Examensarbete

HÖGSKOLAN I SKÖVDE

PRIVAT MOLNLAGRING I ARBETET

En fallstudie om hur ett IT-företag hanterar att anställda använder privat molnlagring för arbetsrelaterad information

PRIVATE CLOUD STORAGE AT WORK

A case study on how an IT company mitigates that employees use their private cloud storage to store work related information

Examensarbete inom huvudområdet informationsteknologi med inriktning mot nätverks- och systemadministration, G2E 22.5 Högskolepoäng
IT610G Vårtermin 2018

2018-06-18

Markus Berg
k15marbe@student.his.se

Handledare: Joakim Kävrestad
Examinator: Marcus Nohlberg

Sammanfattning

Denna fallstudie har undersökt och studerat hur ett företag som arbetar med informationsteknologi (IT) hanterar problemet att anställda lagrar arbetsrelaterad information i sina privata molnlagringstjänster. En enkätundersökning gjordes för att undersöka och jämföra hur olika avdelningar på företaget bland annat använder sin privata molnlagringstjänst och om de är medvetna om risker med molnlagring. En intervju genomfördes med en informant från företaget för att kontrastera svaren från enkätundersökningen. Vidare genomfördes också en valideringsintervju med en informant från ett annat företag som arbetar inom samma bransch.

Resultatet visade att anställda som arbetar inom IT-branschen faktiskt lagrar eller har lagrat arbetsrelaterade information i sina privata molnlagringstjänster. En av avdelningarna som deltog i enkäten var informationssäkerhetsteamet. Anställda som arbetar med informationssäkerhet kan antas vara mest pålästa och kunniga vad gäller säkerhet kring information, trots det så visade resultatet att dessa personer var de som använde privat molnlagring mest, i jämförelse med övriga avdelningar. Vidare så visar resultatet också att företagen arbetar med att motverka och upplysa anställda om risker med hur information hanteras, det ena företaget i synnerhet arbetar väldigt proaktivt och tar informationssäkerhet på stort allvar.

Nyckelord: Molnlagring, privat molnlagring, säkerhet i molnet

Abstract

In this work, a case study was made on one company that is working with IT. The study was made to see how an IT company mitigates and handles the problem that employees use their private cloud storage to store work related information. A survey was sent to three different departments at the company to examine what employees think about private cloud storage and work related information and how and if it differs between different departments. One interview was also made with one informant from the same company to compare with the results from the survey. A second interview with another company was also made to validate the result from the first interview.

The results from the survey showed that employees do store or have stored work related information in their private cloud storage, despite that the company policies forbid it. One of the departments that the survey was sent to was the information security team. It can be assumed that employees that work with information security have better understanding about security regarding information and how it should be stored. Despite that did the results show that the information security team was the department that used private cloud storage the most, compared to the other departments. The results from the interviews shows that the companies at least have policies on how and where the employees are allowed to store work related information. One company in particular works really hard and continuously to educate and enlighten its employees to take great care when dealing with work related information.

Keywords: Cloud storage, private cloud storage, cloud security

Innehållsförteckning

1 Introduktion 1
2 Bakgrund 2
2.1 Vad är molnlagring? 2
2.2 Säkerhet i molnlagring 4
2.3 Relaterade arbeten 5
3 Problemformulering 7
3.1 Syfte 7
3.2 Motivering 7
3.3 Forskningsfråga 7
3.4 Mål och förväntat resultat 8
3.5 Delmål 8
3.6 Avgränsning 9
4 Metod 10
4.1 Strategi 10
4.1.1 Enkätundersökning 11
4.1.2 Intervjuer 12
4.2 Validitet och reliabilitet 13
4.3 Etiska aspekter 14
5 Genomförande 16
5.1 Enkätundersökning 16
5.2 Intervjuer 17
6 Resultat och analys 18
6.1 Enkätundersökning - informationssäkerhetsteamet 18
6.2 Enkätundersökning - kontorschefer 24
6.3 Enkätundersökning – controllers 29
6.4 Analys av enkätundersökning 34
6.5 Intervjuer 39
6.6 Analys av intervjuer 43
7 Slutsats 45
8 Diskussion 46
8.1 Framtida arbete 47
Referenser 48

1 Introduktion

I detta arbete har en fallstudie gjorts för att se hur ett företag som arbetar med IT hanterar problemet att anställda använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information. Molnlagring är idag något som nästan varje människa använder sig av bara genom att ha en smarttelefon som exempelvis en iPhone. Bilder och annan information från mobiltelefonen synkroniseras upp till molnet och detta kan dessutom vara omedvetet. Eftersom att Internet och infrastrukturen kring Internet konstant växer möjliggör det för privatpersoner att alltid kunna komma åt sina filer i molnet.

Däremot så medför molnlagring vissa risker jämfört med lokal lagring. Amara, Zhiqui och Ali (2017) förklarar att det finns risker som exempelvis dataintrång, att kontot kan bli hackat eller dataförlust inträffar. Att information dessutom lämnas över till någon annan som ska ta hand om och säkerställa att information inte läcker eller är intakt är ytterligare en risk som tas. Amara et al. (2017) nämner dessutom att molnleverantörer som Apple, Microsoft, Yahoo och Google har råkat ut för dataintrång vilket bevisar att det inte är helt säkert. Det är en avvägning som får göras och beroende på vad det är för typ av information så kanske informationen inte ska lagras i molnet överhuvudtaget.

Tidigare studier, bland annat den gjord av Lindberg, Marat och Månsson (2015) påvisar att anställda faktiskt använder eller har använt sin privata molnlagringstjänst för att lagra arbetsrelaterad information så detta problem är etablerat. Om tidigare nämnda risker tas med i beräkningen och det faktum att stora molnleveranöterer tidigare har råkat ut för dataintrång kan det vara ett väldigt stort problem om anställda lagrar arbetsrelaterad information i sina privata molnlagringstjänster. Skulle exempelvis känslig kundinformation eller företagshemligheter lagras i en privat molntjänst som sedan råkar ut för dataintrång, eller att kontot blir hackat så kan det få förödande konsekvenser för både företaget och den anställda.

I arbetet, som tidigare nämnt, som undersökt hur ett företag inom IT-branschen motverkar detta problem så har dels en enkätundersökning skickats ut till anställda på olika avdelningar på företaget och två intervjuer har gjorts med två informanter, en intervju gjordes med en informant från företaget som fallstudien gjordes på. Den andra intervjun gjordes med ett annat företag för validering. Enkätundersökningen skickades ut till informationssäkerhetsteamet, kontorschefer och controllers på företaget. Informanten från företaget som studien fokuserade på jobbar som senior informationssäkerhetskonsult och den andra informanten från det andra företaget är säkerhetsansvarig.

2 Bakgrund

I detta kapitel ges en bakgrund till vad molntjänster är för något och hur säkerheten för molntjänster ser ut. Kapitlet tar också upp relaterade studier gällande hur privat molnlagring används för företagsinformation samt medvetenhet hos anställda gällande risker med molnlagring.

2.1 Vad är molnlagring?

Molnlagring är en så kallad molntjänst och Armbrust et al. (2010) beskriver att molntjänster innefattar både mjukvara i form av applikationer, hårdvara och system i datacenter som hanterar applikationerna. Applikationer levereras som tjänster över Internet till kunder och datacenter ansvarar för applikationerna som levereras. Hårdvaran i datacenter kan exempelvis vara hårddiskar för lagring. Ett exempel är Google som har sina egna datacenter och applikationer som exempelvis Google Drive vilken är en applikation som erbjuder kunder lagring. Google Drive är en applikation som levereras som en tjänst till kund. Andra exempel på molnlagringstjänster är Dropbox, Amazon Drive och iCloud.

Molntjänster behöver inte nödvändigtvis vara något som ett företag låter en tredje part hantera, ett företag kan också ha ett eget privat moln. Mell & Grance (2011) förklarar att molntjänster definieras av fem karaktärsdrag, tre servicemodeller och fyra distrubitionsmodeller. De fem karaktärsdragen är *On-demand self-service*, *Broad network access*, *Resource pooling*, *Rapid elasticisty* och *Measured service*.

- *On-demand self-service* innebär att kunder, utan någon interaktion med leverantören av molntjänsten, kan nyttja tjänster som lagring eller hårdvaruresurser i molnet av leverantören.

- *Broad network access* möjliggör att tjänster ska vara tillgängliga över nätverket och kunna nås genom exempelvis bärbara datorer eller mobiltelefoner.

- *Resource pooling* innebär att leverantörens resurser slås samman för att kunna hantera flera kunder samtidigt. Fysiska och virtuella resurser fördelas efter behov och krav från kunden och kunden har nödvändigtvis ingen större uppfattning om var någonstans dessa resurer finns, d.v.s. i exempelvis vilket datacenter eller vilken stad. Resurser kan exempelvis vara lagringsutrymme, processorkraft eller nätverksbandbredd.

- *Rapid elasticity* innebär att resurser dynamiskt kan anpassas, både ökas och minskas, detta för att möta skillnader i krav och behov från kunden. För kunden anses ofta att leverantörens tillgängliga resurser är oändliga.

- *Measured service* syftar på att resursanvändning monitoreras och kontrolleras automatiskt för att optimera resursfördelningen.

Mell och Grance (2011) beskriver att de tre olika servicemodellerna av molntjänster är; *Software as a Service* (SaaS), *Platform as a Service* (PaaS) och *Infrastructure as a Service* (IaaS).

- *SaaS* innebär att kunden via olika typer av enheter nyttjar leverantörens applikationer som körs som en mlontjänst. Enheter kan vara exempelvis en mobiltelefon eller en bärbar dator som via en applikation eller webbläsare kommer åt leverantörens applikation. Ett exempel på en SaaS-tjänst kan vara Googles e-posttjänst Gmail. Med SaaS har kunden ingen som helst kontroll av resurserna som används utan det är helt upp till leverantören att ansvara för applikationer och hårdvara som möjliggör molntjänsten. Däremot kan kunden ändra vissa inställningar i applikationen som nyttjas.

- *PaaS* erbjuder kunden en plattform där kunden kan skapa programvara. Leverantören erbjuder verktyg som exempelvis programmeringsspråk och kontrollerar den underliggande infrakstrukturen som nätverk, servrar, operativssystem och lagring. Kunden har kontroll över applikationer som denne skapar och vissa inställningar i miljön där applikationen distribueras. En PaaS-tjänst kan exempelvis vara Microsoft Azure.

- *IaaS* innebär att leverantören erbjuder hårdvaruresurser i form av bland annat processorkraft, lagring och nätverk. Kunden kan sedan använda dessa resurser för att exempelvis skapa virtuella maskiner i leverantörens moln. Kunden har full kontroll över operativssystem, lagring och distribuerade applikationer. Leverantören kontrollerar den underliggande infrastrukturen för molntjänsten.

De fyra distributionsmodellerna som Mell och Grance (2011) beskriver är; *Private Cloud, Community Cloud, Public Cloud* och *Hybrid Cloud*.

- *Private Cloud* innebär att molninfrastrukturen är endast tillgänglig för en enskild organisation. Infrastrukturen kan ägas och kontrolleras av organisationen själva, en tredje part eller en kombination av dessa. En privatperson kan också skapa ett privat moln med egna resurser hemma.

- *Community Cloud* är en typ av molntjänst som endast är tillgänglig för en grupp av organisationer som delar på molntjänsten så att säga. Det kan handla om organisationer som har samma mål eller behöver samarbeta. Exempel på organisationer som nyttjar denna typ av molntjänst kan vara regeringar eller sjukvård. Molntjänsten kan ägas och hanteras av en eller flera av organisationerna, en tredje part eller en kombination av dessa två.

- *Public Cloud* är en typ av molntjänst som erbjuder resurser och är tillgänglig för offentligheten. Den kan ägas och kontrolleras av exempelvis ett företag eller en akademisk verksamhet. Ett exempel på en sådan typ av molntjänst kan vara Googles molntjänstinfrastruktur som erbjuder bland annat lagring.

- *Hybrid Cloud* är en kombination av två eller fler av de tidigare nämnda distributionsmodeller. Det ger möjligheten att låta kunden välja att använda sitt privata moln för vissa saker och det publika för andra. Kunden kan äga och kontrollera ett privat moln med egna resurser men också nyttja resurser av en leverantör vid behov och avlastning.

2.2 Säkerhet i molnlagring

Säkerhet inom IT är ständigt på tapeten då mer och mer information digitaliseras och molntjänster blir mer och mer vanligare. Hur kan organisationer eller privatpersoner veta med säkerhet att informationen de lagrar i en molntjänst som hanteras av en tredje part, exempelvis Google, är skyddad? Informationen och ansvaret på hur den lagras och hanteras läggs faktiskt helt och hållet över till en annan part. Det betyder dock inte att det är riskfritt även om en organisation äger och kontrollerar en egen molntjänst, informationen bör fortfarande skyddas mot exempelvis otillåten åtkomst.

När det gäller säkerhet för information så bör hänsyn tas för flera aspekter. MSB (2017) skriver att information bör skyddas så att tillgänglighet, riktighet, konfidentialitet och spårbarhet bevaras. Med tillgänglighet menas det att information alltid är tillgänglig när den behövs. Riktighet innebär att informationen inte har manipulerats på något sätt, att den är korrekt. Konfidentialitet innebär att endast behöriga personer får komma åt informationen. Spårbarhet innebär att det ska gå att spåra hur information exempelvis har hanterats.

Amara et al. (2017) beskriver att det trots allt finns fördelar med molntjänster så finns även ett flertal hot mot säkerheten gällande molntjänster. Några av hoten som beskrivs är exempelvis dataförlust, dataintrång, kontohackning eller identitetsstöld. Dessa är några av hoten som finns mot molntjänster, de behöver inte vara unika hot mot just molntjänster men de är likväl ett hot. Det är något som bör beaktas om en organisation eller privatperson bestämmer sig för att använda molnlagring för information. Det möjliggör en ”off-site”-backup eftersom att information också finns lagrad någon annanstans än lokalt och det är en bekväm lösning som kräver en liten insats för att konfigurera. Flera av de stora molnleverantörerna erbjuder dessutom en applikation till datorn som automatiskt synkroniserar filer mellan datorn och molnet. Ett exempel på en sådan applikation är Googles *Säkerhetskopiera och Synkronisera*. Denna applikation synkroniseras med Googles tjänst Google Drive som också går att nå från en webbläsare. Dessutom så kan applikationen installeras på flera datorer och filer synkroniseras då mellan dessa datorer och Google Drive (Google, u.å.). Ur ett användarperspektiv är detta väldigt bekvämt men det kan också innebära risker i form av att skadliga filer som drabbar en dator synkroniseras då över till övriga datorer. Skulle exempelvis en anställd ha denna applikation installerad på sin privata dator hemma och sin arbetsdator så innebär det att virus eller skadliga filer kan synkroniseras mellan datorerna. Blir den anställdas privata dator infekterad med ett virus som exempelvis infekterar filer på datorn, inklusive filerna i molnlagringsapplikationen så synkroniseras dessa infekterade filer även till arbetsdatorn vilket i sin tur skulle kunna sprida viruset vidare i företagets nätverk.

Att vara medveten om att hot och risker finns mot säkerheten för molnlagring är som sagt något att ta hänsyn till. Nyttjas en molnleverantör för privat molnlagring bör det funderas över

på vilken typ av information som ska lagras där. Ska informationen krypteras innan den skickas upp i molnet? Krypterar molnleverantören informationen som lagras? Amara et al. (2017) skriver också att molnleverantörer som Apple, Microsoft, Yahoo och Google dessutom har råkat ut för dataintrång vilket ytterligare visar på att det inte alltid är helt säkert att använda molnlagring.

2.3 Relaterade arbeten

Lindberg et al. (2015) gjorde en studie om privat molnlagring inom arbetet. Studien ämnade att besvara två forskningsfrågor; *Vilka potentiella risker associeras med lagring i externa molntjänster?* och *Varför väljer anställda att lagra yrkesrelaterad data i privata molntjänster före verksamhetens egen lagringstjänst?*. Studien intervjuade sex anställda på två företag inom IT-branschen. Båda företagen är ungefär lika stora och har lika många anställda. Det ena företaget erbjuder kompletta helhetslösningar som exempelvis infrastruktur och datalagring. Det andra företag jobbar endast med att underhålla företagskunder gällande kommunikation och teknisk infrastruktur.

Lindberg et al. (2105) beskriver också vilka risker som finns med molnlagring och undersöker också om de anställda är medvetna om vilka risker som medförs vid användning av molnlagring, särskilt om det är arbetsrelaterad information som lagras i en privat molnlagringstjänst. Intervjuerna skedde med anställda med olika roller inom respektive företag. Bland annat var det beslutsfattare i form av en IT-chef och en avdelningschef men också anställda på en operativ nivå som exempelvis en mjukvaruutvecklare. Studiens resultat visade att det förekommer att vissa av informanterna faktiskt aktivt lagrar arbetsrelaterad information i sina privata molnlagringstjänster. En orsak till detta är att de privata molnlagringstjänsterna, som exempelvis Google Drive eller Dropbox, är mer tillgängliga och smidigare än företagets egna lagringstjänster. Utöver det visar också studien att det saknas en tydlig policy angående hur arbetsrelaterad information får lagras eller att policys faktiskt efterlevs av de anställda.

Studien utförd av Lindberg et al. (2015) bekräftar det faktum att anställda faktiskt lagrar arbetsrelaterad information i sin privata molnlagringstjänst. Orsakerna till detta kan tyckas vara enkla att motverka men om säkerhet inte tas på allvar genom exempelvis policys och uppföljning av dessa eller att företagen erbjuder en egen lättillgänglig lagringstjänst så vänder sig anställda uppenbarligen till privata molnlagringstjänster.

Ashford (2015) skriver om en undersökning av 1000 kontorsanställda i Storbritannien som visade att många anställda använder privata molnlagringstjänster som Google Drive och Dropbox för att lagra arbetsrelaterad information. Undersökningen utfördes av säkerhetsföretaget WinMagic. Vidare skriver Ashford (2015) att företag i Storbritannien riskerar att råka ut för intrång och förlust av information genom det ökande användandet av molnlagringstjänster samtidigt som policys för hur dessa får användas är oklara eller inte existerar överhuvudtaget. Undersökningen visade att 41 % av de anställda använder sin privata molnlagringstjänst minst en gång i veckan och 50 % använder privat utrustning för att komma åt arbetsrelaterad information minst en gång i veckan. Undersökningen visar också att

det endast är 35 % av de anställda som använder en tjänst som är godkänd av företaget och 22 % är inte ens medvetna om att deras företag har policys för molnlagring.

Ashford (2015) förklarar också att företag stöter på stora utmaningar genom att privat molnlagring i arbetet ökar, detta då företagen tappar kontroll över informationen om den lagras i anställdas privata molnlagringstjänster. Företagen måste bli bättre på att tydliggöra och förmedla deras policys för hur information får lagras samt utbilda personal. Dessutom föreslås det att all information kan krypters innan de anställda får möjligheten att kunna ladda upp den i sina privata molnlagringstjänster. Genom kryptering i ett tidigt skede kan det hjälpa till att skydda information från obehöriga. Ashford (2015) skriver att denna undersökning är tänkt att upplysa och göra företag medvetna om problemet och dess risker för att förmedla och utbilda sina anställda för att motverka problemet.

En annan studie utförd av Mijuskovic och Ferati (2015) undersökte medvetenheten hos personer som använder molnlagring för att lagra sin information. Målgruppen i den studien var anställda inom IT-branschen och studerande i Makedonien. Studien undersökte hur medvetna användarna är om risker gällande integritet och säkerhet för molnlagringstjänsterna Google Drive, Dropbox och OneDrive. Trots att studien gjordes på användare i Makedonien så kan det göras en jämförelse med denna studie, detta eftersom båda studierna har anställda inom IT-branschen som målgrupp. I studien skickades en enkät ut över Internet och 28 personer deltog, 14 anställda i IT-branschen och 14 studenter inom IT.

Resultaten från studien gjord av Mijuskovic och Ferati (2015) visar på att studenter är generellt sett mer medvetna om risker gällande integritet och säkerhet än de anställda. Med det sagt så gäller inte det för alla frågor som ställdes. Exempelvis så visade svaren från undersökningen att de anställda var mer medvetna om säkerhet gällande lagring medans studenterna var mer medvetna om bland annat förlorad kontroll och fysisk säkerhet. Resultaten visar också att båda grupperna var lika medvetna om att risker som obehörig delning av filer kan uppstå och att intregritet kan förloras vid delning av filer. På frågan "*Would you be able to explain some of the security and privacy weaknesses that are mentioned above?"* gav 14% av de anställda en knapphändig beskrivning av några problem rörande integritet och säkerhet och lika många studenter är medvetna om risker gällande integritet och säkerhet. Vidare så visar resultaten att det är nästintill ingen skillnad i resultaten beroende på kön. Män och kvinnor svarade i stort sett lika.

Mijuskovic och Ferati (2015) drar slutsatsen att resultaten inte motsvarar det förväntade resultatet. Exempelvis listas olika risker, bland annat förlorad kontroll, delad miljö och fysisk säkerhet som svarsalternativ till frågan "*What are the privacy and security weaknesses/issues you have heard of or you know about*" och resultatet visar att både studenterna och de anställda inte har den kunskap om de olika riskerna som förväntades. Vidare så påvisar resultaten totalt sett att det finns en medvetenhet hos de tillfrågade men kunskap om risker och hur dessa kan motverkas eller minimeras är inte så pass stor som författarna förväntade sig.

3 Problemformulering

Detta kapitel beskriver syftet med studien och vilka forskningsfrågor som studien ska besvaras. Utöver det så beskrivs också förväntat resultat av studien.

3.1 Syfte

Syftet med denna fallstudie är att undersöka hur ett IT-företag hanterar och motverkar problemet med att anställda använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information. Eftersom studien är en fallstudie så är syftet också att undersöka och jämföra hur anställda på olika avdelningar inom företaget ser på säkerhet gällande molnlagring och om de använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information. Som tidigare nämnt är molnlagring väldigt stort idag och det är mycket på grund av nätverksinfrastrukturen som konstant utvecklas världen över. Våra förbindelser från både hemmet och arbetsplatsen blir bara snabbare och snabbare men även våra mobila förbindelser blir snabbare. Det är idag inte ovanligt att en mobil uppkoppling är lika snabb eller snabbare än vad vissa hem har. Det kan också antas att IT-företag ska ligga i framkant vad gäller hantering av detta problem, därför är det av intresse att undersöka IT-företag för att kunna visa och motivera företag inom samma och andra branscher hur problemet kan hanteras.

3.2 Motivering

Studien utförd av Lindberg et al. (2015) och även den undersökning som Ashford (2015) rapporterar om bekräftar det faktum att anställda använder privat molnlagring för att lagra arbetsrelaterad information och därför går det inte att förbise problemet. Studien som Mijuskovic och Ferati (2015) gjorde visar också att medvetenheten gällande säkerhet för molnlagring inte alltid är tillräcklig, även för anställda inom IT. I studien som Lindberg et al. (2015) gjorde intervjuades totalt sex personer på två olika företag.

Till skillnad från tidigare studier så är tanken med denna studie att få information från en bredare massa genom bland annat en enkätundersökning. En enkätundersökning görs för att bland annat undersöka om det är mer regel än undantag att anställda använder privat molnlagring för arbetsrelaterad information och för att skapa underlag för intervjuer.

Genom att göra en fallstudie för att kunna påvisa i vilken utsträckning anställda använder privat molnlagring för arbetsrelaterad information så kan detta upplysa både anställda och ansvariga på företaget om att det faktiskt sker. Som tidigare nämndes i bakgrundskapitlet så finns det risker med att lagra information i molnet och skulle företagsinformation läcka eller hamna i fel händer kan det bli en negativ påverkan på företaget.

3.3 Forskningsfråga

För att precisera problemet ytterligare så är det i synnerhet en övergripande fråga som studien ska besvara:

- *Hur hanterar ett IT-företag att användare lagrar arbetsrelaterad information i privata molnlagringstjänster?*

Denna fråga är det tänkt att studien ska svara på. Det kan antas att IT-företag generellt har ett högre säkerhetstänk och jobbar med att motverka detta problem jämfört andra branscher som inte är verksamma inom IT. Däremot har tidigare studier bekräftat att det förekommer att anställda lagrar arbetsrelaterad information i sin privata molnlagring. Därför blir den stora frågan, som sagt, att studera hur ett IT-företag hanterar problemet.

3.4 Mål och förväntat resultat

Målet med denna studie är att belysa det faktum att molnlagring inte bara är bekvämt och enkelt att utnyttja, utan att det också kommer med vissa risker jämfört med lokal lagring. Dessutom är tanken att studien ska upplysa IT-företag att det faktiskt förekommer att anställda lagrar arbetsrelaterad information på detta vis. Lindberg et al. (2015) har med deras studie visat att anledningar till varför det förekommer att anställda väljer att lagra arbetsrelaterad information i sin privata molnlagring bland annat är på grund av att företaget i sig inte har en egen lagringstjänst som är lika smidig eller att policys för hur information får lagras saknas. Genom att tydliggöra orsaker till varför problemet finns underlättar det för IT-företag att motverka problemet genom att exempelvis implementera policys eller utbilda personal. Dessutom är målet med studien att undersöka hur IT-företag arbetar med att motverka eller förhindra problemet, om det exempelvis är på teknisk nivå eller genom policys och riktlinjer.

Denna studie förväntas tydliggöra och presentera att problemet existerar men också orsaker till varför det existerar. Som tidigare nämnt kan företag behöva upplysas om att det förekommer. Att information, oavsett vilken typ, lagras på molnet hos en extern molnleverantör innebär inte per automatik att den exempelvis kommer att avlyssnas av obehöriga men risken ökar däremot eftersom informationen ligger lagrad i någon annans händer. Studien förväntas också ge anställda, som genom att svara på en enkät, en tankeställare att det faktiskt finns risker med att lagra information i molnet. Det kan faktiskt vara så att anställda kanske inte är medvetna om vilka risker som finns. Studien förväntas också visa att anställda inom IT har en viss medvetenhet när det gäller risker, säkerhet och molnlagring.

Det förväntade resultatet när det gäller hur ett IT-företag arbetar med att motverka eller förhindra problemet är att företaget åtminstone har policys och riktlinjer för hur de anställda får hantera och lagra arbetsrelaterad information.

3.5 Delmål

För att nå målet med studien har två delmål delats upp. Det första delmålet är att göra en enkätundersökning bland anställda på olika avdelningar på ett IT-företag. Det görs för att skapa underlag för intervjuer och visa i vilken utsträckning anställda använder privat molnlagring för arbetsrelaterad information och dessutom identifiera orsaker till varför det sker ur en anställds perspektiv.

Det andra delmålet är att genomföra en intervju med en säkerhetsansvarig person på IT-företaget för att undersöka hur problemet motverkas och kontrastera svaren från enkätundersökningen med exempelvis vilka riktlinjer och policys som finns på företaget.

Dessutom kommer en valideringsintervju att ske med ytterligare ett företag som arbetar inom IT-branschen.

3.6 Avgränsning

Molnlagring och molntjänster generellt är ett väldigt brett område. Denna studie avgränsas dels till att undersöka hur molnlagring används av anställda i arbetet men framförallt om och hur ett IT-företag och ansvariga inom IT-företag motverkar detta problem. Företagen som denna studie avgränsas till är två företag med kontor i Sverige, företag A och företag B. Studien är en fallstudie vilket innebär att fokus kommer att ligga på företag A. Företag B används i studien som en validering.

Företag A är verksamma på fler än 30 orter i Sverige. Företaget har fler än 2000 anställda i Sverige och är ledande inom IT-infrastruktur och system för både privat och offentlig sektor. Företaget erbjuder heltäckande lösningar inom IT-infrastruktur för sina kunder där lösningar kan skräddarsys för att passa kundens behov. Företaget kan ta hand om kundens hela IT-infrastruktur eller vissa delar. Dessutom är företaget återförsäljare av IT-produkter vilket låter kunden handla produkter direkt från företaget.

Företag B är verksamma på fyra orter i Sverige och har drygt 300 anställda. Likt företag A så erbjuder företag B heltäckande lösningar inom IT-infrastruktur till företag och organisationer. Även företag B kan ta över och hantera hela kundens IT-infrastruktur eller delar av den. Företaget förfogar över egna datahallar dit kunden kan flytta hela sin IT om så önskas. Företaget värderar kundrelationer väldigt högt och företaget har vuxit fram snabbt de senaste åren och har ökat i både omsättning och personalstyrka.

Det kan antas att anställda på företag inom IT har mer kunskap om säkerhet och risker gällande molnlagring jämfört med andra branscher som inte är inom IT. Eftersom studien avgränsas till en fallstudie av ett företag ger inte studien ett generellt resultat om hur företag och anställda ser på säkerhet och molnlagring i allmänhet. Resultatet av denna studie kan bli helt annorlunda om studien görs på företag och anställda på andra företag i samma bransch eller i andra branscher.

Studien syftar inte till att fokusera på en särskild leverantör av molnlagring utan snarare om anställda använder en privat molnlagring av en annan leverantör än sitt egna företag. Dessutom syftar studien att undersöka två olika perspektiv. Ena perspektivet är utifrån de anställda och hur de använder privat molnlagring för arbetsrelaterad information och varför. Det andra perspektivet är utifrån systemadministratörer eller ansvariga för IT och säkerhet inom företagen för att se deras syn på detta problem och hur det motverkas eller kan motverkas.

4 Metod

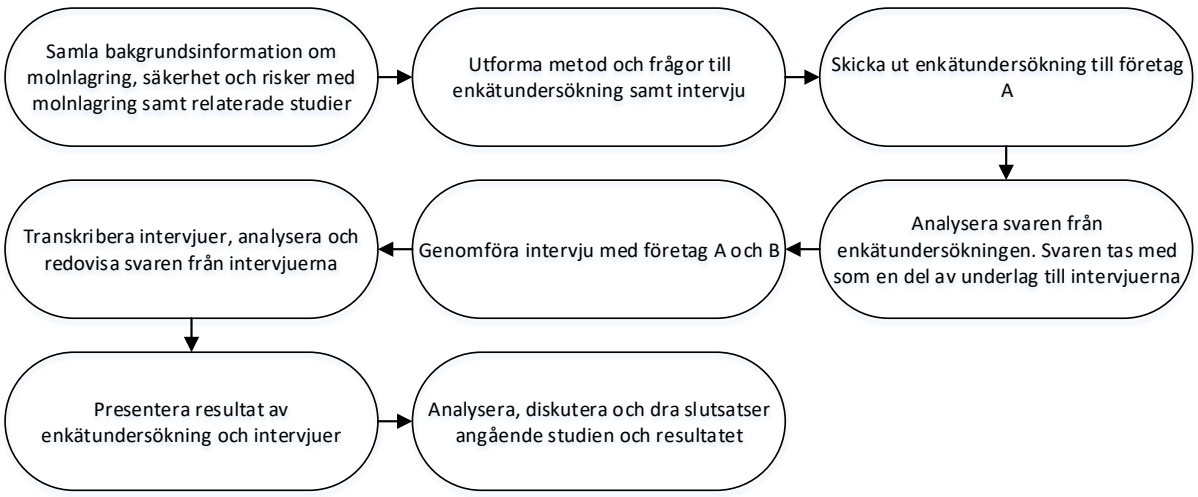
Berndtsson, Hansson, Olsson & Lundell (2008) förklarar att det är av stor vikt att ett mål med studien är satt innan val av metod sker. Om en studie dessutom har flera mindre mål som ska klaras för att nå det slutgiltiga målet kan olika metoder behöva användas. Detta kapitel beskriver studiens övergripande strategi samt val av metoder.

4.1 Strategi

För att besvara forskningsfrågan kommer en fallstudie genomföras på företag A samt en valideringsintervju med företag B. Två olika metoder kommer att användas för att samla in information och presentera ett resultat. Den ena metoden är kvantitativ och består av en enkätundersökning. Denna är tänkt att gå ut till anställda som tillhör olika avdelningar på företag A och ska besvara frågor som handlar om de använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information och orsaker till varför det sker. Enkäten kommer även användas för att besvara om de anställda är medvetna om vilka risker molnlagring medför. Enkäten går ut till olika avdelningar på företaget för att kunna jämföra om det finns skillnader hos anställda som har olika roller i företaget.

Den andra metoden är kvalitativ och består av intervjuer. En intervju kommer att ske med en ansvarig på företag A för att jämföra svaren från enkäten med hur det faktiskt ser ut på företaget vad gäller exempelvis policys och riktlinjer för privat molnlagring. Dessutom är det tänkt att intervjun ska resultera i att visa hur företaget arbetar med att motverka problemet. En valideringsintervju kommer också genomföras med företag B som arbetar i samma bransch för att jämföra hur företagen arbetar med att motverka problemet.

Den övergripande strategin som helhet för studien visas i figur 1. Figuren visar de olika stegen i vilken studien utförs. Det första steget som bland annat består av att samla information om molnlagring togs upp i kapitel 2.



Figur 1. Övergripande strategi för studien.

4.1.1 Enkätundersökning

Berndtsson et al. (2008) förklarar att en enkätundersökning är ett sätt att snabbt nå en bred massa och därmed kunna få in information från många olika individer. En bra formulerad enkät kan ge informativa svar på det som efterfrågas och det kräver ingen större insats från den deltagande. Det är däremot av stor vikt att frågorna som ställs i en enkät är lättförståeliga för den deltagande, detta för att kommunikation mellan författaren och den deltagande inte existerar och är den deltagande osäker på frågan kan det istället ge ett missvisande svar och göra att den deltagande tappar intresset för enkäten. För att försöka motverka att svaren i enkäten blir missvisande eller att den deltagande ska tappa intresset kommer enkäten att försöka ställa så precis frågor som möjligt. Om frågorna är lättförståeliga och inte behöver långa svar så är förhoppningen att det ökar svarsfrekvensen.

Robson (2002) förklarar vidare att enkätundersökningar har vissa nackdelar generellt sett, bland annat att deltagare kan svara på ett sådant sätt att de får sig själva att framstå som en bättre person. Det skulle kunna påverka resultatet om deltagare inte svarar vad de faktiskt känner. När det gäller enkätundersökningar där deltagarna själva svarar utan någon interaktion med författaren så finns det en risk för låg svarsfrekvens, att frågor missuppfattas eller feltolkas eller att deltagarna inte svarar seriöst. Det kan som författare vara svårt att avgöra. Robson (2002) beskriver också vilka fördelar det finns med enkätundersökningar. Generellt sett gällande enkätundersökningar är att det, bland annat, är ett relativt enkelt tillvägagångssätt för att studera attityder, värderingar och motiv. Fördelar med just enkätundersökningar som deltagarna svarar på utan någon interaktion med författaren är att det är ett väldigt effektivt sätt att samla in mycket data på kort tid och med en liten insats. Dessutom erbjuds anonymitet vid denna typ av enkätundersökning vilket kan underlätta för deltagare att svara ärligt.

Med tanke på att enkäten är till för att samla in data från en större massa så används en kvantitativ metod som sedan kan översättas till statistik och siffror. Enkäten skickades ut över Internet till deltagarna som själva får fylla i enkäten, ur författarens perspektiv kräver det väldigt lite tid för att nå ut till många möjliga deltagare. Robson (2002) beskriver olika typer av skalor som kan användas vid enkätundersökningar, en av dessa är en likertskala. Enkäten använder delvis denna skala eftersom att denna typ av enkät är relativt enkel att utforma. Dessutom kan denna typ av skala se intressant ut för deltagarna och de svarar oftast med nöje. Det kan vara avgörande för svarsfrekvensen och seriositeten hos deltagarna. Är något intressant är det större chans att få svar från deltagare. Eftersom vissa frågor ställs för att ren fakta ska kunna samlas in så används också frågor som enbart genererar svaren *ja* eller *nej*. Robson (2002) förklarar även med instruktioner hur en sådan skala utvecklas och enkäten kommer utformas med hjälp av dessa instruktioner. Vid analysen av enkätresultaten så presenteras och jämförs svarsresultaten mellan de olika avdelningarna. Svaren för varje fråga presenteras i grafiska skalor. Beroende på vilken svarsform som använts för frågan så presenteras resultaten i cirkeldiagram eller stapeldiagram.

4.1.2 Intervjuer

Berndtsson et al (2008) förklarar att en intervju kan genomföras på olika sätt och kan formas så att rätt och relevant information kommer fram, olika typer av intervjuer har olika styrkor och svagheter. En öppen intervju är en vanlig typ av intervju vid kvalitativ forskning. En sådan typ av intervju innebär att forskaren på förhand inte har någon kontroll på saker som kan komma upp under intervjun, trots att syftet med intervjun är bestämt. Intervjun kan istället formas efter vad informanten svarar och styras åt vad informanten verkar ha mer kunskap om eller vad denne tycker är intressant. Ledande eller stängda frågor som endast kan besvaras med *ja* eller *nej* bör också undvikas. Fördelen med denna typ av intervju är att information som är relevant för intervjun är det som behandlas, detta för att kontrollen ligger mer hos informanten och att denne får prata fritt om det berörda området. Öppna frågor kan blandas med mer precisa för att ge informanten möjlighet att både prata fritt men också för att intervjuaren ska kunna fastställa någonting genom en mer precis fråga.

Berndtsson et al. (2008) förklarar att motsatsen till en öppen intervju är en stängd intervju där frågor är bestämda på förhand och inga ändringar gällande frågorna görs. Fördelen med denna typ av intervju är att intervjuaren kan kontrollera intervjun på ett helt annat sätt och bestämma vad denne vill ha svar på. Nackdelen blir att informanten kan bli inlåst och svaren på de frågor som ställs kan bli missvisande och informanten kan tappa motivation om denne inte får möjlighet att svara öppet. Denna typ av intervju används vanligtvis vid kvantitativ forskning.

Med tanke på att en kvantitativ enkätundersökning kommer göras bland anställda så kommer intervjuerna vara mer kvalitativa än kvantitativa. Syftet med intervjuerna inte är att intervjua så många som möjligt, utan intervjuerna ska jämföras med svaren från enkätundersökning och gå djupare på hur problemet motverkas och hanteras. Däremot kan en blandning mellan mer öppna frågor och mer precis frågor vara passande för att kunna kontrollera intervjun i viss mån.

Vidare beskriver Robson (2002) att en semistrukturerad intervju vanligtvis används i mer flexibla, kvalitativa designer av studier, antingen som den enda undersökningsmetoden eller i en kombination med en annan. En vanlig strategi vid en semistrukturerad intervju är att de områden som ska behandlas samt tillhörande frågor nedskrivna på papper på förhand för att ha ett schema. Detta schema kan sedan användas som en grund vid intervjun men samtidigt kan intervjun också guidas utefter informantens svar på frågorna i de olika områdena och frågor behöver inte ställas i den ordning de har skrivits upp i samt att frågor kan ignoreras om de inte passar in eller så kan nya läggas till under intervjuns gång. Det är också av stor vikt att planering före och efter intervjuer sker. Dels ska det stämmas av tid med informanter men sedan kräver efterarbetet, som exempelvis transkribering, mycket tid. Robson (2002) förklarar också att det är viktigt att hela intervjun spelas in eller skrivs ner. Vidare beskrivs några viktiga punkter att tänka på under en intervju:

- Lyssna mer och prata mindre
- Ställ klara och raka frågor på ett icke-aggressivt sätt
- Undvik ledande frågor
- Se intresserad ut

Till skillnad från enkätundersökningen så valdes en kvalitativ metod för intervjuerna. Denna metod valdes för intervjun att kommer riktas mot en person vardera från varje företag som har en roll som systemadministratör eller liknande. En semistrukturerad intervju ansågs vara lämplig för samtliga intervjuer för att skapa en form av röd tråd genom intervjuerna men samtidigt låta informanterna svara fritt och dessutom kunna komma med individuella följdfrågor till de olika informanterna. Intervjufrågor som endast genererar svaren *ja* eller *nej* undviks, istället fokuseras frågorna på att vara mer öppna för att kunna ge mer utvecklande svar från informanterna. Intervjuerna spelas in med en mobiltelefon och ljudfilen förs sedan över till datorn för att kunna transkriberas.

Robson (2002) förklarar också vikten av att analysera kvalitativ data. Författaren måste kunna visa hur data som samlats in mynnar ut i slutsatser, det vill säga att beskriva vilken metod som används för att analysera kvalitativ data. För att analysera intervjuerna användes tematisk kodning. Tematisk kodning innebär att särskilda frågor skapas innan intervjuerna och delas in i teman, och dessa teman används för att svara på forskningsfrågorna. Sedan skapas ytterligare frågor för att komplettera dem grundläggande frågorna. Antingen innan intervjun eller under intervjuns gång. När intervjun sedan transkriberas och allt material analyseras så kategoriseras varje svar för att matcha vilken fråga som besvaras.

4.2 Validitet och reliabilitet

Berndtsson et al. (2008) förklarar att validitet och reliabilitet är något som bör beaktas och hur det kan påverka studien och dess resultat. Validitet är förhållandet mellan det som studien är tänkt att undersöka och vad som faktiskt undersöks. Reliabilitet är hur tillförlitlig metoden som används för studien är. Vidare beskriver Berndtsson et al. (2008) att validitet och reliabilitet skiljer sig för en vald metod beroende på vad som ska studeras eller utforskas. Olika metoder har olika nivåer av validitet och reliabilitet beroende på vad den valda metoden ska användas för. Det faktum att studien använder två olika metoder för att besvara forskningsfrågorna stärker ytterligare validiteten för studien. Dels studeras anställda och deras perspektiv men också företagets perspektiv.

Vidare beskriver Wohlin et al. (2012) fyra olika aspekter av validitet och dessa beaktades vid val av metod samt utformandet av enkät – och intervjufrågorna. De fyra aspekterna är följande:

- *Construct validity* – Denna aspekt av validitet syftar på att det som studien är tänkt att undersöka, vad författaren har för avsikt att undersöka, är det som faktiskt undersöks. Det som studien undersöker ska överensstämma med det som behövs för att kunna svara på forskningsfrågorna (Wohlin et al. 2012). Ett exempel av ett hot mot *construct validity* är missförstånd eller feltolkningar av intervjufrågor. Författaren och intervjuaren har sin syn och definition på frågorna som ställs men informanten tolkar frågorna på ett annat sätt. För att hålla en så hög nivå som möjligt av denna aspekt av validitet så formuleras frågorna för både enkäten och intervjun på ett sätt så att feltolkningar minimeras så gott det går. Det är särskilt viktigt vid enkätundersökningen eftersom att denna genomförs av de deltagande helt själva, utan någon interaktion med författaren.

- *Internal validity* – Denna aspekt av validitet syftar på samband mellan olika orsaker och hur dessa undersöks. Om det i studien görs en undersökning på ett samband och forskaren inte tar med i beaktelse att andra faktorer kan påverka sambandet kan det leda till låg *internal validity* (Wohlin et al. 2012). Ett hot mot denna aspekt av validitet i studien skulle kunna vara att enkäterna eller intervjuerna är för långa, att frågorna är för svåra eller lätta att misstolka vilket kan leda till att deltagarna tröttnar eller tappar lusten att svara ordentligt och endast svarar för att bli klara.

- *External validity* – Denna aspekt av validitet syftar på till vilken grad det går att generalisera resultatet av studien. Det innebär också till vilken grad det är intressant för personer utanför det avgränsade området som inte inkluderas i studien (Wohlin et al. 2012). För att undvika hot mot denna aspekt av validitet så görs en noggrann avgränsning för studien och denna avgränsning diskuteras dessutom för att tydliggöra att resultatet av denna studie inte går att generalisera gentemot andra företag i samhället.

- *Reliability* – Denna aspekt syftar på hur tillförlitlig en metod och dess resultat är. Om en annan forskare gör exakt samma studie på så bör resultatet bli detsamma. Därför är det av stor vikt att metodval och underliggande aspekter inte för beroende eller anknutna till författaren (Wohlin et al. 2012). För att hantera hot mot *reliability* så är det viktigt att vara tydlig med vilken grupp av människor eller vilka typer av företag studien undersöker.

4.3 Etiska aspekter

Vetenskapsrådet (2002) förklarar att etiska aspekter är något som måste hanteras när en studie görs där människor är en del av studien. Vidare delas kraven upp i fyra allmänna huvudkrav på forskning som sker med människor. Dessa krav är *informationskravet, samtyckeskravet, konfidentialitetskravet* och *nyttjandekravet.*

Informationskravet handlar om att informera deltagare om deras uppgifter och vilka villkor som gäller för studien. Deltagandet ska vara helt frivilligt och deltagaren har när som helst rätt att avbryta sitt deltagande. *Samtyckeskravet* innebär att den deltagande lämnar samtycke om att delta i studien och lämna uppgifter. Den deltagande bestämmer själv om denne ska delta, hur länge och på vilka villkor. Är deltagaren vuxen lämnar deltagaren själv sitt samtycke men är deltagaren under 15 år behöver vårdnadshavare lämna samtycke. *Konfidentialitetskravet* innebär att tystnadsplikt gäller angående deltagare och information som dessa lämnar. Personuppgifter ska hanteras på ett säkert sätt så att deltagare inte kan identifieras. *Nyttjandekravet* innebär att uppgifter som samlas in vid studien får inte användas i något annat syfte. Uppgifter får endast användas inom studien.

Eftersom att denna studie kommer att behandla företag, människor och information de lämnar i allra högsta grad kommer dessa fyra krav att behandlas med största respekt. Genom att visa på för de människor som ska delta att det är helt frivilligt och sekretess tas på allvar ger det ett

tryggt intryck och kan underlätta att få deltagare att ställa upp. Vidare kommer all information som på något sätt kan härledas till en individ eller ett företag att anonymiseras.

5 Genomförande

Detta kapitel beskriver hur studien har genomförts. Kapitlet delas upp i två delar, den ena delen behandlar enkätundersökningen och den andra delen behandlar intervjuerna.

5.1 Enkätundersökning

Enkäten skapades med Google Formulär som är en gratis tjänst tillhandahållen av Google. Google Formulär valdes, dels för att det är gratis men också för att deltagarna ska kunna vara, för författaren, anonyma. Google Formulär kan dessutom visa statistik över svaren på varje fråga vilket underlättar vid analys av svaren. Det är ett enkelt verktyg för att skapa en enkätundersökning och en länk per enkät, totalt tre stycken, skapades och skickades ut till deltagarna. Kontaktpersonen på företag A, som även var den som intervjuades, hjälpte till med att skicka ut enkäten till tre olika avdelningar på företaget. De olika avdelningarna som deltog i enkätundersökningen var informationssäkerhetsteamet, kontorschefer och controllers. Frågorna i enkäten skapades och diskuterades med hjälp av handledaren och enkäten skickades efter det ut till åtta personer testpersoner i författarens klass för att se om frågorna var tydliga nog och att inga frågor skulle uppstå för deltagarna.

Enkäten utformades med en blandning av olika sätt att svara på frågorna. För att kunna dra vissa slutsatser behövdes frågor som genererade ett *ja* eller *nej* ställas. Vidare ställdes flervalsfrågor men också frågor med en likertskala för att se hur deltagarna upplever det som efterfrågas snarare än om det stämmer eller inte.

Den första enkäten skickades till informationssäkerhetsteamet med hjälp av kontaktpersonen på företag A och den var ute i ungefär en vecka för att kunna samla in så många svar som möjligt. Innan de två andra enkäterna skickades ut så formulerades ett par frågor om då dessa visade sig vara otydliga och svåra att svara på i efterhand. Frågorna som ändras var fråga nummer fyra och tio.

Fråga fyra formulerades om från *”Hur medveten är du om att det finns vissa risker med att använda en molnlagringstjänst?”* till *”Är du medveten om att det finns vissa risker med att använda en molnlagringstjänst?”*. När denna fråga analyserades framkom det att deltagarna kanske inte är medvetna om risker överhuvudtaget och därför blir det svårt att svara på frågan. Den nya frågan kändes mer lämplig och lättare för deltagarna att svara på.

Fråga tio formulerades om från *”Hur sannolikt är det att du skulle lagra arbetsrelaterade filer i din privata molnlagringstjänst efter att du blivit upplyst om vilka risker molnlagring innebär?”* till *”Givet de risker som finns med molnlagring, hur sannolikt är det att du skulle använda din privata molnlagringstjänst för att lagra arbetsrelaterad information?”.* Anledningen till att denna fråga formulerades om var för att den var ledande och för svår att svara på. Om deltagarna redan blivit upplysta om vilka risker som finns så blir frågan överflödig. Istället fokuserade den nya frågan på hur deltagarna ställer sig till att använda privat molnlagring för att lagra arbetsrelaterade filer givet de risker som finns med molnlagring.

Under tiden som enkäterna var ute formulerades intervjufrågor och som underlag för dessa användes bland annat tidigare studier och resultatet från enkätundersökningen. Resultatet från enkätundersökningen presenteras som helhet i kapitel 6.

5.2 Intervjuer

Två intervjuer gjordes med två olika informanter, en från företag A och en från företag B. Utformningen av frågorna baserades delvis på svaren från den tidigare utskickade enkäten men också på vad författaren ansåg vara nödvändigt för att kunna besvara forskningsfrågan. Intervjuerna, till skillnad från enkätundersökningen, avser att skildra hur ledningen på företagen ser på problemet samt och hur problemet förhindras eller motverkas på respektive arbetsplats. Intervjufrågor bestod av tre huvudfrågor och intervjuerna inleddes med att fråga informanterna om deras generella syn på molnlagring med tillhörande risker och säkerhet.

Intervjun gick sedan över till att vara mer specifik. Resterande frågor fokuserade specifikt på att besvara forskningsfrågan *Hur hanterar IT-företag att användare lagrar arbetsrelaterad information i privata molnlagringstjänster.* Även om specifika frågor ställdes så tilläts informanterna prata fritt och överlappa på frågor som ännu inte var ställda. Tanken med det var för att inte avbryta informanterna när dessa pratade och för att ge ett intresserat intryck gentemot informanterna. Varje huvudfråga hade några underfrågor och om dessa besvarades medan informanterna diskuterade kring andra frågor så bockades dessa av emellanåt.

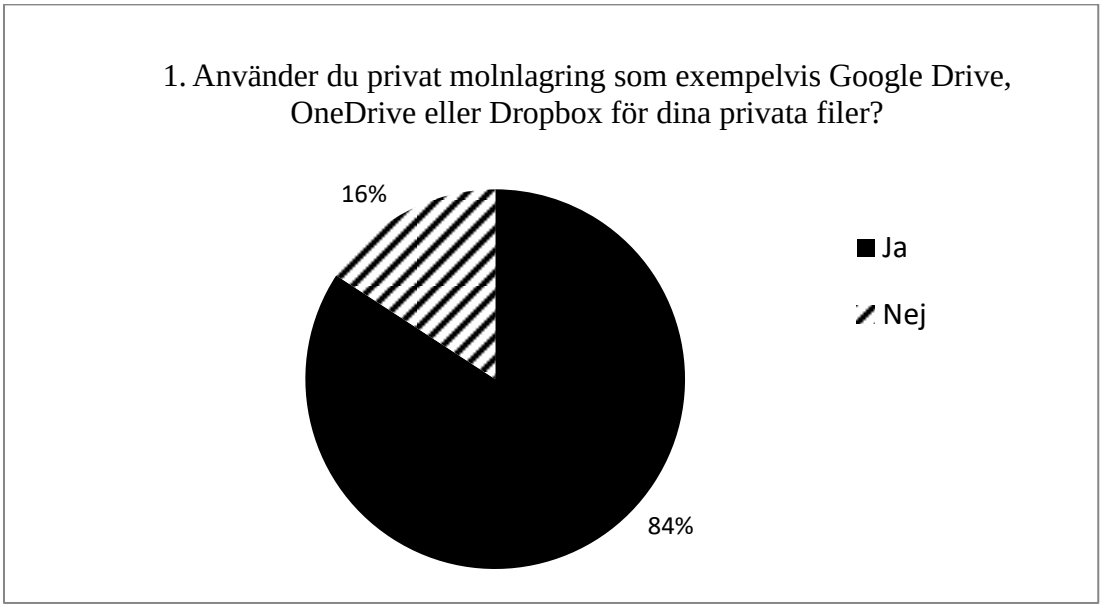
Intervjun med informant 1 från företag A skedde i ett grupprum på högskolan i Skövde efter överenskommelse med informanten och den intervjun tog ungefär 50 minuter. Intervjun med informant 2 från företag B skedde i ett konferensrum på informantens arbetsplats och den intervjun tog ungefär 20 minuter. Båda intervjuerna spelades in med en mobiltelefon för att kunna transkriberas och analyseras. Intervjuerna analyserades med tematisk kodning där varje huvudfråga var ett tema. Informanternas svar matchades sedan ihop med passande tema. Varje informant fick dessutom en chokladask som tack för hjälpen. Resultatet från intervjuerna presenteras i kapitel 6.

6 Resultat och analys

Detta kapitel beskriver resultaten och svaren från enkätundersökningen och intervjuerna samt en analys av dessa. Kapitlet delas upp i underkapitel, ett för varje avdelning, ett för analys och jämförelse av svaren från enkäten, ett med intervjuerna samt ett underkapitel med analys av intervjuerna. Varje fråga i enkätundersökningarna presenteras i en figur med resultatbeskrivning under respektive figur. Analys och jämförelse av enkätsvaren mellan avdelningarna görs i kapitel 6.4.

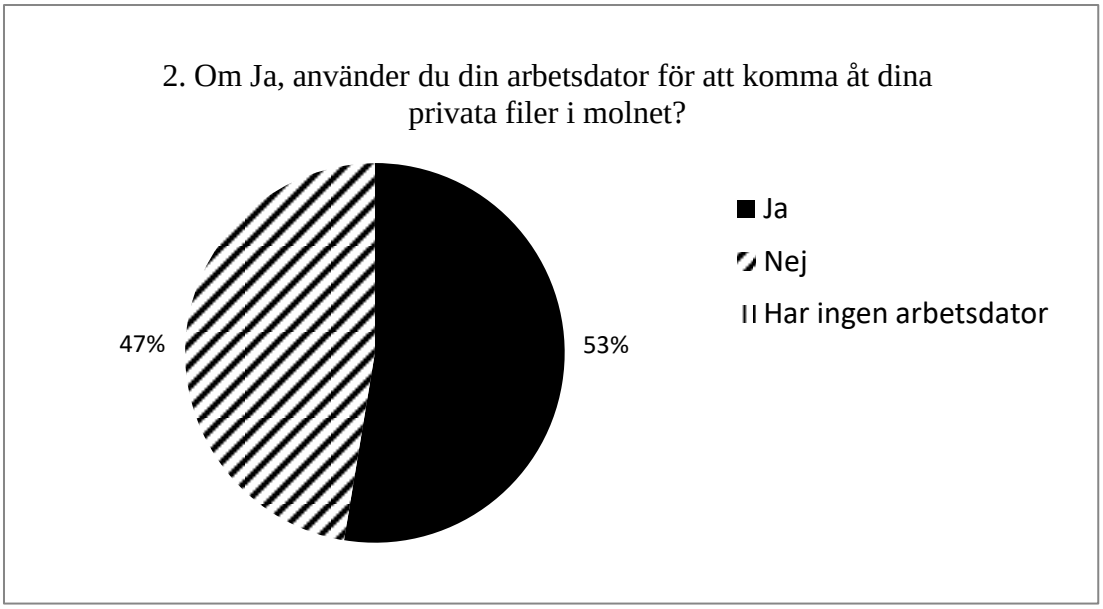
6.1 Enkätundersökning - informationssäkerhetsteamet

Följande underkapitel visar resultatet från enkätundersökningen som gick ut till informationssäkerhetsteamet. För varje fråga presenteras resultat i diagram och svaren diskuteras sedan med underlag från intervjuer och tidigare studier. Som tidigare nämnt var det 19 deltagande.



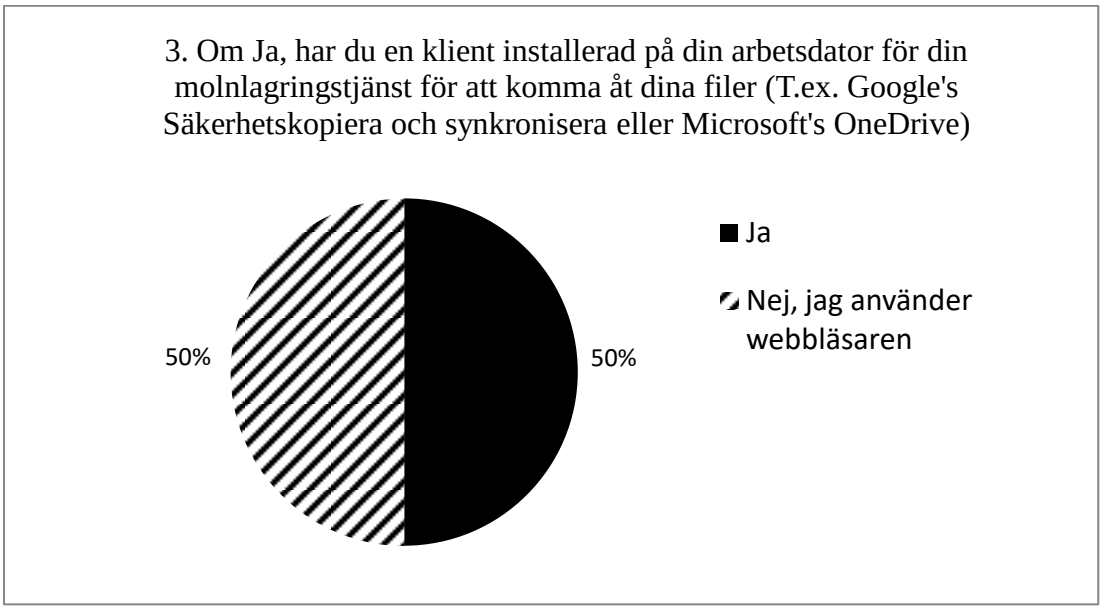
Figur 2. Informationssäkerhetsteamets svar på fråga 1.

Första frågan ställdes för att helt enkelt visa om deltagarna använder en privat molnlagringstjänst överhuvudtaget och resultatet visas i figur 2. Denna fråga var obligatorisk vilket resulterade i 19 svar. Resultatet visar att 84 % använder privat molnlagring för sina privata filer och 16 % gör det inte.



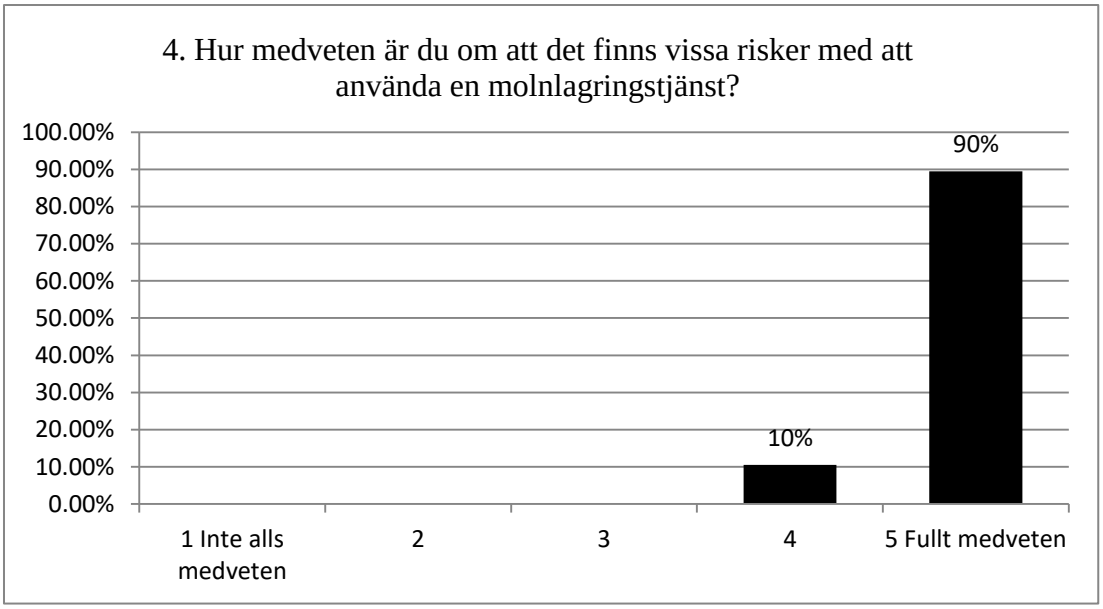
Figur 3. Informationssäkerhetsteamets svar på fråga 2.

Figur 3 visar resultatet från fråga två. Resultatet visar att 53 % använder sin arbetsdator för att komma åt sina privata filer och 47 % gör det inte.



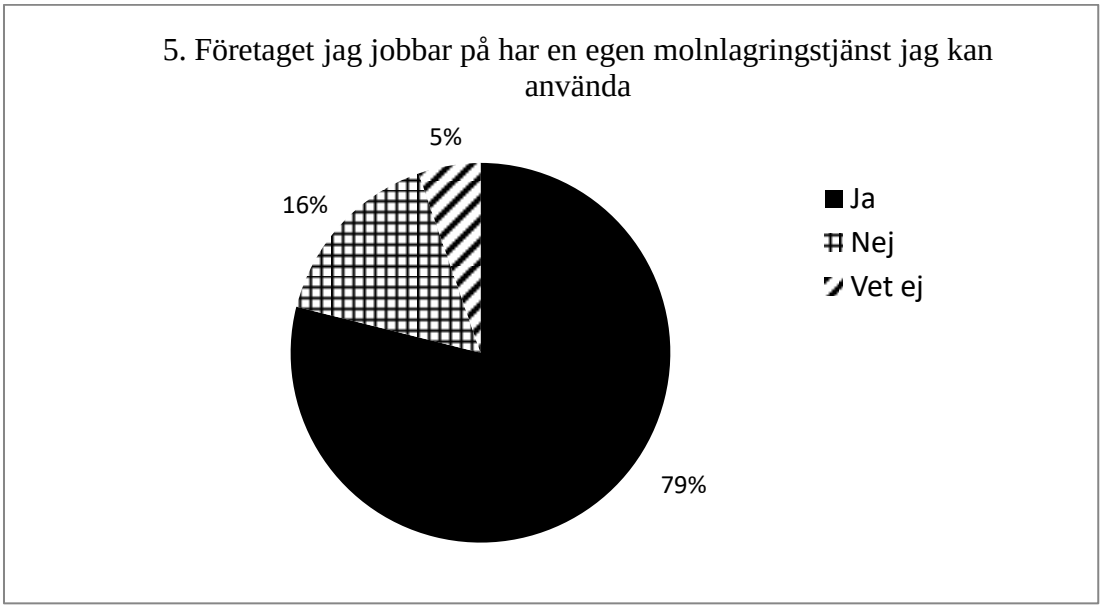
Figur 4. Informationssäkerhetsteamets svar på fråga 3.

I figur 4 visas resultatet från fråga tre. Resultatet visar att 50 % av de svarande har en klient installerad på sin arbetsdator för att komma åt sin privata molnlagringstjänst och 50 % använder webbläsaren. Fråga nummer tre var en följdfråga till fråga två, för att se hur deltagarna kommer åt sina privata filer, via webbläsaren eller en klient.



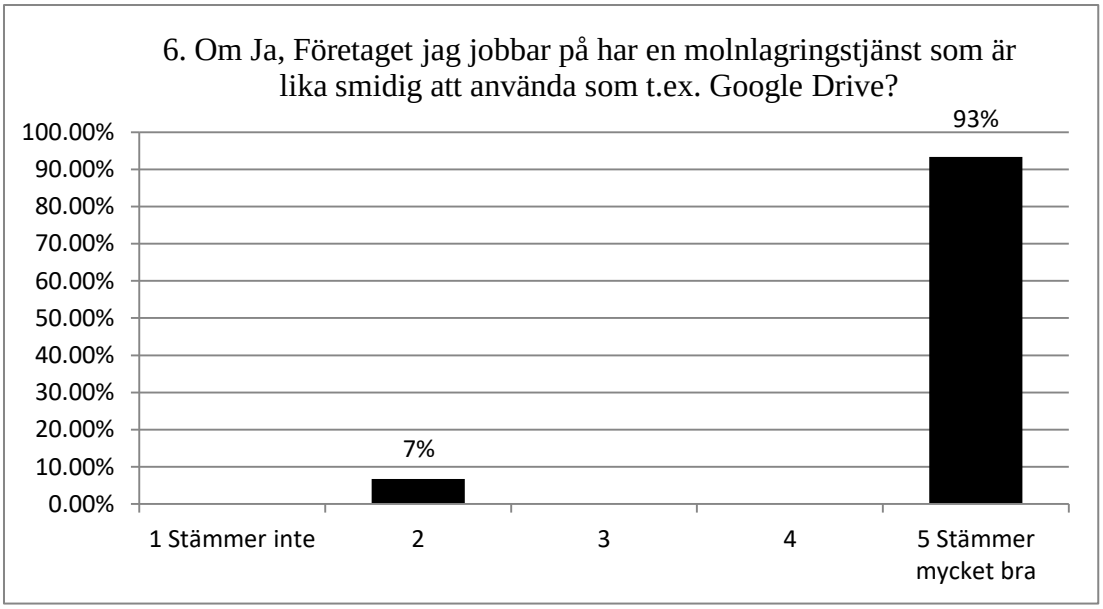
Figur 5. Informationssäkerhetsteamets svar på fråga 4.

Figur 5 visar resultatet från fråga fyra. Denna fråga var obligatorisk vilket genererade 19 svar. Denna fråga ställdes för att ge deltagarna en möjlighet att själva avgöra hur medvetna de är gällande risker med molnlagring. Resultatet visar att deltagarna är mycket medvetna om att det finns vissa risker med molnlagring. 90 % (17 stycken) svarade *5 Fullt medveten* och 10 % (två stycken) svarade *4* vilket innebär att de anser sig vara medvetna men inte fullt medvetna.



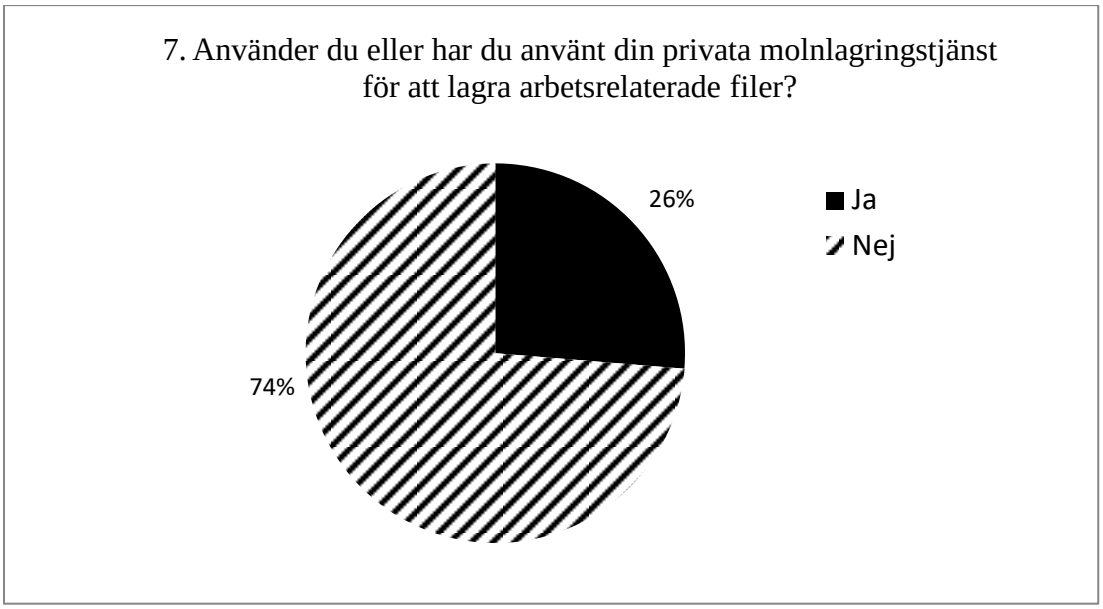
Figur 6. Informationssäkerhetsteamets svar på fråga 5.

I figur 6 visas resultatet från fråga fem. Denna fråga var obligatorisk och därmed erhölls 19 svar. 79 % (15 stycken) svarade *Ja*, 16 % (tre stycken) svarade *Nej* och 5 % (en deltagare) svarade *Vet ej*.



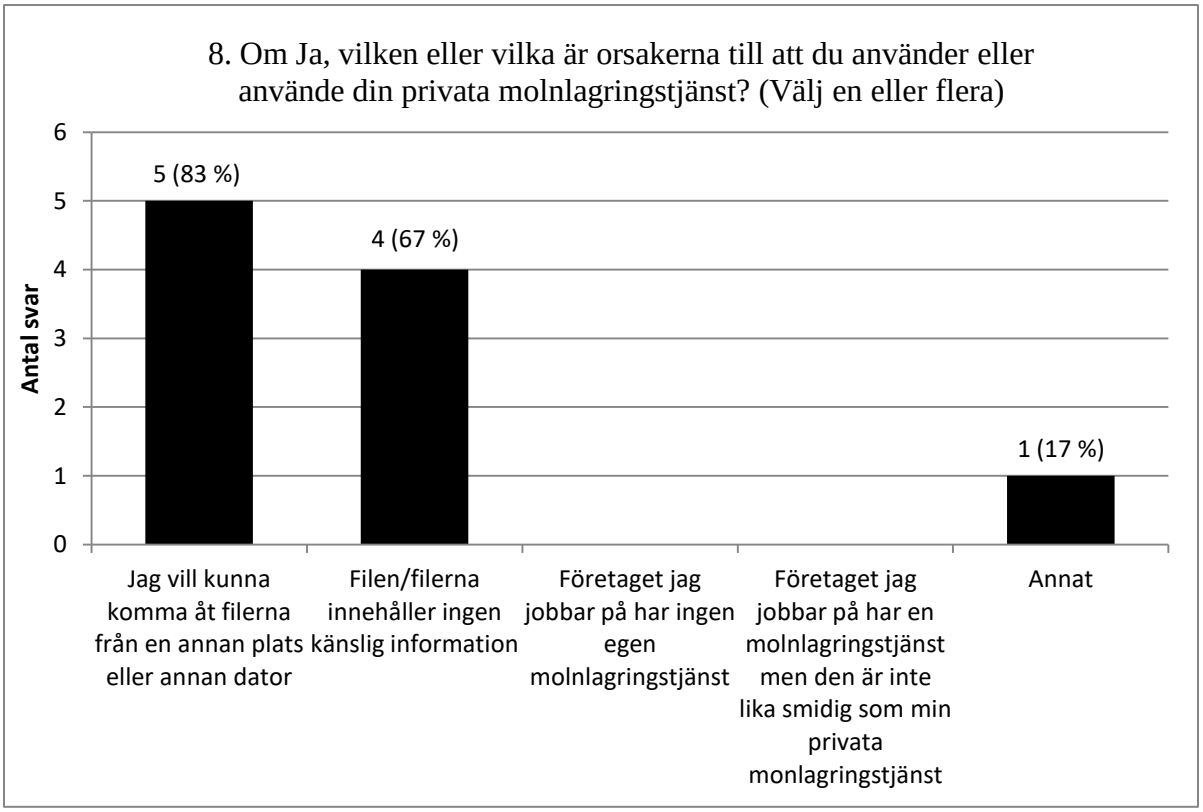
Figur 7. Informationssäkerhetsteamets svar på fråga 6.

Figur 7 visar resultatet från fråga sex. Resultatet visar att 93 % (14 stycken) tycker att företagets egen molnlagringstjänst är lika smidig att använda som exempelvis Google Drive. Det var bara 7 % (en deltagare) som nästintill inte höll med alls om att den är lika smidig.



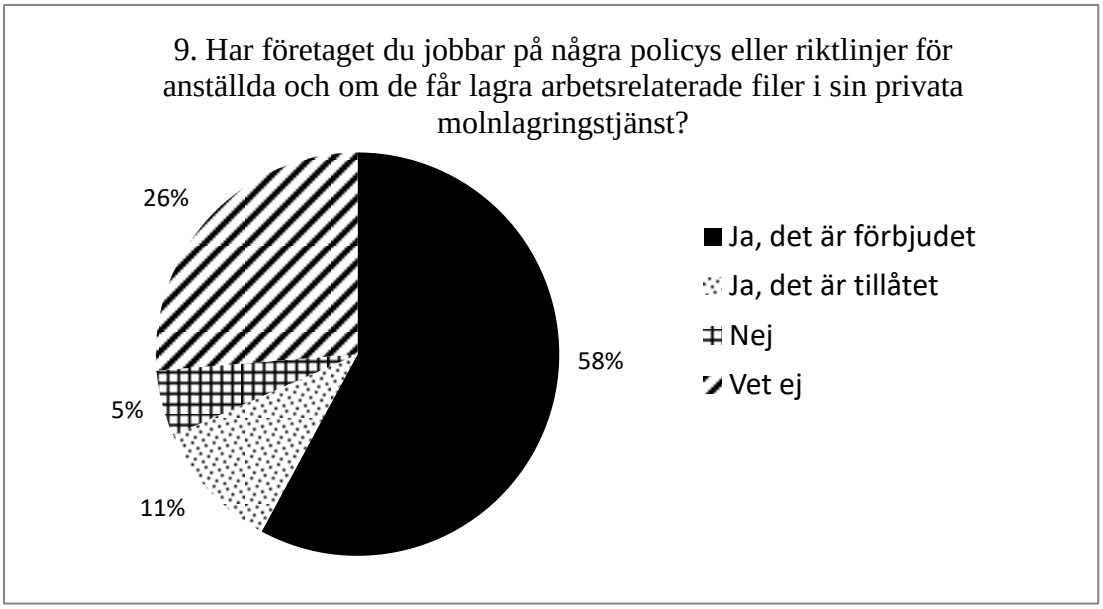
Figur 8. Informationssäkerhetsteamets svar på fråga 7.

I figur 8 visas resultatet från fråga sju. Som resultatet visar så har 74 % (14 stycken) aldrig använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer men 26 % (fem stycken) svarade att de använder eller har använt sin privata molnlagringstjänst för detta syfte.



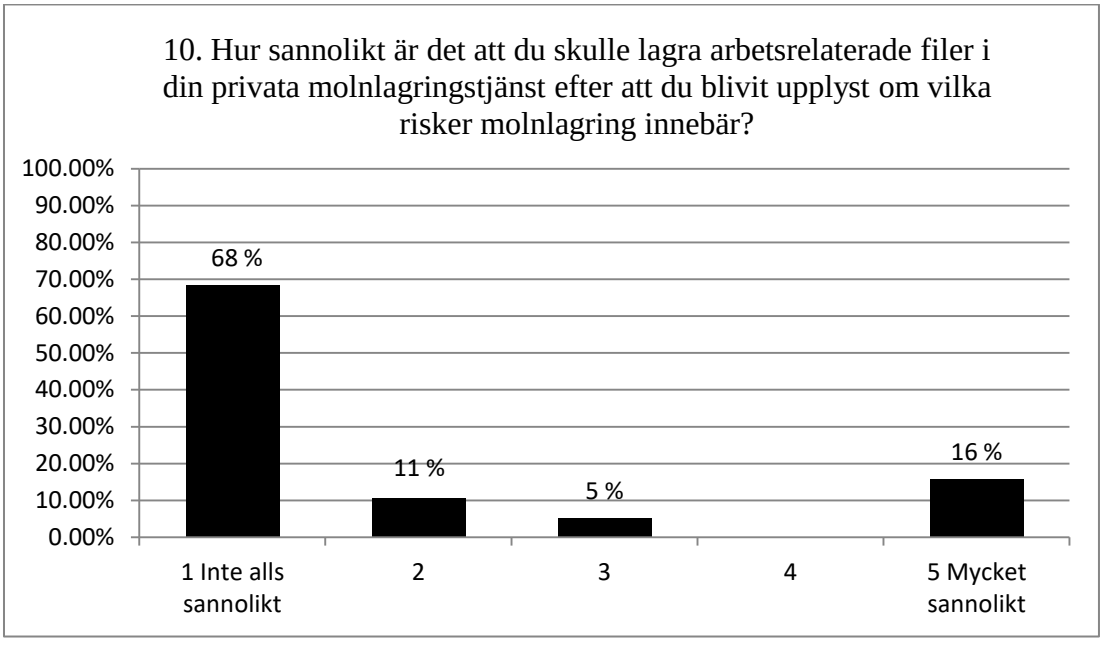
Figur 9. Informationssäkerhetsteamets svar på fråga 8.

I figur 9 visas resultatet från fråga åtta. Totalt svarade sju deltagare på frågan och resultatet visar att den vanligaste orsaken är att deltagarna vill kunna komma åt filen eller filerna från en annan plats eller en annan dator, denna orsak valdes av fem svarande. Den näst vanligaste orsaken är att filen eller filerna inte innehåller någon känslig information, denna orsak valdes av fyra svarande. En deltagare valde *Annat* som orsak och denna orsak var privata behov.



Figur 10. Informationssäkerhetsteamets svar på fråga 9.

Figur 10 visar resultatet från fråga nio. Denna fråga var obligatorisk vilket resulterade in 19 svar. Av 19 svarande är det 58 % (elva stycken) som är medvetna om att det finns policys och riktlinjer för hur arbetsrelaterade filer får lagras och att det är förbjudet att lagra i en privat molnlagringstjänst. 26 % (fem stycken) vet inte om företaget har policys eller riktlinjer för hur information får lagras. 11 % (två stycken) svarade att det finns policys och riktlinjer men att det också är tillåtet att lagra arbetsrelaterad information i en privat molnlagringstjänst. Till sist svarade 5 % (en deltagare) att det inte finns några policys eller riktlinjer överhuvudtaget.



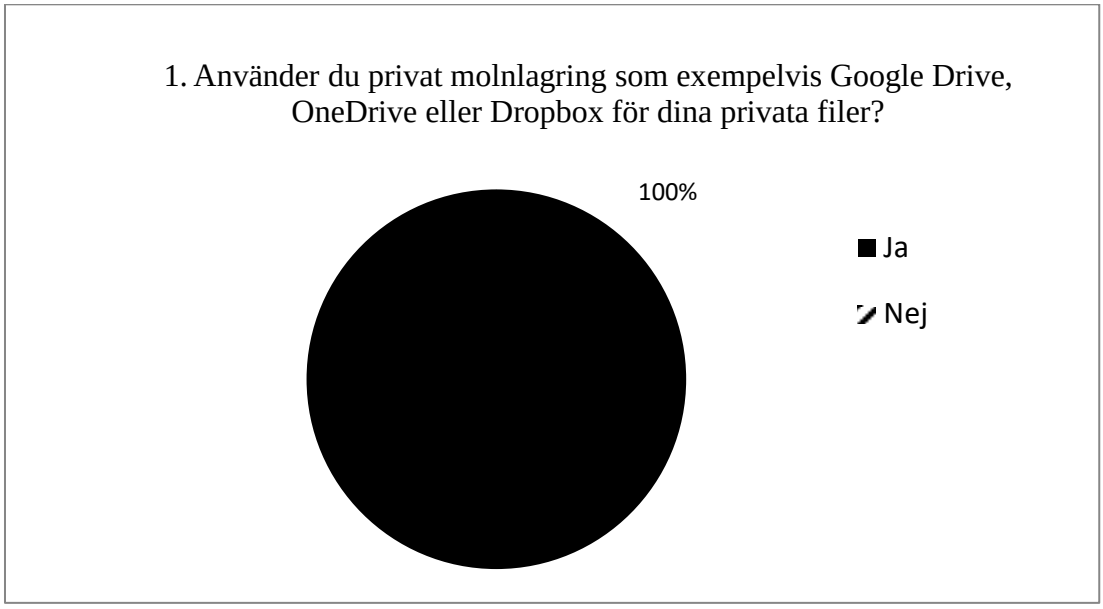
Figur 11. Informationssäkerhetsteamets svar på fråga 10.

Figur 11 visar resultatet från fråga tio. Denna fråga var obligatorisk vilket resulterade i 19 svar. Som resultatet visar så skulle majoriteten, 68 % (13 stycken), inte lagra arbetsrelaterade filer i sin privata molnlagringstjänst om de blev upplysta på något sätt om vilka risker som

molnlagring medför. 11 % (två stycken) svarade att de sannolikt inte kommer lagra arbetsrelaterade filer i sin privata molnlagringstjänst efter dem blivit upplysta om vilka risker det innebär, men det finns en liten risk att de kan göra det. 5 % (en deltagare) svarade en 3:a på den femgradiga skalan, vilket kan antas att deltagaren har en neutral inställning. 16 % (tre stycken) svarade att det är mycket sannolikt att de kommer fortsätta lagra arbetsrelaterade filer i sin privata molnlagringstjänst trots att de blivit upplysta om vilka risker det medför.

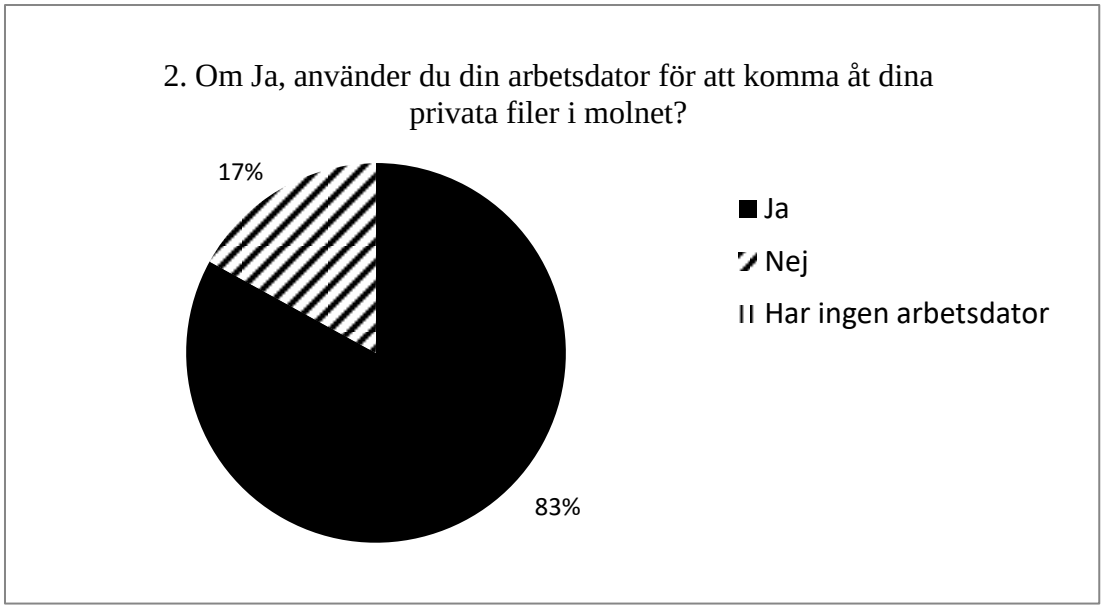
6.2 Enkätundersökning - kontorschefer

Följande underkapitel beskriver resultatet från enkätundersökningen som gick ut till kontorschefer. Totalt svarade sex stycken kontorschefer på enkätundersökningen.



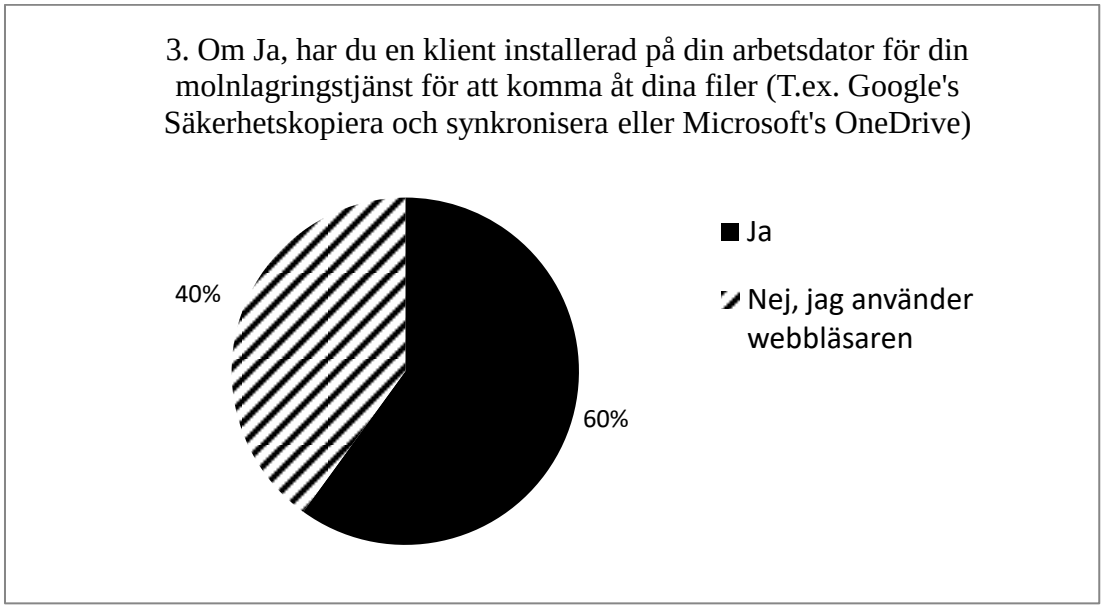
Figur 12. Kontorschefernas svar på fråga 1.

Figur 12 visar resultatet på första frågan för kontorscheferna. På denna fråga registrerades sex svar eftersom frågan var obligatorisk. 100 % svarade att de använder privat molnlagring för sina privata filer.



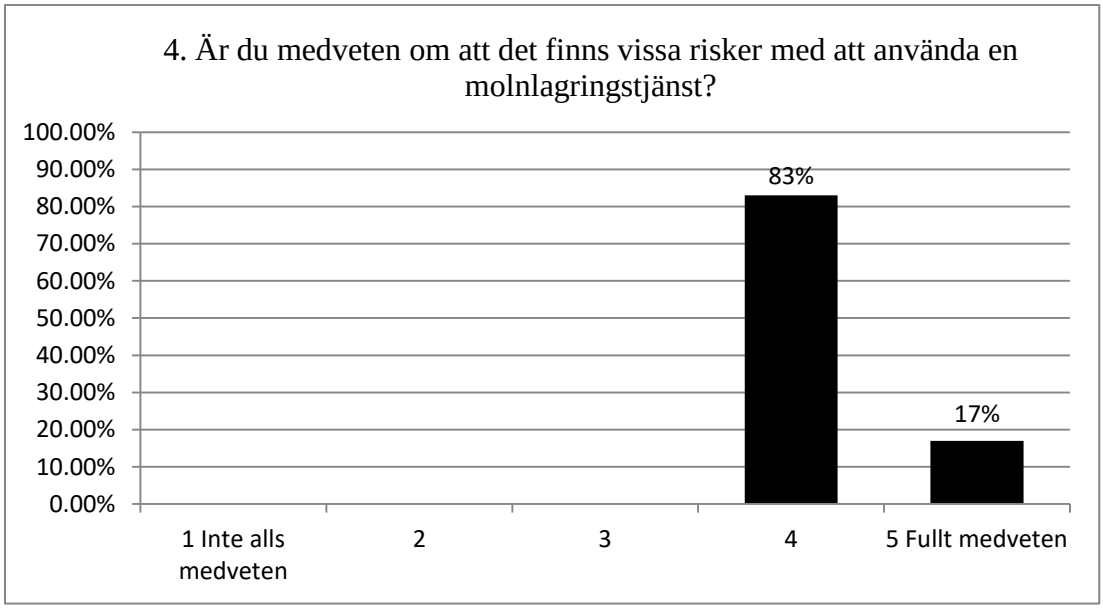
Figur 13. Kontorschefernas svar på fråga 2.

Figur 13 visar resultatet från fråga två. Som figuren visar så använder 83 % (fem stycken) sin arbetsdator för att komma åt privata filer i molnet och 17 % (en deltagare) använder inte sin arbetsdator för att komma åt sina privata filer i molnet.



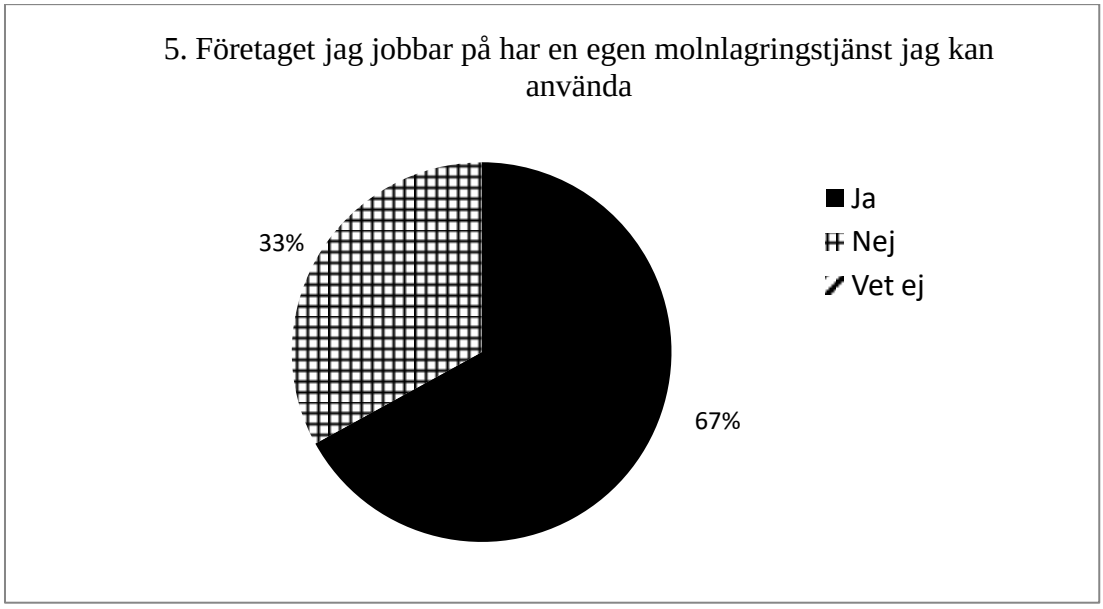
Figur 14. Kontorschefernas svar på fråga 3.

Figur 14 visar resultat från fråga 3. Resultatet visar att 60 % (tre stycken) har en klient installerad på sin arbetsdator för att komma åt sin privata molnlagringstjänst och 40 % (två stycken) använder webbläsaren.



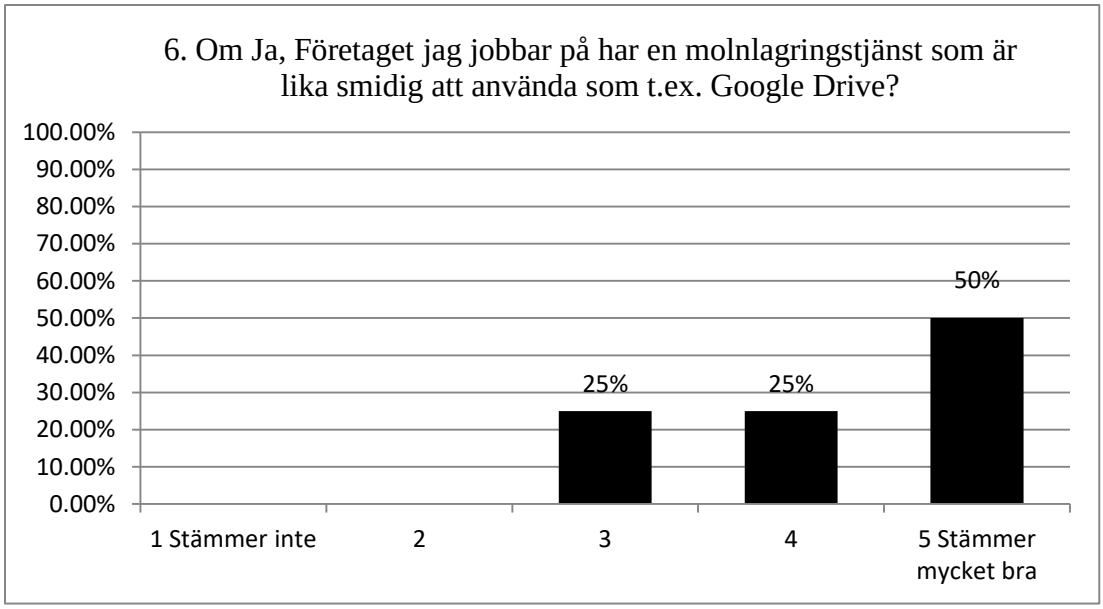
Figur 15. Kontorschefernas svar på fråga 4.

I figur 15 visas resultatet från fråga fyra. Även denna fråga var obligatorisk vilket genererade sex svar. Resultatet visar att deltagarna medvetna om att det finns vissa risker med att använda en molnlagringstjänst, dock inte fullt medvetna. 83 % (fem stycken) anser sig vara medvetna men inte fullt medvetna, 17 % (en deltagare) anser sig vara fullt medveten.



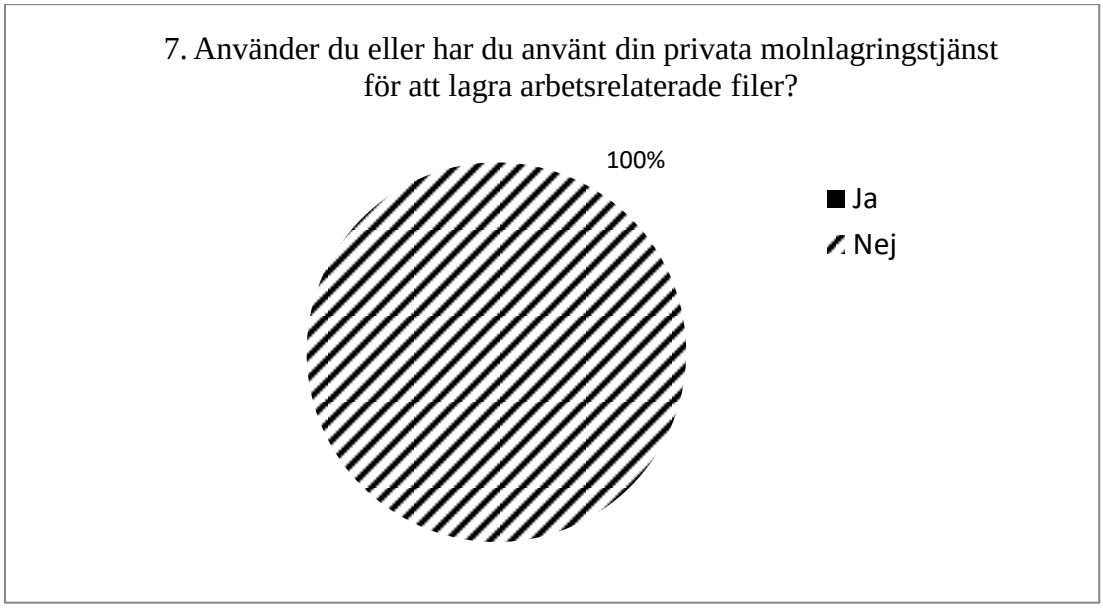
Figur 16. Kontorschefernas svar på fråga 5.

I figur 16 visas resultatet från fråga fem. Denna fråga var obligatorisk vilket resulterade i sex svar. 67 % (fyra stycken) är medvetna om att företaget har en egen molnlagringstjänst för de anställda men 33 % (två stycken) vet inte om att företaget har en egen molnlagringstjänst.



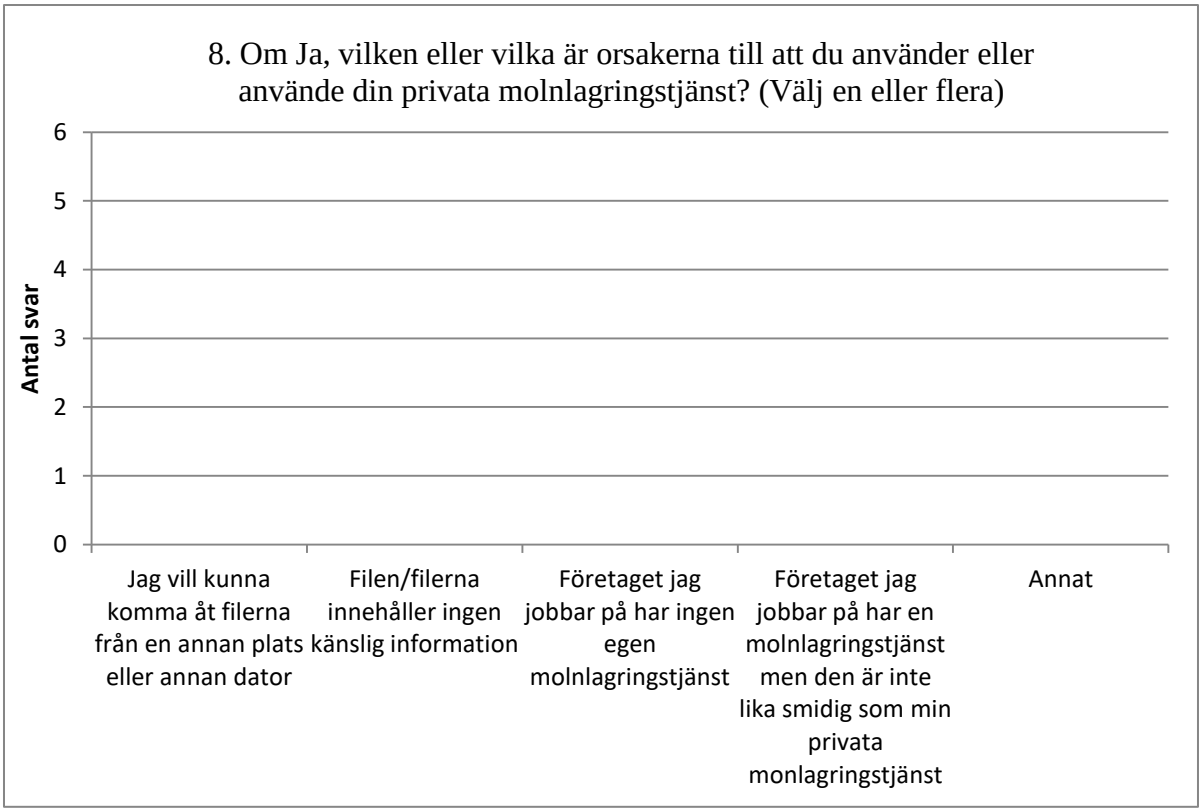
Figur 17. Kontorschefernas svar på fråga 6.

Figur 17 visar resultatet från fråga sex. Resultatet visar att 50 % (två stycken) tycker att företagets egen molnlagringstjänst är lika smidig att använda som exempelvis Google Drive. 25 % (en deltagare) tycker att företagets molnlagringstjänst nästan är lika smidig som exempelvis Google Drive. 25 % (en deltagare) ställer sig neutralt i frågan.



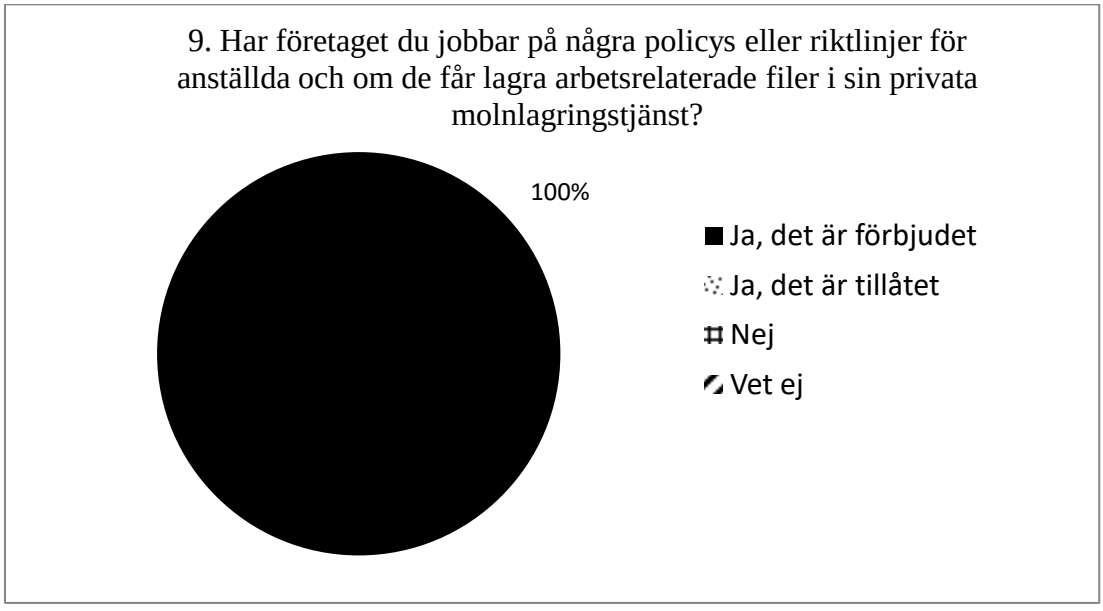
Figur 18. Kontorschefernas svar på fråga 7.

Figur 18 visar resultatet från fråga sju. Resultatet visar att 100 % (sex stycken) inte använder eller har använt sin privata molnlagring för att lagra arbetsrelaterade filer.



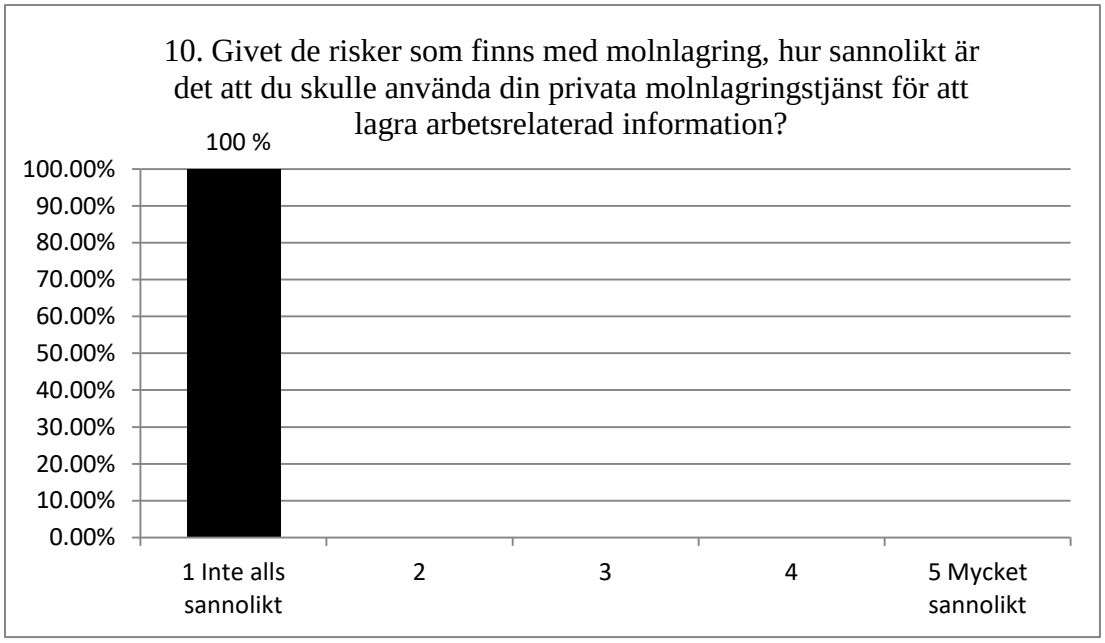
Figur 19. Kontorschefernas svar på fråga 8.

Figur 19 visar resultat från fråga åtta. Inga svar är registrerade på denna fråga eftersom det var en följfråga till fråga sju och ingen av kontorscheferna har använt sin privata molnlagring för att lagra arbetsrelaterad information.



Figur 20. Kontorschefernas svar på fråga 9.

Figur 20 visar svarsresultatet från fråga nio. Resultatet visar att 100 % (sex stycken) är medvetna om att det finns policys och riktlinjer på företaget för om anställda får lagra arbetsrelaterad information i sina privata molnlagringstjänster och att det är förbjudet.

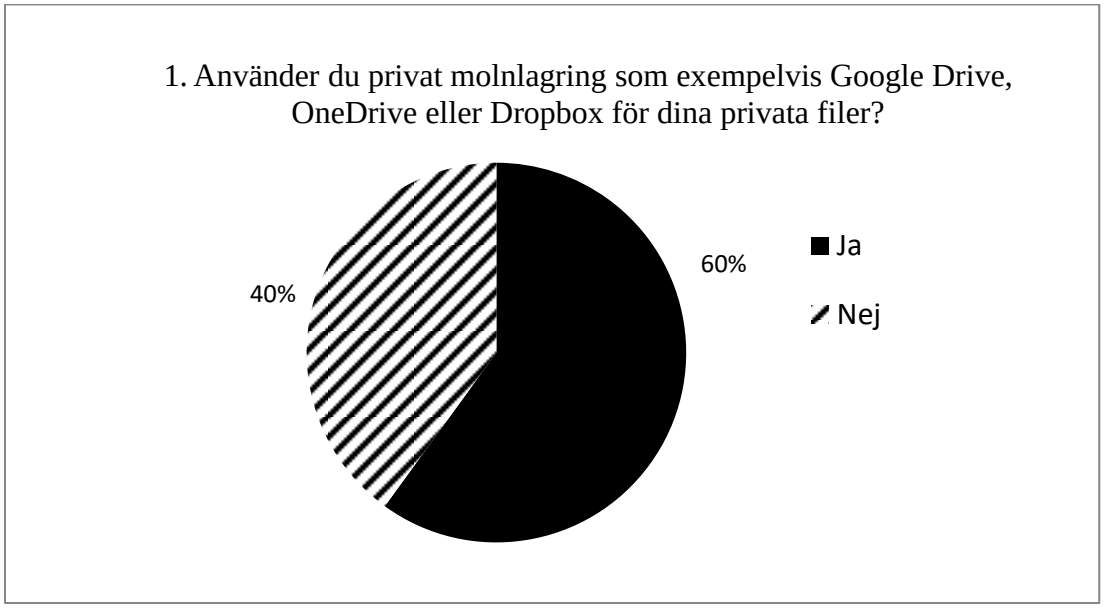


Figur 21. Kontorschefernas svar på fråga 10.

Figur 21 visar resultatet från fråga tio. Resultatet visar att 100 % (sex stycken) svarade att det inte alls är sannolikt att de skulle lagra arbetsrelaterad information i sin privata molnlagringstjänst på grund av de risker som finns med molnlagring.

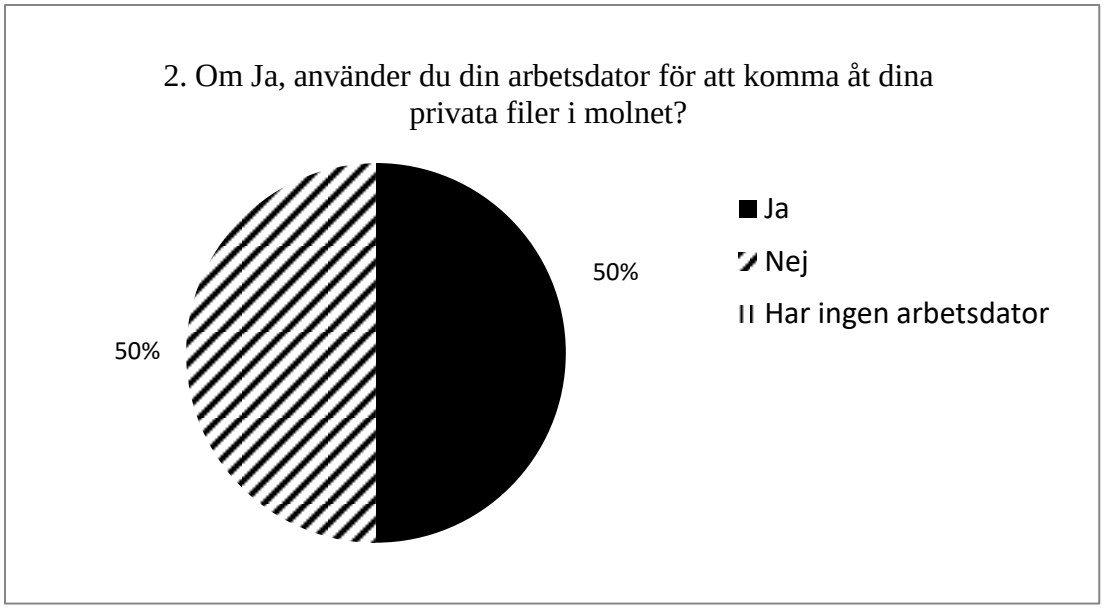
6.3 Enkätundersökning – controllers

Följande underkapitel beskriver resultatet från enkätundersökningen som gick ut till controllers på företaget. Totalt svarade tio stycken controllers på enkätundersökningen.



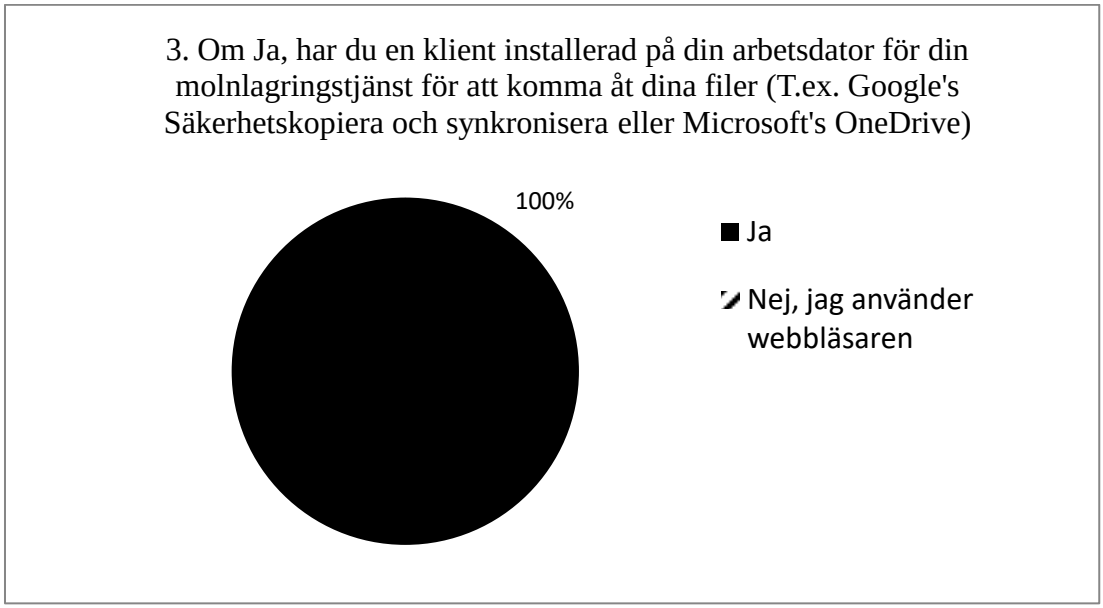
Figur 22. Controllers svar på fråga 1.

Figur 22 visar resultatet på första frågan för företagets controllers. På denna fråga registrerades tio svar eftersom frågan var obligatorisk. 60 % (sex stycken) svarade att de använder privat molnlagring för sina privata filer och 40 % (fyra stycken) gör det inte.



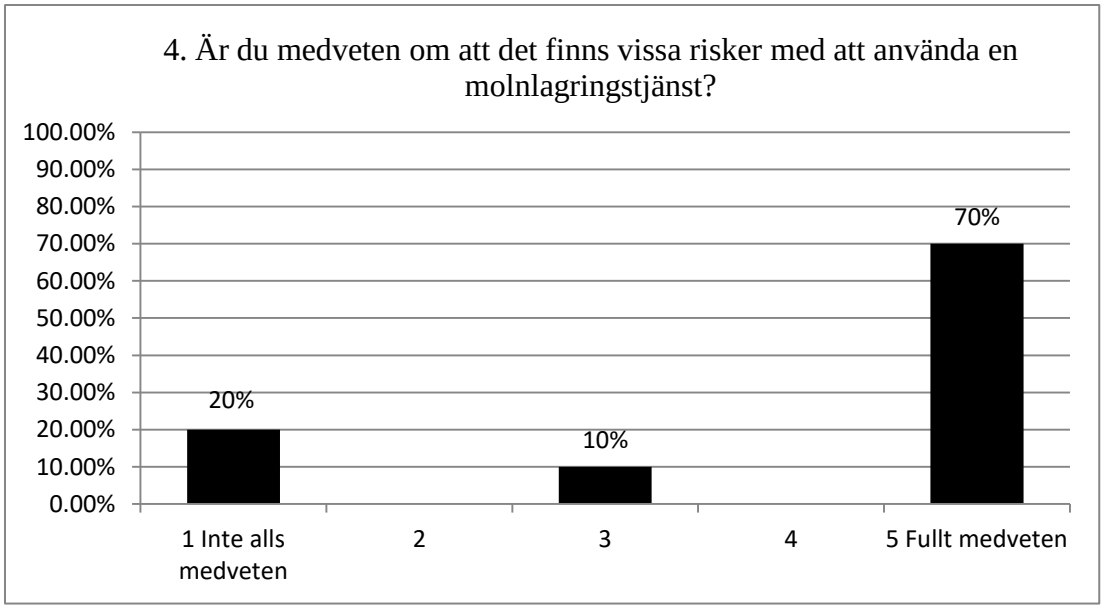
Figur 23. Controllers svar på fråga 2.

Figur 23 visar resultatet från fråga två. Som figuren visar så använder 50 % (tre stycken) sin arbetsdator för att komma åt privata filer i molnet och 50 % (tre stycken) använder inte sin arbetsdator för att komma åt sina privata filer i molnet.



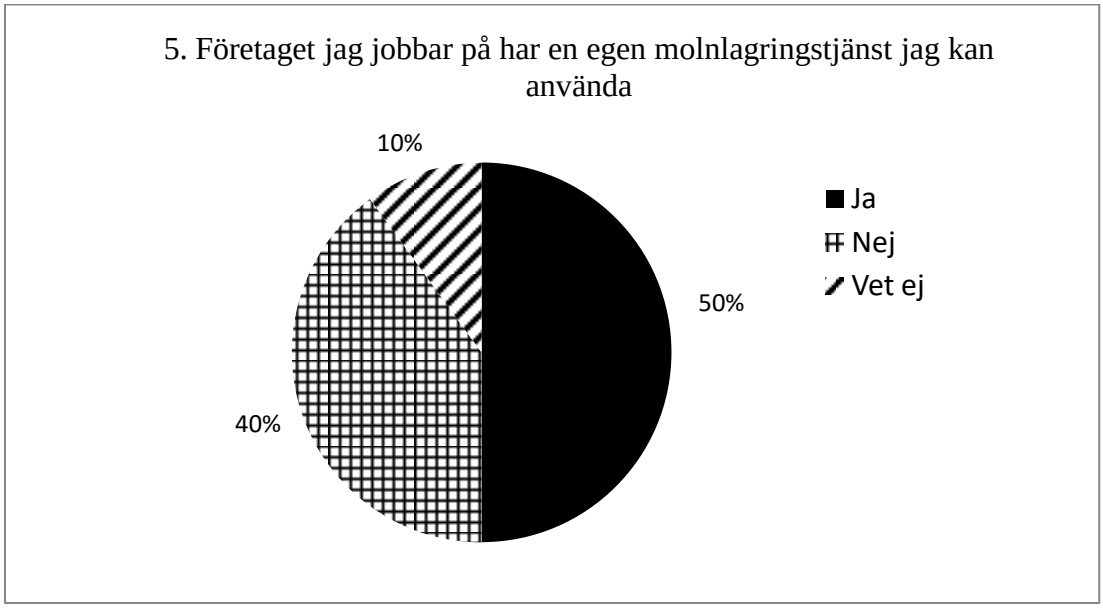
Figur 24. Controllers svar på fråga 3.

Figur 14 visar resultat från fråga 3. Resultatet visar att 100 % (tre stycken) har en klient installerad på sin arbetsdator för att komma åt sin privata molnlagringstjänst.



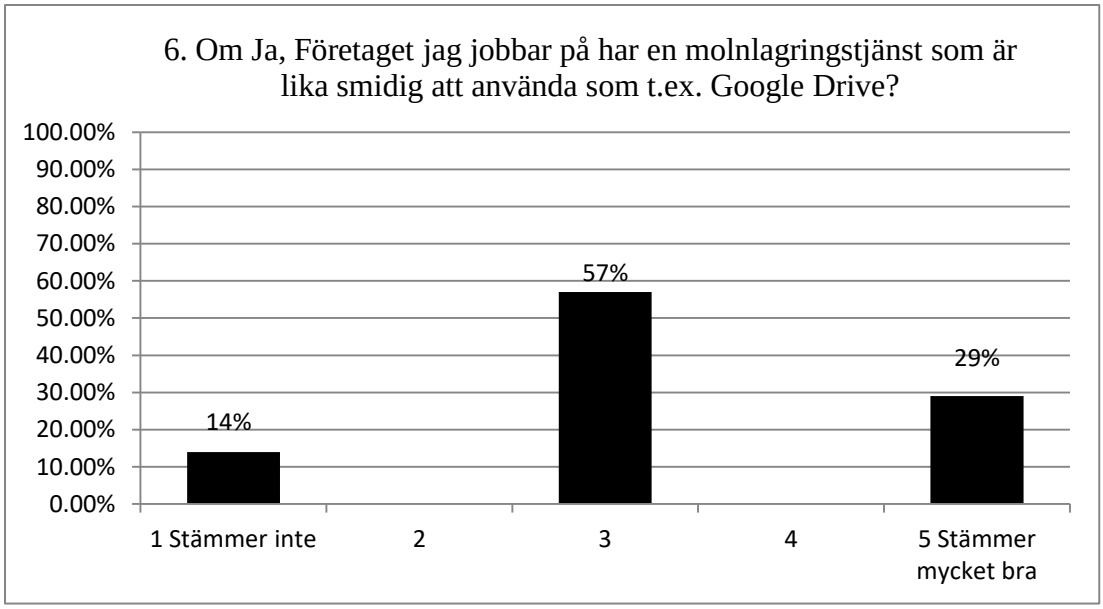
Figur 25. Controllers svar på fråga 4.

Figur 25 visar resultatet från fråga fyra. Som resultatet visar så är majoriteten fullt medvetna om att det finns vissa risker med att använda en molnlagringstjänst. 70 % (sju stycken) svarade att de är fullt medvetna. 10 % (en deltagare) ansåg sig vara neutral i frågan, varken fullt medveten eller inte alls medveten. 20 % (två stycken) svarade att de inte alls är medvetna.



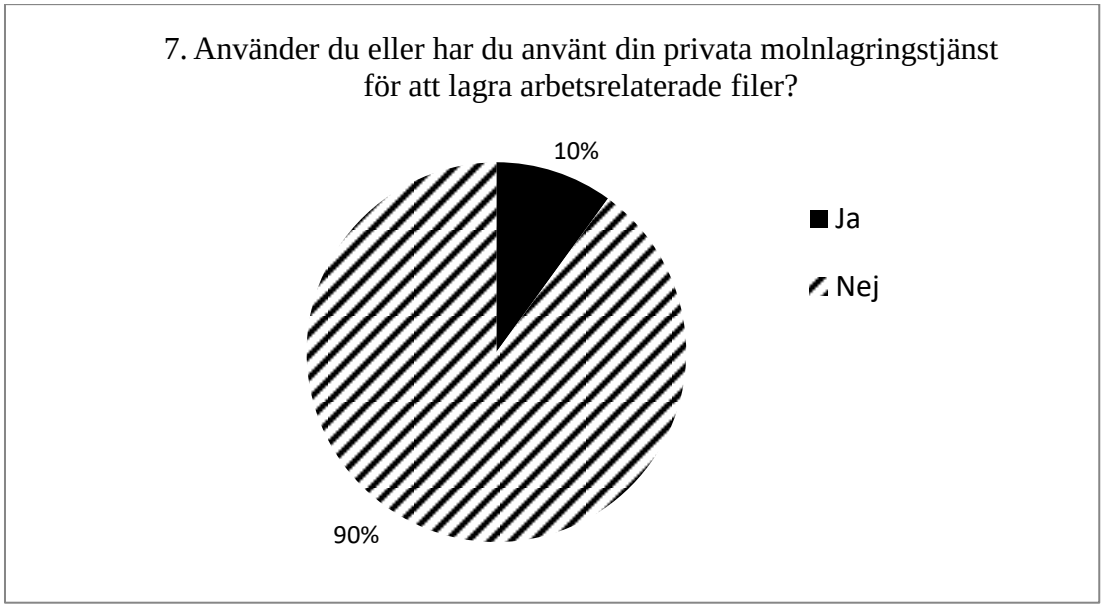
Figur 26. Controllers svar på fråga 5.

Figur 26 visar resultatet från fråga fem. Resultatet visar att 50 % (fem stycken) är medvetna om att företaget har en egen molnlagringstjänst. 40 % (fyra stycken) svarade att företaget inte har en egen molnlagringstjänst och 10 % (en deltagare) vet inte om företaget har en egen molnlagringstjänst.



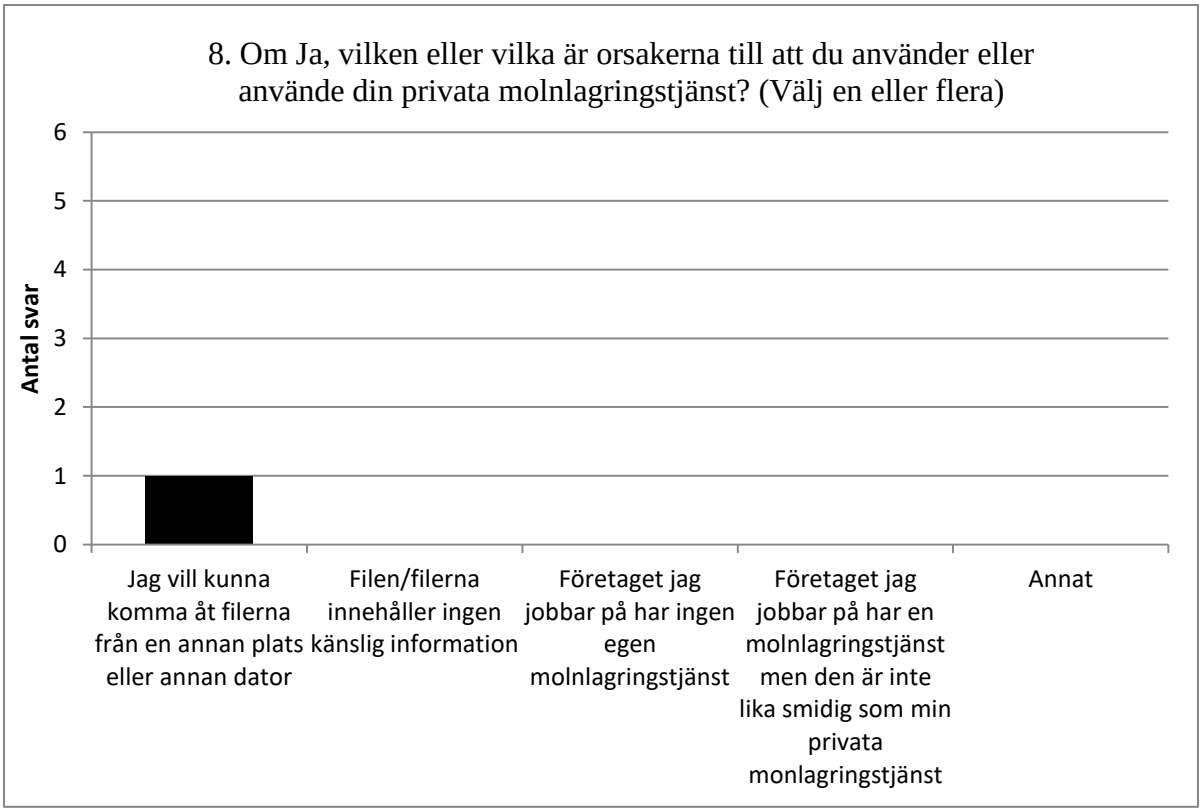
Figur 27. Controllers svar på fråga 6.

Figur 27 visar resultatet från fråga sex. Resultatet visar 57 % (fyra deltagare) är neutrala i frågan. 29 % (två stycken) tycker att företagets molnlagringstjänst är lika smidig som exempelvis Google Drive. 14 % (en deltagare) håller inte alls med om att företagets molnlagringstjänst är lika smidig som exempelvis Google Drive.



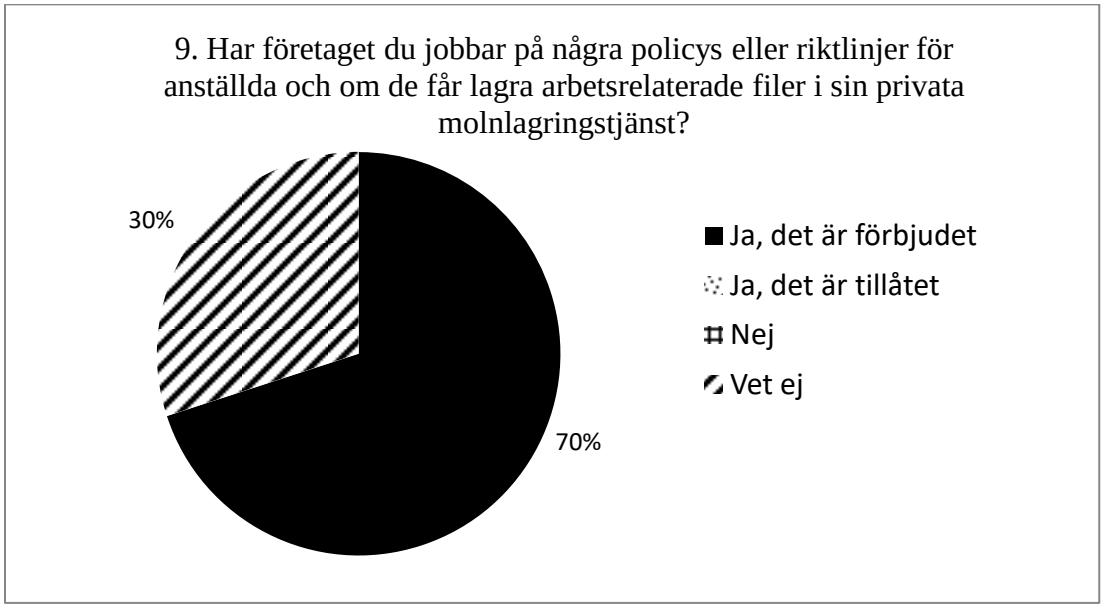
Figur 28. Controllers svar på fråga 7.

Figur 28 visar resultatet från fråga sju. Resultatet visar att 90 % (nio stycken) inte använder sin privata molnlagringstjänst för att lagra arbetsrelaterade filer. 10 % (en deltagare) använder eller har använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer.



Figur 29. Controllers svar på fråga 8.

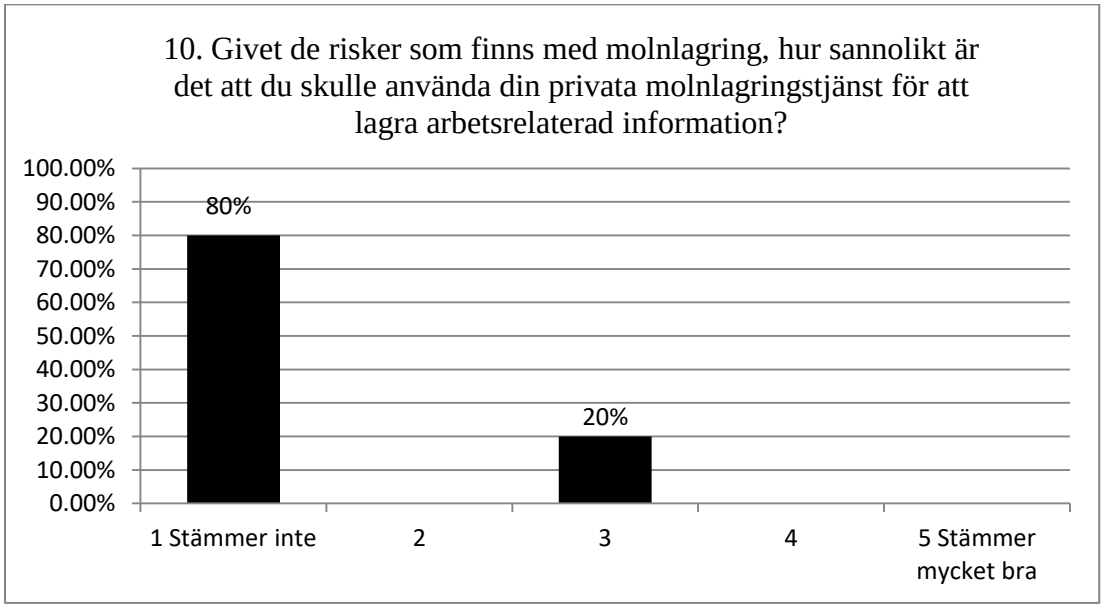
Figur 29 visar resultatet från fråga åtta. Resultatet visar att anledningen till att deltagaren använder eller har använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer var för att kunna komma åt filerna från en annan plats eller en annan dator.



Figur 30. Controllers svar på fråga 9.

Figur 30 visar resultatet från fråga nio. 70 % (sju stycken) svarade att företaget har policys och riktlinjer och att det är förbjudet för anställda att använda sin privata molnlagringstjänst

för att lagra arbetsrelaterade filer. 30 % (tre stycken) vet inte om företaget har några policys eller riktlinjer.



Figur 31. Controllers svar på fråga 10.

Figur 31 visar resultatet från fråga tio. Resultatet visar att 80 % (åtta stycken) svarade att det inte alls är sannolikt att de skulle lagra arbetsrelaterad information i sin privata molnlagringstjänst med tanke på vilka risker som finns. 20 % (två stycken) ställer sig neutrala i frågan.

6.4 Analys av enkätundersökning

Följande underkapitel analyserar svaren från enkätundersökningen och jämför även dessa mellan de olika avdelningarna. Varje fråga analyseras var för sig och listas nedan.

Fråga 1

Den första frågan ställdes för visa om användare använder en privat molnlagringstjänst överhuvudtaget för sina privata filer för att sedan kunna svara på följdfrågor. Informationssäkerhetsteamets svar visade att 84 % använder privat molnlagring för att lagra privata filer medan 100 % av kontorscheferna och 60 % av företagets controllers svarade samma.

Fråga 2

Fråga nummer två och tre ställdes för att undersöka om användaren använder sin arbetsdator, om användaren har en sådan, för att komma åt sina privata filer och om användaren har en klient installerad för att komma åt sin privata molnlagring. Fråga två och tre hör ihop på så sätt att, som tidigare nämnt i rapporten, en klient för molnlagringstjänsten skulle kunna vara en länk in i företagsnätverket. Skulle användaren ha en klient installerad på sin privata dator hemma, exempelvis, och sin arbetsdator så finns det en risk att eventuella skadliga filer från den privata datorn kunna synkroniseras till arbetsdatorn.

Kontorscheferna, som alla svarade att de använder en privat molnlagringstjänst för att lagra privata filer, använder sin arbetsdator i betydligt större utsträckning för att komma åt sina privata filer i molnet jämfört med informationssäkerhetsteamet och företagets controllers. Av kontorscheferna svarade 83 % att de använder sin arbetsdator för att komma åt sina privata filer i molnet. Av informationssäkerhetsteamet svarade 55 % att de använder sin företagsdator för att komma åt sina privata filer i molnet och av företagets controllers svarade 50 % att de gör det.

Resultaten visar att det är fler som använder sin arbetsdator för att komma åt sina privata filer i molnet än dem som inte gör det. En arbetsdator bör egentligen bara vara ett arbetsredskap för att de anställda ska kunna utföra sina arbetsuppgifter. När anställda använder privata tjänster som företaget inte har någon kontroll över kan detta innebära en risk. Det skulle exempelvis kunna leda till att anställdas privata filer i molnet kan vara infekterade av skadlig kod och därmed kunna infektera arbetsdatorn som i sin tur kan leda till att skadliga filer i värsta fall kan leta sig in i företagets nätverk. Det bör ur författarens perspektiv finnas begränsningar på hur anställda får använda sina arbetsdatorer.

Fråga 3

När det kommer till fråga tre är det ett intressant resultat just för att det visar att företag A låter sina användare installera den typen av mjukvara och risken för att klienten skulle kunna vara en inkörsport genom att exempelvis synkronisera skadliga filer från användarens privata dator och klient därmed existerar.

Här svarar 50 % av informationssäkerhetsteamet att de använder en klient på sin arbetsdator och 50 % använder webbläsaren. I jämförelse med kontorscheferna är skillnaden knapp, av kontorscheferna använder 60 % en klient och 40 % använder webbläsaren. Däremot använder 100 % av företagets controllers en klient för sin molnlagringstjänst.

Det intressanta är just att företaget tillåter användare att installera mjukvara på sina arbetsdatorer. Det kanske hade varit en bättre lösning att låsa ned datorerna tekniskt och låta administrationen installera den mjukvara som krävs för att de anställda ska kunna utföra sina arbetsuppgifter. En klient för en privat molnlagringstjänst är med största sannolikhet något som de anställda klarar sig utan i arbetet.

Fråga 4

Fråga fyra handlade om att få en uppfattning om hur medveten deltagaren är om risker som medförs med molnlagring jämfört med lokal lagring. En beskrivning med exempel på risker lades till för att tydliggöra för deltagarna vad frågan syftar på; *Risker med molnlagring skulle exempelvis kunna vara att molnlagringstjänsten blir hackad och dina filer läcker ut på Internet eller att obehöriga läser informationen som du lagrar i din molnlagringstjänst.* En likertskala användes för att låta deltagarna svara utifrån sin egen uppfattning snarare än att något svar är rätt eller fel.

Resultatet blev som förväntat att deltagarna från informationssäkerhetsteamet anser sig vara medvetna om att vissa risker medförs med molnlagring. Även kontorscheferna anser sig vara

medvetna om att vissa risker medförs, däremot svarade majoriteten av kontorscheferna en fyra på den femgradiga skalan, medan majoriteten av informationssäkerhetsteamet svarade en femma.

Svaren från företagets controllers var lite mer utspridda jämfört med de två andra avdelningarna. Majoriteten svarade dock en femma på skalan och övriga svar hamnade i mitten, alltså att de varken var fullt medvetna eller inte alls medvetna. Några stycken svarade dessutom en etta, att de inte alls är medvetna om risker med molnlagring.

Med tanke på att denna fråga ändrades efter den skickats ut till informationssäkerhetsteamet så blir det inte helt rättvist att göra en ren jämförelse mellan svaren från de olika avdelningarna. Trots det så visar resultaten att de tre avdelningarna ändå anser sig vara medvetna om att risker medförs med molnlagring, de enda som avvek från de övriga var några deltagare från företagets controllers som inte alls var medvetna om risker med molnlagring.

Trots att majoriteten av alla deltagare anser sig vara medvetna om att risker medförs med molnlagring så finns det ändå några som inte alls är medvetna. Det räcker inte att majoriteten är medvetna om att det finns risker, är det någon som inte är medveten och exempelvis lagrar arbetsrelaterade filer i sin privata molnlagringstjänst i tron om att det är säkert nog, och dessa filer sedan läcker så kan det bli stora konsekvenser. Det är av stor vikt att alla anställda är medvetna om hur information får lagras och vilka risker som finns med olika lagringssätt.

Fråga 5

Fråga fem ställdes för att undersöka om företaget har en egen molnlagringstjänst och om deltagarna är medvetna om det. Svaren på denna fråga är väldigt intressanta eftersom att företaget i fråga faktiskt har en egen molnlagringstjänst. Vid intervjun med informanten tillika kontaktpersonen på företag A togs denna fråga med svar upp och informanten blev väldigt chockad. Informanten kunde heller inte svara på varför fyra stycken från informationssäkerhetsteamet svarar att företaget inte har en egen molnlagringstjänst eller vet om att det finns en. Att det är 16 % och 5 % som svarar *Nej* respektive *Vet ej* skulle kunna ligga till grund för att en kontinuerlig upplysning eller utbildning på företaget är av behov.

Av informationssäkerhetsteamet är det endast 79 % som vet att företaget har en egen molnlagringstjänst där filer kan nås oavsett var de anställda befinner sig. Av kontorscheferna är det endast 67 % som vet att företaget har en egen molnlagringstjänst och av företagets controllers är det bara 50 % som vet om företagets molnlagringstjänst.

Resultatet visar tydligt att anställda på de olika avdelningarna inte är tillräckligt upplysta om vilka tjänster företaget erbjuder. Resultatet borde visat att 100 % från alla tre avdelningar vet om företagets molnlagringstjänst, eftersom att företaget faktiskt har en egen molnlagringstjänst. Eftersom det finns flera anställda på de olika avdelningarna som inte är medvetna om företagets molnlagringstjänst kan detta i sig vara en säkerhetsrisk då det skulle kunna vara en anledning till att privata molnlagringstjänster används för att lagra arbetsrelaterad information.

Fråga 6

Fråga sex handlar om vad deltagarna tycker om företagets egen molnlagringstjänst jämfört med privata molnlagringstjänster, mer specifikt om den är lika smidig som exempelvis Googles, Dropbox eller OneDrive's motsvarighet. I efterhand och i diskussion med kontaktpersonen på företaget så märktes det att frågan kunde vara något otydlig. Författaren ville få fram och fråga deltagarna om företagets molnlagringstjänst är smidig att använda, då tidigare nämnda privata molnlagringstjänster har egna klienter som gör användandet bekvämare. Frågan som ställdes var *Om Ja, Företaget jag jobbar på har en molnlagringstjänst som är lika smidig att använda som t.ex. Google Drive?* och den borde formulerats bättre då det ur deltagarens perspektiv kan ha syftat på en ren jämförelse mellan företagets molnlagringstjänst och Google Drive. Ordet smidig kan också tolkas på olika sätt men ur författarens perspektiv syftar det på bekvämlighet och tillgänglighet. Det borde ha klargjorts i frågan på ett tydligare sätt.

Denna fråga var en följdfråga till fråga fem och resultatet skiljer sig en del mellan avdelningarna. Informationssäkerhetsteamet anser att företagets molnlagringstjänst är väldigt smidig. Kontorscheferna har lite fler utspridda svar, vissa är neutrala i frågan och några svarade fyra på den femgradiga skalan, dock svarade majoriteten (50 %) att den är lika smidig som exempelvis Google Drive. Även företagets controllers svarar lite utspritt, majoriteten ställer sig neutrala i frågan medan några håller med helt och hållet och andra håller inte alls med.

Varför det skiljer sig så pass mellan de olika avdelningarna är inte helt tydligt. Det skulle kunna handla om teknisk kompetens, att vissa deltagare är mer tekniskt kunniga än andra. Sedan skulle det också kunna bero på om deltagarna tolkar frågan som en ren jämförelse mellan företagets molnlagringstjänst och Google Drive. Anser deltagarna att Google Drive inte är smidig överhuvudtaget, eller tvärtom, kan det avgöra vad resultatet blir.

Som tidigare nämnt kunde frågan vara lite otydlig för deltagarna. Detta resultat visar på att företagets egen molnlagringstjänst faktiskt är användbar för de anställda. I tidigare studier har en av orsakerna till att anställda använder sin privata molnlagringstjänst före företagets egen molnlagringstjänst är just på grund av att den inte är lika smidig och användbar.

Fråga 7

Den sjunde frågan återkommer till deltagarna och undersöker om de använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information. Problemet att anställda gör detta är etablerat genom tidigare studier och därför var det en lämplig fråga att ha med, dels för att se om det förekommer inom ett IT-företag men också för att ha underlag till intervjuerna.

Även detta resultat är intressant då 26 % av informationssäkerhetsteamet faktiskt har använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer. Av kontorscheferna har ingen använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer och av företagets controllers svarade en tiondel att de använder eller har använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer.

Resultatet är intressant för att de som har använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer mest är informationssäkerhetsteamet. Det kan tyckas att anställda som arbetar med informationssäkerhet ska vara fanbärare för just säkerhet gällande information. Att det då är en dryg fjärdel som har lagra arbetsrelaterade filer på detta sätt är enligt författaren oroväckande.

Det är helt förbjudet för anställda på företaget att lagra arbetsrelaterade filer i sin privata molnlagringstjänst och företaget har policys och riktlinjer för hur och var information får lagras.

Fråga 8

Den åttonde frågan var en följdfråga till fråga sju och det var en flervalsfråga som visar vilka orsaker som ligger till grund för deltagarna som svarade *Ja* på fråga sju. Svarsalternativen valdes ut genom att läsa tidigare studier och de vanligaste orsakerna i dessa. En tom kryssruta lämnades dessutom där deltagarna kunde fylla med egna ord om orsaken inte fanns med i listan.

Ingen av kontorscheferna använder eller har använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer och därför registrerades inget svar från kontorscheferna på denna fråga. Ett svar registrerades från företagets controllers och tio svar från informationssäkerhetsteamet.

Som väntat så visar resultatet att tillgänglighet, alltså att kunna komma åt information från olika datorer och platser, är den vanligaste orsaken både för informationssäkerhetsteamet och för företagets controllers. Den näst vanligaste orsaken för informationssäkerhetsteamet är något förvånande, om det är användaren som själv anser att filen eller filerna inte innehåller någon känslig information så kan det vara väldigt relativt. Svaret privata behov, som en deltagare från informationssäkerhetsteamet svarade, är svårt att analysera djupare då det är svårt att veta vad privata behov faktiskt innebär i detta sammanhang.

Vid intervjun med informanten från företaget diskuterades företagets molnlagringstjänst och informanten beskriver tjänsten som väldigt lättillgänglig och kan nås från andra platser och datorer.

Fråga 9

Den nionde frågan handlar om policys och riktlinjer gällande lagring av arbetsrelaterad information. Mer specifikt handlar frågan om företaget har några sådana för de anställda och om de får lagra arbetsrelaterad information i sin privata molnlagringstjänst. Företaget har policys och riktlinjer för sina anställda om hur och var företagets information får lagras, detta bekräftades i intervjun med informanten från företaget. Företaget tillåter inte sina anställda att lagra arbetsrelaterad information i sina privata molnlagringstjänster.

Detta resultat är intressant eftersom att endast 58 % av informationssäkerhetsteamet är medvetna om företagets policys och riktlinjer gällande lagring av arbetsrelaterade filer och att det är förbjudet att lagra sådan information i en privat molnlagringstjänst. Företagets controllers svarade också olika vilket ytterligare visar på att alla inte är helt medvetna om vad

som faktiskt gäller på företaget gällande lagring av information. Företagets kontorschefer däremot är fullt medvetna om att det finns policys och riktlinjer och att det är förbjudet att lagra information på detta sätt.

När denna fråga diskuterades med informanten från företaget så kunde informanten inte svara på varför så många inte vet om vad som faktiskt gäller. Informanten blev väldigt förbluffad av resultatet och förklarade att det finns policys och riktlinjer för vad som är tillåtet och inte gällande lagring av arbetsrelaterade filer. Det visar på att kontinuerlig upplysning eller utbildning för anställda kan vara av stor vikt om det är så att anställda glömmer av vad som gäller med hantering av information eller helt enkelt ignorerar vad som gäller på företaget. Detta resultat, likt resultatet på fråga sju, är intressant då informationssäkerhetsteamet inte verkar ha full koll på vad som gäller angående policys och riktlinjer för lagring av information. Som tidigare nämnt kan det tyckas att informationssäkerhetsteamet ska vara dem som har bäst koll på information och hur denna får och ska lagras.

Fråga 10

Den tionde frågan handlar om hur deltagarnas inställning till att lagra arbetsrelaterade filer i sin privata molnlagringstjänst hade förändrats om de blev upplysta om vilka risker molnlagring innebär. Frågan kom tyvärr i efterhand att bli lite ledande. Tanken med frågan var att undersöka om deltagarna skulle ändra sitt sätt att lagra filer om deltagarna inte var tillräckligt upplysta sedan innan. Denna fråga kunde därför bli något förvirrande för deltagare som redan var medvetna och upplysta om att vissa risker finns med molnlagring. Frågan använde en likertskala för att undersöka deltagarnas uppfattning i frågan. Denna fråga ställdes, som tidigare nämnt, för att undersöka om deltagarna skulle ändra sin inställning om de blev upplysta. Frågan grundar sig på att utbildning för anställda kan vara något som gör skillnad i hur anställda tänker och hanterar information, inte bara när det gäller specifikt molnlagring, detta tas också upp i intervjuerna

Eftersom frågan formulerades om innan den skickades till företagets kontorschefer och controllers så är det inte rättvist att göra en ren jämförelse mellan de olika avdelningarna. Däremot svarar majoriteten av de tre avdelningarna att de inte skulle lagra arbetsrelaterad information i sina privata molnlagringstjänster med tanke på vilka risker som finns. Detta resultat motsvarar inte riktigt vad som förväntades på förhand, det förväntade resultatet var att ingen skulle lagra information på detta vis. Att resultatet blev som det blev kan säkerligen bero på att frågan var svår att svara på och kanske förvirrande för deltagarna.

6.5 Intervjuer

Intervjuerna som gjordes med företag A och företag B hade som syfte att besvara tre huvudfrågor:

- *Hur ser du på säkerheten generellt för molnlagring som hanteras av en utomstående?*
- *Tidigare studier har visat att anställda använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information, vad är din syn på det?*
- *Hur hanterar ni detta problem på ert företag?*

Dessa tre frågor är som sagt huvudfrågorna som var tänkt att besvara forskningsfrågan ”*Hur hanterar ett IT-företag att användare lagrar arbetsrelaterad information i privata molnlagringstjänster?”*. Första frågan ställdes för att informanterna skulle få ge sin egen syn på molnlagring och säkerhet, då i synnerhet molnlagring som hanteras av en extern part, och för att komma in på ämnet i lugn och ro. Fråga nummer två ställdes för att förklara och etablera problemet för informanterna och för att de skulle få förklara deras syn på problemet. Den sista frågan ställdes för att undersöka hur de två företagen arbetar med att motverka eller förhindra problemet. Vilka lösningar företagen använder, om det exempelvis är tekniska lösningar eller utbildning för att göra personalen medveten.

Informant 1 från företag A jobbar som senior informationssäkerhetskonsult på företaget, vilket innebär att informanten är rådgivare åt företag, myndigheter och kommuner när det gäller informationssäkerhet.

Informant 2 från företag B är säkerhetsansvarig på företaget och har varit det i ett år ungefär. Informanten har verksamhetsansvaret kring fysisk och logisk säkerhet och har det senaste året jobbat mycket med olika säkerhetsstandarder, bland annat ISO 27001.

Tematisk kodning användes, som tidigare nämnt, för att para ihop huvudfrågorna med vad informanterna svarade. Svaren från intervjuerna presenteras genom att lista varje huvudfråga med svaren från informanterna i tur och ordning. Istället för att analysera varje informants svar var för sig så presenteras en analys av intervjuerna i kapitel 6.2.1.

Hur ser du på säkerheten generellt för molnlagring som hanteras av en utomstående?

Informant 1 från Företag A:

”Nej men det är ju alltid som med all säkerhet så är det en avvägning vad det är då va. Alltså om man då, alltså om man pratar då konfidentialitet, riktighet eller tillgänglighet eller CIA”

Den första informanten menar på att det alltid är som med all säkerhet, att en avvägning får göras. Specifikt syftar informanten på konfidentialitet, riktighet och tillgänglighet. Är det så att informationen ska vara helt skyddad, då kan inte informationen lämna det inneslutna nätverket eller kanske till och med byggnaden, då kan inte informationen vara uppkopplad överhuvudtaget. Vidare diskuterar informanten om zoner och klassificering av information, viss klassificering av information kanske tillåter informationen bara får nås i företagets nätverk, viss information kanske får nås från biblioteket (där intervjun genomfördes) och annan information kanske får nås oavsett lokalisering. När det gäller publika och öppna nätverk, som exempelvis kaféer, så menar informanten på att då är det snarare miljön som är den stora säkerhetsbristen än själva molnlagringstjänsten. Likadant resonerar informanten om informationen bara nås från det interna och privata nätverket som är helt nedlåst, ja då krävs det att molnlagringstjänsten uppfyller samma krav som ställs på det egna nätverket. I det stora hela menar informanten på att det beror på vilken typ av information som lagras i molnet och hur den är klassificerad samt vilka krav som ställs på tillgänglighet.

Informant 2 från företag B:

”Alltså det är ju ett sådant stort ämne i sig så det är väldigt svårt men vad vi gör här är vi tillåter inte att företagsinformation lagras i privata molntjänster så att säga.”

Informant 2 från företag B hade inte riktigt lika mycket att säga om sin syn på frågan utan förklarade mer direkt hur de på företaget jobbar med att förhindra och motverka att anställda lagrar arbetsrelaterade filer inte lagras i privata molnlagringstjänster. Informanten nämner, likt informant 1, klassificering av information och att det är avgörande för hur information får lagras. Utöver detta så sades inget mer om informantens syn på den specifika frågan.

Tidigare studier har visat att anställda använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information, vad är din syn på det?

Informant 1 från företag A:

”Det finns ingen anledning att använda den privata, alltså Dropbox eller någonting annat för delning egentligen. Enda tillfället där det faktiskt är så, som jag vet då, och när jag själv använder det, det är när jag vill dela en fil med någon annan som är utanför min organisation. Då kan inte jag, som på Dropbox, dela den här filen in för att då måste dem ha ett konto och vara med i min AD”

På företag A är det förbjudet att använda privat molnlagring för att lagra arbetsrelaterade filer och när detta diskuteras, samtidigt som svaren från enkäten togs upp, så hade informanten en teori om varför det ändå sker. Företaget använder OneDrive och Office365 som molnlagring och detta kan alla anställda kom åt var dem än är men däremot är det problematiskt att dela filer med personer utanför organisationen. Informanten förklarar att med den nuvarande molnlösningen som företaget använder så saknas det en tjänst för att kunna dela filer med personer utanför organisationen på ett smidigt sätt.

Informant 2 från företag B:

”Vi har en egen tjänst men den är inte fullt utvecklad och vi har samma regler där så att. Och jag kanske är lite gammalmodig men än så länge ser jag helst att man har sitt arbetsredskap, sin dator som vi har kontroll över och kör VPN-klienter och Citrix för att komma åt information. Men alltså allting ändras men det är som det är nu.”

Informant 2 besvarade redan denna fråga när första frågan ställdes. Det är helt förbjudet för anställda att lagra arbetsrelaterad information i sin privata molntjänst. Företaget har en egen lösning för sina anställda för att lagra information. Anställda kan dessutom komma åt informationen från andra platser, exempelvis om anställda jobbar hemifrån eller om de är ute på fältet hos kunder.

Hur hanterar ni detta problem på ert företag?

Informant 1 från företag A:

”Jajamän, det fick jag göra och det finns policys och dessa är jättebra alltså”

Citatet ovan är som svar på frågan om anställda vid anställning behöver läsa igenom och skriva under dokument innehållandes policys och riktlinjer vad gäller informationssäkerhet. Som informanten tidigare nämnde är det även helt förbjudet för de anställda att lagra arbetsrelaterad information i sina privata molnlagringstjänster. Företaget har också en egen molnlagringstjänst, OneDrive och Office365, som alla anställda kan använda och nå var dem än befinner sig.

Informanten förklarar också att alla anställda har en företagsdator som inte är nedlåst rent tekniskt, vilket innebär att de anställda kan installera mjukvara på datorerna, exempelvis klienter för molnlagringstjänster. Även om företaget administrerar de anställdas datorer så övervakas dem inte på så sätt att de har koll på allt som sker på datorerna hela tiden.

Informanten fick även frågan om personalen utbildas kontinuerligt, exempelvis årligen, om informationssäkerhet generellt för att friska upp minnena hos de anställda om risker med mera. Till denna fråga svarade informanten att informanten inte varit på företaget tillräckligt länge, bara åtta månader, för att kunna svara på det. Däremot förklarar informanten att ISO 27000-certifiering innefattar uppdatering av hantering av informationssäkerhet, vilket företag A har. Informanten förklarar också att i alla verksamheter informanten har varit i så tittas det generellt sett bara på yttre hot, aldrig inre hot. Skulle något hända internt så är det snarare omedvetet, att en användare inte är medvetet elak men samtidigt finns det såklart undantag.

Vidare förklarar informanten att information klassificeras på företag A. Informanten är van vid att vid skapande av ett nytt dokument, redan då sätta en informationsklassificering. Däremot är personalen inte helt medveten om vad informationsklassificering faktiskt innebär, trots att företag har policys och utbildning om saker och ting som berör det här ämnet. Informanten menar även på att kontrollen av efterlevnad är rent generellt dålig.

Informant 2 från företag B:

”Utan det är, ja, det är inte så att vi tekniskt hindrar det utan det är via policys, regler och rutiner som talar om vad man får göra och inte göra.”

Informanten förklarar att företag B inte tekniskt sett hindrar anställda att lagra arbetsrelaterad information i sina privata molnlagringstjänster. Genom policys, regler och rutiner har ett regelverk byggts upp på företaget som anställda ska följa. Även på företag B så är det förbjudet för anställda att lagra arbetsrelaterad information i sin privata molnlagringstjänst.

Likt företag A så klassificerar även företag B information men här går informant 2 mer på djupet om hur företag B klassificerar informationen. Informationen klassificeras utifrån tre olika kategorier; publik, konfidentiell och intern information. Publik information är för alla, konfidentiell information är för en utvald grupp som kan vara inom företag men också inom företaget plus utomstående och intern information är bara för företagets anställda. Det är alltså typen av klassificering som avgör var information får lagras, exempelvis får publik information lagras var som helst eftersom den ändå är till för alla. Informanten nämner också att det finns särskilda regelverk som är lätt att koppla mot viss information. Handlar det om

konfidentiell information så får den exempelvis bara lagras på vissa enheter och måste krypteras.

Vidare förklarar informanten att företaget tittar på ett *Rights Management System* där regler kan läggas på information. Det innebär att information som exempelvis klassificeras som konfidentiell automatisk blir krypterat eller att e-post markeras med att det inte får vidarebefordras. Det går också att sätta rättigheter på dokument att vissa personer bara får komma åt det och skulle dokumentet hamna någon helt annanstans utanför företaget så gäller fortfarande rättigheterna. Informanten menar på att genom att utnyttja ett *Rights Management System* så blir problemet med var informationen finns lagrad inte lika stort eftersom rättigheter och gränser ändå kan sättas.

Informanten förklarar att företaget har, som tidigare nämnt en egen molnlagringstjänst och där gäller samma regler att det bara är publik information och som ännu inte är full utvecklad. Information kan däremot nås av de anställda via *Virtual Private Network* (VPN) om de befinner sig utanför företagets nätverk. Informanten menar också på att allting kan förändras men det är så läget är just nu.

Även på företag B har varje anställd en arbetsdator som administreras av företaget. Informanten menar på att de har full kontroll över datorerna men datorerna är inte nedlåsta rent tekniskt. Företaget övervakar inte sina anställda jämt och ständigt, så det är fullt möjligt att installera mjukvara på datorerna men informanten poängterar att det är genom policys, regler och rutiner som detta hanteras och det förväntas att de anställda förhåller sig till dessa.

När det gäller utbildning och kontinuerlig sådan så förklarar informanten att vid anställning så görs en genomgång vad som gäller angående informationssäkerhet generellt, det innefattar bland annat besökspolicy och hur information får hanteras och lagras. Dessutom görs detta kontinuerligt, två gånger per så måste alla anställda läsa igenom ett visst antal dokument. Dessa dokument innehåller bland annat deras informationssäkerhetspolicy, besökspolicy och säkerhet kring arbetsplatsen.

6.6 Analys av intervjuer

Två intervjuer genomfördes med två informanter från två olika företag i IT-branschen, företag A och företag B. Intervjuerna gjordes för att besvara den övergripande frågeställningen *Hur hanterar IT-företag att användare lagrar arbetsrelaterad information i privata molnlagringstjänster?*

Den inledande frågan som handlade om informanternas generella syn på molnlagringstjänster och säkerhet gav blandade svar. Informant 1 från företag A gav ett väldigt utvecklat svar på vad informanten tyckte om molnlagring generellt sett. Informanten från företag A visade också tydligt att informanten var insatt i ämnet och medveten om olika säkerhetsrisker och bedömningar som behöver göras beroende på vilket typ av information som ska lagras. Informant 2 från företag B gav inte ett lika detaljerat svar om sin syn på samma fråga utan gick mer direkt på hur de på företaget arbetar med att motverka att anställda lagrar arbetsrelaterad information i sina privata molnlagringstjänster. Denna inledande fråga ställdes

för att göra en lättsam start och skapa en relation med informanterna innan intervjun gick över till att ställa mer specifika frågor.

Båda informanterna förklarade att respektive företag har policys och riktlinjer för hur de anställda får hantera och lagra information. Närmare bestämt är det helt förbjudet på båda företagen för de anställda att lagra arbetsrelaterad information i sina privata molnlagringstjänster. Detta var också någon som var förväntat av författaren. Eftersom båda företagen arbetar i IT-branschen och hanterar mycket information, bland annat kundinformation så förväntades det att företagen skulle ha restriktioner på hur information får lagras och hanteras.

Företag A har en egen och komplett molnlagringstjänst i form av OneDrive och Office365. Denna kan alla anställda logga in på var de än befinner sig. Företag B har också en egen molnlagringstjänst men den är ännu inte fullt utvecklad, däremot så kan de anställda komma åt företagsinformation från en annan plats med hjälp av VPN. Just mellan dessa två företag så skiljer det sig lite, det ena företaget har en komplett molnlagringstjänst medan det andra arbetar mer med VPN. Informant 2 från företag B förklarar att det är så det är nu och informanten föredrar egentligen att använda VPN ur säkerhetsperspektiv men informanten nämner också att saker och ting kan förändras. Det finns helt klart olika sätt att lösa detta på och inget är väl rätt eller fel när det gäller hur företagen hanterar detta.

När frågan ställdes om hur företagen hanterar problemet att anställda lagrar arbetsrelaterad information i sina privata molnlagringstjänster så var den ena informanten betydligt mer påläst och det var informant 2 från företag B. Detta kan till stor del bero på att informant 2 från företag B var säkerhetsansvarig på företaget. Vidare hade informant 1 från företag A bara arbetat på företaget i ungefär åtta månader. Företag B jobbar väldigt mycket med att göra sina anställda medvetna och tar informationssäkerhet på stort allvar. Bara det faktum att de anställda får gå igenom och skriva under dokument som berör bland annat informationssäkerhet två gånger per år visar på att företaget tar det på stort allvar.

Inget av företagen hindrar dock sina anställda att installera mjukvara på sina företagsdatorer, rent tekniskt sett det vill säga. Det ger ändå möjligheten för en anställd att installera mjukvara som kanske inte är tillåten från ledningen. Exempelvis att klienter för privata molnlagringstjänster kan installeras på företagsdatorerna och därmed kunna skapa en länk in i företagets nätverk från en privat dator med samma klient installerad. Företagen litar så pass mycket på sina anställda att de sköter sig och förhåller sig till de riktlinjer och policys som gäller på respektive företag.

7 Slutsats

Tidigare studier visade att anställda inom IT använde sin privata molnlagringstjänst för att lagra arbetsrelaterad information, orsaker till detta varierade. Det kunde exempelvis bero på att företaget saknade en egen molnlagringstjänst eller att det fanns en men den var besvärlig att använda jämfört med den privata.

Enkätundersökningen i denna studie visade på samma resultat, anställda har använt eller använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information. Det är dessutom väldigt intressant att deltagarna i enkäten bland annat jobbar med informationssäkerhet på sitt företag. Anställda som jobbar med informationssäkerhet bör vara dem som har bäst kunskap om säkerhet och risker gällande information men resultatet från enkätundersökning visar att det inte är så på företag A. Exempelvis var det informationssäkerhetsteamet som hade flest deltagare som har använt sin privata molnlagringstjänst för att lagra arbetsrelaterade filer.

Resultatet från enkätundersökning visar också att det kan vara betydelsefullt för företag att göra sina anställda medvetna om informationssäkerhet och vad det kan innebära om säkerheten brister samt att det görs någon form av uppföljning att de anställda förstår och fullföljer det som förmedlats. Alla tre avdelningar hade exempelvis några deltagare som inte ens vet om företaget har en molnlagringstjänst för sina anställda och det kan också vara ett tecken på att företaget behöver någon form av kontinuerlig genomgång av information och hur denna får och kan lagras.

För att motverka och förhindra detta problem så har båda företagen som intervjuades i studien policys och riktlinjer för sina anställda om hur informationssäkerhet ska hanteras. Dessutom jobbar det ena företaget väldigt proaktivt genom kontinuerlig upplysning och utbildning och det sker genom att de anställda är tvungna att läsa igenom och signera ett visst antal dokument som behandlar bland annat informationssäkerhet och hur information ska hanteras och lagras.

Det förväntade resultatet på denna studie, som inriktade sig på ett IT-företag, var att det åtminstone skulle finnas policys och riktlinjer för informationssäkerhet och hur och var information får lagras. Det faktiska resultatet stämmer väl överens med det förväntade resultatet. Däremot är flertalet av svaren från enkätundersökning väldigt förvånande med tanke på vad deltagarna arbetar med. Något annat som är intressant är att på båda företagen så tillåts de anställda att installera mjukvara på sina företagsdatorer.

8 Diskussion

I detta kapitel görs en diskussion ur vetenskapliga, samhälleliga och etiska aspekter och vilka begränsningar denna studie har. Förslag på framtida arbete presenteras också

För att undersöka hur IT-företag hanterar problemet att anställda använder sin privata molnlagringstjänst för att lagra arbetsrelaterad information så genomfördes intervjuer med två informanter från två olika IT-företag. Där diskuterades det hur de olika företagen hanterar problemet. Innan intervjuerna genomfördes så gjordes en enkätundersökning som skickades ut till informationssäkerhetsteamet, kontorschefer och controllers på företag A för att se i vilken utsträckning problemet existerar på företaget.

Hoten mot validitet och reliabilitet som togs upp i kapitel 4.2 hanterades till stor del. Däremot kunde några av frågorna i enkätundersökning vara missvisande, mer specifikt frågorna *Om Ja, Företaget jag jobbar på har en molnlagringstjänst som är lika smidig att använda som t.ex. Google Drive?* och *Hur sannolikt är det att du skulle lagra arbetsrelaterade filer i din privata molnlagringstjänst efter att du blivit upplyst om vilka risker molnlagring innebär?* Den förstnämnda frågan kunde tolkas som en ren jämförelse mellan företagets molnlagringstjänst och Google Drive. Den sistnämnda frågan kunde bli lite missvisande om det är så att deltagaren redan var upplyst om risker gällande molnlagring. Dessa frågor skulle kunna vara ett hot mot *internal validity.* Hot mot *reliability* och *external validity* hanterades genom att noggrant förklara inom vilken bransch företagen är verksamma och vilken grupp av människor som deltog i enkätundersökningen.

Någonting som skulle kunna påverka trovärdigheten på studien är det låga antalet deltagare i enkätundersökningen. Trots flera påminnelser av författaren till företaget så registrerades inte så många svar som författaren ville ha. Även om tre olika avdelningar deltog och en jämförelse kunde göras mellan dessa så var helt enkelt antalet deltagare för lågt. Däremot visar studien att det kan finnas skillnader mellan olika avdelningar på företag. Framförallt visar studien att anställda som arbetar med informationssäkerhet inte nödvändigtvis är dem som hanterar information säkrare än andra avdelningar.

Vidare behandlar denna studie ett stort område, molnlagring, som används mer och mer av både privatpersoner och företag i samhället. Molnlagring skapar flexibilitet och tillgänglighet genom att information kan laddas upp i molnet och nås från olika platser och datorer. Delning av information och samarbete är också något som möjliggörs med molnlagring. Samtidigt kan molnlagring bryta mot vissa etiska aspekter. Exempelvis om anställda lagrar eller delar information om företagets kunder på en privat molnlagringstjänst om detta inte är tillåtet. Konsekvenser och påföljder om denna information skulle läcka och den då inte har lagrats på ett korrekt sätt kan bli stora för både företaget men även den anställda.

Denna studie bidrar till att visa att, även inom IT-branschen, så använder anställda sin privata molnlagringstjänst för att lagra arbetsrelaterad information men framförallt så bidrar studien med att visa hur IT-företag hanterar problemet. Med tanke på att problemet förkommer på IT-företaget som enkätundersökningen gick ut till, specifikt personer som arbetar med informationssäkerhet, så kan det bli en tankeställare för företag inom IT men också inom

andra branscher som kanske inte lägger störst fokus på informationssäkerhet. Dessutom så kan studiens resultat om hur IT-företag arbetar med att motverka och förhindra problemet bidra till att andra företag och andra branscher kan anamma samma lösningar om det saknas. Det kan antas att personer som arbetar med just informationssäkerhet bör ha mer kunskap om risker och säkerhet gällande molnlagring, vilket gör resultatet från enkätundersökning väldigt intressant. Då kan nästa fråga bli hur det ser ut i andra branscher och företag som inte arbetar med informationssäkerhet på samma sätt.

Även om denna studie främst gick ut på att undersöka hur ett IT-företag motverkar problemet med att anställda lagrar arbetsrelaterad information i sina privata molnlagringstjänster så undersöktes även om anställda på företag A är en del av problemet. Enkätundersökningen visade, som sagt, att det förekommer att de lagrar eller har lagrat arbetsrelaterad information i sin privata molnlagringstjänst. Vidare så undersökte enkäten de anställdas attityd och medvetenhet kring säkerhet och molnlagring och jämfört med studien av Mijuskovic och Ferati (2015) så svarade majoriteten från företag A att dem är fullt medvetna om att vissa risker finns med att använda en molnlagringstjänst.

Då detta är en fallstudie som inriktade sig på ett företag i IT-branschen så går resultatet av denna studie inte att generalisera. Skulle samma studie göras på företag som är verksamma i andra branscher så kan resultatet bli annorlunda.

8.1 Framtida arbete

Denna studie har framställt resultat om att problemet med att anställda lagrar arbetsrelaterad information i sina privata molnlagringstjänster förekommer inom IT-branschen. Dessutom visar studien hur ett IT-företag arbetar med att motverka problemet, genomgående är att båda företagen åtminstone har policys och riktlinjer för hur anställda ska hantera arbetsrelaterad information.

Det går däremot inte att generalisera detta resultat för samhället i stort. Därför kan det vara av intresse att göra en studie hur det ser ut i andra företag som är verksamma i andra branscher där fokus inte ligger på IT. Information, och i synnerhet arbetsrelaterad information, är förhoppningsvis något de flesta företag värnar om och därför kan det vara intressant och upplysande att göra studier på företag som kanske inte riktigt har informationssäkerhet i fokus. En studie om privat molnlagring i arbetet för företag i andra branscher och domäner är därför en bra idé för fortsatta studier inom ämnet.

Referenser

Amara, N., Zhiqui, H., & Ali, A. (2017). Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (ss. 244-251). Nanjing, Kina: IEEE. doi: 10.1109/CyberC.2017.37

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*(4), 50-58. doi: 10.1145/1721654.1721672

Ashford, W. (2015). Employee use of cloud storage puts UK business data at risk. https://www.computerweekly.com/news/4500254436/Employee-use-of-cloud-storage-puts-UK-business-data-at-risk
[Hämtad 2018-05-14]

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects* (2nd ed.). London: Springer-Verlag.

Google. (u.å.). Ladda ner Säkerhetskopiera och synkronisera - gratis molnlagring. https://www.google.com/intl/sv_ALL/drive/download/backup-and-sync/
[Hämtad 2018-03-09]

Lindberg, A., Marat, K., & Månsson, D. (2015). *Privat molnlagring i tjänsten - Orsaker och potentiella risker.* (Kandidatuppsats, Instutionen för informatik, Lunds Universitet Ekonomihögskolan). http://lup.lub.lu.se/student-papers/record/5471206
[Hämtad 2018-02-20]

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing.* U.S. Department of Commerce. National Institute of Standards and Technology. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf
[Hämtad 2018-02-23]

Mijuskovic, A., & Ferati, M. (2015). User Awareness of Existing Privacy and Security Risks when Storing Data in the Cloud. *International Conference on e-Learning 2015.* http://elearning-conf.eu/docs/cp15/paper-43.pdf
[Hämtad 2018-04-24]

Robson, C. (2002). *Real World Research : A Resource for Social Scientists and Practitioner-researches.* Oxford: Blackwell Publishing.

MSB. (2017). Varför är informationssäkerhet viktigt? https://www.informationssakerhet.se/Om-informationssakerhet-kon/vad_ar_informationssakerhet/
[Hämtad 2018-03-08]

Vetenskapsrådet. (2002). Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning. https://www.gu.se/digitalAssets/1268/1268494_forskningsetiska_principer_2002.pdf [Hämtad 2018-03-27]

Wohlin, C., Runesson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in Software Engineering.* Berlin: Springer-Verlag.