LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Risker inom molntjänster

Molntjänstleverantörernas syn på säkerhet

Kandidatuppsats 15 hp, kurs SYSK02 i Informationssystem
Framlagd Maj 2015

Författare: Oskar Bengtsson
Johan Friborg
Andreas Lundsten

Handledare: Mirella Muhic

Examinatorer: Anders Svensson
Odd Steen

Risker inom molntjänster: Molntjänstleverantörernas syn på säkerhet

Författare: Oskar Bengtsson, Johan Friborg och Andreas Lundsten

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 127

Nyckelord: molntjänster, risker, säkerhetsrisker, juridik, organisation, tillgänglighet, sekretess, integritet

Sammanfattning:

Molntjänster är en populär teknik inom affärsmässig informationsteknologi. Den flexibla och dynamiska infrastrukturen förenklar användningen av IT. Kunderna behöver inte lägga vikt på underhåll och administration av hård- och mjukvara då det driftas av specialiserade leverantörer. I och med användningen av molntjänster finns det många fördelar såsom att det är flexibelt, lättillgängligt och ekonomiskt försvarbart. Men trots de positiva aspekterna uppkommer nya säkerhetsaspekter som inte existerat i traditionella system. I denna studie har fem säkerhetsriskområden identifierats vilket är juridiska aspekter, organisatoriska aspekter, policy och SLA, tillgänglighet, sekretess och integritet. Utifrån vår litteraturstudie skapade vi vårt teoretiska ramverk RIM, Risker Inom Molntjänster, som belyser vikten av säkerhetsriskområdena och relationen mellan dessa. RIM jämförs med en empirisk studie där sex informanter från olika molntjänstleverantörer besvarade frågor kring säkerhetsrisker inom molnet och vad som genomförs i förebyggande syfte gentemot dessa. Resultatet av studien visar att molntjänstleverantörer påvisar medvetenhet angående säkerhetsrisker samt hur säkerhetsrisker kan förebyggas. Resultatet visar att kravstandarden för säkerhet skiftar beroende på externa faktorer såsom kundernas medvetenhet, storlek och verksamhetsområde vilket hindrar ett standardiserat säkerhetsarbete.

Innehållsförteckning

Tabellförteckning

Figurförteckning

1 Introduktion

Effektiv IT-användning spelar idag en allt viktigare roll för moderna företags konkurrenskraftighet. Ullah och Khan (2014) menar att långt fram i raden av effektiva och innovativa IT-lösningar står molntjänster. Molntjänster har sedan dess introduktion, 2007, varit ett centralt ämne i diskussioner angående affärsmässig informationsteknologi och tillförsel av en flexibel och dynamisk IT-infrastruktur (Wang, von Laszewski, Younge, He, Kunze, Tao & Fu, 2008). Wang et al (2008) föreslår följande definition av molntjänster:

> "*A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way*" (Wang et al, 2008, s 139).

Mell och Grance (2011) har en liknande definition av molntjänster vilket skapar förutsättningar för en lätthanterlig nätverksåtkomst till en gemensam pool av konfigurerbara datorresurser. Tekniken inom molntjänster skapar förutsättningar för kunderna att flytta och få åtkomst till data och applikationer på molnet. Hårdvara och dataresurser är benägna att bli föråldrade, däremot är externa datorplattformar en smart lösning för kunderna att söka sig ifrån en komplex implementationsprocess och administrativt underhåll som konfigurering och uppdatering. (Wang et al, 2008). Vidare minskar behov av att utbilda personal och införskaffa licensiering till ny mjukvara (Subashini & Kavitha, 2011).

Utvecklingen av hård- och mjukvara följer en hög takt och ständig anpassning till ny teknik är nödvändig för att ta del av fördelar relaterat till effektiv IT-användning. Molntjänster gör denna anpassning effektiv och ekonomisk även för mindre företag som inte har möjlighet att investera stora resurser i egenutvecklade IT-lösningar. (Wang, Wang & Ren, 2010). Dock skapar denna expansiva och snabba utveckling av molntjänster många utmaningar gällande säkerhet (Ullah & Khan, 2014). Subashini och Kavitha (2011) betonar att säkerhet gällande integritet och dataskydd är den största anledningen till att företagskunder ställer sig frågande gentemot anskaffning av molntjänster.

1.1 Forskningsfråga

Hur ställer sig leverantörer till riskhantering inom molntjänster?

1.2 Syfte

Syftet med denna uppsats är att skapa en förståelse för hur molntjänstleverantörer ställer sig till säkerhetsrisker inom molntjänster samt att analysera deras syn på förebyggande arbete gentemot säkerhetsrisker. Vidare vill vi presentera ett teoretiskt ramverk där vi identifierar riskfaktorer från tidigare forskning inom området och applicera detta på ett nulägesperspektiv.

1.3 Avgränsningar

På grund av den givna tidsramen och undersökningens omfattning har vi valt att avgränsa den empiriska studien till sex intervjuer med företag som är lokaliserade i Sverige.

De riskfaktorerna som identifieras i denna studie påverkar både leverantörer och kunder. I den kvalitativa studien har empirisk data enbart samlats in från informanter som arbetar för molntjänstleverantörer. Detta gör vi då vi anser att leverantörerna har en djupare förståelse angående vilka säkerhetsrisker som existerar inom molntjänster. Anledningen till att vi avgränsar oss från kundens syn på säkerhet är att vi anser det att är svårt att få tag på molntjänstkunder som förfogar säkerhetskunskaper inom den relativt unga branschen.

Utifrån litteraturgenomgång har vi valt att avgränsa oss till fem olika riskområden angående säkerhetsrisker i molnet vilket är juridiska aspekter, organisatoriska aspekter, policy och SLA, tillgänglighet, sekretess och integritet.

I vår teori har vi avgränsat oss till att enbart använda aktuella referenser, 2009 och framåt, med några få undantag för termdefiniering. Då vi anser att molntjänster är ett aktuellt område där litteratur lätt blir inaktuellt.

2 Litteraturgenomgång

I litteraturgenomgången har 60 litterära källor bearbetats, främst vetenskapliga artiklar som belyser områden kring molntjänster. Valet av dessa artiklar utfördes genom analys av hur väl de passade i rapportens kontext samt prioritering genom analys av publiceringsdatum. Fullständig lista med bearbetade artiklar presenteras i Appendix 7.1

2.1 Informationssäkerhet

Informationssäkerhet syftar till hur information skyddas inom en organisation. Detta uppfylls genom att säkra tillgång, ändring samt tillgänglighet till data (Anderson, 2001). Vidare betonar Anderson (2001) vikten av en medvetenhet om att informationssäkerhet innehåller mer än bara den tekniska aspekten som policyer, processer och övervakning. Även Stahl, Doherty och Shaw (2001) nämner att informationssäkerhet är något som går långt utanför det tekniska lagret då sociala och organisatoriska aspekter har betydande roller inom informationssäkerhet. Även om organisationer stadigt utvecklar nya metoder och verktyg för att säkerställa information inom den snabbt växande IT-industrin, kvarstår säkerhetsbrister som ett kärnproblem. (Stahl et al, 2001).

LeVeque (2006) menar att resurserna som avsätts för att skydda informationen måste baseras på dess värde. Typen av säkerhetsresurser som används måste reflektera hur informationen bidrar till värde i organisationen (LeVeque, 2006).

Informationssäkerhetens roll har utvecklats från att skydda data till att bygga upp ett säkert och förtroendeingivande nätverk där data kan delas och kärnfaktorer som integritet, sekretess och tillgänglighet införlivas. Det är viktigt att se till att informationssäkerheten ger maximal strategisk nytta för organisationen för att uppnå mål inom kärnområden. (Leveque, 2006).

2.2 Översikt Molntjänster

Molntjänster har genom sitt tillförande av en flexibel och dynamisk IT-infrastruktur blivit ett uppmärksammat ämne inom affärsmässig informationsteknologi (Subashini & Kavitha, 2011). Istället för implementering av en traditionell IT-lösning som inkluderar hårdvara, mjukvara och underhåll erbjuder molntjänster en extern behovsbaserad lösning. Användare konsumerar grundläggande informationstjänster men komplexa frågor som underhåll och administration av hård- och mjukvara hanteras av specialiserade leverantörer. (Iver & Henderson, 2012). Tekniken möjliggör att kunderna kan flytta och få tillgång till data och applikationer via molntjänster molnet (Bhattacherjee & Park, 2013). Hårdvara och dataresurser är benägna att bli föråldrade, då är outsourcade datorplattformar en smart lösning som hjälper kunderna att söka sig från en komplex implementationsprocess, administrativt underhåll, konfigurering och uppdatering (Wang et al, 2008). Vidare minskar behovet av att utbilda personal och införskaffa licenser till ny mjukvara (Subashini & Kavitha, 2011).

Ullah och Khan (2014) menar att samtidigt som teknologin inom molntjänst ständigt utvecklas ökar samtidigt efterfrågan på grund av ekonomiska och prestandamässiga fördelar. Elasticitet är en egenskap som tillåter användaren och dess tillhörande organisation att administrera IT-kostnader mer effektivt i jämförelse med direkt ägarskap av IT-resurser. Användaren ges möjligheten att justera nivån av hård- och mjukvara efter behov. (Feuerlicht & Govardhan, 2010).

2.3 Presentation av riskområden/riskindelning

För att analysera risker inom molntjänster genomfördes en litteraturstudie där vi utifrån 17 artiklar identifierar och kategoriserar risker och möjligheter som nämns i dessa. Eftersom olika författare definierar identiska risker på olika sätt har vi valt den definitionen vi anser passa bäst i uppsatsens kontext. Nedan presenteras våra fem riskindelningar individuellt med tillhörande risker. Dessa kommer ligga till grund för det teoretiska ramverket.

Inom IT och informationssystem är riskhantering och säkerhet en viktig faktor. Exempel på områden som berörs är juridiska frågor, standardisering, problem med policys, sekretess och integritet. (Subashini & Kavitha, 2011). Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica och Zaharia (2009) förklarar problem som uppstår när användare går ifrån traditionella fasta kostnader till molntjänsters dynamiska kostnader. Detta beskrivs som transference of risk vilket definierar hur riskområden skiftar vid molntjänstimplementering (Armbrust et al, 2009).

Dupré och Haeberlen (2012) kategoriserar risker relaterade till molntjänster i tre områden: tekniska, juridiska samt policy och organisatoriska risker. Géczy, Izumi och Hasida (2012) använder en liknande kategorisering vilket även inkluderar integrering av nya system, kundanpassning samt flytt av applikationer inom eller utanför molnet. Géczy et al (2012) hävdar vidare att de största riskerna inom molntjänster är loss of control, tillgänglighet och juridiska aspekter.

Nedan i tabell 2.1 Riskanalys utifrån artiklar, presenteras en sammanställning av litteraturstudiens identifierade riskområden i tabellform. Syftet med tabellen är sammanställa litteraturens syn på riskområdet samt ge läsaren en tydlig överblick av identifierade riskområden. Ett X i en kolumn betonar att författarna nämnt och identifierat riskområdet.

Tabell 2.1 Riskanalys utifrån artiklar

	Carrol et al, 2011	EU Opinion, 2012	Armbrust et al, 2009	Wade et al, 2008	Géczy et al, 2012	Venters & Whitley, 2012	Subashini & Kavitha, 2011	Gupta, 2010	Zissis & Lekkas, 2010	Chet et al, 2012	Sahito & Slany, 2013	Dupre & Haeberlen, 2012	Feuerlicht & Govardhan, 2010	Khajeh-Hosseini et al, 2010	Motahari-Nezhad et al, 2009	Patel et al, 2009
Juridiska aspekter					X	X										
Sekretess och Transparens	X	X			X	X	X					X				
Datalokalisering		X			X	X	X					X			X	
Organisatoriska, Policy & SLA	X		X					X				X				
Loss of governance					X					X		X				
Inlåsning av data		X	X									X	X		X	
SLA	X		X					X	X	X		X	X	X	X	X
Tillgänglighet	X		X		X	X	X	X	X			X	X	X		
Datatillgänglighet			X			X	X	X	X	X						
Internettillgänglighet			X			X	X		X			X				
Performance unpredictability	X		X			X						X	X	X		X
Sekretess	X	X					X		X	X	X	X		X	X	X
Isolation failure			X		X	X	X	X	X	X	X	X			X	
Identity management	X	X			X		X		X		X	X				
Software confidentiality	X								X	X						
Web application security							X	X								
Dataremanens									X	X		X			X	
Integritet							X		X	X		X				

2.3.1 Juridiska Risker

"*The issues of liability, disclosure and legislative differences in various geographical regions are among the major ones to consider*" (Géczy et al, 2012, s.63). Géczy et al (2012) betonar med detta citat vikten av de juridiska riskerna inom den geografisk obundna infrastrukturen som molntjänster verkar inom. Även Ullah och Khan (2014) nämner att avsaknad av policyns och procedurer gällande granskningar, regleringar och lagar är ett problem som måste åtgärdas.

Sekretess & Transparens

Molntjänstleverantörer strävar efter att undvika ansvarstagande gentemot tredjepartsintressenter och kunder. Detta kan skapa ett motstånd mot molntjänster och leverantörer då intressenter inte juridiskt kan säkra sig mot förlust av data, dataläckage eller liknande som leverantören orsakat. Kunden tappar även kontroll över möjligheten att leverantören frivilligt eller under tvång lämnar ut data eller information till tredje part. (Géczy et al, 2012).

Datalokalisering

En annan juridisk risk inom molntjänster är bristande kunskap om var data lagras geografiskt då många molntjänstleverantörer kan använder sig av flertalet olika datacenter spridda över hela världen. Detta äventyrar kundens rättigheter då lagar och säkerhet skiftar mellan olika länder. Det kan även vara svårt att på en viss tidpunkt tydligt definiera var data geografiskt sett är sparad. (Géczy et al, 2012).

Ett praktiskt exempel är hur personuppgifter lagras inom molnet. Sverige införde 1998 Personuppgiftslagen, PUL, vars syfte är att skydda den svenska befolkningens personuppgifter. PUL är baserat på Europeiska Unionens, EU, dataskydds direktiv vilket har möjliggjort att övriga EU-länder har liknande lagar för hantering av personuppgifter. (Datainspektionen). I EU Opinion (2012) betonas molnanvändarens ansvar att skydda lagrad data i deras applikationer samt behovet av en ingående riskanalys innan övergång till molnet. Målet med en riskanalys bör vara att, vid val av molntjänstleverantör, se till att alla lagar gällande behandling av personuppgifter uppfylls. Användaren av molntjänsten bör därför involvera en tredje part som granskar valet av molnleverantör från en opartisk synvinkel. (EU Opinion, 2012).

2.3.2 Policy och organisatoriska risker

Loss of governance

I en molntjänstmiljö är det leverantören som ansvarar för administration och kontroll av data (Gupta, Dave & Gupta, 2014). Dupré och Haeberlen (2012) menar att vid användning av molntjänster avsäger sig användaren inte endast exklusivt dataägande men även kontroll och säkerhet av data till molntjänstleverantören. Expansionen av delad data bidrar till att behörighetsfrågan blir allt mer komplex (Dupré & Haeberlen, 2012). Vidare betonar Chen och Zhao (2012) problematiken vid användarens säkerhetsställning av att ursprungligt skydd och åtkomstbegränsningar upprätthålls. Användarens begränsade kontroll och styrning av molntjänsten kan leda till säkerhetsbrister inom sekretess, integritet och tillgänglighet av data (Dupré & Haeberlen, 2012).

Inlåsning av data

Armbrust et al (2009) påvisar att en problemfaktor inom molntjänster är kundens begränsningar vid export av data till, från eller mellan molntjänster. Enligt Dupré och Haeberlen (2012) är det höga beroendet en kund har till en enskild leverantör problematisk då byte från en leverantör till en annan kan vara en virtuell omöjlighet. I dagsläget erbjuds ett begränsat utbud av verktyg, medel, standardiserat dataformat och infrastruktur för att garantera kundens portabilitet. Den dynamiska infrastrukturen inom molntjänster baseras på icke standardiserade data och programlogik vilket gör migration från leverantör problematisk. Detta kan dock förebyggas genom en välplanerad utgångsstrategi. (Dupré & Haeberlen, 2012).

Molntjänstleverantören kan ha ett direkt eller indirekt incitament att förhindra överföring av sina kunders tjänster och data. Ett potentiellt beroende av tillhandahållande av tjänster kan leda till konsekvenser för kunden om molntjänstleverantören går i konkurs och en migration till annan leverantör är ekonomiskt och tidsmässigt omfattande. (Dupré & Haeberlen, 2012).

För att förebygga denna problematik bör leverantören erbjuda formella avtal och gemensamma underliggande filformat för export och import av data. Det ligger i molntjänstleverantörens intresse att erbjuda en förenklad portabilitet som både är heltäckande och kostnadseffektiv för kunden. (Dupré & Haeberlen, 2012).

Service level agreement

SLA, Service Level Agreement, är ett avtal mellan leverantör och kund av tjänst. Syftet att stifta ett gemensamt avtal angående förväntningarna vid förmedling av molntjänsten. Det avtal som stiftas mellan leverantör och kund kan brista i ett säkerhetsmässigt perspektiv. (Wu & Buyya, 2010). Baker, Hylender och Valentine (2008) påvisar i en studie att i 59 % av dataintrångsfall,

fanns det säkerhetspolicy och rutiner som inte tillämpats. Baker et al (2008) menar att genom ansvarsfördelning och kontroll av genomförande kan utfallet vid dataintrång minimeras.

Parallellt med övergången från traditionell datalagring till molntjänster menar Patel, Ranabahu och Sheth (2009) att SLA framträder som en nyckelaspekt. Den dynamiska infrastrukturen skapar ett behov av kontinuerlig kontroll och kvalitetsövervakning av tjänsten för att upprätta SLA mellan kund och leverantör (Patel et al, 2009). Buyya och Yeo (2008) menar att förhandling av QoS, Quality of Service, mellan kund och leverantör är nödvändig för framställning av SLA men även hantering av risk om SLA bryts.

Om molntjänstleverantören outsourcar en del av sin tjänst till tredjepart minskar insynen i säkerhetskontroll vidare. Det ligger ett ansvar på molntjänstleverantören att klargöra vilka IT-tjänster som de outsourcar för att skapa korrekta förutsättningar för kunden att utvärdera risknivån. Bristande transparensnivå i avtal och leverans av tjänst riskerar att bidra till minskat kundförtroende gentemot molntjänstleverantören. (Dupré & Haeberlen, 2012).

2.3.3 Tillgänglighet

Tillgänglighet inom molntjänster kan vara en avgörande faktor vid beslut av implementering (Venters & Whitley, 2012). Vid bristande tillgänglighet finns risken att användare inte kommer åt kritisk data eller tjänster (Géczy et al, 2012). Detta ställer höga krav på molntjänstleverantörerna då de måste matcha eller överträffa tillgängligheten för sina tjänster mot traditionella IT-lösningar (Venters & Whitley, 2012). Tidigare forskning visar dock att stora aktörer inom branschen som till exempel Google App Engine och Amazon Simple Storage Services håller en hög standard med uppemot 99,9% tillgänglighet, men detta är inte tillräckligt för organisationer med verksamhetskritiska system (Armbrust et al, 2009; Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011).

Datatillgänglighet

Gupta (2010) nämner prestandan av molnleverantörens system som ett av de största orosmomenten med användning av molntjänster. Frågor som bör besvaras är hur data sparas samt hur applikationer hanteras på molntjänstleverantörens infrastruktur. För att en molntjänstleverantör ska lyckas med att leverera eftertraktade molntjänster bör tjänster levereras med hög tillförlitlighet som uppfyller kundens behov. (Gupta, 2010).

Webbtillgänglighet

Tidigare forskning har visat att stabiliteten i nätverksuppkopplingen har varit en stor begränsning vid molntjänsters expansion. Främst har det existerat problem med höga svarstider hos kunden

men även periodvisa fullständiga bortfall av kontakt med molntjänsten. Dock har de senaste årens globala investeringar i fiberoptik och geografiskt utspridda datacenter, minskat dessa problem. (Armbrust et al, 2009). Molntjänstleverantörer bör använda sig av flera internetleverantörer i sina datorcenter för att eliminera risken med denna problematik (EU Opinion, 2012).

Oförutsägbar prestanda

En annan stor faktor som avgör en molntjänsts tillgänglighet är hur leverantören hanterar skiftande krav på datorkraft över tid (Armbrust et al, 2009). Armbrust et al(2009) menar att en molntjänstleverantör som förmedlar en tjänst till flera kunder med unika krav på datorkraft, ökar risken för en flaskhals i systemet vilket påverkar prestandan negativt. För att uppfylla kundens krav på tillgänglighet använder molntjänstleverantören sofistikerade marknadsanalyser för att få en tydligare bild av framtida behov. För att ytterligare förebygga problematiken är det viktigt att bibehålla transparens mot kunden. (Armbrust et al, 2009).

2.3.4 Sekretess

När en individ, ett företag eller en myndighet väljer att dela information genom molntjänst uppstår sekretessfrågor. Sekretess inom molnet hänvisar till enbart de auktoriserade parterna som skall ha tillgång till lagrad som såväl skyddad data. (Subashini & Kavitha, 2011). Puttaswamy, Kruegel och Zhao (2011) menar att bristande kryptering av data är den största anledningen till att användare uppmärksammar sekretess som den största risken vid migration till molntjänster. För att säkerhetsställa datasekretess krypteras data så den blir oläsbar. För att uppnå effektiv kryptering av data används både krypteringsalgoritmer och nyckelsäkerhet (Puttaswamy et al, 2011). Zissis och Lekkas (2010) menar vidare att säkerhetsriskerna på molnet ökar parallellt med mängden användare, enheter och applikationer som är uppkopplade till samma moln. Användning av en gemensam infrastruktur, begränsar inte bara risker angående tillgänglighet och organisatoriska risker utan även för dataintrång från andra organisationer (Puttaswamy et al, 2011).

Isolering och Datasegregation

Subashini och Kavitha (2010) menar att isolering av kunders databaser på en gemensam server inte uppfylls. Säkerhet och skydd av data och nätverk riktar sig främst mot externa hot för att säkra molntjänstens kritiska infrastruktur dock inte mot interna attacker. Insiderhot hänvisar till en individ som har tillgång till nätverk och data men avser att utföra skadliga handlingar som obehörig åtkomst till känslig information, bedrägeri, olaglig spridning av information till obehöriga eller externa parter. (Subashini & Kavitha, 2010). De nuvarande tekniska

motåtgärderna inkluderar åtkomstkontroll, krypterat lösenord, fysisk- och biometrisk autentisering, brandväggar, krypterad dataöverföring, upptäckt av beteendemönster och förebyggande arbete gentemot dataläckage (Sahito & Slany, 2013). Sahito och Slany (2013) menar vidare att det är av yttersta vikt att vidta åtgärder för att säkerhetsställa den dynamiska infrastrukturen på molnet. Framställning av standardiserade strategier är därför nödvändiga för att hantera det hot och risker inom molntjänster (Sahito & Slany, 2013).

"As the openness of cloud and sharing virtualized resources by multi-tenant, user data may be accessed by other unauthorized users" (Chen & Zhao, 2012, s. 648). Multitenancy hänvisar till molntjänstens utformning i hänseende till resursdelning. Molntjänster baseras på delad resursanvändning där flera användare har tillgång till och delar minne, applikationer, nätverk och data. (Dupré & Haeberlen, 2012; Motahari-Nezhad, Stephenson & Singhal, 2009). Användare skyddas och isoleras på en virtuell nivå men hårdvaran separeras inte till samma grad (Zissis & Lekkas, 2010).

Identitetshantering

Zissis och Lekkas (2010) menar att datasekretess inom molnet är starkt kopplat till auktorisering av användare. Molntjänstleverantören prioriterar skydd av personligt konto vilket är en instans av ett större problem vid säkerhetställning av åtkomst till data (Zissis & Lekkas, 2010). Sahito och Slany (2013) menar att bristande auktorisering kan leda till obehörig åtkomst till ursprungsanvändarens konto vilket är ett direkt hot mot sekretessen och i förlängningen även användarens integritet. Vidare betonar Subashini och Kavitha (2011) problematiken gällande administration av säkerhetsnycklar vid kryptering av data. Vanligtvis är detta en uppgift som administreras av dataägare men överförs till molntjänstleverantörerna då kundernas IT-kunskap är begränsad (Subashini & Kavitha, 2011). Det ställs därför krav på molntjänstleverantören då en stor mängd data och tillhörande nycklar skall administreras vilket skapar ett behov för ökad processorkraft och automatiserade processer (Chen & Zhao, 2012). Subashini och Kavitha (2011) hänvisar till IdM, Identity Management, som är en administrativ metod inom nätverk vilket hanterar och kontrollerar tillgången till resurser genom utplacering av restriktioner på konton.

Sekretess inom mjukvara

"Software confidentiality is as important as data confidentiality to the overall system security." (Zissis & Lekkas, 2010, s.586). Sekretess med hänseende till programvara syftar till att säkerhetsställa att specifika tillämpningar och processer hanterar användarens personuppgifter efter säkra metoder. Applikationssäkerhet hänvisar till användning av mjuk- och hårdvara i syfte att förhindra obehöriga att få tillgång till och kontroll över applikationen och tillhörande information. Obehöriga får tillgång till applikationen genom ofullständig närverkssäkerhet och betraktas av systemet som behörig användare. (Zissis & Lekkas, 2010). Gupta et al (2014) betonar att molntjänstleverantörer använder en föråldrad säkerhetsstandard. Det bör ställas högre krav på företagen och om införskaffning av omfattande säkerhetskontroller (Gupta et al, 2014). Den underliggande mjukvaran bör därför vara certifierad i syfte att säkerhetsställa att mjukvaran inte medför ytterligare sekretess- och integritetsrisker (Zissis & Lekkas, 2010).

Sekretess inom webbtjänster

Säkerhetsrisker inom webbapplikationer skapar en indirekt sårbarhet inom molntjänster och medför en skadlig inverkan hos användare (Subashini & Kavitha, 2011). För att säkerställa nätverkssäkerhet och säkra användarnas sekretess och integritet inom molntjänster skapas det ett behov för striktare åtkomstkontroll och upprätthållning av standard mot yttre hot (Gupta et al, 2014). Zissis och Lekkas (2010) hänvisar till problematiken vid användning av objektiv återanvändning inom molnets infrastruktur då det ställer högre krav på säkerhet och kontroll. Risker som riktas mot molntjänster skiljer sig inte från andra webbapplikationer utan problematiken identifieras inom brandväggar och ställer krav på upptäckande av nätverksintrång och förebyggande system som IDS, Intrusion Detection System (Subashini & Kavitha, 2011).

Dataremanens

Sekretess kan brista oavsiktligt genom dataremanens. Dataremanens är en historisk representation av data som ämnats att raderas men återställas och är fortfarande teoretiskt tillgängligt. (Chen & Zhao, 2012). Säker och fullständig radering av data i molnet kan vara ineffektiv då kopior av data kan vara otillgängliga eller kundernas data lagras gemensamt på enskild server (Dupré & Haeberlen, 2012). Logiska enheter, virtuella separationer och bristande separation i hårdvara mellan en grupp användare kan leda till att dataremanensen oavsiktligt lämnar ut privata uppgifter (Zissis & Lekkas, 2010). Med hänseende till nyttjanderätt och återanvändning av hårdvara, innebär det ett högre risktagande för kunden i jämförelse med dedikerad hårdvara (Dupré & Haeberlen, 2012).

2.3.5 Integritet

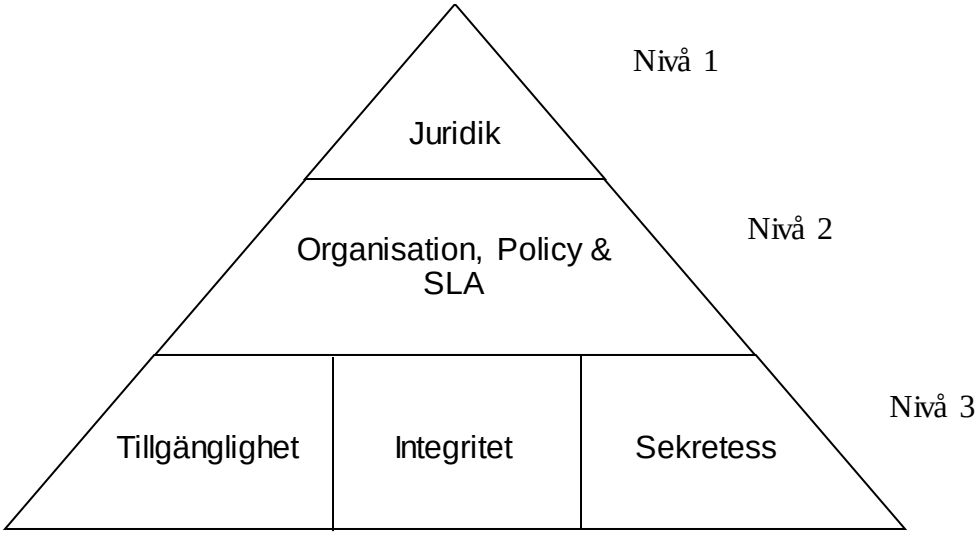
Chen och Zhao (2012) betonar att molntjänstleverantören och användaren skall beakta dataintegritet som en viktig komponent inom molntjänster. Subashini och Kavitha (2011) menar att av de olika elementen i ett system är dataintegritet ett av de mest kritiska. I en liten skala uppnås dataintegritet enkelt genom separation av system och databas. Inom distribuerade system är dataintegritet svårare att upprätthålla då flertalet databaser och system är sammankopplade. För att bevara dataintegritet i distribuerade system krävs det att transaktioner genom olika datakällor behandlas och utförs på ett korrekt och säkert sätt. Vidare har varje applikation och molntjänstleverantör olika nivåer av tillgänglighet och SLA, vilket komplicerar hanteringen av dataintegritet. Avsaknaden av integritetsverktyg eller verktyg som kringgår applikationens logik och kopplar upp sig gentemot databasen direkt, kan resultera i djupgående problem. (Subashini & Kavitha, 2011).

Utmaningen med integritetsskydd är delningen av data utan att personlig information läcker ut till obehöriga parter. Nyckeln till integritetssäkerhet inom molnet är att separera känslig data samt tillämpa korrekt kryptering. (Chen & Zhao, 2012). Vidare menar Dupré och Haeberlen (2012) att multitenancy frambringar flera integritets- och konfidentiella säkerhetsrisker då en gemensam infrastruktur medför risken för bristande separation av kunders data. Wang et al (2010) menar att forskningen inom molntjänster lyfter fram vikten av att säkerhetsställa dataintegritet. Forskningen har kommit fram till tekniker som hjälper användaren att försäkra sig om att data lagras korrekt och på ett säkert sätt. Vidare betonas bristerna i forskningen då den begränsar sig till ett scenario där datalagring äger rum på en isolerad server och tar därför inte hänsyn till den dynamiska molntjänstmiljön. (Wang et al, 2010). Chen och Zhao (2012) betonar att säkerhetsrisker ökar i samband med mängden data då det är svårt att verifiera datans integritet. För att säkerhetsställa integritet bör transaktioner följa ACID, Atomicity, Consistency, Isolation och Durability (Subashini & Kavitha, 2011).

2.4 Teoretiskt ramverk

Med hänseende till tidigare delkapitel har vi framställt detta teoretiska ramverk som representerar de säkerhetsrisker som är kopplade till molntjänster. Detta ramverk ligger till grund för den empiriska studien och genomsyrar uppsatsens struktur. I delkapitlet nedan presenteras och argumenteras ramverket och teori som ligger till grund för framtagandet av detta.

Figur 2.1 är en representation av det teoretiska ramverket som är framtaget av uppsatsförfattarna men uteslutande baserat på tidigare forskning inom området. Vid utformning av strukturen för det teoretiska ramverket utgick vi i första hand från Dupré och Haeberlen (2012) och Géczy et al (2012) kategorisering av riskområden. För att validera ramverket har vi utgått från litteraturstudien, se tabell 2.1, där riskfaktorer i 17 artiklar analyserats. Enligt litteraturstudien och val av metod som förklaras i nästkommande kapitel, anser vi att säkerhetsriskerna inom molntjänster kan delas upp i tre nivåer: Nivå 1 hänvisar till juridiska aspekter, nivå 2 hänvisar till organisatoriska aspekter samt policy och SLA. Nivå 3 hänvisar till det tekniska riskområdet som innehåller tillgänglighet, sekretess och integritet.



Figur 2.1 Risker Inom Molntjänster, RIM

Den triangulära formen påvisar ett vertikalt samband mellan nivåerna och ett horisontellt samband mellan de tekniska riskområdena. De olika nivåerna påvisar ett samband där underliggande nivå är direkt beroende av de ovanliggande. Modellen påvisar även att det finns en koppling men även stark avgränsning mellan de fem riskområdena.

3 Metod

Syftet med nedanstående kapitel är att redogöra för läsaren vilken undersökningsmetod som används för att skapa uppsatsen samt motivering till val av metod. Kapitlet är uppdelat efter moment som genomarbetats för att nå fram till ett resultat.

Vi genomförde en litteraturstudie där vi identifierade olika säkerhetsrisker vid användandet av molntjänster. Utifrån denna litteraturstudie skapade vi ett teoretiskt ramverk som vi använde oss av för att utforma vår intervjumall. Syftet med skapandet av teoretiskt ramverk är att uppnå en jämförande analys mellan litteraturstudien och empiriska data som erhållits från intervjuer med företagsinformanter.

3.1 Litteraturgenomgång

Litteraturgenomgången påbörjades genom sökning efter relevanta artiklar som behandlar problemområdet. Resurser som användes vid sökningen av artiklar var sökmotorer inom Senior Scholars'AIS, Association for Information Systems rekommenderade journaler, Google Scholar och Lubsearch. Sökord som användes var: *cloud computing, risk management, security, information systems, information technology, SLA, availability, confidentiality, Software as a Service, privacy, legal, integrity, data privacy*.

Sökresultatet generade 59 artiklar som behandlar problemområdet vilket senare analyserats. I artikelanalysen utfördes en sammanfattning och bedömning utefter relevans för vår undersökning. Vi valde att utforma vårt litteraturkapitel efter 30 källor som enligt vår bedömning är relevanta för analys av riskområdet. Slutligen i vår litteraturgenomgång presenteraras vårt ramverk som ligger till stöd för den empiriska studien.

3.1.1 Utformning av teoretiskt ramverk

Efter analys av existerande teoretiska ramverk inom forskningsområdet informationssystem, drog vi slutsatsen att de inte gick att tillämpa i kontext av vår frågeställning och val av undersökningsmetod. Med den utgångspunkten valde vi att skapa ett eget teoretiskt ramverk, se

figur 2.1, som är en sammanställning av de identifierade riskområdena, se tabell 2.1, i molntjänster som nämns inom 16 av de 30 valda källorna.

3.2 Metod för insamling av empirisk data

För att uppfylla vår explorativa frågeställning så valde vi att en kvalitativ intervjumetod var den mest lämpade. Jacobsen (2002) betonar att en kvalitativ metod är mest lämplig vid förtydligande av ett oklart ämne. Vidare nämner Denscombe (2003) att metoden är att föredra när man vill analysera hur informanter förstår och tolkar en given situation. Detta passar väl in på vår frågeställning där vi undersöker hur en molntjänstleverantör ställer sig avseende riskhantering inom molntjänster.

3.2.1 Intervjuguide

Vår intervjuguide, se appendix 7.2, utformades utifrån vårt teoretiska ramverk och litteraturgenomgång vilket tjänar syftet att undersöka hur företag ställer sig till de säkerhetsrisker som uppkommer vid nyttjandet av molntjänster.

Säkerhetsrisker inom molntjänster är ett omfattande område vilket bidrog till vårt beslut att avgränsa vår intervjumall efter vårt teoretiska ramverk. Syftet var att säkerhetsställa en kvalité och väsentlighet samt inrikta oss på specifika diskussionspunkter. Vi anser att avgränsningen var nödvändig med hänseende till antalet informanter och möjligheten att jämföra svaren mellan olika företag och företagsroller. Intervjufrågorna diskuterades och analyserades iterativt inom gruppen inför, mellan och efter intervjuer. Vårt huvudsakliga fokus var att utforma en intervjumall som var delvis heltäckande men även begriplig med lite utrymme för misstolkning.

Intervjuguiden inleds med generella frågor vilket kartlägger informanten, dess befattning och vilket företag och kunder han eller hon representerar. Informanten gavs i detta skede möjligheten att vara anonym. Vidare ställs en öppen fråga: *"Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?"* (Intervjuguide, Appendix 7.2, Q1). Syftet med frågan var att undersöka säkerhetsrisker inom molnet utan att eventuellt bidra till ett påverkat svar. Vidare delas intervjuguiden upp i sju delar: förebyggande säkerhetsarbete, juridiska frågor, SLA, tillgänglighet, sekretess, integritet och kundrelaterade frågor. Den tydliga strukturen och avgränsningen inom vår intervjuguide bidrog till en effektiv intervju då vi stadgade tydliga ramar med syfte att följa frågeställningen. Intervjuinformanterna fick tillgång till intervjuguiden innan

intervjun ägde rum med syfte att säkerhetsställa strukturerade och genomtänkta svar med relevanta exempel.

3.2.2 Val av informanter

Vi har valt att rikta oss till företag som levererar molntjänstlösningar och till viss mån använder sig av molntjänster. Inom dessa företag har vi valt att rikta oss till anställda som har bred erfarenhet inom molntjänster. Vi menar att det krävs erfarenhet för identifiering av säkerhetsrisker och förebyggande åtgärder.

I ett inledande stadie utformade vi en lista över molntjänstleverantörer som vi ansåg vara lämpliga för en potentiell intervju. Vi identifierade företagen genom sökning via internet med nyckelorden: *Molntjänster, SaaS, Svenska företag, Cloud computing*. Sökningen resulterade i 23 företag som var relevanta utifrån att de levererar molntjänster till andra företag och till slutkund. En annan faktor som vi sökte efter var bred kunskap kring molntjänster och ett plus var givetvis att de har arbetat med molntjänster en längre tid. Dessa företag kontaktade vi sedan via telefon och mail. Denna metod gav olika resultat då vissa företag var intresserade och behjälpliga medan andra tackade nej på grund av tidsbrist.

Tabell 3.1 Sammanställning av informanter

Företag	Befattning	Namn	Intervjumetod	Tid
Xledger	Sverigeansvarig	Lars Lobelius	Telefon	20.41
Integrationsföretaget	Konsult	Anonym	Telefon	23.12
Telekomföretaget	Software Architect	Anonym	Personligt möte	28.53
Knowit Cloud Innovation	CEO, CXO	Ola Hesselroth & Johan Berneskog	Mail	-
Systemutvecklingsföretaget	Systemutvecklare	Anonym	Telefon	20.30
Affärssystemleverantören	Drifttekniker	Anonym	Telefon	22.45

Efter vår kommunikation med de olika företagen fick vi sex företag som kunde genomföra intervjuer inom tidsramen för vår uppsats. Nedan presenteras de sju informanterna som intervjuades för framtagning av empirisk data. Förutom namn och företagsnamn så presenteras informantens befattning, intervjumetod samt längd på intervjun. Namnen på de informanter som valt att vara anonyma har tagits bort samt att deras företagsnamn har ersatts av fiktiva namn.

3.2.3 Analys av empirisk data

Det första steget i analysen av det empiriska materialet från genomförda intervjuer var att transkribera intervjuerna i sin helhet. I varje transkribering kodades de relevanta svaren på varje fråga med grön färg. Detta användes senare för att skapa en frågesammanställning, se appendix 7.3, där varje informants svar på varje enskild fråga kunde jämföras. Kodningen användes som grund för att presentera det empiriska resultatet i kapitel fyra.

3.3 Analys, diskussion och slutsats

Efter att varje riskområde sammanställts enskilt i empirikapitlet så genomfördes en jämförande analys i kapitel 5, Analys och Diskussion. Denna analys jämför erhållen empiri och teori kritiskt i kontext till frågeställningen. Kapitlet är uppdelat utifrån det teoretiska ramverket. Avslutningsvis presenteras slutsatser utifrån analysen i kapitel 6, Slutsats. Slutsatserna presenteras utifrån uppsatsens teoretiska eller empiriska bidrag, och kapitlet avslutas med förslag på vidare forskning.

3.4 Validitet & Reliabilitet

Validitet hänvisar till en uppsats giltighet, mer bestämt intern giltighet. Det vill säga validiteten av uppsatsens resultat. Över tiden har samhällsforskare förbisett idén om att beskriva samhället med en korrekt sanningsbild. (Jacobsen, 2002). Vidare hänvisar Jacobsen (2002) till intersubjektivitet vilket definieras som det närmsta man kommer sanningen. Intersubjektivitet i en uppsats kan uppnås genom att låta fler personer ifrågasätta och bekräfta giltigheten av innehållet. Internt inom uppsatsgruppen kan validiteten öka genom att kritiskt analysera uppsatsens källor samt dess information. (Jacobsen, 2002). För att uppnå giltighet i vår litteraturgenomgång har vi prioriterat användning av litteratur som publicerats i AIS Senior scholars' basket of journals, vilket är åtta accepterade journaler inom forskningsområdet informationssystem. Uppsatsens författare betonar att samtliga artiklar inte härstammar från dessa journaler men att validiteten har beprövats.

Reliabilitet syftar istället till uppsatsens tillförlitlighet. Det vill säga uppsatsens överförbarhet eller externa giltighet. Relabilitet beskrivs även till vilken grad studien kan generaliseras till att

gälla i andra sammanhang. (Jacobsen, 2002). Våra informanter företräder främst dem själva med deras egna erfarenheter, i förlängningen företagens synsätt kring riskområdet. Vi reserverar oss att denna studie kan uppnå ett annat resultat vid upprepning av studien med andra informanter vid liknande företag då det inte går att garantera att förändringar i branschen och förädling av tekniska faktorer kan förändra resultatet vid upprepning av vår studie. Vidare menar Jacobsen (2002) att tillförlitlighet och trovärdighet är essentiellt för att studien skall vara utförd på ett trovärdigt vis som skapar tillit. Vidare belyses vikten av liknande resultat vid replikering av uppsatsen. (Jacobsen, 2002). Med vår litteraturstudie, se tabell 2.1, med identifierade säkerhetsrisker och vårt empiriska underlag kan vi säga att vid replikering av studien så är möjligheten att få samma resultat hög.

3.5 Etik

I de flesta typer av undersökningar kan etiska dilemman uppstå. Främst sker detta när undersökarna på något vis vill dölja syftet med undersökningen. Anledningen till att dölja syftet är för att personers tillförlitlighet kan försvagas när de hamnar i en situation där de blir studerade. (Jacobsen, 2002). En av grundpelarna i empiriska undersökningar är att alla intressenter frivilligt skall delta i undersökningen. I vårt fall var detta av yttersta relevans då vi använder en kvalitativ metod där vi till viss del ifrågasätter intressenternas arbetsmetoder. För att uppnå detta samtycke så blev samtliga av våra informanter informerade om undersökningens syfte och spridning, de fick även ta del av sammanfattningar av intervjuerna och bekräfta eller bestrida vår tolkning av denna. Jacobsen (2002) nämner dock att för att nå hög tillförlitlighet på sin undersökning bör uppsatsens författare följa en gyllene medelväg där enbart tillräcklig information ges till intressenter. Vi tycker dock att informationen som informanterna delar med sig av är känslig på så sätt att det rör interna säkerhetsrutiner och att ett samtycke krävs för att uppnå hög validitet.

Jacobsen (2002) nämner vikten av informanternas rätt till anonymitet vilket är relevant då studien undersöker ett relativt känsligt område. Av samma anledning undvek vi att för detaljerat beskriva informanterna i studien då Jacobsen (2002) menar att det i kvalitativa studier kan vara relativt enkelt att identifiera intressenter utifrån denna information.

4 Empiri

I nedanstående kapitel presenteras uppsatsens empiriska data. Empirikapitlet inleds med presentation av deltagande intervjureinformanter och följs av en sammanställning av informanternas svar utifrån identifierade riskområden.

4.1 Informanter

Tabell 4.1 Sammanställning av informanter

Företag	Befattning	Namn	Intervjumetod	Tid
Xledger	Sverigeansvarig	Lars Lobelius	Telefon	20.41
Integrationsföretaget	Konsult	Anonym	Telefon	23.12
Telekomföretaget	Software Architect	Anonym	Personligt möte	28.53
Knowit Cloud Innovation	CEO, CXO	Ola Hesselroth & Johan Berneskog	Mail	-
Systemutvecklingsföretaget	Systemutvecklare	Anonym	Telefon	20.30
Affärssystemleverantören	Drifttekniker	Anonym	Telefon	22.45

Lars Lobelius, Xledger AB

Lars Lobelius är sverigeansvarig för Xledger och har 46 års erfarenhet inom IT-branschen och har tidigare arbetat som utvecklare, försäljningschef och företagsledare. Xledger är SaaS-leverantör till mindre och medelstora företag.

Software Architect, Telekomföretaget

Informanten arbetar som software architect på Telekomföretaget och har nio års IT-erfarenhet. Telekomföretaget levererar molntjänster till slutkund och nyttjar även molntjänster som plattform genom bland annat Amazon.

Konsult, Integrationsföretaget

Informanten arbetar som konsult på integrationsföretaget och har åtta års IT-erfarenhet. Integrationsföretaget är ett medelstort företag som levererar bland annat en integrationslösning inom molnet.

Ola Hesselroth CEO och Johan Berneskog CXO, Knowit Cloud Innovation

Ola Hasselroth och Johan Berneskog arbetar på Knowit Cloud Innovation och har båda 20 års IT-erfarenhet. Knowit Cloud Innovation förmedlar molntjänster via Amazon Web Services och Mircosoft Azure.

Systemutvecklare, Systemutvecklingsföretaget

Informanten arbetar som utvecklare på systemutvecklingsföretaget med tre års IT-erfarenhet. Systemutvecklingföretaget levererar ärendebehandlingssystem i form av SaaS till kunder i Sverige.

Drift, Affärssystemsleverantören

Informanten arbetar på affärsleverantörens driftavdelning som drifttekniker och har två års IT-erfarenhet. Affärssystemleverantören levererar bokföringssystem med funktioner som lönehantering och fakturering via molnet.

4.2 Presentation av informanternas svar

Empirin presenteras i tabellform och följer intervjumallens kategorisering. För att tydliggöra empirins koppling till ramverket RIM, Risker Inom Molntjänster, presenteras varje riskområde individuellt. Figuren i tabellernas högra hörn representerar vilken nivå som berörs i relation till RIM. Intervjuerna i sin helhet presenteras i Appendix 7.4 till 7.9.

4.2.1 Övergripande säkerhetsrisker inom molntjänster

I tabell 4.2 presenteras informanternas svar på fråga Q1 i intervjuguiden, se Appendix 7.2.

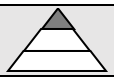
Tabell 4.2 Empirisk sammanställning övergripande säkerhetsrisker

Företag	**Sammanfattning** 
Xledger	-
Telekomföretaget	Informanten nämner bristande kontroll vilket medför risk för hackerattacker. Leverantören måste därav förlita sig till backup vilket leder till andra säkerhetsrisker som att data läcker ut eller att tillgängligheten blir lidande.
Integrationsföretaget	Informanten nämner att en stor risk med molntjänster är att allt sker "[...]utanför din egen bandbrygga[...]" (Integrationsföretaget Transskript, Appendix 7.6, Q1). Han nämner även kundens beroende till leverantören vilket kan leda till att leverantören stänger ner eller ändrar priser.
Knowit Cloud Innovation	Informanten nämner tre stora säkerhetsrisker: felaktig arkitektur, felaktig kommunikation och infrastruktur samt felaktig autentisering.
Systemutvecklingsföretaget	Informanten nämner säkerställning av informationssäkerhet och informationsklassificering som de största riskerna inom molntjänster. Informanten menar vidare att bristande klassificering och säkerhet bidrar till att den mänskliga faktorn förvärras.
Affärssystemsleverantören	Informanten hänvisar till en kombination av användarens okunskap, dåliga mjukvaror och dåliga lösenord. Vidare beskriver informanten att användarnas begränsade förståelse av säkerhetsriskerna är en drivande faktor till bristande hantering av lösenord och personlig data.

4.2.2 Juridiska risker

I tabell 4.3 presenteras informanternas svar på fråga Q8-Q10 i intervjuguiden, se Appendix 7.2.

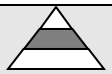
Tabell 4.3 Empirisk sammanställning juridiska risker

Företag	**Sammanfattning** 
Xledger	Informanten nämner att Xledgers servrar lokaliseras i Norge vilket är godkänt utifrån Svensk lag. Xledger menar vidare att en PUL-anmälan inte är nödvändig men det krav som ställs på kunden är att en anmälan skall skickas till skattemyndigheten.
Telekomföretaget	Informanten förklarar att företaget använder servrar som är lokaliserade internationellt och informanten känner inte till om de tar olika hänsyn till de juridiska aspekterna. Företaget använder sig av egna advokater för att säkerhetsställa vad som får göras utan att bryta avtal.
Integrationsföretaget	Informanten förklarar att företaget använder sig av servrar som är lokaliserade internationellt. Utifrån en juridisk synvinkel tar molntjänstleverantören hänsyn till juridiska aspekter som styr arkivering och vem som har åtkomst till data. Informanten menar att de inte hanterar personuppgifter och inte behöver beakta personuppgiftslagen men att *"[...]absolut största processen för oss då det handlar om cloud är den juridiska processen"* (Integrationsföretaget Transskript, Appendix 7.6, Q10).
Knowit Cloud Innovation	Informanterna menar att de inte har egna servrar utan de nyttjar globala molnleverantörer som Microsoft Azure och Amazon AWS. Informanten menar vidare att båda molntjänstleverantörerna har sina datacenter i Europa som följer EU:s lagstiftning vilket överensstämmer med Svensk lagstiftning. Vidare tillhandahåller företaget enbart plattformen för att köra applikationer och lagra data.
Systemutvecklingsföretaget	Informanten förklarar att företaget använder sig av servrar som är lokaliserade i Sverige och med tanke på typen av data som lagras tas ingen hänsyn till några juridiska aspekter.
Affärssystemsleverantören	Informanten förklarar att servrarna lokaliseras nationellt samt att företaget lägger stor vikt för att undvika juridiska komplikationer. Informanten beskriver vidare en upplevd problematik då stor del av deras behandlade data är bokföringsdata som går under bokföringslagen. Samtidigt måste företaget ta hänsyn till PUL, personuppgiftslagen.

4.2.3 Organisation, policy och SLA

I tabell 4.4 presenteras informanternas svar på fråga Q11 i intervjuguiden, se appendix 7.2.

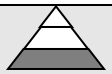
Tabell 4.4 Empirisk sammanställning organisation, policy och SLA

Företag	**Sammanfattning** 
Xledger	Informanten förklarar att Xledger använder helt klart standardiserade avtal med kund men att det finns fallspecifika undantag. Vidare betonar informanten att det finns sekretessförbindelser med kunder men kundernas förhandlingsutrymme är begränsat och att Xledger ställer krav på kunden att följa det avtal som stadgats.
Telekomföretaget	Informanten betonar att Telekomföretaget använder sig av standardiserade avtal gentemot kund.
Integrationsföretaget	Informanten menar att Integrationsföretaget erbjuder ett flertal standardiserade SLA till kunder. Avtalen har skiftande kostnad beroende på nivå av support, tillgänglighetskrav och säkerhetskrav.
Knowit Cloud Innovation	Knowit Cloud innovation använder avtal som baseras på standardavtal från IT & Telekomföretagen. Kunden och företaget ställer ömsesidiga krav på varandra. Det är kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.
Systemutvecklingsföretaget	Informanten nämner att Systemutvecklingsföretaget inte använder standardiserade avtal med kund. Vidare menar informanten att de förmedlar en gratistjänst och att det saknas standardiserat eller situationsbaserat SLA mellan parterna. Som ett kompletterande avtal används istället ett förvaltningsåtagande av företaget.
Affärssystemsleverantören	Informanten menar att Affärssystemsleverantören erbjuder både standardiserade och icke standardiserade avtal. Informanten nämner vidare att företaget har två typer av kunder, de större redovisningsbyråerna som har specialiserade avtal samt de mindre företagen som har ett standardavtal. Företag i större omfattning ställer högre krav på säkerhet och de genomför själva penetrationsattacker för att säkerställa säkerheten. Enligt informanten ställer mindre kunder lägre krav på grund av möjlig okunskap.

4.2.4 Tillgänglighet

I tabell 4.5 presenteras informanternas svar på fråga Q12-Q15 i intervjuguiden, se appendix 7.2.

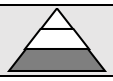
Tabell 4.5 Empirisk sammanställning tillgänglighet

Företag	**Sammanfattning** 
Xledger	Informanten betonar vikten av att tjänsten inte enbart ska vara tillgänglig utan det skall finnas kontroll på svarstid parallellt med utbyggnad av serverparker. I förebyggande arbete gentemot tillgänglighet använde de backup genom dubbla servermiljöer, kontinuerlig loggning av data samt använder tre oberoende internetleverantörer. Vidare menar informanten att det inte fullständigt går att säkerhetsställa tillgänglighet av tjänsten: "*Vi ligger på över ungefär 99,90% någonting. Men vi ger inga garantier utan om det står stilla så står det stilla för alla kunder*" (Transskript Xledger, Appendix 7.4, Q12).
Telekomföretaget	Informanten tar upp vikten av att förmedla en god internetuppkoppling och länk till molntjänsten där den inte är för belastad. Informanten betonar vikten av att använda två olika internetleverantörer samt ett välstrukturerat SLA. Informanten betonar också vikten att utvärdera varje tjänst och vad det får för konsekvenser om tillgängligheten brister. Det bör även finnas en manual som beskriver hur molntjänstleverantören skall agera i en sådan situation.
Integrationsföretaget	Informanten nämner att de har väldigt hög tillgänglighet, uppemot 100 % upptid och att det är viktigt vid hantering av affärsdata. För att uppfylla detta så är det viktigt att använda redundanta system och failoverlösningar vilket sker genom att spegla två servrar som placeras i två serverhallar som är geografisk avskilda. Alternativt i en serverhall med två rum som är brandsäkrade från varandra, samt har olika typer av strömförsörjning från olika leverantörer.
Knowit Cloud Innovation	De säkerhetsriskerna företaget nämner kring tillgänglighet inom molntjänster är först och främst felaktig arkitektur. Vidare erbjuder företaget kunder en tillgänglighet på 99.8% och för att uppfylla detta har man konstruerat en väl genomtänkt molnarkitektur med inbyggd redundans.
Systemutvecklingsföretaget	Informanten nämner att de inte ser tillgänglighet av hög prioritet då tjänsten är delvis gratis samt inte lagrar kritisk information. Vidare svarar informanten att tjänsten inte använder dubbla servermiljöer utan istället dagliga backups samt SLA med serverleverantör.
Affärssystemsleverantören	Informanten nämner att molntjänstleverantörer allt för ofta överdimensionerar de förebyggande åtgärder som implementeras för att göra system tillförlitliga. Detta skapar väldigt avancerade säkerhetssystem vilket blir kontraproduktivt och kan skada tillgängligheten. Inom sina egna avdelningar används dubbla servermiljöer vilket är lokaliserade i olika datorhallar med flera ström- och internetleverantörer.

4.2.5 Sekretess

I tabell 4.6 presenteras informanternas svar på fråga Q16-Q19 i intervjuguiden, se appendix 7.2.

Tabell 4.6 Empirisk sammanställning sekretess

Företag	**Sammanfattning** 
Xledger	Informanten svarar: "*Jag ser inga säkerhetsbrister i vår lösning*" (Transskript Xledger, Appendix 7.4, Q16). Vidare betonar informanten en bristande kunskap hos kunden vid kravställning på tjänsten. Kunden uppvisar dock krav att obehöriga inte ska få åtkomst till deras data. Informanten menar istället att det inte finns någon möjlighet att komma åt andra användares data. Informanten nämner även att Xledger bemyndigar kunden med rollen att underhålla interna restriktioner av användarkonton.
Telekomföretaget	Informanten nämner att Telekomföretaget använder flera säkerhetsfunktioner för att uppfylla olika nivåer av sekretess vilket baseras på kundavtal. Några av funktionerna är användning av separata servar, brandväggar, specifika nycklar, restriktioner och säkerhetsgrupper. Informanten menar på att funktionerna används för att förebygga läckage och obehörig åtkomst till kundens data. Ytterligare menar informanten att Telekomföretaget befogar över IT-personal och admins som har åtkomst till kritisk data och utför interna tester för att kontrollera att sekretessen är uppnådd.
Integrationsföretaget	Informanten nämner vikten av att säkerställa sekretess inom molntjänster. Att rätt personer har tillgång till data och loggar är en viktig faktor samt vikten av att komprimera och kryptera data för att förhindra att data hamnar i fel händer. För att uppfylla sekretess används bland annat RSA-kryptering. Vidare är kundernas krav på sekretess fallspecifika utifrån vilken typ av data som sparas.
Knowit Cloud Innovation	Enligt informanterna kan sekretess säkerhetsställas genom kryptering av data och säker inloggning inom molninfrastruktur och på plattformsnivå. Informanterna menar vidare att sekretess på applikationsnivå inte är specifikt för molnet utan för den applikationen som hanterar och har åtkomst till informationen. Informanterna menar vidare att de krav som företaget ställer på kunden är kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.
Systemutvecklingsföretaget	Informanten menar att data lagras i samma databas och tabeller är en riskfaktor inom sekretess. Vidare menar informanten att vid logiskt fel finns det risk för att obehöriga användare får åtkomst till kritisk data. Säkerhetsställning av sekretess administreras enligt informanten på en logisk nivå genom ett antal säkerhetsnivåer. Informanten menar vidare att kunden inte ställer några krav vilket grundar sig i kundens begränsade kunskap.

Affärssystemsleverantören	Informanten menar att säkerhetsställning av sekretess utförs genom användning av en unik databas på servernivå. Databasen är helt isolerad och inte ens företagets egna supporttekniker får åtkomst till data utan att bli godkänd i en säkerhetsprocess. Informanten menar att detta är av största vikt då bokföringsdata med hög sekretess behandlas och att detta vid läckage kan ha en negativ effekt på kunderna.

4.2.6 Integritet

I tabell 4.7 presenteras informanternas svar på fråga Q20-Q24 i intervjuguiden, se appendix 7.2.

Tabell 4.7 Empirisk sammanställning integritet

Företag	**Sammanfattning**
Xledger	Informanten säger: "Man kommer inte åt något annat än det man ska komma åt" (Transskript Xledger, Appendix 7.4, Q20). Informanten menar att kunderna inte ställer några krav på integritet utan tar det som en självklarhet. Vidare förklarar informanten att om kunden väljer att avsluta tjänsten så avslutas inte kontot förrän all data hämtats ned och registrerats. Slutligen förmedlas ett skriftligt kvitto på datatransaktionen till kunden.
Telekomföretaget	Informanten nämner att krypteringsgraden inte har någon inverkan om datorn/servern finns tillgänglig för obehöriga. Vidare betonar informanten att användarens val av molntjänst är en viktig faktor inom säkerhet i molnet. Informanten nämner att det finns avtal för hur känslig information ska hanteras vilket motverkar att dataläckage. Vid avslut av tjänst tas data bort från molntjänstleverantören. Informanten menar att det används funktioner, checksums, för att säkerhetsställa integritet inom företaget.
Integrationsföretaget	Informanten belyser problematiken med att data flyttas mellan olika servrar samt mellan kunder och leverantörer och hur detta påverkar integriteten. Vidare så är kundernas krav på integritet fallspecifikt.
Knowit Cloud Innovation	Informanterna nämner att felaktig eller obefintlig backuplösning är det främsta problemet vid integritet. Kravet från kunderna är i sin tur backups vilket också ingår som standard i företagets lösningar. Det sker även regelbunden kontroll av rutiner för lagring och backup, samt att molntjänstleverantören utför regelbundna tester tillsammans med kunderna för att säkerhetsställa integritet. Om en kund väljer att avsluta tjänsten tas data bort om inte kunden vill att den ska lagras i ytterligare en period.

Systemutvecklingsföretaget	Informanten menar att riskerna i integritet är kopplade till riskerna i sekretess. Det inbegriper rätten att tillgå och editering av data. Risker som informanten ser är XSS, Cross site scripting, och SQL-injections vilka är svåra att upptäcka i tid. Informanten nämner även att för säkerhetsställa integritet används backups, behandlingsystem och ändringsloggar. Informanten menar att vid avslutning av tjänst raderas inte data men att rättigheterna ändras genom att användarkonton kopplas bort från servern.
Affärssystemsleverantören	Informanten menar vid användning av omfattande behandlingshistorik säkerhetsställs integritet. Det visas vilken användare som har fått åtkomst och vad som har editerats vilket ligget till grund för en analys om det var berättigat. När en kund avslutar tjänsten sparas data i två månader och raderas om kunden inte efterfrågar annat.

4.2.7 Kundrelaterade frågor

I tabell 4.8 presenteras informanternas svar på fråga Q25-Q28 i intervjuguiden, se appendix 7.2.

Tabell 4.8 Empirisk sammanställning kundrelaterade frågor

Företag	Sammanfattning
Xledger	Informanten förklarar att kundens insikt i Xledgers förebyggande arbete varierar. Vissa större kunder har stor insikt i det förebyggande arbete medan andra kunder enbart ställer grundläggande frågor. Informanten förklarar vidare att han inte ser någon problematik om kunder vill migrera till eller från en annan leverantör då de har stöd för grundbehovet som är export av data.
Telekomföretaget	Informanten nämner att kunden inte har någon insikt i företagets förebyggande säkerhetsarbete. Samt att det är viktigt att specificera säkerhetsmässiga krav i avtal för att uppnå önskad säkerhet. Informanten menar att det kan vara enkelt att flytta från en molntjänst till en annan om det bara är en server som används och om det är företaget själva som står för driften. Men sen betonar informanten att det kan bli väldigt komplext och kostsamt att flytta från vissa molntjänster då varje molntjänst har unika tjänster som utmärker sig från konkurrenterna
Integrationsföretaget	Integrationsföretagets kunder har begränsad eller ingen insikt i deras förebyggande säkerhetsarbete, men det är tydligt specificerat i avtalet vilka krav som ska uppfyllas. Informanten nämner vidare att om kunden vill byta leverantör kan detta vara *"[...]väldigt smärtfritt då vi står för själva kommunikationen till och från molntjänsten"* (Integrationsföretaget Transskript, Appendix 7.6, s 6).
Knowit Cloud Innovation	Informanterna berättar att de erbjuder full transparens i sitt säkerhetsarbete gentemot sina kunder. Vidare så ser de ingen problematik vid migrering mellan olika leverantörer, de har till exempel hjälpt en kund med att flytta mellan Microsoft Azure och Amazon AWS.

Systemutvecklingsföretaget	Informanten menar att beroende på kund, bransch och system ställs det olika krav på säkerhet vilket ligger i linje med kundens insikt i företaget. I den tjänst som informanten levererar, lagras ingen känslig data vilket enligt informanten inte bidrar till konsekvenser av en större omfattning vid angrepp.
Affärssystemsleverantören	Informanten nämner att kundernas insyn i deras förebyggande arbete skiftar från kund till kund. Stora kunderna genomför i vissa fall egna penetreringstester gentemot mindre kunder som enbart ställer sporadiska säkerhetsfrågor. Slutligen ser inte företaget några större problem när kunden byter leverantör då deras tjänster inkluderar funktioner som gör det enkelt för kunderna att flytta data från konkurrenters system till deras utan speciellt stort behov av resurser.

4.2.8 Förebyggande arbete

I tabell 4.9 presenteras informanternas svar på fråga Q2-Q7 i intervjuguiden, se appendix 7.2.

Tabell 4.9 Empirisk sammanställning förebyggande arbete

Företag	Sammanfattning
Xledger	I frågorna angående förebyggande arbete ställs frågan hur företaget ställer sig till förebyggande säkerhetsarbete. Informanten nämner att Xledger utför monumentala säkerhetsanalyser och ständig revidering av tjänsten där kryptering, skalskydd och inloggningsmoment prioriteras. Kontinuerliga tester utförs framförallt vid uppdatering av programvara med fokus på säkerhet och funktion. Vidare existerar en processplan vid allvarliga säkerhetsbrister.
Telekomföretaget	Informanten nämner att de har en intern grupp som utför penetreringstester vilket främst sker vid lansering av tjänst. Vidare utför Telekomföretaget regelbunden patchning av tjänster vid olika former av säkerhetsuppdateringar som till exempel javauppdateringar. Telekomöretaget har även börjat utföra Google-tester där ett scenario utspelas och åtgärdsrutiner testas. Vidare existerar även en processplan att följa vid säkerhetsbrister.
Integrationsföretaget	Informanten redogör för vikten av att designa lösningar med säkerhetstänkt samt att titta på säkerhetscertifieringar. Informanten betonar att kunden inte bör lagra all kritisk data om möjligt för att minimera riskerna. För att ytterligare motverka säkerhetsrisker nämner informanten att molntjänstleverantören har en ”[...]B2B-gateway utanför sitt nätverk som får agera proxy mot molntjänster.” (Integrationsföretaget Transskript, Appendix 7.6, Q2). Angående säkerhetsanalyser och tester nämner informanten att det finns brister men att företaget löpande arbetar med att se till att produkter är riktigt uppdaterade och funktionella. Angående avsatta resurser för förebyggande arbete så nämner han att det saknas, men att applikationerna i grunden är utvecklade med ett säkerhetstänk.

Knowit Cloud Innovation	Säkerhetsanalyser utförs främst vid lansering av tjänst men även löpande vid större förändringar. Företaget utför även penetrationstester och lasttester för att identifiera säkerhetsbrister. Om en säkerhetsbrist identifieras existerar det en processplan att följa.
Systemutvecklingsföretaget	Informanten menar att Systemutvecklingsföretaget fokuserar på upprätthållning av rättighetsnivåer för att bättre klassificera information samt klargöra behörighetsnivåer. Informanten betonar vidare att strikta behörighetsprinciper och regelverk motverkar misstag från en användare med begränsad IT-erfarenhet. "Han kan inte och får inte tillgång till att göra fel" (Transskript Systemutvecklingsföretaget, Appendix 7.8, s 6). Vidare menar informanten att som skydd mot den mänskliga faktorn använder företaget sig av övervakning för att se vem som gjort vad inom systemet samt dagliga backups.
Affärssystemsleverantören	Informanten nämner att företaget utför ett omfattande förebyggande arbete som bland annat omfattande penetrationstestning av externa parter. Informanten berättar även att Affärssystemsleverantören utför en stor säkerhetsanalys varje år samt mindre modulspecifika analyser för att motverka säkerhetsbrister. På en teknisk nivå menar informanten att de lägger stor vikt på uppdatering av applikationer för att minimera risken för säkerhetshål.

5 Analys och diskussion

För att analysera resultatet från teorin och empirin utgår vi från det tidigare presenterade teoretiska ramverket som mall. Först analyseras varje riskområde enskilt för att sedan avslutas med en sammanfattning där kritiska riskområden i ramverket identifieras och analyseras. Dessa två steg svarar på vår forskningsfråga vilken är:

Hur ställer sig leverantörer avseende riskhantering inom molntjänster?

I inledningen av samtliga delkapitel presenteras en sammanfattning av empirisk data i tabellform som används som stöd i diskussionen.

5.1 Juridiska risker

Tabell 5.1 Jämförelse av empiri angående juridiska aspekter

	Xledger	**Telekom-företaget**	**Integrations-företaget**	**Knowit Cloud Innovation**	**System-utvecklings-företaget**	**Affärs-systems-leverantören**
Server-lokalisering	Internationellt	Internationellt	Internationellt	Internationellt	Nationellt	Nationellt
Före-byggande	Inget behov	Avsätta resurser Tydliga SLAs	Avsätta resurser	Spara data inom EU	-	Avsätta resurser Spara data nationellt

Géczy et al (2012) menar att molntjänsternas dynamiska lagring av data oberoende av geografisk plats har identifierats som den främsta juridiska riskfaktorn. Vidare betonar Géczy et al (2012) vikten av de juridiska riskerna som uppkommer med molntjänsternas obundna

infrastruktur, vilket är i linje med uppsatsens empiriska data då flera av våra informanter identifierar detta som en säkerhetsrisk. Vi har dock identifierat att typen av data som sparas avgör en mängd resurser som avsätts för att förebygga denna risk. Affärssystemsleverantören nämner att de medvetet valt att lokalisera sina servrar nationellt för att undvika juridiska komplikationer kopplade till bokföringslagen (Transskript Affärssystemsleverantören, 7.9). Systemutvecklingsföretaget menar istället att tjänsten de erbjuder inte innehåller någon data som går under någon specifik lagstiftning och att de därför avsatt resurser för förebygga relaterad problematik. Vidare berättar Knowit Cloud Innovation att de sparar sin data inom EU, vilket är i linje med EU Opinion (2012) angående hur personuppgifter och liknande data får överföras mellan medlemskapsländer.

Sammanfattat stödjer majoriteten av respondenterna Géczy et als (2012) syn på vikten av de juridiska säkerhetsriskerna, bland annat säger informanten på Integrationsföretaget: *"[…]absolut största processen för oss då det handlar om cloud är den juridiska processen"* (Transskript Integrationsföretaget, Appendix 7.6, Q10)

Vi har insett att juridiska risker är ett viktigt område som kan få konsekvenser för molntjänstleverantören. Vår uppfattning är att företag överlag investerar stora resurser på att förebygga problematik inom det juridiska riskområdet, vilket kan bero på risken med finansiella skador samt påverkan på ett företags varumärke vid lagbrott. Vi har även insett att EUs relativt tillmötesgående lagstiftning underlättar molntjänstleverantörernas förebyggande arbete men att problematiken troligen är större inom andra globala regioner.

5.2 Organisatoriska risker samt risker relaterade till policys och SLA

Tabell 5.2 Jämförelse av empiri angående organisatoriska risker samt policy och SLA

	Xledger	**Telekom-företagetet**	**Integrations-företaget**	**Knowit Cloud Innovation**	**System-utvecklings-företaget**	**Affärs-systems-leverantören**
Företagets krav	Avsatta resurser vid implementerings process	-	-	Kvalificerad personal Säker hantering av tillträde till lokaler, information, miljöer och inloggnings-uppgifter.	-	Modern webbläsare
Kundens krav	Kunderna har begränsat förhandlings-utrymme	-	Säkerhet, tillgänglighet, uppe och ner tid, trueput	Kvalificerad personal Säker hantering av: Tillträde till lokaler, information & inloggnings-uppgifter	-	Skiftande, höga till minimala
Avtalstyp	Standardiserade	Standardisera de	SLA baserat på kundbehov	Standardisera de avtal	Standardisera t förvaltnings-åtagande	Standardisera de & Kundspecifika avtal

Molntjänsters dynamiska infrastruktur ställer höga krav på både leverantören och kunder gällande organisatoriska risker såsom bristande ansvarsfördelning, kontroll och övervakning (Baker et al, 2008). Buyya och Yeo (2008) menar att en väl fungerande kommunikation mellan parter är essentiell för att effektivt konsumera molntjänster. En central faktor för att förebygga organisatoriska risker är väl upprättade SLA's mellan kunden och leverantören, men även leverantören och eventuell tredje part (Buyya & Yeo, 2008). Detta är i linje med vad majoriteten av informanterna visar, de använder sig av väl standardiserade avtal med sina kunder eller avtal som är baserade på en standard men anpassade för att passa kundens behov. Integrationsföretaget har ett standardavtal som kan anpassas till exempel vid behov av support (Transskript Integrationsföretaget, Appendix 7.6). Dock finns det undantag, Affärssystemsleverantören nämner att de har stora kunder som till exempel redovisningsföretag och att man därför använder sig av skräddarsydda avtal för att uppfylla kundens specifika behov.

Gällande kraven i avtalen visar informanterna en skiftande syn på vilka som är de viktigaste faktorerna. Ett fåtal informanter nämner att företaget kräver att kunden avsätter tekniskt kunnande personal vid implementering och drift för att förebygga säkerhetsbrister (Transskript Xledger, Appendix 7.4; Transskript Knowit Cloud Innovation, Appendix 7.7). Även kundernas krav på leverantörerna är spridda. Två informanter nämner att mindre kunder saknar teknisk kunskap för att ställa riskförebyggande krav på leverantören (Transskript Xledger, Appendix 7.4; Affärsystemsleverantören, Appendix 7.9). Motsatt visar flera informanter, som har större globala kunder, mer detaljerade krav gällande bland annat testning, tillgänglighet och personal. Informanten på Knowit Cloud Innovation beskriver kraven: "*Kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.*" (Transskript Knowit Cloud Innovation, Appendix 7.7, Q11a)

Vår syn på de organisatoriskt relaterade riskerna är att företag lägger stor vikt vid SLA, men att de även använder detta som en fallskärm vilket kan begränsa deras behov av ett förebyggande säkerhetsarbete. Vi anser att ett begränsat säkerhetsperspektiv påverkar andra riskområden negativt då molntjänstleverantören kan definiera SLA utefter en lägre säkerhetsstandard än vad som är att föredra. Vi anser även att företagen inte prioriterar kundens medverkan i det förebyggande arbetet, vår uppfattning är att kundens kunskap förbises och att detta kan vara en viktig resurs.

5.3 Tillgänglighet

Tabell 5.3 Jämförelse av empiri för tillgänglighet

	Xledger	Telekom-företaget	Integrations-företaget	Knowit Cloud Innovation	System-utvecklings-företaget	Affärs-systems-leverantören
Risker	-	Internet-leverans	Beroende till leverantör, Internet-leverans	Felaktig arkitektur Val av leverantör	-	Överdimensionerade säkerhets-system, Okunskap Felaktig användning av redundans-replikering
Upptid	99.9%	~100%	~100%	99.8%	99.47%	Mycket höga krav
Förebyggande	Dubbla servermiljöer, Tre internet-leverantörer	Två olika internet-leverantörer Åtgärdsplan	Dubbla servermiljöer Ström-försörjning från olika leverantörer Redundanta system Failover-lösningar Brandsäkrade	Genomtänkt moln-arkitektur med inbyggd redundans	Dubbla servermiljöer	Dubbla servermiljöer Flera internet-leverantörer Redundans-replikering

Litteraturen nämner tillgänglighet som både ett stort hinder och möjlighet för molntjänster. Bland annat Armbrust et al (2009), Marston et al (2011) samt Venters och Whitley (2012) nämner tillgänglighet som en kritisk faktor för molntjänsters fortsatta tillväxt, även om nuvarande leverantörer kan påvisa en väldigt hög standard. I vår empiriska studie betonar informanterna att känslighetsnivån på data som lagras har en direkt påverkan för kravsättningen

på tillgänglighet. Till exempel medför affärskritisk data inom bokföringssystem högre krav på upptid.

Detta medför till att våra informanter har en skiftande syn på tillgänglighet, majoriteten påvisar en upptid på över 99 %, men vissa har en mindre kritisk syn till problemet och säger bland annat att: "*Hade det legat nere en dag så hade det inte varit the end of the world eftersom att det är gratis*." (Transskript Systemutvecklingsföretaget, Appendix 7.8, Q13).

Även Affärssystemsleverantören har en annorlunda syn på tillgänglighet:

> "*Jag upplever i alla fall att man ofta överdimensionerar dom failsafes som skall finnas på plats för att skydda tjänsten. För mycket säkerhet och redundans kan ibland vara kontraproduktivt och leda till att det faktiskt blir problem istället för att sådana avancerade system bara för att hålla det uppe då.*" (Transskript Affärssystemsleverantör, Appendix 7.9 Q12).

Armbrust et al (2009) nämner att stabiliteten i nätverk och datatillgänglighet är en stor begränsning i molntjänsters expansion. För att säkerställa detta påvisar majoriteten av våra informanter att de använder sig av dubbla servermiljöer, där data speglas i realtid och detta kan på så sätt säkerställa drift även vid förlust av tillgänglighet till en server. Dessa redundanta servermiljöer har även flertalet olika leverantörer av ström samt internetuppkoppling för att ytterligare säkerställa drift.

Kravet på låga svarstider är också en avgörande faktor då flera av informanterna levererar verksamhetskritiska system. Armbrust et al (2009) nämner vikten av låga svarstider även under tider då kraven på datorkraft är högre. För att säkerställa detta berättar bland annat Lars Lobelius på Xledger att de bara utför releaser på natten mellan lördag och söndag då kravet på datorkraft är lågt.

Vi anser att leverantörer lägger hög prioritet på tillgänglighet för sina applikationer. Uppvisandet av dåligt resultat kan få direkta och tydliga konsekvenser på molntjänstens drift. Vidare är det även enkelt att belysa och påvisa resultat vid förebyggande arbete vilket senare kan användas som ett säljargument.

5.4 Sekretess

Tabell 5.4 Jämförelse av empiri för sekretess

	Xledger	Telekom-företaget	Integrations-företaget	Knowit Cloud Innovation	System-utvecklings-företaget	Affärs-systems-leverantören
Risker	-	Vissa projekt får inte se varandras data Dataläckage mellan projekt	Vem som har access till loggar Intrång Borttappade säkerhets-nycklar	Vem som kan komma åt den Autentisering sbrist	Felaktig separering av data	-
Förebyggande	Rättighets sättning	Separata servrar Säkerhets-grupper Firewall Intern testning Specifika nycklar	Certifierad komprimering Dekryptering av data Standarder som RSA	Kryptering av data Säker Inloggnings-applikation Kvalificerad personal Säker hantering av: Tillträde till lokaler, information & inloggnings-uppgifter	Ren logisk nivå Säkerhets-lager i applikationen	Låsta datahallar Lösenords-skyddade system Rättighetsbaser ade system Kund har en egen unik databas
Kundens krav	-	Kontrakt Säkerhetsbe dömning	Fallspecifika avtal Specifik integration	Kryptering av data Säker inloggning.	-	Väldigt höga krav Bokföringsdata Data ska vara hemlig

Zissis och Lekkas (2010) menar att fördelarna vid övergång till molntjänst och en förenklad dataadministration även skapar problematik inom sekretess och integritet. En stor

säkerhetsriskrisk är att misslyckas att segregera data mellan användare (Puttaswamy et al, 2011). I det empiriska resultatet identifierar flertalet informanter segregering av data som en säkerhetsrisk. Empiriska resultatet varierar angående sekretess och tillhörande säkerhetsrisker inom molntjänster. Det som skiljer empirin från litteraturen är problematiken vid begränsningen av molntjänstleverantörens åtkomst av data. Affärsystemsleverantören betonar problematiken att vid åtkomst till data, felsökning av data och tillgång till historiska loggar saknas det begränsning angående antal anställda och avdelningar som har behörighet:

> *"Men som jag nämnde tidigare så är det svårt att hitta en balans med vem som ska ha tillgång till vad och vem behöver tillgång till vad i vardagen för att det ska fungera i förhållande till sekretess och integritet"* (Transskript Affärssystemsleverntören, Appendix 7.9, Q19a)

Informanten på Systemutvecklingsföretaget berättar vidare att det finns underliggande säkerhetsrisker gällande klassificering av känslig information och hur detta påverkar sekretessen: *"Hur kan man veta om informationen är känslig eller inte."* (Transskript Systemutvecklingsföretaget, Appendix 7.8, Q1).

Sahito och Slany (2013) betonar behovet av säkerhet i den dynamiska infrastrukturen inom molnet samt att framställning av standardiserade motåtgärder. Användarnas sekretess säkerhetsställs främst genom datakryptering och användning av krypteringsalgoritmer och nyckelsäkerhet (Sahito & Slany, 2013). Sahito och Slany (2013) menar vidare att det ställer krav på administration av autentisering, åtkomst, brandväggar, kryptering i syfte att förebygga dataläckage. Det empiriska resultatet som hänvisar till det förebyggande arbete varierar inom molntjänster. Informanterna menar på att upprätthållning av sekretess uppnås genom strikt reglering av åtkomst till data. Det empiriska resultatet visar att förebyggande arbete bedrivs dels på en fysisk nivå genom låsta datahallar, separata serverar, kompetent personal och strikt reglering av tillträde till lokaler. Samt på en digital nivå med certifierad kryptering av data, rättighetsreglering, användning av autentiseringsapplikationer och behandlingsloggar.

De säkerhetsmässiga krav som ställs på leverantören av kund är kundspecifika enligt avtal och typen av data. Enligt Affärssystemsleverantören (Transskript Affärssystemsleverantören, Appendix 7.9) medför deras bokföringssystem höga krav på grund av kritiskt data. Systemutvecklingsföretaget menar istället att deras system inte innehåller affärskritisk data vilket sänker kundens krav på sekretess. Vidare menar informanten från Xledger, Systemutvecklingsföretaget och Affärssystemsleverantören att kunden saknar kunskap inom området vilket påverkar de säkerhetsmässiga krav som kunden ställer på dem som molntjänstleverantörer.

Vi anser att sekretess är ett område som företag ser som svårdefinierat då företagen har olika förhållningsregler både inom företagen och inom olika projekt. På grund av detta är vår uppfattning att en branschstandard för sekretess är essentiell för ett förebyggande arbete. Denna standard borde innehålla delområden som till exempel hanterar kryptering, autentisering, databasisolering, fysisk skydd av datorhallar och personalcertifiering.

5.5 Integritet

Tabell 5.5 Jämförelse av empiri för integritet

	Xledger	**Telekom-företaget**	**Integrations-företaget**	**Knowit Cloud Innovation**	**System-utvecklings-företaget**	**Affärs-systems-leverantören**
Risker	-	Fysisk kontroll av server	Data försvinner Att data inte är i dina lokaler	Felaktig eller obefintlig Backup-lösning	Åtkomst XSS Cross site SQL-injections	Manipulation
Förebyggande	Kunden själv underhåller sin lösning	Fil-lagrings program Checksums Åtkomst-kontroll	Gör det svårt att spåra	Backup Regelbundna tester	Backup Behandlings-system Loggar	Behandlings-loggar Unik databas
Vid avslut av tjänst, vad händer med data?	När kund har fått utkvitterat data och den är säkert inläst, då raderas data.	Raderas	-	Raderas, om inte kunden vill att det ska sparas en period	Data ligger kvar, Kopplar bort konton vilket tar bort tillgången till data.	Lagrar data i två månader sen raderas den

Subashini och Kavitha (2011) menar att av alla riskområden är dataintegritet ett av de mest kritiska och är därför viktigt att upprätthålla. Med ett isolerat system uppnås integritet relativt enkelt men vid användning av molntjänster ökas komplexiteten då flera databaser och

applikationer är sammankopplade. För att bibehålla integritet krävs det att transaktioner utförs på ett korrekt och säkert sätt (Subashini & Kavitha, 2011). Det empiriska resultatet påvisar en medvetenhet hos informanterna vilket ligger i linje med teorin. Flertalet informanter hänvisar till användning av isolerade databaser för lagring av kundernas data vilket minimerar risken för obehörig åtkomst. Affärssystemsleverantören berättar: *"[...] varje kund har en egen unik databas. Vi delar inte kundens data i samma databas utan alla har en isolerad databas på liksom servernivå [...]"* (Transskript Affärssystemsleverantören, Appendix 7.9, Q17).

Det finns undantag där informanten på systemutvecklingsföretaget säger: *"I vårt system ligger alla data i samma databas och samma tabeller."* (Transskript Systemutvecklingsföretaget, Appendix 7.8, Q17) och vidare berättar informanten att:

> *"Om kunden skulle kunna få tillgång till en annan kunds data så är ju det inte bra. För kunden har ju i viss mån rättigheter till att editera data i ett visst ärende."* (Transskript Systemutvecklingsföretaget, Appendix 7.8, Q20).

Chen och Zhao (2012) menar att det finns ett behov av behörighetskontroll vid åtkomst och modifiering av data vilket även påvisas i empirin. Informanten från Telekomföretaget menar att behörighetskontroll utförs på interna och externa användare (Transskript Telekomföretaget, Appendix 7.5).

Affärssystemsleverantören nämner problematik avseende dataintegritet till exempel när kundens data laddas ned för en buggfix. Affärssleverantören menar vidare att det är en sekretessfråga som ligger i linje med integritetsproblematiken (Transskript Affärsystemsleverantören, Appendix 7.9).

Subashini och Kavitha (2011) menar att för säkerhetsställning av integritet krävs förebyggande åtgärder genom att vid transaktioner använda sig av standarder som till exempel ACID. Empirin påvisar meningsskiljaktigheter inom de förebyggande åtgärderna vid säkerhetställning av integritet. Knowit Cloud Innovation och Systemutvecklingsföretaget hävdar att backups är den främsta förebyggande åtgärden. Telekomföretaget hävdar att data ska vara svårt att spåra i syfte att uppnå en hög integritet. Affärssystemsleverantören menar istället att molntjänstleverantörer skall använda sig av system som underlättar att spåra data och vem som har ändrat. Wang et al (2010) betonar att det finns tekniker för att säkerhetsställa integritet då data lagras på ett korrekt sätt. Dock finns det brister i dessa tekniker för att de är utformade för att klara av en miljö med en isolerad server och inte tar hänsyn till den dynamiska molntjänstmiljön (Wang et al, 2010).

Chen och Zhao (2012) tar upp problematiken med att leverantörer behåller data från kunder när en tjänst avslutas och att det i sin tur är en säkerhetsrisk om det skulle läcka ut. Majoriteten av informanterna hävdar att data tas bort direkt vid avslutande av tjänst. Men att kunderna har möjlighet att spara data under en period för att säkerställa en fullständig export av data.

Informanten från Systemutvecklingsföretaget nämner att data ligger kvar och att man istället begränsar istället behörigheten. (Transskript Systemutvecklingsföretaget, Appendix 7.8).

Vi anser att integritet inom molntjänster är svårt att säkerställa. Detta kan bero på att säkerhetsbrister medvetet eller omedvetet kan vara dolda under längre perioder, vilket kan få konsekvenser i framtiden.

5.6 Jämförande diskussion relaterat till RIM

I tabell 5.6 Empiriska relationer i förhållande till RIM presenteras identifierade relationer mellan riskområden. Tabellen används som underlag för att styrka diskussionen nedan. Punkter med streck påvisar att informanter nämnt dessa riskområden i relation till varandra.

Tabell 5.6 Empiriska relationer i förhållande till RIM

	Xledger	Telekomföretaget	Integrationsföretaget	Knowit Cloud Innovation	Systemutvecklingsföretaget	Affärssystemsleverantören
Juridiska risker			●			● ●
Organisatoriska risker, Policy & SLA	●	●	●	● ●	●	
Tillgänglighet				●	●	
Sekretess	●	●	●	●	●	●
Integritet		●	●	● ●	●	● ● ●

Dupré et al (2012) kategoriserar risker relaterade till molntjänster i tre områden: tekniska, juridiska samt policy och organisatoriska risker. Vidare menar Wang et al. (2010) att de huvudsakliga säkerhetskraven för att skydda data inom molntjänster är sekretess, integritet och tillgänglighet. Bland annat dessa två källor användes som grund för framtagandet av ramverket RIM, Riskområden I Molnet. Dock visar empirin på en sammanhängande problemkontext där gränserna mellan riskområdena är mjuka. Vi kan se samband då informanterna i vissa fall har svårt att separera de olika delområdena och det påvisar även att relationen mellan dem är tydliga. Ett exempel är separationen mellan sekretess och integritet där identifiering av risker och förebyggande arbete går hand i hand. Informanten på Affärssystemföretaget (Transkribering

Affärssystemsföretaget, Appendix 7.9) belyser bland annat problematiken vid intern likväl extern åtkomst till den lagrade data vid sambandet av sekretess och integritet. Vidare menar Telekomföretaget att om dataintegriteten blivit äventyrad har även sekretessen brustit (Transkribering Telekomföretaget, Appendix 7.5).

Patel et al (2009) betonar att SLA framträder som en nyckelaspekt vid övergång till molntjänster från traditionell datalagring. Informanten på telekomföretaget (Transkribering Telekomföretaget, Appendix 7.9) betonar att det är vid förhandling av avtal som molntjänstleverantören och kunden bestämmer nivån på sekretess och integritet men även involverar den juridiska aspekten. *"[...]absolut största processen för oss då det handlar om cloud är den juridiska processen"* (Transskript Integrationsföretaget, Appendix 7.6 Q10).

Detta påvisar vikten av ett helhetsperspektiv vid betraktelse av säkerhetsrisker inom molnet. Informanten på telekomföretaget förklarar relationen i följande citat:

> "*Vi har advokater som säkerhetsställer vad som får göras och inte. Speciellt är det kontrakten som är man är mest rädd för att brytas [...] En variant är SLA kontrakt och andra, vem vi får dela information med och inte. Ofta skriver man kontrakten på att vissa ställen få ha den här datan och även vissa molntjänster är tillräckligt säkra för att ha datan också.* " (Transskript Telekomföretaget, appendix 7.5 Q.10)

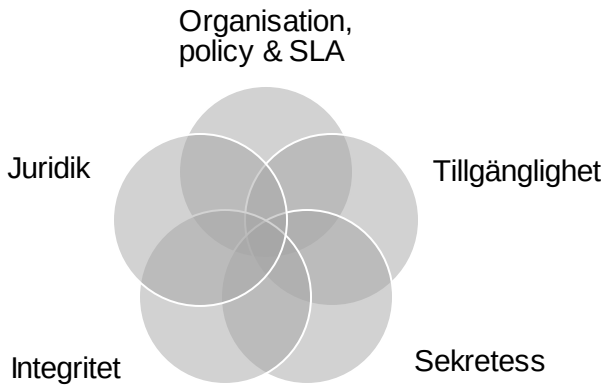
6 Slutsats

Nedan presenteras de sammanfattade slutsatserna i vår studie i kontext av forskningsfrågan. Kapitlet går igenom det teoretiska och empiriska bidraget samt undersökningens begränsningar och vidare forskning.

6.1 Vårt Teoretiska bidrag

Tidigare forskning av risker inom molntjänster har visat på en tydlig indelning av riskområden vilket även visas i vårt teoretiska ramverk, Risker Inom Molntjänster. Utefter vår empiriska undersökning har vi fått en annan syn på problematiken då vi inte ser en tydlig avgränsning mellan riskområdena. Vi anser att ett enhetligt säkerhetsperspektiv som omfattar samtliga säkerhetsrisker är essentiellt för ett lyckat förebyggande säkerhetsarbete. Vår empiri visar inte på en hierarkisk ordning av riskområden vilket enligt vår studie motsäger tidigare forskning. Vidare bör säkerhetsriskerna därför jämställas och inte enskilt prioriteras.

Vi har därför reviderat vårt teoretiska ramverk, RIM, där förhållanden mellan riskområdena har stärkts vilket gör att avgränsningarna inte är lika tydliga.



Figur 6.1 Risker Inom Molntjänster, RIM, Version 2

Det reviderade ramverket påvisar även en avsaknad av en hierarkisk ordning mellan riskområden. Slutsatsen är att det är viktigt att jämställa säkerhetsriskerna för att uppnå en hög säkerhetsstandard inom molntjänster.

Empirin betonar, i linje med teorin, att en avsaknad av standarder inom molntjänster hämmar utveckling av förebyggande säkerhetsarbete. En standardisering av säkerhet inom molntjänster som jämställer och inkluderar alla faktorer kan skapa en grund för hög säkerhet inom den snabbt expanderande molntjänstbranschen.

Vidare har vårt resultat identifierat att den mänskliga faktorn har en direkt påverkan på de fem riskområdena. Avsaknaden av den mänskliga faktorn i teoretiska bidraget påvisar att empirin och teorin inte stämmer överens. Vilket gör att teorin bortser från en kritisk faktor vid analys av det säkerhetstänk som bör ligga till grund vid molntjänst hantering. Vår slutsats är att den mänskliga faktorn bör beaktas och vidare studeras för att uppnå en starkare reliabilitet i aktuell forskning.

6.2 Vårt Empiriska bidrag

Resultatet från den empiriska undersökningen visar på att molntjänstleverantörerna är medvetna angående säkerhetsrisker inom molntjänster samt att de visar en vilja att förebygga dessa risker.

En slutsats är att empirin påvisar medvetenhet om säkerhetsrisker och dess relationer som påvisas med vårt teoretiska ramverk, RIM.

Vidare har vår empiriska undersökning påvisat att avsaknaden av standardavtal och policyer har skapat en bransch med skiftande säkerhetsstandarder mellan leverantörer. Vår empiri visar att beroende på typ av applikation, storlek på kund och känsligheten av data påverkar leverantörens resursavsättning vid säkerhetsarbete. Vår slutsats är att det finns en skiftande kravställning på molntjänstleverantören vilket påverkar möjligheter och kraven för standardiserat säkerhetsarbete.

Resultatet från den empiriska undersökningen visar på vikten av den mänskliga faktorn som utlämnats i tidigare forskning. En slutsats är att molntjänstleverantören är väl medvetna om risken i samband med den mänskliga faktorn och har aktivt implementerat säkerhetsåtgärder för att förebygga dessa.

Avslutningsvis visar studien att molntjänstleverantörerna inte nödvändigtvis anser att molntjänster överträffar säkerhetsstandard i traditionella system.

6.3 Undersökningens begränsningar och förslag till vidare forskning

Vi reserverar oss för att storleken på uppsatsens studie bidrar till en generaliserad presentation av verklighetens riskområde. Där det begränsade antalet informationskällor bidrar till en generaliserad slutsats och med en mer omfattande forskning så är det möjligt att resultatet kan skifta samt att tydligare riktlinjer kan utformas gentemot säkerhetsrisker inom molnet.

Vi reserverar oss för att undersökningen fokuserar på molntjänstleverantörernas perspektiv angående säkerhetsrisker inom molnet. Det empiriska resultatet visar på en bristande kunskap hos kunden vilket är en ensidig slutsats. En vidare studie inom detta område hade bidragit till en kartläggning och analys av kundernas IT-kunskap i relation till säkerhetsrisker inom molnet.

Vidare tar undersökningen inte hänsyn till skillnader mellan storleken på de företag, som informanterna representerar, vilket vi anser kan vara en avgörande faktor till informanternas medvetenhet av säkerhetsrisker.

Undersökningen bortser från en djupare teknisk säkerhetsnivå. En teknisk undersökning på djupare nivå skulle möjliggöra en mer konkret jämförelse mellan företag och dess säkerhetstekniska åtgärder.

Gällande de juridiska riskerna är majoriteten av företagen i vår studie aktiva inom Europa och att en mer internationell studie kan genomföras för att säkerställa molntjänsters juridiska risker globalt.

7 Appendix

I kapitlet presenteras uppsatsens tillhörande bilagor som artikeldatabas, intervjuguide, transkribering av intervjuer samt referenslista.

7.1 Artikeldatabas

Titel	Författare	År	Journal	Sammanfattning
CLOUD COMPUTING: THE FUTURE OF IT INDUSTRY	Abualkibash M, Elleithy K	2012	International Journal of Distributed and Parallel Systems (IJDPS)	Positiv artikel till molntjänster. Artikelförfattarna diskuterar konceptet molntjänster från olika synvinklar t.ex. koncept, begrepp, egenskaper och klassificeringar. Dock betonar artikelförfattarna vidare att sökerheten måste förbättras för en ökad användning. Vidare görs en detaljerad förklaring hur Amazon Elastic Compute Cloud samt windows Azure fungerar i praktiken
The truth about cloud computing as new paradigm in IT	Adamov A, Erguvan M	2009	International Conference on Application of Information and Communication Technologies, AICT 2009	Artikeln analyserar cloud computing och tillhörande teknik från ett flersidigt perspektiv och presenterar risker och fördelar vid användning av tekniken. Är molntjänster nästa nivå inom internetutveckling eller är det en hype då plattformen är baserad på etablerad teknik?
Why information security is hard - an economic perspective	Anderson R	2001	Seventeenth Annual Computer Security Applications Conference	Artikeln kritiserar det nuvarande perspektivet avseende användning av tekniska medel för att uppnå god informationssäkerhet. Förebyggande åtgärder som åtkomstkontroll, kryptering och brandväggar är idag de vanligaste motmedel som används. Artikeln menar istället att informationssäkerhet kan förklaras tydligare genom användning av det mikroekonomiska språket som t.ex. mänskliga faktorn, asymmetrisk datalagring osv.

Above the Clouds: A Berkeley View of Cloud Computing	Armbrust M, Fox A, Griffith R, D.Joseph A, Katz Y, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M	2009	UC Berkeley Reliable Adaptive Distributed Systems Laboratory	Generell artikel på cloud, men identifierar och rankar vanligaste "obstacles" relaterad med Cloud Computing.
A View of Cloud Computing	Armbrust M, Fox A, Griffith R, D.Joseph A, Katz Y, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M	2010	Communications of the ACM	Artikeln är positive till användning av Cloud Computing och hänvisar till både tekniska och ekonomiska fördelar vid användning. Vidare hänvisar artikeln till elasticiteten vid anammande av molntjänster och det bidrar till ökning av potentiell tillväxt av kunder.
Opinion 05/2012 on Cloud Computing	Articel 29, Data protection Working Party	2012	EU Data Protection Directive (95/46/EC)	Artikelns/direktivets syfte är att tillförse gemensamma riktlinjer till stat angående lagring och skydd av personuppgifter.
Cloud Implications on Software Network Structure and Security Risks	August T, Niculescu MF, Shin H	2014	Information Systems Research	Artikeln undersöker beslutsunderlaget för kunders säkerhetsinvesteringar inom IS, specifikt SaaS. Kunder tenderar att öka investeringar inom interna lösningar och minskar investeringar av SaaS. I miljöer med låg säkerhetsförluster är SaaS optimalt riktad till en lägre nivå av konsumentmarknaden då den den genomsnittliga säkerhetsriskerna minskar och konsumentöverskottet ökar. Säkerhetsinvesteringar ökar inom båda programversionerna (SaaS, in-house) då riskerna ökar inom båda miljöerna.
Data Breach Investigations Report	Baker W H, Hylender C D, Valentine J A	2008		Rapporten analyserar de nio största riskfaktorerna avseendedataintrång.
Opportunities and risks of software-as-a-service:	Benlian A, Hess T	2011	Decision Support Systems	Författarna genomför en kvalitativ studie på vilka opportunities och risks som finns när man talar om SaaS. Dom identifierar bland annat cost factor och quality improvements som möjliga opportunities, och security- economic- och performance risks.

Findings from a survey of IT executives				Utifrån dessa faktorer så väger de riskerna mot möjligheterna och identfierar möjliga fallgropar.
Drivers of SaaS-Adoption – An Empirical Study of Different Application Types	Benlian A, Hess T	2009	Business & Information Systems Engineering	Artikeln är en kvantitativ studie där författarna analyserar faktorer en SaaS provider måste ta hänsyn till vid försäljning. Bland annat kommer de fram till att det inte är någon skillnad vid beslutstagande i små/medelstora företag jämfört med stora företag. De identifierar även att det är stor skillnad mellan vilken typ av system det är, t.ex. ERP, CRM osv.
Why end-users move to the cloud: a migration-theoretic analysis	Bhattacherjee A, Park S C	2014	European Journal of Information Systems	Undersökning på studenter på Google App.
Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities	Buyya R, Yeo C S, Venugopal S	2008	Proceedings - 10th IEEE International Conference on High Performance Computing and Communications, HPCC 2008	Artikeln framställer en vision avseende användning av datorer sant skapandet av marknadsorienterade molntjänster genom VM. Vidare tar artikeln upp riskhantering och SLA-orienterad resursdelning på en gemensam molnplattform.
Secure Cloud Computing: Benefits risks and controls	Carrol, M, van der Merwe A, Kotzé P	2011	IEEE Computer Society	Ställer upp fördelar och säkerhetsrisker med cloud computing. Vad man ska tänka på inför implementation.
Benefits, risks and recommendations for information security	Catteddu D, Hogben G	2009	European Network and Information Security Agency ' s Emerging and Future Risk programme	Artikeln berör molntjänster från ett övergripande perspektiv avseende fördelar, risker och rekommendationer för riskhantering. Vidare utförs diskussionen utifrån tre kategorier: teknisk, policys och juridiska perspektiv.

The Business Intelligence as a Service in the Cloud	Chang V	2014	Future Generation Computer Systems	Ekonomi! Finanssektorn har under lång tid upplevt felaktiga och otillräckliga riskanalyser genom användning av matematiska modeller som t.ex. “Gaussian distrubution”. BIaaS (Business Intelligence as a Service) över molnet tillåter komplexa uträkningar och riskanalyser till en låg kostnad vilket ökar precisionen.
Data Security and Privacy Protection Issues in Cloud Computing	Chen D, Zhao H	2012		Artikel som tar upp säkerhets och integritetsrisker inom använding av molntjänster vilket identifieras inom varje SPIs service delivery models. "The challenges in privacy protection are sharing data while protecting personal information."
What’s New About Cloud Computing Security?	Chen Y, Paxson V, Katz R	2010	University of California, Berkeley Report No. UCB/EECS-2010-5 January	Artikeln hänvisar till de ekonomiska fördelarna vid användning av molntjänster kontra de tekniska säkerhetsriskerna. Vidare utförs en jämförelse mellan säkerhetsrisker inom traditionella informationssystem och molntjänster då artikelförfattarna menar på att det finns tydliga skillnader.
Some key cloud security considerations	Dave M, Kohlenberg T, Purcell S, Ross A, Sedayao J	2012	Intel Technology Journal	Artikeln tar upp säkerhetsrisker associerade till använding av molntjänster. Specifikt hänvisar artikelförfattarna till riskerna med bristande kryptering och webbläsare.
Application service providers	Dewire D T	2000	Information Systems Management.	Gammal artikel, förklarar vad ASP (Application server provider) är. Dvs det SaaS baserats på. Väldigt grundläggande, kan kanske användas till någon typ av bakgrund.
Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing.	Dlodlo N	2011		Djupgående litteraturstudie som tar fram problem associerade med molntjänster samt hur man skall åtgärda dem. Molntjänster är ett relativt nytt forskningsområde och befinner sig I ett utvecklande stadie. Det saknas information om rättsliga mål,

				integritet, säkerhet, tillgång och regulatoriska problem vid användning av molntjänster.
Cloud Computing: Benefits, risks and recommendations for information security, Rev B	Dupré L, Haeberlen G	2012		Analys av 2009 cloud risk assessment utförd av ENISA (European Network & Information Security Agency) som fokuserar på risker vid användning av molntjänster. Vidare beskrivs de vanligaste riskerna vid användning av molntjänster detaljerat t.ex. sannolikhet, konsekvenser, risker samt detaljerad beskrivning av vad som egentligen händer. Riskerna kategoriseras efter: Technical, policy & organizational och legal
Evaluating application service providers	Ekanayaka Y, Wendy L C, Seltsikas P	2003	An International Journal	Ger ett exempel på en ASP implementation och hur man ska utvärdera den. Dock inte så matnyttig för vår rapport
Impact of Cloud Computing : Beyond a Technology Trend	Feuerlicht G, Govardhan S	2010	Systems Integration, 2010	Artikeln analyserar framtidsvisionen av en full implementering av molntjänster samt applicerar teorin i en historisk kontext gällande både fördelar och nackdelar.
Cloud Computing and Grid Computing 360-Degree Compared	Foster I, Zhao Y, Lu S	2008	Grid Computing Environments Workshop	En jämförande artikel avseende cloud computing, grid computing och cluster computing. Syftet är att jämföra de grundläggande egenskaperna mellan teknikerna.
Cloudsourcing: managing cloud adoption	Géczy P, Izumi N, Hasida K	2012	*Global Journal Of Business Research*	Bra sammanfattande av risker med cloud, skriver även vad som är viktigt samt skillnaden i riskerna mellan public och private cloud.
Understanding Service-Oriented Software	Gold N, Mohan A, Knight C, Munre, M	2004	IEEE Computer Society	Tar upp fel som kan uppkomma med SaaS implementation och lösningar till dessa. Detta görs genom ett exempel

Cloud Computing Growing Interest and Related Concerns,	Gupta A	2010		Artikeln analyserar cloud computing från ett kundperspektiv. Frågeställningarna i artiklen är: Varför ska kunden lita på molntjänster och leverantörer samt vad kan kunden förvänta sig?
A Study of the Issues and Security of Cloud Computing	Gupta S, Dave M, Gupta P	2014	International Journal of Computer Science and Information Technologies	Data storage and security, kryptering, Tar upp säkertaspekter inom molnet och ger konkreta förslag vad man kan göra föra att minimera dessa.
Cloud computing for small business: Criminal and security threats and prevention measures	Hutchings A, Smith R, James L	2013	Australian Institute of Criminology	Uppvisar empirska studier med jättemånga företag som deltagit om säkerhetsrisker inom molnet. Även så beskriver den många olika säkerhetsrisker utförligt och bra.
Business value from clouds: Learning from users	Iver B, Henderson J C	2012	MIS Quarterly Journal	Tar upp scaling risks, innovation risk, inefficeny risk, control risk. Tar även upp lite förebyggande åtgärder av risker. Även hur cloud kan lösa vissa organisationsproblem. Även tips och vad CEO:s ska tänka på vid implementering
Preparing for the future: Understanding the seven capabilities cloud computing	Iver B, Henderson J C	2010	MIS Quarterly Journal	Definitioner av cloud: private cloud osv. Även definitioner på olika Levels såsom Service level etc. Beskriver kortfattat vad man ska tänka på för att undvika säkerhetsrisker, t.ex. ISO 27001
Biometrics: A tool for information security	Jain A K, Ross A, Pankanti S	2006	IEEE Transactions on Information Forensics and Security	Artikeln syftar att betona problematiken avseende åtkomst och behörighetskontroll. Vidare hänvisar artikelförfattarna till alternativa medel och metoder för att bekräfta och bevara sekretess inom informationssäkerhet.
Analysis on Service Level Agreement of Web Services	Jin L, Machiraju V, Sahai A	2010		Service Level Agreement (SLA) är ett avtal mellan kund och leverantör som fungerar som syftar att säkerhetsställa produktens funktion. Artikeln fokuserar på samling av information och analys vid framställning av SLA. Artikelns slutsats behandlar hur olika

				”service levels” ger inblande vid förhandling av SLA en tydlig bild av fördelar och nackdelar av SLA.
Security and control in the cloud.	Julisch K, Hall M	2010	Information Security Journal	Väldigt genrell artikel, den kommer fram till att leverantörer måste vara transperanta mot kunden för att dela på risk. Samt att för kunder måste vara realistiska med vad de köper och vilka risker som tas vid cloud computing, genom ett väl genomförd risk management process.
Security and Privacy Issues in Cloud Computing Environment: A Survey Paper	Kaleem U, Khan M N A	2014	International Journal of Grid and Distributed Computing	Är egentligen en kort version av vår uppsats. Finns mycket fakta till alla kapitel.
Application Service provision: Risk Assessment and Mitigation	Kern T, Willcocks L, Lacity M	2002	MIS Quarterly	Jämnför och diskuterar ASP risker och outsourching mot IT-problem och vad man kan göra åt det. Lite gammal artikel med går att använda
The Cloud Adoption Toolkit: Addressing the Challenges of Cloud Adoption in Enterprise	Khajeh-Hosseini A, Greenwood D, Smith J W, Sommerville I	2010		Artikeln hänvisar till problematiken vid migrering till molntjänster och beslutprocessen. Artikelförfattarna framställer ett ramverk till framtida användare i syfte att förebygga risken för felaktiga beslut och användning.
Exposing cloud computing as a failure	Kumar Chauhan V, Bansal K, Alappanavar P	2012	International Journal of Engineering Science & Technology	Tar upp 4 problem med cloud computing, ger flertalet exempel på kända molntjänster som har kraschat och lite lärdomar man kan dra från dessa
Software as a Service (SaaS) Definition and Solutions	Levinson, M	2007		Generell artikel! Behandlar typiska frågor om vad är SaaS, SaaS vs ASP, säkerthetsfrågor, ekonomiska vinster vid användning samt hur man väljer rätt SaaS.

Cloud Computing: What is Infrastructure as a Service	Loeffler B	2011		Generell artikel! Behandlar generella begrepp som t.ex. skillnaden mellan SaaS, PaaS och IaaS efter följande kategorier: type, consumer, service provider, service coverage och customization. Vidare görs en jämförelse mellan shared public cloud -> hosted private cloud efter följande kategorier: type, achitectural control, scalability etc.
Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution	Mantelero A	2012	European Journal for Law and Technology	Artikeln behandlar lagstiftning och den problematik som medförs av trans-border data flows. Vilken lagstifning gäller? Generellt ställs Europeisk lagstifning mot Amerikansk. Artikeln gör en detaljerad beskrivning av tre fall där personlig data kan behandlas utanför Europeiska gränser och dess problematic. Exempel, google som amerikanskt företag med servrar i Italien. Slutsatsen är att EU direktiven måste konkretiseras för att lyckas försäkra starkare skydd på molnet.
Cloud computing — The business perspective	Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A	2011	Decision Support Systems	Generell artikel! Förklarar bra för Cloud Computing, identifierar cost och funktionalitet som faktorer för att välja SaaS. Kan användas för en övergripande förklaring.
The NIST Definition of Cloud Computing	Mell P, Grance T	2011		NIST (The National Institute of Standards and Technology) producerade denna artikel I samband med anamningen av Fisma (Federal Information Security Management Act) 2002. NIST är ansvariga för utveckling av standard, guidelines och krav med focus på nationella säkerhetssystem och artikeln riktar sig främst mot myndigheter. I artiklen framställs definitioner samt jämförelse mellan olika begrepp som har en koppling till cloup computing.
The NIST Definition of Cloud Computing	Mell P, Grance T	2010	COMMUNICATIONS OF THE ACM	Definition av Cloud Computing. Förklarar hela området väldigt generellt på en sida. Bra för bakgrund och förklaring av område.

Outsourcing Business to Cloud Computing Services: Opportunities and Challenges	Motahari-Nezhad H R, Stephenson B, Singhal S	2009	IEEE Internet Computing, Special Issue on Cloud Computing	Artikeln fokuserar på utvecklingen av outsourcing av affärskrtiska system genom service oriented architecture (SOA) . Vidare framställer artikelförfattarna ett ramverk för en virtuell miljö.
Harnessing the cloud: international law implications of cloud-computing	Narayanan V	2012	Chicago Journal of International Law	Genom cloud computing har har det skapats bättre förutsättning till ökad datatrafik och prestanda. Dock har myndigheter aktivt deltagit i arbetet att försäkra säkerheten för användarna och deras lagrade data. Myndigheternas deltagande och regulationer kan delas upp i två sektioner. Dels myndigheter som söker globala lösningar samt myndiheter som söker att ge lagstifningen ”extraterritorial effect” som skyddar användarnas data utomlands.
Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, Myndigheten för samhällskydd och beredskap	Nyström C, Oehme R	2012		För att förebygga och hantera allvarliga it-incidenter i samhället behöver det förebyggande informationssäkerhetsarbetet stärkas ytterligare – på alla ansvarsnivåer och inom Detta kräver en ökad samverkan mellan offentliga och privata aktörer samt utvecklad riskanalys inför framtida krissituationer med tanke på moderniriserade samhällsuppbyggnaden och dess behov av ständig uppkopplingalla sektorer.
Service -Oriented Computing: Concepts, Characteristics and Directions	Papazoglou M P	2003		Artikeln förklarar begreppet Service-Oriented Computing vilket bygger på Service-oriented Architecture samt hur dess arkitektur bidrar till service-based applications. Slutsatsen är: för at nå en ökad funktionalitet som täcker administration, koordination samt säkerhet krävs ”Extended Service Oriented Architecture”. Vidare med denna arkitetur, flera service att gå igenom en sammansatt service -> ökad kontroll.
Service Level Agreement in Cloud Computing	Patel P, Ranabahu A H, Sheth A P	2009	Kno.e.sis Publications	Artikeln betonar vikten av Service Level Agreement (SoA) som är ett ömsesidigt avtal mellan kund och leverantör avseende säkerhetställning av Quality of Service (QoS). Vidare nämns

				problematiken avseende bristande SLA och dess innebörd vid säkerhetsställning av informationssäkerhet.
Advanced Personnel Vetting Techniques in Critical Multi-Tennant Hosted Computing Environments	Sahito F H, Slany W	2013	International Journal of Advanced Computer Science and Applications	Insider risker, exempel, vad man kan göra åt det! Bra beskrivet av "INSIDER risker inom molntjänster"
Information security policies in the UK healthcare sector: A critical evaluation	Stahl B C, Doherty N F, Shaw M	2012	Information Systems Journal	Artikeln hänvisar till problematiken vid övergång till molntjänster. Fördelarna väger tungt för en övergång från traditionella lösningar om kunder och leverantörer strikt anammar avtal som Service Level Agreement (SLA) i syfte att upprätthålla Quality of Service (QoS).
Cloud computing - The business perspective	Stoneburner G, Goguen A, Feringa A	2002	*National Institute of Standards and Technology*	Artikeln är en kvalitativ studie utförd av US goverment. Den är relativt gammal och presenterar riskanalys utifrån ett väldigt teoretisk ramverk. Artikeln fokuserar på Risk Management i SDLC (system development life cycle). De identifierar de olika aktiviteterna vid risk assessment, threatidentification, cost-benefit analys osv.
A survey on security issues in service delivery models of cloud computing	Subashini S, Kavitha V	2010	Journal of Network and Computer Applications	Artikeln är generell! Behandlar majoriteten av säkerhetsrisker som uppkommit genom ìservice delivery modelsî inom cloud computing system. Artikelförfattaren menar att användare av molntjänster saknar medvetenhet om risker vid användning av molntjänster. Molntjänster bör analyseras i detaljnivå och designas till en mer integrerad form för att öka användning. Artikelförfattarens förslag till ramverk är tillgång och lagring genom meta-data.

Risks and benefits of Business Intelligence in the Cloud	Tamer C, Kiley M, Asharfi N, Kuilboer J.P	2013	*Northeast Decision Sciences Institute Annual Meeting Proceedings*	Artikeln väger möjligheter med risker på BI in molnet. DE risker de identifierar är, Security Risks, Slow Data Breach Recovery (problem med att återskapa förlorad data), External server reliability, Compromise of data integration, Costs are difficult to quantify och Changing and Controversial regulatory environment. De kommer fram till att BI i molnet ger stora möjligheter till effektivisering men samtidigt måste riskerna vägas in. Bra artikel som identifierar risker med molnet.
A critical review of cloud computing: researching desires and realities	Venters W, Whitley E A	2012	Journal of Information Technology	Artikeln hänvisar till ett framtaget ramverk avseende användarnas behov och efterfrågan. Artikelförfattarna stödjer ramverket genom litteratur och empirisk data mellan 2010 och 2012.
Privacy-preserving public auditing for data storage security in cloud computing	Wang C, Wang Q, Ren K	2010	IEEE Infocom 2010	Artikeln tar upp säkerhetsrisker inom molntjänster avseende åtkomst och behörighetskontroll baserat på omfattande analyser inom prestanda och säkerhet.
Cloud Computing: a Perspective Study	Wang L, von Laszewski G, Younge A, He X, Kunze M, Tao J, Fu C	2010	New Generation Computing	Beskriver Cloud Computing, historian bakom och vart det är på väg. Bra artikel för att skriva om historien däravhögt betyg
Service Level Agreement (SLA) in Utility Computing Systems	Wu L, Buyya R	2010	arXiv:1010.2881	Artikeln beskriver vikten av Service Level Agreement vid annammning avmolntjänster. Ett ömsesidigt avtal mellan parterna ökar täänstens kvalité QoS, Quality of Service, samtidigt som att det skyddar kunden och tillhörande data.
Addressing cloud computing security issues	Zissis D, Lekkas D	2012	Future Generation Computer Systems	Artikelförfattarna menar på att övergången från traditionella system till molntjänster ställer högre kravpå säkerhet då det medför nya risker. De största riskerna är säkerhetsställa auktorisering, integritet och sekretess avseende lagrad data.

7.2 Intervjuguide

Kandidatuppsats vid Ekonomihögskolan, Lunds Universitet

Intervjumall

Hur molntjänstleverantörer ställer sig till säkerhetsrisker inom Cloud computing; Vilka är de tekniska säkerhetsrisker och vad görs i förebyggande syfte gentemot dessa.

Allmän information

1. Önskar ni att vara anonyma?

2. Namn, företag, befattning och IT-erfarenhet?

3. Kort beskrivning av företaget och dess verksamhetsområde?

4. Vilka molntjänster levererar ni?

5. Vad är en typisk kund för er?
a. Bransch?
b. Storlek?
c. Geografisk plats?

6. Hur många kunder har ni inom molntjänster?

Säkerhetsfrågor angående molntjänster

Q1. Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?

Förebyggande arbete angående molntjänster

Q2. Vad gör ni för att motverka säkerhetsrisker?

Q3. Hur ofta gör ni säkerhetsanalyser?

Q4. Vilka resurser avsätter ni i förebyggande ändamål?

Q5. Har ni ett eller flera konkreta exempel på säkerhetsbrister inom molntjänster?
a. Vad har hänt efter det för att förebygga att detta ska hända igen? och i så fall är denna process standardiserad?

Q6. Har ni en processplan att följa vid allvarliga säkerhetsbrister?

Q7. Testar ni era system och processer för att identifiera säkerhetsbrister?

Juridiska frågor

Q8. Är era servrar lokaliserade nationellt eller internationellt?

Q9. Beroende på vart datan är lokaliserad, finns det några juridiska aspekter som ni tar hänsyn till och i så fall hur?

Q10. Vilka förebyggande åtgärder gör ni för att upprätthålla lagstiftning t.ex. PUL?

Service level agreement

Q11. Använder ni standardiserade avtal med kund eller är det situationsbaserat?
a. Vilka säkerhetsmässiga krav ställer ni på kunden?
b. Vilka säkerhetsmässiga krav ställer kunden på er som leverantör?

Tillgänglighet

Q12. Vilka säkerhetsrisker anser ni finns inom tillgänglighet till molntjänsten?

Q13. Vilka krav ställer era kunder på tillgänglighet till era molntjänster?

Q14. Vilka förebyggande funktioner har ni för att uppfylla dessa krav? (Till exempel backup eller dubbla servermiljöer)

Q15. Vilket förebyggande arbete har ni för att upprätthålla internetanslutning till era molntjänster? Och även strömtillförsel?

Sekretess

Q16. Vilka säkerhetsrisker uppkommer när man säkerställer sekretess i molntjänster?

Q17. Vilka säkerhetsrisker anser ni finns inom området sekretess i molntjänster?

Q18. Vilka krav ställer era kunder på sekretess inom molntjänster?

Q19. Hur säkerhetsställer ni att obehöriga användare inte får tillgång till en behörig användares data?
a. Ställs det några säkerhetskrav på kunden vid användning era molntjänster?

Integritet

Q20. Vilka säkerhetsrisker anser ni finns inom området data integritet i molntjänster?

Q21. Vilka krav ställer era kunder på data integritet?

Q22. Vilka åtgärder tar ni för att säkerhetsställa (lagring av data) integritet för era kunder?

Q23. Vad händer med sparad data när en kund väljer att avsluta tjänsten?

Q24. Vilket förebyggande arbete gör ni för att information/data inte skall oväntat ändras?

Säkerhetsfrågor angående molntjänster i samband med kunder

Q25. Anser du att era molntjänster motsvarande eller bättre säkerhet än kundernas egna system? och i så fall inom vilka riskområden?

Q26. Vilken insikt har kunden i ert förebyggande säkerhetsarbete?

Q27. Outsourcear ni någon del av er tjänst?
a. Vilken insikt har ni i tredjepartens förebyggande säkerhetsarbete?
b. Specificeras det i det avtal ni har med kund?

Q28. Upplevs det problematik vid övergång mellan olika molntjänstleverantörer?

7.3 Kodning av empirisk data

	Xledger	Telekomföretag	Integrations företag	Knowit Cloud Innovation	Systemutveckling sföretaget	Affärssystemsleverantör
Q1	-	inte har full kontroll över datan, backuper och hackerattacker, data läcker ut, eller att det står stilla	utanför din egen bandbrygga, alltid en risk, sitter du i händerna på det leverantören, extremt känslig också om du växer dig stor på en molntjänst för prisförändringar, VPN-tunnlar, certifikat, molntjänsten blir komprimerad	Felaktig arkitektur, Felaktig kommunikation och nätinfrastruktur, Felaktig autentisering	informationssäkerheten, informationsklassificeringen, informationen är känslig eller inte, mänsliga faktorn	okunskap från användare, gamla mjukvaror och dåliga lösenord
Q2	Revidering varannat år av skalskydd inloggning, kryptering, penetrationstester	penetreringtester vid lansering, patchar vid varje säkerhetsuppdatering	designa lösningar och titta på säkerhetscertifieringar, inte gör i en molntjänst, känslig information, B2B-gateway utanför sitt nätverk som får agera proxy mot molntjänsten.	Innan vi tar ansvar, lösning, granskning av arkitektur, kommunikation, nätuppsättning och lösning för autentisering	mänskliga faktorn, rättighetsnivåer, klassificera informationen, behörigheter, auditing	penetrationstestning, externt företag, säkerhetsanalys, patchar
Q3	Säkerhetsanalyser görs monumentalt	Inte regelbundet, innan lansering	Inte lika ofta som vi borde, fix packets för de protokoll, vitala checkar vad som sker i miljön, släppts förbättring av protokoll, i fas med det	Initialt vid uppsättning och löpande vid större förändringar.	inget sånt, rutinmässigt, när det behövs, mycket aktiviteter, vad som faktiskt händer	stor säkerhetsanalys, en gång om året
Q4	Dom system vi jobbar med samt personal/driftpersonal. Vi har haft tre specialist företag inom säkerhet och två av dom har gjort	En avdelning som försöker samordna så att vi göra likadant, inte så uppstyrt som det skulle kunna vara	Nej, inte för vår interna molntjänst, kanske vi borde, diskuterar, inte direkt byggd från säkerhetstänk, leveransmodells tänk, säkerhetstänk i	Löpande bevakning av nya funktioner/patchar som kan påverka befintliga lösningar.	internt, olika nivåer, arbetsgrupp, patchning av servern, säkerhetsreleaser, uppgraderas det automatiskt,	3-4 personer

	penetrationstester.		grunden, kommunicerar över ett protokoll, kommunikationsadaptrar, SSL, kanske inte till den grad man hade velat ha		kollar loggar, internrevisioner, säkerhetsrevision, kund, säkerhetsrevisioner på vårt företag	
Q5	Nej	Nej	Nej,	Nej	Ja, inte uppdaterar servern eller mjukvaran, automatiserade hackningar, hänt oss, sen, uppdatera säkerhetspatch, exploitat, hackar mjukvaran, botserver, spindlar igenom nätet och försöker hacka	-
Q5 a	-	hypotetiska, port öppen, inte har data krypterad, skickar datan mellan molntjänsten och företaget	protokoll, en kvittens, datan inte har blivit komprimerad, kommunikationsprotokoll	-	redan standardiserat, snabbare, patchningen	
Q6	Ja	Ja	Förmodligen, nog infrastruktur i så fall	Ja	Nej, daily backups, alltid kan återställa, ingen specifik säkerhetsplan	krishanteringsplan
Q7	Ja, vi har kontinuerlig test och process. Vi lägger på 4 nya releaser per år ,natt mellan lördag och söndag. Då är det ju givetvis någon form av testaktivitet i efterhand	Ja, google tester, ett scenario, Filsystemet är korrupt, läs upp allt från backup och få upp systemet så snabbt som möjligt	Jag tror inte det.	Vid behov görs penetrationstester och lasttester		penetrationstestning, externt företag
Q8	Internationellt	Internationellt	i ett annat land,kunderna som	inga egna, globala	I Sverige	nationellt

			nyttjar, både i samma land och i andra länder.	molnleverantörerna Amazon AWS och Microsoft Azure.		
Q9	Det är godkänt då utifrån Svensk lag. Det våra kunder ska göra är att dom ska skicka en anmälan att deras data är lokaliserad i Norge	Ingen aning	vissa integrationer, inte nyttja molntjänsterna, arkivering av data, av lagar, hur länge man får arkivera, var man får arkivera, vem som har rätt att komma åt den datan, absolut det finns viss hänsyn till det	Svensk lagstiftning är enhetlig med EU:s lagstiftning, globala molnleverantörernas datacenter finns inom EU är det inga problem, Amazon AWS, Irland & Frankfurt, Microsoft Azure, Irland & Amsterdam	Nej	undvika juridiska problem med bokförings data
Q10	Det behöver man inte men en kund begärde en PUL-anmälan och då gjorde vi det	advokater som säkerhetsställer vad som får göras, kontrakten, SLA kontrakt, vem vi får dela information med, få ha den här datan och även vissa molntjänster är tillräckligt säkra för att ha datan också.	PUL berör oss inte, mer affärsdata, avtal och överrenskommelser, up to date, absolut största processen, juridiska processen	kunden, äger sin data, vi tillhandahåller en plattform, applikationer, lagra data.	Nej	-
Servicelevelagreement						

Q 11	Vi har helt klart standardiserade avtal med kund	Standardiserade	betalar olika för olika SLA, del av vår supportavdelning, nyttjar en molntjänst eller bara köper support kan du avtala olika former av SLA.	baseras på standardavtal, IT & Telekomföretagen	Nej, gratistjänst, förvaltningsåtagande, inte, SLA,	redovisningsbyråer, specialiserade avtal. Mot den vanliga kunden som beställer direkt av oss där har vi ett standardavtal för alla.
Q 11 a	1 eller 2 engagerade eller kompetenta människor	-	Ingen aning, vi hand om själva adaptern som de kommunicerar med molntjänsten, Vi har själva ansvaret, POD, deras interna nätverk till våran molntjänst	Kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.	Nej inte på det här systemet.	modern webbläsare
Q 11 b	När det gäller kunden så kan dom inte säga till mycket säkerhetsmässigt	-	Säkerhet, tillgänglighet, uppe och ner tid, trueput	Kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.	Nej inte på det här systemet.	Den vanliga kunden ställer inte så höga krav,våra byråer har betydligt högre säkerhetskrav
Tillgänglighet						

Q 12	Vi ligger på över ungefär 99,90% någonting. Men vi ger inga garantier utan om det står stilla så står det stilla för alla kunder.	samma uptime som internt på företaget där kan ju strömmen gå osv, Netflix, som har större procent uptime än vad amazon har och Netflix kör på amazon, lyckats göra det redundans så att det klarar av att har bättre SLA än sitt system, länken till molntjänsten skall vara uppe och inte för mycket belastad, direktlänk till molntjänsten, Internet och WAN	en server någonstans, strömavbrott, händer med meddelande, en transaktion och serverhallen går ner eller tvärtom outsignade system går ner, kommunikationsrisk	Felaktig arkitektur, Val av fel leverantör, Ofta väljs, Amazon eller Azure, bästa, Multi-Cloudlösning, olika leverantörer används, bäst på	Inte riktigt identifierat, inte, kritisk information, legat nere en dag, inte, end of the world, gratis	överdimensionerar, failsafes, redundansreplikering Okunskap
Q 13	Kraven är inte då inte bara att det skall vara tillgängligt utan även att det ska vara kontroll på svarstid samtidigt som vi hela tiden bygger ut våra serverparker.	servrar skall vara uppe 100%, besparing att ha det i molnet för tillfället	väldigt väldigt höga, affärsdata, näst in till 100% tillgänglighet	erbjuder 99,8%	inte riktigt identifierat	mycket höga krav på tillgänglighe
Q 14	Dubbla servermiljöer och kontinuerlig loggning och vi tar kompletta veckobackuper som vi lagrar i upp till 18 månader	Vet inte	redundanta system och failoverlösningar, arkitektuellt beslut kontra infrastruktur, infrastruktur som är redundant, en ESB så är den failover säkrad i sig själv, aktivaktiv miljö, en noden i princip skulle kunna gå ned och då du kan köra på den andra	genomtänkt molnarkitektur med inbyggd redundans	Dubbla servermiljöer, inte, Backups har vi, alltid daily backups, roll-backa, SLA, serverleverantör, garanterar, 85% uptime, bra nog	dubbla datorhallar
Q 15	När det gäller internetanslutning har vi tre internetleverantören in i tjänsten	två olika internetleverantörer, ett väldigt bra SLA med bra uptime, batterier i källaren för att hålla uppe våra egna servrar, utvärdera varje program, en playbook, vad gör vi	två olika serverhallar i två olika delar av en stad, serverhall som är duplicerad i två olika rum som är brandsäkrade från varandra, olika typer strömförsörjning från olika leverantörer eller källor	inga egna molntjänster, kommunikationen mot AWS, redundanta linor, DirectConnect som primär lina	Nej, sköter vår leverantör	dubbla internetlinor till båda datorhallarna från olika leverantörer

		om det här händer		och VPN som fail over		
Sekretess						
Q16	Vi har ungefär 34 roller i vårt system. Om jag som är avdelningschef då har jag ju av naturliga skäl bara tillgång till min avdelnings data och det är ett regelverk som kunden själv sätter upp då i sitt i införande projekt.	vissa projekt får inte se varandras data, kontrakt på att man inte får ta del av datan, separata servrar, säkerhetsgrupper, firewall och sätter det på servernivå, nyckel, de som underhåller system är trusted, Admins och IT-personalen är trusted people och kan läsa allt om de vill	Vem som har access till loggar, inte ha en intrång där vi kopplar upp oss, genom en annan ingång, inte syfte att komprimera våran ESB utan snarare att komma åt något annat, integrationen inte körs i molntjänst om sekretess skall uppnås, låst och att nyckel är bortappad, rätt nyckel för att kunna lösa datan, komprimera datan med olika certifikat, datan är princip oläsbar, rätt nyckel eller certifikat för att dekryptera datan, standarder som RSA	Sekretess på molninfrastruktur- & plattformsnivå, säkerställas via kryptering av data, säker inloggning, Sekretess på Applikationsnivå, inte specifikt, molnet, applikation, hanterar informationen, vem som kan komma åt den	-	-
Q17	Jag ser inga säkerhetsbrister vår lösning	-	-	-	vårt system, all data i samma databas och samma tabeller, logiskt fel, hämtar upp data, risk för att kunder kan komma åt andra kunders data, jätterisk	kund har ern egen unik databas, väldigt höga kav på den här datan för att det är bokförings data
Q18	Kunderna ställer inga krav	kontrakt, bedöma om molntjänsten är tillräckligt säker, stämda om det läcker ut	olika, fallspecifikt, avtal, specifik integration	kryptering av data och säker inloggning.	inga krav, ovetande om riskerna som finns	Den (datan, förf tillägg) ska vara hemlig, Just eftersom att det handlar om bokföringssystem och

						affärssystem så är kraven höga
Q 19	-	testa vår egna säkerhet, specifika nycklar	-	kryptering av data och säker inloggning, applikation som hanterar informationen och vem som kan komma åt den.	ren logisk nivå, ett antal säkerhetslager i applikationen, mappar mot detta då	väldigt låsta datahallar, lösenordsskyddade system och rättighetsbaserade system
Q 19 a	Kunden själv underhåller ju till exempel avdelningar och projekt i sin lösning och tekniskt sätt så finns ju stöd men det måste dom ju göra själva.	-	låst och att nyckel är bortappad, rätt nyckel för att kunna lösa datan, komprimera datan med olika certifikat, datan är princip oläsbar, rätt nyckel eller certifikat för att dekryptera datan, standarder som RLA	Kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.	Nej	-
Integritet						
Q 20	Kunden själv underhåller ju till exempel avdelningar och projekt i sin lösning och tekniskt sätt så finns ju stöd men det måste dom ju göra själva.	Äger man inte datorn, Även om man krypterar det hårdaste, kommer att kunna dekryptera den datan, måste ha trust, bygga hela sin affärsidé på att de inte släpper igenom någonting	Datan försvinner, Att datan inte är i dina lokaler	Felaktig eller obefintlig Backuplösning	tillgång till en annan kunds data, kunden, viss mån rättigheter till att editera data, förebyggande åtgärder, ändringslogg, editering av information så loggas det, vad som editerats och av vem, XSS och SQL-injections, stora risker, Cross server scripting, svårt att upptäcka, rensa datan, backup, säkerhetsåtgärd,	-

					läsa datan, hackade viset, inget sett att upptäcka, körd	
Q 21	Kunderna ställer heller inga krav utan tar det som en självklarhet.	inte att deras användarnamn och password blir offentligt, känslig data som är lagrad så är det avtalat att det inte ska delas	Ingen aning, men förmodligen fallspecifikt	Backup ingår som standard i alla lösningar	-	det får ju inte manipulera s ska ju vara helt solid, Så det är ju en av dom systemen vi har på plats för att säkerhetsst älla att integritet behålls eller att man kan spåra vem som gjort vad med datan då.
Q 22		-	fall till fall, svårt att spåra	Regelbundna tester tillsammans med kund.	-	-
Q 23	Då gör vi så att när kunden kvitterat, han har fått ut all sin bokföringsdata, alla sina skannade fakturor och det som han behöver och att det är inläst och registerat. Inte förrän då stänger vi ner kontot och tjänsten för kunden.	plockas bort	vet inte. Vet inte hur mycket som sparas.	All lagrad data tas bort, inte kunden, ytterligare en period	Datan ligger kvar, kopplar bort alla konton, ingen, tillgång till datan, Administratörer, oss själva rättigheter, i efterhand, data från gamla ärenden, kunder som inte finns längre	vi sparar datan i två månader om kunden vill komma tillbaka, sen raderar vi den
Q 24	-	Fil-lagrings program, checksums beroende, vi märker väldigt snabbt om det är ett fildiskproblem, ändrat i filen, går det alarm för oss	jag vet inte	Regelbunden kontroll av rutiner för lagring och backup	Backup, behandlingssytem och loggning	-

Säkerhetsfrågor angående molntjänster i samband med kunder						
Q25	Det är säkrare än att ha det hemma.	Vi är mer användare och vi har valt ut dom som vi tror på har bra säkerhet	ett bättre säkerhetstänk då vi säkrar data i flera led istället	globala molnleverantörerna, Amazon AWS, Microsoft AWS, mycket säkrare än, driften on-premise, lokal partner, Säkerhet är dyrt, globala leverantörerna investerar stora summor i säkerhet, regionala spelare, Tieto, CGI, inte kan hänga med	kunder, olika branscher, helt okej, inte extraordinär, inte så känslig data, information vid angrepp inte hade gjort så mycket om den blev publik, inte säkerheten så extrem, kunders egna system är ju brutala i jämförelse,	ungefär 50/50, har du har många användare som kan logga in i ditt molnsystem eller bokföringssytem så är det ju en större risk att en laptop som kommer på drift eller bli snodd då.

Q 26	Bolaget Transcendent vet allting för det är deras jobb. Andra frågar ingenting.	Ingen.	Förmodligen ingen.	Full transparens	inte direkt någon insikt alls, som verksamhet, kunder ingen alls och vissa jättegod insikt, kraven som kunden har	byråkunder har ju rätt bra insikt och dom är ganska aktiva, överlag är det ett ganska lågt intresse från vanliga kunder
Q 27	Nej. Serverparker i skyddade datorhallar. Allt annat är helt internt.	Ja	Ja, själva infrastrukturen.	Ja, Cloud Operations, partner i Indien	Nej	några delar av systemet som utvecklas externt
Q 27 a		Jag tror vi fortfarande kör för driften, men de kanske kodar.	Nej, inte mer avtalsmässigt, om de uppfyller dessa krav kan man inte veta säkert.	Full transparens	-	Ganska bra, all projektledning i det vi har outsourcat sköts ändå härifrån.
Q 27 b		"pain in the as", måste specifiera allt man vill ha, bara det man kravställer helt enkelt, inte kravställer säkerhet så får man inte säkerhet.	Ja	Ja	-	Nej
Q 28	Vi har ingen erfarenhet om av att en kund byter molntjänst	Amazon, en vanlig Linux server, inte varit så svårt att flytta den, Varje molntjänst har ju unika tjänster, molntjänst lite bättre än alla andras, inte smärtfritt att flytta saker och ting	våran tjänst, väldigt smärtfritt, står för själva kommunikation till och från molntjänsten, designar man sin lösning, byta ut så är det ganska oproblematiskt, inte, extremt problematiskt och väldigt kostsamt, explicit använda en specifik så sitter man i händerna på den	Nej, hjälpt kunder, flytta lösningar, Microsoft Azure till Amazon AWS, prestandan i Microsoft Azure inte räckte	inte råkat ut för, ingen utarbetad tjänst för dataexport, manuellt, uthämtning av data,	Om man vill byta till vårt system så är det ganska enkelt för då löser våran techsupport på företaget det, Det är smidigt för kunden att smidigt

						byta runt inom onlinebokföring
Övrigt		Vissa saker lämpar sig för molnet men man ska kanske inte lägga allt i molnet. Man ska kanske inte ha allt det hemligaste i molnet.			-	-

7.4 Transkribering Xledger

Allmän information

1. Önskar ni att vara anonyma?
Nej

2. Namn, företag, befattning och IT-erfarenhet?

Mitt namn är Lars Lobelius och företaget är Xledger AB och min befattning är att jag är Sverigeschef och ansvarig för bolaget och startade som det 1a september 2009. Min IT-erfarenhet är 45 år sen jag började med affärssystem.

3. Kort beskrivning av företaget och dess verksamhetsområde?

Xledger AB är ett 100% dotterbolag till Xledger Group AS i Norge

4. Vilka molntjänster levererar ni?

Vi leverar bara en enda tjänst, vårt enda fokus är Xledger. Xledger är äkta webb-baserad lösning där allting körs i en enda installation, en enda databas. Den är alltså byggt på en publik plattform. Men lösningen är ytterst private sak eftersom att du endast kommer in om du är inloggad och avsäkrad kund. Det vi fokuserar på är alltså Xledger innehåller ett komplett ERP, famförallt för projekdrivna företag eller organisationer som är spridda på flera många ställen även globalt är en bra målgrupp. Vi har lager inköp men inget stort fokus på det. Vi levererar ingenting externt. Det enda externa produkt vi levererar med våra lösningar är vår egna integrationsmotor som automatiserar integration.

5. Vad är en typisk kund för er?

Det är alltså 6000 företag i vår databas och av dom är 400-500 svenska företag. Majoriteten av kunderna är i Norge

a. Bransch?

En typisk bransch för vår direktförsäljning i Sverige är IT-bolag, konsultbolag, tjänstorienterade verksamheter och så är det då också inom typ servicenäring där genom ekonomisystem integrerar med andra verksamhetssystem.

b. Storlek?

Storleken på våra kunder i sverige idag de är från 17-18 till 750 anställda.

c. Geografisk plats?

Vi har kontoret i Stockholm men vi jobbar väldigt effektivt på distans. vi mycket kunder även i Skåne, Göteborg och är ofta på plats kanske i 2-3 dagar sen använder vi tekniken som finns idag till att online meetings och skype och så då.

6. Hur många kunder har ni inom molntjänster?

Det är då 6000 företag i lösningen. Många av dom i Norge är partnerkunder

Säkerhetsfrågor angående molntjänster

Q1. Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?

Jag är väldigt tveksam till att kalla våra tjänster för en molntjänst. Då ser man ju framför sig att data hamnar i Hong Kong eller vart som helst. Men det är i alla fall det och vi har då under 2012 och 2013 med en slutrapport i Maj 2014 genomfört en komplett revidering ISAEA3420. Och det är Ernst and Young i Norge som har gjort det och det är både dokumentation och det är hantering etc. Vi stötte på 2009, en av våra största kunder var en anläggningsverksamhet på 130 anställda, alla konkurrenter använde sig av som idag, traditionella system. Vi satte ihop ett dokument på ett a4, vi är inhyrda på två rigoröst skalbevakade oberoende datahallar, där finns det givetvis backupström och backupinternet osv. När jag redogjorde för säkerheten för dom här två företagsledarna så sa jag "Det här är säkrare än att ha det hemma". Det ligger någonting i det. Nu pratar jag enbart om vår egna applikation och tekniska plattform och vi är också granskade av, det här är en börsnoterad verksamhet där en person rapporterar till finansmyndigheten så KPMG IT är reviderad i hela lösningen år 2010.

Förebyggande arbete angående molntjänster

Q2. Vad gör ni för att motverka säkerhetsrisker?

En del av vårt förebyggande arbete är att vi har gjort en revidering och att då arbeta med den rapporten och göra en ny revidering om två år. Så vad vi har gjort, vi har gått igenom skalskydd, vi har gått igenom inloggningsdelar, det är krypterat givetvis. Sen är det också så att när man loggar in så kan man antingen logga in med sin mailadress och säkerhetslösenord eller så loggar

man in och får en engångskod då på mail som gäller under 30 sekunder.

Q3. Hur ofta gör ni säkerhetsanalyser?

Man kan säga att vi har systemstöd för det här som loggar monumentalt. Säkerhetsanalyser görs monumentalt .

Q4. Vilka resurser avsätter ni i förebyggande ändamål?

De resurser vi avsätter är ju dels då dom system vi jobbar med, dels personal/driftpersonal.

Q4.1 Hur många, antal personal avsätter ni i detta arbete?

Ganska kul, 2010 i januari fick vi in en artikel i Computer Sweden. Där jämförde man vår drift av då 3000 företag som uppehölls av 1,5 tjänst med en backuptjänst och jämförde den gamla. ESV driftade 100 småmyndigheter i en citrix lösning och dom var 20 personer. Här ligger allt i 1. Vi har haft tre specialist företag inom säkerhet och två av dom har gjort penetrationstester med väldigt bra utfall. Det dom inte fick göra var massangrepp givetvis. En sen ganska nybliven kund som är experter inom IT och säkerhet. Då hade jag faktiskt med mig vår rapport och gick igenom med dom och då var det ingen tvekan längre.

Q5. Har ni ett eller flera konkreta exempel på säkerhetsbrister inom molntjänster?
a.Vad har hänt efter det för att förebygga att detta ska hända igen? och i så fall är denna process standardiserad?

Q6. Har ni en processplan att följa vid allvarliga säkerhetsbrister?

Ja, finns processplan vid säkerhetsrisk. Det finns processplan vid incidenter. Vi har ju då två kompletta serverparker och på två helt oberoende ställen. Om den ena hallen som är huvudhall då blir bombad så hoppas man ju på att den andra klarar sig.

Q7. Testar ni era system och processer för att identifiera säkerhetsbrister?

Ja, vi har kontinuerlig test och process. Vi lägger på 4 nya releaser per år, natt mellan lördag och söndag. Då är det ju givetvis någon form av testaktivitet i efterhand. Inte bara säkerhet utan funktion framförallt då.

Juridiska frågor

Q8. Är era servrar lokaliserade nationellt eller internationellt?
Servarna är lokaliserade i Norge

Q9. Beroende på vart datan är lokaliserad, finns det några juridiska aspekter som ni tar hänsyn till och i så fall hur?

Det är godkänt då utifrån Svensk lag och det våra kunder ska göra är att dom ska skicka en anmälan att deras data är lokaliserad i Norge. Det är bara en anmälan dom registrerar till skattemyndigheten. Det är ingen ansökan. Vi använder en checklista på de krav vi ställer på kunderna.

Q10. Vilka förebyggande åtgärder gör ni för att upprätthålla lagstiftning t.ex. PUL?

Det behöver man inte men en kund begärde en PUL-anmälan och då gjorde vi det. Vi har ingen lön utan vi har reseräkning och utläggshantering och den kräver ingen PUL-anmälan.

Service level agreement

Q11. Använder ni standardiserade avtal med kund eller är det situationsbaserat?

Vi har helt klart standardiserade avtal med kund. Men det är klart att,det vet du själv att, det finns upphandlingskonsulter med speciella kunder och ibland får man anpassa avtalen.

a. Vilka säkerhetsmässiga krav ställer ni på kunden?

Att de följer avtalen

b. Vilka säkerhetsmässiga krav ställer kunden på er som leverantör?

När det gäller kunden så kan dom inte säga till mycket säkerhetsmässigt.

Tillgänglighet

Q12. Vilka säkerhetsrisker anser ni finns inom tillgänglighet till molntjänsten?

När det gäller tillgänglighet så har vi en statistik från dom ca 7 åren. Vi ligger på över ungefär 99,90%. Men vi ger inga garantier utan om det står stilla så står det stilla för alla kunder. Och det köper dom flesta.

Q13. Vilka krav ställer era kunder på tillgänglighet till era molntjänster?

Kraven är inte då inte bara att det skall vara tillgängligt utan även att det ska vara kontroll på svarstid samtidigt som vi hela tiden bygger ut våra serverparker.

Q14. Vilka förebyggande funktioner har ni för att uppfylla dessa krav? (Till exempel backup eller dubbla servermiljöer)

När det gäller backuper har vi dubbla servermiljöer och kontinuerlig loggning och vi tar kompletta veckobackuper som vi lagrar i upp till 18 månader.

Q15. Vilket förebyggande arbete har ni för att upprätthålla internetanslutning till era molntjänster? Och även strömtillförsel?

När det gäller internetanslutning har vi tre internetleverantören in i tjänsten. Så jag loggar vanligtvis in på www.xledger.net. Så har det stått stilla en gång och då går jag in på www.xledger2.net och kommer in via den leverantören då. Och strömtillförseln det är dom där datahallarna som tar ansvar och som ser till att det finns backuper och allt det där.

Sekretess

Q16. Vilka säkerhetsrisker uppkommer när man säkerställer sekretess i molntjänster?

Vi har ungefär 34 roller i vårt system. Om jag som är avdelningschef då har jag ju av naturliga skäl bara tillgång till min avdelnings data och det är ett regelverk som kunden själv sätter upp då i sitt i införande projekt.

Q17. Vilka säkerhetsrisker anser ni finns inom området sekretess i molntjänster?

Jag ser inga säkerhetsrisker... Jag ser inga säkerhetsbrister vår lösning.

Q18. Vilka krav ställer era kunder på sekretess inom molntjänster?

Kunderna ställer inga krav men det är självklart att det finns dom som är väldigt okunniga som funderar på om man kan komma åt andra kunders data etc genom gemensam databas. Det finns ingen möjlighet att komma åt andra användares data.

Q19. Hur säkerhetsställer ni att obehöriga användare inte får tillgång till en behörig användares data?
a. Ställs det några säkerhetskrav på kunden vid användning era molntjänster?

Kunden själv underhåller ju till exempel avdelningar och projekt i sin lösning och tekniskt sätt så finns ju stöd men det måste dom ju göra själva. Det ingår ju också i själva projektet så att säga.

Integritet

Q20. Vilka säkerhetsrisker anser ni finns inom området data integritet i molntjänster?
Det är samma med integritet. Man kommer inte åt något annat än det man ska komma åt.

Q21. Vilka krav ställer era kunder på data integritet?
Kunderna ställer heller inga krav utan tar det som en självklarhet.

Q22. Vilka åtgärder tar ni för att säkerhetsställa (lagring av data) integritet för era kunder?

Det enda kunden behöver ha är en valfri terminal, pc eller mac, telefon och en webbläsare. Vi stödjer ju alla webbläsare.

Q23. Vad händer med sparad data när en kund väljer att avsluta tjänsten?

Om en kund väljer att avsluta tjänsten händer ju vanligtvis om företaget blir uppköpt då. Då gör vi så att när kunden kvitterat, han har fått ut all sin bokföringsdata, alla sina skannade fakturor och det som han behöver och att det är inläst och registerat. Inte förrän då stänger vi ner kontot och tjänsten för kunden. Men inte förrän man kvitto, skriftligt på att det är okej.

Q24. Vilket förebyggande arbete gör ni för att information/data inte skall oväntat ändras?

Säkerhetsfrågor angående molntjänster i samband med kunder

Q25. Anser du att era molntjänster motsvarande eller bättre säkerhet än kundernas egna system? och i så fall inom vilka riskområden?

Det är som jag nämnde tidigare med kundmötet för 5 år sedan. Det är säkrare än att ha det hemma. Jag har jobbat så många år i den här branschen så jag vet vad det innebär, vilka risker som finns även om dom förvaltar sakerna själv.

Q26. Vilken insikt har kunden i ert förebyggande säkerhetsarbete?

Det varierar väldigt mycket

Q27. Outsourcear ni någon del av er tjänst?

Nej, vi outsourcar ingenting utan det vi outsourcar är att vi ställer våra serverparker i skyddade datorhallar. Allt annat är helt internt.

a. Vilken insikt har ni i tredjepartens förebyggande säkerhetsarbete?
b. Specificeras det i det avtal ni har med kund?

Q28. Upplevs det problematik vid övergång mellan olika molntjänstleverantörer?

Vi har ingen erfarenhet om av att en kund byter molntjänst. men ser heller inget problem vid om en kund skall byta till traditionellt eller annan molntjänst så är ju grundbehoven exporterat data.

Parterna tackar av varandra.

7.5 Transkribering Telekomföretaget

Allmän information

1. Önskar ni att vara anonyma?

Ja

2. Namn, företag, befattning och IT-erfarenhet?

XXXX , Software Architect , sen 2006

3. Kort beskrivning av företaget och dess verksamhetsområde?

Telekom företag som använder moln tjänster som en plattform för att drifta våra program både till internt användning och till slutkund

4. Vilka molntjänster levererar ni?

Telekomföretag som använder moln tjänster som en plattform för att drifta våra program både till internt användning och till slutkund

5. Vad är en typisk kund för er?
a. Bransch?
b. Storlek?
c. Geografisk plats?

6. Hur många kunder har ni inom molntjänster?

Säkerhetsfrågor angående molntjänster

Q1. Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?

Jag vet inte de största, men jag räknar upp några stycken så kan vi värdera sen. Första är att man inte har full kontroll över datan, så man ligger helt i handen på backuper och hackerattacker. Beroende lite på hur molntjänsten ser ut, i vissa molntjänster typ amazon har man själv ansvar för att säkerhetspatcha sitt OS. Man får bara en tom dator men andra molntjänster som till exempel Amazon S3 storage lösning. Där man har en interface med en datorbas i molnet, där litar man mer på att det inte finns något säkerhetshål i deras API. Så den största risken är att data läcker ut, eller att det står stilla. Det kan kosta vårt företags slutskunder kan bli arga om deras tjänst inte är tillgänglig i ett längre stund.

Förebyggande arbete angående molnt tjänster

Q2. Vad gör ni för att motverka säkerhetsrisker?
Vi har en grupp som gör penetreringtester. Inte regelbundet, det sker ofta vid lansering av tjänst. Det bygger mycket på att man patchar vid varje säkerhetsuppdatering som görs. Inte den koden vi skriver utan till exempel javauppdateringar eller OS uppdateringar eller andra verktyg som man använder sig av, som till exempel frameworks.

Q3. Hur ofta gör ni säkerhetsanalyser?
Inte regelbundet som sagt men alltid innan lansering.

Q4. Vilka resurser avsätter ni i förebyggande ändamål?

Vi har även en avdelning som försöker samordna så att vi göra likadant inför varje fall men det är inte så uppstyrt som det skulle kunna vara.

Q5. Har ni ett eller flera konkreta exempel på säkerhetsbrister inom molntjänster?
a. Vad har hänt efter det för att förebygga att detta ska hända igen? och i så fall är denna process standardiserad?

Nej, inte konkreta exempel. Men man skulle kunna säga hypotetiska saker som till exempel att man har någon port öppen eller om man inte har data krypterad när man skickar datan mellan molntjänsten och företaget osv.

Q6. Har ni en processplan att följa vid allvarliga säkerhetsbrister?

Ja, det finns det.

Q7. Testar ni era system och processer för att identifiera säkerhetsbrister?

Ja, vi har försökt att börja lite med google tester. Som fungerar som så att man hittar på ett scenario. Google kör lite roligare exempel som att en Alien har tagit över New York, och då får man inte använda nån av New Yorks servrar och försöka lösa problemet i produktion. Men vi har hittat på saker, som vi har i våra stagemiljöer. Filsystemet är korrupt, läs upp allt från backup och få upp systemet så snabbt som möjligt.

Juridiska frågor

Q8. Är era servrar lokaliserade nationellt eller internationellt?

Internationellt

Q9. Beroende på vart datan är lokaliserad, finns det några juridiska aspekter som ni tar hänsyn till och i så fall hur?

Ingen aning

Q10. Vilka förebyggande åtgärder gör ni för att upprätthålla lagstiftning t.ex. PUL?

Vi har advokater som säkerhetsställer vad som får göras och inte. Speciellt är det kontrakten som är man är mest rädd för att brytas. Har man fått någonting(data), får man då man då skicka vidare det osv osv. En variant är SLA kontrakt och andra, vem vi får dela information med och inte. Ofta skriver man kontrakten på att vissa ställen få ha den här datan och även vissa molntjänster är tillräckligt säkra för att ha datan också.

Service level agreement

Q11. Använder ni standardiserade avtal med kund eller är det situationsbaserat?

Standardiserade

a. Vilka säkerhetsmässiga krav ställer ni på kunden?

b. Vilka säkerhetsmässiga krav ställer kunden på er som leverantör?

Tillgänglighet

Q12. Vilka säkerhetsrisker anser ni finns inom tillgänglighet till molntjänsten?

Helst ska man ha samma uptime som internt på företaget där kan ju strömmen gå osv. En intressant anekdot är Netflix, som har större procent uptime än vad amazon har och Netflix kör på amazon. På nått sätt har de lyckats göra det redundans så att det klarar av att har bättre SLA än sitt system under, vilket är intressant. Det handlar också om länken till molntjänsten skall vara uppe och inte för mycket belastad. Jag vet att det man kan köpa, för mycket mycket pengar en direktlänk till molntjänsten så man inte är beroende på dom som leverar så det kan vara en vettig investering. Internet och WAN är viktigt för att klara av att ha allt i molnet och att man ska kunna ta ner det till de ställena man behöver.

Q13. Vilka krav ställer era kunder på tillgänglighet till era molntjänster?

Våra end-users vill ju att våra servrar skall vara uppe 100%. De bryr sig inte om det är i molnet eller vart det ligger, vi ser mer det som en besparing att ha det i molnet för tillfället.

Q14. Vilka förebyggande funktioner har ni för att uppfylla dessa krav? (Till exempel backup eller dubbla servermiljöer)

Vet inte

Q15. Vilket förebyggande arbete har ni för att upprätthålla internetanslutning till era molntjänster? Och även strömtillförsel?

Jag vet inte riktigt hur det ser ut. Men man hade velat ha antingen två olika internetleverantörer eller ett väldigt bra SLA med bra uptime. Sen har vi batterier i källaren för att hålla uppe våra egna servrar. Vi kör inte hundra procent i molnet och inte hundra procent vårt eget, utan vi har en mix. Man måste utvärdera varje program vad de klarar av och vad som händer om de ligger nere, och helst ha en playbook, vad gör vi om det här händer.

Sekretess

Q16. Vilka säkerhetsrisker uppkommer när man säkerställer sekretess i molntjänster?

Vi sätter upp säkerhet enligt vissa projekt får inte se varandras data. Då är det kontrakt på att man inte får ta del av datan. När man är på en molntjänst så kan man ha separata servrar. Man kan också lösa det genom att ha säkerhetsgrupper. Men vill man vara helt säker så använder man firewall och sätter det på servernivå. Även när man sitter på kontoret och ska in på molntjänsten så måste man ha sin nyckel för att kunna koppla upp sig. Men de som underhåller system är trusted. Det kan man inte komma ifrån. Admins och IT-personalen är trusted people och kan läsa allt om de vill.

Q17. Vilka säkerhetsrisker anser ni finns inom området sekretess i molntjänster?

Q18. Vilka krav ställer era kunder på sekretess inom molntjänster?

Genom kontrakt och det är ju egentligen vårt företag som ska bedöma om molntjänsten är tillräckligt säker för att det är sen vi som kommer bli stämda om det läcker ut. Så det är ju en bedömning från vår sida.

Q19. Hur säkerhetsställer ni att obehöriga användare inte får tillgång till en behörig användares data?

Vi försöker ju testa vår egna säkerhet. Även så använder vi oss av specifika nycklar

a. Ställs det några säkerhetskrav på kunden vid användning era molntjänster?

Integritet

Q20. Vilka säkerhetsrisker anser ni finns inom området data integritet i molntjänster?

Ja, det var väl lite det vi var inne på innan. Äger man inte datorn så kan man ungefär vad som helst med den. Även om man krypterar det hårdaste så är det som om USA la en stationär dator i ryssland. Ryssland kan löda om processorn, eller whatever. De kommer att kunna dekryptera den datan. Så man måste ha trust på det företaget och helst skall de företaget bygga hela sin affärsidé på att de inte släpper igenom någonting.

Q21. Vilka krav ställer era kunder på data integritet?

De vill ju såklart inte att deras användarnamn och password blir offentligt. Dom har också det här, om det är känslig data som är lagrad så är det avtalat att det inte ska delas helt enkelt.

Q22. Vilka åtgärder tar ni för att säkerhetsställa (lagring av data) integritet för era kunder?

Q23. Vad händer med sparad data när en kund väljer att avsluta tjänsten?

Då ska den plockas bort.

Q24. Vilket förebyggande arbete gör ni för att information/data inte skall oväntat ändras?

Dom fil-lagrings program som vi använder är väldigt checksums beroende. Det går inte att ändra bara en fil utan att du måste datorbaser och andra checksums filer så där är en lång kedja av

checksums. Man bara sparar när checksums för en fil i en annan fil, sen har man en annan fil som har checksum på den så man bildar långa kedjor. Som gör att vi märker väldigt snabbt om det är ett fildiskproblem, att disken har ändrat någon byte eller om någon annan har varit inne och ändrat i filen. Vet man inte man inte vad man göra då så går det alarm för oss och man inte kan hämta ut filerna.

Säkerhetsfrågor angående molntjänster i samband med kunder

Q25. Anser du att era molntjänster motsvarande eller bättre säkerhet än kundernas egna system? och i så fall inom vilka riskområden?

Vi är mer användare och vi har valt ut dom som vi tror på har bra säkerhet.

Q26. Vilken insikt har kunden i ert förebyggande säkerhetsarbete?

Ingen.

Q27. Outsourcear ni någon del av er tjänst?

Ja

a. Vilken insikt har ni i tredjepartens förebyggande säkerhetsarbete?

Jag tror vi fortfarande kör för driften, men de kanske kodar.

b. Specificeras det i det avtal ni har med kund?

När man outsourchar så är det "pain in the as" man måste specifiera allt man vill ha. Man får bara det man kravställer helt enkelt. Om man inte kravställer säkerhet så får man inte säkerhet.

Q28. Upplevs det problematik vid övergång mellan olika molntjänstleverantörer?

Det hade det nog varit. Vissa ställen så kör vi Amazon , där man bara får en server. Då kör man till exempel bara en vanlig Linux server , då hade det inte varit så svårt att flytta den. Men det är ändå några specifika saker som lastbalanserar och hur deras interna nätverk ser ut och vilka ip de kör med. Varje molntjänst har ju unika tjänster för att göra deras molntjänst lite bättre än alla andras. Så det är inte smärtfritt att flytta saker och ting.

Övrigt: Har du något att tillägga, något jag har missat?

Det är ju väldigt lätt att för ett litet företag att slänga upp en världsomsträckande webbsite och har bra hastighet till många länder. Det börjar även bli billigt. Det känns som framtiden talar för molntjänster. Det har varit en väldigt chefchargong att man ska lägga allt i molnet. Vissa saker lämpar sig för molnet men man ska kanske inte lägga allt i molnet. Man ska kanske inte ha allt det hemligaste i molnet.

7.6 Transkribering Integrationsföretaget

Allmän information

1. Önskar ni att vara anonyma?

Ja

2. Namn, företag, befattning och IT-erfarenhet?

X, X, Konsult, Ja

3. Kort beskrivning av företaget och dess verksamhetsområde?

X är ett företag som består av cirka 160 anställda. Företaget fokuserar på Integration, Business Process Management och Service Oriented Architecture.

4. Vilka molntjänster levererar ni?

Ja, vi har ju faktiskt en molntjänst som vi levererar, XXXX Cloud heter den. Egentligen en integrationsplattform i molnet som du kan köpa på burk kan man säga. Istället för att du installerar en ESB i din serverhall så kan du då nytta en cloud ESB.

5. Vad är en typisk kund för er?

Nej, ingen typisk kund. Det är faktiskt vitt och brett, vanligtvis är det kunder, initialt som kanske inte har ett så stort intergrations behov. De är ibland ganska kostsamt att börja installera infrastruktur och sätta upp allting. Licenskostnaden osv, och ibland kan det vara ekonomiskt fördelaktigt att bara betala löpande månadskostnader eller bara betala för det du nyttjar istället. En ESB i sig själv är ganska kraftfull och att betala oftast då få en fullfjärd ESB då man kanske nyttjar endast en mindre del av kapciteten, så därför är moln-ESB en ganska bra deal för vissa kunder. Jag kan inte säga att det finns specifik kundgrupp som nyttjar utan initialt att de inte har så har så mycket integrationer. Det finns även kunder som har en egen ESB som nyttjar molnet för vissa tjänster. Det kan vara allt från att de inte har den funktionaliteten i sin ESB och då anroper moln-ESB för att lösa vissa problem osv.

6. Hur många kunder har ni inom molntjänster?

Jag vet inte, kanske 10-20.

Säkerhetsfrågor angående molntjänster

Q1. Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?

Problemet vi har när vi pratar molntjänster över huvudtaget är alltid är utanför din egen bandbrygga, och där är det alltid en risk. Sen har vi massa säkerhetsaspekter t.ex. om vi bortser från den molntjänsten vi har och säg att vi nyttjar en molntjänst över ett stort företag och det företaget säljs och företaget läggs ner. Då sitter du i händerna på det leverantören som du har köpt tjänsten ifrån, du är extremt känslig också om du växer dig stor på en molntjänst för prisförändringar osv, så fort du är beroende av en molntjänst så har du också ett beroende att kunna nyttja den framöver. Det är ju en säkerhetsrisk i sig själv att du blir beroende av din leverantör. Då har du tappat själva outsourcing i sig själv det blir mer som insourcing fast du har outsourcat det till en molntjänst. Sen allt annat, visst du kan sätta VPN-tunnlar i molnet och ha helsköna certifikat och sånt, men det finns ingenting som säger att molntjänsten blir komprimerad. Att man tar sig in på annat håll. Samma sätt, de som handhar själva molntjänsten kan komma åt din data.

Förebyggande arbete angående molntjänster

Q2. Vad gör ni för att motverka säkerhetsrisker?

Det handlar om att designa lösningar och titta på säkerhetscertifieringar på den datan. Vissa integrationer kanske du inte gör i en molntjänst utan de gör du i så fall inom ditt egna nätverk om det t.ex. är känslig information. Sen om vi tittar så kunde vi jobba på nyttjar på molntjänster, om inte våra så finns det en helt annan säkerhetsteknik. T.ex. har man oftast en B2B-gateway utanför sitt nätverk som får agera proxy mot molntjänsten.

Q3. Hur ofta gör ni säkerhetsanalyser?

Inte lika ofta som vi borde, man försöker alltid kolla alla fix packets för de protokoll och de produkter man kör så allt är uppdaterat och klart. Och såklart så gör vitala checkar vad som sker i miljön. Nu är det ett annat bord, jag är ju utvecklare så det är oftast infrastruktur som har hand om det. Men så fort man får reda på att det har släppts förbättring av protokoll etc så är man ju snabb med att kolla att vi ligger i fas med det.

Q4. Vilka resurser avsätter ni i förebyggande ändamål?

Nej, inte för vår interna molntjänst. Men det kanske vi borde. Det är också något vi diskuterar, så som vår molntjänst är byggd är det inte direkt byggd från säkerhetstänk utan mer leveransmodells tänk. Vi har ju ett säkerhetstänk i grunden och botten där vi kommunicerar över ett protokoll egentligen. Man sätter kommunikationsadaptrar hos kunderna som kommunicerar till och från molntjänsterna. Den är ju, kommer inte ihåg om det är SSL eller vad de använder, så öppnar man den porten i brandväggen osv. Visst, det finns ju såklart ett säkerhetstänk men kanske inte till den grad man hade velat ha.

Q5. Har ni ett eller flera konkreta exempel på säkerhetsbrister inom molntjänster?

Nej inte konkreta! I integrationsvärlden har man protokoll som stödjer uppgiften, där man egentligen får en kvittens på det man skickat, och kvittensen är ditt kvitto att det du skickade kom fram så som du skickade det. Det säger ju också till avsändaren och mottagaren att datan inte har blivit komprimerad på vägen. Det finns kommunikationsprotokoll som stödjer den typen transferingar av data med olika data och mottagare.

Q6. Har ni en processplan att följa vid allvarliga säkerhetsbrister?

Förmodligen, men det är nog infrastruktur i så fall

Q7. Testar ni era system och processer för att identifiera säkerhetsbrister?

Jag tror inte det.

Juridiska frågor

Q8. Är era servrar lokaliserade nationellt eller internationellt?

De är i ett annat land och kunderna som nyttjar den kan sitta både i samma land och i andra länder.

Q9. Beroende på vart datan är lokaliserad, finns det några juridiska aspekter som ni tar hänsyn till och i så fall hur?

Det är lite det vi pratade om innan, vissa integrationer kan man då inte nyttja molntjänsterna, det kan ha att göra med att arkivering av data och sånna typer av lagar som säger hur länge man får arkivera och var man får arkivera och vem som har rätt att komma åt den datan. Så absolut det finns viss hänsyn till det.

Q10. Vilka förebyggande åtgärder gör ni för att upprätthålla lagstiftning t.ex. PUL?

PUL berör oss inte så mycket då vi inte har så mycket persondata utan mer affärsdata i så fall. Det man gör för att försöka upprättahålla allting är att använda sig av avtal och överrenskommelser mellan de företagen som nyttjar våran tjänst och våran tjänst är up to date

hela tiden. Vi kan också nämna att den absolut största processen för oss då det handlar om cloud är den juridiska processen.

Service level agreement

Q11. Använder ni standardiserade avtal med kund eller är det situationsbaserat?

Avtal med kunden, man betalar olika för olika SLA. Det är egentligen en del av vår supportavdelning, oavsätt om du nyttjar en molntjänst eller bara köper support kan du avtala olika former av SLA.

a. Vilka säkerhetsmässiga krav ställer ni på kunden?

Ingen aning. I vårat fall så har vi hand om själva adaptern som de kommunicerar med molntjänsten. Vi har själva ansvaret. De har en POD, point on delivery, på sin sida, sen tar vi det från deras interna nätverk till våran molntjänst.

b. Vilka säkerhetsmässiga krav ställer kunden på er som leverantör?

Säkerhet, tillgänglighet och massa sånna saker. Just med integration handlar det mycket om uppe och ner tid, trueput osv.

Tillgänglighet

Q12. Vilka säkerhetsrisker anser ni finns inom tillgänglighet till molntjänsten?

Säkerhetsrisker inom tillgänglighet är ju inte mer en server någonstans. Säkerhetsrisken är ju egentligen vid strömavbrott osv, det är alltid en säkerhetsrisk. Vad som händer med meddelande. Säg att du har en transaktion och serverhallen går ner eller tvärtom outsignade system går ner. Sånna saker är alltid en säkerhetsrisk även om jag inte skulle kalla det säkerhetsrisk utan snarare en kommunikationsrisk.

Q13. Vilka krav ställer era kunder på tillgänglighet till era molntjänster?

Oftast väldigt väldigt höga. Just när vi pratar om affärsdata. Jag skulle tippa på näst in till 100% tillgänglighet

Q14. Vilka förebyggande funktioner har ni för att uppfylla dessa krav? (Till exempel backup eller dubbla servermiljöer)

Det handlar väll om att ha redundanta system och failoverlösningar. Det är egentligen ett arkitektuellt beslut kontra infrastruktur. Så att du har en infrastruktur som är redundant , i och

med att vi kör en ESB så är den failover säkrad i sig själv. Om du då kör den i en aktivaktiv miljö, där den en noden i princip skulle kunna gå ned och då du kan köra på den andra. Oftast har du dem i två olika serverhallar i två olika delar av en stad till exempel. Och om du kör i en serverhall så se alltid till ha en serverhall som är duplicerad i två olika rum som är brandsäkrade från varandra. Dom kör oftast olika typer strömförsörjning från olika leverantörer eller källor.

Q15. Vilket förebyggande arbete har ni för att upprätthålla internetanslutning till era molntjänster? Och även strömtillförsel?

Oftast har du dem i två olika serverhallar i två olika delar av en stad till exempel. Och om du kör i en serverhall så se alltid till ha en serverhall som är duplicerad i två olika rum som är brandsäkrade från varandra. Dom kör oftast olika typer strömförsörjning från olika leverantörer eller källor.

Saken är att vi är en molnleverantör som nyttjar som en annans leverantörs infrastruktur. Vi står ju egentligen bara för ena delen och det är den vi kan säkra upp. Sen får vi avtala med våran leverantör av infrastruktur. Det är egentligen de stora drakarna som har egen infrastruktur där de kan göra vad de vill hela vägen. Där vi mindre spelarna får förlita oss andra osv.

Sekretess

Q16. Vilka säkerhetsrisker uppkommer när man säkerställer sekretess i molntjänster?

Det är lite det vi va inne på innan, även om du säkrar kommunikation så finns det alltid en säkerhetsrisk med molntjänster. Vem som har access till loggar och sånna saker. Man behöver ju inte ha en intrång där vi kopplar upp oss på servern utan det kan finnas risk att det går in genom en annan ingång så att säga, kanske inte syfte att komprimera våran ESB utan snarare att komma åt något annat. Sen sekretess, det kanske blir så att integrationen inte körs i molntjänst om sekretess skall uppnås. Men sen är det som allt annat, i integrationsvärlden, se till att det är låst och att nyckel är bortappad. Sen att du har rätt nyckel för att kunna lösa datan osv. Sen är det från fall till fall, komprimera datan med olika certifikat osv, så att datan är princip oläsbar tills att du har rätt nyckel eller certifikat för att dekryptera datan. Det bygger på vanliga standarder som RSA osv.

Q18. Vilka krav ställer era kunder på sekretess inom molntjänster?

Det är jätte olika, mer fallspecifikt. Oftast har du ett avtal med en kund och sen ska du göra en integration och då får du titta på den specifika integration om man börjar prata sekretess.

Q19. Hur säkerhetsställer ni att obehöriga användare inte får tillgång till en behörig användares data?

a. Ställs det några säkerhetskrav på kunden vid användning era molntjänster?

Men sen är det som allt annat, i integrationsvärlden, se till att det är låst och att nyckel är bortappad. Sen att du har rätt nyckel för att kunna lösa datan osv. Sen är det från fall till fall, komprimera datan med olika certifikat osv, så att datan är princip oläsbar tills att du har rätt nyckel eller certifikat för att dekryptera datan. Det bygger på vanliga standarder som RLA osv.

Integritet

Q20. Vilka säkerhetsrisker anser ni finns inom området data integritet i molntjänster?

Datan försvinner från ett ställe till nån annanstans. Det är väll det som är den största problematiken, så som juridiken. Att datan inte är i dina lokaler eller vad man säger.

Q21. Vilka krav ställer era kunder på data integritet?

Ingen aning, men förmodligen fallspecifikt där också.

Q22. Vilka åtgärder tar ni för att säkerhetsställa (lagring av data) integritet för era kunder?

Från fall till fall, men jag skulle tippa på att i själva integartionsplattformen så ska det vara svårt att spåra.

Q23. Vad händer med sparad data när en kund väljer att avsluta tjänsten?

Bra fråga, vet inte. Vet inte hur mycket som sparas.

Q24. Vilket förebyggande arbete gör ni för att information/data inte skall oväntat ändras?

Det är det som själva nyckeln med integrationsplattform att man faktiskt ändrar data. Men jag förstår vad du menar men jag vet inte.

Säkerhetsfrågor angående molntjänster i samband med kunder

Q25. Anser du att era molntjänster motsvarande eller bättre säkerhet än kundernas egna system? och i så fall inom vilka riskområden?

Det är en väldigt bra fråga, det vi ser hos kunder är att det finns oftast bara ett säkerhetstänk och det är att allt innanför brandväggarna är säkert. Kan väll tycka att våran molntjänst har ett bättre

säkerhetstänk då vi säkrar data i flera led istället. Vanligtvis hos en kund så går man och pratar med nätverksteknikerna så säger de nej till allting som handlar om att öppna en brandvägg för kommunikation utifrån. Men innanför brandväggen så är det oftast inget säkerhetstänk.

Q26. Vilken insikt har kunden i ert förebyggande säkerhetsarbete?

Förmodligen ingen.

Q27. Outsourcear ni någon del av er tjänst?

Ja, själva infrastrukturen.

a. Vilken insikt har ni i tredjepartens förebyggande säkerhetsarbete?

Nej, inte mer avtalsmässigt. Vilka krav vi ställer, men om de uppfyller dessa krav kan man inte veta säkert.

b. Specificeras det i det avtal ni har med kund?

Ja

Q28. Upplevs det problematik vid övergång mellan olika molntjänstleverantörer?

I våran tjänst kan det gå väldigt smärtfritt då vi står för själva kommunikation till och från molntjänsten. Men jag vet fall där man har bytt till olika molntjänstleverantörer och designar man sin lösning för att det ska kunnas byta ut så är det ganska oproblematiskt men gör man inte det inte så är det extremt problematiskt och väldigt kostsamt. Om man designar sin lösning för explicit använda en specifik så sitter man i händerna på den sen, det är därför det är, enligt mig en säkerhetsrisk att göra så.

7.7 Transkribering Knowit Cloud Innovation

Allmän information

1. Önskar ni att vara anonyma?
Nej

2. Namn, företag, befattning och IT-erfarenhet?
Ola Hesselroth CEO och Johan Berneskog CXO, Knowit Cloud Innovation, båda med ~20 års IT-erfarenhet

3. Kort beskrivning av företaget och dess verksamhetsområde?

Innovation by using the Cloud

By using cloud technology Knowit helps companies to deliver highly innovative services based on Amazon Web Services and Microsoft Azure. The intention is to be a strategic advisor around strategy and the cloud. Based on the strategy a number of services are available in order to gradually help customers to transform their business to the cloud by assisting in migration, enabling new environments, optimizing the processes and establishing operations in a cost-effective way.

4. Vilka molntjänster levererar ni?

The following services are offered:

Cloud Strategy

Cloud Movement & Enablement

Cloud Optimized DevOps

Cloud Operations

Cloud Solutions

Storage

Backup

Disaster/Recovery

Networking

Big Data

Application Performance Monitoring (APM)

5. Vad är en typisk kund för er?

a. Bransch?

b. Storlek?

c. Geografisk plats?

Bolag som är utvecklingsintensiva och som börjar i molnet

Bolag som har existerande system och som vill förflytta sig till molnet

6. Hur många kunder har ni inom molntjänster?

Ca 25

Säkerhetsfrågor angående molntjänster

Q1. Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?

Felaktig arkitektur

Felaktig kommunikation och nätinfrastruktur

Felaktig autentisering

Förebyggande arbete angående molntjänster

Q2. Vad gör ni för att motverka säkerhetsrisker?
Innan vi tar ansvar för att drifta en lösning så gör vi en granskning av arkitektur, kommunikation, nätuppsättning och lösning för autentisering.

Q3. Hur ofta gör ni säkerhetsanalyser?
Initialt vid uppsättning och löpande vid större förändringar.

Q4. Vilka resurser avsätter ni i förebyggande ändamål?
Löpande bevakning av nya funktioner/patchar som kan påverka befintliga lösningar.

Q5. Har ni ett eller flera konkreta exempel på säkerhetsbrister inom molntjänster?

Nej

a. Vad har hänt efter det för att förebygga att detta ska hända igen? och i så fall är denna process standardiserad?
N/A

Q6. Har ni en processplan att följa vid allvarliga säkerhetsbrister?

Ja

Q7. Testar ni era system och processer för att identifiera säkerhetsbrister?
Vid behov görs penetrationstester och lasttester.

Juridiska frågor

Q8. Är era servrar lokaliserade nationellt eller internationellt?
Vi har inga egna servrar utan använder de globala molnleverantörerna Amazon AWS och Microsoft Azure.

Q9. Beroende på vart datan är lokaliserad, finns det några juridiska aspekter som ni tar hänsyn till och i så fall hur?
Svensk lagstiftning är enhetlig med EU:s lagstiftning och så länge de globala molnleverantörernas datacenter finns inom EU är det inga problem.

Amazon AWS har datacenter på Irland & Frankfurt medan Microsoft Azure har datacenter på Irland & Amsterdam.

Q10. Vilka förebyggande åtgärder gör ni för att upprätthålla lagstiftning t.ex. PUL?
Det är kunden som äger sin data och vi tillhandahåller en plattform för att köra applikationer eller lagra data.

Service level agreement

Q11. Använder ni standardiserade avtal med kund eller är det situationsbaserat?
Alla avtal baseras på standardavtal från IT & Telekomföretagen.

a. Vilka säkerhetsmässiga krav ställer ni på kunden?
Kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.

b. Vilka säkerhetsmässiga krav ställer kunden på er som leverantör?
Kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.

Tillgänglighet

Q12. Vilka säkerhetsrisker anser ni finns inom tillgänglighet till molntjänsten?
Felaktig arkitektur

Val av fel leverantör. Ofta väljs t.ex. väljs antingen Amazon eller Azure, medan det bästa är en Multi-Cloudlösning där olika leverantörer används för det de är bäst på.

Q13. Vilka krav ställer era kunder på tillgänglighet till era molntjänster?
Vi erbjuder 99,8%

Q14. Vilka förebyggande funktioner har ni för att uppfylla dessa krav? (Till exempel backup eller dubbla servermiljöer)
En väl genomtänkt molnarkitektur med inbyggd redundans

Q15. Vilket förebyggande arbete har ni för att upprätthålla internetanslutning till era molntjänster? Och även strömtillförsel?
Vi har inga egna molntjänster utan använder de globala molnleverantörerna Amazon AWS och Microsoft Azure.

För till exempel kommunikationen mot AWS kan redundanta linor användas i form av DirectConnect som primär lina och VPN som fail over.

Sekretess

Q16. Vilka säkerhetsrisker uppkommer när man säkerställer sekretess i molntjänster?
Sekretess på molninfrastruktur- & plattformsnivå kan säkerställas via kryptering av data och säker inloggning.

Sekretess på Applikationsnivå är inte specifikt för molnet utan för den applikation som hanterar informationen och vem som kan komma åt den.

Q17. Vilka säkerhetsrisker anser ni finns inom området sekretess i molntjänster?

Sekretess på molninfrastruktur- & plattformsnivå kan säkerställas via kryptering av data och säker inloggning.

Sekretess på Applikationsnivå är inte specifikt för molnet utan för den applikation som hanterar informationen och vem som kan komma åt den.

Q18. Vilka krav ställer era kunder på sekretess inom molntjänster?

Sekretess på molninfrastruktur- & plattformsnivå kan säkerställas via kryptering av data och säker inloggning.

Sekretess på Applikationsnivå är inte specifikt för molnet utan för den applikation som hanterar informationen och vem som kan komma åt den.

Q19. Hur säkerhetsställer ni att obehöriga användare inte får tillgång till en behörig användares data?

Sekretess på molninfrastruktur- & plattformsnivå kan säkerställas via kryptering av data och säker inloggning.

Sekretess på Applikationsnivå är inte specifikt för molnet utan för den applikation som hanterar informationen och vem som kan komma åt den.

a. Ställs det några säkerhetskrav på kunden vid användning era molntjänster?

Kvalificerad personal, säker hantering av tillträde till lokaler, information om miljöer och inloggningsuppgifter.

Integritet

Q20. Vilka säkerhetsrisker anser ni finns inom området data integritet i molntjänster?

Felaktig eller obefintlig Backuplösning

Q21. Vilka krav ställer era kunder på data integritet?

Backup ingår som standard i alla lösningar

Q22. Vilka åtgärder tar ni för att säkerhetsställa (lagring av data) integritet för era kunder?
Regelbundna tester tillsammans med kund.

Q23. Vad händer med sparad data när en kund väljer att avsluta tjänsten?
All lagrad data tas bort om inte kunden vill att den lagras under ytterligare en period.

Q24. Vilket förebyggande arbete gör ni för att information/data inte skall oväntat ändras?
Regelbunden kontroll av rutiner för lagring och backup.

Säkerhetsfrågor angående molntjänster i samband med kunder

Q25. Anser du att era molntjänster motsvarande eller bättre säkerhet än kundernas egna system? och i så fall inom vilka riskområden?
De globala molnleverantörerna såsom Amazon AWS och Microsoft AWS är mycket säkrare än att ha driften on-premise eller hos en lokal partner.

Säkerhet är dyrt och de globala leverantörerna investerar stora summor i säkerhet och där även regionala spelare såsom Tieto och CGI inte kan hänga med.

Q26. Vilken insikt har kunden i ert förebyggande säkerhetsarbete?
Full transparens

Q27. Outsourcear ni någon del av er tjänst?
Ja, för Cloud Operations använder vi en partner i Indien

a. Vilken insikt har ni i tredjepartens förebyggande säkerhetsarbete?
Full transparens.

b. Specificeras det i det avtal ni har med kund?
Ja

Q28. Upplevs det problematik vid övergång mellan olika molntjänstleverantörer?
Nej! Vi har hjälpt kunder att flytta lösningar från Microsoft Azure till Amazon AWS pga av prestandan i Microsoft Azure inte räckte till.

7.8 Transkribering Systemutvecklingsföretaget

Allmän information

1.Önskar ni att vara anonyma?

Ja

2.Namn, företag, befattning och IT-erfarenhet?

Befattning är väl systemutvecklare/Account manager. Erfarenhet, ja hur lång tid är det nu. Det är väl nästan 3 år. Så säg 2,5 då. Sedan tre års akademisk utbildning.

3.Kort beskrivning av företaget och dess verksamhetsområde?

Tar företaget i dess korthet då och då är vi ju design och digitals som är huvudområdet för oss i min sektor då,företaget har ju så många olika sektorer. Vi ligger ju lite mellan, vad kan man säga, webb-byrå och teknik.

4.Vilka molntjänster levererar ni?

Du tänker på Software as a Service då. Det enda vi har då på vårt kontor är ticketing system. Så det är bara en tjänst.

5.Vad är en typisk kund för er?
a.Bransch?
b.Storlek?
c.Geografisk plats?

Det är faktiskt helt oberoende av det egentligen. Just nu finns det ju bara i Sverige, eftersom att ticketing är för deras webbplatser så spelar det inte så stor roll för vilken bransch det är i. Just nu i det här så har vi Automotive alltså bilbranschen. Alltså både återförsäljare och varumärkena. Så har vi även från en del från kommunal sektor, alltså från kommun och landsting.

6. Hur många kunder har ni inom molntjänster?

5-6 st

Säkerhetsfrågor angående molntjänster

Q1. Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?

Alltså den största säkerhetsrisken som man har... Svårigheten med det är liksom informationssäkerheten och informationsklassificeringen. Alltså då när vet man vad som är känslig information. Hur kan man veta om informationen är känslig eller inte. Klassificeringen av information. Det är väl dom största säkerhetsriskerna. Att man inte vet. Om man inte vet så blir den här mänsliga faktorn så mycket mer extrem. Så den största risken är ju då framförallt den mänskliga faktorn blir kontentan av det då.

Förebyggande arbete angående molntjänster

Q2. Vad gör ni för att motverka säkerhetsrisker?

Just när det kommer till den mänskliga faktorn. En sak är ju att man kollar på rättighetsnivåer. Så ju bättre man kan klassificera informationen, ju bättre kan man ju veta vem som får se vad. Då kollar man på behörigheter. Alltså att alla inte ska få behörighet och kunna se och hantera vad som helst. Då har man ju gjort en liten motverkan i alla fall. En person som inte kan så mycket kan inte göra fel. Han kan inte och får inte tillgång till att göra fel. Det andra är ju då auditing. Att man ser vem som har gjort vad, vem som har kollat vad.

Q3. Hur ofta gör ni säkerhetsanalyser?

Ehm, vi har ju inget sånt som vi gör rutinmässigt, har vi ju inte. Alltså varannan vecka så kollar vi detta och gör detta. Utan det är nog lite mer när det behövs. Nu ser vi mycket aktiviteter kring detta och nu borde vi granska lite närmare vad som faktiskt händer. Uppdateringar och så vidare.

Q4. Vilka resurser avsätter ni i förebyggande ändamål?

Det sköter vi internt. Ehm, vi har lite olika nivåer i olika arbetsgrupper. Vi har en arbetsgrupp som bara sköter patchning av servern. Patchning av servern, det är alltså då linuxbaserad server det ligger på, då kommer hela tiden säkerhetsreleaser och sånt till Linux så då har vi en arbetsgrupp som har koll på det. Det är ju inte bara för det här systemet utan det är för alla servrar. Sen har vi en annan arbetsgrupp när du kommer till mjukvaran. Dvs .. som det bygger på när du säkerhetspatchat den så uppgraderas det automatiskt. Sen har vi då en arbetsgrupp för just det här systemet som kollar loggar och likande. Sen har vi då utöver detta alltid internrevisioner där vi har först då en intern person från ett annat bolag men samma koncern som gör en intern säkerhetsrevision på hela vårat bolag. Sen har vi en kund som jag inte ska nämna vid namn som är ganska hårda när det gäller säkerhet och dom gör också säkerhetsrevisioner på vårt företag. Men då är det sett på företaget i sin helhet och inte enbart det här systemet. Men systemet är ju en del av den säkerhetsrevision som görs då.

Q5. Har ni ett eller flera konkreta exempel på säkerhetsbrister inom molntjänster?

Ja det finns ju flera. En sak är ju att om man inte uppdaterar servern eller mjukvaran så kan man ju råka ut för automatiserade hackningar. Det har ju hänt oss. Vi åtgärdade det ganska snabbt men då var det ju liksom att man är någon dag sen med att uppdatera säkerhetspatch som har kommit till mjukvaran så har det blivit exploitat och så är det en tysk server som bara hackar mjukvaran på en gång då för det är ju en botserver som bara spindlar igenom nätet och försöker hacka.

a. Vad har hänt efter det för att förebygga att detta ska hända igen? och i så fall är denna process standardiserad?

Det var ju redan standardiserat sen innan då bara fick man en liten ögonöppnare för att man ska vara lite snabbare när det kommer till patchningen.

Q6. Har ni en processplan att följa vid allvarliga säkerhetsbrister?

Nej det har vi inte. Vi har ju så att vi sparar alltså daily backups och sånt så att man alltid kan återställa och liknande. Men vi har ingen specifik säkerhetsplan det har vi inte.

Q7. Testar ni era system och processer för att identifiera säkerhetsbrister?

Juridiska frågor

Q8. Är era servrar lokaliserade nationellt eller internationellt?

I Sverige.

Q9. Beroende på vart datan är lokaliserad, finns det några juridiska aspekter som ni tar hänsyn till och i så fall hur?

Nej

Q10. Vilka förebyggande åtgärder gör ni för att upprätthålla lagstiftning t.ex. PUL?

Nej

Service level agreement

Q11. Använder ni standardiserade avtal med kund eller är det situationsbaserat?

Nej utan det här är alltså en gratistjänst som vi förmedlar till kunden som förvaltningsåtagande av oss. Så därför har vi inte heller ett SLA gällande det här systemet.

a. Vilka säkerhetsmässiga krav ställer ni på kunden?

Nej inte på det här systemet.

b. Vilka säkerhetsmässiga krav ställer kunden på er som leverantör?

Nej inte på det här systemet.

Tillgänglighet

Q12. Vilka säkerhetsrisker anser ni finns inom tillgänglighet till molntjänsten?

Alltså grejen är att det är nog inte riktigt identifierat eftersom att det inte är så kritisk information. Hade det legat nere en dag så hade det inte varit the end of the world eftersom att det är gratis.

Q13. Vilka krav ställer era kunder på tillgänglighet till era molntjänster?

Alltså grejen är att det är nog inte riktigt identifierat eftersom att det inte är så kritisk information. Hade det legat nere en dag så hade det inte varit the end of the world eftersom att det är gratis.

Q14. Vilka förebyggande funktioner har ni för att uppfylla dessa krav? (Till exempel backup eller dubbla servermiljöer)

Dubbla servermiljöer har vi inte. Backups har vi. Så vi tar alltid daily backups för att kunna roll-backa på. Sen har vi ju en SLA med vår serverleverantör och dom garanterar ju 99.47% uptime tror jag. Vi har sagt att det är bra nog för oss då.

Q15. Vilket förebyggande arbete har ni för att upprätthålla internetanslutning till era molntjänster? Och även strömtillförsel?

Nej det gör vi inte utan det är samma. Det sköter vår leverantör helt och hållet.

Sekretess

Q17. Vilka säkerhetsrisker anser ni finns inom området sekretess i molntjänster?

I vårt system ligger alla data i samma databas och samma tabeller. Det vill säga att om det blir något logiskt fel där när man hämtar upp data så finns det ju risk för att kunder kan komma åt andra kunders data. Så det är ju en jätterisk.

Q18. Vilka krav ställer era kunder på sekretess inom molntjänster?

I det här ställer dom inga krav. Men det tror jag mest beror på att kunden i sig är ovetande om riskerna som finns.

Q19. Hur säkerhetsställer ni att obehöriga användare inte får tillgång till en behörig användares data?

Det sköts på en ren logisk nivå. Så då har vi ett antal säkerhetslager i applikationen som alltid mappar mot detta då.

a. Ställs det några säkerhetskrav på kunden vid användning era molntjänster?

Nej som tidigare görs inte detta.

Integritet

Q20. Vilka säkerhetsrisker anser ni finns inom området data integritet i molntjänster?

Det är väl lite samma som sekretess. Om kunden skulle kunna få tillgång till en annan kunds data så är ju det inte bra. För kunden har ju i viss mån rättigheter till att editera data i ett visst ärende. Då har vi ju förebyggande åtgärder i form av en ändringslogg. När kunden gör en editering av information så loggas det i form av vad som editerats och av vem. O andra sidan finns det andra risker som XSS och SQL-injections. Just dom två är ju stora risker. Cross server scripting kan vara svårt att upptäcka och när det har upptäckts så kan det vara för sent att göra en roll-back. Beroende på vad det är för SQL-injections så beror det på vad det är för typ men vissa kan ju bara rensa datan och då är det ju backup som gäller som säkerhetsåtgärd. Men vissa kan även läsa datan och tar sig in på det hackade viset så finns det ju inget sett att upptäcka det utan då är man ju körd.

Q21. Vilka krav ställer era kunder på data integritet?

Q22. Vilka åtgärder tar ni för att säkerhetsställa (lagring av data) integritet för era kunder?

Q23. Vad händer med sparad data när en kund väljer att avsluta tjänsten?

Datan ligger kvar precis som den är. Vi rör inte datan men vi kopplar bort alla konton så att ingen har rätt att få tillgång till datan. Administratörer, och det är bara vi på företaget som är

administratörer, har ju rätt att ge oss själva rättigheter. Vi kan ju alltid gå in i efterhand och kolla på data från gamla ärenden från kunder som inte finns längre. Men den finns kvar och tas inte bort.

Q24. Vilket förebyggande arbete gör ni för att information/data inte skall oväntat ändras?
Backup, behandlingssytem och loggning

Säkerhetsfrågor angående molntjänster i samband med kunder

Q25. Anser du att era molntjänster är motsvarande eller bättre säkerhet än kundernas egna system? och i så fall inom vilka riskområden?
Det beror ju helt på vilka system man ska jämföra med Vi har ju kunder från så många olika branscher. Den är helt okej men den är inte extraordinär eftersom att det inte så känslig data som hanteras. Oftast så är informationen vi pratar om information vid angrepp inte hade gjort så mycket om den blev publik. Så därför är inte säkerheten så extrem. Så många av våra kunders egna system är ju brutala i jämförelse när det kommer till säkerhet och vissa är sämre. Så att jämföra med ett konsultbolag och inte ett renodlat molntjänstföretag så är både och.

Q26. Vilken insikt har kunden i ert förebyggande säkerhetsarbete?
För det här systemet specifikt så har dom inte direkt någon insikt alls. Men som oss som verksamhet så har har vissa kunder ingen alls och vissa jättegod insikt. Det beror lite på kraven som kunden har.

Q27. Outsourcear ni någon del av er tjänst?
Nej.
a. Vilken insikt har ni i tredjepartens förebyggande säkerhetsarbete?
b. Specificeras det i det avtal ni har med kund?

Q28. Upplevs det problematik vid övergång mellan olika molntjänstleverantörer?
Det har vi inte råkat ut för. Men vi har ingen utarbetad tjänst för dataexport utan då är det något manuellt som vi själva får göra vid uthämtning av data. Så det är väl lite speciellt att man får be oss att gå in och hämta ut datan istället för att ta ut det själva då.

7.9 Transkribering Affärssystemsleverantören

Allmän information

1. Önskar ni att vara anonyma?
Ja

2. Namn, företag, befattning och IT-erfarenhet?
Jag jobbar ju då på driften inom företaget och min utbildning var på Jönköpings Tekniska Högskola från början för två och ett halvt år sedan ungefär och gick ut datanätteknik vilket var nätverksinriktat men även drift/service-inriktad utbildning. Jag jobbade efter Jönköping ett år på ett företag här i Växjö som heter Boss Media som jobbade med online/nätcasino och där jobbade jag också med drift och sen gick jag hit för ett och ett halvt år sedan till detta företaget där jag är nu. Här jobbar jag ju också då med drift och produktionsdrift. Ja det vi gör egentligen är att vi ser till att alla servrar fungerar som dom ska och att vår programvara snurrar. Vi löser lite dagliga problem och håller uppe patchnivåer och annat. Det är väl det dagliga drift. Det är ju inte interndrift vi arbetar med utan det har vi en separat avdelning för.

3. Kort beskrivning av företaget och dess verksamhetsområde?

4. Vilka molntjänster levererar ni?
Vi jobbar ju då med bokföring på webben så det primära är ju uppenbarligen då bokföring men vi har ju även funktioner för lönehantering, fakturering alltså affärssystem är det egentligen vi levererar som en molntjänst. Det kan man väl säga

5. Vad är en typisk kund för er?
a. Bransch?
b. Storlek?
c. Geografisk plats?

Det är rätt svårt att svara på. Vi har rätt många kunder men vi riktar ju oss till småföretagare framförallt. Jag skulle ju vilja säga att standardkunden är typ en liten hantverkarfirma med ett par anställda. Vår största kundkrets är väl här i södra Sverige men även över hela landet egentligen.

6. Hur många kunder har ni inom molntjänster?

Lite drygt 100,000

Säkerhetsfrågor angående molntjänster

Q1. Vad anser du är de största säkerhetsriskerna vid användning av molntjänster?

Jag skulle säga att det är egentligen en kombination av okunskap från användare med dåliga mjukvaror eller inte dåliga men gamla mjukvaror och dåliga lösenord. Det finns.. Jag tycker att kunskapen från användaren är den största risken som jag ser det för att vi kan ju göra ganska mycket för att säkra upp våra system. Men det hjälper inte när användaren inte är försiktig med sina lösenord och sin personliga data. Det skulle jag säga är de största riskerna vid användning av molntjänster. Som kund att man inte har koll på var säkerhetsriskerna ligger någonstans för man är noga med att låsa sitt hus men när det gäller lösenorden till sin bokföring har man inte riktigt samma koll.

Förebyggande arbete angående molntjänster

Q2. Vad gör ni för att motverka säkerhetsrisker?

Vi har ett ganska omfattande förebyggande arbete ….-testning, alltså penetrationstestning varje år och då är det ett externt företag som vi hyr in som får tillgång till vår mjukvara och källkod. Då kör dom sin säkerhetsanalys av det då. Vi patchar även väldigt aktivt och håller oss allmänt uppdaterade med det som händer I IT-världen med de back-end-systemen vi använder för att hålla alla patchnivåer uppe skulle jag säga.

Q3. Hur ofta gör ni säkerhetsanalyser?

Vi kör en stor säkerhetsanalys varje år en gång om året. Det är det stora grejen vi har. Sen brukar vi ha lite mindre grejer för specifika delar av systemet men det kan vara lite oregelbundet när det dyker upp då.

Q4. Vilka resurser avsätter ni i förebyggande ändamål?

Det är lite svårt att svara på. Vi på driften jobbar ju egentligen alltid mer eller mindre med säkerhetsarbete. Sen kan vi ha grupper, vi har ju 25 programmerare och där kanske vi har ett par programmerare som är mer säkerhetsinriktade eller som jobbar med dom bitarna mer specifikt när det kommer upp. Så det är svårt att svara på. Vi har en intern IT-avdelning och dom jobbar ju också med säkerhet men det är en annan typ av säkerhetsarbete dom pysslar med. Men jag skulle

väl säga att vi har 3-4 personer som jobbar till och från med säkerhetsfrågor, relaterat till molnbitarna.

Q5. Har ni ett eller flera konkreta exempel på säkerhetsbrister inom molntjänster?

a. Vad har hänt efter det för att förebygga att detta ska hända igen? och i så fall är denna process standardiserad?

Jag har svårt att svara på den frågan specifikt. Alltså, okunskap från programmerare kan vara en stor brist. Om dom programmerarna inte förstår hur våra system fungerar i produktionen i praktiken och hur det är uppsatt. Sådana saker kan leda till brister, att man inte har koll på liksom input från användare och sådana saker. Sånt kan leda till problem liksom, alltså det är ju inte medvetna saker det är mer buggar eller att man är omedveten om att "okej jag kodade såhär och det var säkert och jag gjorde det på min burk när jag satt och kodade för mig själv". Men sen när man har flera användare och kunder som är inne som kan komma åt, komma åt varandras grejer eller sådana här saker. Jag skulle säga att okunskap är en ehm en risk egentligen.

Q6. Har ni en processplan att följa vid allvarliga säkerhetsbrister?

Vi har tagit fram en krishanteringsplan egentligen men den är egentligen inte specifikt för kanske säkerhetsbrist i den bemärkelsen utan mer en allmän krishanteringsplan om en större grej händer. Det kan ju vara så att vi får en store driftstörning, att systemen inte går att nå då. Men det finns en krishanteringsplan på plats det gör det.

Q7. Testar ni era system och processer för att identifiera säkerhetsbrister?

Juridiska frågor

Q8. Är era servrar lokaliserade nationellt eller internationellt?

Dom är lokaliserade nationellt. Dom är lokaliserade här i Växjö där vårt företag ligger.

Q9. Beroende på vart datan är lokaliserad, finns det några juridiska aspekter som ni tar hänsyn till och i så fall hur?

Anledningen till att vi gjorde det var just för att undvika juridiska problem med bokföringsdata då. Det finns en del motsägande lagar liksom PUL säger ju då att okej ja men data måste finnas i Sverige och hej och hå. Sen har du bokföringslagen som är lite mer öppen att bokföringsdata får finnas inom EU då och sådana grejer då men dom talar ju emot varandra lite så vi tog det säkra kortet och körde servrarna lokalt.

Q10. Vilka förebyggande åtgärder gör ni för att upprätthålla lagstiftning t.ex. PUL?
Det som jag nämnde innan är de förebyggande åtgärder som vi tar då.

Service level agreement

Q11. Använder ni standardiserade avtal med kund eller är det situationsbaserat?
Ja den är lite speciell för vi har egentligen, man kan säga att vi har två typer av kunder. Vi har dels den vanliga kunden, en liten firma som köpt program direkt från oss. Sen så jobbar vi även med redovisningsbyråer alltså LRF och Grant Thornton och alla dom här. Och mot dom, då är det ju en stor kund som köper in vårt system för att deras kunder skall använda det. Mot dom så har vi specialiserade avtal. Mot den vanliga kunden som beställer direkt av oss där har vi ett standardavtal för alla.

a. Vilka säkerhetsmässiga krav ställer ni på kunden?

Det största kravet vi ställer egentligen är att kunden har en modern webbläsare. För det är en av dom säkerhetsbrister som vi har identifierat. En gammal webbläsare, dels är det jobbigt för oss att få våra system att fungera I gamla webbläsare. Vi vill ju liksom ligga långt fram I tekniken och av säkerhetsskäl så kräver vi att kunden, aa använder en, två tre år sen är det för gammalt liksom Vi later dom inte ens logga in I systemet om dom använder en gammal webbläsare.

b. Vilka säkerhetsmässiga krav ställer kunden på er som leverantör?

Som sagt två typer av kunder. Den vanliga kunden ställer inte så höga krav. Dom använder systemet och funderar inte på det så mycket tills det händer något. Det skulle jag tro har att göra med okunskap. Däremot våra byråer har betydligt högre säkerhetskrav. Det är ju liksom större företag. Dom gör även aktiva penetrationstester mot oss utan att berätta det för att liksom testa vår säkerhet. Så dom har väldigt höga krav.

Tillgänglighet

Q12. Vilka säkerhetsrisker anser ni finns inom tillgänglighet till molntjänsten?

Jag upplever I alla fall att man ofta överdimensionerar dom failsafes som skall finnas på plats för att skydda tjänsten. För mycket säkerhet och redundans kan ibland vara kontraproduktivt och leda till att det faktiskt blir problem istället för att sådana avancerade system bara för att hålla det uppe då. Så det är väl en risk som jag kan se inom tillgänglighet som finns. Men sen även okunskap, att man tror att redundansreplikering att det är liksom backup men det är det liksom

inte för att stör någon datan så skickas ju till andra till platsen då. Så tillgänglighet är ett stort område men jag tycker att vi lyckas bra med det.

Q13. Vilka krav ställer era kunder på tillgänglighet till era molntjänster?

Den uppkopplade världen vi lever I idag så väldigt höga. I och med att vi har så många kunder också, många små kunder, alltså en driftstörning för oss påverkar väldigt många. Idag förväntar man sig att allt ska var online om man reser utomlands och gör underhåll på nätter och sådana saker är inte heller helt självklart för oss. För det kan ju vara dag någon annanstans då. Så jag skulle säga att det är mycket höga krav på tillgänglighet.

Q14. Vilka förebyggande funktioner har ni för att uppfylla dessa krav? (Till exempel backup eller dubbla servermiljöer)

Ja, vi kör ju då med dubbla datorhallar. Där vi replikerar egentligen våra, vad ska man säga, disken replikeras rakt över till den andra hallen då. Så har vi samma uppsättning servrar där och skulle vi behöva göra ett överslag så stänger vi ner ena hallen och startar upp i den andra då.

Q15. Vilket förebyggande arbete har ni för att upprätthålla internetanslutning till era molntjänster? Och även strömtillförsel?

Vi har dubbla internetlinor till båda datorhallarna från olika leverantörer.

Sekretess

Q17. Vilka säkerhetsrisker anser ni finns inom området sekretess i molntjänster?

Det går ihop lite med integritetsfrågorna där kanske. Men det man kan säga egentligen är att de åtgärder som vi åtagit är att varje kund har en egen unik databas. Vi delar inte kundens data i samma databas utan alla har en isolerad databas på liksom servernivå eller i alla fall.. Databasen är isolerad helt enkelt. Men det, det som jag kan tycka är svårt är att det är att du ska hitta en balansgång mellan support, techsupport och liksom kunddata. För om du har en kund som ringer in och har problem då behöver ju supporten logga in på kundernas databaser naturligt då se deras data. Eller om det är en programbugg då måste man kanske dumpa ner kundens data och låta utvecklare titta runt i databasen då. Det man kan göra för att undvika sådana saker är att man kan ju köra scramblers egentligen som när databas dumpas så suddar du allt och ersätter med bubble men det är ju inte alltid lätt att felsöka då heller om det är en specifik grej. Det är väl en svår

balansgång att hitta egentligen. Men kunderna i sig har ju väldigt höga krav på den här datan för att det är bokföringsdata. Det får ju inte läcka ut.

Q18. Vilka krav ställer era kunder på sekretess inom molntjänster?

Ja, jag vet inte. Jag har lite svårt att svara på det. Självklart ställer ju kunderna krav på att data inte ska läcka ut, den ska vara hemlig. Det är ju faktiskt bokföringsdata. Det uppfyller vi ju absolut. Vi tar ju inte den här datan till externa företag för att göra någon kundanalys för att göra någon reklam eller något annat. Just eftersom att det handlar om bokföringssystem och affärssystem så är kraven höga, det är dom verkligen.

Q19. Hur säkerhetsställer ni att obehöriga användare inte får tillgång till en behörig användares data?
a. Ställs det några säkerhetskrav på kunden vid användning era molntjänster?

Ja det finns väl egentligen två typer av kategorier som man vill säkerhetsställa. Dels är det fysisk tillgång och digital tillgång. Den fysiska tillgången är lätt då vi har väldigt låsta datahallar. Vi använder en driftpartner som har hand om hallarna och dom har väldigt solida system på plats som ser till att inte obehöriga kan komma åt den hallen rent fysiskt då. Vi här uppe använder ju lösenordsskyddade system och rättighetsbaserade system också då för att se till att obehöriga användare inte kommer åt fel typ av data då. Men som jag nämnde tidigare så är det svårt att hitta en balans med vem som ska ha tillgång till vad och vem behöver tillgång till vad i vardagen för att det ska fungera i förhållande till sekretess och integritet. Det är väl egentligen vår interna IT-avdelning som ska hantera dom bitarna alltså vem som ska ha tillgång till specifika system. Men vi på driften har blivit dom som i praktiken hanterar tillgången till produktionssystemen och till kunddata egentligen. Det är ju vi som styr vilka som har möjlighet att till exempel dumpa ner en kunddatabas för att felsöka någonting eller något sådant där. Det är vår avdelningschef som styr dom delarna

Integritet

Q20. Vilka säkerhetsrisker anser ni finns inom området data integritet i molntjänster?

Samma som sekretess.

Q21. Vilka krav ställer era kunder på data integritet?

Men kunderna I sig har ju väldigt höga krav på att integriteten på den här datan I och med att det är bokföringsdata, det får ju inte manipuleras ska ju vara helt solid. Vi har även ganska omfattande eller väldigt omfattande behandlingshistorik. Varje gång en kund gör en ändring eller bokför någonting så sparas det liksom I ett separat system som sparar alla ändringar allt som händer i programmet. Om en kund ringer och säger att ”Aa men hej den här fakturan har blivit bokförd men jag har inte klickat. Vad är det som har hänt?” Då kan vi gå in och kolla i behandlingshistoriken och kolla vilken användare i systemet och vad som gjorde vad. Så det är ju en av dom systemen vi har på plats för att säkerhetsställa att integritet behålls eller att man kan spåra vem som gjort vad med datan då.

Q22. Vilka åtgärder tar ni för att säkerhetsställa (lagring av data) integritet för era kunder?

Samma som sekretess.

Q23. Vad händer med sparad data när en kund väljer att avsluta tjänsten?

Det är också ett sånt fall där PUL och bokföringslagen skär i varandra lite grann. För en av lagarna säger att spara bokföringsdata i sju år. Så som vi har gjort det är att vi sparar datan i två månader om kunden vill komma tillbaka, sen raderar vi den

Q24. Vilket förebyggande arbete gör ni för att information/data inte skall oväntat ändras?

Säkerhetsfrågor angående molntjänster i samband med kunder

Q25. Anser du att era molntjänster motsvarar bättre säkerhet än kundernas egna system? och i så fall inom vilka riskområden?

Det är svårt att svara på. Om man ska jämföra liksom säkerheten med ett bokföringssystem som vi använder lokalt eller klassiskt bokföring versus molnbaserat då… Det är väl lite ge och ta där egentligen. Bryter sig någon in på ditt företag så kan dom ju liksom komma åt all din bokföring om du har den lokalt. Det går ju inte att göra om du har det online. Men samtidigt om någon bryter sig in i din onlinebokföring så får dom ju tag på den där. Jag vet inte. Jag skulle väl säga att det är ungefär 50/50. Visst har du många användare, vi stödjer ju många användare per kund,

har du många användare som kan logga in i ditt molnsystem eller bokföringssytem så är det ju en större risk att en laptop som kommer på drift eller bli snodd då. På det sättet kan det väl vara större risk än att ha det lokalt då.

Q26. Vilken insikt har kunden i ert förebyggande säkerhetsarbete?

Igen, byråkunder versus vanliga kunder. Jag skulle säga att byråkunder har ju rätt bra insikt och dom är ganska aktiva och ser till att, dom vill ju veta att vi jobbar hårt med säkerheten medans vanliga kunder. Jag vet inte. En del kunder hör av sig och frågar ”Sparar ni era lösenord säkert”, ”Vad gör ni för att hålla det säkert”. Men överlag är det ett ganska lågt intresse från vanliga kunder i alla fall kring säkerhet då.

Q27. Outsourcear ni någon del av er tjänst?

Hela vårt system utvecklas inte i Sverige. Majoriteten gör det men vi har några delar av systemet som utvecklas externt. Däremot drift körs här i Sverige och allt sparas ju här i Sverige. Men viss utveckling är outsourcad, ja.

a. Vilken insikt har ni i tredjepartens förebyggande säkerhetsarbete?

Ganska bra, all projektledning i det vi har outsourcat sköts ändå härifrån. Det är ändå vi som har ritningen på hur det ska se ut. I och med att projektet körs härifrån så blir det naturligt att vi har ganska bra koll på vad det är vi får i slutändan och hur det är uppbyggt. Det är egentligen vi om bestämmer ”vi vill ha systemet på det här sättet”. Sen är det upp till tredjepart att bygga det då. Så vi har ändå ganska bra koll. Vi har ju tillgång till all källkod så det är ganska bra.

b. Specificeras det i det avtal ni har med kund?

Nej, all drift sköts i Sverige.

Q28. Upplevs det problematik vid övergång mellan olika molntjänstleverantörer?

Ja, vi har lite konverteringssystem på plats för olika konkurrenter då där vi använder deras API för att ja. Kunden kopplar alltså på vårt system via konkurrentens system då sen så kan vi via eras API hämta datan och importera det i vårt system. Om man vill byta till vårt system så är det ganska enkelt för då löser våran techsupport på företaget det. Jag antar att konkurrenten har

liknande system mot oss. Det är smidigt för kunden att smidigt byta runt inom onlinebokföring i alla fall.

8 Referenser

Anderson R (2011): Why information security is hard - an economic perspective, *Computer Security Conference, 2001, Proceedings 17th Annual*, 358-365.

Armbrust M, Fox A, Griffith R, Joseph A D, Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Soica I., Zaharia M., (2009): Above the clouds: A Berkeley view of cloud computing, *Berkeley Reliable Adaptive Distributed Systems Laboratory*, 7-13.

Baker W H, Hylender C D, Valentine J A (2008): 2008 Data Breach Investigations Report, Sid 1–29.

Bhattacherjee A, Park S C (2013) Why end-users move to the cloud: a migration-theoretic analysis. *European Journal of Information Systems*, Vol. 23, 357-372.

Buyya R, Yeo C S, Venugopal S (2008): Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. *Proceedings - 10th IEEE International Conference on High Performance Computing and Communications*, 5–13.

Carroll M, van der Merwe A, Kotze P, Venter H, Coetzee M, Loock M (2011): Secure cloud computing: Benefits, risks and controls, *Information Security for South Africa (ISSA)*.

Chen D, Zhao, H (2012): Data security and privacy protection issues in cloud computing, *In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference*, Vol.1, 647-651.

Datainspektionen: Personuppgiftslagen, http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/ (Access 2015-04-15)

Descombe M (2003): Good Research Guide: For small-scale social research projects (2nd Edition), Berkshire England, McGraw-Hill Education.

Dupré L, Haeberlen G (2012): Cloud Computing: Benefits, risks and recommendation for information security, *European Union Agency for Network and Information Security*, https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (Access 2015-04-10)

EU Opinion, 2012:
Article 29 Data Protection Working Party på uppdrag av direktiv 95/46/EC i EU (2012): Opinion 05/2012 on Cloud Computing. Directorate General Justice, Brussels, Belgium,
http://idpc.gov.mt/dbfile.aspx/WP196.pdf (Access 2015-04-10)

Feuerlicht G, Govardhan S (2010): Impact of cloud computing : Beyond a technology trend. *Systems Integration 2010*, 262–269.

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008): Cloud computing and grid computing 360-degree compared. *2008 Grid Computing Environments Workshop*, 1–10.

Géczy P, Izumi N, Hasida K (2012) Cloudsourcing: Managing cloud adoption, G*lobal Journal Of Business Research (GJBR)*, Vol. 6(2) 57-70.

Gupta A., (2010): Cloud computing growing interest and related concerns. *2nd International Conference on Computer Technology and Development*, 462.

Gupta S, Dave M, Gupta P (2014): A Study of the issues and security of cloud computing. *International Journal of Computer Science & Information Technologies*, Vol. 5, 5429-5434.

Iyer B, Henderson (2012): Business value from clouds: learning from users, *MIS Quarterly Executive*, Vol. 11, 51-60

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

LeVeque, Vincent (2006): *Information security: a strategic approach*. Hoboken, NJ. Wiley.

Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalasi A (2011): Cloud computing - The business perspective. *Decision Support Systems*, Vol. 51(1), 176-189.

Mell P, Grance T (2011): The NIST definition of cloud computing. *Communications Of The ACM*, Vol. 53(6), 50.

Motahari-Nezhad H, Stephenson B, Singhal S (2009): Outsourcing Business to Cloud Computing Services: Opportunities and Challenges. *IEEE Internet Computing*, Vol. 10, 1–18.

Patel P, Ranabahu A, Sheth A (2009): Service Level Agreement in Cloud Computing,http://corescholar.libraries.wright.edu/knoesis/78 (Access 2015-04-10).

Puttaswamy, K. P. N., & Zhao, B. Y. (2011): Silverline : Toward Data Confidentiality in Storage-Intensive Cloud Applications, *Proceedings of the 2nd ACM Symposium on Cloud Computing*.

Subashini S, Kavitha V (2011): A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, Vol. 34(1), 1-11.

Sahito F, Slany W (2013): Advanced Personnel Vetting Techniques in Critical Multi-Tennant Hosted Computing Environments, *International Journal Of Advanced Computer Science And Applications*, Vol. 4(5), 12-20.

Stahl B C, Doherty N F, Shaw M (2012): Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal*, Vol. 22(1), 77–94.

Ullah K, Khan M (2014): Security and Privacy Issues in Cloud Computing Environment: A Survey Paper. *International Journal of Grid and Distributed Computing*, Vol 7(2), 89-98.

Venters W, Whitley E (2012): A critical review of cloud computing: researching desires and realities. *Journal Of Information Technology*, Vol. 27(3), 179-197.

Wang C, Wang Q, Ren K, Lou W (2010): Privacy-preserving public auditing for data storage security in cloud computing. *INFOCOM, 2010 Proceedings IEEE*, 1-9

Wang L, Von Laszewski G, Younge A, He X, Kunze M, Tao J, Fu C (2008): Cloud computing: a Perspective Study *New Generation Computing*, Vol. 28(2), 137-146.

Wu L, Buyya R (2010): Service Level Agreement (SLA) in Utility Computing Systems. *arXiv:1010.2881*.

Zissis D, Lekkas D (2012): Addressing cloud computing security issues. *Future Generation Computer Systems*, Vol. 28(3), 583-592