Uppsala universitet
Inst. för informatik och media

Nulägesanalys av informationssäkerheten gällande molntjänster vid svenska universitet

Cecilia Almgren & Klara Höjenberg

Kurs: Examensarbete
Nivå: C
Termin: VT-15
Datum: 15-06-14

Sammanfattning

Allt fler verksamheter väljer att flytta delar av eller hela sin lagring till en molntjänst, en tjänst som tillhandahålls av en extern leverantör över Internet. Det medför en mängd fördelar som bl.a. minskade kostnader och ökad flexibilitet för användarna, men det finns också risker kopplat till att använda molntjänster. I uppsatsen presenteras en rikstäckande nulägesanalys över informationssäkerhetsläget kring användandet av molnlagringstjänster vid Sveriges 14 universitet. Arbetet genomförs som en fallstudie och granskning av universitetens styrdokument samt intervjuer med personal vid några utvalda universitet ligger till grund för analysen.

Nyckelord:

molntjänster, molnet, informationssäkerhet, lagring, universitet, myndigheter, Personuppgiftslagen, PuL

Abstract

Businesses today choose to move part or all of its storage to cloud services, a type of service provided by an external provider over the Internet. It brings a lot of advantages which includes reduced costs and increased flexibility for users, but there are also risks related to the use of cloud services. The thesis presents a nationwide analysis of information security regarding the use of cloud storage services at Sweden's 14 universities. The research and work process is performed as a case study where reviews of university policy documents and interviews with staff at a few selected universities are the basis for the analysis.

Keywords:

cloud services, the cloud, information security, storage, universities, government agencies, the Personal Data Act

Förord

Med den här uppsatsen avslutar vi våra studier vid det systemvetenskapliga kandidatprogrammet vid Uppsala universitet.

Vi vill rikta vår tacksamhet till de universitet och de universitetsanställda som ställt upp på intervjuer och e-postkorrespondens. Utan deras tid och expertis hade studien inte kunnat genomföras. Särskilt tack går till Stefan Edholm vid Sveriges Lantbruksuniversitet och Veronika Berglund vid Uppsala universitet.

Vi önskar även tacka vår handledare Jenny Eriksson Lundström för hennes hjälp och stora engagemang under hela uppsatskursen.

Tack!

Innehåll

1. Inledning 1
1.1 Bakgrund 1
1.2 Problemformulering 2
1.3 Syfte och forskningsfrågor 2
1.4 Tidigare forskning 3
1.5 Avgränsningar 3
1.6 Kunskapsintressenter 4
1.7 Disposition 4
2. Bakgrund 5
2.1 Informationssäkerhet 5
2.1.1 ISO 27000 5
2.2 Molntjänster 6
2.2.1 Olika typer av molntjänster 6
2.2.2 Fördelar med molntjänster 7
2.2.3 Nackdelar och risker med molntjänster 7
2.3 Styrdokument 8
2.4 Personuppgiftslagen och känsliga personuppgifter 8
2.5 Avtal 9
3. Metod 11
3.1 Forskningsstrategi 11
3.2 Paradigm 11
3.3 Datainsamlingsmetodik 11
3.3.1 Sökstrategi 12
3.3.2 Urval av lärosäten 12
3.3.3 Dokumentanalys 13
3.3.4 Intervjuer 14
3.3.5 Metodik för dataanalys 15
3.4 Kritisk granskning av metoden 16
4. Resultat 18
4.1 Empirisk miljö 18
4.1.1 Myndigheter 18
4.1.2 Universitetens styrning 18
4.2 Resultat av dokumentanalys 19
4.2.2 Val av respondenter 20

4.3 Resultat av intervjuer 21
4.3.1 Uppsala universitet - med styrdokument som berör molntjänster 21
4.3.2 Sveriges lantbruksuniversitet - utan styrdokument som berör molntjänster 22
4.3.3 Örebro universitet - utan styrdokument som berör molntjänster 23
4.3.4 Övriga universitet 23
4.4 Sammanställning av intervjuer 26
4.4.1 Syfte med förekomst eller avsaknad av styrdokument 26
4.4.2 Efterlevnad 26
4.4.3 Konsekvenser 27
4.5 Kompletterande telefonintervju med UU:s biträdande säkerhetschef gällande vikten av avtal med molntjänsteleverantörer 27
5. Analys 29
5.1 Styrdokumenten 29
5.2 Efterlevnad och konsekvenser 29
5.3 Risker 30
6. Avslutande slutsats och diskussion 32
6.1 Slutsats 32
6.2 Diskussion 32
6.3 Förslag till vidare forskning 34

1. Inledning

300 timmar film laddas upp varje minut på YouTube (YouTube, 2015), 500 miljoner tweets postas dagligen på Twitter (Twitter, 2015) och 60 miljoner foton laddas upp på Instagram varje dag (Instagram, 2015). Detta är exempel på att den digitala informationsmängden ökar ständigt och därmed ställer nya krav på informationshanteringen i samhället. Istället för att använda lokalt förvaltade servrar för lagring har användandet av s.k. molntjänster, även kallat molnet, ökat kraftigt den senaste tiden (The Guardian, 2013). Molntjänster innebär enkelt förklarat att tjänsten tillhandahålls av en extern leverantör över Internet (Encyclopedia Britannica, 2015a).

1.1 Bakgrund

Molntjänsters historia går hand i hand med Internets utveckling eftersom Internet är en förutsättning för att molntjänster ska kunna användas. Under 1990-talet lanserades the World Wide Web och i slutet av årtiondet, år 1999, lanserades Salesforce.com som kan ses som en av de första milstolparna i molntjänsternas historia. Deras koncept var att tillhandahålla företagsapplikationer via Internet, d.v.s. det vi idag skulle beskriva som tjänster via en "vanlig" hemsida. (Salesforce, 2015a). Amazon Web Services lanserades år 2002, en tjänst genom vilken Amazon erbjuder sina klienter molnbaserade tjänster för bl.a. lagring. Därefter har utvecklingen av molnet och molntjänster gått framåt med stormsteg och det är idag ett mycket populärt alternativ för lagring (Computer Sweden, 2010).

I Sverige är den vanligaste typen av molntjänster olika streamingtjänster som används till att lyssna på musik eller att titta på TV-serier och film, bl. a. Spotify och Netflix. De näst vanligaste molntjänsterna är sådana som används för lagring (Statistiska centralbyrån (SCB), 2014). Några av de stora aktörerna som erbjuder lagring i molnet för privat- och företagskunder är Box, Dropbox, Google Apps och Microsoft OneDrive. Dessa tjänster lanserades mellan år 2005 och 2010. (Salesforce, 2015a, Computer Weekly, 2015).

Molntjänster medför många fördelar för både företag och privatpersoner. En av de största anledningarna till att molnlagringstjänster blivit så populära är att det är mycket kostnadseffektivt för företag - tack vare molnet är det lättare att lagra större mängder data till ett avsevärt lägre pris (Miller, 2008). Molntjänsternas mjukvara uppdateras ofta automatiskt från leverantörens sida och användarna behöver inte själva stå för underhåll eller serverhallar. Det medför även ökad flexibilitet och tillgänglighet och underlättar samarbete via exempelvis delade dokument. (Löfgren, 2011, About.com, 2015, Miller, 2008).

Det förekommer dock en del nackdelar och risker med användandet. De senaste åren har media frekvent rapporterat om cyberattacker mot stora molntjänster som Apples iCloud och Googles Google Apps. Det har bl.a. rört sig om offentliggjorda nakenbilder och annan personlig data (Smitt, 2012) och förlorad data och dataintrång för företag och privata användare av Oracles lagringstjänst (Nygårs, 2011). Molntjänster levereras ofta av en extern leverantör och beroende på hur avtalet är formulerat kan även det leda till problem med äganderätt och kontroll över vem som har tillgång till informationen. Om det sker uppladdning av känsliga personuppgifter i molnet kan det innebära brott mot Personuppgiftslagen, PuL, vilket är straffbart. (Datainspektionen, 2015a).

För att kontrollera data och informations tillgänglighet, riktighet och konfidentialitet är arbetet med informationssäkerhet av stor vikt för alla typer av organisationer. Informations-säkerhetsarbetet kan effektiviseras genom att upprätta styrdokument, ett vedertaget verktyg som används inom verksamheter och organisationer, för att skapa struktur och ordning samt för att nå ut med information, riktlinjer och regler. (Informationssäkerhet.se, 2015).

I uppsatsen gör vi en rikstäckande nulägesanalys över informationssäkerhetsläget kring användandet av lagringsmolntjänster på Sveriges 14 universitet. Granskning av universitetens styrdokument samt intervjuer med personal vid några utvalda universitet kommer ligga till grund för uppsatsen. Vi kommer att redogöra för begreppet molntjänster, vilka fördelar och nackdelar de kan medföra, samt diskutera styrdokumentens roll för användandet av denna typ av molntjänster. Utöver detta kommer övriga relevanta begrepp att redas ut och förklaras, såsom Personuppgiftslagen, informationsklassificering och termen informationssäkerhet.

1.2 Problemformulering

Som inledningen belyser ökar användandet av molntjänster ständigt, och riskerna och konsekvenserna det kan medföra synliggörs allt mer. En fråga som väckts hos oss författare är huruvida säkerhetsarbete, lagar och regleringar gällande detta hänger med i den snabba utvecklingen. Användning av molntjänster förekommer hos anställda på Sveriges universitet och ett sätt att reglera detta är som tidigare nämnt genom att upprätta styrdokument som vägledning. Genom att införa riktlinjer för användandet av molntjänster kan de anställda få stöd och råd om hur molntjänster bör användas och de kan även bli upplysta och medvetna om de risker som finns om tjänsterna inte används korrekt. Det finns särskilda lagar och regleringar, som t.ex. offentlighetsprincipen, som måste följas i och med att universiteten klassas som myndigheter. Eftersom det är relativt nytt att lagra information i molnet ämnar den här studien att ta reda på i vilken utsträckning universiteten i Sverige har upprättat styrdokument om användandet av molntjänster, hur väl de efterlevs och vad konsekvenserna blir om någon bryter mot dem. För de universitet som inte har upprättat några styrdokument för användandet av molntjänster kommer anledningen till detta att undersökas, alternativt om de planerar att införa det eller om de har något annat sätt att reglera det på.

1.3 Syfte och forskningsfrågor

Syftet med denna uppsats är att genomföra en nulägesanalys av informationssäkerheten kring användandet av molntjänster vid svenska universitet. Frågeställningen som ligger till grund för denna studie är:

- Hur ser säkerhetsläget ut på Sveriges universitet gällande användandet av molntjänster?

Som en del i processen att besvara frågeställningen undersöks följande delfrågor:

- Har universiteten upprättade styrdokument gällande informationssäkerheten kring molntjänster?
- Vad beror förekomsten eller avsaknaden på?

1.4 Tidigare forskning

Mycket finns att läsa om molntjänster - bl.a. vad molntjänster är och om dess användningsområden (Amazon Web Services, 2015), hur användandet av molntjänster ökar (Glaad, 2015), fördelar med molnlagring jämfört med traditionell lagring (Salesforce, 2015b), om molntjänsternas utveckling och framtid (Anderson & Rainie, 2010). Vid sökning på ordet "molntjänster" i databasen Digitala Vetenskapliga Arkivet (DiVA) finner man 30 publicerade kandidat- och masteruppsatser från de senaste 4 åren. De handlar om allt från risker vid personuppgiftsbehandling i digitala molntjänster (Karlsson, 2014) och skiftet mellan datalagring lokalt och i molnet (Edholm & Malm, 2014) till Mehmedagic & Olssons (2011) kvalitativa studie om säkerhet i molnet.

Karlsson (2014) beskriver i sin masteruppsats *Risker vid personuppgiftsbehandling i digitala molntjänster* vilka risker det kan finnas med att ladda upp personuppgifter i molnet och dessa risker kan delas in i två huvudgrupper. Den ena handlar om riskerna som uppstår när användandet av molntjänster sker gränsöverskridande, då olika länders lagstiftningar kan hamna i konflikt med varandra. Den andra gruppen handlar om problematiken i att den personuppgiftsansvarige förlorar den faktiska kontrollen över informationen till en extern aktör om den lagras i en molntjänst. Uppsatsen syftar till att lyfta fram de risker som finns samt fungera som en vägledning i hur molntjänster ska användas i enlighet med Personuppgiftslagen, främst för den personuppgiftsansvarige.

I kandidatuppsatsen *Datalagring - En uppsats om skiftet mellan datalagring lokalt och i molnet* belyser Edholm & Malm (2014) molntjänsternas fortskridande utveckling, ökade användande samt fördelar-och nackdelar med lagring av data i molntjänster. Syftet med uppsatsen är att "undersöka och fastställa vilken affärsnytta organisationer kan utvinna av datalagring i molnet samt om de problem som finns det datalagring idag kan lösas genom att flytta lagringen till molnet" (Edholm & Malm, 2010. s. 2).

Mehmedagic & Olsson (2011) belyser användningsområden för samt säkerhetsfrågor gällande molntjänster i kandidatuppsatsen *Säkerhet i molnet: en kvalitativ studie.* De argumenterar även för införandet av en standard som ska klargöra för användare av molntjänster vilka säkerhetsrutiner molntjänsteleverantörerna erbjuder.

Molntjänster och informationssäkerheten gällande dessa är således ett aktuellt ämne, men ingen litteratur, studier eller vetenskapliga artiklar finns på ämnet informationssäkerhet gällande användandet av molnlagringstjänster hos svenska universitet. Det är detta uppsatsen kommer att handla om.

1.5 Avgränsningar

Det finns många olika typer av molntjänster med olika syften och funktionalitet. Molnet kan delas upp i olika lager som kallas för *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)* och *Software as a Service (SaaS)* (Visma, 2013a). Denna studie behandlar endast SaaS, som är den vanligaste typen av molntjänst.

Denna studie berör endast SaaS som används för lagring, då det är denna typ av molntjänster som främst används vid universiteten. Den har även fokus på informationssäkerheten kring molntjänster, inte molntjänsters funktionalitet, implementering eller liknande.

Ytterligare avgränsningar för uppsatsen är typen av myndighet som har undersökts. Det är endast universitet i Sverige som har staten som huvudman som har inkluderats i denna studie.

Fokus har legat på att analysera olika typer av styrdokument (t.ex. riktlinjer, guider, informationssäkerhetspolicyer) som universiteten har tagit fram för att reglera och ge de anställda vägledningar i användandet av molntjänster. Den är alltså inte begränsad till enbart säkerhetspolicyer. De delar av dokumenten som granskats och analyserats är de som specifikt berörde eller handlade om lagringsmolntjänster eller informationssäkerheten vid användande av dessa.

Analysen av säkerhetsläget vid svenska universitet vi ämnar genomföra begränsar sig till endast aspekter gällande molntjänster.

1.6 Kunskapsintressenter

Denna studie vänder sig främst till de som arbetar med molntjänster eller andra lagringsrelaterade tjänster i sin dagliga verksamhet, och då framförallt universitetens och högskolornas IT-avdelningar och ledning. Uppsatsen kan vara av intresse för myndigheter och verksamheter med staten som huvudman, då det är just denna typ av universitet som har inkluderats i undersökningen. Resultaten av studien kommer belysa vad som görs bra i nuläget men den kan också komma att användas som en vägledning för att förbättra eventuella brister i säkerhetsarbetet i framtiden. Studien kommer även kunna användas som en grund för fortsatt forskning och vidare utveckling inom området.

1.7 Disposition

I kapitel 2 kommer alla begrepp som berörs i uppsatsen att redas ut. Begreppet molntjänster samt fördelar och nackdelar med dessa, PuL och känsliga personuppgifter, styrdokument samt avtal kommer att förklaras ingående.

I kapitel 3 beskrivs vilken forskningsstrategi och vilken datainsamlingsmetodik som ligger till grund för uppsatsen. Även paradigm och metod för dataanalys presenteras.

I kapitel 4, resultat, beskrivs och sammanställs resultaten av dokumentanalysen och intervjuerna samt den empiriska miljön.

I kapitel 5 analyseras resultaten från kapitel fyra.

I det sista kapitlet, kapitel 6, presenteras en diskussion och en slutsats om det vi kommit fram till samt förslag till framtida forskning.

2. Bakgrund

I det här kapitlet redogörs för de begrepp som berörs i uppsatsen. Detta för att underlätta vidare läsning då de kommer att förekomma ofta. Begreppen (informationssäkerhet, molntjänster, personuppgifter, Personuppgiftslagen samt avtal) är centrala för uppsatsens ämne.

2.1 Informationssäkerhet

"Information är värdefullt och behöver skyddas efter behov. Ett bra informations-säkerhetsarbete ger verksamheten förtroende och borgar för effektiv informationshantering." (Informationssäkerhet.se, 2015) Enligt Informationssäkerhet.se (en informativ hemsida framtagen i samarbete med Myndigheten för samhällsskydd och beredskap, Polisen, Försvarsmakten, m.fl.) är informationssäkerhet då man skyddar information på så vis att den alltid finns när vi behöver den (tillgänglighet), att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet).

Informationssäkerhet och IT-säkerhet nämns ofta ihop, men värt att nämna är att de kan ses som två skilda begrepp. Informationssäkerhet syftar, som nämnt ovan, kring själva informationen som hanteras. IT-säkerhet är en del av det övergripande uttrycket informationssäkerhet och avser den tekniska säkerheten av informationshanteringen i IT-system. Det rör sig om hårdvara och mjukvara, såväl som förvaring, rutiner och riskhantering. IT-och informationssäkerhet går därför hand i hand och när det talas om den ena förutsätts ofta att den andra finns med (SS-ISO/IEC 27001:2014, IDT).

2.1.1 ISO 27000

ISO står för Internationella standardiseringsorganisationen och de arbetar med att ta fram standarder för olika områden, bl.a. informationssäkerhet. I Sverige representeras medlemskapet hos ISO av Swedish Standards Institute (SIS) (*Internationella standardiseringsorganisationen*, 2015). I ISO:s 27000-serie ges riktlinjer för hur en organisation, oavsett storlek, ska jobba med informationssäkerhet på ett effektivt och väl beprövat sätt. "Standarderna kan ge en organisation riktlinjer för hur risker och hot kan kartläggas och hanteras på ett systematiskt sätt. Standardserien omfattar ledningens ansvar, administrativa rutiner och övergripande krav på IT-infrastruktur" (*ISO/IEC 27000*, 2014). De har även tagit fram riktlinjer för hur man på bästa sätt ska utforma styrdokument (policydokument) som rör informations- och IT-säkerhet. (Swedish Standards Institute, 2015). För att påvisa att säkerhetskraven ställda av kunder, klienter, branschen eller liknande uppfylls utfärdar SIS oberoende certifiering av informationssäkerhet. (*ISO/IEC 27000*, 2014).

ISO 27000-serien består av två delar, ISO/IEC 27001:2013 som specificerar kraven för upprättande av ledningssystem för informationssäkerhet, LIS, samt ISO/IEC 27002:2013 som ger vägledning för informationssäkerhetsåtgärder. (Swedish Standards Institute, 2015).

2.2 Molntjänster

Traditionell lagring innebär att man lagrar data, t.ex. filer, dokument, bilder, mjukvaruprogram m.m., på (oftast lokala) servrar, hårddiskar eller externa lagringsenheter (Miller, 2008., Encyclopedia Britannica, 2015b). Genom att använda molntjänster behöver användaren inte ha programmen installerade på den egna datorn - de finns i stället på en server som man kommer åt via Internet. En molntjänst är alltså en resurs som tillhandahålls av en leverantör via Internet (Encyclopedia Britannica, 2015a). Molntjänster kan även definieras som följande: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources" (Mell & Grance, 2009). Molnet kan ses som en stor grupp av sammankopplade datorer och enheter och alla behöriga användare kommer åt molntjänsten från vilken enhet som helst, förutsatt att en Internetuppkoppling finns (se figur 1). (Miller, 2008).

Figur 1. Molnet. (Källa: Nya Dagbladet, 2015.)

2.2.1 Olika typer av molntjänster

När man talar om molntjänster delas de upp i olika distributionsmodeller. Den allra vanligaste är det s.k. *public cloud*, vilket betyder att användarna direkt kopplar upp sig mot leverantörens tjänst. *Private cloud* är en molntjänst som drivs privat och internt, vilket ofta medför en hög säkerhet. *Community cloud* kan förklaras som ett privat moln som används av en begränsad mängd företag. *Hybrid cloud* är en kombination av några av de ovan. Ett företag kan exempelvis använda sig av ett privat moln för viss typ av data och ett publikt moln för annan typ av data. (Visma, 2013b).

SaaS - Software as a service - SaaS är den vanligaste typen av molntjänst, där leverantören tillhandahåller programvara över Internet. Applikationerna finns i molnet och kan kommas åt från vilken internetansluten enhet som helst. Användarna betalar inte för att äga programvaran, de betalar endast i vissa fall för att använda den. Motsatsen till traditionell programvarulicens som installeras på en viss dator och bara kan nås från just den datorn. (Miller, 2008. Visma, 2013a).

Som tidigare nämnt i uppsatsen finns det några större aktörer inom molnlagringstjänster (Box, Google Apps, OneDrive, Dropbox m.fl.). SUNET är en svensk organisation som arbetar med att tillhandahålla datorkommunikation och infrastruktur inom forskning och utbildning. SUNET har avtal med Box och tillhandahåller en företagsinriktad molnlagringstjänst, SUNET Box, konfigurerad efter kundens behov. Många svenska lärosäten är anslutna till SUNET Box. (SUNET, 2015).

2.2.2 Fördelar med molntjänster

En av anledningarna till att det har blivit populärt med molntjänster är för att det medför en mängd fördelar för verksamheter och organisationer. Först och främst är det mycket kostnadseffektivt - för en liten peng kan företagen få nästan obegränsat mycket lagringsutrymme. (Löfgren, 2011, About.com, 2015). Eftersom molntjänsterna körs via Internet ställs det inte lika höga krav på datorerna vad gäller processorkraft och hårddiskutrymme. Företagen minskar även sina kostnader för IT-infrastruktur då de slipper investera i servrar, datorhallar och annat fysiskt material. Det leder till att underhåll av både hårdvara och mjukvara minskar, vilket gör att kostnaderna snabbt sjunker. Mycket pengar sparas också på att inte behöva installera en och samma mjukvara på en stor mängd datorer hos ett företag. Ytterligare en fördel är att användarna bara betalar för det de använder och kan dra upp och ner sitt användande vilket man inte kan när man köper en licens per användare. (Miller, 2008, About.com, 2015, Löfgren, 2011).

Molntjänster kan ge utrymme för ett mer flexibelt arbetssätt, då flera personer kan komma åt samma typer av dokument och information. Användaren blir heller inte bunden till en viss plats, en fysisk dator, vilket gör det mer globalt och lättillgängligt. Det underlättar också möjligheterna till att samarbeta på distans. (Salesforce, 2015b). Om en dator skulle bli stulen eller krascha, finns allt kvar i molnet vilket är en stor säkerhet då säkerhetskopiering inte behövs. Mjukvaruuppdateringar av molntjänsten görs av leverantören, vilket också är en fördel för användaren som slipper tänka på det. (Miller, 2008, About.com, 2015).

Utöver detta är molntjänster ett miljövänligt alternativ. Eftersom man bara använder det serverutrymme som behövs sänks koldioxidutsläppen och energiförbrukningen med 30 % genom att inte använda servrar på plats. (Salesforce, 2015b).

2.2.3 Nackdelar och risker med molntjänster

“The cloud is not for everyone, like with all solutions, you have to weigh what level of risk you are comfortable dealing with." - Neil Rerup (Business News Daily, 2013).

Det medföljer också en del nackdelar med att använda molntjänster. Ett av de större problemen är kontrollen av det som finns lagrat i molnet, vem äger egentligen det som ligger

där? Här gäller det att innan man övergår till molnlagring, försäkrar sig om vad som gäller juridiskt för båda parter. Ett sätt att göra det är genom att upprätta ordentliga avtal med leverantören där de juridiska aspekterna regleras. I detta sammanhang bör man ta hänsyn till Personuppgiftslagen, då det är straffbart om man bryter mot den. Myndigheter som använder molntjänster måste vara medvetna om ytterligare några regleringar som offentlighetsprincipen, vilken innebär att allmänheten har rätt att ta del av de allmänna handlingar som finns upprättade hos myndigheten. Dock ska man alltid vara försiktig med att lägga upp känslig data (såsom känsliga personuppgifter) i molnet, oavsett vilket avtal man har. (Datainspektionen 2015c, Datainspektionen, 2011).

Andra risker med molntjänster är cyberattacker. Företaget Apples molntjänst iCloud har varit utsatt för många attacker vilket till stor del beror på den enkla processen att återställa en användares lösenord. Förövaren behöver endast ta reda på tre saker; e-postadress, födelsedatum och svaren på två säkerhetsfrågor. Svaren på dessa frågor finns oftast bara några sökningar bort, vilket gör iCloud till ett lätt offer. (The Guardian, 2014, Tech Times, 2014).

Utöver risken för cyberattacker finns det ytterligare en del nackdelar. Kravet på en stabil och snabb Internetuppkoppling ökar och uppstår det problem med uppkopplingen kommer man inte åt sitt arbete och man kan heller inte synkronisera eller ladda upp nytt material. Om data av någon anledning skulle försvinna från molnet går det inte att få tag på den igen så länge säkerhetskopior inte har gjorts av användaren. (Business News Daily, 2013, Miller, 2008, About.com, 2015).

2.3 Styrdokument

Styrdokument är ett samlingsbegrepp på olika typer av dokument som ger vägledning eller styr agerande eller handling i sammanhang. Exempel på typer av styrdokument är policyer, riktlinjer, regler och regelverk, handlingsplaner, m.fl. (*Definition av styrdokument*, 2014, *Definition av begrepp*, 2013, *Vad menas med styrdokument?*, 2014).

Universitet är i regel decentraliserat styrda och kan ha många fakulteter, sektioner, institutioner och anställda. Exempelvis har Uppsala universitet nio fakulteter och cirka 6850 anställda (Uppsala universitet, 2015). För att skapa struktur och ordning, nå ut med information, viktiga beslut eller förhållningsorder används styrdokument, likt i många andra organisationer och verksamheter.

En policy är enligt Nationalencyklopedin (2015) "grundprinciper för ett företags eller en organisations handlande allmänt el. i visst avseende". Till skillnad från lagtexter förbjuder eller förhindrar inte policyer ett visst beteende eller handling, utan de vägledande och ska erbjuda ett stöd i t.ex. verksamheter och hur anställda ska agera för att uppnå mål och resultat. (*Policy*, 2015).

2.4 Personuppgiftslagen och känsliga personuppgifter

Personuppgiftslagen, förkortad PuL, har funnits sedan 1998 och är till för att i samband med behandling av personuppgifter skydda människor mot att deras personliga integritet kränks. PuL grundar sig på dataskyddsdirektivet som är en gemensam regel för alla medlemsländer

inom EU. Det betyder att alla medlemmar har infört en lagstiftning som motsvarar PuL, något som underlättar samarbeten och informationsflöden i unionen. (Datainspektionen, 2015e).

Känsliga personuppgifter definieras enligt PuL som sådan information som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och information som rör hälsa (graviditet, sjukskrivning, läkarbesök) eller sexualliv. (Datainspektionen, 2015f).

Europeiska kommissionen lade i mars 2012 fram ett förslag om modernisering och uppdatering av dataskyddsdirektivet med syfte att få en mer enhetlig tillämpning inom EU. För Sveriges del betyder det att den nuvarande Personuppgiftslagen inte kommer att vara kvar i den form som den finns idag. De största skillnaderna kommer att bli tydligare rättigheter för den enskilda individen och tydligare regler för ansvar hos de som behandlar personuppgifter, bland mycket annat. De nya reglerna kommer att träda i kraft tidigast i början av 2018. (Datainspektionen, 2015b). Detta kommer att påverka molntjänstleverantörerna och dess användare då de framöver behöver reglera avtalen så de stämmer överens med lagändringen.

Den som behandlar personuppgifter i en molntjänst är personuppgiftsansvarig. Den personuppgiftsansvarige bestämmer vilka uppgifter som ska behandlas samt ändamålen med behandlingen. Molntjänstleverantören och dess eventuella underleverantörer kallas för personuppgiftsbiträde och behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsombudet, som ofta är en anställd, ser efter att personuppgifter behandlas på rätt sätt och enligt lag inom en verksamhet. (Datainspektionen, 2015d).

Den som bryter mot PuL kan straffas med böter eller fängelse i högst två år om det har skett med uppsåt eller grov oaktsamhet (Datainspektionen, 2015a).

2.5 Avtal

Som tidigare redogjort är en molntjänst alltså en resurs som tillhandahålls av en leverantör via Internet. Det innebär att hårdvara (utöver användarens enhet), och i varierande grad mjukvara, inte behöver tillhandahållas av användaren. För att få ta del av tjänsten behöver användaren dock godkänna leverantörens användaravtal. Berglund (2015-05-21) berättar att dessa kan vara utformade på olika vis och påverkar var informationen lagras, vem som äger den, hur den får eller inte får användas, hur den ska finnas tillgänglig, m.m. Att få en tjänsteleverantör att specialanpassa avtalet med en kund beror ofta på affärens omfattning. Box, Google eller Microsoft som är väldigt stora företag är kanske inte benägna att specialanpassa sina avtal för ett universitet.

Det finns företag som agerar som mellanhand med tjänsteleverantören och slutanvändaren, exempelvis SUNET. Dessa företag kan hjälpa slutanvändaren att se över och anpassa avtalet med tjänsteleverantören så att de tar hänsyn till lokala lagar, restriktioner och andra viktiga aspekter. I SUNET:s fall rör det sig om svenska universitet och högskolor, d.v.s. samma typ av organisationer som behöver ungefär samma typ av avtal - SUNET har därför kunnat samla dessa som en större kundgrupp och på så vis förhandlat fram fördelaktiga avtal med Box. (Blåberg, 2015-04-13)

Safe Harbor-principerna är en samling regler som har tagits fram av USA:s handelsdepartement (Department of Commerce - DoC) som berör dataskydd och personlig integritet. Genom att organisationer i USA ansluter sig till dessa regler är det tillåtet att föra över personuppgifter från EU/EES till dem (Datainspektionen, 2015g).

3. Metod

Här presenteras strategi, underliggande paradigm, datainsamlingsmetodik, metodik för dataanalys samt kritik mot metodvalet.

3.1 Forskningsstrategi

Enligt Yin (1984) definieras fallstudie enligt följande:

"A case study is an empirical inquiry that: investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used."

Det är denna forskningsstrategi som uppsatsen bygger på då vi ämnar genomföra en detaljerad undersökning som används för att nyansera, fördjupa, utveckla begrepp och teorier samt illustrera en nulägesanalys av uppsatsens huvudfråga - hur säkerhetsläget ser ut på Sveriges universitet gällande användandet av molntjänster.

Oates (2006) beskriver tre olika typer av fallstudier; explorativ, deskriptiv och förklarande. En deskriptiv fallstudie definieras som "en rik, detaljerad analys av ett särskilt fenomen och dess sammanhang" (Oates, 2006, s.143), vilken är den typ av studie vi har för avsikt att genomföra.

3.2 Paradigm

Enligt Oates (2006, s. 147) har en fallstudie en av tre underliggande paradigm, antingen positivism, interpretivism eller kritisk forskning. Denna studie syftar inte till att bevisa eller motbevisa en hypotes vilket gör att valet av positivistiskt paradigm faller bort (Oates, 2006 s. 286). Även kritisk forskning faller bort då det syftar till att påverka människor genom att identifiera maktförhållanden och konflikter, samt ifrågasätta och kritisera befintliga traditioner (Oates, 2006 s. 297-298).

Målet är att skapa en djupare förståelse av ett unikt sammanhang genom ett tolkande synsätt. Tolkningen är central för interpretivismen och det finns inte ett rätt sätt att se på världen; alla människor uppfattar verkligheten på olika sätt. Det kan finnas flera sanningar och flera sätt att lösa saker på vilket leder till att det kan finnas flera förklaringar till studiens resultat. (Oates, 2006, s. 292-293). Därför är interpretivismen underliggande paradigm för denna uppsats. Ett ytterligare stöd för valet av interpretivismen som paradigm är genomförandet av en kvalitativ studie.

3.3 Datainsamlingsmetodik

De datainsamlingsmetoder som använts för arbetet är dokumentanalys och semistrukturerade intervjuer. För att undersöka om universiteten har styrdokument som berör eller handlar om informationssäkerheten för molntjänster begärdes styrdokument gällande IT- och informationssäkerhet ut från varje universitet. För att komplettera dokumentanalysen samt få en djupare och mer nyanserad kunskap om universitetens informationssäkerhetsarbete

genomfördes intervjuer med ansvarig IT-och/eller säkerhetspersonal vid utvalda universitet. Motiv för urvalet av universitet samt målen för intervjuerna kommer beskrivas nedan. Även tillvägagångssättet för dokumentanalysen och utformningen av intervjufrågor förklaras.

Enligt Oates (2006, s. 37-38) innebär "method triangulation" att en studie använder två eller flera datainsamlingsmetoder. Vi använder två metoder som kompletterar varandra och som är lika viktiga för resultatet. Genom att använda flera datainsamlingsmetoder kan man studera fallet från två olika perspektiv, vilket resulterar i rikare data och därmed mer kvalitet i forskningen.

3.3.1 Sökstrategi

Som vi nämnt tidigare finns det ett stort utbud av litteratur som behandlar molntjänster på olika vis. För att vara säkra på att vår forskningsfråga inte har behandlats tidigare gjordes en grundlig genomsökning i olika databaser. Sökningarna har skett på engelska och svenska i databaser som DiVA, Google Scholar, Scopus, Computer and Information System Abstracts och Web of Science Core Collection. Vi fann uppsatser och artiklar som handlade om övergången från traditionell lagring till molnlagring, risker vid personuppgiftsbehandling i molntjänster, risker och informationssäkerhet gällande molntjänster i privat sektor, men inte någonting om hur det ser ut med användandet av molntjänster vid Sveriges universitet. Detta styrker att vår uppsats och dess tänkta kunskapsprodukt är unik i sitt slag.

Nedan, i figur 2, finns de sökord vi huvudsakligen använde i sökningarna. Dessa användes i kombination med varandra för att få största möjliga bredd i sökningarna.

Sökord	information security	cloud services	university	personuppgiftslagen
Synonymer och närliggande termer	IT-security	the cloud	universities	avtal
	IT-säkerhet	molntjänster	myndigheter	offentlighetsprincipen
	informationssäkerhet	lagring	universitet	dataskyddsdirektivet
	styrdokument	cloud computing	government agency	känsliga personuppgifter

Figur 2. Sökord använda i litteratursökningen.

3.3.2 Urval av lärosäten

Som tidigare nämnt är informationssäkerhet gällande molntjänster ett aktuellt ämne som ständigt diskuteras. Det finns många studier som i något avseende handlar om molntjänster (se sektion 1.4). Med vår uppsats hoppas vi kunna tillföra något helt nytt till forskningsområdet, och det finns inga tidigare studier eller artiklar om svenska universitets eller högskolors användande av molntjänster. Då universiteten arbetar på liknande sätt och finns utspridda över hela landet var de en bra målgrupp för vår studie som på så sätt blir

rikstäckande. I och med att universitet klassas som myndigheter finns det särskilda lagar och regler de måste förhålla sig till, vilket gör det intressant från ytterligare en vinkel.

Av de drygt 50 lärosäten som finns i Sverige valde vi att endast ta med universiteten i vår urvalsgrupp. De är 14 stycken, ett antal som är tillräckligt för att ge en detaljerad undersökning. Dessutom är de spridda över hela landet, och i varierande storlek av antal studerande och anställda. De 14 lärosäten som valdes ut är alla universitet med staten som huvudman; Uppsala universitet (UU), Lunds universitet (LU), Göteborgs universitet (GU), Stockholms universitet (SU), Umeå universitet (UmU), Linköpings universitet (LiU), Karolinska institutet (KI), Kungliga Tekniska Högskolan (KTH), Luleå tekniska universitet (LTH), Karlstads universitet (KAU), Linnéuniversitetet(LnU), Örebro universitet (ORU), Mittuniversitetet (MiUn) och Sveriges lantbruksuniversitet (SLU). Chalmers Tekniska Högskola och Handelshögskolan i Stockholm, räknas som universitet men har inte staten som huvudman, som de övriga universiteten i urvalsgruppen. (Universitetskanslersämbetet, 2013) På grund av detta, samt att vi bedömde urvalet som stort nog för undersökningen syfte, valdes dessa bort.

Den faktiska data vi behövde för att svara väldigt enkelt på våra forskningsfrågor erhölls i stort sett från dokumentanalysen, men för att ge bredd i resultatet samt möjlighet till djupare analys och slutsats valde vi att genomföra intervjuer med några av universiteten. Urvalet grundades på geografisk tillgänglighet (UU och SLU), men framförallt utifrån hur styrdokumenten var utformade. UU och SU hade styrdokument med bakgrundsfakta om lagring och molntjänster, enkelt språk och tydliga riktlinjer för användandet av molntjänster. Därför var det intressant att ställa fördjupande frågor om styrdokumenten till dem. SLU och ORU hade i stort sett inga styrdokument alls som berörde molntjänster, därav valdes även de ut för att få bra spridning på svaren men också för relevansen för forskningsfrågorna. Då vi inte hade resurser till att intervjua alla 14 universitet ingående sändes övergripande intervjufrågor (se bilaga 6) ut till de övriga nio universiteten via e-post. Målet med dessa frågor var att samla in svar gällande syfte med förekomst/avsaknad av styrdokument som berör molntjänster, efterlevnad av dessa samt konsekvenser vid dålig efterlevnad eller brott mot styrdokumentens riktlinjer.

3.3.3 Dokumentanalys

En grundläggande datakälla för fallstudien är styrdokumenten som samlats in från respektive universitet. Oates (2006, s. 240-241) beskriver dokumentanalys som ett sätt att snabbt, billigt och enkelt få tag på stora mängder data. Genom att analysera delar av dokument går det fort att jämföra innehållet på ett övergripande plan. Dokumentanalys görs oftast i samband med fallstudier, etnografier och aktionsforskning. För att få tag på offentliga dokument är Internet en värdefull källa (Bell, 2006, s. 125).

Det huvudsakliga syftet med dokumentanalysen var att få svar på om universitetens styrdokument för IT- och informationssäkerhet innehöll riktlinjer för användandet av molntjänster. Styrdokumenten bestod bland annat av policyer, riktlinjer och andra vägledande dokument. De policyer som analyserats i denna studie har varit IT- och informationssäkerhetspolicyer, vilka signeras och godkänns av rektor vid respektive universitet och väger tyngre än riktlinjer och andra styrdokument inom samma område.

Insamling av dokument och dokumentanalys gick till på följande vis; först sammanställdes en lista med e-postadresser till alla kontaktpersoner vid respektive universitet genom att söka reda på kontaktuppgifterna via universitetens hemsidor. Önskvärda kontaktpersoner var de med ansvar för IT- eller informationssäkerhetsverksamheten vid respektive universitet, alternativt personal med motsvarade erfarenhet och expertis. Därefter komponerades ett meddelande att skicka ut till varje universitet där vi presenterade oss, gav en kort sammanfattning av arbetet och dess syfte samt önskade få ut respektive universitets styrdokument för IT- och informationssäkerhet (se bilaga 1). Vissa universitet skickade dokumenten som PDF-filer och vissa skickade länkar till sidor där det gick att hämta hem styrdokumenten. För att kunna analysera dokumenten på ett systematiskt sätt tog vi fram en analysmall med ett antal kriterier som vi skulle undersöka om respektive universitets styrdokument uppfyllde (se bilaga 2). Efter en vecka skickade vi ut en påminnelse till de universitet som ännu inte svarat. Sedan fortsatte vi med dokumentanalysen och avslutningsvis valde vi ut fyra universitet att intervjua för ta reda på mer information runt styrdokumenten och universitetens informationssäkerhetsarbete gällande molntjänster.

En kritisk del i arbetsprocessen var att tidigt få in styrdokumenten då de spelade en grundläggande roll för vidare arbete. Vi gjorde därför detta tidigt och var noga med att formulera oss kort och koncist i den initiala kontakten med respektive universitet. Att universitet är myndigheter och lyder under offentlighetsprincipen (“allas rätt att ta del av allmänna handlingar”, Sveriges Riksdag (2015)) var av stor betydelse för planeringen av datainsamlingen då det innebär att de är skyldiga att svara på frågor samt att skicka ut styrdokumenten till oss då dessa räknas som allmänna handlingar (Regeringen, 2013). Om detta inte hade varit fallet kanske vi inte hade kunnat använda oss av dokumentanalys som datainsamlingsmetod, då enbart processen för att samla in dokument riskerade att bli långdragen.

Vi skapade ett formulär där vi bokförde när begäran skickades ut till universiteten, när svar med eller utan dokument mottogs, när eventuell påminnelse blev skickad m.m. Vi fick svar och dokumentfiler eller länkar från alla universitet utom MiUn, KTH och GU. De två sistnämnda universiteten svarade aldrig på våra meddelanden, men styrdokumenten fanns att ladda ner från respektive universitets hemsidor. MiUn hade inga styrdokument att skicka ut då de är mitt uppe i arbetet att skriva om och uppdatera de styrdokument de haft. IT-chefen vid MiUn kunde meddela oss att de tidigare inte haft några styrdokument som berör informationssäkerhet för molntjänster, men de arbetar med att ta fram det inom en snar framtid.

3.3.4 Intervjuer

Oates (2006, s. 186-187) beskriver en intervju som en särskild typ av konversation som vanligen går till på så vis att en person ställer frågor till en eller flera andra personer i syfte att erhålla information. Intervjun är alltså inte en slumpartad konversation utan är planerad och följer en viss struktur.

Ostrukturerade intervjuer är en intervjuform utan förbestämda frågor, strikt ordning eller plan att följa. Den som håller intervjun har mindre kontroll över samtalet och presenterar ett ämne för den som ska bli intervjuad, och låter denne tala fritt om sina uppfattningar, idéer och

erfarenheter om det. Intervjuaren kan ställa följdfrågor eller förtydligande frågor men ska försöka att avbryta samtalet så lite som möjligt (Oates, 2006, s. 187-188).

Semistrukturerade intervjuer har fördefinierade frågor som följs, men beroende på flödet i intervjusamtalet kan följdfrågor och tilläggsfrågor ställas som komplement. Denna typ av intervju kommer genomföras med de universitet som gått med på att ta emot oss för intervju, samt med de vi kan hålla telefon- eller Skype-intervjuer med. Utifrån Oates (2006, s. 186-201) och en lathund för intervjuplanering (Tétard, 2015) tog vi fram en intervjuguide som förberedelse och stöd till intervjuerna. Intervjuguiden som vi utgick från och där våra mål med intervjuerna finns definierade, finns i bilaga 3.

Att ställa rätt frågor på rätt sätt är grunden i att få ut den information man söker under en intervju. Vid sammanställningen av intervjufrågorna följde vi intervjuguiden vi hade tagit fram.

För att ta fram intervjufrågor började vi med att fundera över vilka frågor vi kunde tänkas behöva ha med för att nå vårt syfte. Utifrån dessa kunde vi sedan välja ut de frågor som matchade målen samtidigt som vi gallrade bort de frågor som var överflödiga. Frågorna delades upp i kategorierna syfte, efterlevnad och konsekvenser. De slutgiltiga frågorna som vi använde oss av i intervjuerna återfinns i bilaga 4.

För att få ett bredare resultat av empiriinsamlingen valde vi även att skicka ut några korta frågor via e-post till de universitet vi inte genomförde djupare intervjuer med (d.v.s. nio stycken). Vi använde en e-postmall för universitet som har styrdokument om molntjänster och en annan mall till de utan (se bilaga 6). De huvudsakliga frågorna vi ville ha svar på var syftet och anledningen till varför de har gjort på ett visst sätt, men vi inkluderade även frågor om känslig data, efterlevnad av riktlinjerna, påföljder och konsekvenser av eventuella brott mot riktlinjerna, för ytterligare bredd och möjlighet till vidare analys.

Utöver dessa intervjuer genomfördes även två kortare telefonintervjuer. En skedde i början av forskningsprocessen, med IT-chefen på SLU (Edholm, 2015-04-08), med syfte att erhålla större kunskap inom arbetsområdet informationssäkerhet och molntjänster vid universiteten. Den andra skedde med biträdande säkerhetschef på UU och syftade till att reda ut begrepp och frågor, bl.a. gällande molntjänster och avtal.

3.3.5 Metodik för dataanalys

Den empiriska datan för arbetet är av kvalitativ form, vilket innebär att även dataanalysen som genomförts är kvalitativ. Enligt Oates (2006 s. 266-267) är kvalitativ data icke numerisk data, exempelvis ord, ljud eller bilder, och den insamlande datan extraheras för att identifiera teman och mönster som är användbara för forskningen som görs. I vårt fall är den insamlade datan textdokument, intervjuer (intervjuanteckningar och ljudinspelningar) och litteratur.

Vi gick systematiskt igenom all data och delade in den i följande klasser: data som inte tycks vara relevant för uppsatsens övergripande syfte, data som tillhandahåller generell beskrivande information som behövs vid förklarandet av begrepp och termer samt data som kan användas för att besvara vår forskningsfråga.

För att underlätta tillvägagångssättet för dataanalysen av styrdokumenten skapade vi en mall att utgå från (Se bilaga 2). Vi funderade över målet med uppsatsen och hur analysen skulle kunna hjälpa oss att svara på forskningsfrågan samt relevant information som kan komplettera den eller ge möjlighet till vidare analys och insikter. Frågorna som mallen baserades på blev som följer:

- Har universitetet styrdokument för informationssäkerhet?
- Berör styrdokumenten molntjänster?
- Står det vilken molntjänst universitetsanställda bör använda?
- Följer universitetet standarden SS-ISO/IEC 27000?

De två förstnämnda frågorna föll sig naturligt att ta med i analysmallen, då de huvudsakligen svarar på vår forskningsfråga huruvida universiteten har eller inte har styrdokument som berör informationssäkerhet gällande molntjänster. Huruvida universiteten följer 27000-standarden inkluderade vi som fråga då de allra flesta organisationer och myndigheter med IT-verksamhet gör detta, vilket framgått från litteratur vi läst om ämnet samt från den ostrukturerade telefonintervjun som hölls med SLU:s IT-chef i början av forskningsprocessen. Utifrån den telefonintervjun framgick det även att universiteten kan upprätta avtal med specifika molntjänster, som då är tillåtna att använda av de anställda. Därför lade vi till en fråga som berörde huruvida det nämns i styrdokumenten eller inte om de anställda rekommenderas använda en viss molntjänst.

När mallen var sammanställd läste vi metodiskt igenom alla dokument som samlats in och fyllde i svar på frågorna i mallen för respektive universitet.

3.4 Kritisk granskning av metoden

Valet av fallstudie som metod var passande för vårt ändamål då vi ville få fördjupad kunskap inom ämnet. En survey, kvantitativ datainsamling som oftast görs med enkäter, hade varit ett alternativ om vi hade ämnat göra en kvantitativ studie och inte strävat efter den djupare förståelsen vi ville uppnå med vår kvalitativa studie.

Problematiken med fallstudier beskriver Oates (2006, s. 150) som tidskrävande och som leder till generaliseringar med svag trovärdighet. Det finns heller inga fastställda regler i hur en fallstudie ska genomföras vilket kan göra det svårt. Ett annat problem är svårigheten i att få tag på dokument och personer att intervjua.

Eftersom styrdokument skulle samlas in från alla 14 universitet räknade vi med att det kunde gå långsamt att få in data från samtliga. Dokumentinsamlingen följde tidsplanen, med undantag från två universitet som inte svarade på vår korrespondens. De hade styrdokumenten tillgängliga via sina respektive hemsidor vilket gjorde att de gick att få tag på ändå. De intervjuer vi genomförde på plats gav oss djupare kunskap och förståelse. För att få större reliabilitet i studien hade det varit bra med fler respondenter, dels från fler universitet men också flera personer i olika befattningar från samma universitet, för att öka trovärdigheten.

Nackdelar med intervjuer är enligt Oates (2006, s. 198) att transkriberingen är mycket tidskrävande. Man måste också ta hänsyn till att personen som intervjuas endast är en åsikt i en hel organisation, det går inte att dra slutsatser att hela organisationen tycker på just det sättet. Svårigheterna med dokumentanalys är att det kan vara svårt att komma åt vissa dokument. I vårt fall var det allmänna handlingar som begärdes ut vilket underlättade stort, även om alla inte svarade. Dokumentanalysen kan inte stödjas för att ge en objektiv bild av verkligheten. (Oates, 2006, s. 241).

4. Resultat

I detta kapitel presenteras uppsatsens empiriska miljö, samt resultaten från dokumentanalyserna och intervjuerna.

4.1 Empirisk miljö

Här presenteras myndigheter och universitetens styrning.

4.1.1 Myndigheter

Alla statliga och kommunala organ som inte är en beslutande politisk församling klassas i Sverige som myndigheter. Universiteten i Sverige är statliga myndigheter vilket betyder att det är riksdagen, efter förslag från regeringen, som fattar beslut om den högre utbildningen samt forskningen. Inom regeringens ramar finns det utrymme för universiteten att själva besluta om antagning av studenter, studieorganisation och utbud av utbildningar m.m. (*Myndighet,* 2014).

Offentlighetsprincipen innebär att allmänheten har rätt att ta del av statens och kommunernas verksamhet. För myndigheters del, och därmed universitetens, betyder det att medborgarna får begära ut det som klassas allmänna handlingar. Regeringen (2013) beskriver det som att "en handling är allmän om den förvaras hos en myndighet och enligt särskilda regler anses inkommen dit eller upprättad där". En del allmänna handlingar är dock hemliga och går inte att begära ut. Dessa särskilda förhållanden behöver universitet och andra myndigheter ta hänsyn till vid lagring av data.

4.1.2 Universitetens styrning

I Sverige ligger ansvaret för högre utbildning och forskning hos riksdag och regering. Hos regeringen är det Utbildningsdepartementet som ansvarar över all utbildning. Det finns ett undantag i Sverige, Sveriges lantbruksuniversitet, SLU, som i stället ligger under Näringsdepartementet. Alla lagar styrs av riksdagen medan regeringen styr myndigheternas verksamhet. (Universitetskanslersämbetet, 2015b).

I Sverige finns det en del lagar med bestämmelser för universitet och högskolor med staten, kommuner eller landstings om huvudman. De största är Högskolelagen (1992:1434) samt Högskoleförordningen (1993:100) som är ett komplement till den först nämnda. Utöver dessa två finns det särskilda föreskrifter som Universitets- och högskolerådet har utfärdat. (Universitetskanslersämbetet, 2015a).

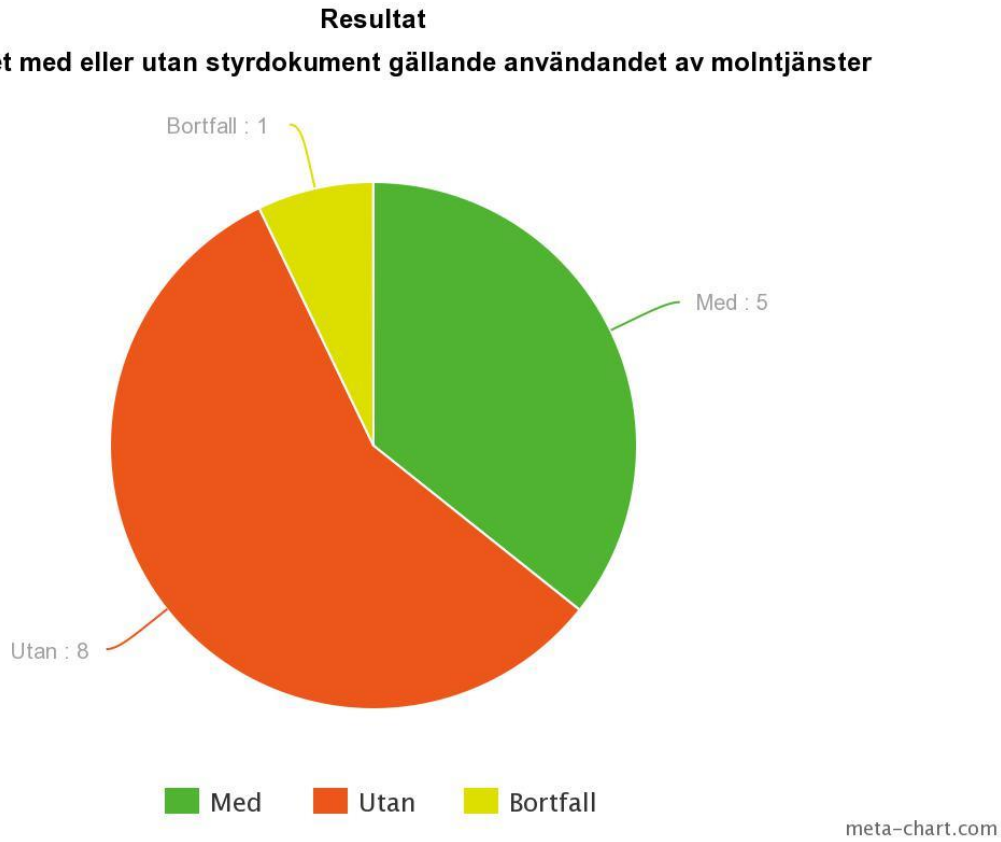
För att förstå hur information sprids i decentraliserade organisationer som universitet underlättar det att förstå hur styrningen ser ut. Alla universitet har en rektor, en prorektor och en universitetsdirektör i ledningen. Rektorn klassas som universitetets myndighetschef och har det övergripande ansvaret. Verksamheten på universiteten bedrivs inom institutioner, som i sin tur tillhör en fakultet. Prefekten leder institutionen tillsammans med en institutionsstyrelse och de delegerar i sin tur vidare olika ansvarsområden och uppgifter till sin avdelning (Universitetskanslersämbetet, 2015b).

Lagen om offentlig anställning, LOA (1994:260), reglerar anställningen för alla statligt anställda, d.v.s. alla universitetsanställda.

4.2 Resultat av dokumentanalys

Efter att dokumentanalysen var genomförd (se hela resultatet i bilaga 5) kunde vi konstatera att samtliga 14 universitet hade styrdokument gällande IT- och informationssäkerhet. Som nämnt ovan håller Mittuniversitetet på att skriva om sina styrdokument, vilket gjorde att det var 13 stycken vi fick tillgång till och därmed kunde analysera. Styrdokumenten varierade i storlek, innehåll och upplägg och gick metodiskt igenom och jämfördes mot analysmallen vi skapat.

Av de 13 universitet vi analyserade var det fem universitet som berörde molntjänster i sina styrdokument. Samtidigt var det styrdokument från åtta universitet som inte alls berörde molntjänster.



Figur 3. Cirkeldiagram över avsaknad/förekomst av styrdokument gällande molntjänster

Under dokumentanalysens gång kom vi till insikt om att majoriteten av universiteten använde sig av en modell för informationsklassificering som Myndigheten för samhällsskydd och beredskap (MSB) publicerat tillsammans med Swedish Standards Institute (SIS). Det är rekommendationer för klassificering av information, och "vänder sig både till myndigheter och andra organisationer och syftar till att stödja dem i deras arbete med att klassificera information på ett enhetligt sätt." (Myndigheten för samhällsskydd och beredskap, 2009). Vissa hade andra modeller för informationsklassificering, men själva tillvägagångssättet och vikten av att dela in information i olika klasser och typer var ett återkommande tema.

Vi kunde även konstatera att majoriteten av universiteten nämnde i sina styrdokument att de följde eller arbetade efter ISO-standardsserien 27000.

Några av universiteten inkluderade även stycken med bakgrundsinformation för informationssäkerhet och/eller molntjänster och säkerhetsaspekter gällande dessa, vilket vi upplevde gjorde dessa dokument mer lättlästa och lättare att tillgodogöra sig informationen i dessa.

Dessa iakttagelser ledde till att vi iterativt lade till ytterligare kriterier i vår dokumentanalysmall. Hela dokumentanalysen var således en iterativ process som resulterade i en sammanfattning av vad universitetens styrdokument berörde gällande informationssäkerhet, särskilt för molntjänster. Den resulterade även i en iterativt framtagen modell som skulle kunna användas i studier med samma syfte, i liknande organisationer och sammanhang.

Sammanfattningsvis utökades modellen med de tre nya kriterierna "Bakgrundsinformation (om molntjänster)?", "Modell för informationsklassificering?" och "Följer MSB 2009:10?". Se bilaga 5.

4.2.2 Val av respondenter

När sammanställningen av dokumentanalysen var gjord valde vi ut vilka universitet vi ville intervjua. För att få en bra spridning på respondenterna ville vi intervjua minst två universitet som inte berörde molntjänster alls, eller mycket lite, samt minst två som hade väl utformade och täckande styrdokument.

UU:s styrdokument var bland de som var allra bäst utformade, då de innehöll tydliga riktlinjer om användandet av molntjänster samt bakgrundsinformation som var lätt att ta till sig. Därför ville vi möta upp dem för en intervju. Även SU hade mycket tydliga och täckande styrdokument om molntjänster. Att få till en intervju fysiskt eller via telefon med SU visade sig inte vara genomförbart, därför skickade vi i stället intervjufrågorna via e-post till vår kontaktperson. UU och SU är båda stora universitet med över 5000 anställda.

Till skillnad från UU och SU berörde inte SLU:s styrdokument molntjänster. Då vi redan haft kontakt med deras IT-chef gick det bra att möta upp honom för en längre intervju in situ för att ta del av deras tankegångar och arbetssätt. SLU skiljer sig något från de övriga universiteten i Sverige då de ligger under Näringsdepartementet i stället för Utbildningsdepartementet. ORU var det universitet som fick nej på flest kriterier i dokumentanalysmallen, vilket var anledningen till att vi valde ut dem som respondent. Av samma orsak som med SU skedde även den intervjun via e-postkorrespondens. ORU är det minsta av dessa fyra universitet med sina 1260 anställda (Universitetskanslersämbetet, 2014). Intervjufrågorna som ställdes till dessa fyra universitet återfinns i bilaga 4.

Till övriga nio universitet skickade vi ut ett mindre antal frågor via e-post med mål att ta reda på orsak till förekomst eller avsaknad av styrdokument. Dessa frågor finns i bilaga 6. Vid behov, som i Umeå universitets fall, ställdes även specifika, förtydligande frågor för att reda ut vissa oklarheter som uppstått vid dokumentanalysen.

4.3 Resultat av intervjuer

Här redovisas resultaten från de genomförda intervjuerna. Intervjuerna med UU och SLU skedde in situ på respektive universitet. Övriga intervjuer skedde via e-postkorrespondens. Mål med intervjuerna var som tidigare nämnt att ta reda på syftet för avsaknad eller förekomst av styrdokument för molntjänster, huruvida universitet med avsaknad av styrdokument har planer på att införa det, vilken typ av information som inte bör laddas upp i molnet, hur riktlinjerna efterföljs och vad konsekvenserna blir om de inte gör det.

Först presenteras universitet med styrdokument som berör molntjänster, därefter de utan. Dessvärre fick vi aldrig svar från SU, vilket innebär att de uteblir från avsnittet.

4.3.1 Uppsala universitet - med styrdokument som berör molntjänster

Uppsala universitet, UU, är ett av de universiteten som hade bäst utformade styrdokument som berörde molntjänster, med tydligt bakgrundsinformation, instruktioner och direktiv. Intervjun skedde in situ med biträdande säkerhetschef Berglund 2015-05-05. Syftet med Uppsala Universitets riktlinjer är framförallt att ge stöd och råd till enskilda medarbetare och chefer i samband med att de överväger att använda molntjänster. Innan riktlinjerna infördes var det många som frågade hur de skulle agera när det kom till molntjänster, vilket ledningen tolkade som att behovet av att införa riktlinjer för användande av molntjänster fanns. Riktlinjerna ska vara lättlästa och enkla att ta till sig, annars gör de ingen nytta i verksamheten.

Känslig information hör inte hemma i molnet, berättade Berglund. D.v.s., inte information som omfattas av sekretess eller som innehåller känsliga personuppgifter. Verksamhetskritisk information, alltså information som kan vara kritisk för en enskild forskare eller forskargrupp, en institution eller för hela universitetet klassas också som känslig information. Det kan t.ex. vara original till avhandlingar, avtalsoriginal, data/information som samlats in över lång tid och/eller inte går att återskapa eller samlad information om värdefull egendom etc.

Allmänna handlingar får inte enbart finnas i molnet p.g.a. säkerhetsskäl. De måste finnas tillgängliga någon annanstans också, i fall att det t.ex. skulle bli problem med uppkoppling till molntjänsten.

För att få ut styrdokumenten ut i organisationen är det prefekten som bär det stora ansvaret genom att sprida det till sin respektive institution. Det brukar bli en varierad spridning beroende på hur insatt prefekten är. När IT-avdelningen går ut på plats och informerar brukar det fungera bäst med spridningen. Ungefär 4 gånger per år anordnar universitetet informationssäkerhetsträffar med syfte att informera och uppdatera de anställda med aktuell information. Säkerhetsavdelningen brukar också besöka institutionerna och prefekten regelbundet för att få bättre insikt i deras säkerhetsarbete.

Det är mycket svårt att kontrollera att riktlinjerna följs. Informationssäkerhet är extra svårt då det inte går att ha full koll på vad den enskilde individen gör. Det klassas som tjänstefel om det upptäcks och disciplinåtgärder i form av erinran, varningar, löneavdrag eller avstängning beroende på hur allvarlig en incident har varit. Personalansvarsnämnden bestämmer påföljd

för individen. Lagbrott är oftast enklare att upptäcka och straffa i och med att det finns en straffskala.

Det har tidigare inte skett någon incident med användandet av molntjänster. På det stora hela upplevs inte molntjänster som ett stort säkerhetsproblem, det är t.ex. inte värre än att anställda använder sig av sociala medier på fel sätt. Riktlinjerna berättar inte vad man inte *får* göra, UU litar på individens sunda förnuft och förser dem med riktlinjer som stöd och råd.

4.3.2 Sveriges lantbruksuniversitet - utan styrdokument som berör molntjänster

Sveriges lantbruksuniversitet, SLU, var ett av de universitet som inte hade styrdokument som berörde molntjänster. Intervjun skedde med universitetets IT-chef Edholm 2015-05-07. Det mesta av universitetets IT-verksamhets sköts av Edholm och hans kollegor, men vissa institutioner har även egna interna IT-avdelningar som kan sköta allt från systemutveckling och IT-stöd till lagring.

SLU har inga specifika styrdokument för informationssäkerhet gällande molntjänster. Edholm menar att de dokument de redan har (informationssäkerhetspolicy, m.fl.) täcker dessa områden ändå, indirekt. Edholm upplever inte att det finns några större problem med att anställda vid SLU lagrar data i molnet, men säger att de funderar på att ta fram specifika styrdokument för molntjänster som ett stöd och hjälpmedel för de anställda. I dagsläget når information om styrdokument, riktlinjer och liknande framförallt ut till de anställda via intranätet, men även e-postutskick och information från respektive institution eller avdelning.

SLU har idag en så kallad hybridlösning för lagring av data. En del data lagras på egna servrar och en del lagras genom Microsofts molntjänster OneDrive och Office 365 som används i stor utsträckning i arbetet. Inga specifika incidenter har uppstått kring oaktsam lagring i molntjänster, men han är medveten om att det förekommer, med ett så stort antal anställda. En molntjänst som har blivit spärrad från att installeras på universitetets datorer är Dropbox. Dropbox orsakar tekniska problem på så vis att tjänsten kolliderar med SLU:s backupsystem och avbryter synkningen till denna. Som den organisatoriska strukturen ser ut på SLU är det svårt kontrollera helt vilka molntjänster de anställda använder, men de har även undanbett de anställda att använda sig av onlineversionen. Det stör inte synkningen på samma sätt, men enligt Edholm bryter användaren mot vissa lagar genom användning av tjänsten (inget säkerhetsproblem, mer juridiskt). Det avtal SLU har slutit med Microsoft för användande av deras lagringstjänster täcker de lagar och direktiv som krävs. All lagring sker inom EU och de har även ett PuL-biträdesavtal.

Datainspektionens direktiv är styrande i hur de arbetar med informationssäkerhet, framförallt hur man ska gå tillväga vid informationsklassificering. Datainspektionen har direktiv som säger att man måste göra en riskanalys om man lägger saker i molnet. Edholm menar att den klassificering som görs av information som ska läggas upp i molntjänster inte skiljer sig nämnvärt från den “vanliga” klassificeringen för lagring lokalt.

Den information som SLU klassar som information som inte får spridas eller offentliggöras är personuppgifter, verksamhetsdata/arbetsmaterial och sekretessbelagd information. Diarium lagras till exempel lokalt. Majoriteten av SLU:s forskningsdata lagras i molnet, då det är ofantligt stora mängder att det inte skulle gå att lagra lokalt. Forskarna som tagit fram datan

har själva fått göra avvägningen att det är okej att lagra den i molnet. Oftast är datan inte av känslig art då det kan röra sig om ren numerisk data, att det ska offentliggöras ändå, osv.

Lokal lagring kostar universitetet hundra tusentals kronor varje år medan lagringen i Microsofts tjänster de använder sig av är i stort sett helt gratis. Det är naturligtvis en avgörande faktor i hur mycket data som lagras i molnet, då SLU ger sina forskare valmöjligheten att välja själva mellan lokal lagring eller molnlagring. Forskarna (eller forskningens uppdragsgivare) bekostar lagringen. Om de klassificerar data som sådan som får läggas i molnlagring brukar detta alternativ väljas. Edholm menar att det handlar mycket om sunt förnuft och eget ansvar.

Det är i dagsläget svårt att kontrollera efterlevnad av styrdokumenten. Det finns inga direkta sanktioner mot om någon skulle bryta mot korrekt lagar eller direktiv vid oaktsam lagring i molntjänster då ansvaret ligger hos individen, men följder som det kan ge är att forskare förlorar data, arbetsmaterial offentliggörs för tidigt, brott mot PuL osv. Edholm berättar att en modernisering av PuL snart införs och det ska då bli lättare att kontrollera att den efterföljs. Brott mot PuL kommer då bl.a. innebära höga böter.

SLU känner till SUNET Box och att intresset för att införa den som primär molnlagringstjänst finns, men även här är det en kostnadsfråga. Möjligheten att endast införa SUNET Box på vissa delar av lärosätets avdelningar finns inte, något som skulle vara nödvändigt i SLU:s fall. Det skulle inte vara praktiskt att använda det, i stället för nuvarande lösning, på exakt alla avdelningar. Det skulle även innebära för höga kostnader, därför har de valt bort SUNET Box som alternativ i dagsläget.

4.3.3 Örebro universitet - utan styrdokument som berör molntjänster

Respondent: IT-chef, A. Öhrn. Datum: 2015-05-18.

Örebro universitet var ett av de universitet vars styrdokument inte omfattade molntjänster över huvud taget. Vi ville därför gärna intervjua lämplig person vid ORU för att förstå hur det kommer sig, om de ser ett behov av att införa det i framtiden, m.m. På grund av kolliderande scheman och tidsbrist var inte en telefon-eller Skype-intervju genomförbar, men vi fick svar på några av våra frågor via e-post, vilket redovisas nedan.

ORU har en helt centraliserad IT-verksamhet som sköter allt från support, användarstöd, drift och systemförvaltning samt administrativ IT. ORU:s IT-chef menar att anledningen till att universitets styrdokument inte berör molntjänster är för att ORU har byggt en intern molnlösning för all verksamhet på universitetet. “Vi har byggt en intern molnlösning för all verksamhet på universitetet. Om något år kommer vi se om det finns ekonomi i extern molnlagring”. (Se avsnitt 6.2 för kommentar.)

4.3.4 Övriga universitet

Utöver de universitet vi valde att intervjua och ställa djupgående frågor till hörde vi av oss till samtliga universitet via e-post för att få reda på syftet med varför de har respektive inte har styrdokument som rör molntjänster. Nedan redovisas de svar vi fick.

Karolinska institutet - med styrdokument som berör molntjänster
Respondent: Informationssäkerhetssamordnare, L. Hertzell. Datum: 2015-05-20.

Syftet att KI tagit fram styrdokument för molntjänster är att de ser lagring av universitetets information i molnet som en potentiell risk.

Den information de anser känslig att ladda upp i molnet beror på flera faktorer gällande leverantörens säkerhetsnivå - hur avtalet med denne ser ut, om de är ISO 27000-certifierade, kravet på underleverantörer, var informationen behandlas och lagras geografiskt. Om den lagras i USA är det relevant om de har ett Safe Harbor-avtal. En risk-och sårbarhetsanalys krävs således i varje fall vid användande av olika leverantörers tjänster.

Känslig information kan klassas enligt följande aspekter:

- Ur konfidentialitetssynpunkt: Information som omfattas av sekretesslagstiftning, t.ex. OSL, PuL eller Patientdatalagen. Ett konkret exempel är känsliga personuppgifter.
- Ur tillgänglighetssynpunkt: All information som har någon form av tillgänglighetskrav på sig.
- Ur riktighetssynpunkt: Bör inte vara ett problem, men molnleverantörens ansvar bör avtalas.

Idag sker ingen kontroll av hur styrdokumenten efterföljs. ”Vi har inte kommit så långt ännu, men planer finns. En möjlighet vi diskuterar är att använda sig av ett complianceverktyg.”

Styrdokumenten sprids till de olika delarna av KI via internwebb, e-post samt personliga presentationer. De som ansvarar för att de anställda tar del av och följer styrdokumenten är verksamhetscheferna och/eller prefekterna.

Exakt vilka juridiska konsekvenser det kan leda till om styrdokumenten inte efterföljs är osäkert, men “då styrdokumenten bl.a. ska syfta till att KI ska uppfylla gällande lagstiftning inom informationssäkerhetsområdet kan det utgöra en juridisk risk att inte följa de interna styrdokumenten.” För universitetet kan det innebära större risk för informationssäkerhetsincidenter med allt vad det kan innebära i form av t.ex. badwill, rättsprocesser, ekonomisk skada etc. Vår kontaktperson på KI vill betona att han inte är rätt person att svara på vilka konsekvenser felaktig lagring i molntjänster kan ha för de anställda vid universitetet, men det skulle kunna handla om allt från att individer skadas om deras känsliga personuppgifter laddas upp, till lagbrott och eventuella bestraffningar, avstängning m.m. för de anställda, i samband med detta. “Men min gissning är allt från muntlig varning till disciplinära åtgärder som t.ex. avskedande. Om brott misstänks kan det naturligtvis även leda till anmälan och rättsprocess.“

Mittuniversitetet - utan styrdokument som berör molntjänster
Respondent: IT-chef, M. Edin. Datum: 2015-04-23.

Omarbetar alla sina styrdokument gällande IT för tillfället och kommer framöver att inkludera ett avsnitt om molntjänster, då ledningen har bestämt att det måste finnas med.

Linköpings universitet - utan styrdokument som berör molntjänster
Respondent: IT-direktör, J. Nejdeby. Datum: 2015-05-17.

Berör enligt vår uppfattning inte användandet av molntjänster i sina styrdokument.

"Våra styrdokument som finns på http://styrdokument.liu.se/ omfattar även molntjänster även om dessa i dag inte nämns explicit. Vi har diskuterat och har en del tankar på hur ett styrdokument som hanterar lagring kan se ut. Men ännu finns inget färdigt beslut. Vi håller på att se över hela vårt arbete med Ledningssystem för Informationssäkerhet och i samband med det kommer vi se över även vår Informationssäkerhetspolicy."

Lunds universitet - utan styrdokument som berör molntjänster
Respondent: IT-arkitekt, M. Persson. Datum: 2015-05-18.

Har inga styrdokument som berör användandet av molntjänster.

"Det har nog bara varit så att ingen tagit sig tid till att göra det. Jag vet inte om någon har det på agendan just för tillfället men det är något som jag anser behöver göras."

Umeå universitet - utan styrdokument som berör molntjänster
Respondent: IT-samordnare/IT-ansvarig/webbansvarig, M. Wallmark. Datum: 2015-05-18.

Umeå universitets sammantagna styrdokument berör i princip inte användandet av molntjänster. Generell hantering av information och data täcks dock, vilket kan anses täcka molntjänster rent tekniskt. När vi ställde frågor till Umeå universitets IT-samordnare för att förtydliga detta berättar han att de i sin verksamhet följer Datainspektionens riktlinjer för molntjänster inom offentlig sektor samt tillämpliga lagar. "För att informera om detta i verksamheten har vi till exempel bjudit in vår PuLO för seminarier med våra IT-kontaktpersoner utsedda vid varje institution/enhet. För alla system med personuppgifter ska informationsägaren anmäla detta till PuLO. Vi har också rutiner för integrationer där informationsägare vid varje enskilt fall måste godkänna en integration och vilken information som får utbytas."

Syftet med riktlinjerna är främst att belysa att det finns riktlinjer att beakta och att inte bara hoppa på en molntjänst utan eftertanke.

Den information som Umeå universitet anser är känslig att ladda upp i molntjänster är framförallt känsliga personuppgifter. Utöver detta kan det finnas regler för hur forskningsdata får hanteras och i vissa fall är molntjänster inte ett alternativ. Ofta är det finansiärer som har regler kring forskningen.

Ansvaret för efterlevnad av styrdokumenten följer delegationsordningen. Informationen om säkerhetsåtgärderna och riktlinjerna för informationssäkerhet sprids främst genom olika informationsträffar och via webben. "Sedan ett par månader är informationssäkerhetspolicyn också med som del i utbildning av centrala och lokala IT-systemadministratörer."

Konsekvenserna vid brott mot riktlinjer, eller bristfällig efterlevnad av dessa, är kontextberoende. "Att bryta mot Datainspektionens riktlinjer har fram till nyligen inte haft någon faktisk påverkan. Däremot har det nyligen beslutats att Datainspektionen fått utökade

befogenheter och också kan utdela vite till organisationer som bryter mot reglerna. Beloppet begränsas av procent av omsättningen och kan utdömas retroaktivt fem år bakåt i tiden. Detta kan bli kännbart oavsett organisation som drabbas. En annan tänkbar konsekvens är att forskningsfinansiärer drar tillbaka sina pengar. Utöver detta finns massor av scenarier beroende på vad som inte efterföljs och på vilket sätt.”

4.4 Sammanställning av intervjuer

Här görs en sammanställning av resultaten. Mål med intervjuerna var som tidigare nämnt att ta reda på syftet för avsaknad eller förekomst av styrdokument för molntjänster, huruvida universitet med avsaknad av styrdokument har planer på att införa det, vilken typ av information som inte bör laddas upp i molnet, hur riktlinjerna efterföljs och vad konsekvenserna blir om de inte gör det.

4.4.1 Syfte med förekomst eller avsaknad av styrdokument

Det som gällde för alla universitet med riktlinjer gällande molntjänster var att det övergripande syftet med dessa var att ge sina anställda stöd och vägledning i arbetet.

För de universitet som inte hade riktlinjer för molntjänster var orsakerna till detta lite blandade. Vissa universitet, som t.ex. SLU, hade inga skriftliga riktlinjer för detta då deras informationssäkerhetspolicy och/eller övriga styrdokument täckte det rent tekniska för vad som är tillåtet eller inte i samband med att lagra information, oavsett om det är i lokala servrar eller i molntjänster. Dock höll dessa universitet alla med om att det kan vara något som är bra att införa för att vägleda de anställda i sitt arbete samt att minimera risken av felaktig hantering av information i samband med användandet av molntjänster.

Lund och Linköpings universitet hade inga planer i nuläget på att ta fram dessa riktlinjer men båda kunde se vikten och behovet för det och det skulle därför övervägas i planering inför framtiden.

Mittuniversitetet reviderar sina styrdokument i dagsläget och planerar att ta fram styrdokument för användandet av molntjänster.

Örebro universitets orsak till avsaknaden av riktlinjerna var unikt i sitt slag - de har tagit fram en intern molnlagringstjänst och har således inte samma krav eller behov att kontrollera vad som lagras i den.

4.4.2 Efterlevnad

I decentraliserade organisationer som universitet är det svårt att kontrollera efterlevnad, något som konstaterades av bl.a. SLU, UU och KI. Universiteten har snarlik delegeringsordning där rektor är huvudansvarig för policyer, därefter har prefekter vid respektive institution eller avdelning ansvaret att förmedla och delegera information och informationsspridning nedåt i leden. Att kontrollera hur styrdokumenten och riktlinjerna följs är enligt intervjuerna svårt att genomföra praktiskt och inga universitet kan ge exempel på någon specifik säkerhetsincident kopplad till molntjänster.

Trots avsaknad av specifika riktlinjer framgick det i intervjun med SLU att de arbetar mycket med molntjänster och lagring av stora mängder data i både moln- och traditionell lagring. De har en hybridlösning där de erbjuder sina anställda att använda sig av OneDrive och Office 365 samt lokal, traditionell lagring. De ber sina anställda att inte använda Dropbox p.g.a. tekniska och lagliga skäl. Utöver Örebro universitet som använder en internt anpassad molntjänst, framgick det inte om något annat universitet rekommenderade eller förbjöd någon specifik molntjänst. Enligt SUNET:s hemsida framgår det dock att en del av universiteten som intervjuats använder deras molntjänst Box.

4.4.3 Konsekvenser

Felaktig eller oaktsam uppladdning av känslig information i molnet kan ha följder som att forskare förlorar sitt data, arbetsmaterial offentliggörs för tidigt och brott mot PuL. IT-chefen vid SLU berättar att en modernisering av PuL kommer att införas 2018 och det ska då bli lättare att kontrollera att den efterföljs. Brott mot PuL kommer då bl.a. innebära ännu högre böter.

Då de flesta av universitetens styrdokument täcker hur information ska lagras, speciellt de som har avsnitt gällande molntjänster, är individen ansvarig för sina egna handlingar. Det framgår av intervjuerna att vid eventuella brott mot lagar, regler eller riktlinjer ligger ansvaret hos individen. Om det rör sig om lagbrott kan det ha juridiska påföljder. Om det rör sig om tjänstefel kan personen bli varnad eller avstängd, beroende på graden av felet.

4.5 Kompletterande telefonintervju med UU:s biträdande säkerhetschef gällande vikten av avtal med molntjänsteleverantörer

Enligt Berglund (2015-05-21) är några av de aspekter som är avgörande för informationssäkerheten i de avtal universiteten (eller andra myndigheter eller organisationer) sluter med molntjänsteleverantören följande:

- **Var informationen lagras, geografiskt.**
  Inom EU/ESS har alla länder lagar som motsvara PuL, vilket innebär att det i princip är godkänt att lagra data i dessa länder. Det är därför "viktigt att ta ställning till om molntjänstleverantören kan komma att lämna över personuppgifter till ett så kallat tredjeland, det vill säga ett land utanför EU/EES, och om den överföringen i så fall har stöd i personuppgiftslagen."
- **Vem äger informationen och vem har rätt att använda den?**
  Vid lagring av information i extern parts molntjänst, vem är det som kommer att äga informationen och vem har rätt att använda den? Det är relevant att se över då det kan handla om forskning, arbetsmaterial och annan verksamhetskritisk data man kanske inte vill eller bör förlora upphovs-eller äganderätten till. Det kan även handla om att materialet användes i reklamsyfte, eller till annat än dess primära syfte. Ytterligare en aspekt är att om informationen är upphovsrättsskyddat material får det inte tillgängliggöras för extern part, då det kan medföra brott mot upphovsrättslagen.
- **Vilka underleverantörer finns?**
  Detta bör vara reglerat, så att inte underleverantörer anlitas som helt plötsligt lagrar informationen utom EU/ESS eller inte tar hänsyn till huvudleverantörens avtal.

- **Vad händer med informationen om avtalet upphör eller avslutas?**
  Får man tillbaka den? Hur ska det i så fall ske praktiskt?
- **Är avtalet anpassat efter lagar som organisationen är skyldig att följa?**
  T.ex. PuL.

5. Analys

I det här avsnittet analyseras resultaten från kapitel fyra. Resultaten kommer även kopplas till tidigare forskning.

5.1 Styrdokumenten

Som tidigare konstaterats i studien används styrdokument för att skapa struktur och ordning samt för att förmedla information, viktiga beslut och förhållningsorder. Det är ett vedertaget sätt att strukturera och effektivisera arbete inom en organisation och gemensamt för alla universitet är att de har just styrdokument för informationssäkerhet. De är dock olika utformade och omfattande, trots att majoriteten följer standardserien ISO-27000 för säkerhetsarbetet. Det som knyter dem samman är vikten som läggs vid informationsklassificering. I sin studie om risker vid personuppgiftsbehandling i digitala molntjänster bekräftar Karlsson (2014) vad flera av respondenterna konstaterat: om man klassificerar informationen korrekt innan lagring lokalt eller i molnet kan riskerna vid personuppgiftsbehandling minimeras i digitala molntjänster. Riskerna som berör informationens tillgänglighet, riktighet och konfidentialitet kan även hanteras till stor del av klassificering av informationen innan lagring, vilket bekräftas av Mehmadagic & Olsson (2011) i deras kvalitativa studie om säkerhet i molnet.

Syftet med styrdokumenten, för de universitet vars styrdokument rör molntjänster, är att de ska vara vägledande och ett stöd i de anställdas arbete. En del av de vägledande riktlinjerna handlar om just informationsklassificering, som ska vara lätt och snabbt för de anställda att genomföra. Vid UU pågår i dagsläget arbetet med att ta fram en enkel checklista för informations-klassificering. Målet med checklistan är att den ska vara så enkel och lätt att förstå att de anställda ska kunna lära sig den utantill och integrera den i sitt vardagliga arbete där lagring av information behöver göras (Berglund, 2015-05-05).

Av de universitet som inte har styrdokument som berör molntjänster menar flera att skälet till avsaknaden är att deras övriga styrdokument täcker säkerhetsaspekterna gällande lagring av information. Edholm (2015-05-07) påpekar att direktiven för lagring av information inte skiljer sig nämnvärt mellan lagring i molnet eller traditionell, lokal, lagring. De menar alltså att dessa styrdokument är överflödiga för att täcka säkerhetsaspekterna gällande lagring i molntjänster, men flera jobbar trots det med, eller överväger att, ta fram riktlinjer som ska vara vägledande och hjälpa de anställda vid användandet av molntjänster.

SLU och ORU har avtal med tjänsteleverantörer av molnlagring. Dessa avtal är framtagna och anpassade efter lagar och direktiv universiteten måste ta hänsyn till, som PuL och offentlighetsprincipen, samt de säkerhetsaspekter som angivits av Berglund (2015-05-21); var data lagras, vem som äger den, hur den får användas och vad som händer om avtalet avslutas.

5.2 Efterlevnad och konsekvenser

Majoriteten av universiteten har inte en särskild molntjänst de erbjuder eller rekommenderar sina anställda att använda. I dessa fall är deras eventuella användande av molntjänster på eget

initiativ och risken finns att de sluter ofördelaktiga avtal eller lagrar känslig data i molnet om de inte har vägledning eller kunskap i detta.

Huruvida styrdokumentens innehåll efterlevs samt huruvida felaktig informationslagring i molntjänsterna faktiskt sker är svårt att följa upp enligt respondenterna. Merparten av universiteten har inga rutiner för att följa upp eller kontrollera hur de anställda följer styrdokumenten för informationssäkerhet och, i de fall där de finns, riktlinjer för användande av molntjänster. Universiteten litar stort på de anställdas sunda förnuft vilket inte går att mäta. Enligt UU:s biträdande säkerhetschef (2015-05-06) brukar de anställda ta till sig informationen bäst om IT-avdelningen själva går ut på plats och informerar de anställda om riktlinjerna och vikten varför de måste följas, i stället för att endast skicka ut ett styrdokument eller meddelanden på e-post som i många fall inte läses noggrant, om ens alls, av mottagaren.

Trots att konsekvenserna av att ladda upp känslig information i molnet är många och brott mot PuL kan innebära böter eller fängelsestraff, vilket även belyses av Karlsson (2014), framgår det att det är svårt att kontrollera de anställdas efterlevnad av styrdokumenten och användande av molntjänsterna. Detta kan bero på att universiteten är decentraliserade organisationer vilket gör att det inte går att styra de anställdas beteenden eller arbetssätt på samma sätt som det går att göra i en privat eller centralt styrd organisation.

Inga respondenter kunde ge exempel på incidenter som har skett i samband med användandet av molntjänster vid respektive universitet vilket även det kan vara en bidragande orsak till att vissa av dem inte anser att styrdokument behövs.

Om svårigheterna med att kontrollera de anställdas beteende och handlingar gällande användandet av molntjänster kvarstår kan det även fortsättningsvis vara få fall som upptäcks. Svårigheterna i kontrollen gör att det är omöjligt att uppskatta hur många som faktiskt bryter mot PuL. Dock innebär detta inte att eventuella brott mot lagar eller universitetens riktlinjer är accepterbara. Den nya versionen av PuL, som träder i kraft 2018, kommer att medföra högre straff för den som bryter mot lagen (Edholm, 2015-05-07).

5.3 Risker

Det de flesta av universitetens representanter ger uttryck för är att användandet av molntjänster praktiskt inte innebär några större problem eller höga risker. De menar alla att användande av t.ex. sociala medier på ett oaktsamt sätt av de anställda kan medföra större säkerhetsrisker, då information som delas där är publik och kan nå ut direkt till obehöriga personer eller skada den anställdes eller universitetens anseende. Risken med att något faktiskt sker med den data som inte bör laddas upp i molnet, men laddas upp ändå, är relativt liten och därför inget större problem. Dock anser de att det är bra att införa styrdokument för att förebygga problem och hjälpa och vägleda de anställda i den alltmer vanliga användningen av molntjänster och vi fick uppfattningen av att många av de universitet som inte berör molntjänster i sina nuvarande styrdokument har för avsikt att göra det i framtiden.

Det gäller dock att de risker som finns inte underskattas (se kapitel 2.2.3). Molnlagring innebär alltid att man lämnar ut sin information till någon annan, en tredje part som inte fullt ut kan kontrolleras. Då det har hittats brister i säkerheten i molnet och cyberattacker har skett

senaste tiden går det inte att blunda för att det faktiskt kan hända olyckliga saker. Dessa risker belyses bl.a. i Mehmedagic & Olssons (2011) studie.

Att universiteten lyder under offentlighetsprincipen innebär att de måste kunna lämna ut allmänna handlingar vid begäran. UU:s biträdande säkerhetschef berättade att en allmän handling aldrig får finnas i molnet utan att också alltid vara säkerhetskopierad till en lokal lagringsenhet.

6. Avslutande slutsats och diskussion

I det här avsnittet presenteras svaren på uppsatsens frågeställningar samt en diskussion kring dessa. Det redogörs även för en reflektion kring arbetsprocessen. Frågeställningen och dess underfrågor ser ut som följer:

- Hur ser säkerhetsläget ut på Sveriges universitet gällande användandet av molntjänster?
    - Har universiteten upprättade styrdokument gällande informationssäkerheten kring molntjänster?
    - Vad beror förekomsten eller avsaknaden på?

6.1 Slutsats

Efter genomförd kartläggning av säkerhetsläget gällande användandet av molntjänster på Sveriges universitet kan vi konstatera att det över lag ser bra ut, trots att förbättringar och vidareutveckling av t.ex. nämnda vägledande riktlinjer, checklistor för informationsklassning, uppföljning av rutiner, med fördel kan ske. Samtliga av de universitet vi fått svar från är medvetna om molntjänsters risker och säkerhetsbrister och arbetar kontinuerligt med att förbättra säkerheten.

Fem universitet berörde molntjänster i sina styrdokument, åtta gjorde det inte. Att de inte gör det är inget mått på att deras säkerhetsarbete och rutiner kring användandet av molntjänster är sämre än de andra. Som vi nämnt beror det i många fall på att universitetet har ett avtal med en viss molntjänst vilket de menar gör det säkrare för de anställda att använda den och därför inte nödvändigtvis upprättat styrdokument med särskilda riktlinjer. Det kan också bero på att det inte har hunnits med i och med att lagring i molnet är någonting som blivit allt vanligare de senaste åren och sätt att reglera och kontrollera detta inte riktigt har blivit framtagna än.

Syftet med de styrdokument som berörde molntjänster var främst att ge stöd och vägledning för de anställda i deras dagliga arbete. Det görs bland annat via modeller för informationsklassificering, som är en av grunderna till ett lyckat informationssäkerhetsarbete. Genom att använda sig av dessa modeller kan de anställda på ett snabbt och enkelt sätt ta reda på vilken information som får respektive inte får laddas upp i molnet.

En slutsats vi kan dra är att användandet av molntjänster inte ses som ett så stort problem hos universiteten. De flesta känner sig trygga i och med de avtal som tecknats med molntjänstleverantörer och upplever inte att de anställda bryter mot de regleringar som finns. Visserligen är kontroll av efterlevnad svårt att genomföra men många litar på individens sunda förnuft.

6.2 Diskussion

Mycket pekar på att användandet av olika typer av molntjänster och lagring i molnet kommer fortsätta att öka i framtiden, men studier visar att vi inte kommer att övergå helt och hållet till molnlagring. (Edholm & Malm, 2014, Anderson & Rainie, 2010, Edholm 2015-05-07,

Berglund, 2015-05-05). Vår uppfattning är att lokal lagring kommer att finnas kvar framöver men, som en konsekvens av det ökade molnanvändandet, i allt mindre utsträckning.

I och med de stora kostnadsbesparingar som sker med lagring i molnet, samt övriga fördelar det för med sig, kan detta peka på att allt fler universitet i framtiden kan komma att använda sig av molntjänster och hybridlösningar. Det skulle kunna innebära att anpassning och optimering av avtalen mellan tjänsteleverantörerna och universiteten blir ett naturligt utvecklingssteg. Vi ser det som tyder på att det kommer vara mer fördelaktigt för både molntjänstleverantörerna och användare som universitet och myndigheter att fler färdiga avtal anpassat för olika kunder och ändamål tas fram då det borde göra det lättare för båda parter att ingå avtal. Dataskyddsdirektivet underlättar för oss som EU-medlemsland att sluta avtal med andra EU-länder då det finns en motsvarande PuL i samtliga medlemsländer.

Styrdokument fyller en viktig funktion och vi tror att de kommer att finnas kvar i den traditionella meningen när det gäller övrig informationssäkerhet, men just molntjänster kommer kunna regleras bättre på annat sätt. Som Berglund (2015-05-20) antydde i telefonintervju, och som även andra intervjusvar från de olika universitetens pekar på, kan avtalen eventuellt komma att räcka som reglering för molntjänster, tillsammans med t.ex. en checklista för informationsklassificering samt informerande och vägledande riktlinjer, likt de som UU tagit fram. Det kommer alltid finnas viss typ av information som inte får lagras i molnet och då gäller det att veta vilken. I grunden handlar det om att nå ut med informationen till användarna - i det här fallet forskare och övriga anställda på universiteten. Vikten av att formulera styrdokumenten på ett så enkelt och lättförståeligt språk som möjligt är av stor betydelse och likaså modellen eller checklistan för informationsklassificering. Upplever de anställda att det är en krånglig process att klassificera informationen kommer merparten inte att genomföra det i praktiken.

Ett resultat av studien och något som vi i efterhand kunnat konstatera är vikten av avtalen mellan molntjänsteleverantören och kunden (universiteten). Om detta hade varit klart från början hade vi gjort mer efterforskningar i detta ämne samt lagt större vikt vid att få utförliga svar på frågorna till universiteten som berörde just detta. I intervjuerna hade frågorna formulerats annorlunda för att få tydligare svar från respondenterna, t.ex. ”Har X universitet i dagsläget ett avtal med någon molntjänstleverantör?”. Relevant att veta är då vilken tjänst, vad avtalet omfattar, hur det påverkar deras säkerhetsarbete o.s.v., eftersom avtal med tjänsteleverantör, eller det faktum att universitetet har en specifik tjänst att använda påverkar mycket. Vissa av respondenterna svarade inte på frågan huruvida de använde sig av en särskild molnlagringstjänst så att det framgick tydligt. Vid efterforskningar för att förtydliga detta erhölls information bl.a. från SUNETS hemsida som tyder på att flera är anslutna till SUNET Box.

Listan av studiens universitet som är anslutna till SUNET är Göteborgs universitet, Karlstads universitet, KTH, Linköpings universitet, Linnéuniversitetet, Luleå tekniska universitet, Lunds universitet, Mittuniversitetet, Stockholms universitet, Umeå universitet, och Örebro universitet (SUNET, 2015). Om vi hade känt till detta vid början av studien hade intervjufrågorna anpassats bättre för att få fram utförligare svar och information om användandet, från dessa universitet.

När vi började läsa på om ämnet insåg vi snabbt hur aktuellt molntjänster samt informationssäkerheten gällande molntjänster är. Det märktes även när vi kontaktade representanter ute på universiteten där engagemanget var stort. Till exempel så publicerade UU sina nyligen framtagna riktlinjer för molntjänster i mars 2015 och några andra universitet har berättat att det är på ingång med riktlinjer för molntjänster. Mittuniversitetet är just nu mitt i revidering och uppdatering av sina styrdokument för informationssäkerhet och uppgav även de att de ska införa styrdokument som berör molntjänster. Det vore intressant att följa upp denna studie inom en viss tidsintervall, t.ex. 1 år, 3 år eller 5 år, för att se om säkerhetsläget ändras, som exempelvis hur rutinerna kring informationssäkerhet utformas och följs av universitetens anställda.

6.3 Förslag till vidare forskning

Som nämnt i tidigare avsnitt tyder mycket på att lagar, regler och användningsområden gällande molntjänster inte hänger med i den snabba utvecklingen och det ökade användandet. Det kommer därför mycket troligt behöva undersökas hur detta samt universitet, myndigheter och andra berörda verksamheter och privatpersoner ska agera och hantera molntjänst-användandet.

Som nämnt i bl.a. avsnitt 6.2 finns det som tyder på att själva avtalen kan komma att bli mer centrala i hur verksamheter använder sig av molnlagring - utformningen och innehållet av dessa avtal vore därför relevant att undersöka vidare.

Då det blir allt vanligare att använda molntjänster kan det leda till att kunskapen inom området ökar vilket innebär att fler blir medvetna om de risker som finns och på så sätt kommer ”felhanteringen” av molnet förhoppningsvis att minska. I dagsläget visar intervjuerna på att styrdokumentens innehåll och riktlinjer är något som är svårt att nå ut med till universitetens anställda, samt att kontroll av efterlevnad av rutiner är bristfällig. Det kan tyda på att förbättring av dessa områden bör undersökas. Vidare forskning på detta skulle t.ex. kunna resultera i förslag på hur riktlinjer och information gällande molntjänster och liknande områden bör vara utformad för att nå ut till och tillgodogöras på bästa sätt av anställda vid stora organisationer, eller rutiner för uppföljning av efterlevnad och korrekt användande av molntjänster.

De efterforskningar som gjorts i samband med denna studie, de artiklar och den litteratur som presenterats samt de experter vi talat med vid Sveriges universitet pekar sammantaget på att molntjänster och säkerheten kring dem är ett ämne och forskningsområde som kommer vara aktuellt många år framöver.

Källor

About.com (2015). *Advantages and Disadvantages of Cloud Computing*. Hämtad 17 februari 2015 från http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm

Amazon Web Services, (2015), *What is Cloud Computing - Benefits of the Cloud*. Hämtad 25 maj 2015, från Amazon Web Services, http://aws.amazon.com/what-is-cloud-computing/

Anderson, J. & Rainie, L. (2010). *The future of cloud computing.* (Future of the Internet", nr 2010:4).

Washington, Pew Research Center's Internet & American Life Project and Elon University's Imagining the Internet. Hämtad 24 maj 2015 från http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing/

Bell, J. (2006). *Introduktion till forskningsmetodik.* (4., [uppdaterade] uppl.) Lund: Studentlitteratur.

Business News Daily (2013). *8 reasons to fear Cloud Computing.* Hämtad 23 maj 2015 från http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html

Computer Sweden (2010). *"Molnet är som kejsarens nya kläder".* Hämtad 15 maj 2015 från http://computersweden.idg.se/2.2683/1.293834/molnet-ar-som-kejsarens-nya-klader

Computer Weekly (2015). *A history of cloud computing.* Hämtad 7 maj 2015 från http://www.computerweekly.com/feature/A-history-of-cloud-computing

Datainspektionen (2015a). *Dina rättigheter enligt personuppgiftslagen.* Hämtad 19 maj 2015 från http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/dina-rattigheter/

Datainspektionen (2015b). *EU:s dataskyddsreform.* Hämtad 11 maj 2015 från http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/

Datainspektionen (2015c). *Molntjänster och personuppgiftslagen.* Hämtad 16 februari 2015 från http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/

Datainspektionen (2015d). *Personuppgiftsansvarig och personuppgiftsombud*. Hämtad 24 maj 2015 från http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig-och-personuppgiftsombud/

Datainspektionen. (2015e). *Personuppgiftslagen*. Hämtad 5 maj 2015 från http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/

Datainspektionen (2011). *Risker med otydliga avtal för molntjänster*. Hämtad 15 maj 2015 från http://www.datainspektionen.se/press/nyheter/2011/risker-med-otydliga-avtal-for-molntjanster/

Datainspektionen (2015f). *Vad menas med känsliga personuppgifter?* Hämtad 5 maj 2015 från http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-menas-med-kansliga-personuppgifter/

Datainspektionen (2015g). *Vad är Safe Harbor-principerna?* Hämtad 9 maj 2015 från http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/vad-ar-safe-harbor-principerna/

Definition av begrepp (2013). Region Gotland. Hämtad 15 maj 2015 från http://www.gotland.se/48595

Definition av styrdokument (2014). Uppsala universitet. Hämtad 15 maj 2015 från http://regler.uu.se/Def_av_styrdokument/

Edholm, S. & Malm, J. (2014). *Datalagring: En uppsats om skiftet mellan datalagring lokalt och i molnet.* Kandidatuppsats, Uppsala Universitet, Institutionen för Informatik och Media.

Encyclopædia Britannica (2015a). *Cloud computing.* Hämtad 2 februari 2015 från http://global.britannica.com/EBchecked/topic/1483678/cloud-computing

Encyclopædia Britannica (2015b). *Data storage.* Hämtad 9 juni 2015 från http://global.britannica.com/EBchecked/topic/1473838/data-storage

Glaad, M. (2015). *Skiftet kommer sakta men säkert.* Cloud Magazine, IDG. Hämtad 25 maj 2015 från http://cloud.idg.se/2.16150/1.379401/skiftet-kommer-sakta-men-sakert

Informationssäkerhet (2015). *Vad är informationssäkerhet?* Hämtad 18 maj 2015 från https://www.informationssakerhet.se/sv/informationssakerhet/allmant/

Instagram (2015). *About us.* Hämtad 6 maj 2015 från https://instagram.com/about/us/

Internationella standardiseringsorganisationen (2015). I: Wikipedia, den fria encyklopedin. Hämtad från http://sv.wikipedia.org/wiki/Internationella_standardiseringsorganisationen

ISO/IEC 27000 (2014). I: Wikipedia, den fria encyklopedin. Hämtad 6 maj 2015 från http://sv.wikipedia.org/wiki/ISO/IEC_27000

Karlsson, N. (2014). *Risker vid personuppgiftsbehandling i digitala molntjänster.* Masteruppsats, Stockholms Universitet, Juridiska Institutionen. Hämtad 24 maj 2015 från http://www.diva-portal.se/smash/get/diva2:765059/FULLTEXT01.pdf

Löfgren, C. (2011). *Sex skäl för att använda molnet.* Cloud Magazine, IDG. Hämtad 10 juni 2015 från http://cloud.idg.se/2.16150/1.414070/sex-skal-for-att-anvanda-molnet

Mehmedagic, F. & Olsson, S. (2011). *Säkerhet i molnet: en kvalitativ studie*. Kandidatuppsats, Örebro universitet, Handelshögskolan vid Örebro universitet. Hämtad 21 maj 2015 från http://www.diva-portal.org/smash/get/diva2:408971/FULLTEXT01.pdf

Mell. P & Grance. T (2011). The NIST Definition of Cloud Computing. National Institute of Standars and Technology. Hämtad 22 maj 2015 från http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Miller, M. (2008[2009]). *Cloud computing: web-based applications that change the way you work and collaborate online.* Indianapolis, Ind.: Que.

Myndigheten för samhällsskydd och beredskap (2009). *Modell för klassificering av information - rekommendationer*. Hämtad 18 maj 2015 från https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nytt-informationssakerhet/Modell-for-klassificering-av-information---rekommendationer/

Myndighet (2014). I: Wikipedia, den fria encyklopedin. Hämtad 6 maj från http://sv.wikipedia.org/wiki/Myndighet

Nygårs, O. (2011). *Myndighet slår larm om IT-läckor.* Svenska Dagbladet. Hämtad 9 juni 2015 från http://www.svd.se/myndighet-slar-larm-om-it-lackor_5909395

Oates, B. J. (2006). *Researching Information Systems and Computing*. SAGE.

Policy. I Nationalencyklopedin. Hämtad 25 maj 2015 från www.ne.se/uppslagsverk/ordbok/svensk/policy

Policy (2015). I: Wikipedia, den fria encyklopedin. Hämtad 20 maj från http://sv.wikipedia.org/wiki/Policy

Regeringen (2013). *Offentlighetsprincipen - rätten till insyn.* Hämtad 8 maj 2015 från http://www.regeringen.se/sb/d/504/a/3029

Salesforce (2015a). *The complete history of cloud computing.* Hämtad 28 april 2015 från http://www.salesforce.com/uk/socialsuccess/cloud-computing/the-complete-history-of-cloud-computing.jsp

Salesforce (2015b). *10 Benefits of Cloud Computing.* Hämtad 25 maj 2015 från http://www.salesforce.com/uk/socialsuccess/cloud-computing/why-move-to-cloud-10-benefits-cloud-computing.jsp

Smitt, J. (2012). *Använd molnet - på egen risk*. Dagens Nyheter. Hämtad 9 juni 2015 från http://www.dn.se/ekonomi/din-ekonomi/anvand-molnet-pa-egen-risk/

SS-ISO/IEC 27001:2014 (2014). *Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav (ISO/IEC 27001:2013 IDT).* Hämtad 24 april 2015 från https://enav.sis.se/sv/Standard/?std=STD-101246

Statistiska centralbyrån (2014). *IT bland individer, 2014: Sju av tio har använt någon molntjänst.* Hämtad 15 maj 2015 från http://www.scb.se/sv_/Hitta-statistik/Statistik-efter-amne/Levnadsforhallanden/Levnadsforhallanden/IT-bland-individer/15269/15276/Behallare-for-Press/379419/

SUNET (2015). *SUNET Box*. Hämtad 23 maj 2015 från http://www.sunet.se/Tjanster/SUNETs-tjanster-/SUNET-Box.html

Sveriges Riksdag (2015). *Vad är allmänna handlingar?* Hämtad 5 maj 2015 från http://www.riksdagen.se/sv/Sa-funkar-riksdagen/Forvaltningen/Allmanna-handlingar-och-arkiv/Vad-ar-allmanna-handlingar/

Swedish Standards Institute (2015). *Vad är ISO 27000?* Hämtad 12 februari 2015 från http://www.sis.se/tema/ISO27000/Vad_ar_ISO_270001/

Tech Times (2014). *Cloud hacking isn't as hard as most would think.* Hämtad 23 maj 2015 från http://www.techtimes.com/articles/14800/20140903/cloud-hacking-isnt-hard-think.htm

Tétard, F. (2015). *En lathund för intervjuplanering.* Kurslitteratur för kursen "Examensarbete", UU 2015.

The Guardian (2014). *How easy is it to crack into an Apple iCloud account? We tried to find out.* Hämtad 23 maj 2015 från http://www.theguardian.com/world/blog/2014/sep/03/after-nude-celebrity-photos-i-tried-to-hack-my-colleagues-apple-icloud-account

The Guardian (2013). *Why are so many businesses switching to cloud computing?* Hämtad 18 februari 2015 från http://www.theguardian.com/media-network/partner-zone-microsoft/why-businesses-switching-cloud-computing

Twitter (2015). *About.* Hämtad 6 maj 2015 från https://about.twitter.com/company

Universitetskanslersämbetet (2015a). *Lagar och regler som styr högskolan.* Hämtad 9 maj 2015 från http://www.uka.se/studentratttillsyn/lagarochreglersomstyrhogskolan.4.782a298813a88dd0dad800011224.html

Universitetskanslersämbetet. (2014). *Riksuppgifter*. Hämtad 17 februari 2015 från http://www.uka.se/statistikuppfoljning/statistikdatabasomhogskolan/riksuppgifter.4.575a959a141925e81d1b22.html

Universitetskanslersämbetet (2015b). *Så styrs högskolesektorn.* Hämtad 9 maj 2015 från http://www.uka.se/faktaomhogskolan/sastyrshogskolesektorn.4.782a298813a88dd0dad800011790.html

Universitetskanslersämbetet (2013). *Årsrapport 2013.* Hämtad 6 maj 205 från http://www.uka.se/download/18.1c251de913ecebc40e78000854/1403093617550/Arsrapport-2013.pdf

Uppsala universitet (2015). *UU i siffror.* Hämtad 23 maj 2015 från http://www.uu.se/om-uu/i-korthet/siffror/

Vad menas med styrdokument? (2014). Falu kommun. Hämtad 15 maj 2015 från http://www2.lugnet.se/www/edemokrati2.nsf/doc/vadstyr

Visma (2013a). *Vad är en molntjänst? Del 1: SaaS, PaaS och IaaS.* Hämtad 19 maj 2015 från http://www.visma.se/blogg/vad-ar-en-molntjanst-del-1-saas-paas-och-iaas/

Visma (2013b). *Vad är en molntjänst? Del 2: Distributionsmodeller.* Hämtad 19 maj 2015 från http://www.visma.se/blogg/vad-ar-en-molntjanst-del-2-distributionsmodeller/

Yin, R.K. (1984). *Case study research: design and methods*, Newbury Park: Sage Publications, s. 23

YouTube (2015). *Statistics*. Hämtad 5 maj 2015 från https://www.youtube.com/yt/press/sv/statistics.html

Muntliga källor

Berglund, V. *Biträdande säkerhetschef på Uppsala universitet.* Intervju 5 maj 2015.

Berglund, V. *Biträdande säkerhetschef på Uppsala universitet.* Telefonintervju 21 maj 2015.

Blåberg, E. *Systemförvaltare på SUNET.* E-postkorrespondens 13 april 2015.

Edholm, S. *IT-chef på Sveriges Lantbruksuniversitet, SLU*. Intervju 7 maj 2015.

Edholm, S. *IT-chef på Sveriges Lantbruksuniversitet, SLU.* Telefonintervju 8 april 2015.

Edin, M. *IT-chef på Mittuniversitetet*. E-postkorrespondens 23 april 2015.

Hertzell, L. *Informationssäkerhetssamordnare på Karolinska institutet.* E-postkorrespondens 20 maj 2015.

Nejdeby, J. *IT-direktör på Linköpings universitet.* E-postkorrespondens 17 maj 2015.

Persson, M. *IT-arkitekt på Lunds universitet.* E-postkorrespondens 18 maj 2015.

Wallmark, M. *IT-samordnare, IT-ansvarig och webbansvarig på Umeå universitet.* E-postkorrespondens 18 maj 2015.

Öhrn, A. *IT-chef på Örebro universitet.* E-postkorrespondens den 18 maj 2015.

Bild

Figur 1. *Molnet*. Hämtad 23 maj 2015 från http://nyadagbladet.se/wp-content/uploads/2014/09/icloud-1024-450x379.jpg

Bilagor

Bilaga 1 - E-post till universiteten, begäran av styrdokument 41
Bilaga 2 - Dokumentanalysmall - version 1 43
Bilaga 4 - Intervjufrågor 45
Bilaga 5 - Dokumentanalysmall - version 2 (den slutgiltiga versionen) 47
Bilaga 6 - Korta intervjufrågor 49

Bilaga 1 - E-post till universiteten, begäran av styrdokument

Hej,

vi heter Klara Höjenberg och Cecilia Almgren och läser sista terminen av det systemvetenskapliga kandidatprogrammet vid Uppsala Universitet. Vi skriver en C-uppsats på ämnet informationssäkerhet gällande lagringsmolntjänster.

Vi kontaktar er med anledning att en del av vår forskningsprocess är att samla in och analysera utvalda universitets styrdokument för IT-och informationssäkerhet. (Läs gärna vidare information om uppsatsämnet i slutet av detta mail.)

Vi ber er att sända (via e-post) de styrdokument *(namn på universitetet)* har för IT-och informationssäkerhet.

Om vi har skickat denna begäran till fel mottagare för uppgiften ber vi er att meddela oss omgående.

Tveka inte att kontakta oss om ni har frågor gällande detta, eller har ytterligare information eller kommentarer om säkerhetsarbetet rörande molntjänster som ni vill dela med er av. Tack på förhand.

Med vänliga hälsningar,

Klara Höjenberg

Tel.: 0732 517 519

LinkedIn: se.linkedin.com/in/klarahojenberg/

Cecilia Almgren

Tel.: 0738 022 183

LinkedIn: se.linkedin.com/pub/cecilia-almgren/52/14/64a

Ytterligare information om C-uppsatsen samt UU:s systemvetenskapliga kand.program:

Om C-uppsatsen: Vi har valt att fördjupa oss i ämnet informationssäkerhet kring lagringsmolntjänster då det är ett högaktuellt och intressant ämne där utvecklingen och användandet av tjänsterna ökar snabbt. Det rapporteras i media om händelser såsom brott mot PUL, läckt data, hackade tjänster som iCloud och liknande, vilket lyfter frågan om säkerhetsrutiner, arbete, lagar och regleringar hinner med utvecklingen och användandet av denna typ av tjänster. Universitet hanterar stora mängder samt olika typer av känslig data, vilket kräver speciella säkerhetsåtgärder. Som myndighet behöver ett universitet även ta hänsyn till ytterligare faktorer jämfört med vanliga företag och organisationer.

Vi och våra medstudenter använder sig frekvent av lagringsmolntjänster i studierna, och vi har även märkt att lärare och andra anställda på universitetet ibland gör detta. Vi har dock inte tänkt särskilt långt på vad det innebär att ladda upp data i tjänsterna, eller vilka säkerhetsrutiner eller lagar anställda vid universiteten bör ta hänsyn till i sitt användande.

Vi har därför valt att ta oss an den rikstäckande uppgiften att utföra en nulägesanalys av svenska universitets styrdokument och arbetsrutiner kring IT-och informationssäkerhet gällande lagringsmolntjänster.

Programmet: Systemvetenskapliga kandidatprogrammet vid Uppsala Universitet är en bred samhällsvetenskaplig IT-utbildning som ger kunskaper i hur system och program samverkar med individer och grupper inom olika verksamheter. Huvudområde inom programmet är informationssystem. I programmet ingår till exempel kurser i system- och programutveckling, databasdesign, internetbaserade system och ett valfritt ämne. Programmet leder till en filosofie kandidatexamen med informationssystem som huvudområde. Under utbildningen ges studenterna möjlighet att lära sig att utveckla lättillgängliga och effektiva datasystem riktade mot olika branscher såsom media, marknadsföring, handel, bank och finans, spel, försäkring och offentlig service.

Bilaga 2 - Dokumentanalysmall - version 1

Universitet	Har de styrdokument?	Berör de molntjänster?	Står det vilken molntjänst de bör använda?	Följer SS-ISO/IEC 27000?
SU	Ja	Ja	Ja, Box	Ja
Linné	Ja	Ja	Endast molntjänster som det finns skriftliga avtal på central nivå får användas för myndighetsinformation	Ja
SLU	Ja	Nej	Nej	Ja
Umeå	Ja	Nej	Nej	Ja
Uppsala	Ja	Nej	Nej, men tydliga instruktioner om vad som får/inte får laddas upp i molntjänster, samt hur man går till väga för att ev. ingå avtal med molntjänstleverantör.	Ja
Luleå	Ja	Nej	Nej	Ja
KTH*	Ja	Nej	Nej	Nej
Karolinska	Ja	Ja	Nej	Ja
Mittuni.	De skrivs om i nuläget			
Karlstad	Ja	Nej	Nej	Ja
Lund	Ja	Nej	Nej	Nej
Örebro	Ja	Nej	Nej	Nej
Linköping	Ja	Nej	Nej	Ja
Göteborg*	Ja	Ja	Nej	Nej

***** = Svarade aldrig på mailen men gick att få tag på styrdokumenten online.

Bilaga 3 - Intervjuguide

För att ta fram en intervjuguide att stödja oss på vid genomförande av intervjuerna följde vi en lathund för intervjuplanering (Tétard, 2015).

Allmän process för intervjuplanering:
1. Planera intervjuprocessen
2. Arrangera intervjun
3. Genomföra intervjun
4. Sammanfatta intervjun

Vad: Vad är målet? Vilken information/kunskap behöver jag med tanke på målsättningar? På vilket sätt får jag tag på denna information/kunskap?
Mål är att få reda på följande:

Mål med intervjuerna:
För universitet med styrdokument som rör molntjänster

- Syfte - varför har universitetet styrdokument för lagringsmolntjänster?
    - Vilken typ av information är känslig att ladda upp? Varför just denna typ?
      Hur kontrolleras det att styrdokumenten efterföljs?
    - Hur sprids de till olika delar i organisationen?
    - Vem har ansvar för att anställda får information/följer styrdokumenten?
      Vilka blir konsekvenserna om de inte efterföljs?
    - Juridiskt?
    - För universitetet?
    - På individnivå?
      (Hur de togs fram och underhåll.
    - Hur de togs fram
    - Hur ofta ska de ses över och/eller uppdateras?)

För universitet utan styrdokument som rör molntjänster:

- Varför har inte universitetet styrdokument för lagringsmolntjänster?
- Finns planer på att införa det?
    - Om ja, varför och hur ska detta i så fall genomföras?
    - Om nej, varför inte?

Bilaga 4 - Intervjufrågor

Här finns intervjufrågorna, del 1 med frågorna vi ställde till universitet med styrdokument om molntjänster (UU och SU) och del 2 de frågor vi ställde till universiteten utan (SLU och ORU).

1. Universitet med styrdokument om molntjänster (UU och SU)

Intro

1. Kan du berätta lite kort om dig själv och din erfarenhet inom IT-och informationssäkerhetsområdet?
2. Hur länge har du arbetat på UU och vilka är dina arbetsuppgifter och ansvarsområden vid universitetet?

Syfte och bakgrund

1. Vad är UU:s syfte med styrdokumenten för lagringsmolntjänster?
2. Hur gick ni till väga när ni tog fram styrdokumenten?
3. Har ni någon uppfattning om styrdokumenten har gjort skillnad i UU:s informationssäkerhet (har den fyllt sitt syfte)?

Underhåll och efterlevnad

1. Hur kontrollerar UU att styrdokumentens rutiner efterföljs?
2. Vilka blir konsekvenserna om styrdokumentens innehåll inte efterföljs?
   - Juridiskt?
   - För universitetet?
   - För individen?
3. Kan du ge något exempel på säkerhetsproblem med lagringsmolntjänster som har uppstått vid UU?
4. Vad klassar UU som information som ej får spridas eller offentliggöras? (Utöver (känsliga) personuppgifter, kan du ge exempel eller förklara närmare om ni anser att det finns annan information som inte bör läggas upp i lagringsmolntjänster?)
5. Enligt styrdokumenten använder sig UU av MSB:s Modell för klassificering av information.
6. Hur förväntas anställda följa MSB:s modell i praktiken?
7. Har du någon uppfattning om det är genomförbart i det dagliga arbetet?
8. (Hur ofta uppdateras styrdokumenten?)

Molntjänster

1. Enligt din uppfattning, använder eller använde UU:s anställda molntjänster till att lagra information som rör arbetet? (T.ex. Dropbox, Google Drive, OneDrive osv.)
2. Finns det någon/några molntjänster ni rekommenderar respektive undanber de anställda att använda?
3. Känner ni till Sunet Box? Kommer ni att införa Sunet Box? Motivera gärna varför "ja" eller "nej".

2. Universitet utan styrdokument om molntjänster (SLU och ORU)

Intro

1. Kan du berätta lite kort om dig själv och din erfarenhet inom IT-och informationssäkerhetsområdet?
2. Hur länge har du arbetat på SLU och vilka är dina arbetsuppgifter och ansvarsområden vid universitetet?

Syfte och bakgrund

1. Varför har SLU inga styrdokument eller riktlinjer som specifikt rör lagringsmolntjänster?
2. Finns det planer på att införa specifika styrdokument eller riktlinjer för användandet av lagringsmolntjänster?
   a. Motivera "ja"/"nej".

Problematik

1. Upplever du att det finns problem med att anställda vid SLU oreglerat lagrar data i molnet?
    a. Om ja, finns det några exempel på säkerhetsproblem med lagringsmolntjänster som uppstått vid SLU?

Molntjänster och information

1. Finns det någon/några molntjänster ni rekommenderar respektive undanber de anställda att använda?
2. Kommer ni att införa Sunet Box?
3. Vad klassificerar SLU som information som ej får spridas eller offentliggöras?
4. Enligt SLU:s styrdokument följer universitetet MSB:s Modell för klassificering av information. I vilka sammanhang och för vilken lagring gäller denna modell?
    a. Hur förväntas anställda följa MSB:s modell i praktiken, och har du någon uppfattning om det är genomförbart i det dagliga arbetet?

Utöver (känsliga) personuppgifter, kan du ge exempel eller förklara närmare om ni anser att det finns annan information som inte bör läggas upp i lagringsmolntjänster?

Vilka är påföljderna om existerande säkerhetsrutiner inte efterföljs?

a. Skulle dessa skilja sig från påföljderna av brott mot framtida rutiner gällande molntjänster?

Bilaga 5 - Dokumentanalysmall - version 2 (den slutgiltiga versionen)

Universitet	Har de styr-dokument?	Berör de moln-tjänster?	Bakgrundsinfo?	Står det vilken molntjänst de bör använda?	Följer SS-ISO/IEC 27000?	Modell för informations-klassificering	Följer MSB 2009:10
SU	Ja	Ja	Ja	Ja, Box	Ja	Ja	Ja
Linné	Ja	Ja	Ja	Endast molntjänster som det finns skriftliga avtal på central nivå får användas för myndighets-information	Ja	Ja	Ja
SLU	Ja	Nej	Nej	Nej	Ja	Ja	Ja
Umeå	Ja	Nej	Ja	Nej	Ja	Ja	Ja
Uppsala	Ja	Ja	Ja	Nej, men tydliga instruktioner om vad som får/inte får laddas upp i molntjänster, samt hur man går till väga för att ev. ingå avtal med molntjänst-leverantör.	Ja	Ja	Ja
Luleå	Ja	Nej	Nej	Nej	Ja	Ja	Ja
KTH*	Ja	Nej	Nej	Nej	Nej	Nej	Nej
Karolinska	Ja	Ja	Nej	Nej	Ja	Ja	Ja
Mitt-universitetet	De skrivs om i						

	nuläget						
Karlstad	Ja	Nej	Nej	Nej	Ja	Ja	Ja
Lund	Ja	Nej	Nej	Nej	Nej	Ja	Ja
Örebro	Ja	Nej	Nej	Nej	Nej	Nej	Nej
Linköping	Ja	Nej	Nej	Nej	Ja	Ja	Ja
Göteborg*	Ja	Ja	Nej	Nej	Nej	Ja	Nej

***** = Svarade aldrig på mailen men gick att få tag på styrdokumenten online.

Bilaga 6 - Korta intervjufrågor

Dessa frågor skickades ut via e-post till de nio övriga universitet vi inte genomförde längre intervjuer med.

För universitet med styrdokument som rör molntjänster

- Syfte - varför har universitetet styrdokument för lagringsmolntjänster?
    - Vilken typ av information är känslig att ladda upp? Varför just denna typ?
      Hur kontrolleras det att styrdokumenten efterföljs?
    - hur sprids de till olika delar i organisationen?
    - Vem har ansvar för att anställda får information/följer styrdokumenten?
      Vilka blir konsekvenserna om de inte efterföljs?
    - Juridiskt?
    - För universitetet?
    - På individnivå?

För universitet utan styrdokument som rör molntjänster:

- Varför har inte universitetet styrdokument för lagringsmolntjänster?
- Finns planer på att införa det?
    - Om ja, varför och hur ska detta i så fall genomföras?
    - Om nej, varför inte?