LUNDS UNIVERSITET

Säkerhet i molnet

Vilka är molntjänstleverantörernas och kundernas ställningstagande kring säkerheten i molnet?

Kandidatuppsats, 15 högskolepoäng, SYSK01 i informatik

Framlagd:	Juni, 2011
Författare:	Fisnik Qeriqi
	Rebin Osman Taha
	Amir Dzindo
Handledare:	Anders Svensson
Examinatorer:	Hans Lundin
	Markus Lahtinen

Abstrakt

Titel:	Vilka är molntjänstleverantörernas och kundernas ställningstagande kring säkerheten i molnet?
Författare:	Fisnik Qeriqi Rebin Osman Taha Amir Dzindo
Utgivare:	Institutionen för informatik
Handledare:	Anders Svensson
Examinatorer:	Hans Lundin Markus Lahtinen
Publiceringsår:	2011
Uppsatstyp:	Kandidatuppsats 15 Hp
Språk:	Svenska
Nyckelord:	Datormoln, moln, Cloud computing, datasäkerhet, SaaS, PaaS, IaaS

Abstrakt

Datormoln är en teknik baserad på användning av applikationer och data över Internet. Molnet som det även kallas erbjuder användarna resurser och tjänster på Internet som exempelvis lagring, applikationer och processorkraft. Tekniken har sina fördelar så som låga IT-kostnader för företag. Ett omtalat och diskuterat ämne är säkerheten kring molnet, det är denna aspekt arbetet kommer att beröra. Denna uppsats kommer att svara på frågan: *Vilka är molntjänstleverantörernas och kundernas ställningstagande kring säkerheten i datormolnet?* För att kunna besvara frågan har det utförts en insamling av teori samt teoretisk granskning för att utesluta fakta som inte är relevant för vår forskningsfråga. I uppsatsen har den empiriska datan samlats in via enkätundersökningar som har besvarats av VD, drifttekniker och IT-chefer för vardera företag som bedriver sin verksamhet i Sverige. Undersökningens resultat visar att ställningstagandena kring säkerheten i molnet är likt på många punkter angående säkerhetsaspekter men det finns skillnader kring vissa aspekter på hur molnleverantörerna och kunderna ställer sig till säkerheten samt vilka hot vardera part anser vara störst mot molnet.

Innehållsförteckning

1 Inledning

I inledningen presenteras bakgrund till vårt valda ämne samt vår forskningsfråga som vi kommer fram till genom att formulera kring de valda problemen. Detta för att läsaren ska få en bättre inblick i vårt forskningsområde. Syftet, avgränsning och hur vi angriper uppsatsen presenteras.

1.1 Bakgrund

Cloud computing eller datormolnet som det heter på svenska, är en teknik som är baserad på användning av datorer och applikationer över Internet. Med denna teknik kan användare tillhandahålla resurser som exempelvis lagring och funktioner genom tjänster på Internet (Rittinghouse och Ransome 2010). Datormolnet kan kort definieras som en samling IT-resurser som görs tillgängliga av molnleverantörer på användarens begäran (Brendl, 2010).

Det som skiljer traditionell datoranvändande från molntjänster är att programvaran behöver inte vara installerad på en persondator. Programvaran kan befinna sig i ett distanserat datacenter och ändå användas via Internet utan att behöva installeras på datorn. På grund av de tekniska möjligheterna finns det ett stort intresse för datormolnet samt att det leder till nya möjligheter med datoranvändandet. (Mirashe och Kalyankar, 2010)

Datormolnet erbjuder många fördelar och en av dessa är att företagen kan i förväg beräkna sin IT-kostnad. Men det finns även omdiskuterade brister i datormolnet och en omtalad brist är säkerheten. Säkerheten i datormolnet är det som vi blev intresserade av att undersöka om.

1.2 Problemformulering

Säkerheten i datormolnet har inte utvecklats i samma takt som intresset för implementering av en molnlösning. En undersökning av Cloud Security Alliance (CSA) och IEEE visar att företag i olika sektorer är ivriga att gå ut i molnet men att säkerheten behöver utvecklas för att locka företag att införa molnlösningar, då potentiella användare väntar på bättre lösningar och standards kring säkerheten innan de väljer att ta steget ut i molnet. (Subashini och Kavitha, 2010).

Datasäkerhet går ut på att skydda data samt att denna skall vara tillgänglig. I datormolnet läggs resurser ut i stora datacentraler där mängder av data samlas vilket leder till att kundens integritet kan bli sårbar. Detta innebär att det uppstår nya utmaningar för säkerheten. (Wang och Ren 2010). Användare av molntjänster förlorar alltså kontrollen av sin information när den flyttas ut till ett datacenter som kontrolleras av någon annan. Då företag har olika data i

sina informationssystem är kundernas behov av säkerhet varierande. Detta innebär att molnleverantörer kan ha varierande säkerhetskrav att uppfylla för att skapa en säker miljö. Samspelet mellan kunder och leverantörer kan påverka datasäkerheten i molnet. Dessa faktorer ser vi som en barriär som vi vill veta mer om. Det kan finnas intressanta synpunkter och åsikter från molntjänstleverantörer och kunder vad gäller säkerheten i molnet. Med synpunkter och åsikter menar vi det de anser vara viktigt att ta hänsyn till och de åtgärder de vidtar för att göra molntjänster säkrare. Därför lyder vår forskningsfråga:

Vilka är molntjänstleverantörernas och kundernas ställningstagande kring säkerheten i datormolnet?

För att besvara forskningsfrågan har vi fokuserat på tre delar, det vill säga tre säkerhetsaspekter inom molnet som vi ska undersöka för att få en helhetssyn av vad de anser om säkerheten i datormolnet. Vi utgår från och söker ställningstagande kring följande delfrågor:

- Vilka är leverantörers och kunders ställningstagande kring integritet, konfidentialitet och tillgänglighet?

- Vilka är leverantörernas och kundernas ställningstagande kring datalokaliseringen och de juridiska frågorna som uppkommer med molntjänster och på vilka sätt löser de detta?

- Hur pass viktigt är förtroendet mellan leverantörerna och kunderna för att uppfylla den säkerhet som krävs i datormolnet?

Vi har utifrån litteraturen och tidigare genomförda undersökningar utformat vår undersökningsmodell och utifrån den tagit de aspekter vi tycker utgör säkerheten i molnet. Dessa aspekter är viktiga att ta hänsyn till då litteraturen och tidigare genomförda undersökningar anser att dessa är vanliga säkerhetsproblem och därmed säkerhetsfrågor som leverantörer och kunder bör ta hänsyn till.

1.3 Syfte

Vårt syfte med undersökningen är att belysa molntjänstleverantörernas och kundernas synpunkter kring säkerheten i datormolnet. Det vill säga att vi vill identifiera de säkerhetsaspekter molnleverantörer och kunder anser vara av stor vikt respektive mindre vikt gällande säkerheten samt vilka åtgärder leverantörer respektive kunder utför eller bör utföra för att skapa en säkrare molnmiljö.

1.4 Avgränsningar

Vi har avgränsat oss till tre leveransmodeller: Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS) och Software-as-a-service (SaaS). Anledningen till att vi avgränsat oss till dessa är för att en molntjänst oftast levereras genom dessa leveranssätt och då vi antar att de flesta företag utgår från dessa leveransmodeller. Inom datasäkerhet har vi avgränsat oss till att inte gå djupare in i de tekniska säkerhetsåtgärderna så som kryptering, backup och auditlogg. Den djupare kunskapen om olika säkerhetsåtgärder och tekniker inom datormolnet är inte intressant för vår undersökning då det inte är detaljerna kring olika tekniker vi vill få fram inom varje ställningstagande.

2 Litteraturgenomgång

I detta kapitel presenterar vi och beskriver den litteratur vi valt att ha som stöd för vår undersökning. Vi beskriver bland annat vad datormolnet är och hur det är uppbyggt, olika säkerhetsrisker med datormolnet, de vitala delarna kring datasäkerhet, riskanalys samt en granskning av tidigare genomförda undersökningar som behandlar de områden som kopplas till vår forskningsfråga. Anledningen till att vi valt att ha genomgång av dessa delar är för att ge en inblick på vad datormoln och datasäkerhet är. Vi har även tagit upp mest kända säkerhetsbrister. Den kunskap vi får genom att få grepp om vad datormoln är och dess säkerhetsrisker ger den grund vi behöver för att förstå vilka risker leverantörerna och kunderna utsätter sig för när de hyr ut eller hyr en molntjänst. För att koppla teori till vår undersökning har vi utformat en undersökningsmodell vilken vi kommer att utgå ifrån för våra undersökningsfrågor.

2.1 Datormolnet

För att förstå varför det förekommer säkerhetsrisker inom molnet som vi tar upp här i vår litteraturgenomgång inför vår undersökning, kan det vara värdefullt att först och främst känna till hur molnet fungerar. Därför är det vårt intresse att ge en relativ kort presentation om molnet, dess olika sätt att levereras och hur datan lagras för kunden.

Molnet har olika definitioner, en omfattande definition är av Brendl (2010), där författaren definierar molnet som en samling av IT-resurser (servrar, databaser och tillämpningar) som är tillgängliga på begäran (on-demand) av kunden, som sköts och levereras av en molntjänstleverantör genom Internet och är en resurssammanslagning mellan flera användare. (Brendl, 2010).

Molnet är en konstruktion som tillåter användaren att komma åt applikationer som är placerade på ett annat ställe än det datorn befinner sig, oftast är det en applikation som finns på ett distanserat datacenter. Molnet omfattar flera servrar och flera nätverk som är sammankopplade via Internet. Datorerna som är länkade i datormolnet kan vara persondatorer eller nätverksservrar och kan vara offentliga eller privata. (Rittinghouse och Ransome, 2010). Molnet är tillgängligt för alla som har tillgång till Internet oberoende det geografiska läget. Alla behöriga användare kan komma åt dokument och program från vilken dator som helst via webbläsaren. Infrastrukturen och den teknik som används finns bakom molnet och är osynlig för användaren. (Mirashe och Kalyankar, 2010; Rittinghouse och Ransome, 2010).

Datormolnet kan erbjudas genom tre olika leveranstjänstmodeller, *SaaS*, *PaaS* och *IaaS*. Alla dessa modeller har alla olika egenskaper och används för olika ändamål.

2.1.1 SaaS – Software as a Service

Leveranstjänstmodellen som omfattar leverans av programvara på nätet är SaaS och står för *software-as-a-service*. Genom traditionell datoranvändning installerar användaren en programvara på persondatorn och applikationen kan endast användas på den dator programvaran är installerad på, men så är inte fallet med en SaaS-tjänst. SaaS innebär att användaren kan använda sig av en programvara på Internet direkt via webbläsaren från vilken dator som helst oberoende av vart användaren befinner sig. (Rittinghouse och Ransome, 2010). Exempel på SaaS-tjänster är Google Docs och webbmailtjänster som Hotmail.com (Julisch och Hall, 2010). De som kan bli ideala användare för SaaS är de som vill utföra en så simpel uppgift som möjligt utan större interaktion med andra system. (Velte T, Velte A och Elsenpeter, 2010).

2.1.2 PaaS – Platform as a Service

Den andra leveranstjänstmodellen avser plattform för att bygga och driva egna anpassade webbaserade applikationer, ett begrepp som kallas *Platform-as-a-Service* (PaaS). Här kan kunderna använda utvecklingsverktyg för att utveckla egna applikationer genom applikationens programmeringsgränssnitt (API). Exempel på PaaS är Microsoft Azure och Google Apps (Julisch och Hall, 2010). PaaS- modellen innebär alla de faciliteter som krävs för att stödja hela livscykeln, för att bygga och leverera webbapplikationer och tjänster helt tillgängliga från Internet. Dessa tjänster kan användas utan att behöva laddas ned eller installeras. (Rittinghouse och Ransome, 2010).

2.1.3 IaaS – Infrastructure as a Service

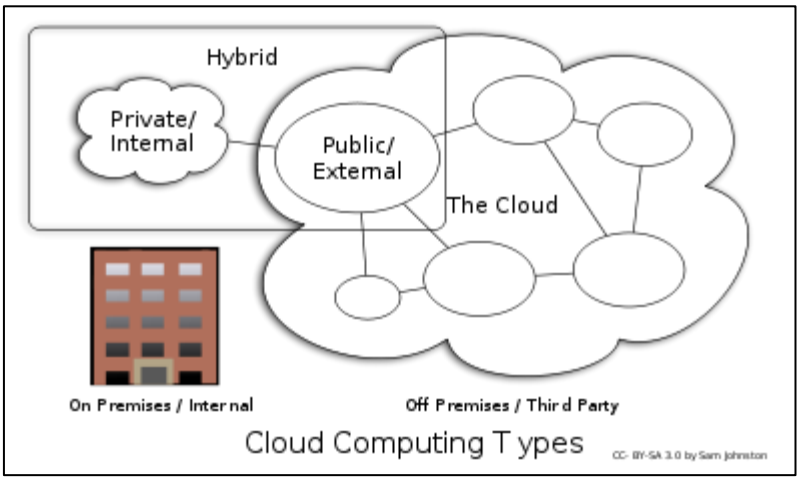
IaaS står för *infrastructure-as-a*-service och är en leverans av IT-infrastruktur. Det är en fördefinierad och standardiserad infrastruktur som är optimerad efter kundens applikationer. Användare av IaaS behöver inte ha något datacenterutrymme, servrar, programvara, nätverk, IT- utrustning etcetera i sina lokaler. Som kund kan du istället hyra dessa tjänster och debiteras endast för de förbrukade resurserna. (Rittinghouse och Ransome, 2010).

2.1.4 Publikt, privat och hybrid moln

Datacentret där hårdvara, mjukvara och data lagras kallas för ett moln. Dessa moln har tre olika lagringsvarianter, publika moln, privata moln och hybrida moln. I ett *publikt moln*, delas datorresurser med andra företag i ett gemensamt datacenter utanför organisationen.
Detta innebär att du inte har någon kännedom eller kontroll över var resurserna körs (Rittinghouse och Ransome, 2010).

Termen *privat moln* hänvisar till interna datacenter av en verksamhet eller organisation där data inte är tillgänglig för allmänheten. Detta innebär att användaren har en molnlösning som bara används internt men användaren kan även komma åt tjänsterna från alla geografiska lägen så länge användaren har en Internetanslutning och rätt till åtkomst av tjänsten. (Armbrust, Fox, Griffith, 2009).

Hybrid moln är en kombination av både publikt och privat moln. Det som gör hybridlagringen attraktiv är möjligheten att lagra känslig data i den privata delen av molnet och samtidigt kunna utnyttja den elastiska kapaciteten och kostnadseffektiviteten för lagring av mindre känslig data i den publika delen av molnet. En annan fördel med det hybrida molnet är att de är användbara för arkivering och backupfunktioner. (Mirashe och Kalyankar, 2010)



Figur 2.1 Lagringsvarianter (Mirashe och Kalyankar, 2010)

Figur 2.1 visar en överblick av de olika varianterna inom moln. I ett publikt moln delas resurserna i ett gemensamt datacenter. Privata moln innebär att användaren har ett internt datormoln som inte är tillgängligt för obehöriga. Hybrida moln är en kombination av de två ovan nämnda varianterna.

2.1.5 Fördelar och nackdelar med molntjänster

Den molnbaserade arkitekturen levererar en rad möjligheter där företag kan driva sin verksamhet med hjälp av molntjänster. Det är viktigt för oss att kort analysera de för- och nackdelar som följer med genom att implementera en molntjänst. Företagens intresse för molnet har ökat de senaste åren på grund av kostnadsbesparingar, lägre infrastruktur- och mjukvarukostnader, omedelbara programvaruuppdateringar, obegränsad datalagringskapacitet, på begäran (on-demand) tjänster för olika krav och andra fördelar för företag att gå ut till molntjänster (Mirashe och Kalyankar, 2010; Farell, 2010; Julisch och Hall, 2010).

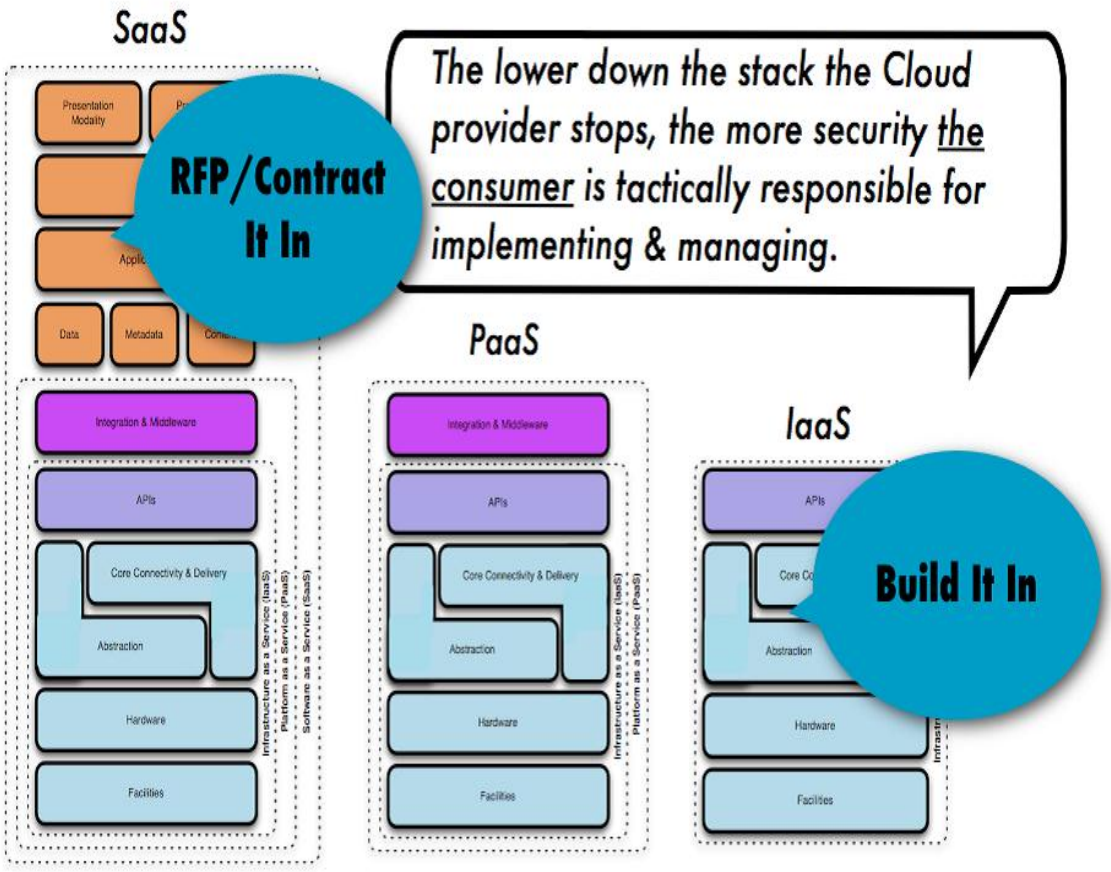
Det förekommer även en del nackdelar med molntjänster så som behovet av Internetanslutning och säkerhet. I en inte allt för avlägsen framtid kommer sårbarheterna för virus, hackare och cyberattacker att öka på grund av kriminella eller terrorister som kommer att se detta som en ny möjlighet för att försöka stjäla privat information eller sabotera tjänster. (Bisong och Rahman, 2011). Säkerheten i datormolnet är flitigt omdiskuterad för de potentiella hot arkitekturen står inför på grund av sina sårbarheter. Då kunder hyr en molntjänst lagras data inom ett moln och att lagra data utan att ha egen kontroll över datan kan öka behovet av en hög datasäkerhet.

2.2 Datasäkerhet i molnet

I detta delkapitel beskriver vi hur datasäkerheten ser ut i molnet och vi definierar även vad datasäkerhet innebär. Vi har valt att utgå från datasäkerhet och kända säkerhetsaspekter då vi funnit att sårbarheterna och hoten som finns mot molnet inte skiljer sig avsevärt från vanlig datasäkerhet. Efter att ha studerat kring molnets säkerhetsrisker belyser forskare att de flesta säkerhetsaspekter är förknippade med datasäkerhet, därför har vi tagit hänsyn till detta för vårt urval av teori samt utformning av undersökningsfrågor. Då vi söker leverantörernas samt kundernas ställningstagande kring säkerheten i molnet är det lämpligt för oss att finna parternas attityder kring datasäkerheten. Vidare beskriver vi i detta kapitel de olika säkerhetsbegreppen och de åtgärder som bör utföras för att göra systemen säkra. Vi tar upp de begrepp och åtgärder som är relevanta för vår forskningsfråga. Vi går inte djupt in i de tekniska säkerhetsåtgärderna utan enbart nämner och utför en kort beskrivning av de allra viktigaste säkerhetsåtgärderna som är relevanta för molnet.

Datasäkerhet i molnet är för det mesta lik den datasäkerhet som finns i vilken IT miljö som helst men på grund av leveranstjänstmodeller och den teknik som används för molntjänster kan datormolnet bidra till annorlunda risker än traditionella IT-lösningar (Brunette och Mogull, 2009). Säkerhetsansvaret mellan molntjänstleverantören och kunden skiljer sig beroende på vilken leveranstjänstmodell kunden väljer. De olika modellerna har även olika säkerhetsmöjligheter i molnmiljön (Subashini och Kavitha, 2010).

En färdigintegrerad säkerhet i molntjänsten uppfattas ofta som stel. Ju mer säkerhet som leverantören står för och integrerar, desto mindre möjligheter har kunderna för en utbyggnad av tjänsten i de fall detta skulle önskas (Brunette och Mogull, 2009).



Figur 2.2 säkerhetsfördelning i leveranstjänstmodellerna (Brunette och Mogull, 2009)

Figuren 2.2 visar de olika leveranstjänstmodellerna samt vilken säkerhet som följer med dem. Den förklarar även att ju längre ner i skikten leverantören slutar ta ansvar desto mer säkerhet är kunden ansvarig för att genomföra och förvalta. Detta ansvar behandlas i avtal mellan kund och leverantör. Det bestäms i avtal till vilket skikt eller servicenivå leverantören ska säkra molntjänsten, resten av säkerheten är kundens ansvar (Hosseini, Sommerville och Siriam, 2010).

IaaS ger få programliknande funktioner med mindre kapacitet och funktionsduglighet, men det ger enorma utbyggbarhetsmöjligheter. Säkerheten är väldigt svag i detta skikt eftersom infrastrukturen förväntar att säkerheten i de två övre skikten, det vill säga operativsystemet, applikationer och innehållet tas hand om av kunden (Mell och Grance, 2009). Samtidigt som säkerheten är svag i *IaaS* har utvecklaren eller kunden bättre kontroll då de kan anpassa säkerheten efter sin tjänst (Farell, 2010).

Väljer kunder *PaaS* och leverantörerna slutar ta ansvar för säkerheten i detta skikt måste kunderna själv ta ansvar för resterande säkerhet och utvecklingen av mjukvara. *PaaS* erbjuder i allmänhet mindre integrerade funktioner eftersom den är utformad så att utvecklare kan bygga egna

applikationer på plattformen och är därför mer utbyggbar än *SaaS* (Brunette och Mogull, 2009).

SaaS innehåller mer färdigintegrerad säkerhet där kunden själv inte kan bygga ut denna i lika stor utsträckning. Denna modell är lite stelare på grund av att den har väldigt låg utbyggbarhet, det vill säga att kunderna inte har så stora möjligheter att påverka och ytterligare bygga ut tjänsten (Brunette och Mogull, 2009). I *SaaS* är kunden beroende av att leverantören utför korrekta säkerhetsåtgärder då leverantören är ansvarig för infrastrukturen och applikationsmjukvaran (Subashini och Kavitha, 2010).

Datasäkerhet handlar bland annat om att skydda sina tillgångar (Gollmann, 2011). För att skydda dessa måste det sättas upp vissa skydd. Gollmann (2011) anser att skydd är delat i tre delar; förebyggande, upptäckt och reaktion. I förebyggnadsfasen vidtas det åtgärder för att hindra att ens tillgångar skadas. I upptäcktsfasen vidtas det åtgärder för att upptäcka när en tillgång har skadats, hur det har skadats och vem som ligger bakom skadan. I reaktionsfasen vidtas det åtgärder som tillåter en att återställa tillgångar eller att återställa skadan av tillgångar (Gollmann, 2011). För att få en förståelse för vad säkerhet är i informationssystem och datasammanhang tar vi upp de viktigaste begreppen som utgör datasäkerhet.

2.2.1 Tillgångar och hot gällande informationssystem

Datasäkerhet är uppbyggt på samma sätt för alla arkitekturer som innefattar informationssystem, detta gäller även för molnets arkitektur. Därför är det naturligt för oss att redogöra vilka tillgångar som finns i IT-sammanhang. Det är viktigt att veta vilka tillgångar och hot som finns då leverantörer och kunder behöver vidta olika säkerhetsåtgärder för olika typer av tillgångar och hot.

Nedan beskrivs vilka tillgångar som kan finnas (Stallings och Brown, 2008):

> *Hårdvara:* All typ av hårdvara som datorsystemet består av till exempel processorer, hårddiskar och kommunikationsapparater.
>
> *Mjukvara:* Detta är tillgångar som operativsystem, verktyg och applikationer.
>
> *Data:* Filer och databaser, lösenordsfiler och annan data.
>
> *Nätverk:* Det nätverk som utgörs av routrar, linkar, bridges etc.

Datan kan ha olika typer av sårbarheter när det gäller datasäkerhet. Tillgången som organisationen har kan vara *korrupterad*, datavärden kan variera för att någon kan ha modifierat den. Den kan *läcka*, till någon som inte bör ha tillgång till

informationen. Den sista sårbarheten är att data kan vara *otillgänglig*. Tillgången till datan eller systemet blir omöjlig eller opraktisk. Dessa sårbarheter som kan inträffa orsakas av de olika hot som finns och som kan öppna upp för sårbarheter. Ett hot representerar en möjlig säkerhetsrisk mot en tillgång. (Stallings och Brown, 2008).

2.2.2 Integritet, konfidentialitet och tillgänglighet

Det är viktigt att integritet, tillgänglighet och konfidentialitet värderas högt när datasäkerhet nämns. Därför anser vi att integritet, tillgänglighet och konfidentialitet är även tre värdefulla delar som är viktiga att uppmärksamma för kunder och leverantörer när datan i molnet kan bli sårbar då integriteten, tillgängligheten samt konfidentialiteten är i ständigt hot för dess Internetbaserade arkitektur. Dessa tre delar är även vitala delar för vår undersökning då vi fokuserar på datasäkerheten och är intresserade av ställningstagande kring dessa tre vitala delar.

Konfidentialitet handlar om att skydda privat information (Dhillon, 2007). Användaren vill ha säker information samt motverka att icke-auktoriserade ska kunna läsa eller ta del av information från systemet. Konfidentialitet kan delas in i avskildhet och sekretess. Gollmann (2011) förklarar att avskildhet (privacy) står för skyddande av personlig information medan datasekretess (secrecy) står för skyddande av organisatorisk information.

Eftersom företag eller myndighet kan dela information i molnet, kan det dyka upp avskildhets- och datasekretessfrågor (Subashini och Kavitha, 2010). Några utav resultaten i samband med datasekretess är bland annat att:

- Molnet har betydande konsekvenser för att skilja åt personlig information samt för skyddandet av affärshemligheter och statlig information.

- Kundens avskildhets- och datasekretessrisker varierar beroende av villkoren och säkerhetspolicyn som stiftas av leverantörerna.

- Lagar kan tvinga en leverantör att undersöka kunduppgifter som bevis för brottslig verksamhet.

(Subashini och Kavitha, 2010)

Avskildhet och datasekretess varierar även i publika moln jämfört med privata moln med hög innehållande av känslig data. Beroende på hur känslig information kunden har, täcker publika och privata moln olika krav från kunden (Harautz, Kaufman och Potter, 2009). Molnet presenterar risker som personuppgiftsexponering samt behörighetsrättigheterna för kundernas uppgifter. Ur organisationssynvinkel presenterar molnet risker för rättsligt ansvar.

Medan konfidentialitet är relaterad till förhindrande av läsning så koncentrerar sig integritet på förhindrande av skrivning. För att kunna skriva över något måste man ha tillgång (läsning)

till en fil, integritet brukar kallas för dubbel konfidentialitet (Gollmann, 2011). Integritet kan delas in i två koncept. Det ena är dataintegritet som ser till att information och program endast förändras genom auktoriserade sätt, det vill säga att dataändringen har en befogenhet. Medan systemintegritet innebär att systemet utför den tänkta funktionen på ett felfritt sätt, fri från avsiktlig obefogad manipulation av systemet (Gollmann, 2011).

Dataintegritet kan uppnås genom fristående system med en enda databas. I distribuerade system finns det flera databaser och många applikationer. För att behålla integriteten i distribuerade system bör transaktioner bland flera källor hanteras på ett korrekt sätt. Varje applikation i ett distribuerat system bör delta i den globala transaktionen via en resurshanterare (Subashini och Kavitha, 2010). För att försäkra integritet i molnet har vissa föreslagit användandet av åtkomstkontroller och identitetsmetoder (Khan och Malluhi, 2010). Kryptografiska metoder och användande av policys måste bli mer uppmärksammade. När någon vill komma åt data, bör systemet kontrollera dess policy och enbart tillåta åtkomst om policyn är uppfylld (Subashini och Kavitha, 2010). Oftast är det inte tillräckligt att upptäcka datakorruption just när datan är åtkommen, eftersom det inte ger de riktiga garantierna för en säker molntjänst. Det kan vara för sent att återställa datan eller skadan (Wang and Ren, 2010).

Det finns ett antal attacker och hot mot informationssystem, *DoS (denial-of-Service)-attack* är ett stort sådant. En DoS-attack som slår till på systemets resurser försöker överbelasta eller krascha dess nätverkshanteringsmjukvara. En attack på en specifik applikation som en webbserver involverar ett antal valida förfrågningar. Detta gör att den begränsar serverns förmåga att kunna svara på de förfrågningar som görs utav användarna och leder till att tjänsten inte längre är tillgänglig (Stallings och Brown, 2008).

Inom informationssystem är det viktigt att få tillgång till sin data och att skydda sig mot att någon avsiktligt hindrar tillgång till datan (Dhillon, 2007). För att skydda sig mot DoS-attack och andra händelser som kan innebära att användarna inte får tillgång till information eller att den går helt förlorad, kan de enligt Dhillon (2007) använda sig av redundans, backup, återhämtningsplan eller stark mönsterigenkänning. Precis som författaren påstår är tillgängligheten svårast när det gäller att skydda sig och upptäcka i förväg.

Molntjänstleverantören kan hantera datan på flera platser i olika länder för syftet att möjliggöra en hög tillgänglighet (Subashini och Kavitha, 2010). Leverantörerna bör se till att kunderna har sina tjänster tillgängliga dygnet runt. Föreställ er ett företag som fullständigt är beroende av sin molntjänst, men där systemet är nere i flera timmar eller dagar. Affärsverksamhetens eller kundens förlust kan bli enorm om de anställda är beroende av systemet (Bisong och Rahman, 2011).

2.2.3 Åtkomstkontroll

Åtkomstkontroll är en av de vitala delarna i datasäkerhet och går ut på att kontrollera de som försöker komma åt en resurs. Definitionen av åtkomstkontroll är att förhindra obehörig användning av en resurs, samt förebygga användning av en resurs på ett otillåtet sätt. Ett allmänt problem är nätverk och den Internetbaserade miljön där det finns ett antal klientsystem, ett antal serversystem och ett antal användare som kan komma åt servrarna. Detta introducerar nya säkerhetsproblem och leder till komplexa lösningar där åtkomstkontroll inte alltid är säkert (Whitman och Mattord, 2008). Nästan allt som är förknippad med datasäkerhet har att göra med en åtkomstkontroll, en vital del i nästan varje säkerhetssystem. Åtkomstkontroll utgörs normalt utav tre delar:

- *Autentisering:* Verifikation av den identitet en användare påstås ha och den entitet som finns är valida.

- *Auktorisation:* Systemet kontrollerar och beviljar ett tillstånd för en systementitet att komma åt en systemresurs. Detta bestämmer vem som är tillåten för ett sådant syfte.

- *Audit:* Det är en självständig genomgång och utvärdering av ett systems journaler och aktiviteter för att testa funktionsdugligheten av systemens kontroll så som åtkomstkontrollen. Detta för att försäkra de säkerhetspolicyerna leverantören har för att titta på säkerhetsöverträdelser och för att föreslå ändringar i form av policyer eller kontroll.

(Whitman och Mattord, 2008).

Databastillstånd används för att bestämma vilka som är berättigade till tillgångarna. En *auditing* funktion lagrar information om vem som har åtkomst till systemresursen (Whitman och Mattord, 2008).

Genom molntjänster kan leverantörerna komma åt kundens information som lagras i molnet därför är det väldigt viktigt att det bestäms vad leverantören får göra och inte göra med kundens lagrade data. Det är därför viktigt att kunden förstår avtalen med leverantörerna och att de godkänner och accepterar villkoren för avtalen. Leverantörers policy styr hanteringen och bevarandet av kundens data (Velte et al, 2010). Ett exempel är Googles policy, där det framgår att Google kan dela med sig data med regeringen om de har en "god tro" för regeringen och att åtkomst till data är nödvändigt för en juridisk utredning. Det är även möjligt att leverantörers anställda kan komma åt kundens data utan deras tillstånd.

2.2.4 Dataintrång och den mänskliga faktorn

Eftersom data från flera olika användare är lokaliserade i en gemensam molnmiljö, blir dataintrång en möjlig potentiell attack mot alla användare i molnet (Subashini och Kavitha,

2010). I en tidigare rapport (Verizon business breach report) framgår det att externa hot i form av exempelvis attacker utgör 73 % av hoten men har minst påverkan på kunderna, det vill säga det gör minst skada. Medan den mänskliga faktorn utgör det minsta hotet men har störst påverkan, det vill säga det gör störst skada. Det som inte får glömmas är att SaaS kan vara det säkraste alternativet men att leverantörsanställda fortfarande har tillgång till och kan komma åt kundens data (Cooper, 2008, enligt Subashini och Kavitha, 2010). Leverantörer som Google och Amazon har en infrastruktur för att motstå och överleva en cyberattack, men alla leverantörer har inte den kapaciteten eller möjligheten. Moln kan bestå av flera entiteter, i en sådan konfiguration kan inget datormoln vara mer säkert än dess svagaste länk (Harautz et al, 2009).

2.2.5 Säkerhetsåtgärder – backup, kryptering och auditlogg

Detta delkapitel behandlar tre säkerhetsåtgärder som är ytterst viktiga för molntjänster. Det är viktigt att det utförs backup på datan så att den snabbt kan återställas. Det är väldigt viktigt att backupen skyddas genom kryptering. Med auditlogg spåras informationen och på så vis kompletterar dessa åtgärder varandra.

Molntjänstleverantören behöver försäkra att all känslig kunddata regelbundet backas upp för att underlätta snabb återställning i fall en katastrof skulle inträffa. Användandet av starka krypteringsarrangemang för att skydda den uppbackade datan är rekommenderad för att hindra eller förebygga eventuella olycksfall som läckage av känslig information. (Subashini och Kavitha, 2010)

Att skydda sin data som kund är viktigt när det gäller tjänster över Internet. Det är ett bra men kanske inte det mest tids-effektiva sättet att kryptera sin data innan kunden skickar det. Program som *PGP* eller *Opensource truecrypt* är exempel på program där datan kan krypteras så att enbart de med ett lösenord kan komma åt datan. Om någon försöker komma åt datan behöver de obehöriga korrekta referenser annars är allt de kommer åt oanvändbart. (Velte et al, 2010; Hosseini et al, 2010; Gollmann, 2011).

Kunden får sällan en inblick av leverantörens kontrollmiljö och måste lita på att allt stämmer mellan certifieringarna. Den här strukturen är allt mer oacceptabel för många kunder som när som helst kan hållas ansvariga för säkerheten av sina egna informationssystem eller molntjänster. (Julisch och Hall, 2010). Att tillåta offentliga auditloggs kommer att spela en viktig roll som innebär att dataägarna kommer att behöva ett sätt att bedöma risker och vinna förtroende (Wang and Ren, 2010). Ömsesidig granskning kan också hjälpa till med incidenthantering och återvinning eftersom både leverantör och kund kan vara källan eller ett offer för en attack (Chen, Paxson och Katz, 2010).

2.2.6 Datasegregation

Det är viktigt att segregera användarnas data i en ”fleranvändarmiljö” annars kan användaren bli ett offer för en attack. Med segregering menas att molntjänstleverantören separerar användarens data från andra användares data. *Multihyrande* är en av de största fördelarna och egenskaperna i datormolnet. Behörig data för flera användare kommer att vistas på samma plats. Dataintrång blir en säkerhetsrisk i en sådan miljö. En kund kan skriva en maskerad kod och införa det i applikationen. Om applikationen utför den här koden utan verifikation, finns en hög potential för intrång i andra användares data. En leveranstjänstmodell bör därför försäkras med klara gränser där varje användares data segregeras (Subashini och Kavitha, 2010). Takabi och Joshi (2010) menar att tydlig resursfördelning och tillgängliga skyddsmekanismer kan göra en skillnad för detta bekymmer.

2.2.7 Datalokalisering

En omdiskuterad säkerhetsaspekt som nämns i tidigare studier kring säkerheten i molntjänster är var kunders data lagras. Detta anser vi vara viktigt då datasäkerheten samt ansvaret för datan kan variera beroende på vart den är lagrad. Anledningen till detta är då vi undersökt att ansvaret för datan skiljer sig beroende på vart datan lagras därför är datalokalisering en viktig aspekt för oss att ställa till kunder och leverantörer.

Kunder och användare av molntjänster vet vanligtvis inte vart deras data lagras. I många fall kan detta vara eller bli ett problem. Det kan dyka upp bekymmer där användaren inte vet exakta platsen för var deras data befinner sig eller att andra kunders data finns bland den kollektivt lagrade datan (Harautz, Kaufman och Potter, 2009). Frågan om vem som är behörig till datan kan dyka upp ifall det startas en juridisk utredning mellan kund och leverantör. Detta kan skapa ett stort problem för kunden ifall värdlandet inte har lagar för att skydda känslig information eller om regeringen ändrar lagar (Bisong och Rahman, 2011; Hosseini et al, 2010). För att veta vilka lagar som gäller är det därför viktigt att ha kännedom av vart kundernas data lagras (Subashini och Kavitha, 2010; Brodkin, 2008; Zhou et al, 2010). Rättsliga beslut kommer bestämma ”vem” som är ansvarig för att säkerställa informationen i molnet. För att försäkra att sådana beslut är underrättade bör industrin själv inrätta sammanhängande policy och ledning för att identifiera och implementera rätt säkerhetsmetoder (Harautz et al, 2009).

2.2.8 Ansvar (accountability)

En förutsättning för att förstå ansvarigheten för säkerheten i molnet är att förstå skillnaden mellan begreppen ansvar och ansvarsskyldighet. Tidigare studier belyser vikten av att förstå denna skillnad då de anser att detta är en säkerhetsbrist i molnet. Denna aspekt anser vi kan vara intressant för kunderna och leverantörerna att ta hänsyn till i molnet då en molntjänstleverantör och kund arbetar parallellt genom hela livscykeln av molntjänsthyrandet,

till skillnad från vanlig informationssystemslösning där kunder får en färdig produkt och själv får ansvara för processer och drift. Vi anser även att det är en viktig aspekt att ta med då den spelar roll både för vart datan lagras samt är värdefullt som en grund för att bygga en god förtroende mellan leverantör och kunder.

Ansvar är en skyldighet att göra något enligt vissa parametrar. Kunden är ansvarsskyldig för sina tillgångar, inklusive tillgångar som har lagts ut av leverantörerna. Leverantörerna ansvarar endast för att en molntjänst beräknar uppgifter enligt vissa parametrar, men ansvarsskyldigheten förblir hos kunderna. Utmaningen blir därför hur en kund kan definiera och övervaka säkerhetsåtgärder som leverantören är ansvarig för. (Julisch och Hall, 2010)

Många leverantörer låter deras kunder konfigurera egna konton och lösenord. Detta flyttar delvis ansvarigheten tillbaka till kunden. Kunden blir ansvarig för konfigureringen, utförandet av lämplig säkerhetspolicy och leverantören förblir ansvarig för genomdrivningen av policyn via dess kontroller. Säkerhetspolicy är en formell sammanställning av regler och utövningar för att skydda känslig eller viktig systemresurs. Vid utveckling av säkerhetspolicyer bör företaget ta hänsyn till följande faktorer (Stallings och Brown, 2008):

- Värdet av tillgången som skyddas.
- Sårbarheterna av systemet.
- Potentiella hot och möjliga attacker.
- Avvägningar mellan ”lätt att använda” och säkerhet, då dessa i vissa fall motarbetar varandra.
- Avvägningar mellan kostnaderna av att införa säkerhet och säkerhetsåterställning.

Leverantörer bör implementera alla nödvändiga kontroller för att bemöta kraven från kunder. Här gör leverantörerna en bedömning om de vill bemöta kundernas krav eller riskera att förlora dem som kunder. (Julisch och Hall, 2010)

Det är både leverantören och kunden som ansvarar för att uppnå säkerhet (Brunette och Mogull, 2009). Det är en fördel att ansvarsfrågor löses innan kunden börjar migrera applikationer till molnet. (Hosseini et al, 2010)

2.2.9 Förtroende, standards och rekommendationer

För att kunna besvara vår forskningsfråga behöver vi besvara våra tre delfrågor. Då förtroende spelar en stor roll för säkerheten i molnet är det viktigt för oss att undersöka vad leverantörer och kunder anser om förtroende.

Förtroende innebär en akt av tro, förtroende och tillit till något som förväntas att uppträda eller levereras utifrån ett löfte. Det är en tro på kompetens av andra, att kunna lita på någon att ta hand om ens värdefulla tillgångar (Khan och Malluhi, 2010). Förtroende kan förknippas med säkerhet och många tror att tillit och säkerhet är synonymt. Kunden kan ifrågasätta

molnets kapacitet även om de litar på leverantörerna när det gäller molntjänster (Khan och Malluhi, 2010). Samtidigt är inte utmaningarna att ha förtroende helt bara till själva tekniken, kundernas förtroende beror även på bristen av öppenhet från leverantörer, en förlust av kontroll över datatillgångar och oklara säkerhetsgarantier (Takabi and Joshi, 2010; Khan och Malluhi, 2010). Att kontrollera egen data och egna tillgångar ger större förtroende då kunderna själva styr dessa. Säkerhetsgarantier kan bland annat erbjudas genom avtal. Att binda avtal mellan leverantör och kund genom *service level agreement* (SLA) är ett sätt att utöka förtroendet mellan bägge parter. Dataintegritet, åtkomstkontroll och kryptering är alla sätt att uppnå förtroende om en säker molntjänst.

Det finns inga lösningar på att övertyga kunder att molnet är helt pålitligt. Förtroende varierar från organisation till organisation beroende på datans värde. Ju mindre förtroende kunden har för leverantören ju mer vill kunden kontrollera sin data. En kund kan prenumerera på en IaaS-tjänst från en leverantör, lägga till en PaaS- tjänst från en annan och förvärva olika delar av SaaS från en tredje leverantör. De antaganden som alla leverantörer har om molntjänsterna påverkar den framväxande tilliten. (Takabi and Joshi, 2010).

Trovärdig säkerhet (assurance) är en viktig aspekt där det bland annat kan uttryckas som förtroende. Stallings och Brown (2008) definierar trovärdig säkerhet som den grad av förtroende någon har gentemot någon annan för att utföra en säkerhetsåtgärd. Anledningen till att det väljs en grad av förtroende är för att det är väldigt svårt och nästan omöjligt att garantera ett helt säkert system (Stallings och Brown, 2008).

Khan och Malluhi (2010) anser att det är väsentligt att leverantören följer certifieringar för att skapa ett förtroende mellan kund och leverantör. Genom att leverantören följer säkerhetsstandards och andra rekommendationer skapas ett förtroende mellan kund och leverantör (Pauley, 2010).

Det finns även en del organisationer som bildats för att lära ut det bästa sättet att utveckla säkerheten kring molnet. Dessa organisationer arbetar med standards som fokuserar på olika områden. Avtal, rekommendationer, kravvillkor och säkerhetshantering i molnet är några områden som sätts i fokus. *The cloud security alliance* (CSA) är en av de främsta och mest uppmärksammade organisationer som arbetar med frågor kring säkerhet i molnet. CSA har publicerat en uppsättning av bästa praxis och riktlinjer för organisationer att följa innan en molnimplementering. Dessa riktlinjer är i form av problemredogörelser och frågor som måste beaktas av kunden (Takabi och Joshi, 2010).

CSA gjorde en undersökning och identifierade sju större hot mot molnet (Bisong och Rahman, 2011), dessa är:

- Missbruk och usel användning av molnet
- Osäker ApplikationsProgrammeringsgränsnitt (API)
- Insiders, (så som leverantörers anställda)
- Gemensamma tekniska sårbarheter
- Dataförluster och Läckage
- Konto, Tjänst & Trafik kapning
- Okänd risk profil

Den amerikanska *NIST* (National institute of standards and technology) har skapat en säkerhetsgrupp för molnet. NIST har nyligen släppt ett utkast (guide to adopting and using security content automation protocol) som identifierar en mängd specifikationer och uttrycker säkerhetsrelaterad information (Harautz et al, 2009; Mell och Grance, 2009). Vi går inte djupare in på dessa specifikationer i denna uppsats.

Europeiska nät-och informationssäkerhet (ENISA) är en annan organisation som också publicerat en rapport om säkerhetsfrågor i datormolnet. De identifierade 35 risker för användning av datormolnet, som är uppdelat i följande kategorier (Hosseini et al, 2010):

- Policy och organisatoriska risker såsom inlåsning, förlust av styrning, utmaningar regelefterlevnad.

- Tekniska risker såsom dataläckage, distribuerade DoS-attacker, förlust av krypteringsnycklar och konflikter.

- Juridiska risker som dataskydd och mjukvara risker licensiering.

- Risker, såsom nätverksproblem, otillåten tillgång till datacenter, och naturkatastrofer.

2.4 Riskanalys

Då varje företag och organisation har varierande sårbarheter och behöver olika säkerhetsåtgärder i sina system anser vi att kunder bör göra en riskanalys för att bedöma den grad av säkerhet som de är i behov av. Vi anser inte att det är en vital del för säkerheten i molnet men det är intressant för oss att undersöka om kunderna har utfört en riskanalys.

SIG Security definierar risk som sannolikheten för att en störning som medför skada eller förlust ska inträffa. Risk kan kategoriseras efter en mängd olika kriterier, exempelvis enligt *International Electrotechnical Commision*, IEC(1995) (Engberg & Forsman, 2001):

Naturmässiga: Översvämningar, jordbävningar, stormar etc.

Teknologiska: Industrianläggningar, strukturer, transportsystem, konsumentprodukter, kemikalier etc.

Sociala: Överfall, krig, sabotage etc.

Alla företag och organisationer har olika syn och behov av säkerhet. För att ta reda på vilken säkerhet som behövs och vart företagen ska lägga vikten av säkerheten behöver de göra en riskanalys (LeVeque, 2006).

En riskanalys innebär att organisationen tar reda på sårbarheterna samt dess informationssystem och en sannolikhetsbedömning av att ett visst scenario eller attack ska ske mot sina sårbarheter. För att slutföra sin riskanalys behöver organisationen göra en riskbedömning och riskreducering. En riskbedömning innebär att det görs en bedömning av vad kostnaden av en förlust blir. Företagen behöver bedöma hur mycket kostnaden blir vid olika typer av förluster. Kostnaden kan se olika ut vid olika tillfällen och i olika former. Organisationen kan exempelvis förlora teknologisk utrustning vid brand, stöld och sabotage vilket ger en förlust som de kan beräkna i en valuta av kronor, medan den information organisationen kan förlora som finns i utrustningen är mycket svårare att bedöma som en kostnad av pengar (LeVeque, 2006; Gollmann, 2011).

LeVeque (2006) skriver att en riskanalys är ett sätt att bedöma sannolikheter för att en händelse inträffar och konsekvensen av dessa. Han tar även upp två olika metoder för att utföra en riskanalys. Dessa två är *compliance approaches* och *risk approaches.*
Compliance approaches är färdiga mallar som är standardiserade och/eller "best practice". Standardiserade mallar är metoder som är generellt accepterade och föreslagna av kunniga inom säkerhet, ett exempel på en standardiserad mall är ISO 17799. Dessa mallar beskriver hur ett företag ska gå tillväga, hur de ska tänka och vart fokusen ska ligga. I dessa mallar finns det även krav att gå efter för att kontrollera att det hålls en relativ hög säkerhet i ett system.

Att utföra en riskanalys efter standards och bäst praxis har både för och nackdelar. Fördelarna med att följa en standard är att det är enkelt, det kräver inte en långgående process av riskbedömningar och kostnads- eller vinstanalyser. En nackdel med *compliance approaches* och bäst praxis är att det inte är en självklarhet att dessa metoder leder till ett säkert system. Alla organisationer har olika behov av system och säkerheten kring den. En internationell standard eller bäst praxis är ett sätt att veta hur det ligger till i jämförelse med konkurrenter och att företagen följer de hänvisade regler och lagar som råder (LeVeque, 2006). *Risk approaches* hänvisar till att företag går igenom syftet med systemet och vad de behöver för att skydda sig mot attacker och förluster. LeVeque (2006) anser att det organisationer och företag behöver ta hänsyn till och undersöka är:

Hot - vilka hot finns?
Sårbarhet - hur sårbart är systemet eller organisationen mot dessa?
Sannolikhet - hur stor är sannolikheten att en skada eller förlust sker?
Kostnad - Vad är kostnaden av förlusten?

Organisationen måste undersöka och finna de hot som finns för organisationen och dess information i systemen. Nästa steg är att de måste undersöka hur sårbar organisationen och dess system är. Sannolikheten att en skada eller förlust sker måste undersökas och konkretiseras till ett hanterbart resultat. Slutligen måste de bedöma hur stor förlusten blir och vad det kan kosta organisationen.

2.5 Tidigare genomförda undersökningar

Vi har, förutom litteraturstöden vi valt, kommit fram till att studera ett antal olika undersökningar som tidigare gjorts kring säkerhetsfrågor i datormolnet. Undersökningarna handlar om de säkerhetsbekymmer som kan existera i molnets arkitektur. Vi valde att följa fyra säkerhetsundersökningar som behandlar detta område.

Subashini och Kavitha (2010) presenterar och kartlägger olika säkerhetsrisker som utgör ett hot mot molnet. Pauleys (2010) undersökning är till för att hjälpa företagen att bedöma leverantörernas öppenhet kring säkerhet, integritet, revision och avtal. Även Brodkin (2008) valde att undersöka olika säkerhetsproblem och betonar vikten av att kunder bör bedöma säkerhetsrisker och kräva öppenhet från leverantörer. Författaren bidrar med sju olika kritiska punkter som kunder bör uppmärksamma. Zhou, Zhang, Xie, et al (2010) undersöker leverantörernas bekymmer kring säkerhet och andra säkerhetsrelaterade aspekter. De betonar även nya iakttagelser kring dessa aspekter som bör behandlas för en säker molntjänst.

2.5.1 Undersökningarnas syfte

Vi valde att fokusera på undersökningar från olika författare där alla har målet att först och främst undersöka den skada som kan påträffa ifall kunder hyr en tjänst från en leverantör eller planerar en eventuell molnimplementering för sin verksamhet. Alla artiklar delar i stort sett ett gemensamt syfte för sin undersökning där de presenterar och betonar vikten av att uppmärksamma de hot och faror som kan finnas i molnet.

Det som är anmärkningsvärt gällande alla undersökningar vi valde att studera är att det är undersökningar som gjorts något år tidigare än vår undersökning, förutom Brodkins undersökning som är publicerad år 2008. Detta kan vara på grund av att säkerheten i molnet nyligen blivit ett stort fenomen. Det är även värt att nämna att publiceringsåret inte har någon påverkan på vår undersökning.

2.5.2 Undersökningarnas utgångspunkt och metod

- Subashini och Kavitha (2010) undersöker säkerhetsfrågor kring molnet genom att betona sårbarheterna i varje leveranstjänstmodell. Subashini och Kavitha (2010) utgår ifrån andra författares verk och standardorganisationers rapporter kring sårbarheter som kan existera i molnet. Subashini och Kavitha (2010) använder sig inte utav några intervjuer med leverantörer eller kunder, utan enbart belyser viktiga säkerhetsfrågor. Undersökningen utgår mest från teorier och litteratur angående säkerheten i molnet.

- Pauley (2010) presenterar sin undersökning genom att skapa ett protokoll i form av ett ramverk där kunderna själva kan utvärdera leverantörernas öppenhet och säkerhetsbrister. Pauley (2010) utför själv en undersökning och grundar sina frågor på olika nyckelområden baserat på olika standardorganisationers arbete. Pauley (2010) använder sig av enkätfrågor och gör en bedömning av leverantörernas öppenhet kring säkerhetsfrågor.

- Brodkin (2008) introducerar med att uttrycka att molnet är fylld med säkerhetsproblem och anser att kunder bör göra säkerhetsbedömningar av molntjänster innan de överväger att hyra en tjänst hos en leverantör. Brodkin (2008) utgår från en tidigare analys och undersökning från Gartners rapport för att bedöma säkerhetsrisker i molnet. Brodkin (2008) sammanställer Gartners sju säkerhetsfrågor.

- Zhou et al (2010) undersöker säkerhetsbekymmer utifrån leverantörens synpunkt och presenterar ytterligare element som de anser bör läggas till när det gäller säkerheten i molnet. Zhou et al (2010) utgår från olika molntjänstleverantörer samt olika teorier kring säkerhetsfrågor i molnet.

2.5.3 Undersökningarnas resultat

Undersökningsartiklarna hade varierande utgångspunkter och metoder. Trots det hade undersökningarna överensstämmande resultat med få skillnader. Vi antar att det i överlag överensstämmande resultatet beror på att undersökningarna utgår från ungefär samma undersökningssyfte. Samtliga författare förutom Pauley (2010) nämner att det är viktigt att ha en hög tillgänglighet (se tabell 2.1) och hålla molntjänsterna aktiva för kunder. Dataintegritet är en annan aspekt som är viktigt enligt undersökningarna (se tabell 2.1). Att bistå kunden och dess användare med hög integritet bör prioriteras. Samtliga författare anser att det är viktigt att hålla en hög säkerhet. Detta anser de genom att leverantörer använder sig av rätt åtkomstkontroller samt att följa olika certifieringar och säkerhetsrekommendationer. Tre av undersökningarna anser att datakonfidentialitet är viktigt, att kundernas information och att data bör kunna vara hemligt och privat i en molnmiljö. Tre av undersökningarna tyckte att datalokalisering är en juridisk fråga som bör uppmärksammas i en säker molntjänst (se tabell

2.1). Att kunderna inte känner till vart deras data befinner sig kan enligt författarna innebära juridiska problem för kunderna. Tre författare anser även att det är betydande att kontrollera både kunders och leverantörers aktiviteter. En författare anser även att kunden själv bör bestämma om de vill ha en Auditlogg eller inte.

Tabell 2.1 Resultat av undersökningarna

Säkerhetsaspekter	*Subashini och Kavitha*	*Pauley*	*Brodkin*	*Zhou et al.*
Datasäkerhet	X	X	X	X
Datalokalisering	X		X	X
Dataintegritet	X	X	X	X
Datasegregation	X		X	
Dataåtkomst	X		X	
Autentisering och auktorisering	X			
Datakonfidentialitet	X	X		X
Dataintrång	X			
Tillgänglighet	X		X	X
Backup	X		X	
Auditlogg		X	X	X
Juridiska frågor			X	X

Ovanstående tabell visar en sammanställning av alla de säkerhetsfrågor och aspekter som författarna anser är viktiga att observera som kund och leverantör. X betyder att frågan har tagits upp av författarna.

2.5.4 Våra enkätfrågor

Här nedan redovisar vi alla våra egna enkätfrågor där vi först omvandlar dem in i olika kategorier för att lättare kunna få grepp om de säkerhetsperspektiv vi valt att fokusera på. Vi har även presenterat frågorna nedan utan att ta hänsyn till vilka vi riktar vår enkätundersökning till. Vi har delat in våra frågor i två delar, första delen innehåller frågor i värdeskala och den andra delen innehåller intervjufrågor. Fullständiga enkätformulär finner ni i bilaga B2.1 och B2.2.

Tabell 2.2 Våra enkätfrågor i värdeskala

Fråga	*Kategori*	*Enkätfråga i värdeskala*
Fråga 1	Datasäkerhet	Hur säker är data i: moln?
Fråga 2	Dataintegritet	Hur viktigt är det att ingen kan ta del av data i datormolnet?
Fråga 3a	Tillgänglighet	Hur viktigt är det att tjänster alltid är tillgängliga?
Fråga 3b	Datasäkerhet	Hur viktigt är det att tjänster alltid är Funktionella?
Fråga 3c	Säkerhet	Hur viktigt är det att de tjänster som erbjuds alltid är Säkra?
Fråga 4	Datalokaliser-ing	Hur viktigt är det att man vet vart data/information lagras?
Fråga 5	Backup	Hur viktigt är det att man gör regelbunden backup på data/informationen?
Fråga 6	Ansvarighet	Hur viktigt är det med ansvarighet?
Fråga 7	Dataintegritet	Hur viktigt är det att vara säkra mot att ingen skall kunna manipulera information?
Fråga 8	Förtroende	Hur trygg känns det med den säkerhet som erbjuds i molntjänster?
Fråga 9	Data-segregation	Hur viktigt är det att data är krypterad och segregerad från andra kunders data i molntjänster?
Fråga 10	Säkerhets-standards	Hur viktigt är det att man följer säkerhetsstandards, så som ISOs etc. och andra rekommendationer?

Tabellen 2.2 visar alla frågor som besvaras i en värdeskala där kunder och leverantörer kan ange värden i olika grader. Dessa frågor har kategoriserats och numrerats för att kopplas till en specifik säkerhetsaspekt.

Tabell 2.3 Enkätens intervjufrågor

Fråga	*Kategori*	*Intervjufrågor*
Fråga 1	Datasäkerhet	Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att man bör skydda sig mot dessa?
Fråga 2	Dataintrång	Vilka säkerhetsåtgärder bör man ta för att förhindra dataintrång i molntjänster?
Fråga 3	Juridiska frågor	Hur försäkrar man privat information skyddas på ett lagligt sätt?
Fråga 4	Datasäkerhet	Erbjuds någon form av kryptering av sparade data i molnet?
Fråga 5	Auditlogg	Erbjuds någon form av auditlogg där man kan följa upp vad som sker i de system/molntjänst som erbjuds?
Fråga 6	Tillgänglighet	Hur försäkrar man att hyrda molntjänster alltid är tillgängliga och funktionella?
Fråga 7	Dataåtkomst	Vilka åtkomsträttigheter har man inom de tjänster, som att komma över och/ eller ändra er information och till vilket syfte?
Fråga 8	Datalokaliser-ing	Känner man till vart data lagras?
Fråga 9	Förtroende	Har man kunnat ta del av säkerhetspolicys och procedurer från molntjänstleverantörerna?
Fråga 10	Juridiska frågor	Vilka SLAs erbjuds av leverantören?
Fråga 11	Tillgänglighet	Ifall det skulle vara så att leverantören skulle gå i konkurs eller bli uppköpt, har man på något sätt blivit försäkrad att data ej går förlorad och att det fortsätter att vara tillgängligt?
Fråga 12	Datasäkerhet	Finns det något som skiljer angående säkerheten mellan olika molntjänstleverantörer, i så fall vad?

Tabell 2.3 är vår sammanställning av våra intervjufrågor som vi valt att ha med i enkäten. Dessa frågor är kategoriserade samt numrerade, vi har enbart valt att redogöra alla enkätfrågor som är anmärkningsvärda att kategorisera och som är relaterade till datasäkerhet.

2.5.5 Våra enkätfrågor kopplade till tidigare genomförda undersökningar

I detta delavsnitt redogör vi alla våra enkätfrågor och kopplar våra frågor med undersökningarnas resultat. Dessa kan vara rekommendationer som kunder och leverantörer bör överväga och reflektera kring innan implementering av molntjänster. Vi har kategoriserat våra enkätfrågor i form av olika säkerhetsaspekter, beroende på författarnas olika utgångspunkter och metoder som de använt sig av, jämför vi våra enkätfrågor med undersökningarnas resultat i form av säkerhetsaspekter. Detta gör vi då det blir mer begripligt att jämföra och göra det överskådligt för oss. Detta är möjligt då författarna delar liknande syften. Vi jämför våra enkätfrågor med samtliga författares verk genom två tabeller, tabell 2.4 och 2.5.

Tabell 2.4 Våra frågor i värdeskala kopplade till undersökningen

Fråga	*kategori*	*Subashini och Kavitha*	*Pauley*	*Brodkin*	*Zhou et al*
Fråga 1	Datasäkerhet	X	X		
Fråga 2	Dataintegritet	X			X
Fråga 3a	Tillgänglighet	X		X	X
Fråga 3b	Datasäkerhet	X	X		
Fråga 3c	Datasäkerhet	X	X		
Fråga 4	Datalokalisering	X		X	X
Fråga 5	Backup	X			
Fråga 6	Ansvarighet				X
Fråga 7	Dataintegritet	X			X
Fråga 8	Förtroende				
Fråga 9	Datasegregation	X		X	
Fråga 10	Standards	X	X	X	

Tabell 2.4 visar att våra värdeskalsfrågor förknippas med de flesta säkerhetsområden från undersökningarna. Datalokalisering, datasegregation, tillgänglighet samt datasäkerhetsfrågorna är alla ofta nämnda samt hänvisade att uppmärksamma enligt författarna.

Tabell 2.5 Våra intervjufrågor kopplade till undersökningen

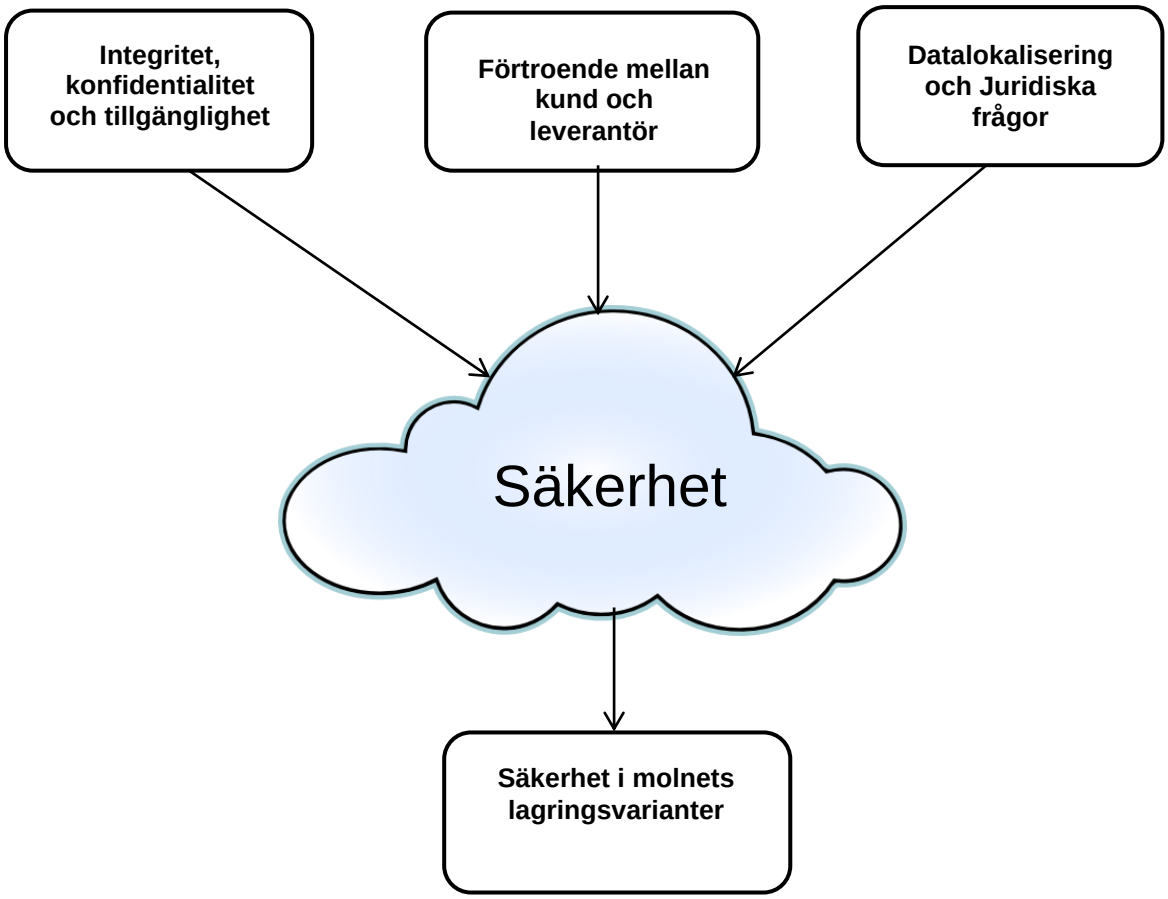
Fråga	*Kategori*	*Subashini och Kavitha*	*Pauley*	*Brodkin*	*Zhou et al*
Fråga 1	Datasäkerhet	X	X		
Fråga 2	Dataintrång	X			
Fråga 3	Juridiska frågor			X	X
Fråga 4	Datasäkerhet	X	X		
Fråga 5	Auditlogg		X	X	X
Fråga 6	Tillgänglighet	X		X	X
Fråga 7	Dataåtkomst	X		X	
Fråga 8	Datalokalisering	X		X	X
Fråga 9	Datasäkerhet	X	X		
Fråga 10	Juridiska frågor		X		X
Fråga 11	Tillgänglighet	X		X	X
Fråga 12	Datasäkerhet	X	X		

I Tabell 2.5 redogör vi alla våra intervjufrågor med undersökningarnas olika säkerhetsaspekter. Återigen är datasäkerhet och tillgänglighet väldigt viktigt enligt nästan samtliga undersökningar och ett stort bekymmer för leverantörer och kunder att tänka över. Datalokalisering visar sig även vara en säkerhetsfråga som kunden bör fokusera på och känna till. En annan viktig faktor är att kunderna har möjligheten att följa upp sina aktiviteter i form av auditlogg. En ytterligare viktig faktor enligt undersökningarna och en fråga vi valt att ha med i vår undersökning är leverantörernas åtkomstmöjligheter och kundernas kännedom om detta.

2.6 Vår undersökningsmodell

Vår undersökningsmodell är en sammansmältning av det teorin anser vara viktigt gällande säkerheten för ett informationssystem och resultaten från de tidigare genomförda undersökningarna som vi valt att ha med.

För att en molntjänst ska anses som säker bör både tekniska och icke-tekniska säkerhetsåtgärder behandlas. De tekniska säkerhetsåtgärderna bör behandla och uppfylla dataintegritet, datakonfidentialitet och tillgänglighet av molntjänster i den grad som krävs för att uppfattas som en säker molntjänst (se figur 2.3). I tekniska säkerhetsåtgärder ingår även datalokaliseringen, då kunddata bör segregeras ifrån andra kunders data för att undvika dataintrång av användare i samma moln (se figur 2.3). De icke-tekniska säkerhetsåtgärderna är inte mindre viktiga för säkerheten i molnet (se figur 2.3). För att en molntjänst ska anses som säker behöver kunder även skapa ett förtroende för leverantörerna gällande säkerheten och deras processer för att bemöta kundernas säkerhetskrav samt ha avtalade ansvar och ansvarsskyldigheter kunder och leverantörer emellan. Detta är ett sätt för kunderna och leverantörerna att känna sig trygga i de fall säkerhetsproblem skulle dyka upp och juridiska frågor kommer på tal. Då det finns olika lagringsvarianter i molnet är det intressant att veta vilken av dessa varianter som kunderna och leverantörerna tycker är säkrast.



Figur 2.3 Vår undersökningsmodell

Vi har utformat vår undersökningsmodell för att ta reda på vilka leverantörernas och kundernas ställningstagande är kring säkerheten i molnet. För att ta reda på deras synpunkter behöver vi ha svar på våra tre delfrågor. Denna undersökningsmodell (se figur 2.3) kommer att stå till grund för vår insamling av empiri då vi utifrån denna modell kommer att utforma våra undersökningsfrågor. För att ta reda på vad de anser om integritet, konfidentialitet och tillgänglighet behöver vi få en insyn i vad de tycker om detta samt vilka åtgärder de tar för att skydda sig kring dessa säkerhetsaspekter. Datalokaliseringen och juridiska frågor kommer att behandla frågor angående hur de ställer sig till datasegregation, åtkomstkontroller, vart de lagrar kunddatan samt vem som är ansvarig och vem som är ansvarsskyldig för säkerheten. Vi kommer att ta upp frågor gällande säkerhetsstandards, rekommendationer, säkerhetspolicy och hur trygga kunderna känner sig med leverantörernas öppenhet av deras procedurer. Förtroendet mellan kunder och leverantörer har en påverkan i hur säkra molntjänster är. Dessa tre delfrågor kommer att spela en roll i kundernas resultat om hur pass säkra de olika lagringsvarianterna anses vara.

3 Metod

I metod kapitlet presenterar vi de ansatser vi har tagit del av för vår undersökning. Vi beskriver även de metoder vi använt oss av för vår insamling av empiri, undersökt validiteten och reliabilitet för de data vi samlat in samt tagit upp de bortfall vi haft i vår undersökning.

3.1 Undersökningens förhållningsätt

Efter fastställandet av vår problemformulering, syfte och avgränsning använde vi oss av olika processer som vi ansåg var lämpliga att använda för att genomföra vår undersökning och för att besvara vår forskningsfråga. Den metod vi använde oss av bestod av två delar. Dessa delar är två undersökningar där den ena delen gick ut på att undersöka molntjänstleverantörer och den andra delen gick ut på att undersöka kunder. Vår tanke med undersökningen är att se hur molntjänstleverantörerna och kunderna ställer sig kring säkerheten i datormolnet. För att ta reda på detta utformade vi frågor (se bilaga B3.1 och B3.2) som berör hur säkert de anser de olika molnvarianterna vara, hur de ställer sig kring datasäkerheten, det vill säga integriteten, konfidentialiteten och tillgängligheten i datormolnet, hur de ställer sig kring datalokaliseringen och de juridiska frågorna som uppkommer med molntjänster samt hur viktigt förtroendet mellan leverantör och kund är för att uppfylla den säkerhet som behövs. Jacobsen (2002) menar att en undersöknings förlopp bland annat går ut på att ha frågor, det vill säga något vi undrar över för att sedan samla in data från empiri för att få besvara våra frågor. En motivering till våra valda undersökningsfrågor finns att hitta i bilaga 2. För att ta reda på vilka skillnader det finns med molntjänstleverantörernas och kundernas åsikter om säkerhet och vad de tycker är säkert, utformade vi en liknande undersökning för kunderna där vi i princip ställde samma frågor med annorlunda formuleringar. Detta gjorde vi för att följa upp det leverantörerna tror är viktigt för kunderna samt se hur verkligheten ser ut för befintliga kunder. Jacobsen (2002) menar att data från empiri är ett sätt att besvara hur verkligheten faktiskt ser ut.

Vårt mål är att få en inblick i vad molntjänstleverantörerna respektive kunderna anser om säkerheten i datormolnet, vad de anser vara viktigt att undersöka om och vilka är skillnaderna mellan de två parternas syn på säkerheten samt vikten av dessa och dessutom undersöka vilka åtgärder som utförs. Molntjänstleverantörernas och kundernas synpunkter var det viktigaste eftersom dessa utgjorde den empiriska delen.

Vår undersökning beträffande leverantörernas och kundernas synpunkter genomfördes genom två enkäter, en för leverantörerna och en för kunderna. Vi valde att undersöka både leverantörers och kunders synpunkter eftersom det i regel finns många människor med olika synpunkter (Jacobsen, 2002). Vår empiriska del utgjordes av VD, drifttekniker eller IT-

chefer och bestod av en enkät, som skickades ut i form av elektronisk webbenkät till respondenten som skulle besvara på frågorna.

3.2 Val av metod

Här nedan presenteras vilken undersökningsmetod vi valt, urvalet av respondenter, genomförandet och utformningen av enkätundersökningen.

3.2.1 Metodik

På grund av att vi valt att göra en kvantitativ och kvalitativ undersökning har vi utformat en undersökning som består av två delar, den första delen är kvantitativ och den andra delen är kvalitativ. Jacobsen (2002) menar att denna metod innebär att datan är nyanserande vilket betyder att de som intervjuas diskuterar sina tolkningar och åsikter. Enligt Jacobsen (2002) består en kvantitativ struktur av kryssfrågor med fasta svarsalternativ, medan en kvalitativ struktur har öppnare frågor. Vår kvantitativa del bestod av undersökningsfrågor som besvaras i form av värdeskalsfrågor (1-7). Vår kvalitativa del bestod av intervjufrågor som besvarades i löpande text.

3.2.2 Undersökning

Vår undersökning bygger på en e-postintervju där vi utformat en enkät och använder frågor som graderas på en värdeskala på 1-7 som sedan följs upp av intervjufrågor. Eftersom alla säkerhetsaspekter vi valt att ha med i vår undersökning ansågs som viktiga i tidigare undersökningar (se delkapitel 2.5), förväntade vi oss därför att de flesta respondenterna skulle tycka att dessa var viktiga. Om vi istället valt att ha färre värden, exempelvis 1-5, tror vi inte att detta skulle ge oss en rätt uppfattning då endast 4 och 5 innebär att det är viktigt, därför tyckte vi att en värdeskala på 1-7 skulle ge oss en tydligare uppfattning av hur viktigt de anser de säkerhetsaspekterna vara. Med intervjufrågorna har vi velat få mera fördjupning och klarhet inom vissa områden. Frågorna med värdeskala har vi använt för att få svar på enklare frågor för att åstadkomma någon form av statistik inom en del områden där vi ansett statistiken vara det bästa sättet att föra fram ett resultat (Jacobsen, 2002).

Vi har valt att genomföra vår undersökning genom e-post eftersom våra respondenter önskat detta på grund av tidsbrist, fullbokade scheman och det i vissa fall inte varit ekonomiskt möjligt för oss att göra en besöksintervju. Genom en e-postundersökning har vi fått möjligheten att ställa bredare intervjufrågor så att respondenterna skulle kunna diskutera utveckla dem och inte enbart göra en enkätundersökning där vi inte får lika stor djup och bredd i svaren (Jacobsen, 2002). Vi har valt en enkätundersökning före telefonintervju då det kan finnas ett antal nackdelar med telefonintervjuer. En respondent kan under intervjuns gång befinna sig i en stressig miljö vilket kan leda till att vi inte får de svar vi söker efter. Vi får

istället korta och snabba svar för att respondenten ska ha tid att genomföra hela intervjun och i stressiga omständigheter är det lätt hänt att respondenten glider utanför ämnet. Genom en enkätundersökning har respondenten en möjlighet att bilda sig en uppfattning om vad denne behöver för att besvara frågorna och skapa en förståelse för undersökningens syfte. Detta gör de genom att läsa igenom undersökningen och på så vis sätt kunna vara pålästa innan de besvarar frågorna. En annan stor fördel med en enkätundersökning istället för en telefonintervju är att respondenterna kan besvara frågorna när de har tid och hinner förbereda svaren vilket är bra för respondenterna i fall det dyker upp något viktigt för dem som leder till att de inte har tid för en intervju vid en specifik tid. Vi anser att vår undersökningsmetod gav oss mer underlag och fördjupning genom de öppna frågorna för att vidare analysera- och forska inom vår forskningsfråga.

Det vi tycker att vi gått miste om är att vi inte utfört någon form av besöksintervju, vilket är en mer naturlig miljö öga mot öga, är att vi inte kunnat ta del av kroppsspråk så att respondenterna kan utöka sin uppfattning på grund av närvaron. Jacobsen (2002) menar att det är enklare för två personer att få personlig kontakt när de fysiskt sitter mitt emot varandra och att det är lättare att genomföra ett givande och öppet samtal vid besöksintervjuer än över telefon.

3.2.3 Urval

Vi har gjort ett urval av olika molntjänstleverantörer och kunder för att kunna analysera resultatet vi samlat in utav enkätfrågorna. De molntjänstleverantörer vi valt är företag som i någon form erbjuder molntjänster. Kunderna har däremot kunnat vara både företag eller myndigheter som redan hyr någon form av molntjänst eller har planer på att skaffa sig en sådan tjänst. Genom att undersöka leverantörer som redan erbjuder dessa tjänster samtidigt som vi följt upp med kunder, har detta varit till hjälp för att besvara forskningsfrågan. Urvalen utgår från följande.

Molntjänstleverantörerna:

- Hyr ut eller säljer någon form av molntjänst.
- Har en VD, drifttekniker eller IT-chef som känner att de har rätt kunskap för att svara på frågor kring säkerheten i datormolnet.

Kunderna:

- Hyr eller köpt någon form av molntjänst.
- Har planer på att införskaffa sig någon form av molntjänst.
- Har beslutat att inte införskaffa sig någon form av molntjänst.

För att hitta och kontrollera om leverantörerna erbjuder någon form av molntjänst besökte vi först deras webbsidor och sedan valde vi att ta kontakt med dem via telefon och kontrollerade att de hyrde ut sådana tjänster. För att hitta kunder som hyr en molntjänst och kontrollera detta frågade vi leverantörerna i undersökning om de hade några referenser på befintliga

kunder som vi kunde ta del av. De svarade genom att referera till deras webbsidor där de presenterar vilka kunder de arbetar med.

3.2.4 Genomförande av enkätundersökning

Vi undersökte sju olika företag varav två av dem är leverantörer, tre av dem är kunder och två av dem är företag som inte är befintliga kunder men har planer på att den närmsta tiden hyra en molntjänst. Vår undersökning genomfördes under maj månad 2011.

Vi intervjuade endast en person på varje företag. De vi intervjuade är inom företagen med arbetsroller så som VD:n, drifttekniker och IT- chefer. Vi har valt de som ansåg sig var säkerhetsexperter inom molntjänster och har en bra insyn i de datormolnbaserade tjänster de erbjuder eller hyr för att få validitet och kvalitet för vår undersökning. Vi har vänt oss till företag inom Sverige, både större företag, med många anställda, många kunder och till mindre företag med färre anställda. Att utföra en besöksintervju var inte möjligt för oss då de flesta av våra respondenter finns i Stockholmregionen medan vi är från Malmö- och Lundregionen.

Efter vi samlat in all material från respondenterna utförde vi en transkribering.

3.2.5 Utformning av enkätformulär

Vi använde oss av enkäter för att samla in information för vår undersökning (se bilaga B3.1 och B3.2). Vi tog kontakt med företagen genom att ringa dem per telefon, i de samtalen vi förde med respondenterna (VD:n, drifttekniker och IT- chefer) förklarade vi för dem vad vår undersökning handlade om samt vilka frågor det handlade om. För att friska upp deras minne och för att det inte skulle bli något missförstånd skrev vi även en kort beskrivning i början av våra enkäter med samma information (För att se hela enkäten se bilaga B3.1 och B3.2).

Då de flesta företagen förklarade att de var väldigt upptagna i maj månad, kom vi överens och utförde undersökningen genom e-post. För att det skulle bli enkelt för både respondenterna att svara på frågorna och för oss att sammanställa enkäterna använde vi oss utav webbformulär. Vi skickade länken till webbformuläret till VD:n, drifttekniken eller IT- chefen som skulle svara på frågorna.

Vår enkät består av två delar den första delen innehåller frågor med värden som respondenterna har möjlighet att svara genom att kryssa i en siffra eller nivå på frågan och den andra delen är öppna frågor som respondenterna svarar på genom att skriva text. Vi har format vår enkät så att frågorna med värden och intervjufrågor på något sätt kompletterar varandra. Där vi har en fråga med värden har vi en intervjufråga som berör samma ämne och område för att få mer djup i svaren. Vi har valt ut våra undersökningsfrågor utefter vår

insamlade teori som ni finner i kapitel 2 *Litteraturgenomgång*, ur vår undersökningsmodell (kapitel 2.6) och ur våra egna tankar och funderingar.

Efter insamlingen av svaren från enkäterna gick vi igenom och analyserade dem, då insåg vi att vi inte tagit med två frågor till enkätundersökningen för kunderna. Vi kompletterade enkätundersökningen genom att skicka e-post till kunderna där vi förklarade händelsen och bad dem att svara på dessa två i efterhand per e-post om möjligt. Två kunder var vänliga nog och svarade på dessa frågor. Vi insåg i efterhand även att det var svårt för oss att belysa vilka säkerhetsaspekter kunder och leverantörer ansåg vara viktigare än andra då de flesta aspekterna ansågs som viktiga. Därför valde vi att komplettera detta genom att be kunder och leverantörer att rangordna säkerhetsaspekterna utefter deras relevans och vikt.

3.3 Genomförande av analysen

Efter insamlingen av informationen från vår undersökning resulterade det i en massa data. Att ha massa data kan vara svårt att analysera speciellt de data från undersökningar där vi har frågor som kan leda till respons med mer öppna svar. Genom att strukturera och välja en analysmetod gör vi det enklare att analysera den inkomna datan. Efter att vi samlat in all data från enkäterna gick vi igenom alla svar och transkriberade dessa. Vi har transkriberat alla svar var för sig för att på ett enklare sätt kunna analysera. Utifrån transkriberingen har vi för att göra det lättare för läsaren att förstå och läsa svaren från vår undersökning lagt in datan i tabeller i kapitel 4 *Resultat av empiri*. Transkriberingen i sin helhet finns i bilaga B4.3 och B4.4 och översikten av transkriberingen i form av tabeller finner ni i bilaga B4.1 och bilaga B4.2.

Vår enkätundersökning är utformad på så sätt att vi får en strukturerad insamling av vår oanalyserade data. Vi analyserade och jämförde den empiri vi samlat in. Detta gjorde vi för att fånga upp all användbar data med hjälp av Jacobsens (2002) översiktliga analysprocess. Först fick vi en grundlig och detaljerat beskrivning av datan, sedan gör vi en systematisering genom att förenkla informationen för att slutligen kunna tolka datan och leta efter dold information. För att ytterligare förenkla för läsaren har vi utifrån transkriberingen kategoriserat de olika ämnena, det vill säga att vi har kategoriserat genom att strukturera frågor i ordningsföljd där vi har lagt säkerhetsfrågor under varandra och frågor vad gäller ansvarsfördelning under varandra etc.

3.4 Undersökningens kvalitet

3.4.1 Etik

Då intervjupersonen kan känna sig påträngd i sitt privatliv under en intervju och undersökning så kan det uppstå etiska dilemman. Därför har vi följt och beskrivit Jacobsens (2002) etiska riktlinjer: *Informerat samtycke, privatliv* och *vikten av korrekt data.*

Informerat samtycke – Innan intervjuerna har de informanter vi kontaktat haft möjlighet att frivilligt bestämma huruvida de är intresserade och villiga att delta i intervju och en empirisk undersökning. Jacobsen (2002) och Kvale (1997) menar på att detta är ett villkor för undersökning.

Privatliv – Med detta menar Jacobsen (2002) att informanten har rätt till ett privatliv. Information som samlas in under undersökningen kan anses som privat för den som undersöks därför är det viktigt att ta hänsyn till detta. Det är ytterst viktigt att ge informanten en möjlighet att vara anonym då det behövs anonymitetsåtgärder samt då respondenterna själva önskar vara anonyma och även att ge dem möjlighet att anonymisera deras företag vid publicering av information. Då möjligheten för anonymitet är en viktig aspekt har vi valt att diskutera detta med respondenterna och beskriva i vilket syfte undersökningsresultatet kommer att användas för. En annan viktig aspekt enligt DiCicco-Bloom & Crabtree (2006), är att ge möjlighet för respondenterna att bekräfta informationen som samlats in under intervjuerna om så önskas, samt att resultaten av intervjuerna inte ska användas i andra sammanhang än de som förklarats för respondenterna. Då respondenterna själva har skrivit sina svar och skickat detta till oss har de inte behövt ytterligare en bekräftelse på detta. Vi har däremot i våra samtal med respondenterna informerat dem att informationen endast ska användas i de sammanhang som vi kommit överens om.

Vikten av korrekt data – Jacobsen (2002) tar upp vikten av att ha riktig presentation av data. Med det menar han att de som gör en undersökning ska försöka återge resultat fullständigt och i rätt sammanhang i den utsträckning det är möjligt. Citat som är utbrutna ur ett större sammanhang kan ofta få en annan betydelse än om de sätts in i en större kontext, (Jacobsen 2002).

Våra intervjuer har även följt Oates (2006) riktlinjer för deltagarnas rätt. Där vi innan intervjuerna förklarat och gav respondenterna följande rätt:

- Rätt till att inte delta
- Rätt att frånträda
- Rätt att ge informerat samtycke
- Rätt till anonymitet
- Rätt till sekretess

Vi har gett våra respondenter möjlighet att ta del av vår uppsats när det är färdigt ifall de önskar det. Alla leverantörer och fyra av fem kunder har svarat att de vill ta del av arbetet när

det är färdigt. Båda leverantörerna och en av fem kunder har valt att inte vara anonyma men resten av kunderna, det vill säga fyra kunder önskar att vara anonyma.

3.4.2 Validitet och reliabilitet

I denna undersökning har vi försökt uppnå validitet genom att rätta oss efter de riktlinjer som beskrivs i Jacobsen (2002) **.**

Vi har intervjuat säkerhetsexperter med arbetsroller som VD:n, drifttekniker eller IT- chefer från både leverantörerna och kunderna på grund av att de har bäst översikt och kunskap om säkerheten kring molntjänsterna.

I vår undersökning har vi försökt hålla respondenterna till ämnena kring våra enkätfrågor för att inte ge dem möjlighet att tala om annat som är irrelevant för undersökningen. Detta löste vi genom att utforma ett webbformulär för att genomföra vår enkätundersökning per e-post. Tack vare denna metod har vi kunnat hålla respondenterna till våra frågor genom att formulera våra enkätfrågor på ett enkelt och precist sätt tillsammans med en förklaring där vi beskrivit vad vi menar med frågan så att frågan inte misstolkas. Vi fick svaren svart på vitt genom en enkätundersökning via ett webbformulär, det fungerade som hjälpmedel för att inte glömma eller misstolka någon information vid datainsamlingen.

Efter att ha fått tillbaka svaren på vår undersökning sammanställde vi och analyserade respondenternas information. Vi läste igenom materialet flera gånger för att minska felmarginalen och för att kontrollera så att det inte varit något som misstolkats eller glömts bort.

Vi har även gjort litteraturundersökningar för att kunna utföra en bra analys och för att få en djupare förståelse för forskningsfrågan. Vi har använt oss av tillförlitliga källor inom forskningsområdet för att sedan anknyta litteraturen med resultatet.

På grund av de få respondenter i vår undersökning representerar vårt resultat inte en helhetsbild för de flesta leverantörers och kunders ställningstagande kring säkerheten i molnet. Vi uttalar oss endast om de slutsatser vi tar utifrån våra respondenter.

3.4.3 Bortfall

Vi antog att vårt val av forskningsfråga skulle kunna vara känslig för vår målgrupp, bestående av leverantörer och kunder. Ett stort problem i en urvalsundersökning brukar vara de bortfall som kan förekomma (Jacobsen, 2002). Bortfallet i vår undersökning var att de urvalsunderlag vi valt, bestående av utvalda personer för vår undersökning som inte kunde ställa upp och svara på våra frågor. Vårt urvalsunderlag bestod av personer som hade en ansvarsroll för företagets uthyrning respektive hyrning av molntjänster.

Vi har ringt 37 företag varav 14 varit leverantörer och 23 var kundföretag och av dem var det 2 leverantörer samt 5 kundföretag som valde att delta i vår undersökning. Många leverantörer tog avstånd från vår undersökning vilket påverkade vårt slutresultat en aning då vi inte fick möjlighet att få tillräckligt hög kvantitet gällande ställningstagande från leverantörernas sida. Men vi har uppfyllt vårt mål som var minst 2 ställningstagande från respektive leverantör och kund. Att leverantörer och kunder inte valde att ställa upp på vår undersökning berodde främst på grund av tidsbrist att delta i undersökningen eller i vissa fall, för att den undersökning vi valt att göra har varit för känsligt för företagen att delta i och tagit avstånd från våra enkätfrågor. Det har i vår undersökning förekommit att vissa respondenter stått över vissa frågor. Till en början hade vi 4 klara leverantörer som var redo att ställa upp på undersökningen men där 2 av dessa i sista stund avstod från detta. Vi försökte hålla oss borta från bortfall när det gäller deltagandet för vår undersökning. Detta gjorde vi bland annat genom att påminna och betona vikten av leverantörernas åsikter. Vi kontaktade även dem som hade planer att delta i vår undersökning. Men trots våra försök gav det inte större resultat.

4 Resultat av empiri

I detta kapitel presenterar vi resultatet av våra tre delfrågor som respondenterna besvarat. Vi har även med resultatet över hur respondenterna upplever säkerheten i de olika lagringsvarianterna inom datormolnet. Vi genomförde två separata undersökningar. Dessa två bestod av en undersökning för leverantörernas och en undersökning för kundernas synpunkter på säkerheten i molnet. Vi valde att presentera vårt resultat genom diagram. Detta valde vi för att tydligt jämföra och visa skillnaderna mellan resultaten vi samlat in. Svaren presenteras i form av olika värden i en värdeskala. Kundernas diagram är sammanställda till vänster och leverantörernas till höger. Svaren är sammanförda i siffror där kunderna besvarat frågorna med olika värden från 1 till 7. Vi lägger även fram en presentation av leverantörernas samt kundernas ställningstagande från intervjufrågorna. Detta redogörs i form av tabeller. Tabellerna har samma uppsättning som diagrammen, där kundernas svar redogörs till vänster och leverantörernas till höger.

Vår granskning bygger på de svar vi samlat in. Dessa svar har vi fått och jämfört för att kunna få ett bra resultat och besvara vår forskningsfråga. Den fullständiga responsen finner ni i bilaga B4.3 samt B4.4.

4.1 Integritet, konfidentialitet och tillgänglighet

Här redogör vi våra resultat från respondenterna vad gäller konfidentialitet och integritet av data, hur de ställer sig till kryptering och segregation för datan samt vilka hot som anses vara de största hoten.

Kunder *Leverantörer*

Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?

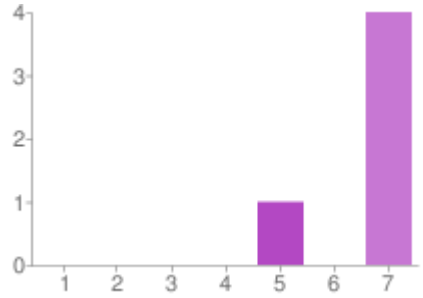


Diagram 4.1.1

Hur viktigt tror ni det är för kunderna att ingen kan ta del av deras data i datormolnet?

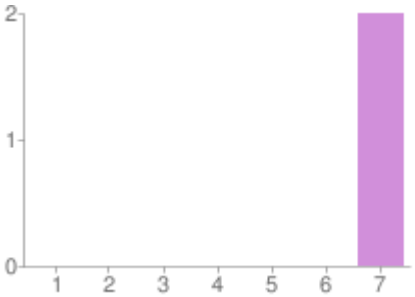


Diagram 4.1.2

Detta resultat berör konfidentialitet av informationslagring där en av kunderna anser att konfidentialitet inte är så viktig som resten av respondenterna anser (se diagram 4.1.1 och 4.1.2). Detta kan bero på att kunden inte har lagt ut känslig information i molnet och kan vara anledning till att de anser det vara mindre viktigt än de andra kunderna.

Hur viktigt är det att ni är säkra mot att ingen skall kunna manipulera er information?

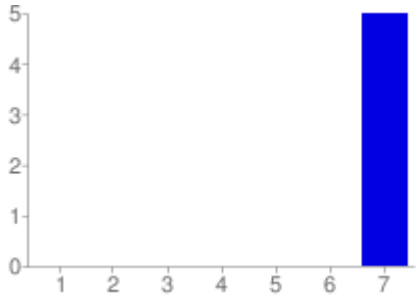


Diagram 4.1.3

Hur viktigt är det att kunderna är säkra mot att ingen skall kunna manipulera deras information?

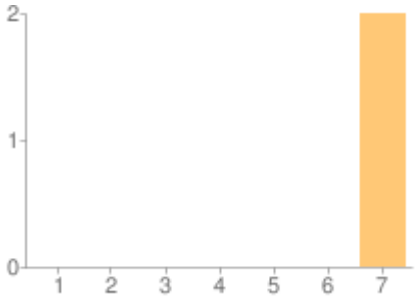


Diagram 4.1.4

Att det är ytterst viktigt att ingen obehörig ska kunna manipulera kundens data ute i molnet är något våra respondenter anser (se diagram 4.1.3 och 4.1.4).

Hur viktigt är det att er data är krypterad och segregerad från andra kunders data i molnet ?

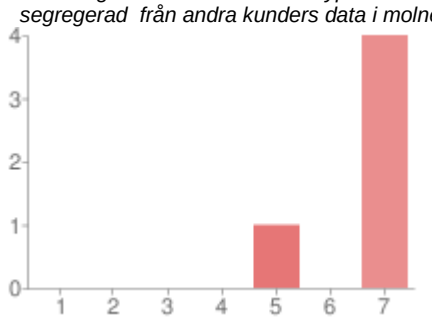


Diagram 4.1.5

Hur viktigt är det att kundernas data är krypterad och segregerad från andra kunders data i molnet?

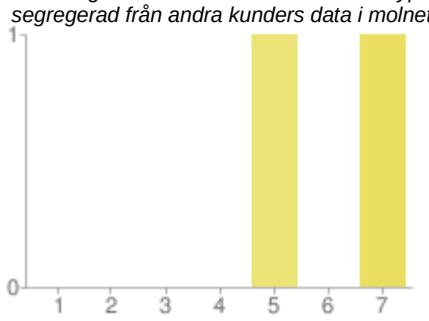


Diagram 4.1.6

Som diagram 4.1.5 och 4.1.6 visar håller sig kunderna och leverantörerna på samma nivå vad gäller betydelsen av att ha krypterad och segregerad data i molntjänsterna. Fyra av fem kunder tycker att det är väldigt viktigt och en kund tycker det är ganska betydelsefullt med kryptering och segregering. Leverantörerna har liknande åsikter där en leverantör tycker att det är ganska viktigt och en leverantör tycker att det är mer viktigt att ha krypterad och segregerad data i molntjänster.

Hur viktigt är det för er att de tjänster molntjänst leverantörerna erbjuder alltid tillgängliga?

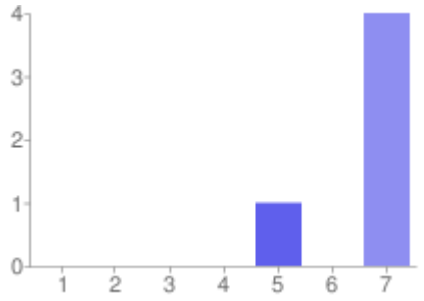


Diagram 4.1.7

Hur viktigt tror ni det för kunderna att de tjänster ni erbjuder alltid är tillgängliga?

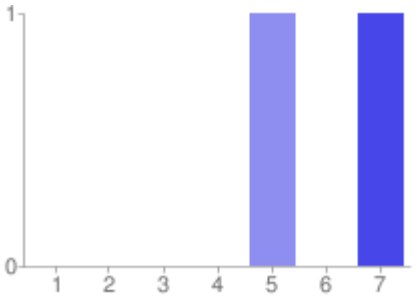


Diagram 4.1.8

Hur viktig är tillgängligheten för er som erbjuder en molntjänst?

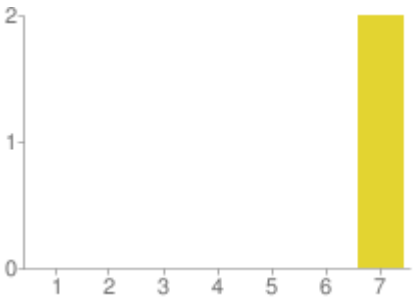


Diagram 4.1.9

Eftersom tillgängligheten är en viktig aspekt i molnet är det värt att lyfta detta resultat trots färre skillnader. Leverantörerna har en bra uppfattning om vad kunderna tycker angående tillgängligheten, detta visas på diagram 4.1.7 och diagram 4.1.8. Kunderna anser det vara mycket viktigt att tjänsterna alltid är tillgängliga förutom en kund som inte anser det vara av lika stor vikt. Leverantörerna anser att det är mycket relevant att deras tjänster är tillgängliga enligt diagram 4.1.9 vilket stämmer bra överens med vad kunderna tycker i diagram 4.1.7.

Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är funktionella ?

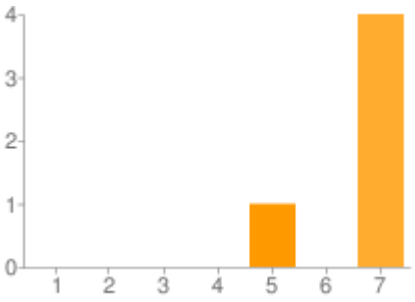


Diagram 4.1.10

Hur viktigt tror ni det är för kunderna att de tjänster ni l erbjuder alltid är funktionella?

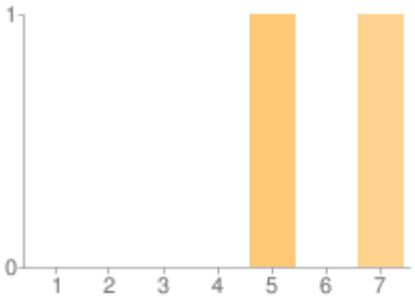


Diagram 4.1.11

Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är säkra ?

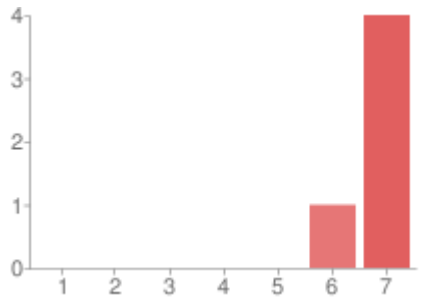


Diagram 4.1.12

Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är säkra?

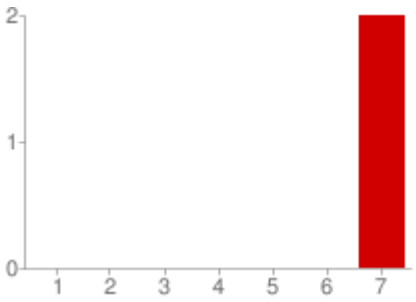


Diagram 4.1.13

Leverantörerna har en ganska bra översikt över vad kunderna tycker då de svarat i enlighet med kunderna om hur viktigt det är att molntjänster alltid är funktionella (se diagram 4.1.10 och 4.1.11). Alla respondenter anser även att det är viktigt att deras molntjänster är säkra (se diagram 4.1.12 och 4.1.13).

Hur viktigt är det för er att molntjänstleverantören gör regelbunden backup på er data/information?

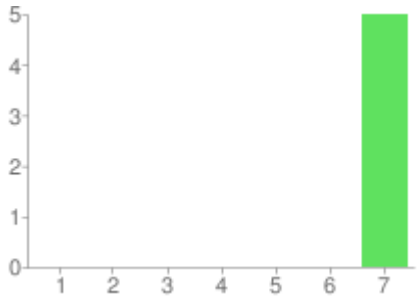


Diagram 4.1.14

Hur viktigt tror ni det är för kunderna att ni gör regelbunden backup på deras data/information?

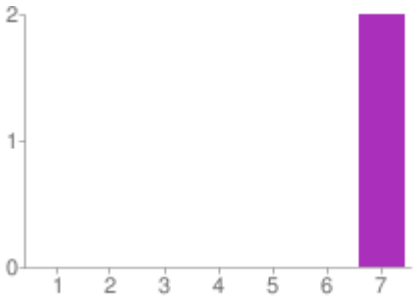


Diagram 4.1.15

Diagram 4.1.14 och 4.1.15 visar att leverantörerna och kunderna tycker att det är absolut viktigt att regelbunden backup görs på kundernas data i molnen.

Tabell 4.1 Intervjufrågorna av undersökningen

Fråga	*Kunder*	*Leverantörer*
Vilka säkerhetsåtgärder bör tas från leverantörer respektive kunderna för att förhindra dataintrång i molntjänster?	*Aktivt gemensamt säkerhetsarbete på alla plan.* *Central hantering av data och lösenord.*	*Kunder bör:* *krypterade & säkra förbindelser.* *HTTPS inloggning, SMS/kodbox, VPN.* *Leverantörer bör:* *Dubbla brandväggar, krypterade förbindelser Starka lösenord och inloggning i form av HTTPS, SMS/Kodbox, VPN*
Erbjuds någon form av kryptering av kundernas sparade data i molnet?	*Ja, de leverantörer de valt att samarbeta med.*	*Beroende på efterfrågan.*
Vilka åtkomsträttigheter har leverantörerna till kundernas data för att komma över eller ändra information och till vilket syfte?	*Specifika SLA för resp. system.* *Sekretessavtal bör skrivas med de som är administratörer eller på annat sätt kan få tillgång till informationen hos leverantören.*	*Rent tekniskt har leverantören åtkomst till data. Men ingen rätt eller intresse att ändra kunddata.* *Regleras i sekretessavtal.* *Superanvändare som har tillgång till all information och kan tilldela andra användare på kundsidan rättigheter.*
Hur försäkras kunderna att de hyrda molntjänsterna alltid är tillgängliga och funktionella?	*Via SLA och andra avtal*	*Har en viss garanterad upptid men systemet är ofta uppe bortsett från att man gör underhåll.* *Bestäms i avtal.* *Tekniken är byggd för att vara stabil.* *Ha en speglad miljö och dubbla linor in.*
Om det skulle vara så att leverantören går i konkurs eller blir uppköpt, hur försäkras kunderna att deras data ej går förlorad och det fortsätter att vara tillgängligt?	*Har blivit försäkrade via avtal att deras data ej går förlorad.*	*Kunden äger alltid rätten till sin data. Regleras i avtal.*
Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive kunderna bör skydda sig mot dessa?	*Data försvinner, obehöriga får tillgänglighet, data ej tillgängligt vid behov. Osäker på molntjänstleverantörens hantering av information på lång & kort sikt*	*Mänskliga faktorn.* *Dåliga processer & rutiner.* *Molntjänster skiljer sig från traditionell data miljö.* *Krånglande teknik.*
Hur har ni kommit fram till vilken säkerhet ni är i behov av, har ni gjort en riskanalys eller dylikt?	*Vi har låtit vårt revisionsbolag göra en riskanalys.* *Vi har gjort en allmän riskanalys utifrån företagets riktlinjer för IT-säkerhet.*	

I tabell 4.1 presenteras resultatet för intervjufrågorna, utifrån resultatet anser kunder att kunder och leverantörer gemensamt bör samarbeta på alla plan kring säkerheten för att

förhindra dataintrång. Leverantörerna föreslår olika sorters tekniska lösningar så som dubbla brandväggar och krypterade förbindelser.

Vi har fått två olika svar i intervjun där den ena leverantören använder kryptering medan den andra leverantören anger att ingen av deras kunder har frågat efter kryptering. Kryptering av sparad data beror på molnleverantören samt vilka molntjänster kunder använder. Kunderna har blivit erbjudna kryptering på deras sparade data (se tabell 4.1).

Rent tekniskt har leverantörerna åtkomst till kundernas data, men de har ingen rätt eller intresse att ändra kundens data. Det finns en superanvändare som har tillgång till all information och tilldelar andra användare rättigheter på kundsidan. Detta regleras från kundernas sida genom att följa specifika SLA samt att skriva sekretessavtal med dem som är administratörer för deras information (se tabell 4.1).

Leverantörerna har en viss garanterad upptid i molntjänsten som bestäms i avtal, men systemet är oftast uppe, förutom när leverantörerna gör underhåll (se tabell 4.1) och dessa behöver inte meddelas till kunden. Dessa avtal så som SLA görs i samarbete med leverantören och kunden så att användandet av molntjänsten inte påverkas.

Kunden äger alltid rätten till sin data och via avtal som skrivs mellan leverantör och kund går informationen alltid tillbaka till kunden. Kunderna är garanterade att informationen kommer tillbaka till dem om leverantören skulle gå i konkurs. Kunderna kan dessutom välja att köpa ut lösningen eller att avbryta kontraktet om detta skulle ske (se tabell 4.1).

Kunderna anser att de viktigaste hoten mot molntjänster är förlust, dataintrång eller otillgänglig data och att de är osäkra på leverantörens hantering av information. Leverantörerna anser att de största hoten mot molntjänster istället är den mänskliga faktorn, dåliga processer och rutiner och krånglande teknik (se tabell 4.1). Kunderna tycker att hoten handlar om datasäkerhet och förtroende medan leverantörerna tycker att den mänskliga faktorn och krånglande teknik är stora hoten (se tabell 4.1).

4.2 Datalokalisering och juridiska frågor

I detta avsnitt tar vi upp vad kunderna och leverantörerna anser om vart datan befinner sig samt hur de skyddar datan på ett lagligt sätt och vad de anser om ansvarighet från kundernas och leverantörernas sida.

Kunder

Hur viktigt är det för er att ni vet vart er data/information lagras?

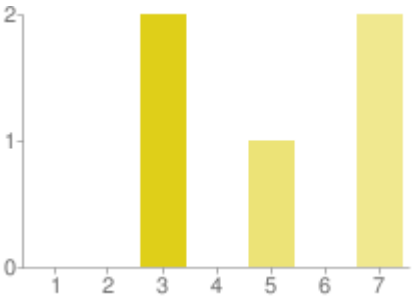


Diagram 4.2.1

Leverantörer

Hur viktigt tror ni det är för kunderna att de vet vart deras data/information lagras?

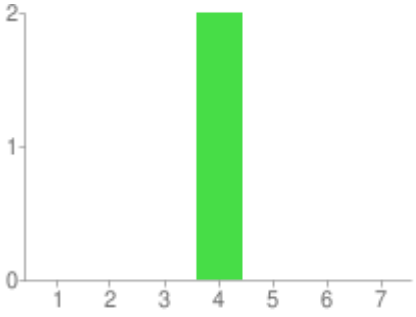


Diagram 4.2.2

Det finns skilda åsikter kring kännedomen om vart kundernas data lagras. Leverantörerna är eniga om att det inte är det allra viktigaste att veta vart kundernas data lagras. Kunderna har mer varierande synpunkter. Två av fem kunder tycker att det nästan är irrelevant att veta vart datan lagras, två kunder tycker däremot att det är ytterst viktigt medan en tycker att det är relevant (se diagram 4.2.1 och 4.2.2).

Hur viktigt är det med ansvar (accountability) från molntjänstleverantörernas sida?

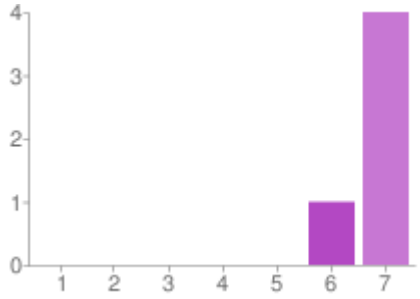


Diagram 4.2.3

Hur viktigt tror ni ansvar(accountability) är för kunderna?

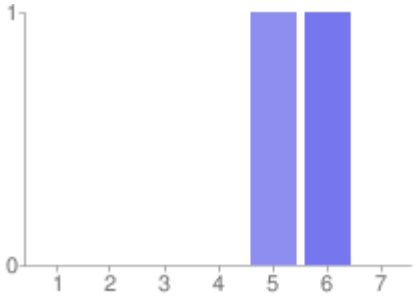


Diagram 4.2.4

Både leverantörerna och kunderna anser att det är betydelsefullt med ansvar (*accountability*) fast åsikterna skiljer sig med små marginaler. Kunderna tycker att det är ytterst viktigt med ansvar från leverantörernas sida. Leverantörerna anser det vara betydande för kunderna att ta hänsyn till ansvar (se diagram 4.2.3 och 4.2.4).

Tabell 4.2 Intervjufrågorna av undersökningen

Fråga	*Kunder*	*Leverantörer*
Känner kunden till vart deras data lagras?	*Ja*	*Ja*
Hur försäkras kunderna att deras privata information skyddas på ett lagligt sätt?	*Via avtal. Sedan är det en fråga om förtroende.*	*Data sparas i Sverige. Stipuleras i avtal.*

Då kunderna från vår undersökning känner till om vart deras data lagras, antar vi att leverantörerna har angivit den informationen till kunderna. Det är endast en kund som inte vet

vart deras data lagras. För att kunderna ska vara garanterade att deras privata information skyddas på ett lagligt sätt, stipulerar leverantörerna detta genom avtal (se tabell 4.2). Kunderna förklarar att det sedan handlar om förtroende.

4.3 Förtroende mellan kund och leverantör

Nedan visar vi vad parterna anser om trygghet och hur viktigt det är att följa olika säkerhetsstandards. Vi redogör även om leverantörernas öppenhet kring att dela ut sina policys och om de följer några ISOs eller säkerhetsstandards.

Kunder

Hur trygga känner ni er med den säkerhet molntjänstleverantörerna erbjuder i sina tjänster?

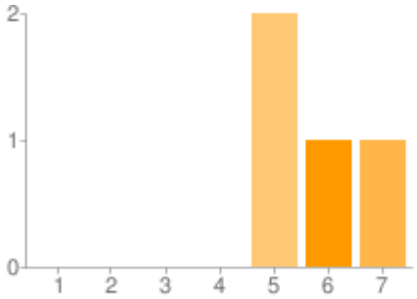


Diagram 4.3.1

Leverantörer

Hur trygga tror ni era kunder känner sig med den säkerhet ni erbjuder i era tjänster?

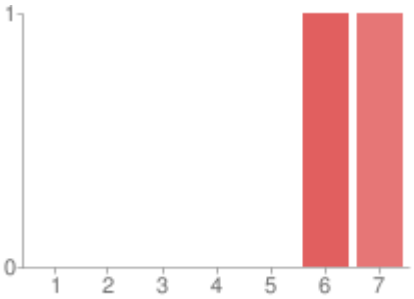


Diagram 4.3.2

Vad gäller kundernas förtroende för deras leverantörer, har leverantörerna överskattat sin säkerhet lite genom att tro att kunderna är ytterst trygga med säkerheten som de erbjuder i sina tjänster. I diagram 4.3.2 ser vi att en leverantör tror att kunderna är trygga och en annan leverantör tror att kunderna är mycket trygga. Även om leverantörernas svar inte är helt missvisande så finns det en liten avvikelse jämfört med i diagram 4.3.1. Där kan vi se att en av fem kunder är mycket trygg med den säkerhet som leverantörer erbjuder i sina tjänster, en kund är trygg, två av de fem kunderna vi undersökt är relativt trygga och där en av kunderna i vår undersökning har valt att stå över denna fråga.

Hur viktigt är det att leverantörerna följer säkerhetsstandards och rekommendationer?

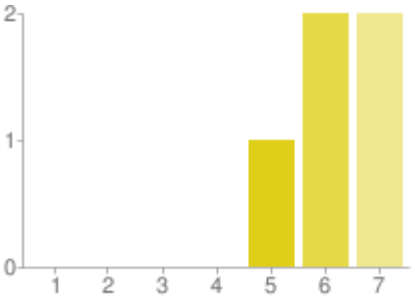


Diagram 4.3.3

Hur viktigt är det för kunderna att ni följer säkerhetsstandards och andra rekommendationer?

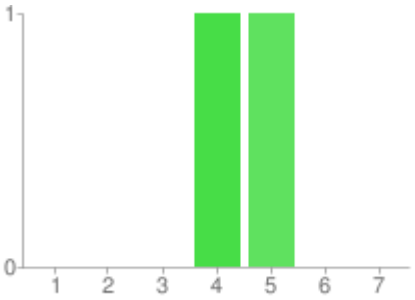


Diagram 4.3.4

Leverantörerna anser inte att det är allra viktigast att de följer säkerhetsstandards och rekommendationer (se diagram 4.3.4). Kundernas åsikt lyder däremot lite annorlunda, de anser att det är viktigt att de följer standarder och rekommendationer. Fyra av fem kunder tycker att det är mycket viktigt att de följer dessa (se diagram 4.3.3). Här syns en tydlig skillnad på kundernas och leverantörernas åsikter kring säkerhetsstandards och rekommendationer.

Tabell 4.3 Intervjufrågorna av undersökningen

Fråga	*Kunder*	*Leverantörer*
Följer ni någon/några säkerhetsstandards så som ISOs eller andra rekommendationer, i så fall vilka? ***(Frågan ställdes enbart till leverantörerna)***		*Beror på vilka leverantörer man har. En leverantör dokumenterar processerna enligt branschpraxis ITIL. En leverantör använder inga ISOs eller rekommendationer.*
Publiceras leverantörernas säkerhetspolicys och procedurer så att kunderna kan ta del av dessa?	*Kunderna i undersökningen har fått ta del av leverantörernas säkerhetspolicys.*	*Beror på leverantören. En av leverantörerna i vår undersökning gör det en annan gör inte det ännu.*
Gäller er säkerhetspolicy för alla leverantörer av molntjänster, i de fall andra leverantörer är inblandade?		*Ja*

Leverantörer skiljer sig i frågan om de följer säkerhetsstandards och rekommendationer. En leverantör följer standards och rekommendationer och en gör inte det. Samma avvikelse finns för publicering av leverantörernas säkerhetspolicy och procedurer där en leverantör publicerar detta så att kunderna kan ta del av dess ansvar kring sin policy och en leverantör publicerar inte detta för stunden. Kunderna däremot är eniga om att de alla har fått ta del av deras leverantörers säkerhetspolicys och procedurer. Leverantörerna bekräftar att deras säkerhetspolicys gäller för alla inblandade parter då andra leverantörer eller underleverantörer är inblandade i en molntjänst (se tabell 4.3).

4.4 Säkerhet i lagringsvarianterna inom datormolnet

Här presenteras en överblick över kundernas och leverantörernas synpunkter om hur säkra de anser om de olika lagringsvarianterna, som består av publika, privata samt hybrida moln.

Kunder

Diagram 4.4.1

Leverantörer

Diagram 4.4.2

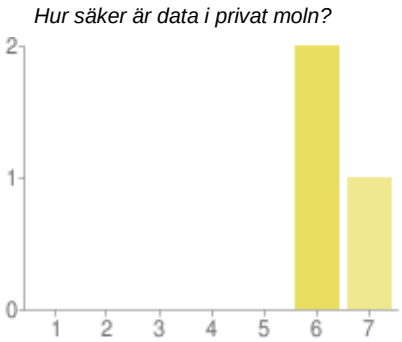


Diagram 4.4.3

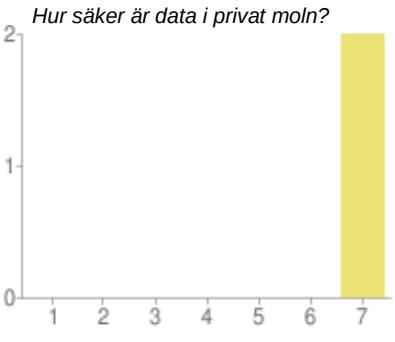


Diagram 4.4.4

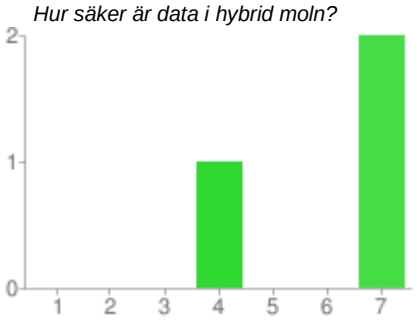


Diagram 4.4.5

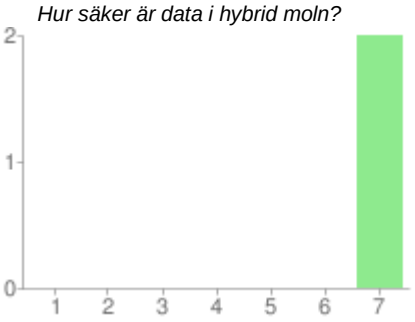


Diagram 4.4.6

Två av tre kunder anser att publikt moln är mycket säkert och en kund anser att det är ganska säkert (se diagram 4.4.1). Alla leverantörer anser att publikt moln är mycket säkert (se diagram 4.4.2). Leverantörerna anser även att privat och hybrid moln är mycket säkert (se diagram 4.4.4 och 4.4.6). Kunderna anser också att privat och hybrid moln är mycket säkert förutom en kund som inte anser att hybrid moln är säkert (se diagram 4.4.3 och 4.4.5). Utifrån resultaten på dessa frågor ser vi att det finns en skillnad mellan kundernas och leverantörernas synpunkter på hur säkra de olika lagringsvarianterna anses vara. Leverantörerna anser att säkerheten i de tre olika lagringsvarianterna är mycket säkra medan kundernas synpunkter skiljer sig en aning. Sett från kundernas perspektiv så är privat moln aningen säkrare som lagringsvariant.

4.5 Prioritering av säkerhetsaspekter

Nedan presenteras en prioriteringslista av säkerhetsaspekter där respondenterna har rangordnat säkerhetsaspekterna utefter vilka som är viktigast att ta hänsyn till. Siffran 1 innebär att respondenten anser att den säkerhetsaspekten skall prioriteras högst och siffran 14 innebär att säkerhetsaspekten skall prioriteras lägst.

Tabell 4.4 Prioriteringslista av säkerhetsaspekter

Säkerhetsaspekter	*Lev1*	*Lev2*	*Lev3*	*Kund1*	*Kund2*	*Kund3*	*Kund4*	*Kund5*
Integritet	12	5	7	4	3	1	2	2
Konfidentialitet	7	4	6	8	8	8	5	4
Tillgänglighet	1	8	5	5	14	7	3	5
Hot mot molntjänst	11	7	4	7	7	14	12	9
Dataintrång	3	6	11	6	4	2	6	7
Åtkomstkontroll	2	10	12	13	10	6	9	10
Backup	5	3	9	12	11	5	8	13
Kryptering	8	11	8	2	2	10	10	12
Auditlogg	9	12	13	14	12	11	14	14
Datasegregation	10	13	10	3	9	3	7	6
Datalokalisering	13	14	14	9	13	4	13	3
Ansvar	4	2	3	10	5	12	11	8
Förtroende	6	1	2	1	1	13	4	1
Juridiska frågor	14	9	1	11	6	9	1	11

För att rangordna säkerhetsaspekterna efter prioritet har vi beräknat svaren från tabellen ovan (tabell 4.4) så att den säkerhetsaspekt som har flest låga nummer är högst prioriterad respektive den som har flest höga nummer är lägst prioriterad. Resultatet är följande:

1. Förtroende
2. Integritet
3. Tillgänglighet
4. Ansvar
5. Dataintrång
6. Konfidentialitet
7. Backup
8. Juridiska frågor
9. Datasegregation
10. Kryptering
11. Hot mot molntjänst
12. Åtkomstkontroll
13. Datalokalisering
14. Auditlogg

4.6 Sammanfattning av empirin

I överlag anser leverantörerna och kunderna att de flesta säkerhetsaspekterna är viktiga att ta hänsyn till i molnet. Alla respondenter anser att det är viktigt att skydda datakonfidentialitet, dataintegritet och att molntjänster alltid bör vara tillgängliga, som även är grundpelare inom datasäkerhet. Alla respondenterna ansåg att det är av absolut yttersta vikt att skydda sig mot manipulation av den data som lagras i molnet. (se 4.1) I frågan om hur viktigt det är att leverantörerna redovisar sitt ansvar anser kunderna att det är mycket viktigt vilket leverantörerna håller med om men de anser inte det vara av lika stor betydelse som kunderna tycker (se 4.2). I överlag så känner kunderna sig trygga med den säkerhet som leverantörerna erbjuder i sina molntjänster (se diagram 4.3.1). Respondenterna i vår undersökning anser att det privata molnet är den säkraste molnvarianterna. Det som är anmärkningsvärt är att respondenterna har skilda åsikter kring de hot respondenterna upplever finnas mot molntjänster. Kunderna fokuserar mer på den tekniska delen i form av att data försvinner, data blir tillgängligt för obehöriga och att tjänsten inte är tillgänglig när de önskar medan leverantörerna anser att den icke-tekniska delen är ett större hot i form av den mänskliga faktorn. Respondenternas åsikter skiljer sig även kring vikten av att känna till vart data lagras samt hur viktigt det är att leverantörer följer standars, bäst praxis och rekommendationer.

5 Analys och diskussion

I detta kapitel analyseras och diskuteras resultatet från den empiriska undersökningen. Kundernas och leverantörernas synpunkter jämförs med varandra och vi diskuterar skillnaderna mellan deras synpunkter med vad teorin belyser. Analysen omfattar en diskussion där vi redogör förståelsen av undersökningens empiri och analyserar kring uppsatsens forskningsfråga.

Baserat på vår undersökning har vår uppsats haft tre delfrågor att besvara. Vi analyserar och diskuterar även i korthet säkerheten i de olika lagringsvarianterna. Detta kapitel lyfter fram diskussion för de främsta resultaten från vår undersökning.

5.1 Integritet, konfidentialitet och tillgänglighet

Den första delfrågan lyder: *vilka är leverantörernas och kundernas ställningstagande kring integritet, konfidentialitet och tillgänglighet*?

En säker tjänst går ut på att integritet och konfidentialitet av data skyddas så att obehöriga inte kommer åt känslig information. På grund av att informationssystem ligger ute på molnet blir kunddatan mer sårbar då många användare har sin information i samma moln. Därför kan det vara viktigt att skydda konfidentialitet och integritet på all data som lagras i molnet. Leverantörerna och kunderna i vår undersökning anser att det är viktigt att skydda konfidentialiteten och integriteten av data i molnet. Det som i vår undersökning skiljer leverantörernas och kundernas åsikter åt är huruvida leverantörer och kunder bör gå tillväga för att ha en säker tjänst och vilka hot som finns mot molntjänster. Våra respondenter menar att förhindrande av dataintrång kan ske på olika sätt beroende på vilken leverantör och vilka tjänster som kunderna hyr. För att förhindra dataintrång, så att obehöriga inte får tillgång till data och på så sätt kan manipulera datan, anser kunderna att leverantörer och kunder bör samarbeta för att på bästa sätt lösa säkerhetsproblem och uppnå hög integritet, konfidentialitet och tillgänglighet (se tabell 4.1). Samarbetet mellan parterna är nödvändigt då ansvarsskyldigheten för dataintrång kan skilja sig åt beroende på leveranstjänstmodell. Det är därför en fördel att lösa ansvarsfrågor innan kunder börjar implementera applikationer till molnet (se delkapitel 2.2.8)

Det finns ett antal olika åtgärder som kan vidtas för att skydda data. Enligt vår undersökning anser leverantörer att leverantörer och kunder bör ha krypterade och säkra förbindelser. Leverantörerna och kunderna är dock eniga om att de gemensamt bör sköta säkerhetsarbetet på alla plan.

Tillgänglighet är en viktig aspekt i datasäkerhet och det är en förutsättning för ett säkert system att det alltid bör vara tillgängligt och funktionellt för de befogade användarna eller kunderna (se delkapitel 2.2.2). Respondenterna i vår undersökning stödjer detta påstående, som diagram 4.1.7 – 4.1.11 och tabell 4.1 visar, de anser att det är viktigt att de alltid har tillgång till sina tjänster och att de ska vara funktionella. Leverantörernas tjänster är enligt våra respondenter alltid tillgängliga och funktionella bortsett från den tid de avser för underhåll av systemet. Enligt leverantörerna stipuleras detta i avtal med kunden och på så sätt kommer de överens om en acceptabel upptid från båda parter (se tabell 4.1). Något respondenterna ansåg som positivt var backup av data. Backup är en viktig säkerhetsåtgärd som leverantörer bör genomföra för att garantera att all känslig kunddata finns tillgänglig för en snabb återställning vid en eventuell katastrof där all data kan gå förlorad (se delkapitel 2.2.5.). I delkapitel 2.2.5 belyses vikten av att en kund bör garanteras att deras tjänst och data på något sätt fortsätter att vara tillgänglig även om en leverantör blir uppköpt eller går i konkurs. Detta är något som kunderna och leverantörerna i vår undersökning reglerat via avtal. Leverantörerna medger att kunder alltid äger rätten till sin data, detta tolkar vi som att kunderna i sådana lägen får tillbaka sin data. Leverantörerna förklarar vidare att de via avtal ger kunden möjligheten att köpa ut sin lösning i de fall kunden vill avbryta kontraktet, att leverantören går i konkurs eller blir uppköpt. Detta bekräftar kunderna genom följande *” Ja, de leverantörer vi accepterar att samarbeta med.” (Kund C).*

I delkapitel 2.2 nämns att datasäkerhet går ut på att skydda integriteten, konfidentialiteten och tillgängligheten av datan och systemen. Majoriteten av de tidigare genomförda undersökningarna, som ni finner i kapitel 2.5, påpekar att integritet, konfidentialitet och tillgänglighet av data är vanligt förekommande säkerhetsbrister i molnet. Vi har funnit att detta stämmer överens med de säkerhetsbrister och hot som kunderna i vår undersökning anser finnas i molnet. Kunderna nämner att de största hoten som finns mot molntjänster är att:

> *”Data försvinner, data blir tillgängligt för obehöriga, datat är inte tillgängligt när jag önskar” (Kund D).*

Kunderna i vår undersökning anser att leverantörer och kunder tillsammans bör avtala om vilka säkerhetsåtgärder som bör vidtas för att uppnå en hög datasäkerhet och för att garantera tillgänglighet av molntjänster. Förutom dessa hot har vi i vår undersökning även funnit att mänskliga faktorn utgör ett av de största hoten mot molntjänster, vilket skiljer sig från det som framgår i litteraturen där det istället framgår att den mänskliga faktorn inte är ett av de absolut största hoten mot molnet (se delkapitel 2.2.4).

> *”Hoten är de vanliga. Dvs molntjänster skiljer sig inte från en traditionell datamiljö. Störst problemet är mänskliga faktorn dvs dåliga processer och rutiner…” (Leverantör A).*

Detta resultat tolkar vi som att leverantören menar att den mänskliga faktorn beror på kundernas dåliga processer och rutiner. Kunderna däremot anser att osäkerheten för hantering av deras data från leverantörernas sida utgör den mänskliga faktorn som ett hot. Den mänskliga faktorn kan enligt oss tolkas på två olika sätt. Den ena tolkningen kan vara att anställda från leverantörernas sida kan missbruka sina rättigheter till kundernas data eller att de anställda från kundernas sida kan vara oaktsamma vad gäller inloggningsuppgifter och dylikt och på så sätt bli ett stort säkerhetsproblem. Den andra tolkningen kan vara att den mänskliga faktorn både medvetet och omedvetet kan ligga bakom hindret av att viktiga säkerhetsåtgärder inte tas i utvecklingsstadiet för molntjänsterna. Detta resultat skiljer sig från vad som framgår i delkapitel 2.2.4. I samma kapitel anses även att i de fall den mänskliga faktorn ligger bakom en säkerhetsincident blir skadan mycket mer allvarlig än vid andra säkerhetsincidenter. Ett sätt att finna sina sårbarheter på och för att skydda sig mot dessa är att göra en riskanalys. Genom riskanalysen får företagen fram vilka sårbarheter de står inför och kan på så sätt överväga vilka säkerhetsåtgärder som bör utföras. Vi tycker att kunder och leverantörer bör se över denna säkerhetsaspekt i större utsträckning och ge den mänskliga faktorn en högre prioritet gällande säkerheten i molntjänster eftersom resultatet i vår undersökning påvisar att det råder skiljande åsikter litteratur, kunder och leverantörer emellan vad gäller den mänskliga faktorn (se citaten ovan). Vi tycker att detta är värt att lyfta fram eftersom datasäkerhet, i form av konfidentialitet, integritet och tillgänglighet, fick alla höga prioriteringar i respondenternas rangordning (se tabell 4.4). Vi tycker då att det är av stor vikt att leverantörer och kunder får en gemensam bild av vilka hot som finns för att kunna lägga vikt på lämpliga säkerhetsåtgärder.

Våra kunder kände till vilka rättigheter och tillgångar leverantörerna har till deras data, vilket är viktigt att ta hänsyn till (se delkapitel 2.5). Kunderna menar att de tar hänsyn till denna aspekt för att veta och reglera leverantörernas åtkomsträttigheter genom:

> *”Specifika SLA för resp system” (Kund B).*

> *”Sekretessavtal bör skrivas med de individer hos leverantören som är administratörer eller på annat sätt kan få tillgång till informationen” (Kund C).*

Leverantörerna i vår undersökning skriver att de har:

> *”… rent tekniskt åtkomst till kunddata men vi har ingen rätt eller intresse att ändra kunddata. Sekretessavtal reglerar detta.” (Leverantör A).*

> *”En superanvändare som har tillgång till all information via ett avancerat gränssnitt och som dessutom kan tilldela andra användare på kundsidan rättigheter.” (Leverantör B).*

Vi tolkar det sista citatet som att leverantörer behöver ha tillgång till all kunddata då de som en superanvändare skall kunna tilldela nya användare (kunder) rättigheter att få tillgång till deras data. Kunderna kan ha känslig data och i dessa fall har kunderna i vår undersökning

reglerat detta genom att inte lägga ut känslig data ute på molnet. Kunderna anser även att de bör skriva ett sekretessavtal med de som är administratörer eller på annat sätt kan få tillgång till kunders information.

5.2 Datalokalisering och Juridiska frågor

Den andra delfrågan gick ut på att ta reda på *Vilka är leverantörernas och kundernas ställningstagande kring datalokaliseringen och de juridiska frågorna som uppkommer med molntjänster och på vilka sätt löser de detta?*

Enligt vår undersökning är förståelse för vart data kan befinna sig och vart det lagras något som varierar från kund till kund. Kundens information kan vara placerad bland andra kunders data (publika moln) eller att kunden får ett eget internt moln så att endast de får tillgång till sin data (privata moln). Dessa olika platser där datan är lagrad på kan leda till att kunder utsätter sig för risker som är viktiga att uppmärksamma som kund. Här finns risken så som att obehöriga kunder från samma moln kan ta del av deras data.

Tabell 4.2, diagram 4.2.1 och 4.2.2 (se delkapitel 4.2) visar att kunderna känner till var deras data lagras men de har blandade åsikter kring hur betydelsefullt det var för dem att känna till vart datan lagras där vissa kunder anser att det är av yttersta vikt och vissa anser det som mindre viktigt. Detta kan vara värt att veta om, då datalokaliseringen och hur leverantören försäkrar att kundens data skyddas på lagligt sätt kan skapa en del problem. Frågan om vem som är behörig till datan kan dyka upp ifall det startas en brottsutredning mellan kund och leverantör. Detta kan skapa ett stort problem för kunden om de inte känner till värdlandets lagar för skydd av känslig information (se delkapitel 2.2.7). Känner kunder inte till vart ens data skickas och vilka länder den temporärt kan hamna riskerar de att inte känna till vilka lagar som gäller vid en säkerhetsincident då dessa lagar kan skilja sig från land till land.

Vad gäller lagringen av data och hur leverantörer garanterar kunderna att deras privata information skyddas på ett lagligt sätt svarar de:

> *”Via avtal. Sedan är det en fråga om förtroende.” (Kund C)*

Kunderna menar att de blir garanterade om detta via avtal och att det sedan handlar om förtroende. Detta tolkar vi som att avtalet mellan dem och leverantörerna inte är en garanti utan snarare ett sätt för leverantörerna att skapa ett förtroende om att de skyddar kundernas data på ett lagligt sätt. Att kunderna i vår undersökning redan har kännedom av vart deras data lagras tror vi har en direkt påverkan i deras anseende av innebörden av att känna till vart deras data lagras.

> *”Data sparas hos oss i Sverige. Stipuleras i avtal.” (Leverantör A)*

De leverantörer som vi undersökt lagrade sina kunders data inom Sverige och att de stipulerar i avtal för att skydda deras data på ett lagligt sätt. De ansåg däremot inte att det är av yttersta vikt för deras kunder att känna till vart datan lagras. I de fall där leverantörer sparar data i

olika länder eller i de fall där leverantörers kunddata hanteras av andra leverantörer anser vi att det är av yttersta vikt för kunderna att:

- Känna till vart datan lagras.
- Vilka lagar som gäller.
- Vilka ansvarsskyldigheter kunder respektive leverantörer har.

Det råder stora meningsskiljaktigheter vad gäller datalokaliseringen i undersökningen. Det är väldigt viktigt som kund att veta var datan lagras (delkapitel 2.2.7). Enligt vår undersökning finns det skillnader mellan respondenternas åsikter om vikten av att känna till vart datan befinner sig vilket inte våra respondenter anser då få tycker att det är av stor vikt.

Den lilla avvikelse som vi ser enligt diagram 4.2.3 visar att det är viktigt att leverantörer sköter sitt ansvar samtidigt som leverantörerna själva anser det vara viktigt för kunden. Men det som är anmärkningsvärt är att kunder är ansvarsskyldiga för sina tillgångar, inklusive ytterligare tillgångar som har lagts ut av leverantörerna (se delkapitel 2.2.8). Detta är något kunder bör uppmärksamma och känna till.

Vi tycker att det är viktig att ta hänsyn till datalokaliseringen och ha kännedom av vart kunders data lagras. Vi tycker därför att det är underligt att respondenterna inte ansåg detta som en viktig aspekt då de tycker att datalokalisering bör prioriteras som en av de lägst prioriterade säkerhetsaspekterna (se tabell 4.4).

5.3 Förtroende mellan kund och leverantör

Den tredje delfrågan i vår uppsats är att *se hur pass viktigt förtroendet mellan kunderna och leverantörerna är för att uppfylla den säkerhet som krävs i datormolnet*.

Vi har i vår undersökning funnit att det förekommer olika grader av förtroende mellan kund och leverantör vilket är i linje med det som anses i delkapitel 2.2.9 där det framhävs att det inte finns några lösningar som kan övertyga att molntjänsterna är pålitliga, förtroendet varierar från organisation till organisation.

Att gå ut i molnet innebär att kunden lämnar över sina datorresurser till någon utomstående leverantör därför är det väldigt viktigt att kunder har ett stort förtroende till sin leverantör vilket kunderna i vår undersökning har. Hantering av data och dess skydd kommer leverantörerna och kunderna i vår undersökning överens om genom avtal (se tabell 4.3). Genom vår undersökning finner vi att det finns ett samband mellan skydd av data, avtal och förtroende. Då datan kan vara värdefull för kunden kommer kunder och leverantörer överens om hur de ska skydda datan genom avtal. Dessa avtal är enligt våra respondenter viktiga för skydd av data som även teorin i 2.2.9 anser vara viktigt för det förtroende som skapas mellan kunder och leverantörer. En av kunderna bekräftar även att skyddet av datan hanteras genom avtal samt uttrycker att ” *Sedan är det en fråga om förtroende.”*

Vi har i vår undersökning funnit en mindre avvikelse från diagram 4.3.1 som visar att hälften av kunderna känner sig mindre trygga än vad leverantörerna tror om kunders trygghet, men kunderna känner sig dock trygga.

I vår undersökning ställde vi leverantörerna två frågor gällande öppenheten från deras sida genom att fråga dem om de följer några säkerhetsstandards och rekommendationer samt om de publicerar dessa och deras procedurer så att kunderna kan ta del av dessa.

> *”Vi dokumenterar processerna enligt branschpraxis som kallas ITIL.”, ”Ja det händer att man går igenom vissa processer vid avtalsskrivningar.” (Leverantör A)*
>
> *”Nej”, ”Inte ännu.”(Leverantör B)*

Att det förekommer öppenhet bekräftas i vår undersökning genom en leverantör (Leverantör A) som förklarar, enligt citaten ovanför, att leverantören dokumenterar sina processer och att de kan dela med sig denna i avtalsskrivningar. Denna öppenhet är något att ta hänsyn till för att öka förtroendet enligt teorin i 2.2.9.

Den andra leverantören (Leverantör B) medger att de inte följer några säkerhetsstandards och rekommendationer och att de ännu inte delar med sig av varken dessa eller sina procedurer. Det första citatet ovan (Leverantör A) är svaret på frågan om de följer någon säkerhetsstandards eller rekommendationer. ITIL är inte en säkerhetsstandard för molntjänster och vi tolkar detta som att leverantörerna inte följer någon sådan vilken de kan påstå att deras molntjänst vara säker i en accepterad grad utifrån dessa standards. Om detta är fallet så följer inte leverantörerna i vår undersökning den riktlinje som tidigare undersökningar förmedlar för att bygga upp ett förtroende (se delkapitel 2.2.9).

Det som är mest anmärkningsvärt och vi det vi tycker är intressant när det gäller standards är att kunderna och leverantörerna i vår undersökning hade varierande åsikter vad gäller vikten av att följa standards och rekommendationer. Kunderna i överlag anser att det är väldigt viktigt att leverantörerna följer säkerhetsstandards, ISOs och andra rekommendationer. Däremot anser leverantörerna inte att det är av stor vikt att följa dessa. Leverantörernas åsikter om att följa standards och rekommendationer skiljer sig från det som framhävs i teorin, se delkapitel 2.2.9, samt kundernas åsikter. Eftersom leverantörerna inte följer säkerhetsstandards och rekommendationer samt att en leverantör inte publicerar sina procedurer kan detta vara anledningen till att kunderna inte är lika trygga med säkerheten som de erbjuds jämfört med vad leverantörerna tror. Vi tycker att standards, rekommendationer och öppenhet är något som leverantörer bör ta hänsyn till då förtroende mellan kund och leverantör prioriteras högst av säkerhetsaspekterna (se tabell 4.4).

I de fall kunder hyr en molntjänst från en leverantör och den leverantören har någon form av underleverantör så garanterar kundens huvudleverantör att deras säkerhetspolicys gäller för alla inblandade parter (se tabell 4.3).

5.4 Säkerhet i lagringsvarianterna inom datormolnet

Som en slutlig uppföljning av hur leverantörer och kunder ställer sig kring säkerheten i molnet ville vi se *hur säkra de olika lagringsvarianterna anses vara av leverantörer och kunder*.

Det är säkert många företag och privatpersoner som har planer eller är intresserade av att gå ut i molnet och undrar vilken lagringsvariant som är säkrast att lagra data i. Tillvägagångssättet för att skydda information så att obehöriga inte kommer åt datan kan variera beroende på lagringsmodell.

Baserat på undersökningen i sin helhet så är säkerheten i de tre lagringsvarianterna av en accepterad värde från både kundernas och leverantörernas sida. Båda parter har värderat säkerheten högt i undersökningen. Vår undersökning visar en enighet bland kunder och leverantörer om att det privata molnet är aningen säkrare lagringsvarianten att lagra sin data i. Detta kan bero på det att data i privata moln är lagrad i ett internt datacenter och inte är tillgänglig för allmänheten (se delkapitel 2.1.4).

Generellt från resultatet av tabellerna 4.1 och 4.3 i resultatdelen av vår undersökning finns en ganska tydlig bild av att respondenterna generellt upplever en hög säkerhetsvärde i lagringsvarianterna och detta kan därför ha samband med kundernas avvisande syn på att känna till vart deras data befinner sig och att de har god tro för leverantörerna. Detta kan bero på att de förlitar sig på att leverantörerna sparar deras data på en plats som gynnar dem.

6 Slutsatser

Vårt syfte är att belysa molntjänstleverantörernas och kundernas synpunkter kring säkerheten i datormolnet, det vill säga att vi vill identifiera de säkerhetsaspekter molnleverantörer och kunder anser vara av stor vikt respektive mindre vikt gällande säkerheten samt vilka åtgärder leverantörer respektive kunder utför eller bör utföra för att skapa en säkrare molnmiljö.

Leverantörerna och kunderna anser att det är av yttersta vikt att skydda kunders data i molnet samt att deras tjänster alltid ska vara tillgängliga. Leverantörerna och kunderna har i avtal reglerat att deras molntjänster är tillgängliga både på kort och långt sikt, även i de fall leverantören blir uppköpt eller går i konkurs. Leverantörerna tycker att kunder och leverantörer bör skydda konfidentialitet och integritet av data genom att ha krypterade och säkra förbindelser, starka lösenord, dubbla brandväggar, inloggningar i form av HTTPS etcetera. Kunderna däremot tycker att kunder tillsammans med leverantörer bör gå igenom den säkerhet som behövs och komma överens om vilka säkerhetsåtgärder leverantörer respektive kunder bör ta.

Då leverantörerna menar att man har tillgång till all kunddata som superanvändare för att exempelvis kunna tilldela nya användare rättigheter, anser leverantörerna och kunderna att man bör skriva sekretessavtal där kunderna blir garanterade att deras data skyddas på ett lagligt sätt.

Kunderna och leverantörerna i vår undersökning har rangordnat säkerhetsaspekterna utefter hur viktiga säkerhetsaspekterna upplevs och bör prioriteras. Resultatet av detta ser ni i tabell 6.1.

Tabell 6.1 Resultat av prioriteringslista

1. Förtroende
2. Integritet
3. Tillgänglighet
4. Ansvar
5. Dataintrång
6. Konfidentialitet
7. Backup
8. Juridiska frågor
9. Datasegregation
10. Kryptering
11. Hot mot molntjänst
12. Åtkomstkontroll
13. Datalokalisering
14. Auditlogg

Vi har i vår undersökning funnit tre intressanta säkerhetsaspekter som är värda att lyfta fram. I dessa säkerhetsaspekter har vi funnit delade åsikter mellan tidigare undersökningar, kunder och leverantörer. Dessa tre är: *de kändaste hoten mot molntjänster*, *datalokalisering och juridiska frågor samt förtroende*.

Leverantörer och kunder har delade åsikter angående kända hot som finns mot molntjänster, där kunderna är mer osäkra på de tekniska aspekterna då de anser att förlust av data, obehörig får tillgång till data och att tjänster inte är tillgängliga när de behöver dem medan leverantörerna menar på att den mänskliga faktorn i form av slarv och oaktsamhet av kunder tillsammans med krånglande teknik utgör de största hoten mot molntjänster.

Det är intressant att känna till att varken kunder eller leverantörer, från vår undersökning, anser det vara av stor vikt för kunderna att ha kännedom om vart deras data lagras. De kompletterar detta genom att i avtal stipulera vilka lagar som gäller i de fall dessa skulle sparas i andra länder. Leverantörerna och kunderna anser även att ansvarighet utgör en viktig roll för säkerheten i molnet. Det är även intressant att kunder och leverantörer prioriterat kännedom av datalokaliseringen lågt i rangordningen av säkerhetsaspekterna (se tabell 6.1).

Kunderna anser att det är viktigt att leverantörerna följer standards och rekommendationer. Leverantörernas åsikter skiljer sig en aning då de anser att det är mindre relevant. Detta trots att förtroende har prioriterats högst av alla säkerhetsaspekter (se tabell 6.1). Det råder skillnader i hur leverantörerna hanterar sina säkerhetspolicys och öppenhet. En leverantör publicerar sin säkerhetspolicy och sina processer på något sätt så att deras kunder kan ta del av dessa medan en leverantör inte publicerar detta. Standards, rekommendationer och öppenhet förknippas i litteraturgenomgången och i tidigare undersökningar med förtroende och är alla faktorer för att bygga upp förtroende genom. Leverantörerna är dock eniga om att deras säkerhetspolicy gäller för alla inblandade i de fall andra leverantörer kan vara inblandade. Som ett helhetsintryck är kunderna trygga med sina leverantörer.

Då vi haft en förväntan på att molnet inte är så säkert som vi önskat, speciellt i publikt moln har denna undersökning visat motsatsen. I helhet anser kunderna och molntjänstleverantörerna i vår undersökning att alla lagringsvarianter är väldigt säkra, men de anser dock att privat moln är den säkraste av dem även om detta inte är med stora marginaler.

6.1 Förslag till vidare forskning

I vår undersökning anser kunderna att de känner en osäkerhet kring hur leverantörerna hanterar deras information. Leverantörerna anser att dåliga processer och rutiner av kunderna som ett hot. Det hade varit intressant att forska vidare om hur ofta eller på vilka sätt den mänskliga faktorn ligger bakom säkerhetsproblem i organisationer eller för molntjänster.

6.2 Undersökningens begränsningar

I vår undersökning har vi fokuserat på datalokalisering som en del av vår undersökning och som utgör en av våra delfrågor. De leverantörer som vi undersökt lagrade sina kunders data inom Sverige och ansåg inte de vara av yttersta vikt för deras kunder att känna till om. Datalokaliseringen begränsades genom att vi inte undersökte leverantörer och kunder vars data sparas utanför Sverige. Det hade varit intressant att veta hur det påverkar värdet av att ha kännedom om vart ens data är lagrad, i de fall datan lagras i länder där andra lagar kring skyddandet av data råder.

Bilagor

Bilaga 1

Ordförklaringar

SaaS - Användandet av mjukvara över nätet utan att behöva installeras på datorn erbjuds som en tjänst.

PaaS - Används till att bygga och driva webbaserade applikationer. Bygga applikationer utan att behöva köpa mjukvara eller hårdvara erbjuds som en tjänst.

IaaS - Leverans av it utrustning, det är vanligtvis en plattform av en virtualisationsmiljö som en tjänst.

Datormolnet eller molnet - Är baserat på användning av datorer och applikationer över Internet. Som användare kan man tillhandhålla resurser som processorkraft, lagring och funktioner som tjänster på Internet.

Molntjänstleverantör - En leverantör som hyr ut molntjänster.

Kund - Användare av molntjänster

Konfidentialitet - Förhindra obehörigas informations läsning

Integritet - Förhindra obehörig dataändring

Tillgänglighet - Skydd av tillgängligheten innebär att man alltid har tillgång till tjänster eller system

Data segregation - Man separerar användares data från andra användare

Bilaga 2

Motivering av valda enkätfrågor

Frågor i form av värderingskala

1. Hur säker är data i molntjänster?

a) Publikt moln?(*Med publikt moln menar vi när man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen***)**

b) Privat moln? (*Med privatmoln menar vi interna datacenter av en verksamhet eller organisation som inte görs tillgängliga för allmänheten***)**

c) Hybrid moln? (*Med hybrid moln menar vi en kombination av både publikt och privat moln***)**

Publika, privata och hybrida moln är där hårdvara och mjukvara lagras på olika sätt, detta är en väldigt viktig del i datormolnets struktur som beskriv i vår teori som ni finner i kapitel 2.1.5. Vi har ställt denna fråga även till kunderna. Vi ville veta hur bra eller mindre bra säkerheten är i de olika molntyperna för att kunna komma i underfund med leverantörens säkerhetsställningstagande i den här aspekten av datormolnet. Vi jämföra hur säkra leverantörerna respektive kunderna upplever de olika molntyperna för att se ifall de har en liknande syn eller om deras uppfattningar skiljer sig och hur detta påverkar leverantörerna och kunderna i detta syfte.

2. Hur viktigt tror ni det är för kunderna att ingen kan ta del av deras data i datormolnet? (*kundperspektiv***)**

Detta är en konfidentialitetsfråga som finns i vår teori, 2.2.2, där vi tar upp och beskriver konfidentialitet, det vill säga skyddandet av privat och organisatorisk data. Vi ställt denna fråga för att se hur viktigt molntjänsleverantörerna tror att kunderna tycker att ingen ska kunna ta del av deras data i datormolnet. Till kunderna har vi ställt frågan hur viktigt de tycker angående samma fråga. Detta gjorde vi för att kunna se om synen för hur leverantörerna och kunderna skiljer sig i denna fråga.

3. Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är:

a) tillgängliga

b) funktionella

c) säkra (*med säkerhet menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser.)*

Till kunderna har vi ställt samma fråga fast hur viktigt de tycker att de tre delfrågorna är.
Detta är en säkerhetsfråga som vi tagit både från vår teoridel, 2.1.3, där vi beskriver dessa tre ämnen och dess betydelse samt från tidigare genomförda undersökningar som ni finner i 2.5. Med säkerhet menar vi enligt assurance att det finns en grad av förtroende att säkerhetsåtgärder utförs både tekniskt och operationellt för att skydda känslig data och viktiga resurser. Med denna fråga vill vi få reda på hur viktigt leverantörerna tror att kunderna anser att tillgängligheten, funktionaliteten och säkerheten vara i molntjänster. Med hjälp av svaren på denna fråga av leverantörerna respektive kunderna kan vi dra en slutsats om hur viktigt det är att molntjänster är tillgängliga, funktionella och säkra samt vad de två parterna tycker och tror om dessa egenskaper.

4. Hur viktigt är tillgängligheten för er som erbjuder en molntjänst?

Denna säkerhetsfråga har vi tagit precis som i ovanstående fråga utifrån vår teoridel, 2.2.2, där vi beskriver betydelsen av tillgänglighet av system och mjukvaror. Detta är även kopplat till tidigare genomförda undersökningar som ni finner i 2.5. Denna fråga är en fortsättning till frågan ovanför som hjälper oss att få en bättre bild om hur viktigt det är för leverantörerna att deras tjänster alltid är tillgängliga. Med denna följdfråga kan vi se ifall det finns några skillnader eller likheter med vad leverantörerna tycker om tillgänglighet och vad dom tror kunderna tycker om det jämfört med vad kunderna i själva verket tycker. Här vill vi också se om det är någon skillnad på vad leverantörerna tror kunderna anser om tillgängligheten och vad de själv tycker om det. Detta vill vi veta för att dra en slutsats om det är någon skillnad på hur viktigt leverantörerna och kunderna tycker säkerheten är.

5. Hur viktigt tror ni det är för kunderna att de vet vart deras data/information lagras?

Vi har ställt en liknande fråga till kunderna där vi frågar dem om det är viktigt för dem att veta vart deras data lagras. I kapitlet 2.5 tidigare genomförda undersökningar tar vi upp vikten för kunder att veta vart deras data lagras och ni kan även finna teori om datalokalisering i kapitel 2.2.4. Denna fråga ställer vi för att se om leverantörerna och kunderna tycker olika om vikten av att känna till vart kundernas data lagras. Enligt Subashini och Kavitha (2010) är det viktigt att kunderna vet vart deras data är lagrat då juridiska lagar om hantering av data varierar i olika länder. Att ha kännedom om vart leverantörerna lagrar kundernas data är viktigt för kunderna så att de är medvetna om den säkerhet som gäller för deras lagrade data.

6. Hur viktigt tror ni det är för kunderna att ni gör regelbunden backup på deras data/information?

Vi har även frågat kunderna hur viktigt de tycker att det är att leverantörerna gör regelbunden backup på deras data. Genom att få reda på hur viktigt leverantörerna tror att kunderna tycker det är med regelbunden backup och

detta stämmer överens med kundernas svar, kan vi dra slutsatsen att en backup är en viktigt eller mindre viktig funktion som efter deras svar är högt eller mindre efterfrågad. Denna fråga behöver vi för att se om leverantörernas och kundernas om de har samma åsikter eller som dessa skiljer sig åt vad gäller backup samt för att kunna analysera om deras svar överensstämmer med vad teorin säger om att ta regelbunden backup.

7. Hur viktigt tror ni ansvarighet (accountability) på säkerheten är för kunderna?

Kunderna har också fått en fråga om hur viktigt de tycker att man har klart för sig vem som har ansvarighet för säkerheten är för kunderna. Denna fråga kopplas till datasäkerhet i teorin som ni finner i kapitel 2.2.7, där accountability innebär att man spårar en säkerhetsbrist till en ansvarig part. Denna fråga är viktig enligt Julisch & Hall (2010) att det är bestämt vem som är ansvarig för vad. Vi vill då veta om kunderna tycker det är viktigt att ha möjligheten att spåra olagliga aktiviteter för att finna en ansvarig person då givarna inte har skyldighet att finna ansvarig för en sådan händelse.

8. Hur viktigt är det att kunderna är säkra mot att ingen skall kunna manipulera deras information?

Till kunderna har vi formulerat frågan så att vi får svaret på hur viktigt de tycker det är att säkra mot att ingen obehörig ska kunna manipulera deras data. Denna fråga kopplas till teorier kring datasäkerhet i kapitel 2.2.2 där dataintegritet beskrivs. Detta är en viktig fråga för vår frågeställning gällande säkerhet då vi vill få reda på hur viktig det är för kunderna att inte få sin data förändrat av någon obehörig.

9. Hur trygga tror ni att era kunder känner sig med den säkerhet som ni erbjuder i era molntjänster?

Denna fråga kopplas till vår teori gällande datasäkerhet som ni finner i kapitel 2.2.9 där beskrivs trovärdig säkerhet om att den grad av förtroende som någon har för att säkerhetsåtgärder skall utföras för att skydda sin egen information eller data från bland annat intrång. Även författare Khan & Malluhi (2010) tar upp vikten av förtroende och tillit. Denna fråga är viktig för oss då vi vill få reda på hur säkra och trygga kunderna känner sig för att utnyttja en molntjänst, detta vill vi veta då tjänster över Internet aldrig kan vara helt säkra och kräver istället någon grad av tillit eller förtroende för att mäta kundernas och givarnas uppfattning om vad de tycker om säkerheten. Med hjälp av svaren på denna fråga kan vi dra en slutsats om kundernas tillit och förtroende kan ha någon inflytande i hur säkra molntjänster är.

10. Hur viktigt är det att kundernas data är krypterad och segregerad från andra kunders data i molntjänster?

Kunderna har fått frågan om hur viktigt det är för dem att deras data är krypterad och segregerad från andra kunders data i molntjänster. Denna fråga hänvisar vi till vår teori i kapitel 2.2.8 där vi beskriver allmänt om vad kryptering är, samt artiklar som beskriver den vikt av att segregera data som ni finner i 2.2.5. Annan tänkbar teori kan vara åtkomstkontroll. Vi vill veta hur viktigt det är för kunderna samt givarna om att segregera kundernas data ifrån varandra så att ingen obehörig kan komma åt en annans kunds data. Detta är viktigt för oss att veta då många kunders data brukar samlas i samma moln.

11. Hur viktigt är det att följa säkerhetsstandards, så som ISOs etc, och hur viktigt tror ni det är för kunder att ni följer sådana rekommendationer?

Säkerhetsstandards så som ISOs och andra typer av certifikationer refererar vi till ENISA, CSA, NIST där de beskriver de standards som finns. Denna fråga är viktig för att besvara då vi vill veta vad kunderna tycker om att givare skall följa rekommendationer som är framtagna för att hålla en accepterad säkerhet i molnet. Detta är intressant för vår forskningsfråga då säkerhetsstandards fungerar som checklistor för krav och villkor som leverantörer och kunder kan följa för att försäkra sig om att deras molntjänst är relativt säker jämfört med andra molntjänster inom samma område.

Intervjufrågor

1. Vilka sorters molntjänster erbjuder ni?

Vi har för att komplettera denna fråga har vi även ställt kunderna en fråga om vilka tjänster de hyr. Vi vill veta vilka olika molntjänster de erbjuder för att veta respektive företags erbjudanden till kunderna och vilka tjänster de respektive kunderna hyr. Med dessa frågor vill vi se om det finns någon koppling mellan vilka tjänster de hyr eller erbjuder mot hur säkra de upplever de olika molntyperna och hur viktigt de anser vissa säkerhetsaspekter vara.

2. Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive kunderna bör skydda sig mot dessa?

Denna fråga ser precis likadan ut för både leverantörer och kunder. Denna fråga baseras på teori gällande datasäkerhet som ni finner i kapitel 2.1.3 där olika hot beskrivs som en möjlig säkerhetsrisk för en tillgång. Även Brodkin (2008) beskriver vilka hot och säkerhetsbrister är mest kända och förekommer oftast. Vi vill veta vilka hot som är mest kända då det är intressant och viktigt för vår forskningsfråga att få fram de hot som kunder och givarna anser vara viktiga och uppmärksammade av. Vi vill jämföra svaren från kunderna och leverantörerna mot varandra för att se om de upplever liknande eller olika hot. Med resultaten av denna fråga vill vi jämföra och kontrollera om detta är samma hot och säkerhetsbrister som Brodkin (2008) kommit fram till tillsammans med de vi tagit upp i kapitel 2.2.2. Att få deras syner på vad de tycker att de själva respektive motpartnern behöver göra för att skydda sig mot dessa är ett sätt att se vad de anser vara ansvariga för vad gäller dessa hot.

3. Vilka säkerhetsåtgärder bör ni respektive kunderna ta för att förhindra dataintrång i era molntjänster?

Vi ställde samma fråga till kunderna omvänt. I vår teori i kapitel 2.2.2 tar vi upp integritet och konfidentialitet vilket går ut på att man ska skydda sin data så att obehöriga inte får tillgång och kan manipulera den data man har ute i molnet. Med denna fråga vill vi få svar på vilka säkerhetsåtgärder leverantörer och kunder bör ta för att förhindra dataintrång. Svaren från denna fråga bör ge oss ett resultat på vad för krav och förväntningar leverantörer och kunder har vad gäller att skydda sig mot dataintrång. Detta tog vi med eftersom dataintrång är en av de vanligaste säkerhetsbristerna som Subashinin (2010) och Kaufman (2009) tycker är viktigt att skydda sig emot.

4. Hur försäkrar ni era kunder att deras privata information skyddas på ett lagligt sätt. Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?

Både leverantörer och kunder har fått denna fråga där vi formulerat till kunderna på vilket sätt leverantörerna försäkrar dem för vilka lagar som gäller. Vi vill med denna fråga ta reda på om leverantörerna har tänkt på huruvida en rättslig process går till och vilka lagar som gäller angående kunders data beroende på vart datan sparas geografiskt. Med denna fråga vill vi även ha ett svar på ifall de ger sina kunder något att luta sig på genom att försäkra dem att förklara vilket/ vilka länders lagar gäller innan de tecknar ett avtal.

5. Erbjuder ni någon form av kryptering av kundernas sparade data i molnet? Om ja gå till fråga....

Teori om kryptering finner ni i kapitel 2.2.5 och 2.5. Vi vill med denna fråga jämföra om leverantörerna tror att kryptering är viktigt för sina kunder och ifall de i praktiken erbjuder någon kryptering med vad kunderna verkligen tycker om vikten av kryptering.

6. Vad är anledningen/anledningarna till att ni inte krypterar deras data, har ni någon annan lösning så att andra kunder inte kan ta del av data som inte är deras?

Detta är en följdfråga till frågan ovanför där vi vill få reda på anledningarna till att leverantören valt att inte kryptera data för kunderna. Vi vill veta anledningarna varför de inte krypterar data för att det inte fråga 5 ska vara missvisande om fallet är att de inte krypterar data eftersom det kan uppfattas att de inte tycker kryptering av data är viktigt i fall de inte gör detta.

7. Erbjuder ni era kunder någon form av auditlogg där ni och/eller era kunder kan följa upp vad som sker i de system och molntjänster ni erbjuder. Om ja gå till fråga …

Vi ställer frågan till kunderna med och kontrollera om deras leverantörer erbjuder en sådan möjlighet. Den här frågan hänvisar vi till vår teori som ni finner i 2.2.8, som handlar om åtkomstkontroll som bland annat består av en självständig del så kallad audit som testar funktionsduglighet. Vi vill ta reda på om det finns auditloggar för givarna samt kunderna att följa upp de aktiviteter som händer. Vi vill se om leverantörerna eller kunderna genom en auditlogg kan följa upp vad som skett vid ett problem av det system eller den tjänst de erbjuder/ hyr för att på så vis enklare kunna rätta till de problem som uppstår.

8. Om nej, varför anser ni detta inte nödvändigt i de fall kunderna inte själv valt bort detta?

Med denna följd fråga vill vi ta reda på varför givarna väljer att inte ha någon auditlogg för sina kunder och om kunderna har valt bort möjligheten är vi intresserade av deras ställning till varför de väljer bort denna möjlighet. Det gör vi för att det inte ska vara missvisande och uppfattas som en mindre viktig om anledningen skulle vara en ekonomisk fråga eller dylikt.

9. Hur försäkrar ni att kundernas hyrda molntjänster alltid är tillgängliga och funktionella?

Formuleringen till kunderna är utformade så att de svarar på vilket sätt deras leverantörer försäkrar att kundernas molntjänster alltid är tillgängliga och funktionella. Denna fråga är baserad på vår teori gällande datasäkerhet som ni finner i kapitel 2.2.2 där tillgänglighet och funktionalitet beskrivs. Vi vill veta om hur molntjänstgivarna ställer sig till att försäkra och ge ett förtroende om att deras tjänster alltid är tillgängliga för kunden. Eftersom datasäkerhet bygger på bland annat tillgänglighet vill vi följa upp denna fråga med värdeskala för att kontrollera om leverantörerna på något sätt försäkrar dem att deras molntjänster alltid är tillgängliga och funktionella. Om en försäkran på något sätt görs från leverantörernas sida bevisar för oss att de tycker att tillgängligheten och funktionaliteten på molntjänster är en viktig aspekt.

10. Vilka åtkomsträttigheter har ni inom de tjänster ni erbjuder att komma över och/ eller ändra kundernas information och till vilket syfte?

Detta är en fråga som är uppmärksammad i de resultat som Subashinin (2010) och Brodkin (2008) kommit fram till, som enligt författarna är viktigt för kunderna att veta vilka rättigheter leverantörerna har över kundernas data. Vi vill få reda på hur leverantörerna ställer sig till det och vad kunderna tycker om att deras information kan kommas åt av givarna.

11. Känner era kunder till vart deras data lagras?

Vi vill få reda på om kunderna vet var deras privata information är lagrad då detta kan påverka kundernas juridiska rättigheter. Vi vill med denna fråga följa upp fråga 5 från de skalbara frågorna om kunderna får reda på vart deras data lagras för att veta vilka lagar som gäller i de fall hanteringen av data kan gå till juridiska handlingar.

12. Följer ni någon/några säkerhetsstandards så som ISOs eller andra rekommendationer, i så fall vilka?

Vi vill veta vilka standarder som de använder eller andra rekommendationer för att få en bättre inblick i deras säkerhet. Vi vill få en överblick över deras säkerhet så att vi kan förstå helheten vad gäller deras ställningstagande kring säkerheten i datormolnet. Utifrån svaren här kan vi göra en bedömning för vilken grad av säkerhet leverantörerna har på de molntjänster som de erbjuder. Genom att en leverantör följer säkerhetsstandards och andra rekommendationer kan leda till kunderna känner en sorts trygghet gentemot sina leverantörer.

13. Publicerar ni era säkerhetspolicys och procedurer så att kunderna kan ta del av dessa?

Pauley (2010) menar att man bygger någon form av tillit då kunderna har kännedom om leverantörernas säkerhetspolicy och procedurer genom att de kan jämföra deras sätt att arbeta på med vad säkerhetsstandard och rekommendationer säger. Detta tar vi med för att se om leverantörerna använder denna metod för att bygga ett förtroende och tillit mellan dem och deras kunder.

14. Gäller era säkerhetspolicy för alla molntjänstleverantörers tjänster, i de fall andra leverantörer är inblandade?

Pauley (2010) skriver att det är viktigt att ta hänsyn till detta. Vi håller med detta eftersom vi tycker att kunderna bör veta att säkerhetspolicyn gäller för alla parter i de fall någon annan leverantör än de leverantörer de hyr molntjänster från är inblandade. Med denna fråga vill vi se om leverantörerna har några krav på att alla delar i deras tjänster är säkra genom att samma säkerhetspolicy gäller för alla inblandade parter från leverantörernas sida.

15. Vilka SLAs erbjuder ni era kunder? Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om.

Vi frågade även kunderna vilka SLAs som deras leverantörer erbjuda. Takabi et al. (2010) skriver att SLA är ett avtal mellan de två partena där man skriftligt kommer överens om olika ansvar och garantier. Detta är ett sätt att uppnå en överenskommelse mellan leverantörer och kunder där man bestämmer vem som står för vad och en servicenivå. Vi har tagit med denna fråga för att se vad leverantörerna respektive kunderna tycker är viktigt att ha klart för sig vad gäller säkerheten i molnet.

16. Om det skulle vara så att ert företag går i konkurs eller blir uppköpt av något stort företag, hur försäkrar ni kunderna att deras data ej går förlorad och det fortsätter att vara tillgängligt?

Då tillgängligheten är en av byggstenarna för datasäkerhet, teori om datasäkerhet finner ni i kapitel 2.2.2, är det viktigt att ett system alltid är tillgängligt. Men vad händer om ett företag går i konkurs eller köps upp av ett större företag. Brodkin (2008) menar att kunder bör veta vad som händer med deras data vid sådana händelser och vi ställer därför denna fråga för att kolla om leverantörerna försäkrar att kundernas data är tillgängliga även efter en sådan händelse.

17. Har ni något som ni tror skiljer er från andra molntjänstleverantörer angående säkerheten, i så fall vad?

Denna fråga tog vi med för att se om leverantörerna tar hand om någon annan viktig säkerhetsbrist än de vi har funnit utifrån den teori som vi presenterar i kapitel 2 och tidigare genomförda undersökningarna som ni finner under 2.5.

18. Hur försäkrar ni era kunder återskapande av data i de fall där en olycka eller naturkatastrof sker?

Detta är en säkerhetsfråga som påverkar recovery där vi beskriver det. Vi vill veta hur molntjänstleverantörerna gör för att förhindra att förlora kundernas information. Den här informationen behöver vi för att kunna få ett resultat för hur leverantörerna ställer sig i denna fråga då det enligt Brodkin (2008) anser det vara viktigt för kunder att vara säkra på att deras data finns tillgängligt även om en olycklig händelse inträffar.

Bilaga 3

B3.1 Enkätformulär för kunder

Säkerheten i cloud computing

Hej, vi är tre studenter som studerar det systemvetenskapliga programmet i lunds universitet och skriver ett examensarbete.
Detta arbete handlar om säkerhet i datormolnet (Cloud Computing) för att vara mer specifika så vill vi få mer information om molntjänstleverantöremas och kundernas ställningstagande kring säkerheten inom cloud.
Ifall det känns påträngande eller annat som gör att ni inte vill svara på en fråga så går det bra att hoppa över denna.

* Required

Personlig bakgrund

Företagsnamn *

Vill Ni vara anonyma? *
(Företagetsnamnet och ert namn kommer inte vara tillgängligt för läsarna)

- [ ] Ja
- [ ] Nej

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen? *

Skulle Ni vilja ta del av materialet när det är färdigt ? *

- [ ] Ja
- [ ] Nej

Frågor del 1

Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1. Hur säker är data i:

Publikt moln (Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)

	1	2	3	4	5	6	7	
Inte viktig	○	○	○	○	○	○	○	Mycket viktig

Hur säker är data i:
Privat moln (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

Hur säker är data i :
Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

2. Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

3. Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är - Tillgängliga

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är - Funktionella

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är - Säkra
Med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser.

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

4. Hur viktigt är det för er att ni vet vart er data/information lagras?

	1	2	3	4	5	6	7

2. Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive leverantörerna bör skydda sig mot dessa?

3. Vilka säkerhetsåtgärder bör ni respektive leverantörerna ta för att förhindra dataintrång i era molntjänster?

4. Hur försäkrar era molntjänstleverantörer att er privata information skyddas på ett lagligt sätt?
(Med lagligt sätt menar vi vilka lagar som gäller i de fall där er data är sparad i andra länder där andra lagar gäller)

5. Erbjuder er molntjänstleverantör någon form av kryptering av er sparade data i molnet?
(Om Ja gå till fråga 7)

6. Vad är anledningen/anledningarnar till att de inte krypterar er data?

7. Erbjuder er molntjänstleverantör någon form av auditlogg där ni och/eller era leverantörer kan följa upp vad som sker i de systemet/molntjänst de erbjuder
(Om Ja gå till fråga 9)

8. Om nej, har ni själva valt bort någon form auditlogg.

9.Hur försäkrar er molntjänstleverantör att era hyrda molntjänster alltid är tillgängliga och funktionella?

10. Vilka åtkomsträttigheter har er molntjänstleverantör inom de tjänster ni hyr att komma över och/ eller ändra er information och till vilket syfte? .

11. Känner ni till vart er data lagras?

12.Har ni på något sätt kunnat ta del av molntjänstleverantörernas säkerhetspolicies och procedurer?

13. Vilka SLAs erbjuder er molntjänstleverantör?
(Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om)

14. Ifall det skulle vara så att er molntjänstleverantör skulle gå i konkurs eller bli uppköpt, har ni på något sätt blivit försäkrade att er data ej går förlorad och att det fortsätter att vara tillgängligt?

15. Finns det något som skiljer er molntjänstlevernatör från andra leverantörer angående säkerheten, i så fall vad?

Vi är mycket tacksammaför att ni har tagit er tid att ställa upp på denna intervju och om ni har några frågor eller synpunkter så är ni välkommna att kontakt oss.

Kontaktperson
Amir Dzindo
Tlf: 0722 11 13 40
Mail: infa07adz@student.lu.se

Med vänliga hälsningar
Amir Dzindo, Rebin Osman, Fisnik Qeriqi

Submit

B3.2 Enkätformulär för leverantörer

Säkerheten i cloud computing

Hej, vi är tre studenter som studerar det systemvetenskapliga programmet i lunds universitet och skriver ett examensarbete.
Detta arbete handlar om säkerhet i datormolnet (Cloud Computing) för att vara mer specifika så vill vi få mer information om molntjänstleverantöremas och kundernas ställningstagande kring säkerheten inom cloud.
Ifall det känns påträngande eller annat som gör att ni inte vill svara på en fråga så går det bra att hoppa över denna.

* Required

Personlig bakgrund

Företagsnamn *

Vill Ni vara anonyma? *
(Företagetsnamnet och ert namn kommer inte vara tillgängligt för läsarna)

- [ ] Ja
- [ ] Nej

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen? *

Skulle Ni vilja ta del av materialet när det är färdigt ? *

- [ ] Ja
- [ ] Nej

Frågor del 1

Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1. Hur säker är data i:

Publikt moln (Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)

	1	2	3	4	5	6	7	
Inte viktig	○	○	○	○	○	○	○	Mycket viktig

Hur säker är data i:
Privat moln (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

Hur säker är data i :
Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

2. Hur viktigt tror ni det är för kunderna att ingen kan ta del av deras data i datormolnet?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

3. Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är - Tillgängliga

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är - Funktionella

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder är - Säkra
Med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser.

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

4. Hur viktigt är tillgängligheten för er som erbjuder en molntjänst?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

5. Hur viktigt tror ni det är för kunderna att de vet vart deras data/information lagras?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

6. Hur viktigt tror ni det är för kunderna att ni gör regelbunden backup på deras data/information?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

7. Hur viktigt tror ni ansvarighet (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten) är för kunderna?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

8. Hur viktigt är det att kunderna är säkra mot att ingen skall kunna manipulera deras information?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

9. Hur trygga tror ni att era kunder känner sig med den säkerhet som ni erbjuder i era molntjänster?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

10. Hur viktigt är det att kundernas data är krypterad och segregerad från andra kunders data i molntjänster?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

11. Hur viktigt är det att följa säkerhetsstandards, så som ISOs etc, och hur viktigt tror ni det är för kunder att ni följer sådana rekommendationer?

	1	2	3	4	5	6	7	
Inte viktigt	○	○	○	○	○	○	○	Mycket viktigt

Frågor del 2

1. Vilka sorters molntjänster erbjuder ni?

2. Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive kunderna bör skydda sig mot dessa?

3. Vilka säkerhetsåtgärder bör ni respektive kunderna ta för att förhindra dataintrång i era molntjänster?

4. Hur försäkrar ni era kunder att deras privata information skyddas på ett lagligt sätt.
(Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?)

5. Erbjuder ni någon form av kryptering av kundernas sparade data i molnet?
(Om Ja gå till fråga 7)

6. Vad är anledningen/anledningarnar till att ni inte krypterar deras data, har ni någon annan lösning så att andra kunder inte kan ta del av data som inte är deras?

7. Erbjuder ni era kunder någon form av auditlogg där ni och/eller era kunder kan följa upp vad som sker i de systemet/molntjänst ni erbjuder.
(Om Ja gå till fråga 9)

8. Om nej, varför anser ni detta inte nödvändigt i de fall kunderna inte själva valt bort auditlogg.

9. Hur försäkrar ni att kundernas hyrda molntjänster alltid är tillgängliga och funktionella?

10. Vilka åtkomst rättigheter har ni inom de tjänster ni erbjuder att komma över och/ eller ändra kundernas information och till vilket syfte? .

11. Känner era kunder till vart deras data lagras?

12. Följer ni någon/några säkerhetsstandards så som ISOs eller andra rekommendationer, i så fall vilka?

13. Publicerar ni era säkerhetspolicies och procedurer så att kunderna kan ta del av dessa?

14. Gäller er säkerhetspolicy för alla leverantörer av molntjänster, i de fall andra leverantörer är inblandade?

15. Vilka SLAs erbjuder ni era kunder? (Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om)

16. Om det skulle vara så att ert företag går i konkurs eller blir uppköpt, hur försäkrar ni kunderna att deras data ej går förlorad och det fortsätter att vara tillgängligt?

17. Har ni något som ni tror skiljer er från andra molntjänsgivare angående säkerheten, i så fall vad?

18. Har ni någon referens på kunder som ni skulle vilja dela med er till oss, då vi även intervjuar kunder.

2011-05-25 Säkerheten i cloud computing

Vi är mycket tacksammaför att ni har tagit er tid att ställa upp på denna intervju och om ni har några frågor eller synpunkter så är ni välkommna att kontakt oss.

Kontaktperson
Amir Dzindo
Tlf: 0722 11 13 40
Mail: infa07adz@student.lu.se

Med vänliga hälsningar
Amir Dzindo, Rebin Osman, Fisnik Qeriqi

Submit

Powered by Google Docs

Report Abuse - Terms of Service - Additional Terms

spreadsheets.google.com/a/.../viewfor... 8/8

Bilaga 4

B4.1 Enkätsammanställning för kunder

Del 1 av kundundersökningen

Fråga:	*Kund A*	*Kund B*	*Kund C*	*Kund D*	*Kund E*
1 a) Hur säker är data i: Publikt moln?	5	7	7	-	-
1 b) Hur säker är data i: Privat moln?	6	7	6	-	-
1 c) Hur säker är data i: Hybrid moln?	4	7	7	-	-
2. Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?	7	5	7	7	7
3 a) Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är: tillgängliga?	7	7	7	7	7
3 b) Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är: Funkionella?	7	7	7	7	7
3 c) Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är: Säkra?	6	7	7	7	7
4. Hur viktigt är det för er att ni vet vart er data/information lagras?	3	3	7	5	7
5. Hur viktigt är det för er att molntjänstgivaren gör regelbunden backup på er data/information?	7	7	7	7	7
6. Hur viktigt är det med ansvarighet från molntjänstleverantörernas sida?	6	7	7	7	7
7. Hur viktigt är det att ni är säkra mot att ingen skall kunna manipulera er information?	7	7	7	7	7
8. Hur trygg känner ni er med den säkerhet som molntjänstleverantörerna erbjuder i sina molntjänster?	6	7	6	5	7
9. Hur viktigt är det att er data är krypterad och segregerad från andra kunders data i molntjänster?	7	7	7	5	7

10. Hur viktigt är det att molntjänstleverantörerna följer säkerhetsstandards, så som ISOs etc, och andra rekommendationer?	6	7	7	5	7

Del 2 av kundundersökningen

Fråga:	*Kund A*	*Kund B*	*Kund C*	*Kund D*
1. Vilken/ vilka sorters molntjänster hyr ni?	-	*Ännu så länge bara drift av vissa verksamhetssystem där leverantören av systemet även hostar.*	*Informationstjänster och enklare HR-relaterade tjänster*	*E-post Active Directory DNS Övervakning*
2. Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive leverantörerna bör skydda sig mot dessa?	-		*Som slutanvändare måste jag veta var informationen finns och vilket företag som hanterar den. Den största tveksamheten mot att lägga företagsinformation i molnet är att man är osäker över hur molntjänstleverantören kommer att hantera informationen på kort och lång sikt.*	*Data försvinner Data blir tillgängligt för obehöriga Datat är inte tillgängligt när jag önskar*
3. Vilka säkerhetsåtgärder bör ni respektive leverantörerna ta för att förhindra dataintrång i era molntjänster?	-	*Samma skydd som i dagsläget*	*Aktivt gemensamt säkerhetsarbete på alla plan*	*Central hantering av data och lösenord*
4. Hur försäkrar era molntjänstleverantörer att er privata information skyddas på ett lagligt sätt?	-		*Via avtal. Sedan är det en fråga om förtoende.*	
5. Erbjuder er molntjänstleverantör någon form av kryptering av er sparade data i molnet?	-	*Ja, de leverantörer vi accepterar att samarbeta med*	*Ja, de leverantörer vi accepterar att samarbeta med*	
6. Vad är anledningen/anledningarna till att de inte krypterar er data?	-			
7. Erbjuder er molntjänstleverantör någon form av auditlogg där ni och/eller era leverantörer kan följa upp vad som sker i de systemet/molntjänst de erbjuder?	-	*nej*	*Ja, de leverantörer vi accepterar att samarbeta med*	Nej
8. Om nej, har ni själva valt bort någon form auditlogg?	-	*nej*		
9. Hur försäkrar er	-	*Genom SLA*	*Via SLA och andra*	

molntjänstleverantör att era hyrda molntjänster alltid är tillgängliga och funktionella?			*avtal*	
10. Vilka åtkomsträttigheter har er molntjänstleverantör inom de tjänster ni hyr att komma över och/ eller ändra er information och till vilket syfte?	-	*Specifika SLA för resp system*	*Sekretessavtal bör skrivas med de individer hos leverantören som är administratörer eller på annat sätt kan få tillgång till informationen*	
11. Känner ni till vart er data lagras?	-	*Ja*	*Ja, de leverantörer vi accepterar att samarbeta med.*	
12. Har ni på något sätt kunnat ta del av molntjänstleverantörernas säkerhetspolicies och procedurer?	-	*Ja*	*Ja, de leverantörer vi accepterar att samarbeta med*	
13. Vilka SLAs erbjuder er molntjänstleverantör?	-		*Varierar beroende på typ av tjänst*	
14. Ifall det skulle vara så att er molntjänstleverantör skulle gå i konkurs eller bli uppköpt, har ni på något sätt blivit försäkrade att er data ej går förlorad och att det fortsätter att vara tillgängligt?	-	*ja*	*Ja, de leverantörer vi accepterar att samarbeta med*	
15. Finns det något som skiljer er molntjänstlevernatör från andra leverantörer angående säkerheten, i så fall vad?	-	*Vet ej*	*Inget specifikt. Det finns flera leverantörer som skriver i avtal att de tillhandahåller godtagbar säkerhet. Sedan är den kunden som måste våga ta beslutet att köpa tjänsten efter egen bedömning*	
16. Hur har ni kommit fram till vilken säkerhet ni är i behov av, har ni gjort en riskanalys eller dylikt?	*Vi har låtit vårt revisionsbolag göra en riskanalys.*	-	*Vi har gjort en allmän riskanalys utifrån företagets riktlinjer för IT-säkerhet*	-
17. I så fall vilken eller vila metoder har ni använt er av?	*Faktisk ingen aning om vilken metod eller tillvägagångssätt man använt sig av. Vad jag minns hade de någon modell som de arbetade efter.*		*Ingen speciell.* *Vi har inte lagt strategisk information i molnet och riskbedömningen har gjort med utgångspunkt från det.*	

B4.2 Enkätsammanställning för leverantörer

Del 1 molnlevarantör undersökningen

Fråga:	*Leverantör A*	*Leverantör B*
1 a) Hur säker är data i: Publikt moln?	7	7
1 b) Hur säker är data i: Privat moln?	7	7
1 c) Hur säker är data i: Hybrid moln?	7	7
2. Hur viktigt tror ni det är för kunderna att ingen kan ta del av deras data i datormolnet?	7	7
3 a) Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är tillgängliga?	7	5
3 b) Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är funktionella?	7	5
3 c) Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är säkra?	7	7
4. Hur viktigt är tillgängligheten för er som erbjuder en molntjänst?	7	7
5. Hur viktigt tror ni det är för kunderna att de vet vart deras data/information lagras?	4	4
6. Hur viktigt tror ni det är för kunderna att ni gör regelbunden backup på deras data/information?	7	7
7. Hur viktigt tror ni ansvarighet (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten) är för kunderna?	6	5
8. Hur viktigt är det att kunderna är säkra mot att ingen skall kunna manipulera deras information?	7	7
9. Hur trygga tror ni att era kunder känner sig med den säkerhet som ni erbjuder i era molntjänster?		
10. Hur viktigt är det att kundernas data är krypterad och segregerad från andra kunders data i molntjänster?	7	5

11. Hur viktigt är det att följa säkerhetsstandards, så som ISOs etc, och hur viktigt tror ni det är för kunder att ni följer sådana rekommendationer?	5	4

Del 2 av molnleverantörundersökningen

Fråga:	*Leverantör A*	*Leverantör B*
1. Vilka sorters molntjänster erbjuder ni?	*huvudsakligen applikationer distribuerade med hjälp av terminalserver programvaran Citrix*	*BISS - "BI på kran"* *- Business Intelligence inklusive Data Warehouse* *BISS CT* *- Case Tracking (Enklare ärendehantering)* *Detaljhandeln* *BISS LP* *- Bearbetning av Internt svinn* *- Case Tracking (specifikt för säkerhet och deras pågående utredningar)*
2. Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive kunderna bör skydda sig mot dessa?	*Hoten är de vanliga. Dvs molntjänster skiljer sig inte från en traditionell datamiljö. Störst problemet är mänskliga faktorn dvs dåliga processer och rutiner. Därefter allmänt krånglande teknik.*	*Anställda som slutar. Att man slarvar med inloggningsuppgifter*
3. Vilka säkerhetsåtgärder bör ni respektive kunderna ta för att förhindra dataintrång i era molntjänster?	*Går inte att svara på så generellt.*	*Kunder ska ha:* *Krypterade och säkra förbindelser* *Kunderna kan ha:* *HTTPS inloggning* *SMS/kodbox inloggning* *VPN certifikat* *Vi har:* *Dubbla brandväggar* *Krypterade förbindelser* *Starka lösenord och inloggning i form av HTTPS, SMS/Kodbox, VPN* *Kontroll av IP nummer*
4. Hur försäkrar ni era kunder att deras privata information skyddas på ett lagligt sätt.	*Data sparas hos oss i Sverige. Stipuleras i avtal.*	*N/A*
5. Erbjuder ni någon form av kryptering av kundernas sparade data i molnet*? ? (Om ja gå till fråga 7)*	*Informationen är krypterad över internet. Citrix använder SSL*	*Nej, inte idag. Det har ingen kund varit intresserad av.*
6. Vad är anledningen/anledningarnar till att ni inte krypterar deras data, har ni någon annan lösning så att andra	-	*Kunderna har inte varit intresserade av att vi krypterar deras data. Skulle vi ha det så*

kunder inte kan ta del av data som inte är deras?		*tror jag säkert att det tyckte det var bra, men som sagt ingen har varit intresserad eller krävt det. Lösningen vi har är krypterade förbindelser, inloggningar, separata virtuella maskiner*
7. Erbjuder ni era kunder någon form av auditlogg där ni och/eller era kunder kan följa upp vad som sker i de systemet/molntjänst ni erbjuder. *(Om ja gå till fråga 9)*	Ja	*Nej*
8. Om nej, varför anser ni detta inte nödvändigt i de fall kunderna inte själva valt bort auditlogg.		*Det har aldrig kommit på fråga*
9. Hur försäkrar ni att kundernas hyrda molntjänster alltid är tillgängliga och funktionella?	*Tekniken är byggd för att vara stabil.redundant serverplattform reservkraft etc. Funktionen gås igenom kvartalsvis eller månadsvis med kund.*	*Vi har en garanterad upptid mellan 8-17 och sedan är systemet uppe oftast, men vi har rätt att utföra underhåll m m utan att meddela kund om det. Genom att ha en miljö som är speglad och dubbla linor in*
10. Vilka åtkomsträttigheter har ni inom de tjänster ni erbjuder att komma över och/ eller ändra kundernas information och till vilket syfte?	*Vi har rent tekniskt åtkomst till kunddata men vi har ingen rätt eller intresse att ändra kunddata. Sekretessavtal reglerar detta.*	*En superanvändare som har tillgång till all information via ett avancerat gränssnitt och som dessutom kan tilldela andra användare på kundsidan rättigheter.*
11. Känner kunden till vart data lagras?	*Ja*	*På ett ungefär - i ett berggrum i Älvsjö*
12. Följer ni någon/några säkerhetsstandards så som ISOs eller andra rekommendationer, i så fall vilka?	*Vi dokumenterar processerna enligt branschpraxis som kallas ITIL*	*Nej*
13. Publicerar ni era säkerhetspolicys och procedurer så att kunderna kan ta del av dessa?	*Ja det händer att man går igenom vissa processer vid avtalsskrivningar*	*Inte ännu.*
14. Gäller er säkerhetspolicy för alla leverantörer av molntjänster, i de fall andra leverantörer är inblandade?	*Ja*	*Ja*
15. Vilka SLAs erbjuder ni era kunder?	*SLA finns i olika nivåer beroende på vad kunden tecknar för tillgänglighetsnivå*	*Vi har en garanterad upptid mellan 8-17 och sedan är systemet uppe oftast, men vi har rätt att utföra underhåll m m utan att meddela kund om det.*
16. Om det skulle vara så att ert företag går i konkurs eller blir uppköpt, hur försäkrar ni kunderna att deras data ej går förlorad och det fortsätter att vara tillgängligt?	*Kunden äger alltid rätten till sin egen data. Regleras i avtal.*	*Via vårt avtal så går informationen tillbaka till kund om de vill köpa ut lösningen, avbryta kontraktet eller om vi går i konkurs..*
17. Har ni något som ni tror skiljer er från andra molntjänsgivare angående säkerheten, i så fall vad?	*För genrellt för att svara på*	*Nej*

18. Har ni någon referens på kunder som ni skulle vilja dela med er till oss, då vi även intervjuar kunder.	*Finns en del referenser på vår webbsida. Se under Total outsourcing.*	

B4.3 Fullständig transkribering för kunder (intervjuprotokoll)

Kund A

Hej, vi är tre studenter som studerar det systemvetenskapliga programmet i lunds universitet och skriver ett examensarbete. Detta arbete handlar om säkerhet i datormolnet (Cloud Computing) för att vara mer specifika så vill vi få mer information om molntjänstleverantörernas och kundernas ställningstagande kring säkerheten inom cloud.
Ifall det känns påträngande eller annat som gör att ni inte vill svara på en fråga så går det bra att hoppa över denna.

Personlig bakrund/etik
Vill Ni vara anonyma ?*(Företagets namnet och ert namn kommer inte vara tillgängligt för läsarna)*
Svar: Ja

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen?
Svar: Jag arbetar som ekonomichef. I min roll ingår bland annat att arbeta med it-frågor.

Skulle Ni vilja ta del av materialet när det är färdigt?
Svar: Ja
Frågor
Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1.Hur säker är data i:

a) Publikt moln?(Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)

Svar:5

b) Privat moln? (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)

Svar:6

c) Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)

Svar:4

2. Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?
Svar:7

3. Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är:

a) tillgängliga

Svar:7

b) funktionella

Svar:7

c) säkra (*med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser*.)

Svar:6

4. Hur viktigt är det för er att ni vet vart er data/information lagras?
Svar:3

5. Hur viktigt är det för er att molntjänstgivaren gör regelbunden backup på er data/information?
Svar:7

6. Hur viktigt är det med ansvarighet från molntjänstleverantörernas sida (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten)?
Svar:6

7. Hur viktigt är det att ni är säkra mot att ingen skall kunna manipulera er information?
Svar:7

8. Hur trygg känner ni er med den säkerhet som molntjänstleverantörerna erbjuder i sina molntjänster?
Svar:6

9. Hur viktigt är det att er data är krypterad och segregerad från andra kunders data i molntjänster?
Svar:7

10. Hur viktigt är det att molntjänstleverantörerna följer säkerhetsstandards, så som ISOs etc, och andra rekommendationer?
Svar:6

Intervjufrågor: Frågorna i denna del besvaras med text.

Vilken/ vilka sorters molntjänster hyr ni?
Svar: Hyr inga för tillfället.
Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive leverantörerna bör skydda sig mot dessa?

Vilka säkerhetsåtgärder bör ni respektive leverantörerna ta för att förhindra dataintrång i era molntjänster?

Hur försäkrar era molntjänstleverantörer att er privata information skyddas på ett lagligt sätt. *(Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?)*

Erbjuder er molntjänstleverantör någon form av kryptering av er sparade data i molnet*? (Om ja gå till fråga 7)*

Vad är anledningen/anledningarna till att de inte krypterar er data?
Erbjuder er molntjänstleverantör någon form av auditlogg där ni och/eller era leverantörer kan följa upp vad som sker i de systemet/molntjänst de erbjuder. *(Om ja gå till fråga 9)*

Om nej, har ni själva valt bort någon form auditlogg.

Hur försäkrar er molntjänstleverantör att era hyrda molntjänster alltid är tillgängliga och funktionella?

Vilka åtkomsträttigheter har er molntjänstleverantör inom de tjänster ni hyr att komma över och/ eller ändra er information och till vilket syfte?

Känner ni till vart er data lagras?

Har ni på något sätt kunnat ta del av molntjänstleverantörernas säkerhetspolicys och procedurer?

Vilka SLAs erbjuder er molntjänstleverantör? (*Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om*)

Ifall det skulle vara så att er molntjänstleverantör skulle gå i konkurs eller bli uppköpt, har ni på något sätt blivit försäkrade att er data ej går förlorad och att det fortsätter att vara tillgängligt?

Finns det något som skiljer er molntjänstlevernatör från andra leverantörer angående säkerheten, i så fall vad?

Vi är mycket tacksamma för att ni har tagit er tid att ställa upp på denna intervju och om ni har några frågor eller synpunkter så är ni välkomna att kontakt oss.

Hur har ni kommit fram till vilken säkerhet ni är i behov av, har ni gjort en riskanalys eller dylikt ?
Svar: Vi har låtit vårt revisionsbolag göra en riskanalys.
I så fall vilken eller vila metoder har ni använt er av ?
Svar :Faktisk ingen aning om vilken metod eller tillvägagångssätt man använt sig av. Vad jag minns hade de någon modell som de arbetade efter.

Kontaktperson
Amir Dzindo
Tlf: 0722 11 13 40
Mail: infa07adz@student.lu.se
mvh Amir Dzindo, Rebin Osman, Fisnik Qeriqi

Kund B

Hej, vi är tre studenter som studerar det systemvetenskapliga programmet i lunds universitet och skriver ett examensarbete. Detta arbete handlar om säkerhet i datormolnet (Cloud Computing) för att vara mer specifika så vill vi få mer information om molntjänstleverantörernas och kundernas ställningstagande kring säkerheten inom cloud.
Ifall det känns påträngande eller annat som gör att ni inte vill svara på en fråga så går det bra att hoppa över denna.

Personlig bakrund/etik
Vill Ni vara anonyma?*(företagsnamnet och ert namn kommer inte vara tillgängligt för läsarna)*

Svar: Ja

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen?
Svar: IT chef

Skulle Ni vilja ta del av materialet när det är färdigt?
Svar: Nej
Frågor
Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1. Hur säker är data i:

a) Publikt moln?(Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)

Svar: 7

b) Privat moln? (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)

Svar: 7

c) Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)

Svar: 7

2. Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?
Svar: 5

3. Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är:

a) tillgängliga

Svar: 7

b) funktionella

Svar: 7

c) säkra (*med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser*.)

Svar: 7

4. Hur viktigt är det för er att ni vet vart er data/information lagras?
Svar: 3

5. Hur viktigt är det för er att molntjänstgivaren gör regelbunden backup på er data/information?
Svar: 7

6. Hur viktigt är det med ansvarighet från molntjänstleverantörernas sida (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten)?
Svar: 7

7. Hur viktigt är det att ni är säkra mot att ingen skall kunna manipulera er information?
Svar: 7

8. Hur trygg känner ni er med den säkerhet som molntjänstleverantörerna erbjuder i sina molntjänster?
Svar: 7

9. Hur viktigt är det att er data är krypterad och segregerad från andra kunders data i molntjänster?
Svar: 7

10. Hur viktigt är det att molntjänstleverantörerna följer säkerhetsstandards, så som ISOs etc, och andra rekommendationer?
Svar: 7

Intervjufrågor: Frågorna i denna del besvaras med text.

Vilken/ vilka sorters molntjänster hyr ni?
Svar: Ännu så länge bara drift av vissa verksamhetssystem där leverantören av systemet även hostar.
Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive leverantörerna bör skydda sig mot dessa?
Svar: ------
Vilka säkerhetsåtgärder bör ni respektive leverantörerna ta för att förhindra dataintrång i era molntjänster?
Svar: Samma skydd som i dagsläget.

Hur försäkrar era molntjänstleverantörer att er privata information skyddas på ett lagligt sätt. *(Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?)*
Svar: -----

Erbjuder er molntjänstleverantör någon form av kryptering av er sparade data i molnet*? (Om ja gå till fråga 7)*
Svar: Ja, de leverantörer vi accepterar att samarbeta med.

Vad är anledningen/anledningarnar till att de inte krypterar er data?
Svar: -------

Erbjuder er molntjänstleverantör någon form av auditlogg där ni och/eller era leverantörer kan följa upp vad som sker i de systemet/molntjänst de erbjuder. *(Om ja gå till fråga 9)*

Svar: Nej

Om nej, har ni själva valt bort någon form auditlogg.
Svar: Nej

Hur försäkrar er molntjänstleverantör att era hyrda molntjänster alltid är tillgängliga och funktionella?

Svar: Genom SLA

Vilka åtkomsträttigheter har er molntjänstleverantör inom de tjänster ni hyr att komma över och/ eller ändra er information och till vilket syfte?

Svar: Specifika SLA för resp system

Känner ni till vart er data lagras?
Svar: Ja

Har ni på något sätt kunnat ta del av molntjänstleverantörernas säkerhetspolicys och procedurer?
Svar: Ja

Vilka SLAs erbjuder er molntjänstleverantör? (*Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om*)

Svar: ------

Ifall det skulle vara så att er molntjänstleverantör skulle gå i konkurs eller bli uppköpt, har ni på något sätt blivit försäkrade att er data ej går förlorad och att det fortsätter att vara tillgängligt?

Svar: Ja

Finns det något som skiljer er molntjänstlevernatör från andra leverantörer angående säkerheten, i så fall vad?

Svar: Vet ej

Kund C

Hej, vi är tre studenter som studerar det systemvetenskapliga programmet i lunds universitet och skriver ett examensarbete. Detta arbete handlar om säkerhet i datormolnet (Cloud Computing) för att vara mer specifika så vill vi få mer information om molntjänstleverantörernas och kundernas ställningstagande kring säkerheten inom cloud.
Ifall det känns påträngande eller annat som gör att ni inte vill svara på en fråga så går det bra att hoppa över denna.

Personlig bakrund/etik
Vill Ni vara anonyma?*(företagsnamnet och ert namn kommer inte vara tillgängligt för läsarna)*

Svar: Ja

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen ?

Svar: VD för Swecos interna IT-bolag Sweco Connect

Skulle Ni vilja ta del av materialet när det är färdigt?
Svar: Ja

Frågor
Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1. Hur säker är data i:

a) Publikt moln?(Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)

Svar: 7

b) Privat moln? (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)

Svar: 6

c) Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)

Svar: 7
2. Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?
Svar:7

3. Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är:

a) tillgängliga

Svar: 7

b) funktionella

Svar: 7

c) säkra (*med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser*.)

Svar:7

4. Hur viktigt är det för er att ni vet vart er data/information lagras?
Svar:7

5. Hur viktigt är det för er att molntjänstgivaren gör regelbunden backup på er data/information?
Svar:7

6. Hur viktigt är det med ansvarighet från molntjänstleverantörernas sida (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten)?
Svar:7
7. Hur viktigt är det att ni är säkra mot att ingen skall kunna manipulera er information?
Svar: 7

8. Hur trygg känner ni er med den säkerhet som molntjänstleverantörerna erbjuder i sina molntjänster?
Svar: 5

9. Hur viktigt är det att er data är krypterad och segregerad från andra kunders data i molntjänster?
Svar: 7

10. Hur viktigt är det att molntjänstleverantörerna följer säkerhetsstandards, så som ISOs etc, och andra rekommendationer?
Svar:7
Intervjufrågor: Frågorna i denna del besvaras med text.

Vilken/ vilka sorters molntjänster hyr ni?

Svar: Informationstjänster och enklare HR-relaterade tjänster

Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive leverantörerna bör skydda sig mot dessa?

Svar: Som slutanvändare måste jag veta var informationen finns och vilket företag som hanterar den. Den största tveksamheten mot att lägga företagsinformation i molnet är att man är osäker över hur molntjänstleverantören kommer att hantera informationen på kort och lång sikt. Vad händer om t ex molntjänstleverantören säljs eller går i konkurs?

Vilka säkerhetsåtgärder bör ni respektive leverantörerna ta för att förhindra dataintrång i era molntjänster?

Svar: Aktivt gemensamt säkerhetsarbete på alla plan

Hur försäkrar era molntjänstleverantörer att er privata information skyddas på ett lagligt sätt. *(Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?)*

Svar: Via avtal. Sedan är det en fråga om förtoende. Se mitt svar 2 ovan.

Erbjuder er molntjänstleverantör någon form av kryptering av er sparade data i molnet*? (Om ja gå till fråga 7)*
Svar: Ja, de leverantörer vi accepterar att samarbeta med.

Vad är anledningen/anledningarnar till att de inte krypterar er data?
Svar:

Erbjuder er molntjänstleverantör någon form av auditlogg där ni och/eller era leverantörer kan följa upp vad som sker i de systemet/molntjänst de erbjuder. *(Om ja gå till fråga 9)*
Svar: Ja, de leverantörer vi accepterar att samarbeta med.

Om nej, har ni själva valt bort någon form auditlogg.
Svar:

Hur försäkrar er molntjänstleverantör att era hyrda molntjänster alltid är tillgängliga och funktionella?

Svar: Via SLA och andra avtal

Vilka åtkomsträttigheter har er molntjänstleverantör inom de tjänster ni hyr att komma över och/ eller ändra er information och till vilket syfte?

Svar: Sekretessavtal bör skrivas med de individer hos leverantören som är administratörer eller på annat sätt kan få tillgång till informationen

Känner ni till vart er data lagras?
Svar: Ja, de leverantörer vi accepterar att samarbeta med.

Har ni på något sätt kunnat ta del av molntjänstleverantörernas säkerhetspolicys och procedurer?
Svar: Ja, de leverantörer vi accepterar att samarbeta med.

Vilka SLAs erbjuder er molntjänstleverantör? (*Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om*)
Svar: Varierar beroende på typ av tjänst

Ifall det skulle vara så att er molntjänstleverantör skulle gå i konkurs eller bli uppköpt, har ni på något sätt blivit försäkrade att er data ej går förlorad och att det fortsätter att vara tillgängligt?
Svar: Ja, de leverantörer vi accepterar att samarbeta med.

Finns det något som skiljer er molntjänstlevernatör från andra leverantörer angående säkerheten, i så fall vad?
Svar: Inget specifikt. Det finns flera leverantörer som skriver i avtal att de tillhandahåller godtagbar säkerhet. Sedan är den kunden som måste våga ta beslutet att köpa tjänsten efter egen bedömning.
Hur har ni kommit fram till vilken säkerhet ni är i behov av, har ni gjort en riskanalys eller dylikt ?
Svar: Vi har gjort en allmän riskanalys utifrån företagets riktlinjer för IT-säkerhet

I så fall vilken eller vila metoder har ni använt er av?
Svar : Ingen särskild metod
Kommentar: Vi har inte lagt strategisk information i molnet och riskbedömningen har gjort med utgångspunkt från det.

Kund D

Hej, vi är tre studenter som studerar det systemvetenskapliga programmet i lunds universitet och skriver ett examensarbete. Detta arbete handlar om säkerhet i datormolnet (Cloud Computing) för att vara mer specifika så vill vi få mer information om molntjänstleverantörernas och kundernas ställningstagande kring säkerheten inom cloud.
Ifall det känns påträngande eller annat som gör att ni inte vill svara på en fråga så går det bra att hoppa över denna.

Personlig bakrund/etik
Vill Ni vara anonyma?*(företagsnamnet och ert namn kommer inte vara tillgängligt för läsarna)*
Svar: Ja

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen?
Svar: IT chef och Kundprojektledare

Skulle Ni vilja ta del av materialet när det är färdigt?
Svar: Ja

Frågor
Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1.Hur säker är data i:

a) Publikt moln?(Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)

Svar: -

b) Privat moln? (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)

Svar: -

c) Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)

Svar: -

2. Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?
Svar: 7

3. Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är:

a) tillgängliga

Svar: 7

b) funktionella

Svar: 7

c) säkra (*med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser*.)

Svar: 7

4. Hur viktigt är det för er att ni vet vart er data/information lagras?
Svar: 5

5. Hur viktigt är det för er att molntjänstgivaren gör regelbunden backup på er data/information?
Svar: 7

6. Hur viktigt är det med ansvarighet från molntjänstleverantörernas sida (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten)?
Svar: 7

7. Hur viktigt är det att ni är säkra mot att ingen skall kunna manipulera er information?
Svar: 7

8. Hur trygg känner ni er med den säkerhet som molntjänstleverantörerna erbjuder i sina molntjänster?
Svar: 5

9. Hur viktigt är det att er data är krypterad och segregerad från andra kunders data i molntjänster?
Svar: 5

10. Hur viktigt är det att molntjänstleverantörerna följer säkerhetsstandards, så som ISOs etc, och andra rekommendationer?
Svar: 5

Intervjufrågor: Frågorna i denna del besvaras med text.

Vilken/ vilka sorters molntjänster hyr ni?

Svar: E-post
Active Directory
DNS
Övervakning

Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive leverantörerna bör skydda sig mot dessa?

Svar: Data försvinner
Data blir tillgängligt för obehöriga
Datat är inte tillgängligt när jag önskar

Vilka säkerhetsåtgärder bör ni respektive leverantörerna ta för att förhindra dataintrång i era molntjänster?
Svar: Central hantering av data och lösenord

Hur försäkrar era molntjänstleverantörer att er privata information skyddas på ett lagligt sätt. *(Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?)*

Svar: -

Erbjuder er molntjänstleverantör någon form av kryptering av er sparade data i molnet*? (Om ja gå till fråga 7)*

Svar: -

Vad är anledningen/anledningarna till att de inte krypterar er data?

Svar: -

Erbjuder er molntjänstleverantör någon form av auditlogg där ni och/eller era leverantörer kan följa upp vad som sker i de systemet/molntjänst de erbjuder. *(Om ja gå till fråga 9)*

Svar: Nej

Om nej, har ni själva valt bort någon form auditlogg.

Svar: Nej

Hur försäkrar er molntjänstleverantör att era hyrda molntjänster alltid är tillgängliga och funktionella?

Svar: Via avtal

Vilka åtkomsträttigheter har er molntjänstleverantör inom de tjänster ni hyr att komma över och/ eller ändra er information och till vilket syfte?

Svar: Inga

Känner ni till vart er data lagras?

Svar: Nej

Har ni på något sätt kunnat ta del av molntjänstleverantörernas säkerhetspolicies och procedurer?

Svar: Ja

Vilka SLAs erbjuder er molntjänstleverantör? (*Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om*)

Svar: Tillgänglighet 99,9%
Svarstid 100 mS
Åtgärd beroende på prioritet, påbörjad inom 60 min - 3 dagar

Ifall det skulle vara så att er molntjänstleverantör skulle gå i konkurs eller bli uppköpt, har ni på något sätt blivit försäkrade att er data ej går förlorad och att det fortsätter att vara tillgängligt?

Svar: Ja

Finns det något som skiljer er molntjänstlevernatör från andra leverantörer angående säkerheten, i så fall vad?

Svar: Nej

--- Affärs sund har ej molnet men har funderingar kring att gå upp i de

Personlig bakgrund/etik
Vill Ni vara anonyma?*(företagsnamnet och ert namn kommer inte vara tillgängligt för läsarna)*
Svar: Nej

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen?
Svar: VD

Skulle Ni vilja ta del av materialet när det är färdigt?
Svar: Ja
Frågor
Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1. Hur säker är data i:

a) Publikt moln?(Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)

Svar: ---

b) Privat moln? (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)

Svar:----

c) Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)

Svar:-----

2. Hur viktigt är det för er att ingen kan ta del av er data i datormolnet?

Svar:7

3. Hur viktigt är det för er att de tjänster molntjänstleverantörerna erbjuder alltid är:

a) tillgängliga

Svar:7

b) funktionella

Svar:7

c) säkra (*med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser*.)

Svar:7

4. Hur viktigt är det för er att ni vet vart er data/information lagras?
Svar:7

5. Hur viktigt är det för er att molntjänstgivaren gör regelbunden backup på er data/information?
Svar:7

6. Hur viktigt är det med ansvarighet från molntjänstleverantörernas sida (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten)?
Svar:7

7. Hur viktigt är det att ni är säkra mot att ingen skall kunna manipulera er information?
Svar:7

8. Hur trygg känner ni er med den säkerhet som molntjänstleverantörerna erbjuder i sina molntjänster?
Svar:7

9. Hur viktigt är det att er data är krypterad och segregerad från andra kunders data i molntjänster?
Svar:7

10. Hur viktigt är det att molntjänstleverantörerna följer säkerhetsstandards, så som ISOs etc, och andra rekommendationer?
Svar:7

Intervjufrågor: Frågorna i denna del besvaras med text.

1.Vilken/ vilka sorters molntjänster hyr ni?
Svar: inget än

B4.4 Fullständig transkribering för leverantörer (intervjuprotokoll)

Leverantör A
It mästaren

Personlig bakrund/etik
Vill Ni vara anonyma?*(företagsnamnet och ert namn kommer inte vara tillgängligt för läsarna)*
Svar: Nej

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen?
Svar: VD

Skulle Ni vilja ta del av materialet när det är färdigt?
Svar: Ja
Frågor
Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1.Hur säker är data i:

a) Publikt moln?(Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)
Svar:7

b) Privat moln? (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)
Svar:7

c) Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)
Svar:7

2. Hur viktigt tror ni det är för kunderna att ingen kan ta del av deras data i datormolnet?
Svar:7

3. Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är:

a) tillgängliga

Svar:7

b) funktionella

Svar:7

c) säkra (*med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser*.)
Svar:7

4. Hur viktigt är tillgängligheten för er som erbjuder en molntjänst?
Svar:7

5. Hur viktigt tror ni det är för kunderna att de vet vart deras data/information lagras?
Svar:4

6. Hur viktigt tror ni det är för kunderna att ni gör regelbunden backup på deras data/information?
Svar:7

7. Hur viktigt tror ni ansvarighet (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten) är för kunderna?
Svar:6

8. Hur viktigt är det att kunderna är säkra mot att ingen skall kunna manipulera deras information?
Svar:7

9. Hur trygga tror ni att era kunder känner sig med den säkerhet som ni erbjuder i era molntjänster?
Svar:-

10. Hur viktigt är det att kundernas data är krypterad och segregerad från andra kunders data i molntjänster?
Svar:7

11. Hur viktigt är det att följa säkerhetsstandards, så som ISOs etc, och hur viktigt tror ni det är för kunder att ni följer sådana rekommendationer?
Svar:5

Intervjufrågor: Frågorna i denna del besvaras med text.

Vilka sorters molntjänster erbjuder ni?
Svar: huvudsakligen applikationer distribuerade med hjälp av terminalserver programvaran Citrix

Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive kunderna bör skydda sig mot dessa?
Svar: Hoten är de vanliga. Dvs molntjänster skiljer sig inte från en traditionell datamiljö. Störst problemet är mänskliga faktorn dvs dåliga processer och rutiner. Därefter allmänt krånglande teknik.
Vilka säkerhetsåtgärder bör ni respektive kunderna ta för att förhindra dataintrång i era molntjänster?
Svar: Går inte att svara på så generellt.

Hur försäkrar ni era kunder att deras privata information skyddas på ett lagligt sätt. *(Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?)*
Svar: Data sparas hos oss i Sverige. Stipuleras i avtal.

Erbjuder ni någon form av kryptering av kundernas sparade data i molnet*? (Om ja gå till fråga 7)*
Svar: Informationen är krypterad över internet. Citrix använder SSL.

Vad är anledningen/anledningarna till att ni inte krypterar deras data, har ni någon annan lösning så att andra kunder inte kan ta del av data som inte är deras?
Svar: -----

Erbjuder ni era kunder någon form av auditlogg där ni och/eller era kunder kan följa upp vad som sker i de systemet/molntjänst ni erbjuder. *(Om ja gå till fråga 9)*
Svar: Ja

Om nej, varför anser ni detta inte nödvändigt i de fall kunderna inte själva valt bort auditlogg.
Svar: ---

Hur försäkrar ni att kundernas hyrda molntjänster alltid är tillgängliga och funktionella?
Svar: Tekniken är byggd för att vara stabil.redundant serverplattform reservkraft etc.
Funktionen gås igenom kvartalsvis eller månadsvis med kund.

Vilka åtkomst rättigheter har ni inom de tjänster ni erbjuder att komma över och/ eller ändra kundernas information och till vilket syfte?

Svar: Vi *har rent tekniskt åtkomst till kunddata men vi har ingen rätt eller intresse att ändra kunddata. Sekretessavtal reglerar detta.*

Känner era kunder till vart deras data lagras?

Svar: Ja

Följer ni någon/några säkerhetsstandards så som ISOs eller andra rekommendationer, i så fall vilka?

Svar: Vi dokumenterar processerna enligt branschpraxis som kallas ITIL

Publicerar ni era säkerhetspolicys och procedurer så att kunderna kan ta del av dessa?

Svar: Ja det händer att man går igenom vissa processer vid avtalsskrivningar.

Gäller er säkerhetspolicy för alla leverantörer av molntjänster, i de fall andra leverantörer är inblandade?

Svar: Ja

Vilka SLAs erbjuder ni era kunder? (*Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om*)

Svar: SLA finns i olika nivåer beroende på vad kunden tecknar för tillgänglighetsnivå.

Om det skulle vara så att ert företag går i konkurs eller blir uppköpt, hur försäkrar ni kunderna att deras data ej går förlorad och det fortsätter att vara tillgängligt?

Svar: Kunden äger alltid rätten till sin egen data. Regleras i avtal.

Har ni något som ni tror skiljer er från andra molntjänstgivare angående säkerheten, i så fall vad?

Svar: För genrellt för att svara på

Har ni någon referens på kunder som ni skulle vilja dela med er till oss, då vi även intervjuar kunder.
Svar: Finns en del referenser på vår webbsida. Se under Total outsourcing.

---------- Leverantör B

Personlig bakgrund/etik
Vill Ni vara anonyma?*(företagsnamnet och ert namn kommer inte vara tillgängligt för läsarna)*
Svar: Nej

Vad är din arbetsroll samt dina arbetsuppgifter i organisationen?
Svar: VD. Försäljning och marknad samt affärsansvarig för BISS - vår hyrtjänst

Skulle Ni vilja ta del av materialet när det är färdigt?
Svar: Ja
Frågor
Dessa frågor besvaras med en skala 1 – 7 där 1 motsvarar inte viktigt och 7 motsvarar mycket viktigt.

1. Hur säker är data i:

a) Publikt moln?(Med publikt moln menar vi att man delar datorresurser med andra företag i ett gemensamt datacenter utanför organisationen)
Svar:7

b) Privat moln? (Med privatmoln menar vi interna datacenter, av en verksamhet eller organisation som inte görs tillgängliga för obehöriga)
Svar:7

c) Hybrid moln (Med hybrid moln menar vi en kombination av både publikt och privat moln)
Svar:7

2. Hur viktigt tror ni det är för kunderna att ingen kan ta del av deras data i datormolnet?
Svar:7

3. Hur viktigt tror ni det är för kunderna att de tjänster ni erbjuder alltid är:

a) tillgängliga

Svar:5

b) funktionella

Svar:5

c) säkra (*med säkra menar vi assurance, att det finns en grad av förtroende för att säkerhetsåtgärder utförs både tekniska och operationella för att skydda känslig data och viktiga resurser*.)
Svar:7

4. Hur viktigt är tillgängligheten för er som erbjuder en molntjänst?
Svar:7

5. Hur viktigt tror ni det är för kunderna att de vet vart deras data/information lagras?
Svar:4

6. Hur viktigt tror ni det är för kunderna att ni gör regelbunden backup på deras data/information?
Svar:7

7. Hur viktigt tror ni ansvarighet (med ansvarighet och accountability menar vi de som kommer bli ansvariga vid brist i säkerheten) är för kunderna?
Svar:5

8. Hur viktigt är det att kunderna är säkra mot att ingen skall kunna manipulera deras information?
Svar:7

9. Hur trygga tror ni att era kunder känner sig med den säkerhet som ni erbjuder i era molntjänster?
Svar:-

10. Hur viktigt är det att kundernas data är krypterad och segregerad från andra kunders data i molntjänster?
Svar:5

11. Hur viktigt är det att följa säkerhetsstandards, så som ISOs etc, och hur viktigt tror ni det är för kunder att ni följer sådana rekommendationer?
Svar:4

Intervjufrågor: Frågorna i denna del besvaras med text.

1. Vilka sorters molntjänster erbjuder ni?

Svar: Generellt (branschoberoende)
BISS - "BI på kran"
- Business Intelligence inklusive Data Warehouse
BISS CT
- Case Tracking (Enklare ärendehantering)

Detaljhandeln
BISS LP

- Bearbetning av Internt svinn
- Case Tracking (specifikt för säkerhet och deras pågående utredningar)

2. Vilka tre viktigaste hot är kända mot molntjänster och hur tycker ni att ni respektive kunderna bör skydda sig mot dessa?

Svar: Anställda som slutar. Att man slarvar med inloggningsuppgifter

3. Vilka säkerhetsåtgärder bör ni respektive kunderna ta för att förhindra dataintrång i era molntjänster?

Svar: Kunder ska ha:
Krypterade och säkra förbindelser

Kunderna kan ha:
HTTPS inloggning
SMS/kodbox inloggning
VPN certifikat

Vi har:
Dubbla brandväggar
Krypterade förbindelser
Starka lösenord och inloggning i form av HTTPS, SMS/Kodbox, VPN
Kontroll av IP nummer

4. Hur försäkrar ni era kunder att deras privata information skyddas på ett lagligt sätt. *(Med lagligt sätt menar vi vilka lagar som gäller i de fall där kundernas data är sparad i andra länder där andra lagar gäller?)*

Svar: N/A

5. Erbjuder ni någon form av kryptering av kundernas sparade data i molnet*? (Om ja gå till fråga 7)*

Svar: Nej, inte idag. Det har ingen kund varit intresserad av.

6. Vad är anledningen/anledningarna till att ni inte krypterar deras data, har ni någon annan lösning så att andra kunder inte kan ta del av data som inte är deras?

Svar: Kunderna har inte varit intresserade av att vi krypterar deras data. Skulle vi ha det så tror jag säkert att det tyckte det var bra, men som sagt ingen har varit intresserad eller krävt det.
Lösningen vi har är krypterade förbindelser, inloggningar, separata virtuella maskiner

7. Erbjuder ni era kunder någon form av auditlogg där ni och/eller era kunder kan följa upp vad som sker i de systemet/molntjänst ni erbjuder. *(Om ja gå till fråga 9)*

Svar: Nej!

8. Om nej, varför anser ni detta inte nödvändigt i de fall kunderna inte själva valt bort auditlogg.

Svar: Det har aldrig kommit på fråga

9. Hur försäkrar ni att kundernas hyrda molntjänster alltid är tillgängliga och funktionella?

Svar: Vi har en garanterad upptid mellan 8-17 och sedan är systemet uppe oftast, men vi har rätt att utföra underhåll m m utan att meddela kund om det.
Genom att ha en miljö som är speglad och dubbla linor in.

10. Vilka åtkomst rättigheter har ni inom de tjänster ni erbjuder att komma över och/ eller ändra kundernas information och till vilket syfte?

Svar: En *superanvändare som har tillgång till all information via ett avancerat gränssnitt och som dessutom kan tilldela andra användare på kundsidan rättigheter.*

11. Känner era kunder till vart deras data lagras?

Svar: På ett ungefär - i ett berggrum i Älvsjö :-)

12. Följer ni någon/några säkerhetsstandards så som ISOs eller andra rekommendationer, i så fall vilka?

Svar: Nej!!

13. Publicerar ni era säkerhetspolicys och procedurer så att kunderna kan ta del av dessa?

Svar: Inte ännu.

14. Gäller er säkerhetspolicy för alla leverantörer av molntjänster, i de fall andra leverantörer är inblandade?

Svar: Ja

15. Vilka SLAs erbjuder ni era kunder? (*Med SLA menar vi de tjänstekontrakt mellan er och kunder om vilken servicenivå man kommer överens om*)

Svar: Vi har en garanterad upptid mellan 8-17 och sedan är systemet uppe oftast, men vi har rätt att utföra underhåll m m utan att meddela kund om det.

16. Om det skulle vara så att ert företag går i konkurs eller blir uppköpt, hur försäkrar ni kunderna att deras data ej går förlorad och det fortsätter att vara tillgängligt?

Svar: Via vårt avtal så går informationen tillbaka till kund om de vill köpa ut lösningen, avbryta kontraktet eller om vi går i konkurs..

17. Har ni något som ni tror skiljer er från andra molntjänsgivare angående säkerheten, i så fall vad?

Svar: Nej

18. Har ni någon referens på kunder som ni skulle vilja dela med er till oss, då vi även intervjuar kunder.

Svar: Ni får inte kontakta kund utan att vi får hantera det först, men vi har Rusta, Jula, Twilfit, Teknikmagasinet, ÖstgötaTrafiken som några av kunderna.

B4.5 Fullständig transkribering av säkerhetsaspekts prioriteringen

Kund 1

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Förtroende mellan kund och leverantör
2. Kryptering
3. Datasegregation (att data segregeras från andra kunders data i samma moln)
4. Integritet
5. Tillgänglighet
6. Dataintrång
7. Hot mot molntjänst
8. Konfidentialitet
9. Datalokalisering
10. Ansvar (accountability)
11. Juridiska frågor
12. Backup
13. Åtkomstkontroll
14. Auditlogg

Kund 2

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Förtroende mellan kund och leverantör
2. Kryptering
3. Integritet
4. Dataintrång
5. Ansvar(accountability)
6. Juridiska frågor
7. Hot mot molntjänst
8. Skydd av konfidentialitet
9. Datasegregation (att data segregeras från andra kunders data i samma moln)
10. Åtkomstkontroll
11. Backup
12. Auditlogg
13. Datalokalisering
14. Tillgänglighet

Kund 3

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Integritet
2. Dataintrång
3. Datasegregation (att data segregeras från andra kunders data i samma moln)
4. Datalokalisering
5. Backup
6. Åtkomstkontroll
7. Tillgänglighet
8. Konfidentialitet
9. Juridiska frågor
10. Kryptering
11. Auditlogg
12. Ansvar (accountability)
13. Förtroende mellan kund och leverantör
14. Hot mot molntjänst

Kund 4

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Juridiska frågor
2. Integritet
3. Tillgänglighet
4. Förtroende mellan kund och leverantör
5. Konfidentialitet
6. Dataintrång
7. Datasegregation (att datan segregeras från andra kunders data i samma moln)
8. Backup

9. Åtkomstkontroll
10. Kryptering
11. Ansvar (accountability)
12. Hot mot molntjänst
13. Datalokalisering
14. Auditlogg

Kund 5

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Förtroende mellan kund och leverantör
2. Integritet
3. Datalokalisering
4. Konfidentialitet
5. Tillgänglighet
6. Datasegregation (att datan segregeras från andra kunders data i samma moln)
7. Dataintrång
8. Ansvar (accountability)
9. Hot mot molntjänst
10. Åtkomstkontroll
11. Juridiska frågor
12. Kryptering
13. Backup
14. Auditlogg

Leverantör 1

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Tillgänglighet
2. Åtkomstkontroll
3. Dataintrång
4. Ansvar (accountability)
5. Backup
6. Förtroende mellan kund och leverantör
7. Konfidentialitet
8. Kryptering
9. Auditlogg
10. Datasegregation
11. Hot mot molntjänst
12. Integritet
13. Datalokalisering
14. Juridiska frågor

Leverantör 2

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Förtroende mellan kund och leverantör
2. Ansvar (accountability)
3. Backup
4. Konfidentialitet
5. Integritet
6. Dataintrång
7. Hot mot molntjänst
8. Tillgänglighet
9. Juridiska frågor
10. Åtkomstkontroll
11. Kryptering
12. Auditlogg
13. Datasegregation (att datan segregeras från andra kunders data i samma moln)
14. Datalokalisering

Leverantör 3

Kan ni rangordna dessa säkerhetsaspekter efter vilka ni anser vara de viktigaste för säkerheten i datormolnet? *Sätt en siffra mellan 1 (viktigaste säkerhetsaspekten) till 14 (minst viktiga säkerhetsaspekten) vänster om säkerhetsaspekterna.*

1. Juridiska frågor
2. Förtroende mellan kund och leverantör
3.Ansvar (accountability)
4. Hot mot molntjänst
5. Tillgänglighet
6. Konfidentialitet
7. Integritet
8. Kryptering
9. Backup
10. Datasegregation
11. Dataintrång
12. Åtkomstkontroll
13. Auditlogg
14. Datalokalisering

Referenslista

Armbrust M, Fox A och Griffith R, Joseph A D, Katz R H et al, (2009): Above the Clouds: A Berkeley View of CloudComputing. *Communications of the ACM.* Vol. 53, No 4, s. 50-58

Bisong A och Rahman S (2011): An overview of security concerns in enterprise Cloud Computing. *International Journal of Network Security & Its Application.* Vol. 3, No. 1, s. 30 - 45

Brunette G och Mogull R (2009): Security Guidance for critical areas of focus in Cloud Computing V2. 1. *Cloud Security Alliance*

Broadkin J (2008): Gartner: Seven cloud computing security risks. *Network world, 2 Juli.*

Chen Y, Paxson V och Katz R (2010): *Whats new about cloud computing security.* UCB/EECS-2010-5. Electrical Engineering and Computer Science department, University of California, Berkeley

Dhillon G (2007): *Principles of information systems security.* John Wiley & sons

DiCicco-Bloom B och Crabtree B F (2006): The qualitative research interview. *Medical education.* Vol 40, No 4, s. 314-321.

Engberg och Forsman (2001): *Riskanalys och en jämförelse av analys metoder.* Institutionen för Informationsteknologi. Mitthögskolan. Sundsvall

Farell R, (2010): Securing the Cloud - Governance, Risk, and Compliance Issues Reign Supreme. *Information Security Journal: A Global perspective.* Vol 19, No 6, s. 310 – 319.

Gollmann D (2011): *Computer security third edition.* John Wiley & sons

Grance T och Mell P (2009): Draft NIST working definition of Cloud computing v15. *National Institute of Standards and Technology, Information Technology Laboratory*

Harautz J, Kaufman L och Potter B (2009): Data security in the world of cloud. *IEEE Security and Privacy.* Vol 4, No 7.

Hosseini A, Sommerville I och Siriam I (2010): *Research challenges for enterprise cloud computing.* School of Computer Science. University of ST Andrews. UK

Jacobsen D I (2002): *Vad, hur och varför. Om metodval i företagsekonomi och andra samhällsvetenskapliga ämne*. Studentlitteratur, Lund

Julisch K och Hall M (2010): Security and control in the cloud. *Information Security Journal: A global perspective.* Vol 19, No 6, s. 299-309.

Khan K och Malluhi Q (2010): Establishing trust in cloud computing. *IT professional.* Vol 12, No 5, s. 20-27.

Kvale S (1997): *Den kvalitativa forskningsintervjun*. Studentlitteratur, Lund

Leveque V (2006): *Information security: A strategic approach.* Chichester, Hokboken NJ

Mirashe S och Kalyankar N.V (2010): Cloud computing. *Journal of Computing.* Vol 2, No 3.

Oates B J (2006): *Researching information systems and computing.* Sage, London.

Pauley W A (2010): Cloud Provider Transparency an empirical evaluation. *IEEE Security and Privacy.* Vol 8, No 6, s. 32-39.

Rittinghouse J W och Ransome J F (2010): *Cloud computing Implementation, Management and Security.* CRC press, Taylor & Francis group

SIG Security (1998): *Säkerhetsarkitekturer*. Studentlitteratur AB

Stallings W och Brown L (2008): *Computer Security - principles and practice*, Pearson education

Subashini S och Kavitha V (2010): A survey on security issues in service delivery models of cloud. *Journal of network and computer applications.* Vol 34, No 1, s. 1 - 11.

Takabi H och Joshi J (2010): Security and Privacy challenges in Cloud computing environment. *IEEE Security and Privacy.* Vol 8, No 6, s. 24 – 31.

Velte T, Velte A och Elsenpeter R (2010): *Cloud Computing: A practical approach.* The mcgraw hill companies

Wang C, Li J, Lou W och Ren K (2010): Toward publicly auditable secure Cloud Data Storage services. *IEEE Network Magazine.* Vol 24, No 4.

Whitman M E och Mattord H (2008): *Management of information security second edition*. Course technology.

Zhou M, Zhang R och Xie W et al (2010): Security and privacy in cloud computing: a survey. *Sixth International Conference on Semantics, Knowledge and Grids*, Ningbo, China, 1 – 3 nov.