde dem, vilket gjorde att de hade möjlighet att ta ställning till om de ville delta i undersökningen i god tid före samtalet. I e-postmeddelandet gjordes en kort beskrivning av oss och även syftet med studien och även hanteringen av studiens resultat uppgavs. Även vid telefonsamtalet påminde vi om undersökningens syfte och hur vi skulle använda oss av resultatet.

Jacobsen (2002) menar att man i den mån det är möjligt skall försöka återge resultatet av en undersökning fullständigt och i rätt sammanhang. Det har vi eftersträvat i möjligaste mån, vilket innebär att samtliga intervjutranskriberingar som gjorts har utförts så ordagrant som möjligt. För att få en bekräftelse på att det intervjuresultat vi fått fram är korrekt och att vi uppfattat aspekter och förhållande av problemområdet som vår studie omfattar på rätt sätt har som tidigare nämnts samtliga intervjutranskriberingar också skickats tillbaka till respektive informanter för granskning. Genom det har informanterna getts möjlighet att korrigera eventuella missförstånd eller liknande i efterhand.

4 Empiri och Analys

I Emperi- och analyskapitlet presenterar vi resultatet av vår empiriska undersökning utifrån de tre perspektiven (rubrik 2.10) som studien grundar sig på: informationssäkerhet, säkerhetsskillnader mellan olika typer av molntjänster samt de lagar respektive avtal som molntjänsten omfattas av. Materialet är analyserat, grupperat och sammanställt utifrån dem. Litteraturgenomgången jämförs med det empiriska materialet utifrån varje perspektiv och analyseras därefter.

Svaren är sammanställda från både kunder och leverantörer för att få ett bredare perspektiv på det ämnesområde som behandlas. Kapitlet inleds med ett antal tabeller som ger läsaren en överblick av undersökningens resultat. Sammanställningen av analysen redovisas i den kravlista som presenteras i studiens slutsats.

4.1 Empiriskt resultat

De frågor i intervjuguiden som främst ligger till grund för att besvara syftet med vår studie och därmed forskningsfrågan presenteras översiktligt nedan i tabellformat.

Leverantörer	Informant 1, företag A	Informant 2, företag A	Informant 1, företag B
Roll	• Konsult	• Portallösningsansvarig	• Chief security advisor
Hur upprätthålls CIA?	• Kryptering gör det svårare • Placering av servrar • Tydliga avtal med underleverantören	• Kontroll av leverantör samt underleverantörer • Ha rutiner och en noggrant utarbetad hantering av den mänskliga faktorn, viktigt med åtkomstkontroll för systemadministratörerna	• Åtkomstkontroll för anställda • Separera kunders data • Övervakning av anställda • Backup i form av redundanta elledningar, redundanta kylningar, redundanta fiberkopplingar samt redundanta hårddiskar
Säkerhetsskillnad-er mellan molntjänsttyper	• Privata ger mer kontroll • Publika kräver noggrannare avtal och en mer omfattande helhetsbedömning av leverantören	• Data ligger inte på egen server vid användning av en publik molntjänst	• Tillgängligheten är lättare att upprätthålla i en privat molntjänst än i en publik molntjänst
Avtal och lagar	• Står enkla och generella saker i avtalet • Avtal är viktiga • Tillgänglighet i procent • Förtroende är viktigt eftersom man inte kan skriva allt på papper • Svårt att veta vilka lagar som gäller	• Inte lova för mycket i SLA • Nästan alltid Sveriges lagar som gäller • Klausul i avtal om vilken skiljeman man använder • Slutligen går det till rätten men man har aldrig varit med om det • Alla avtal är olika • Kunden får kompensation i form av extra tid för molntjänsten • Olika färdiga SLA för olika nivåer • Står inget om hur information hanteras eller vem som äger den • Garanterar 99, 98 % upptid, men ändå många timmar tjänsten inte är uppe • Få kunder håller räkningen på tjänstens upptid	• Färdigt SLA • 99,9 % tillgänglighet, lite beroende på tjänst • Det är kundens uppgift att se till att man följer de lagar och regler som finns och det ska vara tydligt för kunden. • Beror på hur avtalet ser ut • Våra kunder hamnar på irländsk rätt eftersom datacentret är i Irland vilket står i avtalet • Det är alltid kundens ansvar att se till att lagar och regler följs • Monetär ersättning

Tabell 4.1: Översikt av empiri: leverantörer

Kunder	Informant 3, företag A	Informant 4, företag A	Informant 1, företag C
Roll	• IT ansvarig	• Kvalitetsansvarig	• Chef IT Security Corporate IT
Hur upprätthålls CIA	• Granska leverantören • Bra lösenord • Krypterade förbindelser • Stark autentisering • Separerad data från övriga kunder • Stabil leverantör, skriva supertydliga avtal	• Behörighetskontroller • Etablerad leverantör. • Behöver ha kontroll över underleverantörerna • Kontrollera vem som har behörighet till data • Behovet av kryptering ökar ju längre från verksamheten man kommer	• Bakgrundskontroller av personal, • Krypterad databas, • Krypterad Backup, • SLA med underleverantörer
Säkerhetsskillnader mellan molntjänsttyper	• Har ingen aning om vad ett privat moln är	• Ser inte vitsen med ett privat moln och kan därför inte svara på det	*Privat molntjänst:* • Källkod • Kompetens • Kryptering • Rollbaserade åtkomsträttigheter • Lösenord • Loggning • Uppfylla kundens säkerhetspolicy *Publik molntjänst:* • Veta var data lagras • Ägare till data? • Hur data transporteras • Hur återfås data? • SLA med underleverantörer • Bakgrundskontroll • Intrångsskydd (IPS & IDS) • Brandväggar • Administratörers åtkomstkontroll • Segregation av kunders data • Kryptering • Lösenord • Loggning
Avtal och lagar	• Svårt vid internationella avtal mellan företag i olika länder • Leverantören skickar ett SLA som vi godkänner • SLA enda juridiska dokumentet • Jätteviktigt med supertydliga avtal • Måste vara jurister som tittar på avtalen • Vet inte vems lag som gäller	• Lagar är alltid ett dilemma men normalt sätt köplagen • viktigare att skriva vad som inte ingår, istället för vad som ingår.	• Beror på vem man skriver avtalet med • Oftast svensk lag • Använder engelsk advokatfirma till många avtal • Viktigt att vara med i hela avtalsprocessen • Kundens krav måste avspeglas i avtalen ända till och med implementeringen

Tabell 4.2: Översikt av empir: kunder

4.2 Informanter

Våra informanter har varit kunder och leverantörer från såväl stora som medelstora företag med den gemensamma faktorn att de samtliga har både stor kunskap, erfarenhet samt intresse för molntjänster. Kunderna visade sig inte ha så stor erfarenhet av riskerna med molntjänsternas infrastruktur på de specifika nivåerna, det vill säga nätverksnivå, värdnivå samt applikationsnivå, som vi efterfrågade i vår intervju. Därför redovisas materialet utifrån molntjänsters helhetsperspektiv. Informanterna definierade sina respektive krav olika detaljerat beroende på erfarenhet inom säkerhetsområdet, vilket också avspeglas i tabellen nedan. Våra respektive informanter har haft rollerna som; kvalitetsansvarig, IT-ansvarig, säkerhetsansvarig, säkerhetsrådgivare samt portallösningsansvarig, vilket gett oss en bred spridning på studiens resultat.

4.3 Risker med molntjänster

Enligt litteraturgenomgången (rubrik 2.7) är de främsta riskerna säkerhetsmässigt med molntjänster att informationen skickas över internet, att man inte har kontroll över hur data lagras hos leverantören samt hur leverantören hanterar den lagrade informationen. Informationen om de systemadministratörer som sköter uppgifter av olika slag runt molntjänsten utgör också en stor risk. Vid vår empiriska undersökning framkommer det samma risker som de främsta som vi funnit vid litteraturgenomgången, där man lyfter fram underleverantörerna som en stor risk och även administratörernas åtkomst av data.

> *..Största säkerhetsriskerna med molntjänster….ett konstigt svar kanske…Men det vi har upptäckt, det är att ..de som är underleverantörer.. för normalt sett gör du ett avtal med en molntjänstleverantör och sen outsourcar de driften av hela miljön och administrationen av infrastrukturen till nån annan och de har ju vi inga avtal med. Så våra frågebatterier borde egentligen gå till de också, och det gör de…och vi måste se avtalen nästan och deras SLA. Vad har de för Service Level Agreement mellan den leverantören och den leverantören som vi har som avtalspart?(Informant 1, företag C)*

Informanterna nämner till exempel att en stor risk är att kunden inte vet var datan finns eller vem som har åtkomst till datan. Det är utifrån dessa risker som informanterna senare i våra intervjuer uppger de krav de ställer på molntjänster. Syftet med de olika kraven som kunder ställer på molntjänster, för att de skall anses som säkra, är att minimera de risker som förekommer vid användning av molntjänster. Vi ser det som att de risker som både litteraturen lyfter fram och även vårt empiriska material avspeglar de kraven som kunder har på konfidentialitet, integritet och tillgänglighet.

4.4 Informationssäkerhet

Vid sammanställningen av det empiriska materialet från vår studie har vi under denna rubrik sammanfört svaren från informanterna som handlar om vilka generella krav kunder och

leverantörer ställer på molntjänster oavsett molntjänsttyp för att uppnå informationssäkerhet det vill säga: konfidentialitet, integritet och tillgänglighet.

På samma sätt som konfidentialitet, integritet och tillgänglighet är viktigt för allmän informationssäkerhet är de tre säkerhetsmålen; konfidentialitet, integritet och tillgänglighet viktiga för molntjänster enligt litteraturgenomgången (rubrik 2.3). Vid våra intervjuer fick vi detta bekräftat, då några av våra informanter svarade att det främst är dessa tre säkerhetsmål man tänker på även när man strävar efter att garantera säkerheten för molntjänster.

Enligt (rubrik 2.3.1) garanterar konfidentialiteten att användardata som finns i molntjänster inte kan nås av obehöriga utan endast genom en korrekt krypteringsteknik. De element som används för att försäkra konfidentialiteten är bland annat nätverksautentiering samt kryptering av data. (rubrik 2.3.1) Vid vår empiriska undersökning framkom det att informanterna har i stort sett samma former av generella krav på molntjänster som vi funnit i litteraturgenomgången, det vill säga vikten av åtkomstkontroll av de anställda, kryptering av nätverkstrafiken samt betydelsen av starka lösenord. Informanterna tar även upp vikten av att kundens data är separerad från övriga kunders data. (rubrik 4.1)

> *Där är det väl också så, att det som är viktigt för oss, för säkerheten det är ju det att det är krypterade förbindelser med stark autentisering, alltså att lösenord hanteras på rätt sätt och sen på leverantörssidan att våra uppgifter hålls helt separerade med övriga kunders.(Informant 3, företag A)*

Enligt litteraturgenomgången (rubrik 2.3.2) handlar *integriteten* av data om en garanti för att meddelandet som mottagits är samma som det som skickats. Integritetsförlust kan uppstå genom en attack som görs avsiktligt av någon som vill förändra informationen alternativt oavsiktligt. Enligt litteraturgenomgången (rubrik 2.3.2) är de element som används för att försäkra sig om integriteten bland annat brandväggar och intrångsskyddstjänster, såsom exempelvis IPS och IDS. Det är även dessa som våra informanter tar upp. Vi ser det som att informanterna har stor kunskap och erfarenhet om behovet av dessa former av skydd för data i molntjänster.

Enligt litteraturgenomgången (rubrik 2.3.3) ingår i begreppet tillgänglighet en försäkran för kunden om att det finns en förbindelse som är tillgänglig när det önskas och som tillåter behöriga användare att komma åt system och nätverk . Exempel på hot som riktar sig mot tillgängligheten är Denial of Service attacker (DoS attacker). Ett exempel på ett element som används för att försäkra sig om tillgänglighet är exempelvis backup. Flera av våra informanter som är leverantörer betonar vikten av just tillgängligheten på molntjänsten. För att upprätthålla tillgängligheten lyfter en av informanterna fram hur de som leverantörer har såväl redundanta elledningar som - kylningar, - fiberkopplingar och redundanta hårddiskar.

Vid intervjuerna framkommer det således att såväl kunder som leverantörer använder sig av olika säkerhetsverktyg såsom exempelvis kryptering, intrångstjänster, backup samt åtkomstkontroll för att kunna uppfylla dessa krav. Vår reflektion är dock att de av våra informanter som har störst erfarenhet inom informationssäkerhetsområdet också är de som uttrycker sina generella krav i form av termer som konfidentialitet, integritet samt tillgänglighet. Vår tolkning är att övriga informanter också arbetar efter samma mål vad gäller

informationssäkerheten för molntjänster, men använder en annan terminologi, åtminstone vid intervjuerna. Vi förmodar att förklaringen till det är att de inte har lika stor erfarenhet inom informationssäkerhetsområdet. Ett exempel på det är att flera av informanterna anger kryptering, segregering av data samt lösenord som krav på säkerhet, vilket till exempel är olika exempel på att hantera säkerheten för att uppfylla konfidentialiteten samt integriteten av data.

> *Där är det väl också så, att det som är viktigt för oss, för säkerheten det är ju det att det är krypterade förbindelser med stark autentisering, alltså att lösenord hanteras på rätt sätt och sen på leverantörssidan att våra uppgifter hålls helt separerade med övriga kunders.(Informant 3, företag A)*

> *[…]men det är ju ganska många frågeställningar egentligen, som man måste ta hänsyn till, för att kunna få en komplett bild på vad det egentligen är man köper för någonting. (Informant 1, företag C)*

Det framkommer också vid intervjuerna med både kunder och leverantörer att de anser att de tre begreppen konfidentialitet, integritet och tillgänglighet är generellt sett inbördes lika viktiga, eftersom man inte klarar sig med enbart två av dessa. Dock är det graden av känslighet på kundens information som finns i molnet, som avgör vilken av parametrarna som är av störst vikt för den aktuella informationen.

> *Om man ska hårddra det kan man säga så här, om du har jättebra konfidentialitet och jättebra integritet men noll tillgänglighet skulle ingen använda tjänsten för att de skulle inte kunna komma åt den. Den är ju ganska viktig, för det funkar inte annars. Har du en tjänst som är jättetillgänglig men konfidentialiteten är låg får du kanske ett lägre förtroende för tjänsten men det kan ändå innebära att folk väljer att använda den. (Informant 1, företag B)*

I vår undersökning framgår det också att de avtal som skrivs mellan kunden och leverantören för molntjänsten är av stor betydelse för hur väl konfidentialiteten, integriteten samt tillgängligheten av data upprätthålls i molntjänsten. Det framkommer också i studien att flera av informanterna uppger att det viktigaste kraven de har för att upprätthålla såväl konfidentialitet, integritet som tillgänglighet i molntjänsten är att man som kund har möjlighet att få en helhetsbedömning av leverantören inklusive dess underleverantörer och att man definierar och specificerar de krav man har i avtalet med leverantören. Det är också av största vikt att kunden kan lita på att leverantören följer upp de krav som kunden specificerat i avtalet med leverantören hela vägen till och med implementeringen av tjänsten.

På frågan om vilka generella krav våra informanter ställer på molntjänster svarar de två mest erfarna av informanterna att deras allmänna krav på en molntjänst är att den skall uppfylla kraven på konfidentialitet, integritet samt tillgänglighet. Övriga informanter använder andra begrepp som exempelvis kryptering, som är underordnat exempelvis konfidentialitet. Vår reflektion är att de av informanterna som har störst erfarenhet inom informationssäkerhetsområdet också är de som använder sig av begreppet konfidentialitet, integritet samt tillgänglighet. Vår tolkning är att övriga informanter också i grunden eftersträvar att upprätthålla konfidentialitet, integritet samt tillgänglighet även för molntjänster, men uttrycker det i mer underordnade termer, åtminstone vid våra intervjuer. Vår reflektion är också att det är av stor vikt att både kunder och leverantörer har samma syn

på de olika begreppen; konfidentialitet, integritet samt tillgänglighet. Vid en diskussion med våra informanter om konfidentialitet, integritet samt tillgänglighet uttryckte en av våra informanter att det kan vara ett dilemma. Man kan ju fråga sig när en tjänst räknas som tillgänglig och bedömer man att tjänsten är tillgänglig, även om det tar exempelvis femton minuter att utföra varje anrop?

Vår studie har visat att de tre säkerhetsmålen; konfidentialitet, integritet samt tillgänglighet är lika relevanta för molntjänster som för andra typer av IT tjänster eftersom informanterna utgår från dem när de ställer de olika formerna av krav på molntjänster. Eftersom majoriteten informanterna inte har någon större erfarenhet av PaaS och IaaS har inte studien gett oss något konkret underlag för skillnader i säkerhetskrav mellan de respektive leveransmodellerna. Utfallet av studien pekar dock på att konfidentialitet, integritet samt tillgänglighet inte är mer viktigt för en leveransmodell än en annan. Vår studie visar att leverantörerna lägger extra stor vikt vid kravet på tillgänglighet av molntjänsten medan det är en helhetsbedömning av leverantören samt ett välutformat och välspecificerat SLA, som är det viktigaste från kundens perspektiv.

4.5 Säkerhetsrisker för olika typer av molntjänster

Som vi redogjort för i litteraturgenomgången (rubrik 2.5.2) skiljer sig en privat molntjänst från en publik molntjänst genom att både nätverk, processer och lagring tillhör den egna organisationen när det gäller den privata molntjänsten. Trots att branschen verkar ha en känsla för vad som avses med begreppet privat molntjänst visade det sig att definitionen inte var uppenbar för våra informanter i studien. Vid första intervjutillfället med en av de stora leverantörerna i branschen framkom det att det till och med kunde vara ett dilemma i branschen. För att få klarhet i begreppet privat molntjänst rekommenderade vår första informant oss att komplettera intervjuguiden med denna fråga, vilket vi också gjorde.

> *Men skulle ni inte kunna ha det som en fråga till alla dem som ni pratar med? Vad är definition av ett privat moln? För har de olika definitioner så är det ju ett problem för branschen. Min definition tror jag hyfsat stämmer överens med ganska många. Man har virtualiserat sin IT-infrastruktur som det privata molnet. (Informant 1, företag B)*

Vi menar att det är av största vikt att alla inom IT branschen har samma definition av begrepp som även gäller molntjänster. Vi uppfattar det som att den gemensamma definitionen är en förutsättning för att kunder skall kunna välja och jämföra leverantörers produkter.

Enligt litteraturgenomgången (rubrik 2.7) innebär det en risk att hantera känsliga uppgifter utanför företaget, vilket är fallet vid en publik molntjänst. Det framgick också tydligt vid vår undersökning att så är fallet, eftersom företaget saknar kontroll av både hårdvara och mjukvara. I litteraturgenomgången (rubrik 2.7) beskrivs flera av de säkerhetsrisker som uppkommer i samband med publika molntjänster samt hur man bör hantera dem. Som kund bör man till exempel försäkra sig om att såväl konfidentialiteten som integriteten mellan organisation och molntjänstleverantör upprätthålls. Ett sätt att minska konfidentialitetsrisken är att använda sig av krav på såväl åtkomstkontroll som kryptering. Specifika digitala

signaturer gör det svårare för någon att ändra data, vilket skyddar integriteten. (rubrik 2.3.2) Enligt litteraturgenomgången (rubrik 2.3.2) hanterar man också de olika riskerna med integriteten för molntjänster genom att använder sig av message authentication code (MAC) samt åtkomstkontroll. För att upprätthålla tillgängligheten kan man enligt teoridelen (rubrik 2.3.2) skydda sig genom olika former av behörighetskontroll av nätverket samt tillhandahålla någon form av nätverksbaserat intrångsskydd. En annan riskfaktor som vi tar upp i vår litteraturgenomgång (rubrik 2.7) är osäkra användargränssnitt. Det avser de gränssnitt som kunden använder för att interagera med molntjänsterna. Det är av största vikt att de är säkra vad gäller autentisering, åtkomstkontroll och kryptering, särskilt när det finns en tredje part involverad. Det är också av största vikt att tillhandahålla såväl backup som brandväggar samt säkerhetsuppdateringar för att hantera de olika riskerna som finns med molntjänster. Det som också är betydelsefullt är att man som kund förstår och sätter sig in ordentligt i leverantörernas säkerhetspolicys samt SLA.

Endast några få av våra informanter nämnde krav som exempelvis MAC. Vi ser det som att en av anledningarna till det är att informanterna istället för att gå in på detaljer pratade om mer övergripande begrepp som exempelvis åtkomstkontroll som omfattar även MAC. Vi menar att samtliga krav som nämnts är oerhört viktiga krav att ställa på en molntjänst för att den skall anses som säker.

Vid våra undersökningar med såväl kunder som leverantörer tas det upp en mängd olika exempel på risker med framförallt publika molntjänster samt exempel på hur man kan hantera riskerna.

> *Datormiljön, accesskontroll, brandskydd, kylning alla de här standardgrejorna som vi har, vi måste ju se att de har också har de, hur patchar de systemet och rullar tillbaka det, antivirus, deras interna säkerhetsprocedur, penetrationstestning - hur sker det , kryptering av data, är vi inne på igen ,kapacitetsplanering, - har de hårdvaran så att de kan växa om de får tre nya kunder eller står de helt still då eller vad händer, rollbaserade accessrättigheter, igen. Lösenord samma sak och loggning samma sak, men sen har vi administratörsaccess. Det är ju deras administratörer då, det måste vi ju förstå - vad är det för typ av access och hur kan vi skydda oss , hur segregerar de andra kunders data från vår data, det måste vi ju förstå .(Informant 1, företag C)*

De krav som våra kunder främst tänker på för att öka tilliten till en publik molntjänst och för att anse att tjänsten är säker är att kunden har möjlighet att göra en helhetsbedömning av leverantören. Det framkommer också att det är av stor vikt för kunderna att det avtal som skrivs mellan kunden och leverantören i form av SLA är väldefinierade samt inkluderar samtliga omständigheter runt underleverantörerna av tjänsterna.

> *[…] Största säkerhetsriskerna med molntjänster….ett konstigt svar kanske…Men det vi har upptäckt, det är att ..de som är underleverantörer.. för normalt sett gör du ett avtal med en molntjänstleverantör och sen outsourcar de driften av hela miljön och administrationen av infrastrukturen till nån annan och de har ju vi inga avtal med.(Informant 1, företag C)*

När det gäller publika molntjänster har såväl kunder som leverantörer även krav på att vara garanterad att data är separerad från övriga kunders, vilket också tydligt framgår i vår empiriska undersökning. Kunderna vill också att det skall finnas olika nivåer av

säkerhetskontroller, behörighetskontroller samt väl genomtänkta backuper. För att förebygga olika typer av intrångsförsök såsom Intrusion Detection system (IDS)samt Intrusion Protection system(IPS) använder en av våra intervjuobjekt sig också av övervakning.

> *Sen tittar vi på helt andra saker…IPS och IDS. Hur skyddar man sin miljö med Intrusion Prevention eller Intrusion Detective. Vad har de för backuper? Men nu måste vi också veta hur många generationer backuper har de, är det det vi behöver eller är det för lite eller hur ser det ut och var lagrar de det externt? Är det ute i ett bankvalv eller är det i Kazakstan eller var sjutton är det tro och kan de kryptera backuperna?(Informant 1, företag C)*

På ett av de undersökta kundföretagen har man utarbetat ett antal gedigna mallar över de krav som ställs på leverantören och molntjänsten som man använder sig av i samband med att man köper molntjänster. Kundföretaget ser mallarna som ett hjälpmedel för att på ett kontrollerat och strukturerat sätt hantera de risker som uppkommer i samband med olika molntjänster. Övriga kundföretag har inte kommit lika långt vad gäller liknande processer utan förlitar sig på avtalen som skrivs mellan leverantören och kunden.

> *Jag insåg efter ett tag att ju molnigare det blir, desto tydligare måste man vara. Det är så lite grann hela tiden, att har du en specifik leverantör, så är det ganska lätt, men ju bluddrigare det blir desto mer tid måste jag ägna åt att säkerställa hur fakta ser ut bakom, Många kunder tror jag inte orkar det . Utan man stoppar någonstans där i början, men där ser man inte hela den skogen av risk och hot som finns bakom.(Informant 1, företag C)*

Skillnaderna i säkerhet mellan de olika typerna av molntjänster beror på att arkitekturen av de respektive molntjänsterna är olika. Eftersom man i de privata molntjänsterna själv står för nätverk, processer, lagring och inte delar företagets data med en extern leverantör är således den privata molntjänsten betydligt säkrare än den publika typen. Vid införande av publika molntjänster behöver kunden vara extra observant på att leverantören håller kundens data avskild från övriga kunder samt att leverantören behärskar övriga tekniska aspekter för att skydda kundens data. När kunden väljer en leverantör bör den göra en heltäckande leverantörsbedömning och välja en väletablerad leverantör samt ha i åtanke eventuella underleverantörer. Kunden bör även tänka på att ha ett välskrivet SLA med leverantören. Valet av molntjänsttyp är således avgörande för molntjänstens säkerhet.

4.6 Avtal och lagar

Under den här rubriken presenteras resultaten av vår empiriska undersökning på frågan om vilken typ av avtal som finns mellan kund och leverantör vid införande av molntjänster samt vad som brukar ingå i avtalet.

Enligt litteraturgenomgången (rubrik 2.9.4) är det kundens ansvar att kontrollera och rapportera till leverantören om en molntjänst inte fungerar enligt det överenskomna avtalet. Vid vår studie framkommer det att flera leverantörer inte tar på sig ansvaret för de eventuella problem som kan uppkomma utanför deras kontroll. Exempel på det är om problemet orsakas av kunden alternativt av en tredje part. Trots att leverantören har ansvaret för tjänstens

säkerhet är det således kundens ansvar att kontrollera att den följs. Kunden har oftast en begränsad tid på sig att meddela problemet till leverantören för att få ersättning.

Enligt litteraturgenomgången (rubrik 2.2) har molntjänster många likheter med outsourcing av IT vad avser att kunden överlåter vårdnaden av sitt informationssystem till en tjänsteleverantör. Tjänsteleverantören övertar driften av kundens informationssystem i enlighet med de avtalsvillkor som kunden och leverantören kommit överrens om. (rubrik 2.9) De avtalsvillkor som definierar samarbetet och relationen mellan kunden och leverantörer benämns som för SLA och är också det enda juridiska dokumentet som finns mellan kund och leverantör. Avtalet är centralt för kunden och leverantören och i detta specificeras alla överrenskommelser mellan kund och leverantör av molntjänsten. (rubrik2.9) Vid våra intervjuer framkommer det att det är av stor betydelse att såväl kunden som leverantören är överrens om det man skrivit in i avtalet. Det är också viktigt att kunden följer upp avtalet så att det i slutändan överensstämmer med implementeringen. Vid studien framkommer att det endast står enkla och generella krav i SLA samt att vad som gäller beror på vem man skriver avtalet med. Enligt (rubrik 2.9.4) finns i avtalet definierat exempelvis det sätt som tjänsten skall levereras på samt tjänstens servicekvalitet och ersättningar i form av skadestånd. Det står också att leverantören måste följa kundens säkerhetspolicy och rutiner. I avtalet finns det inte specificerat hur informationen hanteras eller vem som äger den. Undersökningen visar att det är viktigt för kunder att veta att leverantören fullföljer hela processen det vill säga att kundens krav således avspeglas i implementeringen. Vi tolkar det som att det gör att kunden känner tilltro och får ett förtroende för leverantören. Det är ett dilemma för kunden när avtalen inte följs.

> *Ja, avtalen de är centrala. Så gör vi ju också så att jag är ju med i avtalsprocesserna också. Så jag säkerställer ju att vi är nöjda med de svar vi fått. De återspeglas i avtalen. Och sen följer jag upp efteråt att det återspeglas i implementeringen också. För många gånger tappar man på vägen där, man gör den första delen sen gör man inte två eller tre. (Informant 1, företag C)*

Det framkommer i vår studie att det inte finns några försäkringar för kundernas del utan att det är avtalet som gäller och om detta inte följs så finns det olika varianter på hur olika leverantörer kompenserar det.

> *Nä, den enda försäkringen man har är SLA, det finns ingen annan försäkring utan det är den avtalsformen som man skriver.(Informant 1, företag C)*

> *Om vi inte har den här tillgängligheten så kommer vi att bli ersättningsskyldiga till kunden. Och Microsofts molntjänster till skillnad mot många andra leverantörer erbjuder en monetär ersättning, det finns många molntjänster som säger att om inte den här tjänsten fungerar så får ni en månads gratisabonnemang efteråt eller får något extra. Vi har sagt att vi har monetär ersättning vilket vi tycker är starkare. (Informant 1, företag B)*

> *[…]Så får man en ersättning eller avgiftsreduktion eller något sådant. Men det är ju paragrafer i avtalet, det är ju inte försäkringar som jag ser som försäkringar. Utan det är ju prestation, motprestation. Jag brukar säga att det viktiga i ett avtal är inte att man skriver vad som ingår utan vad som inte ingår. (Informant 4, företag A)*

Däremot är det enligt en av våra intervjuobjekt möjligt för leverantörer att teckna olika former av försäkringar för tvister eller mot händelser som inte kan skrivas in i avtal, exempelvis naturkatastrofer.

Enligt litteraturgenomgången (rubrik 2.9) är det alltid kunden som bär det yttersta ansvaret för säkerheten samt integriteten av data som ingår i molntjänsten. Det är av stor betydelse för kunden att känna till det. Vid vår empiriska undersökning är det främst de informanter som är leverantörer som uppger att så är fallet. Vi menar att det är av stor betydelse att informera kunden om det.

> *Till syvende och sist är det kundens uppgift att se till att man följer de lagar och regler som finns och det tycker jag man ska vara tydlig med i sin kommunikation med kunden. Jag finns tillänglig att svara på alla möjliga frågor ni har men jag som leverantör kan inte stå till svars för de beslut som kunden tar. Till sist som jag sa innan, det är kundes ansvar att se till att man följer alla de lagar och regler som gäller där man driver sin verksamhet.(Informant 1, företag B)*

Enligt (rubrik 2.9) är det i första hand avtalslagen, köplagen och personuppgiftslagen som gäller för IT-rätt. Vilket lands lag som gäller vid tvist anser vi och våra intervjuade kunder fortfarande är otydligt. Därför är det av stor vikt att detta finns noggrant specificerat i avtalet mellan kund och leverantör.

> *Det kan jag inte svara på. Det är det som är det luriga när det gäller internationella avtal mellan företag i olika länder. Dom ska man inte låta vanligt folk skriva, utan det måste vara jurister som tittar på detta och avtalen så att det är synkat med lagstiftningen i båda länderna. […]Det är klart att är det ett företag man inte har hört talas om innan då kanske man hellre väljer en svensk.(Informant 3, företag A)*

> *Det beror på var vi har skrivit avtalet. Men normalt sett när vi skriver avtal så är det i Sverige. Men sen beror det ju på vem vi har skrivit avtal med. Så till exempel i vårt globala kommunikationsavtal som vi har med Orange. Där är det ju engelsk lag som gäller så det beror lite på vad det är för.. var den är skriven och hur den är skriven. Vi använder oss av en engelsk advokatfirma till väldigt många av våra avtal, men det är oftast Bacom Mcansy, men vi använder ju normalt sett svensk lag, också är det oftast skrivit i form av corporate så vi kan använda det till alla Alfa Laval bolag också. Vi brukar inte skriva några lokala avtal(Informant 1, företag C)*

Hur avtalen mellan kunden och leverantören ser ut varierar. För mindre företagskunder är avtalet SLA oftast färdigskrivit och utifrån det är det sedan upp till kunden att acceptera avtalet eller avstå och välja en annan leverantör. (rubrik 2.9) Större företagskunder har större möjlighet att förhandla fram ett mer specifikt avtal med specificeringar av vad som gäller om tvist skulle uppstå sinsemellan kund och leverantör. Vår studie visar att leverantörerna är mest angelägna om specificera tillgängligheten i avtalet, medan kunderna vill att många andra faktorer ska ingå såsom exempelvis en helhetsbedömning av leverantören.

Vid vår undersökning framkommer det från flera av informanterna att det tekniskt sett är möjligt att komma åt, modifiera samt radera kunders data. Vår undersökning pekar på att leverantören måste kunna radera information permanent om exempelvis en kund skulle avluta sitt konto. Med utgångspunkt från det juridiska perspektivet krävs dessutom, som vi ser det, att en leverantör kan ta fram data som fungerar som bevismaterial. Dock menar vi att de

seriösa och väletablerade leverantörerna värnar mycket om sitt varumärke, vilket vi hoppas kan vara en anledning för dem att inte missbruka sin möjlighet vad gäller att ha behörighet till kundens data. En av de leverantörer vi intervjuat uttryckte det som att de ser sig som postleverantörer, som levererar kartonger, som skyfflar postpaket från adress till adress. Vi ser det som att denna form av beskrivning avspeglar att innehållet i paketen det vill säga datan är ointressant för dem.

Vi uppfattar det som att det viktigaste för kundens del för att känna sig trygg med molntjänsten är att vara noggrann med att definiera alla överenskommelser vad avser säkerheten i SLA med leverantören så att det inte blir några missförstånd om det skulle uppstå oklarheter. Som det framkommer i vår undersökning är det även avgörande för säkerheten också att man som kund följer upp avtalet hela vägen till och med implementeringen av molntjänsten.

5 Sammanfattande diskussion

I kapitlet för vi en sammanfattande diskussion utifrån det vi kommit fram till i empiri- och analyskapitlet samt forskningsfrågan inklusive dess underfrågor. Syftet med studien var att identifiera kraven som kunder har på en molntjänst för att den skall anses som säker genom att svara på frågan: *Vilka säkerhetskrav behöver kunder ställa på molntjänster för att känna sig säkra?*

För att uppfylla syftet med studien samt besvara forskningsfrågan ovan har vi under studiens gång utgått från de tre perspektiven: informationssäkerhet, olika typer av molntjänster samt avtal och lagar som vi har haft fokus på i studien. Det är också de tre aspekter som är väsentliga för molntjänstleverantörer när det gäller säkerheten av molntjänster.

I vår studie har det framkommit att osäkerheten vad gäller molntjänster främst handlar om den förlorade fysiska samt personliga kontrollen av data. De risker som kunder ser med molntjänster och som också framkommer vid vår studie handlar främst om hur det praktiskt fungerar kring säkerheten när leverantören överför informationen till en ny plats. Hur övervakas den och vem eller vilka kommer att få tillgång till informationen. Vi ser det som att det i princip är samma faktorer som man behöver ta i beaktande vid outsourcingavtal. Utifrån dessa likheter tolkar vi det som att det främst är den mänskliga faktorn som utgör det största hotet mot att uppfylla de tre målen för informationssäkerhet såsom konfidentialitet, integritet samt tillgänglighet. Det är utifrån dessa risker som majoriteten av de krav kunder ställer på molntjänster utgår ifrån.

Vid vår studie har det framkommit att skillnaderna i säkerhet mellan de olika typerna av molntjänster beror på att arkitekturen av de respektive molntjänsterna är olika. Eftersom man i de privata molntjänsterna själv står för nätverk, processer, lagring och inte delar företagets data med en leverantör är således den privata molntjänsten betydligt säkrare än den publika typen. Vid införande av publika molntjänster behöver kunden vara extra observant på att leverantören håller kundens data avskild från övriga kunder, tar kontinuerlig backup samt gå igenom omständigheterna runt den fysiska säkerheten av data. När kunden väljer en leverantör bör den göra en heltäckande leverantörsbedömning och välja en väletablerad leverantör med anställda som är förtroendeingivande och kompetenta, eftersom den mänskliga faktorn utgör en stor risk. Kunden bör även tänka på att ha ett välskrivet SLA med leverantören. Valet av molntjänsttyp är således avgörande för molntjänstens säkerhet.

Vi uppfattar det som att det viktigaste för kundens del för att känna sig trygg med molntjänsten är att vara noggrann med att definiera alla överenskommelser vad avser säkerheten i SLA med leverantören så att det inte blir några missförstånd om det skulle uppstå oklarheter. Som det framkommer i vår undersökning är det även avgörande för säkerheten också att man som kund följer upp avtalet hela vägen till och med implementeringen av molntjänsten.

6 Slutsatser

Forskningsfrågan i vår studie har varit att ta reda på vilka krav kunder ställer på en molntjänst för att den generellt sätt skall anses som säker ur ett informationssäkerhetsperspektiv. Genom analysen av det empiriska materialet har vi kunnat identifiera de krav som kunder ställer på *privata* respektive *publika molntjänster* och sammanfattat dem i nedanstående kravlista. I Kravlistan redovisas dels de säkerhetskrav vi tagit till oss genom våra litteraturstudier dels de vi fått bekräftade i vår empiriska undersökning. I kravlistan specificeras inte kraven för de olika leveransmodellerna. De viktigaste kraven presenteras överst.

Publika molntjänster	Privata molntjänster

• Helhetsbedömning av leverantören
• Välspecificerat SLA med leverantören där det står:
  o var data lagras
  o vem som äger data
  o hur data transporteras
  o hur data återfås
• SLA med underleverantören
• Separera kunders data
• Åtkomstkontroll för samtliga systemadministratörer
• Tillgänglighet
• Kryptering
• Säkra användargränssnitt
• Starka lösenord
• Brandvägg
• Övervakning av intrångsförsök
• Backup
• Allt är redundant exempelvis elledningar och hårddiskar
• Antivirusprogram
• Mjukvaran är säkerhetsuppdaterad
• Loggning
	• Åtkomstkontroll inom organisationen
	• Behörighetskontroll
	• Tillgänglighet
	• Kryptering
	• Säkra användargränssnitt
	• Starka lösenord
	• Backup
	• Allt är redundant exempelvis elledningar och hårddiskar
	• Loggning

Tabell 6.1: Kravlista för säkra molntjänster

6.1 Publika molntjänster

De i särklass viktigaste säkerhetskraven som kunder har på publika molntjänster är dels att de har möjlighet att göra en *helhetsbedömning av leverantören* dels att det finns ett välspecificerat juridiskt avtal; *SLA* mellan kunden och leverantören. Det är mycket viktigt att tillgodose dessa krav för publika molntjänster då det är de största osäkerhetsfaktorerna för

kunder. I helhetsbedömningen innefattas att man i SLA vill ha specificerade krav på de anställda samt insyn i den övergripande informationssäkerheten hos leverantören. Kunder anser också att det är av stor vikt att gå igenom lokala referenser för att känna tillit och förtroende för leverantören. Hur det juridiska dokumentet *SLA* mellan kunden och leverantören är utformat samt dess innehåll är också avgörande faktorer för kundens trygghet. I detta bör specificeras om leverantören inte håller vad den lovar samt var data lagras, om det är kunden, leverantören eller an annan part som äger data, vilka säkerhets aspekter som finns när data transporteras samt hur möjligt det är att återfå data. Antingen bör kunden ha ett separat SLA med underleverantörer vara noga med att i avtalet specificera att underleverantörer inkluderas i SLA med den direkta leverantören.

Att *Separera kunders data* avser att man i molntjänster säkerställer att data i molntjänsten är skild från andra kunders data samt att den övervakas. *Åtkomstkontroll* för samtliga anställda det vill säga molntjänstens förmåga att stödja rollbaserad behörighetskontroll till systemet är också av stor vikt för att kunden skall känna sig trygg. Kravet på *tillgänglighet* avser att man vill veta hur leverantören upprätthåller tillgängligheten och vad man gör för att undvika olika former av nätverksattacker. *Säkra användargränssnitt* innebär att du som kund behöver skydda ditt lösenord som du använder för att logga in och få tillgång till molntjänsten. *Övervakning av intrångsförsök* innebär att du som kund vill ha kontroll över om leverantören använder övervakning och filtrering eller någon form av kontroller för att upptäcka olämpliga dataflöden. Ett annat krav som kunder ställer på molntjänster är *Backup* som då avser vad leverantören har för typ av backup, hur många backuper som finns samt vetskapen om ifall de täcker kundens aktuella behov. Andra funderingar för kunden vad gäller backupen är var data lagras externt och om leverantören har möjlighet att kryptera backup? Vi har också kommit fram till att det är av stor vikt för kunden att veta hur de lösenord leverantören använder ser ut samt vilka alternativ som finns.

6.2 Privata molntjänster

Den största skillnaden mellan en publik och en privat molntjänst är att kunden i en publik molntjänst inte har någon kontroll över data då den är placerad utanför den egna organisationen. Det betyder att det för privata molntjänster inte finns krav från kunden i form av helhetsbedömningen av leverantörerna samt att utformningen av avtalet mellan kund och leverantör inte är lika avgörande, eftersom data finns inom organisationen. Skillnaden i säkerhetskrav jämfört med en publik molntjänst är framförallt att man behöver ställa högre krav på *Åtkomstkontroll inom organisationen* samt *behörighetskontroll*, eftersom molntjänsten befinner sig inom den egna organisationen. Utöver dessa skillnader i krav som lyfts fram ovan är säkerhetsaspekterna för privata molntjänster likvärdiga med dem för publika molntjänster vad gäller krav såsom tillgänglighet, backup, intrångsförsök, kryptering, loggning och lösenord.

6.3 Slutord

Under arbetet med vår studie har vi funnit att om man som kund har en tillräckligt genomarbetad kravlista för de säkerhetskrav som molntjänsten skall uppfylla samt har kunskap och möjlighet att följa upp dessa krav hela vägen fram till implementeringen, har man goda förutsättningar för att implementeringen av en molntjänst skall bli säker. I kravlistan bör det som tidigare nämnts framförallt ingå parametrar såsom en helhetsbedömning av leverantören och eventuella underleverantörer samt krav på ett välgenomarbetat SLA som gör att kunden känner förtroende och tillit till leverantören. Molntjänster kan med rätt förutsättningar öka IT- investeringarnas affärsvärde för företagen och bli ännu mer attraktiva om man kan säkerställa molntjänsten för kunden.

Bilaga 1 Definition av begrepp

Molntjänster/Cloud Computing

Molntjänster innebär att system levereras över internet. Molntjänster underlättar för användare vad avser flexibiliteten att snabbt ha möjlighet att öka och minska sina resurser efter behov samtidigt som flera leverantörer kan dela på resurser i form av exempelvis hårdvara och databaser med andra kunder. Användarna betalar för exakt de resurser och den tid som man utnyttjar molntjänsten (Mather et al., 2009) (ENISA, 2009). Den svenska benämningen av det engelska begreppet Cloud Computing är molntjänster. I vår studie kommer vi främst att använda oss av den svenska benämningen. I de enstaka fall där sammanhanget Cloud Computing passar bättre använder vi det. Begreppen avser dock samma sak.

Åtkomstkontroll

Åtkomstkontroll, engelska Access Control förhindrar att obehöriga har åtkomst till data (Harauz et al., 2009), eftersom man kan styra hur och vilken information som användarna har tillgång till. Åtkomstkontroll kan ske genom att identiteten kontrolleras (autentisering) genom exempelvis lösenord när användaren loggar in i systemet. (Ambrose et al., 2010)

Virtualisering

En virtuell dator är en logisk representation av en dator, i en programvara, där den fysiska hårdvaran är frikopplad från operativsystemet. (IBM, 2007) Verksamheten har med andra ord ingen koppling till infrastrukturen som behövs för att köra tjänsten. (Srinivasamurthy & Liu, 2010) När begreppet används i uppsatsen avses att man gör hårdvarulagret virtuellt och att applikationen inte ska behöva bry sig om hårdvaran.

Autentisering

Med autentisering avses att man kan verifiera att ett meddelande kommer från rätt person och att det inte har modifierats av en utomstående på vägen mellan avsändare och mottagare. (Krawczyk et al., 1997)

Kryptering

Kryptering handlar om att det enbart är de med rättigheter till den aktuella informationen som skall få åtkomst till den. Kryptering åstadkoms med hjälp av någon form av algoritm som omvandlar läsbar information till oförståliga tecken. (Henriksson, 2000)

Konfidentialitet

Svenska Akademin definierar konfidentiell som; meddelad i förtroende, förtrolig, hemlig. (Svenska Akademiens ordlista över svenska språket, 1998) Med andra ord ska inte obehöriga användare se känslig information. (Gollmann, 2006) När begreppet används i uppsatsen avses att kundens information inte hamnar i händerna på obehöriga.

Integritet

Svenska Akademin definierar integritet som; orubbat tillstånd; okränkbarhet; oberoende. (Svenska Akademiens ordlista över svenska språket, 1998). När begreppet används i uppsatsen i anslutning till molntjänster avses att information inte ska förändras på vägen mellan leverantör och kund.

Tillgänglighet

Gollmann (2006) definierar tillgänglighet som att en tjänst ska vara tillgänglig och användbar på begäran av en behörig person till tjänsten. (Gollmann, 2006) När begreppet används i uppsatsen avses att molntjänsten måste vara åtkomlig för kunden och kunna användas.

Bilaga 2 Elektroniskt brev till potentiella informanter

Vi heter Linn Bjärvall och Martin Ståhl och läser sjätte och sista terminen på det systemvetenskapliga programmet vid Lunds universitet. Vi kommer att ägna resten av vårterminen åt att skriva vår kandidatuppsats på 15 HP inom vårt huvudämne som är informatik.

Vår uppsats kommer att behandla ämnesområdet **Cloud Computing och säkerhet** och målet med uppsatsen är att vi genom intervjuer med ett antal företag som har någon form av relation till Cloud Computing besvara vår forskningsfråga som är: *Vilka krav måste uppfyllas för säker användning av molntjänster?* Vi är intresserade av att veta vilka risker som företag ser med molntjänster. Vi har haft kontakt med Stefan Lindén (Malmö) som rekommenderade oss att ta kontakt med dig.

Vi undrar om det finns möjlighet att ställa några frågor till er i någon form av intervju? Vår tanke är att om ca två veckor genomföra en intervju. Vi skickar frågorna före intervjun. Vi kommer självklart att behandla alla uppgifter konfidentiellt.

Ser fram emot möjligheten att få intervjua er!

Med vänlig hälsning

Linn Bjärvall och Martin Ståhl

Bilaga 3 Intervjuguide till leverantörer

Inledande fråga

Vilken typ av leveransmodell för molntjänster levererar ni mest (PaaS, SaaS eller IaaS)?

Säkerhetsrisker med molntjänster
Beskriv de största skillnaderna mellan de tre leveransmodellerna Software as a Service (SaaS), Platform as a Service (PaaS) och Infrastructure as a Service (IaaS) med hänsyn till konfidentialitet, integritet och tillgänglighet?

Vilka anser ni vara de största riskerna med molntjänster?

Vilken är er definition av en privat molntjänst?

Vilka ser ni som de största riskerna med *privata molntjänster* på:

A) Nätverksnivå?
B) Host level?
C) Applikationsnivå?

Vilka ser ni som de största riskerna med *publika molntjänster* på:

A) Nätverksnivå
B) Host level
C) Applikationsnivå

Vilka ser ni som de största riskerna med *hybrida molntjänster*:

A) Nätverksnivå
B) Host level
C) Applikationsnivå

Hur minimerar ni de risker som finns i ovanstående typer av molntjänster?

Fysisk säkerhet
Hur har ni tagit hänsyn till den fysiska säkerheten? Exempelvis placering av server.

Finns det möjlighet för er att:

A. Se kunders data?
B. Radera kunders data?
C. Modifiera kunders data?

Vad har ni för typ av säkerhetskontroller för era anställda innan anställning?

Kan ni spåra vilken anställd som gjort något med kunders data?

Hur utförs spårningen?

Lagar och andra avtal mellan kunder och leverantörer av molntjänster
Vilket lands lagar är det som gäller vid en tvist (leverantörens, kundens eller det land där data befinner sig)?

Service Level Agreement (SLA)

A. Har ni ett eget SLA?
B. Vilka uppgifter i kontraktet anser ni är viktigast för att garantera säkerheten i en molntjänst för kunden?
C. Finns det angivet i SLA vem som äger informationen?
D. Finns det angivet i SLA hur informationen skall hanteras och vem som har rätt att hantera den?
E. Finns det angivet i SLA hur informationen övervakas?

F. Finns det angivet i SLA hur stor tillgänglighet kunden har till sin information?

Bilaga 4 Transkribering, Informant 1, Företag A

A= Informant 1

L= Linn Bjärvall

M= Martin Ståhl

L: Om vi skulle ta lite om vår bakgrund lite kort. Martin och jag går ju det systemvetenskapliga kandidatprogrammet. Som avlutande moment gör vi kandidatuppsatsen. Det fanns ett intresse hos båda två att fördjupa sig i molntjänster och då såg vi ganska snabbt när vi började studera ämnet att det fanns många frågetecken just runt säkerheten så vi tänkte om du bara skulle vilja berätta lite kort om ditt företag.

A: Min roll här just nu. När jag var på Ericsson var detta en... man gjorde en förutsättning för ett nätverk för molntjänster och där var det att ge det mobila paketdatanätverket.. för att ge förutsättningar till att utveckla molntjänster av alla de slag, att man kan ta med sig… alltså en del av molntjänsterna är just att du skall kunna arbeta var du vill.

M: Så då kan man klassificera det som en Platform as a service?

A: Ja det skulle man kunna säga att det är… på en kanske ännu djupare nivå än Platform as a Service eller…

L: Infrastructure då?

A: Ja, just det, Infrastructure as a service

M: Man brukar ju klassificera dem i tre….

A: Ja, plattform är ju det där man ersätter en form av serverhall..

M: Precis

A: Och sen tror jag att användningsområdet för mobila tjänster det blir väl mest ..om man säger..den högsta nivån, vänta vad heter den, vad kallas den…. ?

L: Software as a service

A: Software as a service just det precis, det är ju oftast där det kommer till användning då..

L: Nu skall vi se… Vilken typ av leveransmodell levererar ni mest då?

A: Man skulle ju kunna säga som så att vi gör en fiktiv verklighet… Där man på något vis säger att vi på företag A här …molntjänster är ju nåt som det pratas jättemycket om…. BI - lösningar skulle man ju typiskt sätt kunna leverera… som då tänker jag mig mest som… Software as a Service, ett paket, där företag A skulle hantera… stå för både data och applikation. Och då skulle man ju kunna prata om säkerhet och sådana integritetsaspekter och sådant kring detta. Det finns ju som jag ser det flera dimensioner på säkerhetsaspekten, dels en fysisk säkerhet.. att de finns lokaliserade i vår serverhall så att det är vi som arbetar här som har en direkt kontakt med deras data för det är kanske människor som är på besök här eller vad som helst och …det är såna aspekter och då får man ju ta in den aspekten och diskutera sådana frågor… om vi skulle leverera en sån här tjänst så är det ju också ganska troligt att vi i gengäld köper en Platform as a Service eller Infrastructure as a Service från något annat ställe så att vi köper en Infrastructure as a Service från ett tredjepartsbolag, som sen köper en Platsform as a Service hos någon annan så hamnar den någonstans..så jag tror att som slutanvändare så har du nog väldigt dålig koll

egentligen på var din data finns och vem som kan komma åt den och vilka avtal som finns då bland annat så… så det ser jag nog som en jättegrej att du kan inte förlita dig… Var det inte Amazon nu som… hade någontjänst?

M: Och likadant Playstation, deras konton blev ju hackade… på flera tusentals filer.

A: Det är ju en jättegrej… Samtidigt är det ju en jättestor trend… det är ingen som vill spara allting på sin egen dator lokalt eller... allting skall finnas på din dator för den är beroende av… eller utan man vill ju ha allting globalt öppet.

M: Så hur ser du då på, integritet, konfidentialitet och tillgänglighet när man jämför?

A: Jag skulle vilja prata mycket… jag är ju faktiskt rätt mycket för… att det skall vara. Jo förresten jag kom faktiskt på en sak jag... att vi var med i en föräldrakooperativ förskola när vi bodde i Göteborg och då var det ju som så här att det finns ju telefonnummer och adresslistor sånt som blir huller om buller väldigt snabbt, ingen som har den aktuella adresslistan… så därför tänkte jag att det här måste man göra något … så jag var ju tvungen att göra nåt åt… så det var jätteskoj faktiskt… också satte jag upp det. Jamen tänkte jag.. att då gör man nån form av webbsida, ganska tråkig, helt statisk, men ändå .

L: Ja, vad kul!

A: Där man kunde läsa information både internt och externt och man berättar om vad som är speciellt med vår förskola, vad vi tycker och tänker och då tänkte jag att då kan man ju göra ett litet enkelt databassystem där, ja så då satte jag upp ett sånt där CRM system och så använde jag Joomla också lite tilläggskomponenter, det finns ju ganska mycket färdigt, men det man behövde göra var ju att sy ihop allt så det blir ett koncept av det sen gjorde jag även en databasintegration där så att man, när man loggade in på sidan ..så kunde man även klicka på redigera mina barn och mina kontaktuppgifter så kunde man då skriva ut snygga adresslistor, telefonlistor och barngruppslistor sorterat efter ålder eller… allt sånt där som och då fick vi… enision(?)… och då var ju all data om barnens personuppgifter och sånt ..var ju då i händerna, det låg ju liksom uppladdat på vårt webbhotell och det fick jag ju lobba lite för …för att det skulle vara acceptans på detta och där vi bodde var det många föräldrar som hade mycket tankar om detta med integritet och det var lite viktigt för många av dem. Det är väl ofta så att man inte vill att ens barn… eller det går väl och förstå och då fick man ju ställa frågan vad är viktigt? För oavsett hur du än vänder och vrider på det så finns det ju ingenting som är hundraprocentigt säkert. Och inte ens och ha det lokalt i datorn på förskolan som är uppkopplat mot internet… det är ju inte heller hundraprocentigt det är ju långt mycket jobbigare att försöka få ut den datan där, än att hacka sig in på webbsidan, men man måste ju lösa den balansen. Så får man ställa de här intressena mot varandra. Så egentligen svaret på min fråga är att man måste lösa detta genom att ha den här balansen. Jag står ju för att informationen skall vara fri och tillgänglig i någon enkel variant av Googles versioner.

L, M:& A [småskrattar]

A: Så får du ta det här att de här uppgifterna inte är i superhemligt förvar.

L & M: Nej, det är klart.

M: Sen får man ju också se det som att viss information är ju kanske mer intressant för vissa personer än andra om någon i USA skulle be om er telefonlista så kanske det inte är så jätteintressant…

A: Nej, precis de argumenten använder jag ju mycket, hur stort intressevärde har informationen, på den här adress- och telefonnummerdatabasen - hur högt är det då? Hur motiverat är det för någon at försöka komma åt det?

L: Jag det är klart, det blir det man får titta på

A: Jag tror också en sak är… hur mycket skyltar man med saker och ting, men det tror jag också är viktigt. Från den sidan fanns det ju en inte inloggningsruta, men frånsett så fanns det ju ingen extern information som visade att här finns det adressuppgifter personuppgifter . Så det vi fick göra någon form av avtal, där man fick godkänna

att ens adressuppgifter och personuppgifter finns med i denna och där fick vi också vara med om det klassiska när man skall publicera bilder på barn… Det är en lång väg faktiskt att gå… även om det inte är så svårt så skall det …man måste ha tillstånd från varje förälder eller kan man argumentera genom att det inte går att identifiera barnen enskilt.. men då löste vi det här genom att vara väldigt tydliga och då ha den här diskussionen med hela föräldragruppen med att vad är värdet för oss med att kunna ha det publikt…

L: Tillgängligt

A: Alternativet är ju sådana här adresslistor som hänger i hallen på förskolan.. å andra sidan den där fysiskt där igen… vem..om allting finns i en pärm i hallen, då kan ju en hantverkare lika väl ta med sig den, alla IT relaterade spörsmål… det är ju inte helt…. det är ju inte alltid som problemet ligger i själva IT - lösningen… utan det finns ju ändå…

L: Men en viss typ av kategorier tycks tro… det

A: Men där levererade ju jag en software as a service.

M: Så vad skulle du se som de största riskerna med molntjänster rent generellt?

A: Ja, jag ser nog just detta att du inte vet var de finns… Eller just i själva definitionen att det är moln, att som i definitionen av molntjänster ingår ju på något sätt att du inte är intresserad av var det andra är någonstans. Och per definitionen så har man ju byggt in den där problematiken tycker jag att man inte vet vilka säkerhetsaspekterna är eller vilka avtal som finns mellan leverantörerna och just att saker och ting ändras och det är ingenting som är konstant eller att vissa bolag har avtal med varandra och vissa dagar är det outsourcat till någon helt annanstans också har de… så att problemet är att saker som har högt…saker som du inte vill att någon annan skall få del av ser jag som svårt att..liksom hantera och det är ju samma om du har ett e - mail konto också hur… ja hur… ja

L: Nej, men det är ju lite som du sa att det finns ju en risk med det mesta.

A: Å andra sidan… oavsett om du har en Exchange konto på jobbet och det är ju också en svårighet att hur mycket får min chef läsa min e- post och hur mycket får… men det är mycket som är relaterat till hela mailen… eller… avsett om man har Exchange mailen som ligger som en molntjänst hos Microsoft eller om den ligger sparat i en dator här det är lite samma sak där… men oavsett om den ligger i en dator här, vem har rätt se den och vilka?

M: Och det är ju ändå så också att mailet skickas ju trots allt runt hela världen även om du bara skickar från ett ställe till ett ställe som är mitt framför dig!

A: Ja och vem kan då sniffa den trafiken och det vet man ju att vi kan ju per definition inte kryptera mail och vem som helst som har kört Wireshark kan ju se att det är ganska enkelt och… ju… vi var hemma hos några kompisar också visade jag om man skickar det här mailet… och satte upp Wireshark bara på min dator och så kom ju det där paketet där…

A: Och det är väl också en sådan sak man inte heller tänker på … vilka alla molntjänsterna är och ..apropå den här förskolan så var det så vid det tillfället jag gjorde detta…så var inte trafiken… detta så hade jag ingen SSL kryptering på trafiken heller och det var ju också en sak jag sa att det kan man ju faktiskt köpa till..och bygga in eller att man SSL säkrar. Och det var just att då var det ju faktiskt möjligt att avlyssna trafiken på vägen och det är ju också en säkerhetsaspekt faktiskt, man kanske inte tänker på heller .att … jag tror inte man…att ..om man har ett vanligt mailkonto så är det ju inte alla webbmailklienter som har SSL ..täckning

M: Nej, de flesta har nog inte det.

A: Vissa har det men långt ifrån alla… så det är också en sådan där säkerhetsissue ..vad man tycker.. jag tycker ju per definition..för…jag tycker det är viktigare att informationen finns att den är tillgänglig än att den är hundraprocentigt säker.

M: Det är ju också avvägningen, att om du höjer t ex konfidentialiteten och integriteten extremt högt så kanske tillgängligheten sjunker väldigt mycket och då spelar det ingen roll hur starkt kryptrad den är om du inte kan använda tjänsten.

A: Nej, och sen så vilka delar är krypterade och inte och på vilket sätt? Om vi pratar säkerhetsmässigt så vill jag berätta om när vi bygger det där mobila nätverket för operatörerna så har de enormt olika krav på vad de vill se i kundernas trafikflöden. I Sverige djupanalyseras ungefär fem procent av trafik, djupanalyseras då är det.. då är det så att man tittar på protokollspecifikationen ..vad är det för HTTP eller POP? eller olika? Är det någon form av streamtjänst. Ni vet om man köper Telia och köper en Spotifyprenumeration via Telia så skall du ju inte betala datatrafik för den. Oavsett din abonnemangsform så betalar du ju inte per Megabite som du lyssnar på Spotify och det måste ju lösas tekniskt på något sätt och då tittar man mycket vad det är för protokoll och om det är ett visst så slår det mot djupare och djupare regler som det är som en hierarki då och de här reglerna är ju inte officiella ..exakt vad de tittar på det är ju bara för att ha det själv som de vet de och som de sätter upp det men då har jag ju sett rätt många sådana konfigurationer från olika ..så jag vet ju ungefär vad man brukar tittar på och då är det ju i slutändan fem procent av trafiken som djupanalyseras och då kan de ju i princip analyseras hur långt som helst och då går man ner på paket nivå och tittar på vad som skickas och är det inte krypterat så är det mycket enkelt även där att se och då loggas en del och sen spottas det ut i en databas precis vad som har hänt.

L: Ok

A: Och det skall man ju veta att vad du surfar med mot e-mail där finns ingenting..som man inte kan veta… Som du inte kan se och den är ju så otroligt knuten.. för i de här paketen som skickas så bygger det på själva ..man gör en extension på paketet där du bygger in din identifierare ,ditt nummer på ditt SIM kort, så du skall kunna faktureras på rätt sätt och ibland skickas telefonnumret också med…

L: Ja ha

A: Även land är olika och då kan också ditt telefonnummer skickas med i de här datatrafikpaketen så det är jätteenkelt att se, här är det inte så farligt, men jämför du i Kina är det tvärtom till exempel så är det nog, 70 - 80 % av trafiken som djupanalyseras.

M: Så hur tror du man kan minimera de här riskerna? ..Vi har ju pratat lite om då kryptering…

A: Javisst, kryptering gör det ju genast mycket svårare…

M: Sen är det ju placering av servrar…

A: Ja absolut,

M: Underleverantör till leverantör…

A: Använder du mobilt och du kan lista ut att den här tjänsten ..och man kan lista ut vilken teleoperatör de använder för detta… man kan lista ut…mycket är ganska enkelt att ta reda på, så har du då information med känsliga uppgifter och som även till synes ..att du har ett bra avtal med din leverantör…sen vet man inte riktigt så som jag ser det är risken är allt som finns runtomkring och som man inte tänker på och typiskt är nog hur är kommunikationen mellan internetoperatörer och som är typiskt med molntjänster och som man inte snackar så mycket om.

L: Tycker du att det har tillkommit några nya risker som har tillkommit i samband med molntjänster jämför med outsourcing om man tittar på infrastrukturen?

A: Ja, jämfört med outsourcing… det är ju en form av outsourcing…

L: Förutom att man kan skala upp och ner… och flytta mellan

A: Ja oavsett om du… Jag ramlar nog tillbaka här mycket.. att om man ..du sätter upp ett avtal, men du vet väldigt lite om avtalet och vad och hur det avtalet vidare ser ut, vidare eller vilka i avtalet som binder olika och vad har de för agreements sinsemellan sig för en sak är ju att din leverantör lovar någonting gentemot dig och sen om de inte säkert och sen är det ju inte säkert att de lovar samma sak till deras underleverantörer. Sen kan man ju också säga att en kritik mot molntjänster.. man blir så beroende av andra faktorer..det kan bli väldigt enkla och fåniga misstag som kan få väldigt stora konsekvenser och då kan det ju bli att du lägger ut affärskritiska system som molntjänster och då måste man ju ta det i beaktning också, det där med tillgängligheten.. du ökar ju tillgängligheten men samtidigt blir ju din tillgänglighet ganska sårbar….och återigen vilka avtal har du och vilka garantier har du för upptid hos din internetleverantör? Den i sin tur…

M: Så vad tror du, tror du att din leverantör kan se kundens data, radera den och modifiera den även om det nu är otillåtet?

A: Ja, det tror jag absolut

M: För då gäller det ju att ha ett strakt förtroende för sin leverantör.

A: Ja precis… Oavsett om det är en stark leverantör jag tror att på nåt sätt så man föra en diskussion kring detta, att det här är inte helt okomplicerat, att vi värdesätter att ha det i en molntjänst för att det blir tillgängligt och bra för oss eller vi blir utspridda i flera länder eller det är värdefullt för oss men att så här och så här ser avtalen ut… men på nåt sätt att du inte förlitar dig på allt , utan att man måste ha en sån här dialog. Jag tror att i takt med att det här med molntjänster blir större så kommer man hitta lösningar och lev kommer också hitta roller gentemot varandra ..för det är ju jättesmart att man… Om man kan ha datacenter på Island, det är ju riktigt bra…..

L: Javisst det är klart, har du funderat på hur du definierar en privat molntjänst?

A: Jag använder en privat molntjänst för kontakter och kalenderhändelser så använder jag den här…jag använder Mobile Me… från Apple.

M: Men hur definierar du skillnaden mellan till exempel en privat molntjänst och en publik molntjänst?

A: Privat är ju att den… ja det är ju egentligen att jag måste ha inloggningsuppgifter till min…till det som jag har sparat…på min privata molntjänst…är det inte så?...jag har inte riktigt satt mig in i någon vidare definitionen av det, utan jag ser det som alltså publik molntjänst är ju saker som jag väljer att spara som är publikt, som är åtkomståtkomligt, så att Mobile Me är för mig en privat molntjänst, eftersom …jag inte har del av någon annans data och andra sidan så kan man ju säga att det är det är en publik molntjänst, för att det vänder sig till en allmänhet eller att det är publikt på det sättet.

L: Nej för det är ganska olika, hur man definierar det…för när vi pratade med företag B så sa han..så vi har gjort det som en tilläggsfråga för vi satt mycket själva och diskuterade…

A: Det kan jag tänka mig… hur man definierar, vad säger man där?

M: Ja. Alltså Företag B… Det är egentligen bara nya begrepp på gamla saker och det är just därför det är så svårt att definiera, för folk har kanske använt det förut, men de är inte medvetna om det så man kan säga att en publik molntjänst, det är ju där servrarna… informationen kan befinna sig varsomhelst i hela världen i princip… medan en privat molntjänst är mer likt ett lokalt nätverk så att alla servrarna befinner sig inom företaget men det som gör det till en molntjänst det är att…istället för att du kör det med ett ett till ett förhållande där du har en server med Officepaketet som går till en klient så har du flera servrar som kan innehålla olika former av applikationer som kan flyttas mellan dessa servrarna så om t ex servern bredvid skulle lägga ner så tar den andra över.

A: Ja ha men den definitionen har jag faktiskt hört när jag hör den att man ser att den är lokalt här… Ja precis… så kan man ju säga att vi har ju privata molntjänster här också sånt som… vi använder…

M: Men det är det att man kanske inte använder just begreppet molntjänster man säger bara att vi kör…

A: Nej man kanske säger att vi har… gemensamma filservrar… [småskrattar]

M: Tekniken har ju funnits längre än begreppet…

A: Ja men det tror jag är rätt… så tror jag är en mer korrekt definition av publikt moln och privat moln. Man kan ju säga att man har en filserver hemma och en applikationsserver också har man ett privat moln som man sparar på gemensamma konton eller en egen, en AD, det är ju också.

L: Det är mest ett hypat namn… folk blir mer nyfikna på det…[småskratt]. Också har vi några frågor, vilka ser ni som de största riskerna om vi tittar på de privata molntjänsten också brukar man dela in infrastruktren av molntjänster i network level, host level, och applikationsnivå och det är där som säkerheten kan komma ifråga. Och vilka tycker du då är de största riskerna på då host level hur skyddar man der och?

A: Ja jag ser det lite som att när man har privata moln så… jag tänker mycket på dels här och hemma så sparar vi på en filserver och där förlitar jag mig på att det ordnar sig så även om man pratar om host level så förlitar jag mig på..mer än så vet jag inte riktigt, hemma så sparar jag också på en filserver för oavsett dator så har jag ju tillgång till samma musik… och dokument .eller men den står ju å andra sidan på och är mottaglig dygnet runt så den är ju mottaglig för diverse attacker och på det sättet är det är ju också en ökad risk och det tycker jag också man skall tänka på just detta - hur hanteras den data man lägger där?

L: Access menar du?

A: Access och Backup och lite som i Örebro, ibland stänger de ju ner det här datacentrat för att de skall göra underhåll….och vad händer om… och vem äger informationen? Man kan ju också säga att man har ett filformat om man skall dra den här ett steg till …men för den gamla worddokumentstandarden.doc man vet ju ganska mycket om hur den ser ut men det finns ingen officiell definition för hur ett worddokument är eller hur ett worddokument ser ut ser ut och därmed kan man ju faktiskt ifrågasätta vem som äger den informationen i detta och det är faktiskt bara med Microsoftverktyg man kan extrahera den information man matat in i detta och det blir än mer så när man tittar på applikationerna och datanivåer…hur..man matar in något och men vad krävs för verktyg och säg att de går i konkurs till exempel att…eller om man skulle bli ovänner på nåt sätt eller avtal som man inte har något att säga till om…fighter mellan Oracle och Microsoft…. Det kan ju vara en typ databas som det inte finns support till. Datan kanske ligger i ett format som…

L: Nej, då är det viktigt vad man har skrivit..Tror du att det är någon skillnad om man jämför privata och publika och hybrida på de här tre nivåerna?

A: Jag tror att privata är enklare på det sättet att man har mer kontroll över trafikbiten, att det inte är publikt, då får man ju hela nätverksbiten med dig då som man ska nog veta att man inte har koll över. Man tänker nog inte på det så mycket i slutändan liksom vad man skickar och inte skickar ..å andra sidan skall man väl tänka på det… I en privat molntjänst tror jag att det blir lite mer avslappnat…att man inte behöver tänka på det lika mycket. Men det är klart att det mesta är ju på ett eller annat sätt knutet till Internet ändå så det räcker att man installerar någon form av programvara på en dator innanför nätverket som har kontakt externt så kan du ju sniffa på….

L: Och på host level får man kolla upp de här sakerna som, det har vi lite varit inne på…

A: Ja, vem sitter där och vilken dator det är också vilka fysiska datorer finns det och ligger på och vem supportar dem och vilka avtal har de sinsemellan det är ganska mycket som leverantör vill man ju veta och få statisktik över hur dina prylar används och det ingår ofta i avtalet att det är en förutsättning ofta för att få en viss typ av tjänst eller hårdvara och hur ser det ut även om den inte är hemlig för leverantören?

L: Nävisst!

M: Vet du om det utförs några säkerhetskontroller av de anställda som arbetar här på…och tycker du det är viktigt och hur bör de utföras?

A: För det första… det vet jag inte..visst är det så att när jag sparar i en publik molntjänst eller i en privat molntjänst här och jag vet ju att de som jobbar här har tillgång till det….och jag vet ju inte…det är trettonhundra anställda..

M: Men får de de skriva på ett separat avtal….och godkänna så de inte läcker det vidare..?

A: Ja det har vi, vi har ju ett generellt sekretessavtal har vi, och där vi som konsulter dels att det är saker vi sparar här och saker man gör hos kund men det är ju så generellt… det ligger jättemycket i detta , vilka möjligheter det släpper in…man måste jobba jättemycket med förtroende ..det blir så komplicerat om man skall skriva på papper för att komma åt detta och detta och detta… det blir ju lite fel… mycket är oftast inte så hemligt… men visst vem som helst kan läsa det jag gör..

M: Men vet du om man kan spåra det i så fall ..om någon skulle exempelvis modifiera en kunds data?

A: Ja, men det är inte alltid så enkelt att spåra faktiskt. En sak som är vanlig i sådana här kontorsmiljöer - IT miljöer är väl att man lämnar din dator fysiskt också har du inte låst den också blir det väldigt enkelt för någon att skicka ett mail i ditt namn eller öppna eller spara word i ditt namn…

M: Eller väljer dåliga lösenord...?

A: Ja precis så att det är ju också en sak när det gäller säkerhet och det mesta är ju lösenord och användarnamn och då tror jag också att det räcker ganska långt om man använder lösenord i kombination med något unikt för dig och sen vad det nu må vara för att på nåt sätt bara för att ha en till…det kan ju vara så enkelt så fingeravtryck eller skulle det också kunna vara en fråga för att… nånting mer, men det ser man inte så ofta, men det har man ju inte så mycket, det är ju väldigt sällan men det kanske vi kommer se mer av…

M: Jo, det är det ju. Så med andra ord är det svårt att spåra vem som har gjort något?

A: Ja det kan jag säga att det generellt sätt är svårt att spåra. Men såklart att man kan spåra men då kommer man in och trampar på detta med integritetsfrågor..och sånt också och hur mycket man kan begära

L: Så man kan spåra det till en dator men man kan inte se vem det var…

A: Ja det är ganska enkelt ..att se vilken dator som har haft vilken IP adress och vid vilket tillfälle det är ju ganska enkelt att göra… men sen..vem var påloggad? Vem satt vid den? Då kommer man ju verkligen in på en sådan integritetsfråga, hur mycket är det värt och hur mycket kränkande att söka på det sättet…det är ju mer kränkande ofta …då har man ju en anklagande….Generellt det är nog svårt att spåra.

M: Så vet du vems lagar det är som gäller vid en molntjänst?

A: Nej, det vet man ju inte heller…

M: Nej…Så om du har en leverantör i USA? Är det en amerikansk lag, svensk lag eller där din data befinner sig?

A: Jag tror att det är ganska otydligt… menar jag..som våran företag A:s privata molntjänst applikationsserver i Örebro, den tror jag ..borde ju omfattas av svensk lag, men min privata Mobile Me borde ju omfattas av amerikansk lag, men anpassad eftersom jag köper ju tjänsten och använder den i Sverige och ingen aning… om jag skall vara helt ärlig…om man lagt in ett konto och…använder jag någon form av webbhotell som ligger i nåt annat land så….

L: Det är ju lätt när det är inom Sverige… så fort det blir… utanför...

A: Det är nog många vanliga webbhotell som man använder som inte har servrar i Sverige..Ett jättestort är ju One.com och de har ju servrar i Danmark.

M: Leverantören kan ju vara svensk fast de har servrarna i ett annat land…och är det då i det landet där servrarna är eller….är det svensk lag?

A: Ja precis, det är svårt, men just hur lagar och förordningar och regler och sånt det tror jag inte man tänker på och det är ju klart, det kan ju vara jätteviktigt för hur stora rättigheter någon stat eller myndighet eller… för att utöva kontroll över det de sparat i exempelvis syfte att leta efter terrormisstänkta….

L: Men efter att ha förkovrat oss i detta har vi kommit fram till att man använder sig av SLA och att det är det enda juridiska dokumentet man använder vid molntjänster, har ni något sådant som ni skriver ned …?

A: PÅ företag A här så känner jag inte till…Jag skulle tro att företag A har det mot sitt eget kundcenter, att vi har någon form av SLA, där det skall vara t ex 90 nånting % tillgänglighet, men jag som slutanvändare har inte sett det avtalet och det är inget som är kommunicerat utåt.

L: Nej…

A: Som leverantör, jag tänker på den där förskolan som vi gjorde, så gjorde vi ju i gruppen och pratade om tillgängligheten i och sedan så vet vi ju det beroende på vår webbhotell/Webbhosting vad som stod i vårt avtal med dem, det kanske inte var så tydligt….det är inte så lätt att definiera vad som är tillgängligt och vad det är för definition på tillgänglighet…det är lätt att fastna i definitionen, den kan lätt falla mellan stolarna och att ordsdefinitionen kan vara väldigt olika beroende på vilken sida av bordet man sitter.

L: Ja verkligen… Så om du tänker på avtalet utifrån att vara leverantör, vilka uppgifter i kontraktet skulle du vilja ha med för att garantera säkerheten?

A: Ja… då skulle jag nog gärna vilja ha med ganska tydligt på vilka leverantörer man använder man sig av för att leverera den här tjänsten… på nåt sätt få nån form av total – även med underleverantörer så att… jag levererar detta och då tar jag hjälp av detta och detta ..det tror jag att man väldigt ogärna gör men på nåt sätt skulle jag nog gärna vilja ha det om jag skulle köpt… om jag skulle knyta ihop en sån här molntjänstaffär så skulle jag försöka få till så att mina användare skulle få en så stor bild som möjligt av hur den här faktiskt löses och då kan man ju faktiskt känna sig lite tryggare och då kan man ju också argumentera för att det skall vara på ett visst sätt, t ex datacenter på Island eller att man på nåt sätt kan bygga på argumentationsbasen så man tydliggör… Man får ställa detta mot att detta får vi och

L: Ja, det är ju viktigt, Skulle du vilja att det stod angivet vem som använder informationen?

A: Ja det skulle jag också vilja, men det tror jag inte det gör… en det är väl det med Googlekritiker också vem hostar Google , vem äger informationen och hur mycket?

M: Bör det stå med om informationen övervakas eller tror du att det står med?

A: Ja… Jag tror att man skriver väldigt enkla och generella saker att man oftast skriver att den är backupad eller att man faller på definitionen att man skriver hur den sköts eller hur den övervakas och att den har 98 % tillgänglighet, men det jag inte tror man definierar är vad orden innebär och vem som hanterar den?

L: Stort stort tack för att du tog dig tid!

A: Tack själva, det var bara kul!

Bilaga 5 Transkribering, Informant 1, Företag B

ML = Informant 1

M = Martin Ståhl

L = Linn Bjärvall

M: Vi läser sista terminen på det systemvetenskapliga programmet och skriver kandidatuppsats om säkerhet kring molntjänster. Vi skickade över vår intervjuguide för leverantörer till dig. Har du hunnit titta på den?

ML: Jajjamän

M & L: Jättebra

M: Du kanske kan börja med att berätta lite kort om dig själv och din befattning

ML: Jag heter informant 1 och jobbar som Företag B:s säkerhetsrådgivare i Sverige och min amerikanska titel är chief security advisor

L: OK

ML: och handlar då om att rådge våra kunder under säkerhetsfrågor och innefattar faktiskt alla företag B:s produkter och tjänster så det är en ganska bred tjänst då. Men det som väldigt aktuellt just nu och som jag spenderar merparten av tid med är säkerhetsfrågorna runt molntjänster, eftersom den största blocken eller hindret för att prata svenska att ingå i någon form utav molntjänst oavsett leverantör, den första frågan som dyker upp i 88% av fallen är ju säkerhetsfrågan så jag och våran jurist pratar väldigt mycket med våra kunder med internutbildning inom företag B naturligtvis hur man tar dom är olika säkerhetsdiskussionerna med kunderna.

M & L: Intressant!

M: Det finns olika typer av leveransmodeller som vi även har fått ut av teorin, PaaS, SaaS och IaaS. Vilken av dem är det ni levererar mest, eller levererar ni lika mycket av alla?

ML: Ja. Det blir det eftersom vi är så pass stort företag och satsat på det vi gör. Platform as a Service skulle man kunna mappa det mot vår tjänst som heter Azure, om ni har hört talas om den.

M & L: Ja!

ML: och Software as a Service skulle man kunna mappa mot våran Office 365 tjänst eller the BPOS, business productivity online services och nu då finns också beta på Office 365 och den är också vår mail, sharepoint, lync som vi provade men inte riktigt nådde ändra fram till då [småskratt], online appen då. Infrastructure as a Service, ja där har vi kanske ingen full lösning i det då, vi har en vissa privata partnermolnleverantörer som vi säkert pratar mer om när vi börjar prata om hybridmoln. Azure i en viss del kan man säga är en infrastruktur också beroende på vart man drar gränsen mellan plattform och intrastructure. Så vi verkar nog främst i PaaS och SaaS då om man får säga så.

M: Utifrån teorin har vi kommit fram till att de tre största riskerna är konfidentialitet, integritet och tillgänglighet för kunden. Det vi undrar är ifall det finns några skillnader mellan PaaS, SaaS och IaaS sett till konfidentialitet, integritet och tillgänglighet. Skiljer det sig något säkerhetsmässigt?

ML: De är ju de tre slagdängerna när det gäller säkerhet generellt. Vad är det som är viktigt? Du klarar dig inte med två av tre, och du klarar dig inte med en av tre. Om man ska hårddra det kan man säga så här, om du har jättebra konfidentialitet och jättebra integritet men noll tillgänglighet skulle ingen använda tjänsten för att de skulle inte kunna komma åt den. Den är ju ganska viktig, för det funkar inte annars. Har du en tjänst som är jättetillgänglig men konfidentialiteten är låg får du kanske ett lägre förtroende för tjänsten men det kan ändå innebära att folk väljer att använda den. Det beror ju lite på vilken sorts risk och vilken sorts data. Integriteten är en stor del av hur vi som leverantörer hanterar kunders data och vilka säkerhetmekanismer vi har stoppat in för att se till att inte någon data kan läcka ut eller hamna i orätta händer. De är ju också olika beroende på om vi titta

på en molntjänst för privatpersoner eller en molntjänst för företag. Jag menar att folk slänger ut hela sitt liv på facebook men man vill inte att vissa andra saker ska komma ut över huvud taget och det kan ibland bli lite motstridigt.

L: Det är klart

M: Du nämnde att ni försöker minimera riskerna. Vad gör ni för att minimera riskerna för de här tre?

ML: Nu kommer den här diskussionen spreta lite beroende på vilken molntjänst vi pratar om tillexempel om Bing som är vår sökmotor, om vi pratar om Live Messenger, det är som hette MSN förut som är en chattjänst eller om vi pratar Office 365 eller Azure. Kör du med en SaaS-modell ansvarar Microsoft för hela stacken, om man får använda uttrycket. Egentligen bara kunden som skickar mail eller använder Sharepoint och laddar upp dokument. Vi ansvarar ju för att alltig ska funka till ända upp till den nivån att… ja kunden startar bara sen egen dator eller sin applikation. Vid en plattformtjänst så ansvarar kunden för att applikationer skrivs rätt och vi måste hantera det och där kan man göra alla möjliga konstiga saker men säkerhetsarbetet är med alla olika nivåer. Kunna segmentera kundernas data så att det inte kan läcka ut någon information, se till att alla som är anställda har rätt behörighet och inte har behörighet där de inte ska ha behörighet. Vi går ju inte på de här frågorna lite senare i ert dokument ser jag.

L: Vilka ser ni som de största riskerna om man tittar på de privata molntjänsterna om man tittar på de olika nivåerna som vi också fått fram genom teori. Om vi börjar med de privata molntjänsterna på nätverksnivån eller network level?

ML: Kan vi bara försöka vara överens om så att jag är med på samma sida vad ni menar med ett privat moln. Vad är er definition av det så att jag förstår rätt?

L: Vi har uppfattat det som att man har det internt inom verksamheten. Men vi är inte helt säkra på om det är samma molntjänst som man levererar. Vi hoppades även på en klar definition.

ML: Då ska jag ställa en ledande fråga till er. Vad är skillnaden idag av att ha 50, 100 eller 1000 servrar som står i ett datacenter och tuggar med olika applikationer eller det här såkallade privata molnet.

M: Det är inte så stor skillnad vad vi har kommit fram till. Har du någon bra förklaring?

ML: Jag har ju då en annan uppfattning. Det egentligen det första steget som har jobbat med ganska länge och en del konkurrenter till oss, VMware som jobbat med ganska länge och det är ju i stället för att man har något slags ett till ett förhållande, man har en server med en applikation om det nu är mail eller exchange och sen har man några serverar med databaser, några servrar med sharepoint, man har dedikerat på varje maskin att de gör en sak till att man virtualiserar tjänsterna och applikationerna så att en mailserver med en databasserver kan ligga på flera olika maskiner och kan hoppa mellan dem, eller om någon går ner flyttas det till en annan eller om det är hög last så flyttas någonting undan. Det är det första steget enligt min definition, eller vår definition på det privata molnet, att man går ifrån en tjänst på en maskin, nästan ett till ett förhållande till att man har olika tjänster på maskiner som flyter runt i datacentret och kan arrangera det på ett bra sätt så blir det liksom det privata molnet.

M: Bra förklaring!

ML: aha, tack

L: om vi går tillbaka till de olika nivåerna, om vi tar nätverksnivån till att börja med

ML: Ja..då är ju frågan vad är en nätverksnivå. Ska jag titta på det här som fibern som går in i byggnaden nätversstacken

L: Nej lite mer övergripande. Vi har ju från teorin fått fram att det framförallt är kryptering som man jobbar med. Lite mer övergripande bara.

ML: Jag skulle inte säga att den krypterade delen är den största säkerhetsrisken, för det är så frågan är formulerad, ni frågar inte vilka risker utan de största riskerna och den största risken är om nätverken inte funkar vilket gör att vi kommer tillbaka till de tre sakerna som vi pratade om i början, tillgänglighet. Om någon gräver av fibern och du inte har någon redundans då slutar ju din privata molntjänst att funka, om någon bara rycker ut den. Det är ju det största problemet. Sen vill jag ju gärna ha kryptering och jag vill ha snabbhet och massa saker ,men om det inte funkar så spelar det andra ingen roll.

L: Nä så är det ju

ML: och det genomsyrar ju egentligen alla frågorna. Om det inte funkar så kommer de andra två inte vara så intressanta. Skillnaden i ett privat moln, om vi pratar om det privata molnet så pratar vi förmodligen om det egna företaget, och det företaget kan vara allt från en person, till hundra tio tusen anställda. Och ju större företag det är, ju större resurser har man antagligen till sina egna IT-tjänster och ju mer kraftfull IT-avdelningen är desto större risk är det om något går sönder och desto större budget har jag förmodligen för att se till att vi har någon form av redundans alla de här tre nivåerna som vi pratar om. Ett politikersvar kanske på en kort fråga men.

L: Jättebra. Om vi tittar på de publika, du svarade på både host level och applikation level

ML: Kan ni ge något exempel på en risk på applikationsnivå på ett privat moln så att jag förstår.

L: Vi har egentligen inte fått fram så mycket på de privata, därför vi har varit väldigt konfunderade vad det egentligen innebär med en privat molntjänst. Vi har nu till sist tolkat det som att man inte levererar privata molntjänster utan att man kör det internt på företaget på något sätt. Vi är inte färdiga med vårt arbete utan är mitt uppe i det och lär oss fortfarande.

ML: Men skulle ni inte kunna ha det som en fråga till alla dem som ni pratar med? Vad är definition av ett privat moln? För har de olika definitioner så är det ju ett problem för branschen. Min definition tror jag hyfsat stämmer överens med ganska många. Man har virtualiserat sin IT-infrastruktur som det privata molnet.

L: Jättebra, det ska vi absolut

ML: Sen kan man säkert gå ner på vad ett företag tycker är viktigast med en host-level men de flesta företag idag har ju driftat sitt IT på ett eller annat sätt ganska länge. Och då är frågan, blev någonting av de här a, b och c knepigare i och med att man viritualiserade dem?

L: Om vi kommer tillbaka till det här hur man minimerar riskerna som finns i de olika typerna av molntjänster. Vad är det i första hand som företag B gör?

ML: Nu hoppade vi kanske över de hör publika och hybrida molntjänsterna. I företag B:s fall pratar vi ofta om de publika molntjänsterna, och i vissa fall de hybrida molntjänsterna. Och där igen skulle jag vilja fråga er vad er definition av hybrid är men om jag skulle försöka sammanfatta generellt. I en Office 365 miljö där du kanske köper mail eller Sharepoint eller chat och video konferens av Microsoft så är ju risken, tillgängligheten är ju en risk som vi har tittat på väldigt mycket. Om du inte skulle få kontakt med vår datacenter eller vårt datacenter skulle gå ner av en eller annan anledning då slutar ju tjänsten att fungera och då kommer vi tillbaka till att resten inte spelar någon roll. Därför har vi flera redundanta datacenter. Är du en kund i Sverige tillexempel hamnar du på datacentret i Irland och skulle det av någon anledning gå sönder, explodera eller vad det nu må vara kommer det automatiskt plockas upp av datacentret Holland, Amsterdam. För det är då speglat av datacentrena. Sen efter det har vi ytterligare datacenter, vi brukar säga att vi har mellan tio och hundra datacenter i världen, men vi talar inte riktigt om hur många. Men de två publika datacentrerna som vi pratar om i Europa är på Irland och i Amsterdam. Sen har vi naturligtvis i varje datacenter redundanta elledningar, redundanta kylningar, redundanta fiberkopplingar, redundant disk, allting är redundant. Dels för att man ska kunna flytta tjänsten och för att se till att det inte blir något problem och blir det något problem ska en annan del av datacentret kunna plocka upp det. Det leder då in i den här tillgänglighetsdiskussionen och SLA som kommer lite senare. Om vi inte har den här tillgängligheten så kommer vi att bli ersättningsskyldiga till kunden. Och företag B:s till skillnad mot många andra leverantörer erbjuder en monetär ersättning, det finns många molntjänster som säger att om inte den här

tjänsten så får ni en månads gratisabonnemang efteråt eller får något extra. Vi har sagt att vi har monetär ersättning vilket vi tycker är starkare.

M: Nästa fråga angående den fysiska säkerheten med placeringar av servar etc. Hur hanterar ni det?

ML: Det är som i alla säkerhetstänk, jag kallar det för lökmodellen eller lager på lager modellen. Det är först och främst att se till att rätt personer har rätt access sen har vi allt ifrån murar stängsel och arga hundra, vakter och sådana saker. Sen är det bara vissa personer som har rätt att gå in själva ända in i datacentret. Och när de går in monotoreras de hela tiden så dom kan inte ta någonting, förändra någonting. Och skulle dom behöva byta ut en disk så ser man till att den disken förstör innan tass ut ur kontainern så att ingendata kan komma på vift. Det kanske inte har så mycket med den fysiska säkerheten att göra men processen hur man hanterar driften av datacenter är naturligtvis jätteviktiga

L: Det låter tryggt

M: Vi undrar också vad det finns för möjligheter för er att komma åt kundens data. Är data så pass krypterad att även inte ni kan se den? Kan ni radera en kunds data och kan ni så fall göra det utan kundens medgivande? Med andra ord, finns möjligheten även om kanske ingen skulle göra det?

ML: Om vi säger så här. Vi skulle kunna se kundens data men vi ser istället på oss själva som en postleverantör. Vi har kartonger och vi skyfflar dem från adress till adress och vad som finns i kartongerna är för oss totalt ointressant. Ni som kund köper en tjänst av oss, vad som finns i era mail eller vad som ligger i era dokument eller vad er applikation håller på med det är vi inte intresserade av. Sen finns det sådana här saker som lagar tillexempel. Om en kund skulle bryta mot lagen, det skulle göras en polisanmälan och ett åklagarbeslut om att en viss data måste tass fram så följer vi lagen i det landet där vi levererar tjänsten. Och därför är man skyldig att kunna ta fram data ur ett lagligt perspektiv. Låt er inte luras utav någon som säger att vi kan inte titta på data. Tittar man ex på Dropbox och läser deras FAQ så står det längst ner att vi kommer kryptera upp data innan vi ger den till polisen. Kryptering tycker jag att folk sätter en enorm tilltro till, ibland en lite för hög tilltro. Kryptering är bra men kryptering hindrar tillexempel saker om du skulle kryptera alla dina e-post meddelanden så kan du inte söka i dem. Det här är en ganska fin balansgång mellan tillgänglighet, funktionalitet och kryptering. Om du tittar på Azure och du skapar en applikation så krypteras alla din data i vår databas tillexempel SQL Azure och någon skulle komma åt den informationen, då kan vi bara ge ut den krypterade informationen, vi ingen super duper bakdörrsnyckel och kommer aldrig ha. Så det är lite upp till kunden hur de vill hantera sitt eget. Vi kan radera data, sen om vi skulle göra det, det vet jag inte. Det är möjligtvis så om kund inte vill betala för tjänsten kommer vi antagligen, nu har jag inte finläst vårt avtal men kan finnas en klasul om att, då kommer vi erbjuda någon form utav exit eller avslut och då kommer man få ta hand om data och efter det kommer vi naturligtvis första data så att inte någon annan kan komma åt det. Vi kommer naturligtvis radera kontot och skriva över det, och vi kommer att garantera integriteten in i det sista för alla kunders data

M: När ni raderar data så raderar ni den så pass att det inte går att få tillbaka data. Om man jämför ex med en fil på en PC kan man i vissa fall få tillbaks den.

ML: Det bero på skulle jag vilja hävda. Nu är jag ganska duktig på Windows och kan inte andra operativsystem men om du trycker på delete på en fil så absolut, då kan jag ta tillbaka den men om du skriver över de tomma sektorerna på hårddisken, det finns ett inbyggt program i Windows, som folk inte känner till särskilt ofta, det finns ett program som heter fifer då skriver man över disken, först tre gånger med ettor, sen tre gånger med nollor och tre gånger med slumpmässiga tal och efter det finns det vad jag vet ingen som någonsin kan återställa den data från en disk. Jag har frågat dem som jobbat med återställningar utav diskar att om vi kör det här kan ni få tillbaka data, nej har dom sagt.

L: OK

M: Eftersom det finns möjlighet för er att se, radera och modifiera. Kontrollerar ni era anställda ifall de exempelvis har haft någon kriminell bakgrund, eller något?

ML: Alla som är anställda på företag B-anställda går igen en rigorös anställningsprocess, sen beror det lite på vilken säkerhetsklassificering man har så blir den naturligtvis mer eller mindre känslig. Skulle du handha känslig data inom exempelvis amerikanska staten så måste du ha en högre säkerhetsklassifisering och då ingår det ju sådana saker som olika sorters bakgrundskontroller, även i Sverige då om du ska jobba med vissa hemligheter. Jag tycker det är lite fel att säga att en tidigare kriminell ska vara automatiskt misstänkt så klarar man sig genom att göra en bakgrundskontroll utan det viktigaste är att monotorera alla aktiviteter och att ingen överskrider sina befogenheter. Jag som är chef säger helt plötsligt att jag vill gå in och läsa lite mail hos en kund och det måste jag göra för att jag är chef, gör nu som jag säger. Då skulle det plinga till i alla system eftersom jag har ingen anledning att göra det även om jag kanske skulle ha ett behov ibland att få göra det. Då måste man kunna spåra det, vem har gjort det här och varför. Det är det som är så viktigt att man har processer på plats som ser till att det är olika fack i driften som säger att de som är så pass nära data måste få titta på det, men får aldrig någonsin komma nära själva kunddatat utan ska kanske bara kunna komma åt statistiken av data. Det är så här många mail som skickas från den här servern varje dag och därför så räcker inte kapaciteten utan vi måste skala ut det här eller om man köper Azure tjänsten. Då tar man ju betalt per megabyte som flyger över nätet eller per CPU som man använder och den statistiken måste kunna mätas. Ett långt svar på en ganska knepig fråga.

M: Du nämnde att ni har möjlighet att se vilken anställd som har påverkat vilken data

ML: Absolut. Det loggas rigoröst för att se vem som hållit på med vad

M: Du nämnde lite kort innan vilket lands lag det är som gäller, att det är där leverantören befinner sig, är det alltid så när det uppstår en tvist?

ML: Det beror lite på hur man har förhandlat i sitt avtal. En stor kund i Sverige köper som köper våra tjänster hamnar då på irländsk rätt eftersom datacentret är i Irland och driftas där men det står tydligt i våra avtal också.

L: Vad har ni för avtal, har ni något färdigskrivet SLA?

ML: Jajjamänsan. Vi brukar generellt säga 99,9 % tillgänglighet men det är lite olika beroende på vilka av de olika tjänsterna vi pratar om Azure eller Office 365, nätverksåtkomlighet eller databasåtkomlighet och massa saker har vi spaltat upp men 99,9% tillgänglighet. Kunderna själva kan logga in på sina olika dashboards och titta på hur tjänsten mår och om den nu är nere. Om det nu är så att man inte kan komma åt tjänsten så är det en av tre saker. Antingen är det fel på mig själv eller min dator eller så är det något fel på nätet och det kan vara tredelat, antingen kan det vara mitt nät, internet eller vårt nät eller till sist så kan det vara något fel i vårt datacenter. Kan man logga på en dashboard och titta ifall vi har ett avbrott i tjänsten så är det ganska enkelt att veta om man inte kommer ut på internet över huvud taget så kan man misstänka att felet ligger någonstans på sin egen sida istället. Vi på företag B har valt att gå ut och prata om alla säkerhetsfrågor tidigt med våra kunder och försöka svara på alla de frågor som gäller. Till syvende och sist är det kundens uppgift att se till att man följer de lagar och regler som finns och det tycker jag man ska vara tydlig med i sin kommunikation med kunden. Jag finns tillänglig att svara på alla möjliga frågor ni har men jag som leverantör kan inte stå till svars för de beslut som kunden tar. Till sist som jag sa innan, det är kundes ansvar att se till att man följer alla de lagar och regler som gäller där man driver sin verksamhet. Det som är knöligt är att många av de lagarna som är skrivna i dagens samhällen över hela världen är skrivna med fysiska gränser i åtanke, data ska vara i Sverige, data ska hållas inom EU tillexempel. Jag brukar ifrågasätta det lite försiktigt, när du skickar ett e-postmeddelande så kan det faktiskt gå 4 varv runt jordklotet även om det går till en mailserver som står bredvid den andra mailservern. De flesta kunder idag använder redan molntjänster, utan att man ens tänker på det. Varje gång du knappar in en sökmotor och trycker OK så har du använt en molntjänst. Varje gång du laddat upp något på en webbsite någonstans, delat med dig utav något så använder du en webbtjänst.

M: Tror du att vissa företag väljer att lägga ut vissa saker i molnet och inte vissa på grund av att de anser att det är en säkerhetsrisk.

ML: Jag tror att om du är ett mindre företag är du mer belägen att lägga ut saker eftersom man värderar risken som att vi är 10 eller 50 personer på det här lilla företaget och vi är inga IT-experter, vi vet inte hur man konfigurerar en server, sätter upp och underhåller den. Varför inte köpa tjänsten av en leverantör som är experter

på det och dessutom den som gör produkten är den som driftar den. Det kan ju egentligen inte bli bättre plus att man då har SLA ovanpå som garanterar att det fungerar och dessutom om det är ett stort företag har man ett varumärke att tänka på, varumärket är jätteviktigt för oss, att det funkar. Tittar man på stora företag säger man kanske att vi inte kan lägga ut det här eller vi vill inte lägga ut det här och har ändå driftat det här så länge och vet att det funkar men om vi nu ändå ska ha en ny tjänst varför inte köpa den på nätet. För vissa passar det bättre för och för vissa passar det inte för och vissa har krav på sig att de inte kan, får eller vill. Definitionen är ganska bred beroende på vilken molntjänst vi pratar om, är det PaaS eller SaaS, hur stor är företaget, vad vill man uppnå, är kostnaden viktigare, är tillgängligheten viktig, är var datacentret ligger någonstans viktigt?

M: När en kund beställer en molntjänst, är det i första hand säkerheten de tänker på, eller är det kostnaden?

ML: Varför söker jag mig till en molntjänst? Om jag tittar på lite statistik som vi IDC tillsammans med forster från 2009 och 2010 så säger dom; pay ony what you use så säger 77,9% så säger de att det är den högsta drivern, dvs att man inte har massa licenser för saker man inte använder. På problemen toppar säkerheten på 88%

M&L: Vi kommer att transkribera intervju och mailar den sedan till dig så att du får möjlighet att läsa det innan vi publicerar det i rapporten.

ML: Jag tror jag står för det jag säger men man vet aldrig [småskratt]

M&L: Tack för väldigt bra svar och förklaringar på frågorna

ML: Lycka till med arbetet

Bilaga 6 Transkribering, Informant 2, Företag A

R = Intervjuperson 2

L = Linn Bjärvall

M = Martin Ståhl

M: Vi har nämligen två former av intervjuguider, en för kunder som väljer att köpa och en då för leverantörer som levererar molntjänster så då kanske den för leverantörer passar dig bättre?

R: Ja absolut, prova med den!

L: Ja, då kör vi på den. Du har ju lite av vår bakgrund. Vi går ju det systemvetenskapliga programmet och sista terminen och då är ju detta det sista momentet, uppsatsen och så kände vi båda att vi har gjort många projekt tillsammans och vi var båda nyfikna på molntjänster och eftersom det är lite i ropet just nu. Också när vi började titta på olika teorier om det så märkte vi att det var många frågetecken runt just säkerheten så vi tänkte om du bara skulle vilja berätta lite om din är roll på företaget.

R: Man kan säga att jag är ansvarig för den enhet som jobbar med portallösningar - webblösningar. Och i den rollen ingår allt ifrån försäljning, produktutveckling, leverans, rekrytering och att hantera alla våra partners. Också i min grupp är det ungefär tjugo personer som jobbar med de här grejerna och majoriteten är nog på utvecklarsidan.

L: Skulle man då kunna säga att det finns någon typ av leveransmodell när det gäller molntjänster som ni levererar?

R: Nej, vi har ingen modell, tror jag. Däremot har vi ett par produkter som man kan köpa som molntjänst.

M: Det är ju det, man kan ju dela upp dem i om man levererar en hel platsform eller bara en applikation eller en infrastruktur eller?

R: Nja

M: Så det är ingen speciell av de som ni…?

R: Mmm… det skulle vara applikationer i så fall. Vi kan tillhandahålla till exempel söktjänster som molntjänster eller rena applikationer tillexempel projektplatser eller... Vi har en produkt som heter Compliance Manager som kan tillhandahållas som en molntjänst, men inte infrastruktur, inte på den sidan. Däremot har vi i koncernen drift och förvaltning, där kunderna kan lägga ut sina servrar eller hyra utrymme.

L: Ok, Vilka anser du eller företaget är de största riskerna med molntjänster?

R: För oss eller våra kunder?

M: För kunderna, finns det någon risk för kunder att använda molntjänster och vilka risker skulle det vara?

R: Absolut, en risk är ju det här med tillgänglighet. Man lägger ut lite grann av… tidigare har det kanske varit så att man köper ett SLA från sin IT- avdelning. Där har du ju ett problem. Det är samma organisation som ens egen. Du kan bli arg på dem, men du kan inte få nåt skadstånd riktig. Jag får en känsla av att många kunder tror att om man lägger ut så kan man i alla fall stämma nån. Men om du lägger ut något som är riktigt viktigt och det inte fungerar så lider du ändå, även om du i slutändan kan stämma någon. Så om saker och ting inte finns, eller saker och ting går ner eller inte funkar som det skall. Så är det… Du sitter i samma problematik ändå, du har inte löst problemet med att få det bättre. Däremot kanske du får det billigare eller något annat. Så säg till exempel att du har haft projektplatser internt, du har byggt det själv. Också kanske du köper projektplatsen.se eller av oss . Du har hundra projekt som snurrar samtidigt, sen så åker plattformen ner. Då har du hundra projekt med kanske i snitt fyra personer i varje. Då har du fyrahundra personer som inte kan jobba den dagen. Den risken är lika stor som förut. Eller om saker och ting försvinner - Vad skall man göra?

L: Mm

R: Tidigare kanske man kunde gå till IT avdelningen och sitta bredvid de när de plockade fram det eller hittade det igen. Här kan man inte göra det. Man måste vara väldigt tydlig med och förklara problemet och säga att det inte är som det skall vara… också är det nån som lyssnar och de kan säga ja, enligt vårt SLA så har vi här fyra timmar på oss för att lösa problemet och under tiden sitter det hundra personer utan att kunna jobba medan man tidigare kunde gå till sin egen IT- avdelning och säga lös det här nu, också kanske de gjorde det bara då för att man skrek högt.

L: Javisst, det är ju en stor skillnad, men de applikationerna som ni levererar, då är det främst privata, publika eller hybrida?

R: Det är ju privata för kunderna då. Det är inte så att de delar databas med andra utan det vi gör det är egentligen... Vi använder en produkt som heter VM ware till exempel. Där sätter vi upp en helt egen miljö åt kunden också och sen så får de jobba på den också får de extra access in till vår server, men jobbar du till exempel på salesforce.com då delar du med alla andra. Du ligger inte på en egen server, just dina grejer. Så jag skulle nog kalla det privat.

M: Men vad är din definition av en privat molntjänst om du jämför till exempel ett lokalt nätverk i ett företag, vad är skillnaden?

R: Jag vet inte om man kan hitta en klatschig definition på bara ett par rader. Men, som jag ser det så är det egentligen så att har du inte själva servern, själva logiken hos dig, utan det ligger hos någon annan som du betalar, kanske oftast per månad eller kanske du har en startkostnad och sen så betalar du per månad för att få tillgång till tjänsten. Och det enda du har hos dig är en klient och idag är det allt som oftast en browser som är klienten. Du har inte en den typen av klienter man hade för många år sen. Utan nu är det bara browserbaserat. Sen så pratar du med servern och databasen som ligger hos oss.

L: Nå, varför vi frågar är för att vi hade en intervju med en av leverantörerna häromdagen, vi hade inte med den frågan från början. Också frågade han oss hur vi ser på det och så sa han att det är jätteviktigt att prata med kunderna om det, att det är viktigt att vi ser det på samma sätt och att vi gärna skulle diskutera det med andra så vi har lagt till det som en extrafråga.

R: Vad sa den leverantören då?

M: I princip sa han att är det bara lokalt inom företaget - ej molntjänst, så befinner sig all data på en server inom företaget och är det i ett en privat molntjänst så kan samma data befinna sig på flera olika servrar och flyttas mellan flera servrar inom företaget så det var hans definition, det är fortfarande inom företaget, men skillnaden är att det kan fungera som en molntjänst.

R: Ok, så kanske man kan se det också. Men för oss är det, det vi jobbar med mest, att vi har separerade miljöer för varje kund, där varje kund köper en tjänst som de kommer åt, men vi har inte byggt upp den infrastrukturen på ett sånt sätt att kunderna jackar in sig och delar data med… eller infrastruktur / databas med andra kunder eller företag.

L: Men det är väl oftast så man börjar på också… med privat att man …

R: Nej, men många kör ju så sådana här tjänster som Salesforce.com eller Projektplatsen .se, då man loggar in och sen så delar du med alla andra kunder. Också har de byggt en säkerhetsmodell som gör att man inte kommer åt någon annan data än sin. För det har jag aldrig varit med om, att man går in i Salesforce till exempel, också hittar jag ifrån någon konkurrent liksom deras, det inträffar aldrig [småskratt] men det är ändå i samma databas, Salesforce.

L: OK, Man brukar göra så när man tittar på molntjänster, om man tittar på litteraturen att man delar in infrastrukturen när det gäller molntjänster i network level, host level och application, och så har vi en fråga här; vilka ni ser som de största riskerna när det gäller privata molntjänster på de respektive nivåerna. Skulle du kunna säga något om det?

R: Jag kan gissa… men vi skall se…

L: Det behöver inte vara så strikt indelat.

R: På de privata molntjänsterna med network… jag tror fortfarande när det gäller det privata att det är när du inte får den servicenivå man förväntar sig, och liksom vad händer när du inte får, vad händer när det försvinner eller går ner eller inte kan återskapas på ett bra sätt?

L: Tillgängligheten då?

R: Sen är det ju också så… om man tittar på Microsofts definition så är det ju så att det du alltid har... du har liksom den mänskliga länken som är en stor risk, det är att det finns alltid nån systemadministratör som kommer åt allt och kan läsa allt och se allt och som kan göra vad de vill… och risken med det är att… säg att nån skall sluta, de kan ta med sig all data. Du har en annan risk, det hände, om jag minns rätt så var det nu i San Fransisco på ett ställe, där det var en kille som fick sparken, som var systemadministratör av några sådana jätteviktiga system, efter att han fått sparken som var systemadministratör av några jätteviktiga system. Efter att han fått sparken och när han skulle gå ställde han om alla lösenord och så gick han. Så det betydde att alla som jobbade på det kontoret inom den förvaltningen eller i den stan, ingen kunde logga in i sina system. Så sådant kan inträffa! Så är du till exempel databasadministratör, då kan du ju läsa allt som står i databasen.

L: Herregud.

R: Och tittar man på det publika så är det ju inte samma risk för då har du ju bara tillgång till det du har tillgång till och du har ju inte nån systemadministratör internt, men det betyder ju också att någon hos leverantören istället kan göra det, är det bättre eller sämre jag vet inte… men risken är ju där i alla fall.

M: Ja det är hur ni minimerar de riskerna exempelvis hur ni min att tillgängligheten skall vara så hög som möjligt som du nämnde som en risk? Hur gör ni för att kunna tillfredställa kunden bättre på så sätt?

R: Ja det här är ju liksom inte våra Core business… det här är någonting vi gör som ett mervärde för våra kunder..så vi friskriver oss väldigt noga i våra avtal kring SLA, lovar ingenting som vi inte kan hålla. Det innebär att om någonting går ner så får kunden vara medveten om att det kanske tar två dagar innan det är uppe igen. De som har det här som Core Business, ja, de har ju en helt annan infrastruktur uppsatt ..

L: Jo det är klart.

R: Så går någonting ner så ser man till att det är snabbt uppe, alltså att det finns på plats.

L: Ja jo

R: Och det som vi inte jobbar med och som jag kanske tycker att vi kunde göra mer är till exempel något som på engelska kallas för alerts. När någon gör någonting. Vi har ett kundregister till exempel. Om någon sparar ner hela vårt kundregister på sin hårddisk.

M: Mm

R: Då vill jag kanske som ägare till kundregistret få en alert att nu har den här personen, som jag också vet skall sluta inom kort, laddat ner hela kundregister. Sådana grejer har vi inte.

M: Men loggas ingenting som görs då?

R: Jo du kan logga det, men när du loggar allt.. varje gång jag gör nånting så loggas det, också är det två hundra anställda, varje gång…så de här loggfilerna växer med en gigg om dag. Det är någonting du kan gå in i efteråt och analysera, men det är ingenting som du liksom får ett pling skickat till dig att nu har det här hänt. Det är du har till exempel är Telia, jag var utomlands och då när jag var utomlands fick jag ett sms som sa att nu börjar du närma dig 650 spänn i datakostnader för din utlandsvistelse och det är ju liksom en bra alert men några sådana har vi inte inbyggda.

L: Bra

R: När det gäller användarhantering och sådär, det vi oftast gör är att vi ger en kund, här har du ett adminkonto, du får själv administrera vilka som skall ha tillgång och inte tillgång, vi gör det inte, du lägger själv till dina användare och tar bort dem. Ja, det betyder ju ibland att den personen hos kunden inte sitter och gör det där hela tiden så det kan ju var att det är någon som slutar men aldrig blir att … det är så det funkar.

L: Ja det är mycket och tänka på….

R: Så det är..den ..För att minimera riskerna, mycket har att göra med liksom den mänskliga faktorn, det man behöver göra, det kunder behöver göra framförallt… är att sätta upp rutiner eller en hantering utav. Nu är det här en molntjänst och hur skall vi jobba till exempel när folk slutar ..vanligtvis blir ju folk avstängda från systemen då, men blir du avstängd från dina molntjänster också?

L: Ja, vi var ju hos en leverantör som hade rigorösa listor för varje typ av molntjänst så det märktes att de jobbat länge med den processen.

R: Ja men det är ju den här man kallar Governance eller.. det är ofta det inte finns på plats och även om den finns på plats så följs den inte alltid, för man följer inte upp och jobbar aktivt med det.

M: Så den fysiska säkerheten är kanske inte så intressant då? Eftersom ni kör mest bara privat då lokalt på företaget..

R: Nja… men det där brukar vara en sådan där hygienfaktor som man har när man jobbar med försäljning. Kunden frågar var finns servrarna. Ja, då säger man.. Man brukar säga.. den står i en kärnvapensäker bunker, vi har fingertryckskontroll, vi tar foto på alla som går in . Och sen så säger kunderna: Åh vad bra, då frågar vi inte mer eller det vill vi se eller det säger de aldrig.. det låter bra med oss, men du skulle lika gärna kunna ha servern under ditt skrivbord för kunden begär aldrig att få se den.

M: Så… ja det har du i och för sig pratat om också idag..om det finns möjlighet för er då att se, radera eller modifiera kunders data? Och…

R: Ja skulle kunna tro att ..har vi det hos oss, så kan vi se det.

M: Så det är inte så att det ligger liksom krypterat i databasen så att inte ens ni kan se det, utan ni kan?

R: Jag skulle tro att vi kan se det.. det är de lösningarna vi har. Mm..Sen så finns det ju de som jobbar med kryptering också så att ingen kan se.. förutom ..kanske just för att minimera den här risken med att egna systemadministratörer kan komma in och kolla, men jag tror att det vi har.. så kan vi gå in och se vad vi vill.

L: Och då kan ni spåra också, om det är någon anställd som har ändrat i någon kunds data eller logga?

R: Nån.. kanske man kan se, men inte vem, däremot kanske man kan se vilket konto som är använt, så om jag har ditt lösenord till exempel om jag har sett det och jag loggar in som dig så kan man inte spåra det till dig, däremot kan man spåra det till ditt konto sen så om du säger att ja, men jag har inte gjort det ja, men, jag var ju inte ens här, jag var på tjänsteresa, titta själv, då är det ju svårt…

M: Men de kontouppgifterna, kan man logga in från vilken dator som helst då, eller är det bara en specifik dator?...

R: Ja, alltså en del av de här servrarna vi har… om du skall liksom prata med själva servern.. en del grejer kan du bara göra genom att koppla upp dig, alltså genom att gå in i serverhallen, genom att gå in med ett tangentbord i servern..

M: Jo, men jag tänkte med det du sa att han sa att han som var på tjänsteresa….men på vissa tjänster kan du ju logga in via browsern från vilken dator som helst.

R: Ja, men det skulle du nog se..för du kan ju alltid se från vilken IP- adress det kommer ifrån eller nåt sånt ok, du var inte inloggad via VPN ens, och du var inte i Sverige , ja du var nån annanstans, men någon har loggat in med ditt konto och gjort det här, ja vem var det, jättesvårt….

M & L: Mm

R: Det kan man ju lära sig snabbt med en del kollegor, de har alltid samma lösenord, eller har de samma princip eller så har de en gul lapp liksom på..

M: Ja [småskratt] En gul lapp… typ på skärmen

R: Ja på skärmen[småskrattar] och det är jättesvårt.. du kan inte avskeda någon för att de har varit oaktsamma med sina lösenord…liksom

M: Men får ni bestämma era lösenord själva eller det autogenereras?

R: Vi får bestämma själva…oftast men vi skulle kunna autogenerera men då blir folk oftast vansinniga.

M: Ja de kommer väl sällan inte ihåg dem då?

R: Nja, och vad händer om du inte kommer ihåg det, då har du det nedskrivet någonstans i närheten av dig?

L: Ja, det är ju säkert…[småskrattar] Jag vet att jag nämnde för dig igår när du frågade om vi kommit fram till någon form av slutsats, så är det ju mycket som till syvende och sist handlar om just lagarna och avtalen mellan kund och leverantören, och hur är det då?...vilka lagar är det som gäller?

R: Vi har nästan alltid Sveriges lagar, alltid och ofta så står det också nån sån där klausul om att vid tvist av detta avtal så är det.. jag tror att det brukar vara nån sån där skiljeman eller vad det heter ifrån Stockholms handelskammare eller nåt sånt där som man använder i första hand, så i första hand en medlare som kommer in och tittar och talar om att ni skall betala det, och går man inte med på det så är det väl rätten, men jag har aldrig varit med om någonting sånt där som gått till rätten – aldrig.

M: Nej ok, men generellt sett vilka lagar är det som gäller? Är det köplagen och avtalslagen kanske? Eller?

R: Nej, det är… alltså, alla avtal är ju separata.

M: Så att..de överskrider då avtalslagen så kallat, eftersom det är ..mellan kund och leverantör?

R: Ja… Jag vet inte vilka lagar som är tillämpliga, men det brukar inte stå i avtalen heller, utan man brukar hänvisa liksom till avtalstexten och de allmänna villkor och sen så har du en oftast någon sån här tolkningsordning – du kanske har en tjänstebeskrivning, allmänna villkor, ett avtal talar också om ifall de här avtalen mellan papprena strider mot varandra, så gäller det här före det och det före det och det före det.

L: Mm

R: Men jag har aldrig varit med om vare sig här eller på nåt annat jobba jobb att man har blivit stämd eller nånting när det här inte har funkat. Det enda som händer det är att konsultbolaget kanske ger lite kompensation eller att man säger att de inte behöver betala för den här månaden eller att kunden drar.. till nån annan .

M: Ok

R: Men det är liksom gjort är gjort och man orkar inte dra i det. [småskratt]

L: Har ni något eget färdigskrivet SLA då som..?

R: Ja jag tror att vi har ett par SLA här faktiskt, lite olika beroende på vad det är och lika olika nivåer. Oftast kanske inte det är kopplat till tillgänglighet utan mer på responstider, …[Pling, telefonen ringer]och hur ofta får jag ringa, får jag ringa 24 h om dygnet eller ja, vad det nu kan vara…

L: Hur är det nu behöver du gå vidare till nästa möte eller skall vi fortsätta?..

R: Ja jag har faktiskt nästa möte nu, men…

L: Vi förstod det så, då är det bättre att vi tar detta i lugn och ro när det passar senare i veckan om det passar.. vi hoppas det

M: Det är ju inte så många kvar…

R: Mm

L: Det får du bestämma vad du tycker så du inte stressar….

R: Jag måste nog gå, för jag har mitt möte, det har hållit på i tio minuter… Mm Var det mycket kvar eller..?

M: nej, det är ju de fyra sista…

L: Nej det var lite mer

R: Skall vi ta det eller, vi tar de direkt.

L: Vilka uppgifter grejer i SLA eller kontraktet tycker du eller ni är viktigast för att garantera säkerheten för kunden? Är det något som är…?

R: Nej, men jag tycker att det viktigaste är…Alltså om det här skall funka… någonting som funkar tror jag är …om man har ganska höga vitesbelopp, men… du måste ha något sätt att följa upp det, och som kund är det sällan man följer upp och tittar, utan när man har ett problem då hör man av sig och inte annars och har du ett problem och det inte blir löst fort så skriker du högt. Men liksom det händer liksom aldrig något mer än det. Skulle någon komma till företag A med jättehöga vitesbelopp, då skulle vi bara säga, nej men det är inte intressant, då får ni gå till någon annan, så jag tror liksom att branschen inte är riktigt mogen och om det funkar ja sorry och så länge det funkar så är det väl bra men funkar det inte så sorry, du kan inte få något..Sen så…ja

L: Ok, finns det angivet i ert SLA vem som äger informationen?

R: Nej, inte i själva SLA:et gör det nog inte det, men i avtalen brukar det stå…tydligt för kunderna till exempel vad händer om ni går i konkurs? Ja, men det är OK, för ni äger informationen, så då skriver vi att ni äger informationen men företag A äger applikationen och all liksom programkod, men ni har alltid rätt till er information även i händelse av konkurs eller vad det nu kan vara..

M: Ok, det är bra

L: Finns där också angivet hur man hanterar informationen och vem som har rätt att hantera den? Alltså av vem och hur?

R: Nej sällan, sällan

L: Det är inte så noga …

R: Nej inte i våra SLA. Däremot kan man ha vår beskrivning, tjänstebeskrivning, där skulle det kunna stå, vi följer BITS till exempel eller nåt sant och vad händer om vi inte gör det… det står det ingenting om..

L & M: Nej [småskrattar]

R: Ehh… den kanske skriver att ja, endast ett fåtal servicetekniker har tillgång till servrarna, vad händer om det inte är så?

M & L: Ja, Ok

L: Det är Intressant

R: Om ni inte gör det här, vad får vi då som kund, om.. det visar sig att vilken jeppe som helst har kunnat komma åt det här, vad får vi då? Då säger vi, det kommer inte att hända. Ja, men det är bra, då kan ni ge oss en miljard i skadestånd. Nej det kan vi inte. Då får ni köpa någon annanstans om ni vill ha det. Då köper kunden av någon annan. Så mycket av det här handlar om att lita men om det.. tyvärr alltså, jag gör ju samma sak. Om man…vad skall det vara..till exempel ringer en telefonförsäljare till mig och säger hej, vill du köpa en telefonabonnemang. Då säger jag..Nä jag tycker det är så jobbigt nu när man får sitta så lång tid i kön. Nej säger de, det behöver ni inte alls, vi har investerat jättemycket i vår kundtjänst, och våra väntetider är aldrig mer än fem minuter. Men vad bra säger jag, skriver du in i avtalet bara att om jag får vänta mer än fem minuter så vill jag ha tiotusen per påbörjad minut, då skriver jag avtal med dig. Nej men det kan jag inte skriva in, det går inte. Men du sa ju att jag aldrig behövde vänta mer än fem minuter, då kan du väl skriva in en miljard per påbörjad minut. Nej det är ju ingen garanti då, det är ju ingenting, nej nej OK, det har du ju rätt i, men jag lovar…

L & M: Nej precis [småskrattar] Finns det angivet hur informationen övervakas?

R: Ja, men det står sällan i SLA: et, det är mer i tjänstebeskrivningen kanske, att vi har full övervakning, vi har hundraprocentig redundans, vi har fail over, vi har en backupserver, vi har övervakning och loggning på allt, ja, men vad hjälper det om skadan är skedd?

L: Nej precis... Och slutligen här..finns det angivet hur tillgänglig tjänsten är?

R: Ja, det brukar det stå.

L: Ok, det brukar det…

R: Nej men, nej, vi brukar säga så här.. att vi garanterar 99, 98 % upptid eller 99, 96% upptid och räknar man då hur många timmar är det på ett år.. nu har jag glömt bort, men det är väl 24 * 365 så det är,kanske 8000 h eller nåt sånt så har du 99 % ,då är det 1 % som den får vara nere. 1 % av 8000 är 80 h och att nånting skulle vara nere 80 h, det är jättemycket.

M: Jo

R: Man brukar kunna säga 99.96% eller något sådant där, men det är ju aldrig någon som håller räkningen på det.

L & M: Nej, Ok

R: Så skulle .. vara kund och köpa en molntjänst, då skulle jag säga att ok, det här men mäter vi och det mäter vi genom att pinga den här servern si och så ofta och är den nere då skall ni betala. Men det det inte står heller, det är till exempel responstider, det brukar det aldrig stå. Du vet att när du klickar på en länk.. går det fort så är du nöjd och går den långsamt så är du inte nöjd, så visst servern är tillgänglig men den går jättelångsamt. Det tar två minuter för dig att ladda sidan, men den är tillgänglig, så det vill man ju gärna ha med. Men det är jättesvårt att mäta och jättesvårt att följa upp men det går att göra, absolut.

L & M: Ok, stort stort tack för att du tog dig tid!

R: Lycka till!

Bilaga 7 Intervjuguide till kunder

Inledande frågor
Berätta lite kort om företaget och din roll

Hur väl känner ni till Cloud Computing/molntjänster (skala 1-10)

Vilka tycker ni är tre viktigaste aspekterna generellt sett att ta hänsyn till vid val av molntjänstleverantör? (ekonomi, säkerhet etc?)

Har ni några negativa erfarenheter av molntjänster ur ett säkerhetsperspektiv? Utveckla

Använder ni er av någon molnbaserad tjänst i dagsläget?
Om ni inte använder, vilken skulle ni kunna tänka er att använda?

Vilken leveransmodell (Paas, Iaas eller Saas) och varför?

Vilken typ (Publik, Privat, Hybrid) av molntjänst använder ni idag
kommer ni att använda er av inom kort?
Varför?

Säkerhetsrisker med molntjänster
Gör ni någon form av riskanalys innan ni bestämmer er för vilken information ni vill lägga i molnet? Hur går ni tillväga? Vilken form av riskanalysmetod(modell) använder ni er av? (Kvalitativ eller kvantitativ?)

Vilka ser ni som de största säkerhetsriskerna med molntjänster?

Vilken information kan ni/kan ni inte tänka er att lägga ut i molnet?

Vilka säkerhetskrav anser ni är viktigast när ni väljer molntjänstleverantör?

Skillnader mellan säkerhetskrav på olika typer av molntjänster samt leveransmodeller
Hur definierar ni en privat molntjänst?

Vad har er organisation för säkerhetskrav på ett privat moln på respektive leveransmodell (Saas, Paas, och Iaas) på:

A) Network Level
B) Host Level
C) Application Level

Vad finns det för säkerhetskrav på ett publikt moln respektive leveransmodell (Saas, Paas och Iaas) på:

A) Network Level
B) Host Level
C) Application Level

Juridiska avtal mellan kunder och leverantör
Har ni en egen checklista/ramverk/informationssäkerhetspolicy för molntjänster?
Vad grundas den på och vad innehåller den för krav?

Förlitar ni er exempelvis på ISO 27001 samt BITS?

Vilken typ av avtal finns mellan er och leverantören?

Vem ansvarar för vad?

Är det ett färdigt från leverantören eller något ni gemensamt kommit överens om?

Står det skrivet hur avslut etc sker?

Vet ni vilka som har behörighet till er data hos leverantören samt vilka behörigheter de har?

Vet ni vilket lands lagar som gäller?

Finns det några försäkringar man har möjlighet att teckna?

Avslutande frågor
Tror ni att leverantörer och kunder av molntjänster har samma synsätt på säkerheten?
Skillnader och likheter?

Är det samma krav på säkerheten vid införandet av molntjänster som för outsourcing?
Om inte, vad skiljer dem åt?

Är det OK att återkomma om vi kommer på något vi undrar över?

Bilaga 8 Transkribering, Informant 1, Företag C

PW = Informant 1

L = Linn Bjärvall

M = Martin Ståhl

L: Så vi har intervjuer med kundföretag som er nu till exempel och sen också skickat enkäter till rätt många leverantörer i och fått till en intervju även med en leverantör igår. Lite svårare att få till intervjuer med leverantörer….Hade en igår, en skypeliknande med en leverantör. Det var väldigt givande, man lär sig mycket av varje intervju…

L: Skulle du vilja berätta lite kort om dig och din roll i företaget?

PW: jodå så att min bakgrund då. Jag är civilingenjör från början, har jobbat sju år på Tetra Pak i sju år, varav två år i Singapore. Sen är det nu…. 13 år på företag C, så jag har jobbat i 20 år totalt sett och jobbat med teknisk infrastruktur, egentligen hela tiden fram tills för två år sedan när jag blev CIO två; eller mer säkerhetsansvarig, informationssäkerhetsansvarig, så jag tittar egentligen ju inte alls på teknik längre.

L: Nä

PW: men jag har ju bakgrunden. Jag menar jag har ju jobbat med det i arton år nästan .

L: Ja ja

M: Jo precis

PW: Det är i huvudsak datakommunikation, infrastrukturssäkerhet som jag har jobbat med tidigare, nu har vi mer fokus. Nu har vi tagit helikoptern och tittar lite bredare på det .

M: Mm

PW: Och det är klart när vi börjar titta på molntjänster… Ja jag skulle vilja säga att molntjänster helt generellt har ju funnits under väldigt många år, det är bara det att man har hittat på ett namn. Nä för det är just det här software as a service som finns, det är ju nånting som man har gjort sen början av min tid på Tetra Pak, eftersom just lönesystem och annat.. det vill man ju med fördel outsourca för att slippa hantera de här avierna Osv och det är klart. Så det har ju funnits länge, det är bara det att nu har det blivit bredare och annorlunda.

L: Mm

PW: Men vi har ändå ju trots allt mest erfarenhet av just software as a service. Så vad jag gjorde… Jag gjorde faktiskt så att jag tog era frågor och tryckte in dem ett worddokument

L: Mm, vad bra

PW: Också …. PIP ..har jag delvis svarat på frågorna i det då. Vi använder oss bland annat av templates när vi pratar om…när vi köper mjukvaror internt och när vi köper dem externt. Då har vi gjort en template som egentligen är en kombination av säkerhet och Enterprise Architecture. och Enterprise Architecture det strävar mer till tekniksidan och det finns ju en… skall vi säga 90 frågor ungefär runt Enterpise Architecture t ex hur tänker när det exportfunktioner och importfunktioner men det finns ju även ett antal säkerhetsfrågor och just när det gäller molntjänster så blir det ganska många som vi ställer, jag tror det är 36 stycken, som vi ställer till .. men vi kommer till det.

L: intressant.

PW. Jag skulle vilja säga att vi inte känner till så förtvivlat mycket när ni frågar om Cloud Computing eller molntjänster när ni frågar om molntjänster, skulle vilja säga att vi ligger någonstans i mitten, för det är ju egentligen Software as a service som vi har använt, mer eller mindre, vi har ju inte köpt datorkapacitet hos någon extern leverantör ännu, där vi kan se på fördelar med skalbarhet och annat kostnad per enhet, om man vill skala upp eller skala ner.

M: Ok

PW: Den får man ju stå för själv internt och är det en extern software as a service är den på något sätt inräknad i affären.

L: ok, nähä

Ehhh så att det är lite svårt för mig att svara på egentligen.. de bitarna som har med infrastructure as a service. Vi har inte har någon erfarenhet av det än så länge.

M: ok, nähä

Där i huvudsak kan jag tänka mig att en stor del av problematiken är tillgängligheten, hur fungerar det här egentligen när man lägger ut våra interna system, hur fungerar integrationen med andra system. För just det här med integrationen är en väldigt central punkt.

L: Mm

För har du en molntjänst och den behöver kommunicera med någonting på insidan så kvittar det egentligen om vi själv administrerar den eller någon annan gör det. För det är samma problematik, att man skall kunna göra se säkra filöverföringar och säkra kopplingar mellan utsida och insida och då måste du egentligen göra hål i din brandvägg och det är ju en av problemställningarna.

L: Ja

PW: När vi tittar på aspekterna när det gäller molntjänstleverantörer. Som det ser ut idag så tittar vi på finansiell stabilitet, det får inte vara för litet så det kan försvinna imorgon. Den är jättecentral. Och det är en annan form av risktänkande, det är ju inte riktigt It -säkerhet i sig, utan det är ju ett övergripande rikstänkande.

L: Ja, det är klart

M: Men, finansiell kapacitet och stabilitet …Tänker ni då på att företaget skall vara stort eller att det skall vara billigt för er så kallat?

PW. Ehh stort, ehh nej inte stort, men att det skall vara finansiellt sunt.

M: Du menar att företaget skall vara etablerat så det inte försvinner imorgon??

PW: Ja precis

M: Det är inte finansiellt på det sättet att det är kostnadseffektivt för er? Att ni söker en billig lösning?

PW: Nej det är ju inte det primära.

M: Ok

L: Mm

PW: När vi tittar på en molntjänst är det ju ett sätt att undvika den administrativa funktionen, ha datorkapaciteten här men samtidigt få en bra tjänst. Så att det är….Lösningen måste vara stabil och det är på samma tema, hur är den rent Enterprise Architecture byggd? Hur är den byggd? Kan vi se att den är väldigt stabil och kan vi se

svagheter i lösningen det vill säga, Ja de har en support mellan åtta och tolv varje torsdag. Ja, den funkar ju inte så bra. Och många av de här molntjänsterna som vi tittar på är ju 24 gånger sju lösningar och det gör det ju det väldigt svårt för en viss typ av leverantörer eller så får vi acceptera att det är åtta till sjutton svensk tid. Men det är ett viktigt val.

L: ok Mm

PW: Och sen är det referenser. Och gärna då lokala referenser. För många gånger är det de säger…ja vi har en referens i Sydafrika… Ja jo, lite svårt att hälsa på kanske, men man kan ju ha skype eller något annat att prata när man pratar med dem, men det är ändå en viktig sak att vi kan se att det är någon annan som använder det vi använder så att vi inte är Betatestare, för den är livsfarlig.

L: Ja det är klart

PW: Eh Negativa erfarenheter av molntjänster…..? Vi ..vi har ju en outsourcad logistikfunktion, som kallar sig för Digistical Control Tower och de har ju ingen IT bakgrund, det är DHL som är leverantör och det har vi ju sett, vi har haft en ganska lång relation med dem nu.

L: Mm

PW: Men de är ju inte vana vi det. Och då ser man, de tänker ju inte.. riktigt ..på de här Bussiness continouty planning och disaster recovery planning, säkerhetstänket bakom. Ja..de har tre, fyra underleverantörer. Ja, hur ser de avtalen ut? Vi har ju inte avtal med dem?

M: Nä precis

PW: Hur ser deras planer ut? Hur ser deras bakgrundskontroller av personalen ut och så vidare? Och det har vi ju märkt att det är ju väldigt jobbigt när det är så. Är det en professionell molntjänstleverantör så är det betydligt lättare att jobba med den, för de förstår ju alla frågorna…

M: Jo precis

PW: Men de förstår ju inte ens. Tittar man på till exempel DHL nu som ett exempel, tittar man på deras interna IT -säkerhet och deras interna dokumentation så är den jättebra, men det är ju inte riktigt det de säljer till kunden för de är inte vana vid att vara leverantörer, så där är ju en nackdel som vi kan se.

L: Ok

PW: Vi använder ju ganska många Software as a Service, vi har precis gjort ett avtal runt ett lönesystem i Sverige. Och vi har ju utvecklats här, förr hade vi ju inte de kraven som vi har idag på lönesystemen.

L: Nä

Åh, eftersom det är klassificerat så högt så är ju är allting krypterat. Databasen är krypterad, backupen är krypterad. De kan administrera systemet utan att ha tillgång till data. Sådana där saker är ju jätteviktiga.

L: ja ja visst, det är klart

PW: Och så såg det inte ut innan. Det har ju varit outsoursat i många år, men nu kan vi mer, nu ställer vi högre krav.

L: Ja, jo

PW: SLT – som jag sa, det här logistik. Service now – det är en helpdesk, som vi håller på att implementera. Google Analytics.. Jag vet inte var den kvalificerar, om det är en Software as a service eller en Platform as a service va för det är nån form av.

Ja, jag skulle vilja säga att …skillnaden mellan software och moln.. jag skulle nästan vilja skilja på de där två för moln, där känns det som… där kan man skala upp och ner. Det är något man köper.. inte per hekto, men per någonting så.. , så att man kan skruva lite på parametrarna där för hur mycket man behöver , software as a service är mer en helhetsleverans. Det är inte riktigt samma sak känns det som. Så att.. jag vet inte riktigt var Google Analytics, det är någon form av statistikfunktion för webblösningar som vi har... faktiskt . Det kan man kanske kalla Platform as a Service, jag vet inte… jag är lite osäker på… när det gäller…

M: Förlåt en fråga, ni använder inga av Googles andra tjänster, de har ju rätt många andra tjänster? Det är bara analytics ni kör?

PW: Ja och egentligen bara en test.

M: Ok

PW: Vi har egentligen inte gått in djupare på det.

M: Jaha

PW: När det gäller, publik, privat och hybrid så tycker jag publik och privat är OK, frågan är vad definitionen av privat är…

L& M: Precis, det har vi på nästa fråga här…

PW: därför den är… Därför när jag satt och funderade över det så tänkte jag. Privat måste ju vara som när vi köper vilken typ av mjukvara som helst och implementerar den internt fast har en supportorganisation som är utanför..och det är ju standard, det har vi ju nästan för allting eller… är det så att man har den internt och de externa parterna administrerar den helt och hållet via en VPN- koppling in i vårt nätverk… för det är nåt annat, ju.

M: Mm

PW: men vad är… Jag kan inte riktigt …jag hittade inte någon definition …

M: Nä, men Microsofts definition tolkade jag som att ..eh om man kör bara lokalt, alltså inte inom molnet, så ligger all data på ett ställe på en server exempelvis, och om du kör ett privat moln kan lite av data ligga på en server och lite data på en annan server och lite på en annan server fast fortfarande inom företaget och allt kan flyttas runt.

PW: ja ja ja

M: och då är det klassat som ett moln. Det var hans definition av..

PW: Ja ja ok det behöver ju inte vara fel…det låter ju rimligt…fast det har vi inte

M: Så skillnaden är liksom alltså att det mer utspritt på fler servrar på en molntjänst

PW: Ja ja det låter ju rimligt i och för sig, men den definitionen hittade jag inte, jag funderade ..vi har ju inte haft det på det viset, utan det är ju mjukvaror som vi installerar på våra interna servrar, låt vara att de är VM ware baserade , så att de är virtuella och det kan vara klusters och det kan vara allt möjligt, men inte den typen av tanke där du sprider det på olika kapaciteter till exempel mellan olika världsdelar…eller där det finns ledig kapacitet , det har vi ju inte och det tror jag inte ens vi är nära att implementera heller.

L: Nä…

PW: Hybrid ..mellan det här publika och privata..det är mer tveksamt . Jag är mer tveksam överhuvudtaget till att ha en logik liggande här inne och överföringen från insida till utsida och tvärtom. Kan jag föredra något så är det insida till utsida. Nästan aldrig utsida och plocka data på insidan , det är en betydligt större säkerhetsrisk så att

hybrid…nja kanske….men vi säger aldrig nej. Det kan vara hur känslig information som helst egentligen, men vi säger inte i grunden nej vi tittar på möjligheterna att skydda den på ett åtminstone lika bra sätt som vi kan internt och då måste man ju skydda den från access av administratörer den data som finns där, men det kan vara Ok. Det kan vara helt ok.

L: Mm

PW : Ehh ..Största säkerhetsriskerna med molntjänster….ett konstigt svar kanske…Men det vi har upptäckt, det är att ..de som är underleverantörer.. för normalt sett gör du ett avtal med en molntjänstleverantör och sen outsourcar de driften av hela miljön och administrationen av infrastrukturen till nån annan och de har ju vi inga avtal med. Så våra frågebatterier borde egentligen gå till de också, och det gör de…och vi måste se avtalen nästan och deras SLA. Vad har de för Service Level Agreement mellan den leverantören och den leverantören som vi har som avtalspart?

M: Men hur är det? Uppger de sina underleverantörer?

PW: Ja, de får de ju göra… annars köper vi ju inget.

M: nej precis jo, jag tänkte på om de på något vis ville vara hemlig med det av någon anledning men det…

PW: J det vill gärna inte göra nåt mer med det, men jag vill till exempel se Disaster recovery planen som fungerar hela vägen ner, för om de inte ens har infrastrukturen själv, hur i hela fridens namn skall de kunna återställa

M: Nä, precis

PW: servicen om den bara försvinner. De kanske går bankrutt underleverantören, liksom en billeverantör ….som har väldigt känsliga underleverantörer med plåt eller vad det nu kan vara för nånting.. så är det ju, det är samma sak här.

L: Ja

PW: Och sen när det gäller vilken information vi kan tänka oss att lägga ut, som ja sa, egentligen allt, beroende på hur implementeringen ser ut, vi har inte den typen av restriktioner, men då måste vi ju säkerställa, vi måste förstå och se och kolla och ha rätt att auditera etappen också.

L: JA mm

PW: Säkerhetskrav när vi väljer molntjänster ….Vi kallar ju nåt CIA , det är ju det här.. konfidentialitet, integritet och tillgänglighet.

L: Mm

PW: Det är ju det som är. Och det är i grunden alltihopa och tittar vi sen på ett privat moln så är det väldigt litet.. Jag gjorde en…Och här är lite olika så finansiell status… Källkoden är vi ju intresserade av, när de säljer, jaha bara den inte finns på Sri Lanka enbart nånstans i en källare, det är ju inte så bra. Supportorganisationen , kan de då supportera oss? Kompetensen, hur har de säkerställt den, hur ser det ut i systemen med backup restore, vi tittar på insidan när vi tittar på mjukvaran. Kryptering av data om vi behöver det, det kan ju behövas på insidan också, i vissa fall kan vi själv lösa det, med SQL- kryptering eller något annat, men det kan ju behövas beroende på klassificering. Kapacitetsplanering det är ju egentligen hur systemet kan växa i förhållande till den bas vi har eller använder. Rollbaserade accessrättigheter, det är viktigt för oss att kunna ge access i olika system beroende på vad behovet är för de olika individerna. Lösenord om det nu inte är AD - integrerat eller något annat, vad är det för funktioner och hur ser komplexiteten ut, uppfyller den vår säkerhetspolicy? och gör den det inte så har det har den diskvalificerat sig redan från början. Och sen är det ju loggning, som är viktigt, vad finns det för möjligheter i systemet att se vem som gjorde vad?

L: Ja, det verkar väldigt genomtänkt.

PW: Så den här biten…ja, vi försöker ju….Och sen har vi då utsidan…och då ser ju den här listan helt annorlunda ut. Den är ju mycket mycket större. Den börjar ju likadant. Men där har vi ju lagt till underleverantörer, källkoden är ju kvar, storage, alltså får vår data lov att vara i Iran, eller får den inte vara, vad är det för rättigheter mellan olika länder, var finns vår data, vem äger den?

M: Ja, precis

PW: Det måste vi ju veta. Vi måste ju äga datat, annars kan vi ju inte lägga ut information i molnet. Leverantören kan ju inte äga det, eller som vi fråga en underleverantör, vem äger data, jo det gör då den vi har avtalet med, men det går ju att slå ihop rent juridiskt, men vi måste veta…

L: Mm

PW: Hur får vi datat? Låt säga att de går i konkurs, hur får vi tillbaka datat och i vilket format är det? Finns det några regulatory compliances? Alltså finns det några lagliga krav i olika länder beroende på var den nu finns någonstans?

L: Mm

PW: I en supportorganisation, tillgängligheten av supportorganisationen. Vad är det för SLA med underleverantören? Det vill vi se. Hur går identifieringsprocessen till? Så att hur gör man det här? Är det kunden som gör det eller är det de som gör det? Eller

M: Mm

PW: Hur hanterar vi användaradministratörer, vi ser ju gärna att vi gör det. Att de inte är controler. Bakgrundskontroller, vad är det för folk som jobbar där?, Jag menar ..är det kriminella från andra länder som vi ser som de stora eller är det nån annan? Ehh.. Kompetensen som vanligt. Sen tittar vi på helt andra saker…IPS och IDS. Hur skyddar man sin miljö med Intrusion Prevention eller Intrusion Detective. Vad har de för backuper? Men nu måste vi också veta hur många generationer backuper har de, är det det vi behöver eller är det för lite eller hur ser det ut och var lagrar de det externt? Är det ute i ett bankvalv eller är det i Kazakstan eller var sjutton är det tro och kan de kryptera backuperna?

L: Ja jo

PW: Normalt sett tittar vi ju på att kryptera det som finns på disk och då är det ju krypterat när man packar upp det också. Och Data Recovery, vi måste ju se den här processen, hur återställer man data, det måste vi också kunna se. BCP- Business continuty planning , och Disaster Recovery, det är ju vid en katastrof eller när nånting allvarligt händer , hur återskapar de miljön för oss och då vill vi se företag C:s, hur har de tänkt i vårt fall att återskapa. Och då kan det ju vara flera underleverantörer och det gör det ju känsligt. .

L: Ok, mm

PW: Datormiljön, accesskontroll, brandskydd, kylning alla de här standardgrejorna som vi har, vi måste ju se att de har också har de, hur patchar de systemet och rullar tillbaka det, antivirus, deras interna säkerhetsprocedur , penetrationstestning - hur sker det , kryptering av datat, är vi inne på igen ,kapacitetsplanering, - har de hårdvaran så att de kan växa om de får tre nya kunder eller står de helt still då eller vad händer, rollbaserade accessrättigheter, igen. Lösenord samma sak och loggning samma sak, men sen har vi administratörsaccess. Det är ju deras administratörer då, det måste vi ju förstå - vad är det för typ av access och hur kan vi skydda oss , hur segregerar de andra kunders data från vår data, det måste vi ju förstå . Vi har försökt att tänka på de flesta scenarier här men jag vet inte vad du tycker…om det här materialet..?

L: Jo, det verkar enormt genomtänkt och strukturerat . Jo, jag har ju under första halvan av terminen läst en säkerhetskurs där vi tagit upp de flesta av de punkter du berört. Det har vi ju haft jättestor nytta av också nu när vi skrivit.

PW: Jag kan säga att leverantörerna tycker det är jobbigt att svara på frågorna,

M: Jo jo

PW: Och så skall du lägga till 90 Enterprise Architecture frågor också.

L: Man förstår ju att det tar tid med den här processen…och alla förberedelser.

PW. Ja, processen, oj är den så slut? Oj, Batteriet verkar helt slut, Jag får se om jag hinner med den innan den kraschar. Var var vi? Där nere… Sen tittar på slutet vi på brandväggar , accesskontroll, Set upp, internet – hur ser det ut? Är det redundant? Stödjer det SSl eller certifikatshantering. Vad är det för typ av extranet möjligheter om man vill släppa in kunder i den här miljön och hur skyddar de sig mot Denial of Service – attacker. Så ni ser, där är 38 frågor här som vi ställer till leverantörerna. Det är väl lite grann som vi ser på molntjänster och som listan ser ut idag. Sen utvecklas det ju hela tiden så den här listan vi har den kommer ju säkert att revideras efterhand. Det är ju en krokig väg så att säga så helt plötsligt har vi en säker Platform as a Service och Infrastructure as service och jag vet att min Enterprise Architecture han börjar redan titta på och skrapa på att kunna utnyttja den typen av tjänst och då blir det ju nya säkerhetsfrågor…skulle jag gissa

L: Javisst precis, det är ju ett ständigt pågående arbete.

PW. Ja det tror jag.

L: Det slog oss också att vi skulle vilja fråga er om ni gör någon form av riskanalys innan, och det gör ni ju, eftersom ni har alla de här kraven, men kan man säga att det är någon speciell modell ni använder er av, men brukar ju prata om kvalitativ eller kvantitativ modell?

PW: Nja egentligen inte, Ja kvalitativ, ja det är ju en kombination, det är ju rätt många frågor, det är ju…kvalitativ är ju viktigt beroende på deras svar. Många gånger, det skall jag säga, av de svaren vi får in så är det god dag yxskaft, det är....antingen har de missförstått frågan eller så har de svarat väldigt bristfälligt, det betyder egentligen ingenting. Så många gånger får vi gå tillbaka en tre, fyra fem gånger för att reda ut och ha konferenser för att förstå vad de menar egentligen. Och just, underleverantörerna kan vara ganska komplext ibland att förstå hur många det finns, det kan vara tre, fyra underleverantörer. Då skall alla egentligen ha de här dokumenten också svara på det här och sen skall man sy ihop hela den här systemkartan så bara den förståelsen kan vara svår så det kan gå från väldigt lätt när det är ett väldigt väldefinierat system med en leverantör eller så kan det vara flera.

L: Tror du att leverantörer och kunder har samma syn på säkerheten eller känns det som de försöker komma undan ibland?

PW: Vissa känns det som att de vill bara svara på det här dokumentet för att svara på dokumentet och vissa känns det som att det är väldigt seriöst och oerhört bra svar så det varierar väldigt faktiskt måste jag säga.

L: Det kan jag tänka mig. Det kändes väldigt seriöst när vi pratade med en leverantör.

M: Jo, det var ju väldigt noggranna med att tänka på allting säkerhetsmässigt och han hade väldigt detaljerade svar på allting.

PW: Jo, de har ju ganska bra whitepaper och enbart genom att titta på det kan man få ganska mycket information om dem nä det gäller de bitarna.

L: Förlitar ni er på någon form av ISO?

PW: Nej, vi sneglar ju på, det finns ju …17799 och de här 27000 och 27001. Vi tittar ju på det och sneglar men det är alldeles för komplext i förhållande till den personalmängd vi har och kunna sköta de här bitarna. Det blir lite.. ribban läggs för högt, utan vi sneglar på dem och pratar med våra kollegor i branschen; Tetra Pak såklart och även Atlas Copco och andra för att förstå vilken nivå som är rimlig. Vi tittar mer praktiskt på det vad kan det betyda i praktiken. Det är ju så jag jobbar rent generellt. I den här funktionen så kan man många gånger lätt fastna i en teoretisk värld, där man skapar policys hela tiden som ingen varken läser eller utför. Därmed vill jag se att allting som jag gör har en praktisk konsekvens, som vi jobbar just ni med informationsklassificeringsmodeller och då måste den ju gå att praktiskt kunna implementera också annars blir det ju lite.. både det och en förankring uppåt , det är viktigt, så man för både mandat och en praktisk väg fram .. för vi har sett genom åren att det som är teoretiserat och inte går att implementera det är värdelöst, det är inte lönt att ha.

L: Nej det är klart..

PW: Det blir det ju många gånger med de här ISO 27000, det blir ju miljoner frågor när du sätter ihop de där , hur mycket frågor som helst, eller inte frågor men regler…det du skall bygga upp.

L: Jo. Finns det någon form av försäkring som man har möjlighet att teckna?

PW: Nä, den enda försäkringen man har är SLA, det finns ingen annan försäkring utan det är den avtalsformen som man skriver.

M: Men om det nu skulle ske en tvist vems lag är det som gäller?

PW: Det beror på var vi har skrivit avtalet. Men normalt sett när vi skriver avtal så är det i Sverige. Men sen beror det ju vem vi har skrivit avtal med. Så till exempel i vårt globala kommunikationsavtal som vi har med Orange. Där är det ju engelsk lag som gäller så det beror lite på vad det är för.. var den är skriven och hur den är skriven . Vi använder oss av en engelsk advokatfirma till väldigt många av våra avtal, men det är oftast Baker Mckenzie, men vi använder ju normalt sett svensk lag, också är det oftast skrivit i form av Corporate så vi kan använda det till alla företag C också. Vi brukar inte skriva några lokala avtal,

M: Nej

PW: För det blir tokigt, sen helt plötsligt behöver något annat land ha det och då är det bra att moderbolaget står med sin signatur.

L: Var det något annat Martin?

M: Jag vet inte…

PW: Nej det är många aspekter på säkerhet, det blir mer och mer.

L: Ja o ja, absolut. Det gäller att vara noggrann, ja det är så mycket och tänka på….Men då skickar vi våra transkriberingar innan vi publicerar intervjun?

PW: Ja, jag kan kolla bara så..att det stämmer med…

L: Så skickar vi det till dig och sen slutresultatet när det är färdigt

PW: Ja, gärna det så man ser hur andra har tänkt och vad ni drar för slutsatser av det här…

L: Ja det är självklart. Det är ju bara kul. Då tackar vi så jättemycket för…

M: BITS, Känner du till det?

PW: BITS?

M: Vi kom över det i någon form av artikel, det kan vara något som också är förlegat också för det var någon innan som vi pratade med som använde det mycket, men det är tydligen också nån form av iso…variant fast det kallas BITS. Alltså något sätt för…

L: Det är någon form av basnivå för informationssäkerhet som man inte bör underskrida på nåt vis.

PW: Typ mer en audit, internrevisionsmässigt, det är där man bör ligga när man får en revision på sig.

L: Ja, men mycket betydligt lägre än ISO

PW Ja, det låter ju intressant i och för sig. Vi mäter ju inte oss mot någonting men vi har ju externa revisioner emellanåt till exempel Ernst Young de här som går specifikt in och tittar på vissa delar. Det är klart och då påpekar de ibland en del saker som vi kanske inte helt har fått klart. Det mesta vet vi om…BITS..

L: Nåt annat Martin?

M: Ja vet inte, är det något du har tänkt på som du anser att vi missat bland våra frågor som du anser vara viktigt och som du kanske inte har nämnt sådär?

PW: När det gäller moln?

M: Ja alltså, rent säkerhetsmässigt vad det gäller molntjänster? Om det är något du tycker att vi kan ha missat?

PW: Nej det tycker jag väl i och för sig inte.

M: För våra frågor grundar ju sig ju på teori som vi har hittat i diverse artiklar och böcker i princip så det är ju det vi anser vara det viktigaste för att föra in säkerheten i molntjänster.

PW: På något sätt svarade jag kanske på lite mer än vad ni frågade på slutet, det är väl ingen som har 38 svar på de där frågorna, för det var ju ganska specifika frågor, men det är ju ganska många frågeställningar egentligen, som man måste ta hänsyn till, för att kunna få en komplett bild på vad det egentligen är man köper för någonting Jag tänkte att i stället för att dra ut något och bara svara på dem så kan vi lika bra titta på helheten. Nej det kan jag väl inte påstå….

L: Ja, det var jättebra, verkligen, vi är jätteglada för det. Vi uppfattar det lite som att det inte har uppkommit några nya risker i samband med molntjänster men att riskerna är större…men inga nya.

PW: Det är lite som jag myntade ett uttryck när jag var i London för en session, jag insåg efter ett tag att ju molnigare det blir, desto tydligare måste man vara. Det är lite grann hela tiden att har du en specifik leverantör så är det ganska lätt, men ju bluddrigare det blir desto mer tid måste jag ägna åt att säkerställa hur fakta ser ut bakom, Många kunder tror jag inte orkar det . Utan man stoppar någonstans där i början, men där ser man inte hela den skogen av risk och hot som finns bakom.

L: Så långt vi har kommit nu har vi kommit fram till att det är just avtalen som avgör. Om man är tydlig…

PW: Ja avtalen de är centrala. Så gör vi ju också att jag är ju med i avtalsprocesserna också. Så jag säkerställer ju att de svar vi fått och som vi är nöjda med. De återspeglas i avtalen. Och sen följer jag upp efteråt att det återspeglas i implementeringen också. För många gånger tappar man på vägen där, man gör den första delen sen gör man inte två eller tre. Och då kan jag se ibland att även vi internt har ett glapp där, när det gäller andra saker, service management och annat. Men jag vill gärna se alla tre stegen, så att man ser det verkligen implementerat och sen gör vi ju ibland… VI till och med har utsourcingar till Indien och annat. Då åker vi ju dit och auditerar dem och tittar hur ser det ut egentligen - vem har access och det är ju en liten kostnad i förhållande till utbildning, man får ju mäta det i förhållande till den potentiella förlusten. . om det skulle gå åt pepparn - vad händer då? Då kanske vi står där med tio tusen användare som står stilla och det är ju inget bra.

L & M: Nej det är klart! Tack så hemskt mycket för att du tog dig tid. Det var otroligt givande.

PW: Tack själva!

L: Och skulle vi komma på något mer så skickar vi ett mail.

PW: Ja det är inga problem, bara gör det.

L: Tack än en gång!

Bilaga 9 Transkribering, Informant 3, Företag A

J = Informant 3

L = Linn Bjärvall

M = Martin Ståhl

L: Vi kan börja berätta lite om oss själva. Vi går systemvetarprogrammet och skriver uppsats nu om molntjänster och säkerhet och då är vår frågeställning att vi ska undersöka vilka krav som kunder, eller vilka krav som måste uppfyllas för att kunder ska känna sig säkra när det gäller molntjänster. Vi vill gärna ha kundernas perspektiv som vi jämför med leverantörernas, så vi intervjuar både kunder och leverantörer. Om vi uppfattade det rätt så är det kundperspektivet, kundunderlaget som passar bäst

J: Ja

L: Annars har vi en intervjuguide för leverantörer också

J: OK

L: OK, men då kör vi på kundfrågorna. Skulle du vilja berätta lite kort om dig och din roll?

J: Ja, jag heter Jonas och jag har jobbat på företag A i elva år och är IT-ansvarig för koncernen. Och IT-organisationen inom företag A ser ju ut som så att jag är någon form utav intern beställare och kravställare och sedan har vi ett driftsbolag uppe i Kista som levererar till oss och där betraktas ju företag A, som vilken kund som helst. Det är ett driftsbolag som har externa kunder främst företag i läkemedels- och energi-branscherna. Och där ligger ju företag B injackat som ett utav andra externa företag, det är ju ett internt bolag, intern kund va men hanteras som vilken kund som helst med SLA och de avtal som behöver finnas. Så där kravställer jag för företag A:s del hur den interna IT-leveransen ska se ut, vilken nivå vi ska ha på säkerhet och responstider, svarstider och vad hela paketet ska innehålla.

M: Vilka tycker du är de tre viktigaste grejerna man bör tänka på vid val av molntjänst? Är det ekonomin, är det säkerheten, stabilitet?

J: Ja, den allra viktigaste eller vad sa du?

M: Ja, de tre

J: De tre viktigaste, säkerheten är ju väldigt viktig. Det är klart det är svårt att rangordna

M: Klart det är en helhetslösning

J: ja det är lite en fråga som om du vill vara blind eller döv. Vad vill du helst vara [småskratt]? Nä men ekonomi och säkerhet är ju jätteviktigt. Tillgänglighet är också viktigt men det är nog inte lika viktigt. Vi har ju inte den verksamheten som är så tidskritisk, om en tjänst är nere i några minuter, eller kanske en tjugo minuter, upp till en

tjugofem minuter att vi tappar jättestora intäkter på grund av det då. Utan vi är lite mer flexibla, har några timmar så att man kan jobba med lite andra saker undertiden i ett kortare avbrott, men det får ju inte vara hur långt som helst, de klart. Medan vissa andra branscher exempelvis cdon.com som säljer cd-skivor till privatpersoner dom kan ju inte vara utan sin internet - site i en timme eller så, det skulle vara katastrof för dom.

L: Varför vi frågar är när vi båda två kom fram till att vi ville skriva om molntjänster kom vi fram till ganska snabbt genom teori att det är i säkerheten alla frågetäcken fann.

J: Det blir ju ett praktiskt bekymmer när man har en, på vissa molntjänster som man ska köpa in, tillexempel om man säger att vi ligger till director allihopa med domänanslutna användare och så här. Då är ju företag C: s miljö byggd på att alltig ska vara integrerat och ihopagrötat till en enda tjock smet alltihopa och så finns det då mjuka länkar och hårda länkar i den här gröten så att man kommer åt allting och så vidare. Börjar man då med att lägga ut vissa tjänster externt då blir det kanske ytterligare ett lösenord som folk ska hålla reda på tillexempel om du lägger ut mailen i en molntjänst ja då ska du ha separat lösenord för det. Så ska man ha ett separat lösenord om man lägger ut ekonomisystem och så vidare och det är också något som man får tänka på. Annars tycker jag att molntjänster i grunden är bra, men det passar ju inte alla företag. Det passar väl framförallt företag som inte har någon intern kometens. Det är ju ett väldigt smidigt sätt att köpa det på.

L: Så kan man i stället fokusera på sin egen kärnverksamhet

J: Men min grundinställning är ju också i och för sig att har man kompetens så blir det alltid billigare. För man ska man köpa något så är det alltid någon annan som ska tjäna pengar och då blir det oftast i slutändan dyrare.

M: Har du några negativa erfarenheter säkerhetsmässigt utav Cloud Computing?

J: Nä, det kan jag inte säga. Nä, jag har ju själv ingen erfarenhet utav det eftersom vi kört alltig internt här själva. Men jag skulle nog välja min leverantör med rätt stor omsorg om jag skulle välja att lägga ut någonting.

M: Du skulle satsa på en stor leverantör? Är det viktigt?

J: Nä det behöver det inte va, men eftersom jag kan teknik rätt så bra själv, eftersom jag har bakgrund som tekniker så hade jag försäkrat mig genom att göra ett besök ute hos dom här personerna om det nu är en svensk man väljer . Och när man kommer ut och tittar på verksamheten och företaget som tillhandahåller dom här tjänsterna så får man rätt snabbt en magkänsla för hur företaget är organiserat. Sen finns det naturligtvis även andra system man kan luta sig mot exempelvis ISO-certifieringar, så att man får ett kvitto på att någon annan har certifierat den här leverantören, tillexem ISO27000, så blir det ett kvitto. Men annars hade jag nog tittat på hur det ser ut på arbetsplatsen och hur dom sköter det, pratat med lite folk och så får man en magkänsla. Med det är klart att då är det en molnbaserad tjänst som bygger på att det är rätt nära. Men om man köper någonting i USA så kanske man inte kan ta sig dit.

L: Använder ni er utav någon molnbaserad tjänst i dagsläget?

J: Ja det gör vi faktiskt, vi har ett nyhetsbrev som vi skickar ut till personalen. Som går via en extern internetbaserad, för det är ju det det handlar om, Cloud Computing, det går ju via internet, man köper tjänster som går genom krypterade förbindelser. Så det gör vi, nyhetsbrev använder vi. Men det är väl i princip det enda tror jag.

L: Då är det en form av Software as a Service?

J: ja, precis.

L: Men de andra varianterna, Platform as a Service och Infrastructor as a Service har inte ni det då?

J: Vi har ju inte det, nä. Det kommer upp i diskussion lite då och då. Jag tror i och för sig att vissa av våra system skulle vi kunna köra billigare om vi hade köpt in det som en tjänst utifrån. Sen finns det ett egenvärde att vi som IT-aktör på marknaden ska kunna visa för våra kunder att vi har kompetens på detta här. Då blir det rätt svårt att

ha en trovärdighet om man själv inte kör det. Om vi går ut och säger att vi kan SQL-server och vi kan Sharepoint och allt vad det nu är. Sen kör vi inte det själv internt alls i våra egna system utan köper in allting. Då undrar kunderna varför gör ni det? Ni är ju vassast på marknaden på det är. Det är mer ett trovärdighetsproblem i det här, ett egenvärde att köra saker internt även om det i det kortare perspektivet är dyrare.

L: Ja man får se det på lång sikt

J: Ja

L: Vilka ser ni som de störta säkerhetsriskerna med molntjänster?

J: Det beror lite på vilken typ det är. Det är klart lägger man ut sin bokföring och annat. Det är klart sin mail och affärssystem och allt vad det nu är. Jag kan tyvärr inte svara på det.

M: Om vi säger att ni skaffar en molntjänst skulle ni göra någon form av riskanalys vad ni skulle kunna tänka er att lägga ut? Eller skulle ni kunna tänka er att lägga ut all information? Exempel som du nämnde mail och bokföring.

J: Nu kom jag faktiskt att tänka på att vi har tänkt på att lägga ut något av det alla hemligaste, nja det är inte vårt alla hemligaste, men vårt allra känsligaste utanför företaget just på grund av att vi tror att risken för exponeringen minskar. Det handlar om våra anställningsavtal och våra lönenivåer där alltid specificeras i anställningsavtalen. Dom har vi nu valt att lägga ut utanför bolat och köpa in som en tjänst i stället. Vi tycker att det är en tryggare lösning för att vi har det så att ingen intern personal kommer åt det vilket man alltid har när man har det internt när man har administratörer, domain admins och allt vad det heter. Sen har du inte det incitamentet att det är inte så attraktiv information, det är inte så intressant information för någon som är helt utomstående. Som när det är interna som kan titta på det, jaha vad har kollegan, och hur ser kollegans villkor ut och så där. Ser du bara ett papper på en medarbetare på ett helt annat företag då är det liksom helt ointressant. Då har vi valt att lägga det utanför.

L: Hur länge har ni haft det, är det nyligen?

J: Vi har inte börjat med det, men vi har tagit beslutet att göra det och vi får göra en process nu här under våren och under sommaren, börja flytta över. Där är det väl också så att det som är viktigt för oss för säkerheten det är ju det att det är krypterade förbindelser med stark autentisering alltså att lösenord hanteras på rätt sätt och att sen att på leverantörssidan att våra uppgifter hålls helt separerade med övriga kunders. Så att där inte finns någon möjlighet att gå in.

L: Då har du själv svarat på nästa fråga vilka säkerhetskrav ni tycker är viktigast vid val av leverantör

J: Ja…Sen är det naturligtvis också att man väljer en leverantör som man bedömer har en chans att överleva i långa perspektivet, det vill säga överleva en lågkonjunktur så att kan inte lägger kritisk information hos en leverantör som går knagglet eller som har dåliga siffror, hög personalomsättning är också jättestor risk hos leverantören, hög personalomsättning är också ett tecken på att någonting inte är friskt.

M: Vi har även fått fram att många molnleverantörer använder sig utav ytterligare en leverantör, dvs en underleverantör. Är det något som ni också tittar på?

J: Nä det gör vi väl inte

M: Om tillexempel underleverantören skulle lägga ner kanske det drabbar er leverantör också

J: Jo det är klart, det är ju en risk. Men det är alltid ett ansvar som den som levererar tjänsten tar, och får lösa. Ta bara ett exempel som Telia, de har något som heter Telia säker lagring för alla deras bredbandskunder runt om i hela Sverige. Då kan man som kund gå in på Telia och aktivera ett konto men det är inte Telia själv som har den utan ett företag som heter store gate. Och skulle där bli problem med store gate då är det ett problem som Telia får ta med store gate. Som slutkund så ska man stå trygg.

L: och det skrivs in i avtalen

J: Ja, och där kan man inte som slutkund gå in och titta och där sätter ju Telia sin stämpel på den här tjänsten, dom tar ansvar för att den här fungerar och dom äventyrar ju hela sitt varumärke om dom skulle fumla med det.

M: Enligt en leverantör så är många kunder inte helt eniga om vad som menas med ett privat moln om man jämför med ett vanligt lokalt nätverk. Har du någon definition på ett privat moln?

J: Nej det har jag tyvärr inte, jag har ingen aning om vad ett privat moln är för någonting. Jagtycker att hela begreppet kring Cloud Computing är förvirrande och jag förstår att många som inte är så insatta tycker det här är lite hokus pockus. Men det är ju internetbaserade tjänster som är paketerade .

L: som man kan skala upp och ner i olika grad

J: Ja precis

L: Vad vi har kommit fram till så finns det inga nya risker utan kan liknas med Outsourcing, men skillnaden är att man har ingen aning om vara data är. Riskerna ökar på vissa plan men det finns inga nya risker som har kommit med molntjänster utan det är avtalen som skrivs mellan kunder och leverantörer som styr och avgörande för hur trygg kunden känner sig.

J: Jag tror att det kommer att bli mer och mer av detta. Alla system som man har nu och som släpps som produkter från företag C, Oracle och så vidare. De blir ju mer och mer komplexa, dom kräver och mer från företag, nu är vi ju en bransch som lever på detta så vi kan ju dom här bitarna men om vi säger dom som sitter där borta i andra huset [pekar] som håller på med fastigheter och arkitekter, rita fastigheter dom har ju inte IT som sin kärnverksamhet. Det är ju helt omöjligt för dom, om utvecklingen fortsätter som den har gjort hittills. Man kan ju inte ha en kompetens på alla system SQL Server, på exchange, på Active Directory, CRM och så vidare. Det krävs enorma interna resurser. Så jag tror att det här är helt rätt väg att gå. Då väljer man från olika leverantörer och då blir de som levererar de här molntjänsterna mer och mer specialiserade. Så kanske man väljer bara en leverantör som bara levererar e-posten och en som bara levererar ett affärssystem och en som bara levererar CAD-support för att rita fastigheter. Då blir de duktiga på det också, leverantörerna. De blir ju nischade på det . Så jag tror det är helt rätt väg att gå egentligen.

L: Har ni någon uttalad checklista som ni går igenom innan ni bestämmer er?

J: Nej det har vi inte. Eftersom vi inte har det så mycket så har vi inte det och det är ju rätt tidigt än men man vill ju att en leverantör ska vara väldigt trovärdig för att man ska lägga sin data externt. Ett väldigt starkt varumärke. För några dagar sedan så såg man att Sony fick sina PlayStation network hackat och miljoner användare som fick sina konto/kredigtkortsuppgifter stulna. Och det var ändå Sony som ändå är ett väldigt starkt varumärke.

L: Sen var det som du sa att eftersom ni har IT som kärnverksamhet så finns inte behovet.

J: När inte än så länge men allting kan förändras. Intern IT är ju inte vår kärnverksamhet utan vår kärnverksamhet är ju att göra affärer på kunder och kan vi hitta och jag är inte helt främmande ifall den här utvecklingen fortsätter, de molnbaserade tjänsterna kanske blir billigare och billigare. Det blir dyrare och dyrare att behålla kompetens internt. Det blir det även för oss. Så då är det inte omöjligt att även vi börjar titta på en molnbaserad tjänst för vårt interna behov. Vi är inte där idag men om två, tre år så kanske vi är det, det vet man inte.

M: Vi pratade lite om de här ISO -standerna innan, tror du att dom täcker in så det räcker, förlitar ni er på dem?

J: Företag A själv är ISO 9000 certifierade. Sen finns det ytterligare en certifiering som heter ISO 27000 som är för informationssäkerhet som då vi inte har på just detta dotterbolaget. Men jag tror att i grunden sätter jag rätt hög trovärdighet till ett företag som är ISO-certifierat, det gör jag. Det är kanske inte det som styr men det är alltid ett pluspoäng när man gör helhetsbedömningen. Det är ungefär som när vi gör affärer med våra kunder så

tittar kunderna naturligtvis på att vi har ett ISO-certifikat och naturligtvis stärker det helhetsbilden men jag tror inte det är det som fäller avgörandet. Men det stärker helhetsbilden av företag A att vi har certifierat oss.

L: Har ni skrivit något from av avtal eller SLA när ni tecknade er för molntjänsten.

J: När det har vi inte gjort eftersom det är två väldigt små bland annat ett nyhetsbrev som vi skickar ut till personalen, det är inget verksamhetskritiskt så det ser vi inget större behov av och skulle inte det funka eller klappa ihop fullständigt så kan vi lösa det ändå på något annat sätt. Däremot så är det viktigt nu när vi börjar lägga ut våra anställningsavtal externt att det fungerar så där kommer vi att ha ett avtal som då reglerar. Som vi då skriver i samarbete med leverantören. Så förmodligen skriver leverantören själva avtalet och så skickar de avtalet till oss för godkännande.

L: Är det bara ett SLA?

J: Nä det är inte en tjänst på det viset. Utan det är mer en, eller något form av SLA måste det vara. Det är inte jag som håller i det så jag är inte sådär jätteinsatt för det ligger under personal.

L: För som vi har försmått det så är det enda judiska avtalet

J: Ja, ja det är ju.

M: Nu är det i och för sig bara ett nyhetsbrev men vet ni om det är någon hos leverantören som kan se er data?

J: Rent tekniskt sett så tror jag att de skulle kunna göra det, även om jag nu inte tror att dom gör det eftersom dom jobbar professionellt. Men jag tror säkert dem kan göra det rent tekniskt. Det har ju faktiskt hänt en gång och det var ju inte så lyckat där vi råkade skicka ett internt nyhetsbrev till vår externa sändlista för våra kunder. För vi skickar ju ett nyhetsbrev till våra kunder med reklam och så vidare. Sen har vi ett internt nyhetsbrev där vi skriver om våra kunder och det är inte så lyckat att skicka ut denna interna information till kunderna. Det hände en gång utav misstag att vi tog ett internt nyhetsbrev och skickade till en sändlista för externa kunder. Men det var ju fel handhavandefel i systemet, den mänskliga faktorn.

M: Vet du vems lag det är som gäller om det skulle uppstå en tvist mellan er och leverantören.

J: Det kan jag inte svara på. Det är det som är det luriga när det gäller internationella avtal mellan företag i olika länder. Dom ska man inte låta vanligt folk skriva, utan det måste vara jurister som tittar på detta och avtalen så att det är synkat med lagstiftningen i båda länderna.

L: Känner du att du heller skulle välja en molntjänstleverantör från Sverige?

J: Inte nödvändigtvis, det finns ju ett par stycken väldigt starka och trovärdiga leverantörer och den ena av dem är ju företag C. Börjar de att erbjuda molntjänster i egen regi då kan jag nog tänka mig det, eller Oracle eller de riktigt starka varumärkena, IBM exempelvis, HP det finns ju en mängd olika . Det är klart att är det ett företag man inte har hört talas om innan då kanske man hellre väljer en svensk.

L: Känner du till om det finns några försäkringar man har möjlighet att teckna om leverantören inte skulle hålla de här avtalen? Finns oftast en massa avtal, men vad händer om de inte följs?

J: Problemet är att det går inte att försäkra, det går inte att sätta belopp på tjänster. En tjänst som inte fungerar och som är verksamhetskritisk för oss, jag tror aldrig att vi kan försäkra oss runt det.

L: Det blir så fall att ni väljer en annan i stället?

J: Ja, och det är det samma det här med skadestånd. Det är väldigt svårt när man har skrivit skadeståndsklausuler vilket jag vet att många företag är väldigt glada för och i vissa branscher är det väldigt praktiskt att man har det exempelvis om du köper en bil och så får du ett leveransdatum men så får du inte bilen till det datumet eftersom

det är en komponentbrist på en fabrik i japan. Så du kanske står utan bil i två månader. Då finns det ju branschpraxis om skadeståndsklausuler om att du får avräknat bilpriset eller häva köpet fast att du har betalt handpenning som man får tillbaka etcetera. Men den typen av skadeståndsklausuler är inte så vanliga i IT-branschen, och man ska vara väldigt försiktig när man använder något för det kan göra mer skada än nytta.

M: Tror ni att leverantörer och kunder ser på samma säkerhetsrisker vad det gäller molntjänster?

J: Det tror jag däremot inte utan jag tror att man har helt olika perspektiv.

M: Vad tror du skiljer dem åt?

J: Även inom leverantören så har man också olika perspektiv beroende på om man är tekniker eller säljare eller driftsansvarig för tjänsten. Det är helt olika vem man är och vilken position man har och vilken sida av bordet man sitter, så det är nog jättesvårt att svara på den frågan.

L: Tror du det är samma säkerhetskrav vid införandet av molntjänster som det är vid Outsourcing?

J: ja, det skulle jag tro.

M: Finns det någonting gällande säkerheten runt molntjänster som du känner att vi har missat? Något man som kund bör tänka på innan man väljer molntjänster.

J: Nä, det man ska vara medveten om är att man inte har någon kontroll över det. Att man släpper kontrollen och att man litar på att någon annan verkligen gör vad den ska. Men utöver det så har jag egentligen inget. Man har inga möjligheter att kontrollera något själv och det kan man ju inte göra heller. Det är mycket magkänslan som man får köra på och så skriva väldigt tydliga avtal. Sen tror jag att den största säkerhetsrisken, eller hotet när det gäller molntjänster, det är ju otydliga avtal. Och då blir det alltid diskussion om någonting händer . Eftersom företag A är en intern kund till det här bolaget i Kista som jag berättade tidigare så står vi ofta inom den problematiken själv att avtalen inte är så tydliga som de borde vara. Vilket genererar problem som vad ingår i tjänsten, hur mycket support ska vi leverera. Står det inte i vårt avtal att leverantören ska svara på om några av våra användare ringer in och ställer frågor om Office paketet tillexempel, då vet inte de om de ska svara på det eller inte. Ingår det i tjänsten eller inte, så blir det en diskussion? Supertydliga avtal tror jag är det viktigaste.

L & M: Det var vår sista fråga. Tack så mycket!

J: Tack så mycket

Bilaga 10 Transkribering, Informant 4, företag A

K= Informant 4

L = Linn Bjärvall

M = Martin Ståhl

L: Skulle du kunna berätta lite kort om dig själv?

K: Jag är anställd som konsult och har jobbat som konsult i 31 år och har mer och mer gått mot kvalitetsfrågor och har varit kvalitetsansvarig på företag A sedan 2005. Vi är ISO 9001 certifierade och det var för att vi ska kunna upprätthålla det certifikatet som jag fick den delen av min tjänst.

K: Sen ser jag att det står hur väl jag känner till Cloud Computing. Jag har inte så stor erfarenhet av det. Det känns liksom back to basics som det var på 70-talet när jag började, att man har terminaler och körde mot en server.

L: Nä, det är inte så nytt egentligen.

K: Nä, men det är ju som med alltig annat, ny teknik som man gör och då måste man döpa om det till något fancy. Det är som objektorienterad programmering, när det kom. Det var som när vi fick folk som hade gått på systemvetenskapliga programmet och kom nya i slutet av 90-talet när det var så himla poppis. Så sa de att vi gamla begrep ju ingenting, för då var det ju objektorienterad programmering. Så sa jag att jag har alltid programmerat objektorienterat för att människan är av naturen lat och har man gjort någonting en gång så gör man inte gärna om det. Det var bara det att det inte var färdigt utan vi fick göra det själv. Jag började exempelvis med datumkonvertering i assembler, det var det första jag fick göra när jag kom ut. Som jag ser det är det lätta klienter och så kör man standardiserat mot en server i stället.

M: Skillnaden är också att man kan flytta mellan servarna, inom molnet.

K: Inom molnet ja.

M: Så man kör inte ett ett till ett förhållande server- klient

K: Man har alltså en massa server så man kan flytta data och så ska man inte bry sig om var det befinner sig. Vi har ju inte jobbat med molntjänster än, det kan jag väl inte säga att vi har, för det är ju väldigt nytt. Men ur säkerhetsperspektiv så är det som med alltig annat. Har du inte kontroll över ditt data så att säga, utan det är någon annan som kontrollerar det så är du väldigt beroende av dom. Sen har vi de här hackers, kan man hacka sig in på Pentagon så kan man säkert hacka sig in på ett moln Microsoft också. Så det är ju de sakerna och som sagt eftersom inte jag vet hur de här molnen är uppbyggda, det är säkert krypteringar hit och dit, fram och tillbaks som kan styra det. Men det är ju alltid en säkerhetsrisk, naturligtvis, när man inte har allting själv. Men jag kan ju inte peka på någonting specifikt, men det är det jag skulle kunna tänka mig.

L: Vilka tycker ni är de tre viktigaste aspekterna att ta hänsyn till vid val av en molntjänstleverantör?

K: Säg så här, om jag har två alternativ. Det är någon typ av applikation och jag vill köpa en tjänst. Det första hade väl varit, nu är det i och för sig så att jag inte bara är kund utan ser det ur ett leverantörsperspektiv också. För att få effektivitet i molntjänster så blir leverantörerna mer och mer standardiserade, take it or leave it. Du kan inte göra en massa personliga anpassningar, vilket jag då som köpare kan tänka, men vadå jag som har så specifika behov, det är ingen annan som har dem. Och det är så jag har råkat ut för som konsult, för jag är mycket för standardsystem, men det jobbar ju inte vi med alls här. Och ur ett kvalitetsperspektiv så tycker jag det är mycket bättre med standardiserade grejer. För att då har man färdiga processer, färdiga rutiner. Jag tycker att kunderna får anpassa sig till det, än att leverantörerna ska anpassa sig till kunderna. För det är väldigt mycket best practice och väldigt mycket kunskap om det hos leverantörerna, vad det är folk vill ha generellt sätt. Om jag skulle köpa en tjänst skulle jag ha valt en leverantör som jag visste höll sig i ajour med vad som händer inom det området där den här applikationen ska täcka behov. Så att man inte riskerar att efter tre år så finns inte det längre, eller den är gammalmodig och så ska man behöva betala multum för att få en ny applikation. Så den kontinuerliga utvecklingen av molntjänsten. Det skulle jag se som viktigt om jag var leverantör, inte hoppa på första bästa fancy grej.

M: Så tycker du det är viktigt att det är ett stort företag, om man som kund sluter ett avtal?

K: Om jag skulle köpa in en vardagstjänst, om vi säger ett ordbehandlingsprogram eller något sådant så vill man naturligtvis att det ska vara ett etablerat företag med gott rykte. Sen finns det ju andra aspekter också, man kan ju som kund bli en del i utvecklingen av någonting. Det finns ju många som sluter sådana här partneravtal, alltså leverantörerna sluter med kunderna som då får rabatterat mot att de är med och utvecklar det hela. Det beror ju på, och tycker man då som kund att det är väldigt intressant att få vara med och påverka…då kan ju det vara en fördel för en. Men när det gäller de här vanliga hygienfaktorprodukterna som man behöver i ett företag så tycker jag nog att ett etablerat som man vet finns om tio år. Visst man säger att om tre år är det gammalt, ja men Cobolt är fortfarande det programspråk som används mest i världen. Företag är så att de byter inte ut allting vart annat, vart tredje år. Sen finns det naturligtvis tjänster som är unika och då är det ju företag som är väldigt nischat och har hög kompetens inom det. Så det beror helt och hållet på vad man har för behov.

M: Sen finns det ju leverantörer som även dom hyr in tjänster från andra, det vill säga en underleverantör

K: Ja, och det är därför det är en stor risk. Om vi tar Microsoft så är det klart att de har underleverantörer. Men de är ändå så etablerade så att dom inte går om kull om fyra, fem år.

M: Och de tar ju ansvaret om deras underleverantörer skulle göra något…

K: Ja, precis. Men som sagt beror det på vad man har för specifikt behov

L: ja, självklart

K: Ja och sen säkerhet, ja men man kan ju inte försäkra sig mot allting. Och det är ju också så att man vet ju att de här stora som har system som är känsliga i sitt moln så att säga. Att de har tänkt på det och har en hög säkerhet. Sen vissa saker har man inte de behoven av den säkerheten. Det är ju också så att man överdriver väldigt mycket, åååå…det här är jättehemligt.

M: Ja, för vissa saker kan ju vara hemligt på en plats men inte så hemligt någon annanstans. Exempelvis inom ett företag kan vissa saker vara väldigt känsliga men för en utomstående part kan samma information…

K: …inte alls vara lika känslig, nej. Och sen är det så att är det någon som vill komma åt någonting, så gör de det. Och det kan man aldrig…såvida man inte har ett handskrivet dokument som man bär med sig närmast hjärtat alltid.

L: Precis.

K: Ja det är ju så va. Det är ju många som blev så förvånade att det fanns folk på Google som kunde gå in och läsa allting vad alla hade gjort. Men det måste finnas någon som administrerar.

L: Då kanske det är lite svårt att svara på om ni har några negativa erfarenheter utav molntjänster men om ni tittar på andra…

M: Om ni har hört någon som har upplevt några negativa erfarenheter utav molntjänster säkerhetsmässigt?

K: Nä, inte specifikt utav molntjänster. Jag har inte kommit i kontakt med det så mycket, hands on. Och jag känner inte så många företag heller som har det, hands on.

L: Det har vi ju märkt, när vi gjort intervjuer att det är inte så många som kör mer än några enstaka applikationer, det vill säga inte fullt ut.

K: Nä, och vi har ju inte vad jag vet molntjänster på det där viset. Nu är vi ju så pass stort, även om vi inte är ett jätteföretag, att vi har det inom företaget. Centrala servrar och så som flyttat till Kista, som vi kör en del applikationer på men vi har ändå så att säga inhouse ändå. Så det kan jag inte säga.

L: Det finns tre olika leveransmodeller

K: Jaha

M: I princip är det Software as a Service där man hyr endast en applikation som man kan nå genom webbläsaren, sen Platform as a Service, dvs att man hyr en hel plattform som kan vara en utvecklingsplattform där kunden själv skriver sina egna applikationer till den plattformen och sen infrastruktur är ju allting.

K: Jag tänkte på det att man hyr en plattform. Jag tror att någon i huset har hyrt något sådant inom utveckling, någonting inom .NET. Dom som håller på mer med sådant tekniskt föreslog att vi skulle sätta upp en

utvecklingsserver här just i kvalitetssammanhanget för ett par år sedan. De utvecklarna struntade i det för det tog sådan tid att administrera det här internt hos oss. Så de gick hellre ut och hyrde. Det finns ju en del här som är väldigt intresserade av teknisk och sådant som sitter och labbar och så utan att det egentligen är någon kundapplikation eller så. Då var det så svårt att få till en labbserver och så, så då hyrde som in sig på en sån här i stället på en sån här extern. Men jag vet inte vad den heter.

L: Sen brukar man prata om tre typer, privat moln, publikt moln och hybridmoln.

M: Har du hört talas om dem?

K: Nä inte inom molntjänster, det kan jag inte säga men man kan ju lista ut lite vad det är för någonting.

M: Så vad tror du är skillnaden mot att ha ett privat moln mot att köra ett vanligt lokalt nätverk inom företaget?

K: Ett moln för mig är egentligen att... Här har du en leverantör som skapar ett moln utav ett antal applikationer och tjänster. Sen att du har din egen lilla bit i den här jätteserverparken där du lagrar, om vi säger att vi skulle hyra in Officepaketet från ett moln då är det publikt anser jag. Sen har du din egen lilla svär där du lagrar dina dokument som är säkra utifrån ditt perspektiv. Sen ett privat moln ser jag inte riktigt vitsen med.

L: Det är som vi säger att det är svårt att definiera det och när vi pratade med Microsoft ville han gärna att vi skulle höra med kunderna så att vi är överens.

K: Ja för är det ett privat moln så har du inte vunnit någonting. Ja för att istället för att Microsoft har Officepaketet så ska man ha ett moln för olika konstellationer och då ser jag inte att man har vunnit något på det.

M: Microsoft säger ju att de försöker sträva efter att försöka få samma definition av ett privat moln och deras definition är att i stället för att man kör ett ett till ett förhållande där varje server kör något till klienten. Så egentligen skillnaden ligger i att informationen kan flyttas mellan servarna inom företaget.

K: Men det är ju egentligen bara hur du rent tekniskt löser det. För jag menar om du kör med hårddiskar med rack och grejer. Om du har en server med 71 hårddiskar och speglingar hit och dit. Jag var projektledare i Norge och där hade man två servrar och de speglade och oberoende vad som hände och belastning och allt sådant så ska ju inte klienten, eller kunden strunta i var det fysiskt ligger.

M: Det är ju så att man har börjat sätta namn på saker även om det har funnits länge men folk vet inte riktigt vad det är eftersom de inte har hört namnet

K: Som sagt det har ju funnits länge men nu när det har blivit poppis med Cloud och moln så döper de om det till privata moln i stället för en intern serverpark.

L: Så man kan säga att det är mer som privata moln ni har när

K: Vi har ju vissa applikationer som vi kör webbaserade, vi har exempelvis Microsoft CRM-system. Där har vi lätta klienter som kör det webbaserade gränssnittet. Medan de som jobbar mycket med det de har det installerat på dina PC. Det finns både och. Vissa av applikationerna är webbaserade men allt annat har vi på våra egna.

L: Vad tror du om man tittar framåt, är det någon om dem som ni skulle kunna tänka er att använda.

K: Vi kan väl säga att för det första så är det en kostnadsfråga. Skulle det bli mycket billigare för oss att ha hela Officepaketet publikt då hade man varit intresserad av det. Sen är det också så att vi inte vill hyra in eftersom det krävs att vi har full koll. Tror i och för sig inte att det gör det men man har den känslan. Det är inte bara det att det krävs utifrån utan man vill ha kollen själv, så vi ska ha några sådana här gubbar i vita rocka som skriver på grejerna [småskrattar]. Sen är det också så att vi har i de andra delarna av företaget har man något SO, Service Office. Det har ju körts på solutions tidigare, nu har det ju köpts av ett annat företag och är mycket som en servicebyrå. Där har vi ju små privata moln åt våra kunder. Att de hyr in sig på applikationer, vi sköter driften

och allt sånt. Det är ju det gamla servicebyråtänket. Men jag tror det är svårt att övertyga. Ekonomerna skulle säkert gärna ta ett publikt om det var mycket billigare än vad vi har nu medan folket här som jobbar säkert vill hålla det själv för då kan vi göra vad vi vill.

L: Om vi tittar på riskerna vad det gäller molntjänster. Gör ni någon form av riskanalys efter någon speciell modell? Innan ni tar ett beslut att ni vill köpa en molntjänst?

K: Det skulle man säkert göra och jag som kvalitetsnisse tycker att man ska göra det. Vi gör riskanalys inför offerter, projekt etcetera. Men som nu när vi omorganiserade så hade vi en externrevision och då frågade revisorn, har ni gjort någon riskanalys för hela den här omorganisationen? Nä, men nu har man bara bestämt sig för att nu ska man göra det, och man gör ingen konsekvensanalys heller efteråt. Så på den sidan är det dåligt, man gör inte det men absolut skulle jag säga att man skulle göra det, jag skulle förorda det, definitivt.

L: Hur skulle ni göra då?

K: Om man gör en riskanalys så som jag ser det så tar man och definierar riskerna och det kan ju som sagt vara tillgänglighet, säkerhet, svarstider, alla sådana här saker som man tror kan vara en risk. Sen så klassificerar du dom och sen ser man hur stor är sannolikheten att det här inträffar och vad blir konsekvensen. Sen om man når ett visst värde så ska man göra en handlingsplan om risken inträffar. Sen är det så att man gör en riskanalys och så lägger man det till handlingarna och så kollar man aldrig upp det.

L: Men ingår det i er informationssäkerhetspolicy att göra en form av riskanalys?

K: Inte så strukturerat. Utan det enda vi har med riskanalys det är ju i affärssammanhang gentemot kund. Fast det skulle mycket väl behövas internt här också.

L: Så man går igenom alla informationsentiteter och så graderar men dem?

K: Ja det är det sätter vi gör riskanalyser på, om vi gör det. Så kan man göra oberoende om det är affärsrisk, projektrisk eller vad det är.

M: Vilka ser ni som de största säkerhetsriskerna med molntjänster?

K: Jag ser inte större säkerhetsrisker där egentligen än på alla andra typer av informationsbehandling som är digitaliserad. Det gör jag inte.

M: Finns det någon information du skulle kunna tänka dig eller inte kunna tänka dig att lägga ut i molnet? I stället för att köra det lokalt? Finns det någon information som skulle vara för känslig för att ligga i en molntjänst?

K: Inte som vi har. Vi har inte sådana extrema säkerhetsrisker. Det säger jag, men de som är personalansvariga skulle säkert aldrig lägga ut personalakterna. Nu har vi ju stoppat in de här personalakterna i Sharepoint, det har jag gjort och skrivit på ett speciellt sekretessavtal för att jag inte ska yppa den informationen. För jag har ju gått in på vart enda anställd och vet precis vad de har för anställningskontrakt och allt sånt där. Bara det, att jag har fått de har gjort att många av konsultcheferna har vägrat att släppa informationen och har det lokalt på sin PC och händer då någonting med hårddisken. Dom tycker det är säkrare att ha det i mailsystemet, i foldrar i Outlook än att ha det i vår Sharepoint för att jag är definierad resurs som dom vet har tillgång. Det är som jag sa att folk på Google går in och kollar, när man inte vet vem det är och har ett ansikte på den som har makten över data så känns det inte så. Sen finns det dem som håller på med offerter och avtal som tycker att det är för hemligt, tänk om våra konkurrenter skulle läst våra offerter. Men det är ju en helt annan sak om du kommer in på NASA, den informationen är ju mer säker. Vårt företag står ju inte och faller ifall någon läser ett anställningskontrakt en offert eller ett avtal. Så det finns inget jag skulle säga att vi skulle exkludera. Sen är det också så att vi är börsnoterade, då lever man också under offentlighetsprincipen, att vi ska ut och informera, vi kan inte vara så hemliga som IKEA och Ingvar Kamprad till exempel.

L: Så vilka krav skulle du vilja ha på molntjänstleverantörer?

K: Man ska ha möjlighet till olika nivåer utav säkerhetskontroller, med behörighetskontroller och allt det här och olika kryptering. Så att den typen av data i molnet behöver man bara sätta upp så att man kommer åt, men här för att kunna skicka och ta emot måste vi ha det krypterat. Att ha informationssäkerhetsklassat och IT-säkerhetsklassat. Vi får ju klassa dokument när vi började för tre, fyra år sedan och prata om informationssäkerhet, vi är inte mogna för det men kan börja med IT-säkerheten. Men folk har en förmåga att blanda ihop det där och tror att det är samma sak. Jag sa det att enda sättet att få folk att läsa något som man vill förmedla är att skriva att något är konfidentiellt när man kör ut det i printern.

L: När man pratar om molntjänster så brukar man dela in infrastrukturen i tre nivåer, Network level, Host level och application level. På nätverksnivån skulle man kunna säga att det är kryptering. Är det något annat?

K: Ja tror inte vi har det så mycket nu men det är ju den typen för att säkerställa när man skickar. Har man då så att säga en molntjänst med många servar och så, så kräver det mer. Sen host level, har man åtkomst eller har man inte åtkomst och sen på applikationslevel olika typer av åtkomst som jag ser det. Det är människans vilja att inte ha full kontroll som styr det tror jag. Man tror att man har betydligt större kontroll om man har det inhouse än om man har det i molnet. Men det har man ju egentligen inte.

L: Sen har vi det publika molnet om du ser någon skillnad på de olika nivåerna mot privat moln.

K: Den enda skillnaden är egentligen att behovet av kryptering ökar ju längre ifrån verksamheten det befinner sig när man skickar allt fram och tillbaks. Annars tycker jag att det är samma.

M: Sen har vi avtalen. Vet du om ni har någon speciellt checklista om ni skulle införa en molntjänst? Eller kommer ni göra en checklista när det blir aktuellt?

K: Det kommer vi säkert ha. Vi har ju gått ifrån att ha allt styrt nere i serverrummet till att nu köpa in det där vi har ett SLA gentemot dem. Just det att vi köper in alla tjänster och allt sådant där. Då har man ju definierat kraven redan för att flytta det centralt inom företaget. Jag tror inte det är så mycket andra krav egentligen, antingen har du en inhouse -leverantör eller så har du en uthouse-leverantör[småskratt]. Det kommer man garanterat att ha precis som vi kräver kravspecifikationer utav våra kunder så levererar vi kravspecifikationer om vi ska köpa in något. Det blir ju liksom en checklista.

M: Då kommer vi in på ditt ämne, ISO och så vidare. Tycker du att det räcker att ett företag har en ISO-certifiering för att klassas som säkert?

K: Nej. ISO har inget med kvalité att göra. Det är inte bara så att det inte räcker, det behövs inte alltid. Det viktiga är att man har processer och rutiner för det man gör. Det är det jag säger till alla människor, förväxla inte ISO med kvalité.

L: Intressant

K: Vi har ju ett ISO-certifikat. Det har vi för att det blev jätte hippt i mitten av 90-talet att bli ISO-certifierat. Sen är det så att kunder, i synnerhet offentliga förvaltningar och i samband med ramavtal så är det så att en hel del kunder kräver att man har ett ISO-certifikat. Det är ju så att vissa kunder kräver det men att vi har det certifikatet säger inte alls hur vi jobbar kvalitativt internt. Vi kunde haft dom processerna, rutinerna, checklistorna och kravdokumenten även om vi inte hade varit ISO-certifierade.

M: Med andra ord kan man säga att du tycker inte det spelar så stor roll om en molntjänstleverantör är certifierad eller inte.

K: Skulle jag som köpare titta på det så hade jag inte bara tittat på att de har ett certifikat. OK då jobbar de med kvalité.

M: Men det stärker kanske helhetsintrycket?

K: Ja det är klart att det gör, det är ju inget negativt att de har ett certifikat, definitivt inte. Men det borgar ju inte för att dom uppfyller dom kraven som jag har. Så man måste gå förbi det om man ska köpa och kolla, hur jobbar ni med det, vilka olika krypteringsalgoritmer har ni. Så att vifta certifikat under näsan på mig som köpare hade inte…

M: Har du hört talas om BITS som vi stött på men som det inte finns så mycket information om?

K: Nej det har jag inte.

L: Vilka avtal finns det mellan er och leverantören?

K: Om vi nu tar internt så är det SLA som vi har jämte mot vår servicebyrå del. Sen har vi även Microsoft CRM och några andra som vi har supportavtal på produkten. Sen har vi så sanslöst många egenutvecklade applikationer och det är jag extremt motståndare till som kvalitetsansvarig för då är det så i den här typen av företag där man håller på mycket med utveckling. Så är det några konsulter som tänker nu utvecklar vi en applikation och sen använder vi den här i huset. Ja, jättebra [ironi]. Sen försvinner de på uppdrag och sen slutar dom och så händer någonting fyra år senare med applikationen så är det ingen som kan någonting och inget finns dokumenterat. Jag har ingenting emot att vi utvecklar någonting internet men då ska vi ha samma krav på paketering, releasehantering, support som vi ger till våra kunder för är det på det viset så är det inga problem med egenutvecklat. Därför ska vi köpa in eftersom det finns så mycket kompetenssystem på marknaden och säkerställa att vi får support, kontinuerlig uppgradering och allt sådant. Men det är precis som vår benägenhet att köpa en molntjänst, att det är dumt att vara i händerna på någon annan.

L: Är det ett färdigt avtal eller skriver ni det tillsammans med leverantören?

K: Det SLA som jag har varit involverad i det var ju turer fram och tillbaks i nästan ett års tid innan det kom på plats. Så hade vi krav, och så sade dom att de kan ni inte få, så fall kostar det si…så det var ju under en dialog. Det var inget standardavtal. Men det skulle jag kunna tänka mig blir lättare om man från leverantörer utav molntjänster, för där är det take it or leave it. Vi kan säga om du köper ett supportavtal på en färdig applikation, som vi säger det här CRM-avtalet, där tror jag det är mycket mer standardiserat. För där köper du supporten av applikationen, köper du bara en tjänst exempelvis som är Service Office som innehåller flera applikationer, då är det lite mer av en dialog man får ha för att kunna acceptera avtalet.

M: Vet du vilket lands lagar det är som gäller om det skulle uppstå en tvist?

K: Det är ju i och för sig ett dilemma som jag inte funderade på innan om det just kommer till tvister. Men normalt sett så är det väl en köplag, och då är det ju köplagen där köpet…säg att köper jag något från USA så är det ju den lagen där som gäller för köpet och tvärt om. Så det borde gå in inom det…säg, det finns alltid en ägare till den här molntjänsten men sen kan det ändå va…det kan ju bli vanskligt eftersom det kan finnas var som helst i världen. För mig som köpare spelar det ingen roll egentligen, men inom molnleverantören kan det göra det, det kan ju vara säkerhetsaspekter, brandkrav och allt sånt som kan vara väldigt olika i olika länder. Men det förutsätter jag att molnleverantören har fixat.

L: Vet du om det finns några försäkringar man har möjlighet att teckna om man inte följer avtal?

K: Normalt sett så är det leverantören som försäkrar sig mot, för tvister och andra sådana här andra saker, om dom inte kan uppfylla kraven i dom här avtalen. Men som köpare brukar man inte…

M: …Exempelvis det finns skrivet i avtalet att om det inte är 98% tillgänglighet så…

K: …Så får man en ersättning eller avgiftsreduktion eller något sådant. Men det är ju paragrafer i avtalet, det är ju inte försäkringar som jag ser som försäkringar. Utan det är ju prestation, motprestation. Jag brukar säga att det viktiga i ett avtal är inte att man skriver vad som ingår utan vad som inte ingår. Därför det är svårt att skriva avtal med Danskar, för det är de duktiga på och kan alltid hitta ett kryphål. Därför är det viktigare att skriva vad som inte ingår. Det är samma sak för dem som säljer sådana här tjänster, du ska skriva vad som inte ingår och du ska skriva vad som är kundens ansvar. Det är det viktigaste. För att kunden förutsätter att allt som inte står, det

gäller. Det är samma sak här, det blir en massa paragrafer men sen kan du som leverantör alltid försäkra dig mot saker och ting som du inte kan styra i avtal. Jag menar om det skulle bli kärnvapenkrig och alla servar…ja sånt kan man inte skriva i avtal men det finns ju försäkringar mot sådana här saker. Det behöver inte vara så dramatiskt men jag menar att det finns saker man inte kan styra i själva avtalet. Men jag tycker inte man som kund skulle behöva någon separat försäkring för att köpa en molntjänst.

M: Tror du att kunder och leverantörer ser på säkerheten på samma sätt vad det gäller molntjänster?

K: Nej det tror jag inte.

M: Vad tror du skiljer dem åt?

K: Jag tror att många kunder är omogna när det gäller säkerhet. De flesta ser bara att för att du ska vara säker ska du ha ett rigoröst sätt när du loggar in, exempelvis tumavtryck eller något liknande. Det är ju egentligen inte det som är säkerheten, accessmöjligheten. Som jag ser det är det mer hur man skickar informationen.

M: Så du tror att kunden bara se front end medan leverantören mer ser back end?

K: Ja! Om man nu ser vanliga kunder, de flesta som köper sådana här tjänster är förmodligen inte i IT-branschen. Det är inte vi som är de typiska kunderna för sådant här, egentligen. Vi ser det säkert annorlunda. Men är du bara ett företag, vad för något som helst som köper det här så tror jag det är front end säkerheten som dom ser som det viktigaste.

M: Som vi har varit inne lite på innan. Anser du att det finns stora likheter med Outsourcing och molntjänster?

K: Ja, jag tycker att det är samma för att om du outsourcar eller om du köper in dit på ett moln så har du släppt den omedelbara kontrollen. Så jag ser ingen skillnad på det.

M & L: Tack så mycket för att du tog dig tid

K: Det var ingen fara, det var bara trevligt.

Referenser

Almulla, S.A. & Yeun, C.Y., 2010. Cloud Computing Security Management. *Second International Conference on Engineering System Management and Applications*.

Amazon, 2008. *Amazon EC2 Service Level Agreement*. [Online] Available at: http://aws.amazon.com/ec2-sla/ [Accessed 14 May 2011].

Amazon, 2011. *AWS Customer Agreement*. [Online] Available at: http://aws.amazon.com/agreement/ [Accessed 08 April 2011].

Ambrose, W., Niclas, D. & Athley, S., 2010. Cloud Computing - Security Risks, SLA and Trust.

Archer, J. et al., 2010. Top Threats to Cloud Computing V1.0. *Cloud Security Alliance*.

Augustson, M. & Sten, V.B., 1999. *Outsourcing av IT - tjänster*. Stockholm: Industrilitteratur.

Calder, A. & Watkins, S., 2008. *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002*. 4th ed. London and Philadelphia: Kogan Page.

Covert, E. & Nielsen, F., 2005. Measuring Risk Using Existing Frameworks. *Information Security Journal: A Global Perspective*, 14, pp.21-25.

ENISA, 2009. Cloud Computing: Benefits, risks and recommendations for information security. *European Network and Information Security*.

Forsén, K., 2010. Molntjänster - Ta kontroll över molnet. *Steria*.

Gerhard, P., 2008. *Köprättens grunder*. 10th ed. Liber.

Glaad, M., 2011. Skiftet kommer sakta men säkert. *Cloud Magazine*.

Gollmann, D., 2006. *Computer Security*. JOHN WILEY & SONS.

Google, 2011. *Google Apps Service Level Agreement*. [Online] Available at: http://www.google.com/apps/intl/en/terms/sla.html [Accessed 15 May 2011].

Google, 2011. *Google Terms of Service*. [Online] Available at: http://www.google.com/apps/intl/en/terms/user_terms.html [Accessed 08 April 2011].

Hamilton, G., 1996. *Risk Management 2000*. 2nd ed. Studentlitteratur.

Harauz, J., Kaufman, L.M. & Potter, B., 2009. Data Security in the World of Cloud Computing. *It All Depends*, 7, pp.61-64.

Henriksson, S., 2000. Utvärdering av IPSec och SSL.

Hofmann, P. & Woods, D., 2010. Cloud Computing: The Limits of Public Clouds for Business Applications. *IEEE Internet Computing*, 14, pp.90-93.

Holme, I.M. & Solvang, B.K., 1997. *Forskningsmetodik*. 2nd ed. Lund: Studentlitteratur AB.

IBM, 2007. Virtualization in Education. *IBM Global Education*.

ISO27000, 2007. *The ISO 27000 Directory*. [Online] Available at: http://www.27000.org/ [Accessed 16 May 2011].

Jacobsen, D.I., 2002. *Vad, hur och varför?* 1st ed. Lund: Studentlitteratur AB.

Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L.L., 2009. On Technical Security Issues in Cloud Computing. *International Conference on Cloud Computing*, pp.109-16.

Julisch, K. & Hall, M., 2010. Security and Control in the Cloud. *Information Security Journal: A Global Perspective*, 19, pp.299-309.

Kandukuri, B.R., Paturi, R.V. & Rakshit, A., 2009. Cloud Security Issues. *IEEE International Conference on Services Computing*, pp.517-20.

Krawczyk, H., Bellare, M. & Canetti, R., 1997. HMAC: Keyed-Hashing for Message Authentication.

Krutz, R.L. & Russel, V.D., 2010. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Indianapolis: Wiley publishing.

Lesk, M., Stytz, M.R. & Trope, R.L., 2005. Averting Security Missteps in Outsourcing. *Digital Protection*, pp.70-73.

Magnusson, S.E., 1999. Integrerad regional riskbedömning och riskhantering.

Mather, T., Kumaraswamy, S. & Latif, S., 2009. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. First Edition ed. Sebastopol: O'Reilly.

Microsoft, 2010. *Service Level Agreements*. [Online] Available at: http://www.microsoft.com/windowsazure/sla/ [Accessed 14 May 2011].

Olsson, S.H., 2009. *Från servicebyrå till moln*. Definitivus AB.

Ramgovind, S., Eloff, M.M. & Smith, E., 2010. The Management of Security in Cloud Computing.

Rienecker, L. & Jørgensen, P.S., 2008. *Att skriva en bra uppsats*. 2nd ed. Malmö: Liber.

Rosengren, L., 2008. *Så tycker IT-cheferna om cloud computing*. [Online] Available at: http://www.idg.se/2.1085/1.187989/sa-tycker-it-cheferna-om-cloud-computing [Accessed 17 March 2011].

Schött, K., Melin, L., Strand, H. & Moberg, B., 2007. *Studentens skrivhandbok*. 2nd ed. Stockholm: Liber.

Somashekar, S., 2010. Opportunities for the Cloud in the Enterprise. *CA*.

Sparrow, E., 2003. *Successful IT Outsourcing*. London: Springer-Verlag.

Srinivasamurthy, S. & Liu, D.Q., 2010. Survey on Cloud Computing Security.

Svenska Akademiens ordlista över svenska språket, 1998. Svenska Akademien.

Wei, Y. & Blake, M.B., 2010. Service-Oriented Computing and Cloud Computing. *Web-Scale Workflow*.