LUNDS UNIVERSITET
Ekonomihögskolan
Institutionen för informatik

Med huvudet bland molnen

En undersökning av beslutsfattares medvetenhet kring informationssäkerhet vid användning av SaaS i affärsverksamhet

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Axel Bengtsson
Eddie Blad

Handledare: Markus Lahtinen

Rättande lärare: Björn Svensson
Christina Keller

Med huvudet bland molnen: En undersökning av beslutsfattares medvetenhet kring informationssäkerhet vid användning av SaaS i affärsverksamhet

ENGELSK TITEL: Head in the Clouds: A Study of decision makers' awareness of information security in the use of SaaS in businesses.

FÖRFATTARE: Axel Bengtsson och Eddie Blad

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Odd Steen, Docent, Fil Dr

FRAMLAGD: januari, 2020

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 51

NYCKELORD: Software as a service, informationssäkerhet, sekretess, tillgänglighet, kontroll

SAMMANFATTNING (MAX. 200 ORD): Denna uppsats ämnar att undersöka medvetenhet kring informationssäkerhet hos beslutsfattare i deras användning av SaaS-applikationer i affärsverksamhet. Denna undersökning görs med hjälp av fem semistrukturerade telefonintervjuer med beslutsfattare inom olika branscher. Tre delområden för informationssäkerhet har identifierats i litteraturgenomgången. Dessa faktorer är: sekretess, tillgänglighet och kontroll, och ligger till grund för den intervjuguide som skapats i syfte att besvara vår frågeställning. Efter genomförd empirisk undersökning jämfördes resultat med tidigare litteratur kring området i ett diskussionsavsnitt. Där belystes likheter och skillnader, vilket i sin tur låg till grund för den slutsats som presenterades i sista avsnittet. Efter avslutad undersökning kan det konstateras att beslutsfattare besitter medvetenheten inom vissa specifika områden. Trots denna medvetenhet och identifiering av risker, saknas många gånger motverkande åtgärder oftast på grund av
att informanterna anser sin verksamhet irrelevant i diskussionen kring informationssäkerhet.

Innehåll

Figurer

Tabeller

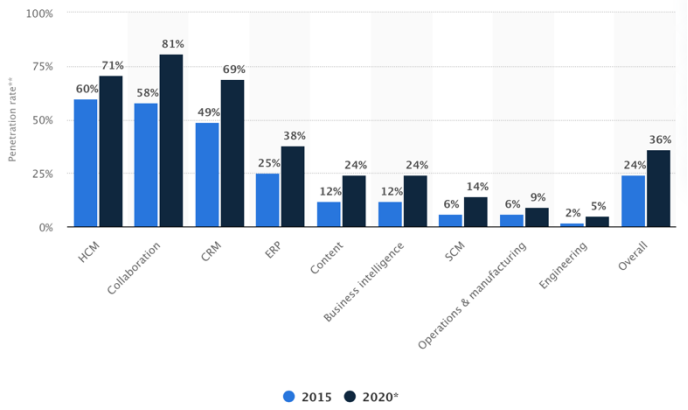
Begreppslista

Beslutsfattare	Personer som har i uppgift att fatta beslut inom ett visst område, vars beslut berör ett större antal människor.
Cloud computing	I denna uppsats använder vi den definition som NIST formulerat. Se avsnitt 2.1 för en mer utvecklad definition.
SaaS leverantör	I denna uppsatsen använder vi begreppet SaaS leverantör när vi hänvisar till det företag som tillhandahåller tjänsten (Sehgal & Bhatt, 2018).
SaaS applikation	I denna uppsats använder vi begreppet SaaS applikation när vi hänvisar till den tjänst som tillhandahålls av leverantör över Internet (Sehgal & Bhatt, 2018).
Public cloud	Public cloud tillhandahålls av en tredjepartsleverantör via Internet och är tillgängligt för allmänheten för användning. Public clouds kan erbjudas utan vidare kostnad, eller mot en återkommande prenumerationsavgift, där man betalar för faktiskt förbrukning (Sehgal & Bhatt, 2018).
Medvetenhet	Kännedom om vissa fakta och insikten om deras relevans (ofta något moraliskt viktigt)

1 Introduktion

1.1 Bakgrund

Varje dag genereras användbar data, en siffra som successivt ökar i takt med teknologins utveckling. Det senaste året användes i genomsnitt 4 416 720 gigabyte data per minut, vilket är en 41% ökning sedan 2018 (Domo, 2019). Beslutsfattare behöver således använda lämpliga metoder för att generera och lagra data som är relevant till respektive affärsverksamhet. Användning av molntjänster är en trend som växt sig stark som konsekvens av detta accelererande behov av datahantering (Wang & Chen, 2011). År 2018 använde 57% av samtliga svenska företag med minst 10 anställda någon form av molntjänst. Bland dessa företag är de vanligast förvärvade tjänsterna e-post och fillagring (SCB, 2018).



Figur 1. Penetrationsgraden av SaaS kategoriserat i arbetsfunktion över hela världen 2015 och 2020 (Liu, 2017).

Ser man till diagrammet ovan blir det också tydligt att SaaS är en populär plattform för företag runtom i världen. Användningen av SaaS ökade med 12 procentenheter till hela 36% av den totala användningen av IT-applikationer. Några av fördelarna med SaaS applikationer innefattar sänkta kostnader, snabb skalbarhet och förenklade implementeringsprocesser (Wang & Chen, 2011). Flera stora cloud leverantörer såsom Microsoft, Yahoo och Accenture har däremot drabbats av olika typer av dataintrång sedan SaaS applikationerna introducerades, där intrånget 2014 i Apples iCloud var det mest uppmärksammade av olika anledningar (Kelion, 2014). Dataintrång är dock endast en av flera risker med att övergå till cloud computing och SaaS applikationer (Amara, Zhiqui & Ali, 2017).

1.2 Problemområde

Julisch och Hall (2010) visar att det historiskt sett föreligger en tveksamhet kring SaaS applikationer på grund av oklarheter kring säkerheten. I en senare publikation prognostiserar Liu (2017) att 36% av alla applikationer levereras via SaaS år 2020. Med sådan statistik kan det ifrågasättas om rådande säkerhet fortfarande är ett orostecken hos användare inom cloud computing och framförallt software as a service modellen.

Seghal och Bhatt (2018) menar att professionella inom IT-sfären fortfarande anser säkerhet som den främsta utmaningen inom cloud computing. SaaS lösningar implementeras ofta för att undvika höga uppstartskostnader, undgå komplicerad installation och drift av avancerad mjukvara och system (Carroll, Van Der Merwe & Kotze, 2011). Detta i samband med lättillgänglig skalbarhet ger användare i behov av att effektivisera sina IT-relaterade processer goda incitament till att implementera SaaS applikationer (Janssen & Joha, 2011; Julisch & Hall, 2010; Wang & Chen, 2011).
Samtidigt påvisar Wang och Chen (2011) att användare av SaaS ofta inte besitter samma nivå av expertis som sakkunniga inom IT-branschen. Med det i åtanke kan det ifrågasättas om beslutsfattare på företag som använder sig av SaaS delar medvetenhet om eller förhållningssätt till informationssäkerhet inom cloud computing.

1.3 Forskningsfråga

Hur ser medvetenhet kring informationssäkerhet ut hos beslutsfattare vid användning av SaaS?

1.4 Syfte

Syftet med denna uppsats är att utifrån ett säkerhetsperspektiv utreda hur medvetenhet hos beslutsfattare ser ut kring informationssäkerhet i deras användning av SaaS i sin verksamhet.

1.5 Avgränsningar

I denna uppsats begränsas urvalet till små företag. Definitionen för små företag är tagen från Europakommissionen (2003) och säger följande: "*Med små företag avses företag med färre än 50 anställda och en årsomsättning eller balansomslutning som inte överstiger 10 miljoner EUR.*" Vidare vill vi belysa att uppsatsen endast kommer behandla så kallade public cloud-applikationer, och kommer således bortse från andra deployment modeller, som hybrid eller private cloud.

2 Litteraturgenomgång

I litteraturgenomgången kommer begreppet *cloud computing* först definieras. Därefter kommer modellen *software as a service* presenteras. Sedan introduceras begreppet *informationssäkerhet* vilket övergår i en utveckling av informationssäkerhet inom cloud computing.

Utifrån tidigare litteratur inom området identifieras tre framstående säkerhetsområden som medföljer SaaS applikationer. Det första delområdet är *sekretess* och hämtas ur *CIA-triaden*

(se figur 2). Sekretess syftar till att skydda information från obehöriga. I detta avsnitt behandlas därför olika former av dataintrång och hur detta motverkas. *Tillgänglighet* hämtas också ur CIA-triaden och syftar till att information måste vara tillgängligt när det behövs. Inom detta delområde behandlas därför hur man kan reglera applikationens tillgänglighet med olika åtgärder. Det sista delområdet i uppsatsen är kontroll, vilken hämtas ur *Parkers hexad* (se figur 3), och syftar till de problem som relaterar till dataförlust. Inkluderat i detta delområde är därför hantering och förebyggande av dataförlust samt olika typer av lock-ins och hur detta förebyggs. I slutet av kapitlet presenteras begreppet *förtroende* och hur detta enligt litteraturen spelar en stor roll inom det teoretiska området för SaaS applikationer.

2.1 Definition av cloud computing

Sehgal och Bhatt (2018) använder sig av NISTs definition av cloud computing, likt andra publikationer om cloud computing (Amara et al. 2017; Wrinkler 2011). Enligt NIST definition finns det fem kriterier som måste uppnås inom cloud computing.

Rapid Elasticity
Molnets resurser ska enligt denna definition vara skalbara för både ökad och minskad användning. Ur konsumentens perspektiv är kapacitet inom cloud computing ofta oändlig, och de har möjlighet att bruka hur mycket, eller hur lite de än har behov av (Mell & Grance, 2011)

Measured Service
Leverantörer av cloudtjänster kan mäta resursanvändning och prestanda av olika aspekter inom cloud computing, beroende på typen av tjänst som utförs. Användningen av resurserna kan därav bevakas, kontrolleras och rapporteras, vilket bidrar med transparens mellan användare och leverantör. Det här en väsentlig komponent för cloudtjänsters resursoptimering, fakturering och behörighetskontroll (Mell & Grance, 2011).

On Demand Self Service
Användare ska kunna tillhandahålla sig leverantörens tjänster så som server tid eller lagring automatiskt, vid behov. En mänsklig bilateral interaktion ska inte behövas mellan användare och leverantör (Mell & Grance, 2011).

Ubiquitous Network Access
Tjänsterna som tillhandahålls ska vara tillgängliga över ett nätverk och vara åtkomliga från diverse plattformar som mobiltelefoner, bärbara datorer, och surfplattor (Mell & Grance, 2011).

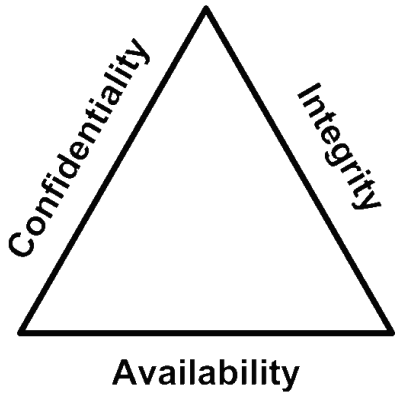
Resource Pooling
Fysiska och digitala resurser som minne, lagring och processorkraft är samlade för att tillhandahållas till olika användare och klienter samtidigt. Resurserna kan tilldelas dynamiskt till olika användare baserat på efterfrågan. Med detta tillkommer det att resurserna inte är bundna till specifika platser, då användare ej har insikt eller kontroll över någon exakt lokalisering av de tillhandahållna resurserna (Mell & Grance, 2011).

2.1.1 Software as a Service

Software as a Service (SaaS), är en av tre servicemodeller som existerar inom cloud computing; de andra två modellerna är *Platform as a Service* (PaaS) och *Infrastructure as a Service* (IaaS). Av de tre så är SaaS det översta eller yttersta lagret. Inom SaaS kan användare få tillgång till leverantörers applikationer via sin egna apparatur och använda sig av tjänsten via ett interface, utan att behöva hantera den underliggande infrastrukturen. Användare behöver därmed inte oroa sig för operativsystem, lagring, CPU typer eller några andra resurser som krävs för att driva applikationerna som de använder (Amara, Zhiqui & Ali, 2017). Samtidigt kan SaaS-leverantörer rulla ut nya versioner eller uppdatera applikationerna utan att ta hänsyn till några andra distributionsmodeller eller samarbete med kunden. Kunder kan enkelt faktureras enligt en prenumerationsmodell (Segahl & Bhatt, 2018). Exempel på SaaS-applikationer är Google Docs, Rackspace och Salesforce (Amara et al., 2017).

2.2 Informationssäkerhet inom cloud computing

Informationssäkerhet i teorin har funnits sedan en lång tid tillbaka. Redan under Julius Caesars tid chiffrerades meddelande för att skydda information (Rao & Nayak, 2014). I samma anda byggdes Enigma under andra världskriget. När CIA-triaden skapades var informationssäkerhet således inte ett nytt fenomen. Målet med denna modell var istället att kartlägga faktorerna sekretess (konfidentialitet), integritet och tillgänglighet. Genom att förhålla sig till CIA-triadens tre faktorer kan beslutsfattare stärka informationssäkerhet (Samonas & Coss, 2014).



Figur 2. CIA-triaden (Rouse, 2014).

Som en förlängning av CIA-triaden skapades sedan Parkers Hexad (se figur 3 nedan), vilket breddar begreppet informationssäkerhet ytterligare. Parker adderar användbarhet, kontroll och autenticitet. Attributet kontroll syftar till den fysiska kontroll över data som genereras (Parker, 2012).

Figur 3. Parkers hexad (du Toit, 2018).

2.2.1 Sekretess

Syftet med sekretess är enligt Andress (2014), att skydda information från de som inte har befogenhet att ta del av den. Detta avsnitt är därme avsett för att behandla dataintrång och möjliga åtgärder. Dataintrång är en risk som medförs vid användning av SaaS-applikationer där en illvillig eller obehörig person bryter sig in i nätverket och får tillgång till känslig eller konfidentiell information (Kumar & Goyal, 2019). Skadan som orsakas av dataintrång beror på hur känslig den information är som blir utsatt (Kumar & Goyal, 2019). Intrång kan orsakas av en rad olika anledningar som otillräcklig verifiering eller autentiseringsmekanismer, granskingskontoller, brister i operationssystem, opålitlig användning av kryptering eller osäkrade API (Amara et al., 2017). Större leverantörer har upplevt problematik med dataintrång, med Microsoft, Google, Yahoo och Apple bland de drabbade (Amara et al., 2017).

Kapning är en form av intrång som sker när någon obehörig stjäler eller på annat vis får tillgång till inloggningsuppgifter till en cloud applikation eller tjänst (Tirumala, Sathu & Naidu, 2015). Vid kapning används konton som en plattform för att utföra attacker som att avlyssna användares verksamheter (Tirumala et al., 2015). Där kan kapare övervaka transaktioner, sprida falsk information, manipulera data, eller omdirigera användare till skadliga sidor (Tirumala et al., 2015). Utöver skada som sker direkt för användarnas verksamhet så kan det även orsaka rättsliga påföljder för både konsument och leverantör (Tirumala et al., 2015). En stor svaghet inom cloud computing som kan leda till kapning är bristfälliga autentiseringsmekanismer, vilket både kan orsakas och åtgärdas av användare (Grobauer, Walloschek & Stocker, 2011). Konton kan bli känsliga för kapning på grund av att användare väljer svaga lösenord eller användarnamn eller använder samma till flera tjänster (Grobauer et al., 2011). Enstegsautentisering anses även vara svagt i sig själv och ett annat sätt att undvika kapning är tvåstegsautentisering, vilket kan förhindra eller komplicera intrång trots att obehöriga har tillgång till inloggningsuppgifter (Prakash & Dasgupta, 2016).

Illvilliga medlemmar av en organisation eller ett företag kan utgöra en risk då de förutsättningsvis har tillgång till konfidentiell information (Kandias, Virvilis & Gritzalis, 2013). Då kan de orsaka skada utan att behöva bryta sig in i systemet. De har möjlighet att orsaka skada på konfidentiell data eller tillgångar och skada varumärkets image (Prakash & Dasgubta, 2016). Genom att maskera sin aktivitet som auktoriserad så kan de även sänka

produktivitet och orsaka finansiella förluster (Kandias et al., 2013). Kandias et al. (2013) menar att det inom cloud computing tillkommer en risk att det kan finnas illvilliga medlemmar inom leverantörs organisation. Ur en användares perspektiv förekommer det samtidigt sällan någon direkt kontakt eller exponering för leverantörens personal som hanterar applikationen och kan ha tillgång till respektive data (Winkler & Meine, 2011). Trots att konsumenten ofta inte har något direkt inflytande eller kontroll över denna personal så är de beroende av dem (Winkler & Meine, 2011). Vid val av leverantör kan det därför vara viktigt att granska vem som kommer ha tillgång till eller hantera datan inom leverantörens organisation. Winkler och Meine (2011) menar även att det är värt att begrunda bland annat bakgrundskontroller, krav på erfarenhet och meriter för anställda.

Kryptering av data är ett ytterligare sätt att motverka riskerna av dataintrång. Genom att kryptera datan som lagras menar Barona och Mary Anita (2017) att användare delvis kan skydda sig när det skett eventuellt intrång. Genom till exempel homomorphic encryption så tillhandahålls en mekanism för att utföra en specifik typ av beräkningar på chiffrerad text som inte möjliggörs med något annat krypteringsschema (Barona & Mary Anita, 2017). På så sätt har konsumenten möjlighet att lagra data i molnet i ett chiffertext-format. Med det kan alla nödvändiga beräkningar ske utan behovet av att dekryptera datan. På så sätt finns ett extra lager skydd för känslig information även om det skulle ske intrång (Barona & Mary Anita, 2017).

2.2.2 Tillgänglighet

Tillgänglighet är ett säkerhetsattribut som syftar till hur ofta ett system eller en komponent är tillgängligt när det behöver användas. Enligt CIA-triaden kan förlust av tillgänglighet bero på flera olika saker, såsom strömförlust eller felaktigheter i operativsystem (Andress, 2014). Chaczka, Mahadevan, Aslanzadeh och McDermid (2011) skriver vidare att tillgänglighet är en av de främsta svårigheterna med cloud computing. Fortsatt skriver de att tillgänglighet bör mätas i längd mellan problem samt tiden det tar att åtgärda dessa problem. Manuel (2013) visar med hjälp av IEEE (Institute of Electrical and Electronics Engineers) att man kan mäta förlust av tillgänglighet hos sin leverantör. Den totala nedtiden mäts genom att ta tiden från den tidpunkt felet upptäcks och sedan räkna till och med tiden det tar att reparera felet. Förlust av tillgänglighet definieras som;

"*1. A part of service of the resource is denied to the user. 2. The resource is shut down. 3. The resource is too busy to process the job request.*" (IEEE 90 1990).

Även Benlian och Hess (2011) hänvisar till detta som en säkerhetsrisk inom cloud computing. De hänvisar till förlust av tillgänglighet som en prestationsrisk i sin studie. Där belyser de även riskerna relaterade till SaaS-applikationers interoperabilitet. Sammantaget finner flera författare att förlust av tillgänglighet leder till organisatorisk ineffektivitet (Benlian & Hess, 2011; Manuel, 2013; Chaczka et al, 2011). Författarna menar att det är särskilt kritiskt med tillgänglighet ifall SaaS applikationen används i anslutning till en kundorienterad verksamhetsprocess (Benlian & Hess, 2011).

Ett sätt att reglera tillgänglighet är genom upprättande av ett service-level agreement, vilket är ett juridiskt bindande dokument som specificerar hur tjänster ska levereras, samt hur eventuella serviceavgifter ser ut (Alhamad, Dillon & Chang, 2010). Vidare skriver Alhamad et al (2010) att huvudkraven i ett SLA bör vara:

1. Beskriva tjänsten på ett sätt så att konsumenten enkelt kan förstår hur den fungerar.
2. Presentera den tänkta nivån av service.
3. Definiera hur serviceparametrarna kan övervakas samt redovisa hur dessa rapporter ser ut.
4. Definiera hur eventuella påföljder ser ut ifall servicekrav inte möts.
5. Specifikationer kring fakturering, samt hur tjänsten kan avslutas och eventuella påföljder.

Även Takabi, Joshi och Ahn (2010) skriver att ett SLA är nödvändigt för att definiera nivå av service hos leverantören, men även för att ta del av garantier och säkerheter som erbjuds. En vanlig företeelse inom SaaS-applikationer är standardiserade SLA-avtal som ger undermåligt skydd ur en säkerhetsaspekt (Duncan & Whittington, 2016; Lins, Grochol, Schneider & Sunyaev, 2016). Lins et al. (2016) hävdar vidare att beslutsfattare inte ska avskräckas från SaaS-applikationer på grund av denna standardisering, men att verifiering av SLA-avtalet bör genomföras.

2.2.3 Kontroll

Enligt Andress (2014) är kontroll den del av Parkers Hexad som syftar till fysisk dataförlust. Dataförlust eller en potentiell oförmåga att kunna förhindra dataförlust är en uttalad risk inom cloud computing (Prakash & Dasgubpta, 2016). Samtidigt skriver Lee (2012) att dataförlust, likt dataintrång även kan ske på grund av illsinta attacker mot nätverket så finns det en mångfald av andra möjliga orsaker. Data kan skadas eller påverkas av modifikationer, radering, eller förlust av krypteringsnycklar (Lee, 2012). Utomstående förhållanden kan också ha oönskad påverkan, såsom jordbävningar, eldsvådor och översvämningar som skadar fysisk infrastruktur (Amara et al., 2017). På grund av hotens opålitliga natur så bör företag ha ett övergripande system för producering och lagring av backup av sin data (Amara et al., 2017). För att gardera sin verksamhet är det rekommenderat att skapa en plan för hur man återfår data eller tillgång till data vid en eventuell kris eller förlust (Liu, 2012). Utöver att en leverantör kan utsättas för kriser och ligga nere, så kan de även gå i konkurs eller på annat vis stängas ner permanent (Winkler & Meine, 2011). Företag av all kapacitet är sårbara för dataförlust, men mindre företag anses vara under större risk då de ofta har mindre tillgång till eller resurser för expertis (Winkler & Meine, 2011).

Gandhi och Gandhi (2019) hävdar vidare att brist på transparens angående belägenheten av lagrad data också utgör ett hot. På grund av att data kan lagras utspritt i olika datacenter så finns möjligheten att användare tappar översikten om var deras lagras (Gandhi & Gandhi, 2019). Om datan lagras i olika länder eller områden så kan de juridiska regelverken och kraven för informationssäkerhet variera (Gandhi & Gandhi, 2019). Om ett datacenter dessutom lagrar fullständig data så har den fysiska platsen en direkt koppling till datasäkerhet, och ovisshet om var det är utgör således ökad risk för användare (Gandhi & Gandhi, 2019).

Ett annat fenomen när man ser till minskad kontroll är lock-ins. Lock in är en risk som utgörs av att användare förlorar sin kontroll eller frihet till att byta från en molntjänst till en annan (Amara et al., 2017). Problemet kan uppstå för att leverantörer har utvecklat sina produkter eller system med specifik teknologi. Då kan det ofta saknas tillräcklig interoperabilitet för att användare lätt ska kunna migrera sin data till ett annat system (Opara-Martins, Sahandi & Tian, 2014). En typisk barriär för användare blir höga kostnader som uppstår vid ett skifte mellan två inkompatibla system (Opara-Martins et al., 2014). Lock-in blir speciellt skadligt i

fall då användare har byggt upp en hög nivå av beroende av tjänsten. Används det till exempel till en nyckelfunktion inom verksamheten eller till den primära rapporteringen av verksamhetens status, så orsakar det stor skada om data blir låst (Winkler & Meine, 2011). Risken är inte heller isolerad till situationer där konsumenten vill byta, utan ökar även sårbarheten i fall leverantören går i konkurs eller på annat vis lägger ner (Winkler & Meine, 2011). Då blir det återigen relevant att ha en plan eller att system för att inte bara få tillgång till backups, men även överföra data till en ny leverantör (Winkler & Meine, 2011). En annan fråga som bör ställas är vad som sker med en konsuments data som är kvar hos en leverantör, och vem som kommer kunna ha tillgång till den (Chen & Zhao, 2012). Gammal data som inte längre används eller ligger hos en tidigare leverantör kan riskera att känslig information blir utsatt (Chen & Zhao, 2012). Chen och Zhao (2012) menar att användare bör uppmuntras att tillse garanti på radering av sin data från leverantörens system.

2.3 Förtroende inom cloud computing

Litteraturen nämner en annan faktor som behöver beaktas i diskussionen om informationssäkerhet relaterat till cloud computing. Manuel (2013) menar att *förtroende* är en av de största svårigheterna inom cloud computing. Grandison och Sloman (2000) definierar förtroende enligt följande: "*The firm belief in the capability of an entity to act consistently, securely and reliably within a specified context*". Samtidigt definierar Evans och Kreuger (2011) förtroende: "*A psychological state comprising the intention to accept vulnerability based upon the positive expectations of the intentions or behavior of another*". Vidare säger de att förtroende är en samling av faktorer såsom reliabilitet, ärlighet, trovärdighet, säkerhet, pålitlighet, kompetens, QoS (Quality of Service) samt avkastning (Grandison & Sloman, 2000). Servicekvalitet och dess påverkan på användare har behandlats av flera författare. Chou och Chiang (2013) menar att ökat förtroende för leverantörer reducerar oro kring integritetsfrågor. Vidare finner Wu, Lan och Lee (2011) att förtroende är resultatet av upplevda fördelar i förhållande till upplevd risk.

2.4 Litteratursammanfattning

Utifrån befintlig litteratur framlagt i detta kapitel har författarna valt att arbeta fram en tabell som sammanfattar den litteratur som använts och som ligger till grund för det empiriska arbetet som ska genomföras. Tabellen kommer att delas in i delområde, säkerhetsfaktorer inom delområde och författare som behandlat dessa delområde i tidigare litteratur.

Tabell 1 - Sammanfattning över litteratur som ligger till grund för empirisk undersökning

Delområde	Säkerhetsfaktorer	Författare
Sekretess	• Dataintrång • Kapning • Illvilliga medlemmar • Autentisering • Kryptering	(Amara, Zhiqui & Ali, 2017) (Kumar & Goyal, 2019) (Prakash & Dasgupta, 2016) (Grobauer, Walloschek & Stocker, 2011) (Winkler & Meine, 2011)

		(Barona & Mary-Anita, 2017) (Tirumala, Sathu & Naidu, 2015) (Kandias, Virvilis & Gritzalis, 2013)
Tillgänglighet	• Förlust av tillgänglighet • Mätning av tillgänglighet • Reglering med SLA	(Andress, 2014) (Chaczka, Mahadevan, Aslanzadeh & McDermid, 2011) (Manuel, 2013) (IEEE, 1990) (Benlian & Hess, 2011) (Alhamad, Dillon & Chang, 2010) (Takabi, Joshi & Ahn, 2010) (Duncan & Whittington, 2016) (Lins, Grochol, Schneider & Sunyaev, 2016)
Kontroll	• Dataförlust • Lock-ins • Lokalisering av data	(Andress, 2014) (Prakash & Dasgubpta, 2016) (Amara, Zhiqui & Ali, 2017) (Opara-Martins, Sahandi & Tian, 2014) (Winkler & Meine, 2011)
Förtroende	• Förtroende en svårighet • Upplevda fördelar ställs mot upplevda risker	(Manuel, 2013) (Grandison & Sloman, 2000) (Evans & Kreuger, 2011) (Chou & Chiang, 2013) (Wu, Lan & Lee, 2011)

3 Metod

Arbetet inleddes med att identifiera ett ämne inom cloud computing som kunde avgränsas tillräckligt mycket med hänsyn till kursens omfång. En utförlig litteraturstudie ledde till att författarna identifierade SaaS som ett passande forskningsområde inom cloud computing. Genom att koppla SaaS till informationssäkerhet kände författarna att man funnit ett område som skulle passa omfånget, och samtidigt understödja forskningen inom detta område. Efter noggrann utvärdering valde författarna att anta den kvalitativa metoden i form av semistrukturerade intervjuer. Denna metod samlar in data i form av ord, och är mer djupgående och detaljerad än den kvantitativa (Jacobsen, 2002). Vidare menar Jacobsen (2002) att genom att anta ett mindre urval kan författarna fokusera mer på helheten och således utvinna maximalt med information från informanterna. En annan fördel med de semistrukturerade intervjuerna är att man får ta del av intervjuobjektens egna berättelser och upplevelser, vilket Denscombe (2009) menar är hela essensen med den kvalitativa metoden.

3.1 Datainsamling

Vid sökning efter sekundärdata användes vetenskapliga databaser såsom LUBsearch som Lunds Universitet tillhandahåller, samt Google Scholar som innehåller akademiska artiklar från diverse journaler. Några av sökorden som användes var “Software as a Service”, “SaaS Security Risks”, “Information Security in Cloud” etc. Sökorden har använts både på svenska och engelska.

3.1.1 Semistrukturerade intervjuer

Primärdata samlades in genom fem semistrukturerade intervjuer med beslutsfattare som arbetar med SaaS-applikationer i sin affärsverksamhet. Inför intervjuerna skapades en intervjuguide för att säkerställa att intervjuerna gjordes på ett likartat sätt, vilket Jacobsen (2002) menar är en bra teknik. Vi använde oss av den skapade litteratursammanfattning när intervjuguiden skapades för att säkerställa att informationen från intervjuerna skulle svara på den formulerade frågeställningen, samt att empirin skulle spegla litteraturen (Jacobsen, 2002).

3.1.2 Intervjuguidens utformning

Tabell 2 - Intervjuguidens utformning

Typ av frågor	**Frågornas utformning**	**Motivering till frågorna**
Inledande frågor	• Vilken eller vilka SaaS applikationer använder ni idag? • Vilka skulle du bedöma är de viktigaste orsakerna bakom	En inledande fråga för att reda ut ifall beslutsfattaren använder sig av SaaS i affärsverksamheten samt en fråga som utreder vilka de viktigaste orsakerna var bakom förvärvet.

	förvärvet av dessa SaaS applikationer?	
Fördelar och risker med SaaS	• Vilka skulle du bedöma är de största fördelarna med er SaaS applikation? • Vad upplever ni som den främsta risken vid användning av er SaaS applikation?	Genom att ställa dessa frågor ville vi skapa en bild av deltagarnas attityd till SaaS applikationer. När de själv får reflektera innan vi ställer mer specifika frågor skapar vi oss bild av vad de anser viktigt.
Fördjupande frågor		
Sekretess	• Användandet av SaaS applikationer kan leda till ökad risk för obehörig åtkomst av företagets data. Påverkade detta faktum er vid valet av en SaaS applikation? • Vet ni vem som har tillgång till er lagrade data? • Vad har ni för typ av autentisering för att få tillgång till er SaaS applikation? • Har ni någon insikt eller inflytande på nivå av kryptering av datan?	Baserat på den litteraturgenomgång som genomförts har frågor relaterade till delområdet sekretess skapats.
Tillgänglighet	• Mäter ni kontinuerligt SaaS applikationens tillgänglighet? • Hur bedömer ni att den operativa verksamheten skulle påverkas av driftstopp i SaaS applikationen? • Har ni skrivit någon form av serviceavtal med SaaS leverantören som reglerar kvalitetssäkring av	Baserat på den litteraturgenomgång som genomförts har frågor relaterade till delområdet tillgänglighet skapats.

	leveransen? Är ni nöjda med detta?	
Kontroll	• Finns det en plan för datahantering ifall SaaS applikationen sägs upp? • Har ni tillgång till en backup av den data som produceras? • Har ni möjlighet att garantera radering av data från SaaS leverantörens databaser? • Vet ni i vilket land er data lagras?	Baserat på den litteraturgenomgång som genomförts har frågor relaterade till delområdet kontroll skapats.

3.1.3 Intervjuernas genomförande

Vid ett tidigt stadium i undersökningen bestämde vi oss för att genomföra intervjuerna över telefon. Detta eftersom den uppskattade tidsåtgången inte var speciellt lång, men även för att det skulle underlätta för deltagarna (Jacobsen, 2002). Inför intervjuerna med de olika deltagarna säkerställdes ett etiskt korrekt tillvägagångssätt (se avsnitt 3.5) genom informerat samtycke samt utskick av skapad intervjuguide. Under intervjuernas gång lades fokus på deltagarna. De skulle få tala oavbrutet medan vi passivt lyssnade och ställde eventuella följdfrågor för att reda ut oklarheter. Vi informerade att samtalen spelades in för att undvika att anteckna under intervjun. Genom detta tillvägagångssätt kan vi gå tillbaka och analysera data obehindrat (Jacobsen, 2002). Framförallt har exakta citat och uttryck varit av stort värde vid analys.

3.2 Urvalsprocess

Urvalet påverkades av att vi behövde komma i kontakt med beslutsfattare i näringslivet, vilket framgår av vår frågeställning. Som beslutsfattare söktes personer som har direkt kontroll över användning av SaaS i en verksamheten. Storleken på beslutsfattarnas respektive företag var inte relevant för undersökning. Däremot ska det sägas att i vår strävan efter att finna personer med en beslutsfattande kapacitet limiterades urvalet naturligt till småföretag (se avsnitt 1.5 för avgränsningar).

Tabell 3 - Översikt av urval

Beslutsfattare	**Befattning inom företag**	**Typ av företag**	**Datum**	**Typ av intervju**
Informant 1	Ägare	Restaurang- och livsmedelsförsäljning	10/10-19	Telefonintervju

Informant 2	Ägare	Försäljning av produkter till grönytor	09/10-19	Telefonintervju
Informant 3	Ägare	Agentur inom nöjesbranschen	29/10-19	Telefonintervju
Informant 4	Delägare	E-handel med inriktning på kläder	11/10-19	Telefonintervju
Informant 5	Delägare	Reservdelsförsäljning inom industri	08/10-19	Telefonintervju

3.3 Dataanalys

Ett första stadium i bearbetning av datan var transkribering, som gjordes en och en i en avskild, lugn miljö för att undvika fel. Den transkriberade texten tar inte hänsyn till upprepade ord och dylikt eftersom Jacobsen (2002) menar att dessa texter kan bli längre än nödvändigt. Deltagarnas namn uppges inte vid namn i transkriberingen, delvis för deltagarnas egna sekretess, men även för att vi upplevde att denna avidentifiering säkerställde en objektiv analys av datan (Denscombe, 2009).

Efter transkriberingen startades tidigt en kategorisering av resultatet från intervjuerna. Kategorisering gjordes samtidigt fast på olika platser för att kunna utnyttja olikheter i kategorisering till diskussionsavsnittet (Jacobsen, 2002). Insamlad data lästes igenom i sin helhet och kopplades till de olika delområden som iden§tifierats. Vid avslutad kategorisering fick vi en tydlig och överskådlig bild av hur medvetenhet såg ut kring de utvalda delområdena. För att visualisera detta skapades flera tabeller där relevant utdrag från transkribering redovisades.

3.4 Validitet och reliabilitet

Validitet (giltighet) och reliabilitet (tillförlitlighet) kommer från den kvantitativa metodiken, men artar sig något annorlunda i ett kvalitativt syfte. Enligt Jacobsen (2002) har anhängare till den kvalitativa metoden kritiserat de båda begreppen, och menar att de inte hör hemma inom de kvalitativa studierna.

Ser man till validitet så handlar det om författarnas förmåga att undersöka vad som ursprungligen avses. Med andra ord kan man ställa sig frågan ifall man lyckats mäta det som varit avsett att mäta (Jacobsen, 2002). Vidare menar Jacobsen (2002) att man kan börja med att kontrollera intern validitet. Detta gör författarna genom att ställa problemställning och slutsatser mot varandra. Frågan som bör ställas är: Har slutsatsen besvarat den fråga som formulerats i inledningen av studien (Jacobsen, 2002)? Vidare menar han att man bör genomföra en kritisk granskning av sitt resultat för att utesluta eventuella misstag i hanteringen. Som yttre validitet ska man istället bedöma huruvida resultat och slutsatser är överförbara till andra likvärdiga situationer, alltså om resultatet går att generalisera (Jacobsen, 2002).

När man undersöker reliabilitet så ligger emfas på huruvida resultatet i undersökningen kan komma att påverkas av metodvalet (Jacobsen, 2002). Likaså måste man ta ställning till ifall utfallet skulle bli det samma ifall studien gjordes igen.

3.5 Etik

Inför intervjuerna identifierade vi de etiska principer som man bör tänka på vid kvalitativa undersökningar. En av de främsta principerna är att man informerar deltagarna om frivillighet. Ett informerat samtycke är viktigt att understryka, både innan, under och efter intervjun (Jacobsen, 2002). Genom att tydligt klargöra syftet med intervjun samt skicka iväg frågorna i förväg med en kort introduktion av SaaS kunde deltagarna skapa sig en bild av hur intervjun skulle gå till. Detta gav samtliga deltagare möjligheten att själv avgöra huruvida de ville delta eller inte (Jacobsen, 2002).

En annan viktigt aspekt enligt Jacobsen (2002) vid kvalitativa undersökningar är att koncist återge resultatet vid avslutad intervju, för att säkerställa att inga missförstånd uppstått under samtalets gång. Efter genomförd transkribering skickades den i sin helhet till informanter som fick godkänna utkomsten av intervjun. Vi informerade även om att uppsatsen i sin helhet kan skickas till deltagarna när uppsatsen skrivits klart.

4 Resultat

I denna del redovisas det empiriska material som samlats in. Kapitlet delas upp i de olika delområde som intervjuguiden skapats utifrån. Utifrån skapade tabeller ämnar vi att skänka god struktur och överskådlighet i empirin som samlats in.

4.1 Inledande frågor

I tabell 3 presenteras svar på de inledande frågorna. Dessa frågor svarar på vilka SaaS-applikationer som används av informanterna samt motiven bakom varför de förvärvats. Genom att ställa dessa frågor kan vi säkerställa att informanterna de facto använder sig av SaaS-applikationer.

Tabell 3 - Resultatdel inledande frågor

Beslutsfattare	**Vilken eller vilka SaaS applikationer använder ni idag?**	**Vilka skulle du bedöma är de viktigaste orsakerna bakom förvärvet av dessa SaaS applikationer?**
Informant 1	Molnlösning som laddar upp dokument och filer till ett moln varje kväll Timecheck vid in- och utcheckning samt löner Kassorna ansluta till molnet via timecheck	Datorn har kraschat innan, alltså den jag använder då, och det var ett helvete. Vi tappade ju hur mycket av vår data och information som helst, allt ligger ju där i princip.
Informant 2	OneDrive Fortnox	Valet grundar sig till stor del i tradition, och vi sedan länge arbetat med företagen. När jag köpte upp företaget så var båda tjänsterna redan i bruk, och jag har fortsatt med dem sedan dess. Just Microsoft som gör OneDrive har vårt företag arbetat med sedan 20-25 år tillbaka.
Informant 3	Microsoft 365 Google Mail	Jag använder mig av tjänsterna för jag tycker det är smidigt att ha allting samlat på ett ställe men också att jag smidigt kan komma åt mail osv oavsett om jag är på mobilen eller datorn. Användarvänligheten i form av tillgänglighet är helt enkelt bättre än andra alternativ.
Informant 4	Google Mail Google Ads	Smidigheten att kunna dela jobb och redigera det direkt och ha det ute på internet är väl den främsta anledning skulle jag säga. Att veta att

	Microsoft 365	man har det liggandes utan att behöva klydda med en massa överföringar och så vidare.
Informant 5	Tele2 E-mail	Det var en prisfråga, vi använde oss redan av telefonin genom Tele2 och sen hade vi en form av konsult i samband med inköp av datorer som rekommenderade att vi tog vår email via dem också. Då hade vi som sagt möjlighet att få e-mail också till ett bra pris, och Tele2 kändes som en stabil leverantör också, ingen som skulle försvinna eller gå in konkurs de närmsta åren i alla fall.

4.2 Fördelar och risker med SaaS

I tabell 4 ställs frågor kring fördelar och nackdelar med SaaS-applikationer. Genom att ställa dessa frågor ville vi skapa en bild av deltagarnas attityd till SaaS applikationer utan påverkan från oss. När de själv får reflektera innan vi ställer mer specifika frågor skapar vi oss därför en bra bild av vad de anser viktigt.

Tabell 4 - Resultatdel fördelar och risker med SaaS

Beslutsfattare	Vilka skulle du bedöma är de största fördelarna med er SaaS applikation?	Vad upplever ni som den främsta risken vid användning av er SaaS applikation?
Informant 1	Ja det är att inte behöva oroa sig för det själv, eller oroa sig för att tappa sina uppgifter. Nu är det ett proffs som tar hand om det istället för att jag som inte är så kunnig när det kommer till datorer ska hålla på. Man glömmer ju lätt att göra backup själv och även om man inte gör det så är det väl någon gång i månaden som det sker. Där hinner hända jävligt mycket mellan de tillfällena och där är massor av uppgifter som man kan gå förlorade. Nu laddar ju den upp alla mina filer till molnet varje natt istället.	Har inga super-hemligheter som vi lagrar i molnet, eller som de här tjänsterna behandlar. I dagsläget känns det som det finns så många risker så man kan ju aldrig vara helt säker på att man inte kommer bli hackad eller att där blir intrång. Men jag känner ju att det är en större risk för oss om vi tappar tillgång till uppgifterna, så att vi till exempel tappar kollen på löner och semesterdagar och så vidare. Det är sånt som bara måste fungera.
Informant 2	Det handlar främst om tillgång till support. Vår verksamhet är inte fokuserad på IT och det är inte där vår expertis ligger. Vi har störst behov av någon som inte bara bidrar med en produkt utan också kan komma med rådgivning och drift som ett helhetspaket. Jag vill ha möjlighet att lagra mina dokument i molnet så att jag har tillgång till dem oavsett var jag är men de tekniska detaljerna som ligger bakom det är inte något jag vill oroa mig för att driva.	Det är om det sker någon form av avbrott från kontakten med tjänsterna så att de inte går att använda. Så som jag ser det så är det den största risken för företaget för då tappar vi tillgång till den information och data som vi är arbetar med och är beroende av för vår verksamhet. Om jag inte får tillgång till de dokument som är uppladdade alltså, eller inte har tillgång min bokföring eller möjlighet att ta betalt kunder eller andra administrativa behov. Jag ser nog det som en mer sannolik risk än dataintrång och att någon utomstående ska försöka få tillgång till de uppgifter som hanteras i tjänsterna.
Informant 3	Det måste vara att jag alltid kan komma åt information som jag har sparat vart jag än befinner	Det skulle vara om jag till exempel tappade bort min telefon och någon lyckades komma åt information som

	mig. Alltså via mobilen eller laptop.	inte berör utomstående. Det hade jag nog tyckt vara jobbigast.
Informant 4	Hänger väl ihop lite med föregående fråga, alltså smidigheten och att slippa skicka över massa filer via mail är väl de främsta fördelarna. Arbetet förenklas otroligt när man kan dela filer och så vidare som man arbetat med på ett så enkelt sätt.	När man inte är insatt så vet man ju inte riktigt, behöver man egentligen ytterligare backup? Tänk om det händer något med filerna man lagrar i tjänsten? Rädslan för att filer ska försvinna är väl det första jag tänker på. Till exempel insåg vi häromdagen att ett dokument vi satt och arbetade i där länken var åtkomlig för alla, detta var ju väldigt oroväckande, någonting vi inte alls hade tänkt på. Det skulle jag vilja ändra på. Det borde ju vara default att med stänga dokument för allmänheten, för att sedan öppnas ifall vi önskar det.
Informant 5	Det är lite svårt att säga, vi använder det bara till mejl. Det jag skulle säga ät att det är en fördel att ha någon man kan kontakta om det går fel, som kan hjälpa till och även har något sorts ansvar. Tele2 är ju ett känt företag för oss, och de har en helt annan expertis än vad vi har inom IT och det digitala.	En stor risk som jag ser är att Tele2 har utvecklats ifrån den här typen av tjänst och inte riktigt bryr sig om den längre. Handläggningen kan ta väldigt långt tid, de har knappt några som sitter och jobbar med det längre. Det är en väldigt liten avdelning, om man ens kan kalla det så. Det känns som det har blivit svårare att få tag på dem när jag upplever ett problem, eller behöver hjälp. Eftersom de verkar dedicera mindre resurser kanske det tar längre tid för dem att identifiera problem eller få kontakt med mig om något skulle ske på deras sida också. Nu när jag betalar så lågt pris som jag gör så upplever jag att de nästan är lite ovilliga att hjälpa till. Det ligger ofta på mig att bevisa att det inte ligger något fel hos mig, med min dator eller nätet här och det kan vara svårt att få fram data jag tappat tillgång till. Sen i ett generellt perspektiv med en sådan här tjänst så är väl den största oron vad som skulle hända med ens uppgifter eller data om leverantören går i konkurs eller tjänsten på annat vis upphör. Ja jag har nog klagat några gånger, men det känns inte som där finns så mycket

		att göra. Nu har ju det så billigt tillsammans med min telefoni och så men det är inte omöjligt att jag byter här någon gång snart om jag hittar ett bra erbjudande

De upplevda fördelarna med att använda SaaS-applikationer till sin verksamhet har bland informanterna i denna undersökning varit centrerade runt tillgänglighet och tillgång till support eller högre expertis inom IT och mjukvara. Riskerna är främst fokuserade på dataförlust eller tillgänglighet. I3 uppger även att intrång i känslig data upplevs som den primära risken. I1 erkänner att där finns en risk för dataintrång som aldrig helt kan undkomma, men anser inte att det är en primär risk i dess egna användning.

4.3 Sekretess

I tabell 5 inleds delområdet med frågor relaterade till sekretess. Dessa frågor behandlar det faktum att användning av SaaS-applikationer kan leda till obehörig åtkomst av användarens data, samt vem som har tillgång till data i en SaaS-applikation.

Tabell 5 - Resultatdel Sekretess 1.0

Beslutsfattare	**Användandet av SaaS applikationer kan leda till ökad risk för obehörig åtkomst av företagets data. Påverkade detta faktum er vid valet av en SaaS applikation?**	**Vet ni vem som har tillgång till er lagrade data?**
Informant 1	Nej det skulle jag inte säga. Det blev intrång på vår dator när vi bara hade allt på hårddisken också, så jag tycker ju molnet är bättre. Överlag så låg valet mest i att det blev smidigare för oss med de här tjänsterna och att allt inte står still om någon av hårdvaran skulle gå åt.	Ja de som är vår handläggare hos de vi anlitar kan ju gå in och se. De kan logga in och använda systemet från sin sida, det är ju så vi får support ifall någonting skiter sig. Som sagt så känner inte jag att det är någonting superhemligt som vi har lagrat.
Informant 2	Ja. Vi använder oss av företag som vi har ett förtroende för ju. De är stora företag som vi anser har ett kapital av förtroende och historiskt välfungerande produkter. Under tiden vi har arbetat med dem så har det inte uppstått några större problem.	Ja företaget som vi anlitar har också tillgång till datan och har en fysisk backup som de producerar, ifall det skulle uppstå problem med molnet.

Informant 3	Nja, eftersom jag är en liten enskild firma har jag inte tänkt så mycket på det. Litar på att leverantören håller min data säker.	Man blir lite skrämd när man får denna fråga men även här har jag ingen aning om vem som har tillgång till min data.
Informant 4	Nja inte direkt, det är Google liksom. Det känns stort och pålitligt. Behöver inte tänka så mycket över det. Inte påverkat valet varken positivt eller negativt. Men nu när du ställer frågan så börjar man väl tänka lite på vem som kan ta del av datan.	Nej ingen aning om det. Obehagligt att resonera kring, tänk om de säljs till tredje part? Man förlitar sig så himla mycket på Google som leverantör. De har funnits med och varit störst ett tag nu. Det känns som att datan existerar på ett tryggt ställe.
Informant 5	Nej jag valde mest baserat på att det var ett namn vi kände till och att vi då fick ett bra pris i samband med telefonin. Vi hade också en viss tillit till Tele2 eftersom de var väldigt stora inom detta på den tiden då vi först tecknade tjänsten. Det har ju ändrats lite nu, och det finns många fler företag som är mer specialiserade. Sen vet jag inte, det här med integritet av datan och så har inte varit någon större oro. I mina mejl så känner jag inte att det finns så mycket att dölja. Det är som jag nämnde innan, det viktigaste var för mig att välja något som skulle leva ett långt tag till.	Nej det vet jag inte säkert. Jag fattar det som att de inte har tillgång hur som helst i alla fall. Sist jag hade problem så hade jag överbelastat min kapacitet, eller överskridit den snarare, på servern. Då fick jag göra mycket själv, med hjälp av deras instruktioner för att de skulle kunna se vad som var fel, men sen blev det oklart för det verkade som de kunde komma in sen från sin sida. Det var i alla fall mycket fram och tillbaka mellan oss.

Svaren i tabell 5 visar att en ökad risk för dataintrång inte spelar någon större roll för samtliga informanter i deras val av SaaS-applikation. Fyra informanter uppger att där finns ett högt förtroende för leverantörer av deras SaaS-applikationer och därmed ingen upplevd risk. I1 uppger även att de anser SaaS-applikationer vara ett säkrare val. Två informanter svarade med säkerhet att deras leverantörer också hade tillgång till den data som lagras men gick inte in i detalj på vem hos leverantören som hade åtkomst. I5 var osäker på hur det fungerade men antog att dess leverantör hade tillgång, samtidigt som I3 och I4 uppgav att de inte visste alls.

I tabell 6 fortsätter frågor relaterade till delområdet sekretess. Dessa frågor behandlar datakryptering och reder ut vilken insikt eller inflytande informanter har. Sedan reder vi ut vilken typ av autentisering som används inom de olika applikationerna för att reda ut hur medvetenhet ser ut.

Tabell 6 - Resultatdel Sekretess 2.0

Beslutsfattare	**Har ni någon insikt eller inflytande på nivå av kryptering av datan?**	**Vad har ni för typ av autentisering för att få tillgång till er SaaS applikation?**

Informant 1	Nej. De bara tankar ner våra uppgifter och sen vet jag inte vad de gör med dem. Asså det är inte så viktigt för mig, jag tror det beror på vilken branch man är i och så.	Ja, asså jag har ju lösenord till var och en.
Informant 2	Nej det har vi inte i den bemärkelsen, vi kan bara kontrollera hur mycket av vår data som ska sparas i OneDrive till exempel.	Jag får ju logga in med ett lösenord om det är det du menar. Ja asså, det är kanske lite tabu att ha det så men jag försöker byta ganska ofta så då är det lättare om jag använder mig av samma till båda tjänsterna eller programmen.
Informant 3	Nej inte vad jag vet. Detta har ju aldrig tänkt på.	Asså mitt lösenord? Jag har faktiskt samma lösenord till min Google Mail som jag har till mycket annat.
Informant 4	Det vet jag inte. Svår fråga för en någon som mig som inte sysslar direkt med sådant.	Jag har ett par lösenord som jag byter mellan. Arbetade tidigare på en arbetsplats där det krävdes att man bytte varannan månad eller så. Så jag har anammat detta sedan dess.
Informant 5	Nej det har vi inte. Jag vet inte om det känns så relevant för min typ av verksamhet, kanske är viktigare för de som är större.	Auktorisera och auktorisera, det är bara en mejl liksom. Jag har ett helt vanligt lösenord som jag tar mig in med.

Samtliga informanter har, som kan ses i Tabell 6, förmedlat att de inte har någon form av insikt eller inflytande på nivån av kryptering som används till data i SaaS-applikationerna de använder. Lösenord är även den enda formen av autentisering som informanterna i den här undersökningen har använt sig av. Användandet av lösenord skiljer sig däremot mellan informanter som använder samma lösenord till ett flertal SaaS-applikationer till informanter som kontinuerligt byter lösenord för att öka säkerheten.

4.4 Tillgänglighet

I tabell 7 övergår frågorna till delområdet för tillgänglighet. Här reder vi ut ifall informanterna kontinuerligt mäter applikationernas tillgänglighet, samt frågar hur den operativa verksamheten skulle påverkas vid ett eventuellt driftstopp i applikationen. Avslutningsvis inom detta området behandlas området för SLA-avtal. Vi reder ut ifall informanterna har skrivit serviceavtal och ifall de är nöjda med dessa avtal.

Tabell 7 - Resultatdel tillgänglighet

Beslutsfattare	Mäter ni kontinuerligt SaaS	Hur bedömer ni att den operativa	Har ni skrivit någon form av serviceavtal

	applikationens tillgänglighet?	**verksamheten skulle påverkas av driftstopp i SaaS applikationen?**	**med SaaS leverantören som reglerar kvalitetssäkring av leveransen? Är ni nöjda med detta?**
Informant 1	Nej. Vi har ju haft det i 1.5 år och det har aldrig varit otillgängligt. Man märker ju om det inte funkar, och skulle det ske ofta så hade man ju såklart tänkt om när det gäller valet av leverantör, men en än så länge har som sagt ingenting skett.	Det beror på vilken. Om kassorna inte fungerar så blir det ju kaos, då påverkas vi direkt eftersom vi inte kan ta betalt av kunderna. Men ja allt ligger ju molnet så det ställer ju såklart till förödelse om det inte skulle fungera. Jag gör ju egna backups då och då på det som ligger på min dator, men det är ju inte nära lika ofta som datan laddas upp i molnet.	Vi har ju skrivit på att de ska sköta det. Man märker ju om det skulle rasa, men det är klart man är ju ändå livrädd för att det ska sluta fungera.
Informant 2	Nej det gör vi inte, det har inte varit några problem än så länge så det har inte känts nödvändigt.	Det hade varit katastrofalt eftersom vi hade tappat tillgång till den datan vi använder oss av när vi arbetar. Speciellt om det är vår OneDrive, där filerna som vi använder varje dag är lagrade. Om jag kommer in på morgonen och det inte funkar, så får jag det väldigt svårt att utföra mitt jobb.	Nja, jag har skrivit på ett vanligt användaravtal. Nu kan jag det ju inte utantill, men visst jag är nöjd med det. Tjänsten gör det som jag behöver och vi har inte haft några problem än.
Informant 3	Nej det gör jag inte. Jag är inte så beroende av en ständigt uppkopplad tjänst med tanke på att jag är en enskild firma. Så lite down time här och där gör inte mig någonting. Självklart hade det	Som sagt med tanke på att jag är en liten enskild firma hade det påverkat mig men det hade inte varit hela världen för just min firma.	Nej det har jag inte. Såklart har jag godkänt de allmänna avtalen när jag förvärvade dessa tjänster, men det läser väl ingen.

	varit störigt att inte komma in i mailen när man behöver den, men det är inget jag märkt under mina år med Google Mail.		
Informant 4	Nej det gör vi inte. Känns inte värt det med tanke på hur lite som lagras av oss i nuläget. Hade vi sett problem så hade vi kollat på andra SaaS tjänster.	I dagsläget har vi backup, vi har kört över alla filer och kör endast drive nu. Däremot sedan vi gick över till Drive har vi slutat lagra backupfiler, och de finns alltså inte den externa hårddisken just nu. Det betyder ju att vi hade kunnat sitta där utan tillgång till viktiga avtal och fakturor när vi behövde dem. Ja det hade ju ställt till det massor. Klart vi hade kunnat skaka fram gamla kunduppgifter o så men det hade tagit tid och varit kostsamt.	Nej, det har vi inte gjort. Vi har inga jättetunga filer, och har inte tänkt så mycket. Alltså jag antar att sånt står i avtalet man godkänner, alltså licensavtalet. Jag har hittills inte upplevt några problem med kvalitet på tjänsten. Skulle vi drastiskt växa de kommande åren kanske man ska se till att ha allt sånt på plats.
Informant 5	Nej, inte ens nära.	Nu för tiden så sker ju en stor del av företagets kommunikation via mejl. Att boka möten med kunder eller ta emot betalningar eller utföra betalningar, det kommuniceras via mejl. På det sättet är man ju till råttorna om det inte fungerar. Det största problemet jag kan se är ju om jag missar en offert eller något liknande som jag går miste om för att tjänsten ligger nere, eller får betalningsanmärkningar för att räkningar inte kommer fram.	Nej inget sådant. Jag betalat ju nästan ingenting för den här tjänsten och jag förutsätter mest att de hjälper till om det blir problem bara. I nuläget så är det nästan så att jag måste bevisa att problemen inte har med något från min sida att göra, så som min uppkoppling. Alltså för den lilla summan jag betalar så bryr de sig nog inte så mycket om att säkerställa oavbruten tillgänglighet.

Sammanfattningen av svar i Tabell 7 visar att ingen av informanterna mäter tillgängligheten kontinuerligt på de SaaS-applikationer som används. Svaren angående påverkan av driftstopp på den operativa verksamheten varierar från mindre besvär till kritisk påverkan. Samtliga informanter svarar även att de inte skrivit något specifikt SLA till de använda SaaS-applikationerna utan snarare grundläggande användaravtal. Ett flertal informanter uppgav även att de inte ansåg ett SLA vara proportionerligt till deras nivå av användning.

4.5 Kontroll

I tabell 8 inleds delområdet för kontroll. I denna tabell behandlas för ifall informanterna har någon plan för hur eventuell datahantering ser ut ifall SaaS-applikationen sägs upp. Vidare reder vi ut ifall de har tillgång till backups av den data som produceras.

Tabell 8 - Resultatdel kontroll 1.0

Beslutsfattare	Finns det en plan för datahantering ifall SaaS applikationen sägs upp?	Har ni tillgång till en backup av den data som produceras?
Informant 1	Nej det har jag inte tänkt på riktigt. Det är som sagt inga högtidliga uppgifter vi har uppladdade där. Det skiter jag i lite faktiskt, de kan få behålla dem om det nu av någon anledning skulle vilja det. Viktigast är att det fungerar när vi måste använda det.	Det vet jag inte riktigt. Det har jag inte frågat om, men det antar jag att vi har.
Informant 2	Nej, det har aldrig riktigt varit aktuellt så vi har inte haft något behov av en sådan plan.	Ja det har vi om den stängs ner på längre tid så har vi tillgång till fysiska backups, det har hänt tidigare.
Informant 3	Inte vad jag har tänkt på i nuläget. Jag är väldigt nöjd med nuvarande lösning och ser inte varför jag skulle vilja eller behöva byta inom snar framtid.	Nej det har jag inte. Har länge tänkt på att undersöka om det går att göra, så att man inte går miste om gamla mail och kontakter. Men man är ju bekväm, ja du vet säkert.
Informant 4	Nej alltså det finns väl ingen plan. Har inte tänkt på det så mycket. Det får vi ta då tänker jag. Alltså återigen det är Google liksom, det kommer man väl alltid vara nöjd med och så. Som jag sa precis, skulle vi växa så kanske man får kolla på sånt då istället.	Ja det har vi, som vi sa innan. Men eftersom vi hela tiden genererar ny data vet jag inte hur pass uppdaterad den är i nuläget. Det var längesedan jag använde den.

Informant 5	Nej det har vi inte. Vi har inget affärskritiskt där som vi är beroende av, så det finns ingen uttalad plan. Men det är klart där ligger ju saker i mejlen som är halvviktiga som jag får erkänna att jag inte har koll på vad som händer med.	Det som är riktigt kritiskt har jag sparat i fysisk form på antingen hårddiskar eller i pappersform, det beror lite på. Från deras sida vet jag inte riktigt, jag tror de har en backup med alla sina saker. Det förutsätter jag men jag vet inte säkert.

I tabell 8 tydliggör svaren att ingen av informanterna har någon plan för datahantering vid eventuell uppsägning eller annan avlusting av SaaS-applikationernas användning. Ett flertal informanter uppgav att de inte var aktuellt med uppsägning av tjänsten och att det därmed inte fanns någon plan. I frågan om tillgång till backups på data så kunde I2 med säkerhet svara att leverantören tillhandahöll det, samtidigt som I1 och I5 var osäkra men antog att deras leverantörer gjorde det. I5 uppgav samtidigt att de själva genererade backups på kritisk data, vilket I4 också gjorde. I3 hade ingen tillgång till backups.

I tabell 9 behandlas de sista frågorna inom delområdet för kontroll. Här reder vi ut ifall informanterna vet i vilket land deras data lagras, samt ifall de har någon möjlighet att garantera radering från leverantörens databaser.

Tabell 9 - Resultatdel kontroll 2.0

Beslutsfattare	**Har ni möjlighet att garantera radering av data från SaaS leverantörens databaser?**	**Vet ni i vilket land er data lagras?**
Informant 1	Nej det vet jag inte heller. Jag har aldrig haft behov av att göra det. Det kan man kanske, jag har ingen aning. Det är i alla fall inget jag tänkte över när jag valde de här tjänsterna. Jag tänker att man får överväga de uppgifter som kommer att hanteras, vi har ju inget superhemligt.	Nej det gör jag inte, de är ju svenska företag vi anlitar oss av men jag vet ju inte om de faktiskt lagrar vår data här.
Informant 2	Nej, det vet jag inte om vi har faktiskt, det kanske står i något av avtalen.	Nej, det gör jag inte. Det borde man kanske förstås, men det är inget jag har koll på såhär på rak arm.
Informant 3	Det har jag ingen aning om. Vet inte vad jag skulle behöva radera.	Nej, ingen aning faktiskt.
Informant 4	Ja det tror jag att vi har, men med tanke på att man är småföretagare så har vi väl inte riktigt övervägt denna möjlighet.	Nej, verkligen inte den blekaste. Men jag utgår från att de är transparenta med det?

	I nuläget behöver vi väl inte radera något heller vad jag vet.	
Informant 5	Det vet jag inte riktigt heller. Det borde stå in några villkor men det är inget som stör mig direkt. Jag känner inte att där finns något som hade kunnat skada mig affärsmässigt eller privat för den delen.	Nej det gör jag inte, men jag skulle tro att det är Sverige. Det är inte något jag heller bryr mig särskilt mycket om. Det är klart, jag kan tänka mig att det kan skapa legala problem om data lagras i andra länder, där det finns annorlunda lagstiftning men jag känner inte att jag lagrar någon data i den kapacitet där det hade orsakat några större problem.

Av de fem informanter som undersökts kan man se i Tabell 9 att endast I4 visste att de kunde få sin data raderad. Resterande informanter visste varken om de kunde eller inte. Ingen informant hade heller vetskap om var data lagrades fysiskt. Ett flertal uppgav däremot att de antog att det var i samma land som leverantören befann sig i.

5 Diskussion

I detta avsnitt analyseras insamlad data och kopplas till respektive litteratur.

5.1 Sekretess

I den litteratur som behandlar sekretess menar bland andra Kumar och Goyal (2019) att risken för dataintrång kan öka vid användning av SaaS-applikationer. Vidare menar de att konsumentens verksamhet kan avlyssnas eller på annat sätt utnyttjas eller skadas vid intrång. Utifrån de intervjuer som genomförts har denna risk inte visat sig spela stor roll i användandet av SaaS-applikationer. Majoriteten av informanterna i undersökningen förmedlar att de inte påverkats av den ökade risk för intrång, där en del även uttrycker att intrång i deras data inte påverkar personligt- eller verksamhetsmässigt. Se utdrag nedan från bilaga 6;

" [...] *Sen vet jag inte, det här med integritet av datan och så har inte varit någon större oro. I mina mejl så känner jag inte att det finns så mycket att dölja. Det är som jag nämnde innan, det viktigaste var för mig att välja något som skulle leva ett långt tag till.*" (Informant 5, stycke 12).

Samtidigt uttrycker I2, I3, I4 och I5 ett stort förtroende för sina leverantörer. Detta ligger i linje med Chou och Chiangs (2013) tankar som argumenterar för att oro kring integritetsfrågor tenderar att minska vid ökat förtroende för leverantörer. Samtliga informanter menar att de valt leverantörer utifrån namnkunnighet, vilket bekräftar befintlig teori om att förtroende är en avgörande faktor inom cloud computing (Manuel, 2013). Som

exempel på detta hävdar I2 i sitt svar att ett långsiktigt samarbete utan incidenter med leverantören eller deras produkter, har skapat ett starkt förtroendekapital.

Winkler och Meine (2011) menar att det sällan förekommer någon kontakt eller exponering hos leverantörens personal, trots att beslutsfattare är beroende av denna personal i sin användning av SaaS-applikationer. Vidare menar Kandias et al. (2013), att medlemmar av organisationen, utan att nödvändigtvis göra något större angrepp, har tillgång till klientens data. Skulle sådana medlemmar vissa sig vara illvilliga kan de orsaka skada för användare. Med detta som bakgrund insisterar Winkler och Meine (2011) att beslutsfattare bör eftersträva en god inblick i vem som kommer ha tillgång till eller hantera deras data. Av svaren framgår det av I1 och I2 att de är medvetna om att leverantörens personal har tillgång till deras data. Däremot uppvisas ingen vetskap om vilken specifik typ av anställd eller hur det fungerar. Se utdrag från bilaga 3;

"Ja företaget som vi anlitar har också tillgång till datan och har en fysisk backup som de producerar, ifall det skulle uppstå problem med molnet." (Informant 2, stycke 12).

För att försäkra sig mot dataintrång såsom kapning, där en angripare får tillgång till inloggningsuppgifter, skriver Prakash och Dasgupta (2016) att användare bör komplicera eller förstärka verifieringsprocessen. De tar som exempel upp tvåstegsautentisering som en metod för att bromsa intrång trots att inloggningsuppgifter läckt ut. Samtliga informanter använder grundläggande metoder för autentisering, detta innefattar olika varianter av lösenord. Några inser risken med den simpla autentiseringsmetod och använder således multipla lösenord, medan t.ex. I3 erkänner att samma lösenord används till flera olika applikationer. Med detta påvisar därmed I3 ett exempel på hur användare av SaaS-applikationer kan ha direkt påverkan på säkerhetsrisken med sin hantering av lösenord, vilket Grobaur et al. (2011), tidigare diskuterat.

Enligt Barona och Mary Anita (2017) så är kryptering en viktig del av datasekretess vid användning av SaaS-applikationer. Krypteringen ger ett extra lager av säkerhet ifall det blir intrång i en databas. Detta leder till att datan inte blir brukbar utan vidare behandling, således menar Barona och Mary Anita (2017) att det kan vara tillrådligt att utvärdera nivån av kryptering hos leverantören. Detta är en åtgärd som bland samtliga av våra informanter inte har begrundats. Samtliga återger förhållandevis korta och tydliga svar, där de informerar att de inte alls tänkt över denna aspekt. Ett flertal uppger samtidigt att de inte anser det vara viktigt med tanke på den lagrade datans natur. Se bifogat utdrag från bilaga 2;

"Nej. De bara tankar ner våra uppgifter och sen vet jag inte vad de gör med dem. Asså det är inte så viktigt för mig, jag tror det beror på vilken branch man är i och så." (Informant 1, stycke 20).

I ovanstående utdrag framgår det även att I1 länkar betydelsen av kryptering till branschen som verksamheten ingår i. Svaret påvisar därmed inte en fullkomlig omedvetenhet om kryptering eller dess potentiella användbarhet, utan snarare som en låg prioritet till sin egen verksamhet. Vidare så kan det vara möjligt att denna tendens uppstår på grund av att de upplevda fördelarna med SaaS-applikationerna överskrider de upplevda riskerna, vilket Wu et al. (2011) hävdar skapar förtroende. Framförallt bör man ha i åtanke att flera av informanterna använder gratis-applikationer, vilket leder till att upplevda fördelarna förstärks, och därmed minskar medvetenhet inom integritetsfrågor, i enlighet med Chou & Chiang (2013).

Överlag inom området för sekretess påvisas en genomgående trend bland informanternas svar, att sekretess inte är en prioritet. Detta kan förklaras med teorin om att upplevde fördelar skapar förtroende, som i sin tur minskar integritetsoro, som vi diskuterat ovan. Vidare kan deras förhållningssätt vara grundat i att datan inte anses vara hemlig, eller de inte skulle skadas om någon skulle se eller övervaka deras data. Däremot verkar de inte begrunda aspekter som potentiell manipulering av data eller spridande av falsk information, vilket Tirumala et al. (2015), belyser som ett hot inom cloud computing med avseende på sekretess.

5.2 Tillgänglighet

Tillgänglighet är en av de största svårigheterna inom cloud computing och det bör mätas kontinuerligt (Chaczka et al, 2011; Manuel, 2014; Benlian & Hess, 2011). Detta påstående stämmer överens med de svar som vi erhållit från informanterna i vår undersökningen. Samtliga informanter ansåg att den största risken med SaaS-applikationer var de skulle förlora tillgång till applikationen, samt den data som behandlades. Detta illustreras väl i svaren på frågan om hur verksamheten skulle påverkas av driftstopp i tjänsten. Nedan bifogas utdrag från flera bilagor;

" [...] Om kassorna inte fungerar så blir det ju kaos, då påverkas vi direkt eftersom vi inte kan ta betalt av kunderna. Men ja allt ligger ju molnet så det ställer ju såklart till förödelse om det inte skulle fungera [...]" (Bilaga 2, Informant 1, stycke 24).

"Det hade varit katastrofalt eftersom vi hade tappat tillgång till den datan vi använder oss av när vi arbetar. Speciellt om det är vår OneDrive, där filerna som vi använder varje dag är lagrade. Om jag kommer in på morgonen och det inte funkar, så får jag det väldigt svårt att utföra mitt jobb."
(Bilaga 3, Informant 2, stycke 22).

Utöver detta var det flera som i inledningsfrågorna identifierade tillgänglighet eller tillgång till sin applikation som den största risken vid användning av SaaS-applikationer. Benlian och Hess (2011) lägger stor vikt vid verksamhetsstrukturen, där de menar att kundorienterade processer är speciellt beroende av en hög tillgänglighet. Detta sentiment delas tydligt av I1 och I2 i de bifogade utdragen ovan samt de inledande frågorna kring upplevda fördelar och risker. Trots detta behov av tillgänglighet är det ingen av informanterna som mäter tillgängligheten av sin SaaS kontinuerligt, vilket strider mot vad Chaczka et al. (2011) hävdar vara en prioritet. Anledningen till detta uppges vara att de inte upplevt problem tidigare, och kan igen anknytas till betoningen på förtroende som uppkommit flera gånger tidigare.

Takabi et al (2010) anser att ett SLA är högst nödvändigt för att definiera servicegrad hos sin leverantör. Ser man vidare till de specifikationer som Alhamad et al (2010) presenterar för ett SLA, så kan användare försäkra en nivå av service och ansvarsskyldighet hos leverantören. I undersökningen som gjorts är det återigen ingen av användarna som vidtar åtgärder för att reglera eller påverka tillgänglighet i form av SLA. Denna iakttagelse går därför i strid med Lins en al. (2016), som menar att SaaS-användare bör verifiera sitt kontrakt inför och kontinuerligt under användning. Flera informanter svarar att de skrivit under avtal, men de verkar inte ha klarhet i om detta är ett SLA eller ens innehåller paragrafer som reglerar tillgänglighet. Se utdrag från bilaga 3;

" [...] jag har skrivit på ett vanligt användaravtal. Nu kan jag det ju inte utantill, men visst jag är nöjd med det. Tjänsten gör det som jag behöver och vi har inte haft några problem än." (Informant 2, stycke 24).

Allmänt kan det sägas att informanterna i denna undersökning visar en förhållandevis hög medvetenhet kring de risker som SaaS-applikationer tillbringar i form av tillgänglighetsproblem. Däremot har de inte vidtagit någon av de två främsta sätten som litteraturen lyfter fram för att gardera sig mot dessa risker, nämligen upprättande av ett adekvat SLA och kontinuerlig mätning av applikationens tillgänglighet.

5.3 Kontroll

Ett hot inom delområde kontroll är dataförlust, eller till och med oförmågan att kunna förhindra dataförlust (Prakash och Dasgupta, 2016). Dataförlust anses även vara ett hot då det både kan ske som följd av illasinnade attacker och på grund av naturfenomen som skadar fysisk lagring, detta enligt Amara et al (2017). De menar även, i samförstånd med Liu (2012) att det därav är viktigt för användare ha ett utförligt system för att lagra backups och återfå tillgång till sin data vid en eventuell kris. I vår undersökning har tre av fem informanter någon form av tillgång till backups om någonting skulle hända med SaaS-applikationen som de använder sig av. I5 har till exempel meddelat att hen själv producerar backups på data som anses vara kritisk för verksamheten. Det tycks dock inte finnas någon uttryckt plan eller ett system för datan som sparas till backup, utan sker istället manuellt i olika former som på hårddisk eller fysisk papperskopia.

Vidare uppgav I1 att hen antog att backups producerades av leverantören men att de inte var helt säkra. Samtidigt svarade både I2 och I4 att det producerades backups, men att det låg hos leverantören. I fallet I2 verkade det finnas något form av system, då de uppgav att det hänt tidigare och de återfått sin data via leverantörens backups. Se utdrag från bilaga 3 nedan;

"Ja det har vi som sagt, om den stängs ner på längre tid så har vi tillgång till fysiska backups. Det har hänt tidigare." (Informant 2, stycke 28).

För I4 var det en mindre säker situation då de beskrev att lagring till backups inte skedde regelbundet och att datan antagligen inte var uppdaterad. Båda informanterna har därmed påvisat en medvetenhet om att datan i den SaaS de använder kan gå förlorad och tilsett en åtgärd i form av leverantörernas backups.

Både Amara et al. (2017) och Opara-Martins et al. (2014) hävdar att ett säkerhetshot inom kontroll är lock-ins, där man förlorar frihet att byta eller säga upp sig ifrån den SaaS-leverantör som man använder. Opara-Martins et al. (2014) belyser risken med brist interoperabilitet mellan leverantörer, vilket betyder att sparad data i en applikation blir svår att överföra vid byte av leverantör. Även om det existerar interoperabilitet mellan leverantörer så kan kostnaderna relaterade till en övergång vara så höga att detta i sig skapar en barrikad. I vår undersökning finner vi att majoriteten av informanter är nöjda med nuvarande lösning och har således inte uttänkt plan för datanhantering vid eventuell övergång. Flera informanter påvisar återigen förtroende för respektive leverantörer, vilket återigen kan förklaras av Wu et als. (2011) tankar om upplevda fördelar i förhållande till upplevda risker. Se utdrag från bilaga 5 nedan;

"Nej alltså det finns väl ingen plan. Har inte tänkt på det så mycket. Det får vi ta då tänker jag. Alltså återigen det är Google liksom, det kommer man väl alltid vara nöjd med och så. Som jag sa precis, skulle vi växa så kanske man får kolla på sånt då istället." (Informant 4, stycke 26).

Å andra sidan uttrycker I5 ett missnöje med sin SaaS-applikation. Hen är missnöjd med leverantörens servicekvalitet, vilket är en viktig faktor för att bygga förtroende hos användare (Grandison & Sloman, 2000; Evans & Kreuger, 2011). I en av inledningsfrågorna kring upplevda risker svarar I5 även att hen överväger att byta SaaS-leverantör, men verkar sakna kunskap samt en plan för hur detta ska gå till. Återigen illustreras vikten av ett befintligt SLA, då detta definierar hur avslutat avtal ser ut (Alhamad et al, 2010) vilket i sin existens kan motverkar risken lock-ins.

Chen och Zhao (2012), skriver att det också är värt att överväga vad som händer med den data som ligger kvar efter avslutad tjänst och om denna ligger kvar och är tillgänglig för leverantören. När vi därför valde att fråga om de visste ifall de kunde garantera radering från leverantören så påvisade samtliga informanter att de inte hade någon uppfattning om detta. Återigen uppkom en attityd, där informanterna inte upplever en tredje parts tillgång till deras data som ett större hot. Se utdrag från bilaga 6 nedan;

"Det vet jag inte riktigt heller. Det borde stå in några villkor men det är inget som stör mig direkt. Jag känner inte att där finns något som hade kunnat skada mig affärsmässigt eller privat för den delen." (Informant 5, stycke 30).

Gandhi och Gandhi (2019) skriver vidare att brist på transparens eller översikt av vart data fysiskt lagras också kan utgöra ett hot för informationssäkerhet inom SaaS-applikationer. Eftersom dessa applikationer kan lagra fullständig data blir den fysiska platsen direkt kopplad till informationens säkerhet. Vidare menar Gandhi och Gandhi (2019) att datalagring som överskrider nationella gränser kan utgöra hot då juridiska säkerhetskrav kan variera. Här framgår det tydligt av svaren från informanterna att kunskap kring leverantörens fysiska datalagring ej förekommer. I vissa fall antas det att datan lagras i Sverige för att leverantörerna är svenska. Exempel på detta illustreras i bilaga 6 enligt nedan;

"Nej det gör jag inte, men jag skulle tro att det är Sverige. Det är inte något jag heller bryr mig särskilt mycket om. Det är klart, jag kan tänka mig att det kan skapa legala problem om data lagras i andra länder, där det finns annorlunda lagstiftning men jag känner inte att jag lagrar någon data i den kapacitet där det hade orsakat några större problem."
(Informant 5, stycke 32).

6 Slutsats

I detta avsnitt avser vi besvara den forskningsfråga som formulerades i det tidiga stadiet av vår undersökning. Frågan lyder; “Hur ser medvetenhet kring informationssäkerhet ut hos beslutsfattare vid användning av SaaS?”. Efter avslutad undersökning finner vi att beslutsfattare överlag saknar kunskap för att kalkylera för samtliga risker relaterade till informationssäkerhet. En trend som observerats hos de informanter som ställt upp i undersökningen är att medvetenheten inom vissa specifika område existerar. Trots medvetenhet och identifiering av risker, saknas många gånger motverkande åtgärder oftast på grund av att informanterna anser sin verksamhet irrelevant i diskussionen kring informationssäkerhet.

Utav de tre studerade delområdena för informationssäkerhet inom cloud computing var sekretess det minst prioriterade, vilket resulterade i en förhållandevis låg medvetenhet inom detta område. Frågor såsom dataintrång, och förhindrande åtgärder som kryptering och autentisering var inte betänkta av någon av informanterna. Den genomgående attityden var att informationen som behandlas i verksamheten inte var hemlig och att läckage till utomstående inte kunde orsaka skada. I samma anda observerades en låg medvetenhet kring delområdet kontroll. Ingen av beslutsfattarna som undersöktes hade någon plan för hur data skulle hanteras vid eventuell uppsägning av nuvarande SaaS-applikation. Likt frågorna för sekretess observerade vi en attityd att garanti på radering av data inte var viktig då den inte ansågs vara hemlig. Undersökta beslutsfattare kunde heller inte ge ett säkert svar på var deras data lagras, utan gjorde på sin höjd antagande om att det var i samma land som leverantören befann sig i. Det påvisades däremot större medvetande och angelägenhet till att förhindra dataförlust då flertalet beslutsfattare hade tillgång till backups.

Tillgänglighet var det delområde som undersökta beslutsfattare visade störst medvetenhet kring. Ett flertal beslutsfattare ansåg att den största risken för deras verksamhet var att de skulle förlora tillgång, och att det var betydligt viktigare än att till exempel säkerställa att utomstående inte fick det. Trots denna påtagliga angelägenhet om att upprätthålla tillgång hade ingen undersökt beslutsfattare tagit åtgärd i form av SLA eller mätning av tillgänglighet. Istället finner vi, i samhörighet med litteraturen, att förtroende spelar en övertygande roll vid användning av SaaS applikationer. Samtliga informanter uttryckte ett förtroende för sina leverantörer på grund av namnkunnighet och långa erfarenhet i branschen.

För att vidareutveckla denna undersökning tror vi att man bör undersöka ett annorlunda urval och jämföra eventuella likheter och skillnader på medvetenhet inom olika storlekar på företag. Exempelvis kan man inrikta sig på medelstora och stora företag. Utöver detta kan en mer extensiv undersökning göras med fler informanter som ger bättre generaliserbarhet åt resultatet.

Bilagor

Bilaga 1 – Intervjuguide

Inledande frågor

1. Vilken eller vilka SaaS applikationer använder ni idag?

2. Vilka skulle du bedöma är de viktigaste orsakerna bakom förvärvet av dessa SaaS applikationer?

Fördelar och nackdelar med SaaS

3. Vilka skulle du bedöma är de största fördelarna med er SaaS applikation?

4. Vad upplever ni som den främsta risken vid användning av er SaaS applikation?

Sekretess

5. Användandet av SaaS applikationer leder till ökad risk för obehörig åtkomst av företagets data. Påverkade detta faktum er vid valet av en SaaS applikation?

6. Vet ni vem som har tillgång till er lagrade data?

7. Vad har ni för typ av autentisering för att få tillgång till er SaaS applikation?

8. Har ni någon insikt eller inflytande på nivå av kryptering av datan?

Tillgänglighet

9. Mäter ni kontinuerligt SaaS applikationens tillgänglighet?

10. Hur bedömer ni att den operativa verksamheten skulle påverkas av driftstopp i SaaS applikationen?

11. Har ni skrivit någon form av serviceavtal med SaaS leverantören som reglerar kvalitetssäkring av leveransen? Är ni nöjda med detta?

Kontroll

12. Finns det en plan för datahantering ifall SaaS applikationen sägs upp?

13. Har ni tillgång till en backup av den data som produceras?

14. Har ni möjlighet att garantera radering av data från SaaS leverantörens databaser?

15. Vet ni i vilket land er data lagras?

Bilaga 2 - Intervju med Informant 1

1. Axel: Vad för typ av verksamhet bedriver ni?
2. Informant 1: En fiskaffär och restaurang.
3. Axel: Hur många anställda har ni i det företaget?
4. Informant: Ja vi är 20 stycken.
5. Axel: Vilken eller SaaS-applikationer brukar ni idag?
6. Informant: Ja du, det är inte min starkaste sida men, vi har en molnlösning som laddar upp mina dokument och filer till ett moln varje kväll. Sen har vi något som heter Timecheck som vi använder för att anställda ska skriva in sig och så, och till löner. Ja och så kassorna såklart, där har vi tecknat något via Kassahuset i Malmö, så våra kassor ät också uppkopplade till molnet.
7. Axel: Okej, och vilka skulle du bedöma är de viktigaste orsakerna bakom förvärvet av de här SaaS-applikationer?
8. Informant: Datorn har kraschat innan, alltså den jag använder då, och det var ett helvete va. Vi tappade ju hur mycket av vår data och information som helst, allt ligger ju där i princip. Då fick jag ringa till min kontaktperson på Lomma IT och så fick de komma ner och försöka rädda så mycket de kunde. Sån tur är så har jag ju själv backuper som jag för ibland på min hårddisk och vi hade många lönespecifikationer och så i utskrivna kopior. Sen då efter det hände så rekommenderade min kontakt på Lomma IT att vi skulle gå över och använda oss av en sån mellantjänst som sparar varje kväll. Det är ju en firma jag har haft småarbete med i många år och som vi köper företagets datorer av. Så han installerade allt och löser de problem som kan uppstå till oss också.
9. Axel: Och vad är då enligt din bedömning de största fördelarna med de här SaaS-applikationerna?
10. Informant: Ja det är att inte behöva oroa sig för det själv, eller oroa sig för att tappa sina uppgifter. Nu är det ett proffs som tar hand om det istället för att jag som inte är så kunnig när det kommer till datorer ska hålla på. Det var ju IT företaget vi anlitar som föreslog att vi skulle gå över till molnlagring av alla filer som jag har på min dator. Och det är klart, man glömmer ju lätt att göra backup själv och även om man inte gör det så är det väl någon gång i månaden som det sker. Där hinner hända jävligt mycket mellan de tillfällena och där är massor av uppgifter som man kan gå förlorade. Nu laddar ju den upp alla mina filer till molnet varje natt istället.
11. Axel: Vad upplever du då som den främsta risken vid användning av de här applikationerna?
12. Informant: Så som jag ser det så har vi inga super-hemligheter som vi lagrar i molnet, eller som de här tjänsterna behandlar. I dagsläget känns det som det finns så många risker så man kan ju aldrig vara helt säker på att man inte kommer bli hackad eller att där blir intrång. Men jag känner ju att det är en större risk för oss om vi tappar tillgång till uppgifterna, så att vi till exempel tappar kollen på löner och semesterdagar och så vidare. Det är sånt som bara måste fungera.
13. Axel: Ja okej, för att användandet av SaaS-tjänster kan leda till ökad risk för obehörig åtkomst av företagets lagrade uppgifter. Påverkade det dig i valet av att förvärva de här applikationerna?
14. Informant: Nä, nä det skulle jag inte säga. Det blev intrång på vår dator när vi bara hade allt på hårddisken också, så jag tycker ju molnet är bättre. Överlag så låg valet mest i att det blev smidigare för oss med de här tjänsterna och att allt inte står still om någon av hårdvaran skulle gå åt.
15. Axel: Okej, vet du vem som har tillgång till den lagrade datan då?
16. Axel: Vad har ni för typ av autentisering för att få tillgång till er SaaS?

17. Informant 1: Ja, asså jag har ju lösenord till var och en.
18. Informant: Ja de som är vår handläggare hos de vi anlitar kan ju gå in och se. De kan logga in och använda systemet från sin sida, det är ju så vi får support ifall någonting skiter sig. Som sagt så känner inte jag att det är någonting superhemligt som vi har lagrat.
19. Axel: Men har ni något inflytande på nivån av kryptering på datan då?
20. Informant: Jasså nej, nej, nej, nej. De bara tankar ner våra uppgifter och sen vet jag inte vad de gör med dem. Asså det är inte så viktigt för mig, jag tror det beror på vilken branch man är i och så. Jag skiter ju i om någon får reda på att jag säljer 30 kilo torsk, så länge jag kan använda det och driva min verksamhet så är det lugnt.
21. Axel: Mäter ni kontinuerligt applikationernas tillgänglighet då?
22. Informant: Nä det har vi inte gjort, eller det gör vi inte. Vi har ju haft det i 1.5 år och det har aldrig varit otillgängligt. Man märker ju om det inte funkar, och skulle det ske ofta så hade man ju såklart tänkt om när det gäller valet av leverantör, men en än så länge har som sagt ingenting skett.
23. Axel: Hur skulle du bedöma att den operativa verksamheten skulle påverkas av driftstopp i applikationerna ni använder?
24. Informant: Det beror på vilken. Om kassorna inte fungerar så blir det ju kaos, då påverkas vi direkt eftersom vi inte kan ta betalt av kunderna. Men ja allt ligger ju i molnet så det ställer ju såklart till förödelse om det inte skulle fungera. Jag gör ju egna backupper då och då på det som ligger på min dator, men det är ju inte nära lika ofta som datan laddas upp i molnet.
25. Axel: Har ni skrivit någon form av serviceavtal med de leverantörer ni använder er av, för att kvalitetssäkra leveransen, är du nöjd med detta?
26. Informant: Njaaa, vi har ju skrivit på att de ska sköta det. Man märker ju om det skulle rasa va, men det är klart man är ju ändå livrädd för att det ska sluta fungera.
27. Axel: Okej, och finns det någon plan för datahanteringen ifall tjänsterna säga upp?
28. Informant: Nej det har jag inte tänkt på riktigt. Det är som sagt inga högtidliga uppgifter vi har uppladdade där. Det skiter jag i lite faktiskt, de kan få behålla dem om det nu av någon anledning skulle vilja det. Viktigast är att det fungerar när vi måste använda det.
29. Har ni tillgång till en backup av den data som produceras?
30. Informant: Äe det vet jag inte riktigt. Det har jag inte frågat om, men det antar jag att vi har.
31. Axel: Har ni möjlighet att garantera radering av data från SaaS-leverantörens databaser?
32. Informant: Nej det vet jag inte heller. Jag har aldrig haft behov av att göra det. Det kan man kanske, jag har ingen aning. Det är i alla fall inget jag tänkte över när jag valde de här tjänsterna. Jag tänker att man får överväga de uppgifter som kommer att hanteras, vi har ju inget superhemligt. Om de har tillgång till dem så gör det inte oss så mycket, som sagt viktigast att jag har tillgång själv.
33. Axel: Okej, en avslutande fråga, vet du i vilka länder tjänsterna lagrar er data?
34. Informant: Nej det gör jag inte, de är ju svenska företag vi anlitar oss av men jag vet ju inte om de faktiskt lagrar vår data här.

Bilaga 3 - Intervju med Informant 2

1. Axel: Vilken eller vilka SaaS-tjänster brukar ni idag?
2. Informant 2: En av de tjänster vi använder är OneDrive , samheten. Det är den tjänst jag använder mest på daglig basis eftersom det är där informationen och datan jag behöver i mitt

arbete ligger lagrad. Sen använder vi oss även av fortnox till det administrativa, bokföringen och så.
3. Axel: Ja okej, och vilka skulle du säga är de viktigaste orsakerna bakom förvärvet applikationerna?
4. Informant 2: Ja du, valet grundar sig till stor del i tradition, och vi sedan länge arbetat med företagen. När jag köpte upp företaget så var båda tjänsterna redan i bruk, och jag har fortsatt med dem sedan dess. Just Microsoft som gör OneDrive har vårt företag arbetat med sedan 20-25 år tillbaka.
5. Axel: Och vad upplever du då är de främsta fördelarna med att använda de SaaS applikationer ni har?
6. Informant 2: Det handlar främst om tillgång till support. Vår verksamhet är inte fokuserad på IT och det är inte där vår expertis ligger. Vi har störst behov av någon som inte bara bidrar med en produkt utan också kan komma med rådgivning och drift som ett helhetspaket. Datorerna som vi använder i företaget köps också där. Vi alltså varken kunskapen eller resurserna för att lägga fokus på den biten. Jag vill ha möjlighet att lagra mina dokument i molnet så att jag har tillgång till dem oavsett var jag är men de tekniska detaljerna som ligger bakom det är inte något jag vill oroa mig för att driva.
7. Axel: Ja jag förstår, och vad är det då som du ser som största risken med er användning av Fortnox och OneDrive?
8. Informant 2: Det är om det sker någon form av avbrott från kontakten med tjänsterna så att de inte går att använda. Så som jag ser det så är det den största risken för företaget för då tappar vi tillgång till den information och data som vi är arbetar med och är beroende av för vår verksamhet. Om jag inte får tillgång till de dokument som är uppladdade alltså, eller inte har tillgång min bokföring eller möjlighet att ta betalt kunder eller andra administrativa behov. Jag ser nog det som en mer sannolik risk än dataintrång och att någon utomstående ska försöka få tillgång till de uppgifter som hanteras i tjänsterna.
9. Axel: Ja så pass, för det kan annars vara en ökad risk att obehöriga får åtkomst till till företagets data. Påverkade detta faktum er vid valet av en SaaS applikation?
10. Informant 2: Ja asså det kan väl säga. Vi använder oss av företag som vi har ett förtroende för ju. De är stora företag som vi anser har ett kapital av förtroende och historiskt välfungerande produkter. Under tiden vi har arbetat med dem så har det inte uppstått några större problem.
11. Axel: Vet ni vem som har tillgång till den lagrade datan?
12. Informant 2: Ja företaget som vi anlitar har också tillgång till datan och har en fysisk backup som de producerar, ifall det skulle uppstå problem med molnet.
13. Axel: Vad har ni för typ av autentisering för att få tillgång till er SaaS applikation?
14. Informant 2: Jag får ju logga in med ett lösenord om det är det du menar.
15. Axel: Ett lösenord, är det samma till båda tjänsterna eller programmen?
16. Informant 2: Ja asså, det är kanske lite tabu att ha det så men jag försöker byta ganska ofta så då är det lättare om jag använder mig av samma till båda då.
17. Axel: Okej, och har ni något inflytande på nivån av kryptering av datan?
18. Informant 2: Ehhh, nä det har vi inte i den bemärkelsen, vi kan bara kontrollera hur mycket av vår data som ska sparas i OneDrive till exempel.
19. Axel: Mäter ni kontinuerligt SaaS-applikationens tillgänglighet?
20: Informant 2: Nej det gör vi inte, det har inte varit några problem än så länge så det har inte känts nödvändigt.
21. Axel: Okej, hur bedömer ni att den operativa verksamheten skulle påverkas av ett driftstopp i de här tjänsterna?
22. Informant 2: Det hade varit katastrofalt eftersom vi hade tappat tillgång till den datan vi använder oss av när vi arbetar. Speciellt om det är vår OneDrive, där filerna som vi använder

varje dag är lagrade. Om jag kommer in på morgonen och det inte funkar, så får jag det väldigt svårt att utföra mitt jobb.
23. Axel: Har ni skrivit någon form av serviceavtal med leverantören som reglerar kvalitetssäkring av leveransen, och är ni i så fall nöjda med det?
24. Informant 2: Njaaaa, asså jag har skrivit på ett vanligt användaravtal. Nu kan jag det ju inte utantill, men visst jag är nöjd med det. Tjänsten gör det som jag behöver och vi har inte haft några problem än.
25. Axel: Har ni någon plan för datahantering ifall ni säger upp dessa SaaS-?
26. Informant 2: Nä, nä, det har aldrig riktigt varit aktuellt så vi har inte haft något behov av en sådan plan.
27. Axel: Har ni en backup på den data som företaget producerar?
28. Informant 2: Ja det har vi som sagt, om den stängs ner på längre tid så har vi tillgång till fysiska backups. Det har hänt tidigare.
29. Axel: Okej, och har ni möjlighet att garantera radering av er data från SaaS-leverantörens databaser?
30. Informant 2: Nej, det vet jag inte om vi har faktiskt, det kanske står i något av avtalen.
31. Axel: Okej, avslutningsvis, vet ni i vilket land de här leverantörerna lagrar er data?
32. Informant 2: Nej, det gör jag inte. Det borde man kanske förstås, men det är inget jag har koll på såhär på rak arm.

Bilaga 4 – Intervju med Informant 3

1. Eddie: Vilken eller vilka SaaS-applikationer brukar ni idag?
2. Informant 3: I dagsläget använder jag mig av Microsoft 365 samt Google Mail.
3. Eddie: Okej, och vilka skulle du bedöma är de viktigaste orsakerna bakom förvärvet av er SaaS applikation?
4. Informant 3: Jag använder mig av tjänsterna för jag tycker det är smidigt att ha allting samlat på ett ställe men också att jag smidigt kan komma åt mail osv oavsett om jag är på mobilen eller datorn. Användarvänligheten i form av tillgänglighet är helt enkelt bättre än andra alternativ.
5. Eddie: Jag förstår, vilka skulle du bedöma är de största fördelarna med er SaaS-applikation?
6. Informant 3: Det måste vara att jag alltid kan komma åt information som jag har sparat vart jag än befinner mig. Alltså via mobilen eller laptop.
7. Eddie: Yes, och vad upplever ni som den främsta risken vid användning av SaaS?
8. Informant 3: Det skulle vara om jag till exempel tappade bort min telefon och någon lyckades komma åt information som inte berör utomstående. Det hade jag nog tyckt vara jobbigast.
9. Eddie följdfråga: Du menar att informationen i telefonen inte berör den personen som ser det?
10. Informant 3: Ja precis, det som finns i min telefon är privata, arbetsrelaterade saker som inte ska användas av någon utom mig.
11. Eddie: Precis som vi varit inne på precis. Användandet av SaaS-tjänster kan leda till ökad risk för obehörig åtkomst av företagets lagrade data. Påverkade detta faktum er vid valet av en SaaS-programvara?
12. Informant 3: Nja, eftersom jag är en liten enskild firma har jag inte tänkt så mycket på det. Men detta påminner lite om det jag sa precis. Däremot litar jag på att leverantören håller min data säker. De kan inte hjälpa att jag tappar min telefon på gatan och på så sätt blir utsatt för dataintrång.

13. Eddie: Vet ni vem som har tillgång till er lagrade data?
14. Informant 3: Man blir lite skrämd när man får denna fråga men även här har jag ingen aning om vem som har tillgång till min data.
15. Eddie: Vad har ni för typ av autentisering för att få tillgång till er SaaS?
16. Informant 3: Asså mitt lösenord? Jag har faktiskt samma lösenord till min Google Mail som jag har till mycket annat.
17. Eddie: Ja verkligen, har ni någon insikt eller inflytande på nivå av kryptering av datan?
18. Informant 3: Nej inte vad jag vet. Detta har ju aldrig tänkt på.
19. Eddie: Ok, mäter ni kontinuerligt SaaS-applikationens tillgänglighet?
20. Informant 3: Nej det gör jag inte. Jag är inte så beroende av en ständigt uppkopplad tjänst med tanke på att jag är en enskild firma. Så lite down time här och där gör inte mig någonting. Självklart hade det varit störigt att inte komma in i mailen när man behöver den, men det är inget jag märkt under mina år med Google Mail.
21. Eddie: Hur bedömer ni att den operativa verksamheten skulle påverkas av driftstopp i tjänsten?
22. Informant 3: Som sagt med tanke på att jag är en liten enskild firma hade det påverkat mig men det hade inte varit hela världen för just min firma.
23. Eddie: Har ni skrivit någon form av serviceavtal med leverantören som reglerar kvalitetssäkring av leveransen? Är du nöjd med detta?
24. Informant 3: Nej det har jag inte. Såklart har jag godkänt de allmänna avtalen när jag förvärvade dessa tjänster, men det läser väl ingen (skrattar).
25. Eddie: Nä men så är det väl, finns det en plan för datahantering ifall SaaS-tjänsten sägs upp?
26. Informant 3: Inte vad jag har tänkt på i nuläget. Jag är väldigt nöjd med nuvarande lösning och ser inte varför jag skulle vilja eller behöva byta inom snar framtid.
27. Eddie: Har ni tillgång till en backup av den data som produceras
28. Informant 3: Nej det har jag inte. Har länge tänkt på att undersöka om det går att göra, så att man inte går miste om gamla mail och kontakter. Men man är ju bekväm, ja du vet säkert.
29. Eddie: Jo men absolut, har ni möjlighet att garantera radering av data från leverantörens databaser?
30. Informant 3: Det har jag ingen aning om. Vet inte vad jag skulle behöva radera.
31. Eddie: Okej, en sista fråga, vet ni i vilket land er data lagras?
32. Informant 3: Nej, ingen aning faktiskt.

Bilaga 5 – Intervju med Informant 4

1. Eddie: Vilken eller vilka SaaS-applikationer brukar ni idag?
2. Informant 4: Google Mail främst, men även Google Ads och så faktiskt Microsoft 365. Jag är inte helt såld på Googles motsvarighet på Microsoft Excel. Så för att summera så blir det väl Google och Microsoft 356.
3. Eddie: Vilka skulle du bedöma är de viktigaste orsakerna bakom förvärvet av dessa SaaS-applikationer?
4. Informant 4: Nä men smidigheten att kunna dela jobb och redigera det direkt och ha det ute på internet är väl den främsta anledning skulle jag säga. Att veta att man har det liggandes utan att behöva klydda med en massa överföringar och så vidare.
5. Eddie: OK! Vilka skulle du bedöma är de största fördelarna med er SaaS-applikation?
6. Informant 4: Hänger väl ihop lite med föregående fråga, alltså smidigheten och att slippa skicka över massa filer via mail är väl de främsta fördelarna.

7. Eddie: Ja såklart, men är det något ny fördel som du inser nu efter förvärvet av tjänsten, eller är fördelarna precis så som du bedömde inför, ifall du förstår hur jag menar.
8. Informant 4: Ja jag förstår hur du menar, alltså nä egentligen inte. Utan det är återigen att arbetet förenklas otroligt när man kan dela filer och så vidare som man arbetat med på ett så enkelt sätt.
9. Eddie: Vad upplever ni som den främsta risken vid användning av era SaaS-applikationer?
10. Informant 4: När man inte är insatt så vet man ju inte riktigt, behöver man egentligen ytterligare backup? Tänk om det händer något med filerna man lagrar i tjänsten? Man vet ju inte. Rädslan för att filer ska försvinna är väl det första jag tänker på. Till exempel insåg vi häromdagen att ett dokument vi satt och arbetade i där länken var åtkomlig för alla, detta var ju väldigt oroväckande, någonting vi inte alls hade tänkt på. Det skulle jag vilja ändra på. Det borde ju vara default att med stänga dokument för allmänheten, för att sedan öppnas ifall vi önskar det.
11. Eddie: Ja det kan man tycka, det borde de faktiskt ändra på. Användandet av SaaS-applikationer kan leda till ökad risk för obehörig åtkomst av företagets data. Påverkade detta faktum er vid valet av SaaS-applikationer?
12. Informant 4: Nja inte direkt, det är Google liksom. Det känns stort och pålitligt. Behöver inte tänka så mycket över det. Inga konstigheter. Inte påverkat valet varken positivt eller negativt. Men nu när du ställer frågan så börjar man väl tänka lite på vem som kan ta del av datan.
13. Eddie: Haha ja det kanske man bör kolla, vet ni vem som har tillgång till er lagrade data?
14. Informant 4: Nej ingen aning om det. Obehagligt att resonera kring, tänk om de säljs till tredje part? Man förlitar sig så himla mycket på Google som leverantör. De har funnits med och varit störst ett tag nu. Det känns som att datan existerar på ett tryggt ställe.
15. Eddie: Vad har ni för typ av autentisering för att få tillgång till era SaaS-applikationer?
16. Informant 4: Jag har ett par lösenord som jag byter mellan. Arbetade tidigare på en arbetsplats där det krävdes att man bytte varannan månad eller så. Så jag har anammat detta sedan dess.
17. Eddie: Har ni någon insikt eller inflytande på nivå av kryptering av datan?
18. Informant 4: Aehh, det vet jag inte. Svår fråga för en någon som mig som inte sysslar direkt med sådant.
19. Eddie: Ja, mäter ni kontinuerligt SaaS-applikationernas tillgänglighet?
20. Informant 4: Nej det gör vi inte. Känns inte värt det med tanke på hur lite som lagras av oss i nuläget. Hade vi sett problem så hade vi kollat på andra SaaS tjänster.
21. Eddie: Hur bedömer ni att den operativa verksamheten skulle påverkas av driftstopp i SaaS-applikationerna?
22. Informant 4: I dagsläget har vi backup, vi har kört över alla filer och kör endast drive nu. Däremot sedan vi gick över till Drive har vi slutat lagra backupfiler, och de finns alltså inte den externa hårddisken just nu. Det betyder ju att vi hade kunnat sitta där utan tillgång till viktiga avtal och fakturor när vi behövde dem. Ja det hade ju ställt till det massor. Klart vi hade kunnat skaka fram gamla kunduppgifter o så men det hade tagit tid och varit kostsamt.
23. Eddie: Okej, har ni skrivit någon form av serviceavtal med SaaS-leverantörerna som reglerar kvalitetssäkring av leveransen? Är ni nöjda med dem?
24. Informant 4: Nej, det har vi inte gjort. Vi har inga jättetunga filer, och har inte tänkt så mycket. Alltså jag antar att sånt står i avtalet man godkänner, alltså licensavtalet liksom. Jag har hittills inte upplevt några problem med kvalitet på tjänsten. Skulle vi drastiskt växa de kommande åren kanske man ska se till att ha allt sånt på plats.
25. Eddie: Jag förstår, finns det en plan för datahantering ifall någon av SaaS-applikationerna sägs upp?

26. Informant 4: Nej alltså det finns väl ingen plan. Har inte tänkt på det så mycket. Det får vi ta då tänker jag. Alltså återigen det är Google liksom, det kommer man väl alltid vara nöjd med och så. Som jag sa precis, skulle vi växa så kanske man får kolla på sånt då istället.
27. Eddie: Har ni tillgång till en backup av den data som produceras?
28. Informant 4: Ja det har vi, som vi sa innan. Men eftersom vi hela tiden genererar ny data vet jag inte hur pass uppdaterad den är i nuläget. Det var längesedan jag använde den.
29. Eddie: Har ni möjlighet att garantera radering av data från SaaS-leverantörernas databaser?
30. Informant 4: Ja det tror jag att vi har, men med tanke på att man är småföretagare så har vi väl inte riktigt övervägt denna möjlighet. I nuläget behöver vi väl inte radera något heller vad jag vet.
31. Eddie: OK, vet ni i vilket land er data lagras?
32. Informant 4: Haha nej, verkligen inte den blekaste. Men jag utgår från att de är transparenta med det? Haha men vem vet, kanske Zimbabwe man vet inte?

Bilaga 6 – Intervju med Informant 5

1. Axel: Vilken eller vilka SaaS-applikationer använder ni idag?
2. Informant 5: Tele2 för email.
3. Axel: Och vilka skulle du bedöma är de viktigaste orsakerna bakom förvärvet av denna SaaS-applikation?
4. Informant 5: Det var en prisfråga, vi använde oss redan av telefonin genom Tele2 och sen hade vi en form av konsult i samband med inköp av datorer som rekommenderade att vi tog vår email via dem också. Då hade vi som sagt möjlighet att få email också till ett bra pris, och Tele2 kändes som en stabil leverantör också, ingen som skulle försvinna eller gå in konkurs de närmsta åren i alla fall.
5. Axel: Ja, och vilka skulle du bedöma är de största fördelarna med er SasS-applikation?
6. Informant 5: Det är lite svårt att säga, vi använder det bara till mejl. Det jag skulle säga ät att det är en fördel att ha någon man kan kontakta om det går fel, som kan hjälpa till och även har något sorts ansvar. Tele2 är ju ett känt företag för oss, och de har en helt annan expertis än vad vi har inom IT och det digitala.
7. Axel: Vad upplever ni då som den främsta risken vid användning av er SaaS-applikation?
8. Informant 5: En stor risk som jag ser är att Tele2 har utvecklats ifrån den här typen av tjänst och inte riktigt bryr sig om den längre. Handläggningen kan ta väldigt långt tid, du vet de har knappt några som sitter och jobbar med det längre. Det är en väldigt liten avdelning, om man ens kan kalla det så. Det känns som det har blivit svårare att få tag på dem när jag upplever ett problem, eller behöver hjälp. Eftersom de verkar dedicera mindre resurser kanske det tar längre tid för dem att identifiera problem eller få kontakt med mig om något skulle ske på deras sida också. Nu när jag betalar så lågt pris som jag gör så upplever jag att de nästan är lite ovilliga att hjälpa till. Det ligger ofta på mig att bevisa att det inte ligger något fel hos mig, med min dator eller nätet här och det kan vara svårt att få fram data jag tappat tillgång till. Sen i ett generellt perspektiv med en sådan här tjänst så är väl den största oron vad som skulle hända med ens uppgifter eller data om leverantören går i konkurs eller tjänsten på annat vis upphör.
9. Axel: Ja okej, men har du tagit någon åtgärd som att klaga eller har du tänkt byta till någon annan?

10. Informant 5: Ja jag har nog klagat några gånger, men det känns inte som där finns så mycket att göra. Nu har ju det så billigt tillsammans med min telefoni och så men det är inte omöjligt att jag byter här någon gång snart om jag hittar ett bra erbjudande.
11. Användandet av SaaS-applikationer kan också leda till ökad risk för obehörig åtkomst av företagets data. Påverkade detta faktum er vid valet av en SaaS-applikation?
12. Nej jag valde mest baserat på att det var ett namn vi kände till och att vi då fick ett bra pris i samband med telefonin. Vi hade också en viss tillit till Tele2 eftersom de var väldigt stora inom detta på den tiden då vi först tecknade tjänsten. Det har ju ändrats lite nu, och det finns många fler företag som är mer specialiserade. Sen vet jag inte, det här med integritet av datan och så har inte varit någon större oro. I mina mejl så känner jag inte att det finns så mycket att dölja. Det är som jag nämnde innan, det viktigaste var för mig att välja något som skulle leva ett långt tag till.
13. Axel: Ja, och vet ni vem som har tillgång till er lagrade data då?
14. Informant 5: Nej det vet jag inte säkert. Jag fattar det som att de inte har tillgång hur som helst i alla fall. Sist jag hade problem så hade jag överbelastad min kapacitet, eller överskridit den snarare, på servern. Då fick jag göra mycket själv, med hjälp av deras instruktioner för att de skulle kunna se vad som var fel, men sen blev det oklart för det vekade som de kunde komma in sen från sin sida. Det var i alla fall mycket fram och tillbaka mellan oss.
15. Axel: Vad har ni för typ av autentisering för att få tillgång till er SaaS-applikation?
116. Informant 5: Autentisering och autentisering, det är bara en mejl liksom. Jag har ett helt vanligt lösenord som jag tar mig in med.
17. Axel: Har ni någon insikt eller inflytande på nivå av kryptering av datan?
18. Informant 5: Nej det har vi inte. Jag vet inte om det känns så relevant för min typ av verksamhet, kanske är viktigare för de som är större.
19. Axel: Mäter ni kontinuerligt SaaS-applikationens tillgänglighet?
20. Informant 5: Nej nej, inte ens nära.
21. Axel: Hur bedömer du att den operativa verksamheten skulle påverkas av driftstopp i SaaS-applikationen?
22. Informant 5: Nu för tiden så sker ju en stor del av företagets kommunikation via mejl. Att boka möten med kunder eller ta emot betalningar eller utföra betalningar, det kommuniceras via mejl. På det sättet är man ju till råttorna om det inte fungerar. I just mitt fall är det kanske lite lättare att hantera eftersom min verksamhet inte är så stor. Jag vet i stort sett vilka mejl jag borde få så om det inte är tillgängligt eller något inte dyker upp så kan jag reagera på det och kanske lösa det på annat vis. Har man däremot en större verksamhet så är man ju beroende av sina system på ett helt annat sätt och då blir det ju problem på riktigt. Det största problemet jag kan se är ju om jag missar en offert eller något liknande som jag går miste om för att tjänsten ligger nere, eller får betalningsanmärkningar för att räkningar inte kommer fram.
23. Axel: Har ni skrivit någon form av serviceavtal med Tele2 som reglerar kvalitetssäkring av leveransen? Och är ni i så fall nöjda med detta?
24. Informant 5: Nej inget sådant. Jag betalat ju nästan ingenting för den här tjänsten och jag förutsätter mest att de hjälper till om det blir problem bara. I nuläget så är det nästan så att jag måste bevisa att problemen inte har med något från min sida att göra, så som min uppkoppling. Alltså för den lilla summan jag betalar så bryr de sig nog inte så mycket om att säkerställa oavbruten tillgänglighet.
25. Axel: Finns det en plan för datahantering ifall SaaS-applikationen skulle sägas upp?
26. Informant 5: Nej det har vi inte. Vi har inget affärskritiskt där som vi är beroende av, så det finns ingen uttalad plan. Men det är klart där ligger ju saker i mejlen som är halvviktiga som jag får erkänna att jag inte har koll på vad som händer med.
27. Axel: Har ni tillgång till en backup av den data som produceras?

28. Informant 5: Det som är riktigt kritiskt har jag sparat i fysisk form på antingen hårddiskar eller i pappersform, det beror lite på. Från deras sida vet jag inte riktigt, jag tror de har en backup med alla sina saker. Det förutsätter jag men jag vet inte säkert.
29. Axel: Har ni möjlighet att garantera radering av data från Tele2s databaser?
30. Informant 5: Det vet jag inte riktigt heller. Det borde stå in några villkor men det är inget som stör mig direkt. Jag känner inte att där finns något som hade kunnat skada mig affärsmässigt eller privat för den delen.
31. Axel: Och vet ni i vilket land datan lagras.
32. Informant 5: Nej det gör jag inte, men jag skulle tro att det är Sverige. Det är inte något jag heller bryr mig särskilt mycket om. Det är klart, jag kan tänka mig att det kan skapa legala problem om data lagras i andra länder, där det finns annorlunda lagstiftning men jag känner inte att jag lagrar någon data i den kapacitet där det hade orsakat några större problem.

7 Referenser

Alhamad, M., Dillon, T., & Chang, E. (2010, September). Sla-based trust model for cloud computing. In 2010 13th international conference on network-based information systems (pp. 321-324). IEEE.

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 (CyberC)*.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Barona, R. & Mary Anita, E. (2017). A survey on data breach challenges in cloud computing security: Issues and threats. In: *2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)*. IEEE.

Carroll, M., Van Der Merwe, A., & Kotze, P. (2011, August). Secure cloud computing: Benefits, risks and controls. In *2011 Information Security for South Africa* (pp. 1-9). IEEE.

Chaczko, Z., Mahadevan, V., Aslanzadeh, S., & Mcdermid, C. (2011, September). Availability and load balancing in cloud computing. In International Conference on Computer and Software Modeling, Singapore (Vol. 14). ISO 690

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

Chou, S. W., & Chiang, C. H. (2013). Understanding the formation of software-as-a-service (SaaS) satisfaction from the perspective of service quality. Decision Support Systems, 56, 148-155.

Denscombe, M. (2009). Forskningshandboken. Lund: Studentlitteratur.

Domo (2019). Data Never Sleeps 7.0. Domo. Available at: https://www.domo.com/learn/data-never-sleeps-7 [Accessed 1 Dec. 2019].

Du Toit, A. (2018). Confidentiality, Integrity and Availability (CIA) of data. Cyberdirective. Available at:https://cyberdirective.com/confidentiality-integrity-and-availability-cia-of-data/ [Accessed 9 Nov. 2019].

Duncan, R. A. K., & Whittington, M. (2016). Enhancing cloud security and privacy: the cloud audit problem. Cloud Computing 2016.
Evans, A. M., & Krueger, J. I. (2011). Elements of trust: Risk and perspective-taking. Journal of Experimental Social Psychology, 47(1), 171-177.

Gandhi, K. & Gandhi, P. (2019). Cloud computing security issues: An analysis. In: *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE.

Grandison, T., & Sloman, M. (2000). A survey of trust in Internet applications. IEEE Communications Survey and Tutorials. Fourth quarter.

Grobauer, B., Walloschek, T. & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy Magazine*, 9(2), pp.50-57.

Heiser, J., & Nicolett, M. (2008). Assessing the security risks of cloud computing. *Gartner report*, *27*, 29-52.

IEEE 90—Institute of Electrical and Electronics Engineers (1990). IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries, New York.

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

Janssen, M., & Joha, A. (2011). Challenges for adopting cloud-based software as a service (SaaS) in the public sector.

Julisch, K., & Hall, M. (2010). Security and control in the cloud. Information Security Journal: A Global Perspective, 19(6), 299-309.

Kelion, L. (2014). Apple toughens iCloud security after celebrity breach. BBC News. Available at: https://www.bbc.com/news/technology-29237469 [Accessed 12 Nov. 2019].

Kumar, R. & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 33, pp.1-48.

Lee, K. (2012). Security threats in cloud computing environments. International journal of security and its applications, 6(4), 25-32.

Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic certification of cloud services: Trust, but verify!. IEEE Security & Privacy, 14(2), 66-71.

Liu, S. (2017). *Rate of public cloud application services/software as a service (SaaS) penetration worldwide in 2015 and 2020, by application type*. *Statista*. Statista Inc. Available at: https://www.statista.com/statistics/782240/worldwide-software-as-a-service-applications-penetration-rate/ [Accessed 9 Nov. 2019].

Liu, W. (2012, April). Research on cloud computing security problem and strategy. In *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)* (pp. 1216-1219). IEEE.

Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, *233*(1), 281-292.
Pender-Bey, G. (2016). The Parkerian Hexad.

Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing. *Nist Special Publication 800–145, National Institute of Standards and Technology*, Gaithersburg, MD. [Accessed 2019-12-18]

Opara-Martins, J., Sahandi, R. & Tian, F. (2014). Critical review of vendor lock-in and its impact on adoption of cloud computing. In: *International Conference on Information Society (i-Society 2014)*. [online] IEEE.

Parker, D. B. (2012). Toward a new framework for information security? Computer security handbook, 3-1.

Prakash, C. & Dasgupta, S. (2016). Cloud computing security analysis: Challenges and possible solutions. *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*.

Rao U.H & Nayak U. (2014) History of Computer Security. In: The InfoSec Handbook. Apress, Berkeley, CA

Rouse, M. (2014). Available at: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Accessed 18 Dec. 2019].

Samonas, S., & Coss, D. (2014). The cia strikes back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Sehgal, N. & Bhatt, P. (2018). *Cloud computing*. Cham: Springer.

Statistiska Central Byrån (2018). Användning av molntjänster ökar bland företag. SCB [Accessed 13 Oct. 2019].

Tirumala, S., Sathu, H. & Naidu, V. (2015). Analysis and Prevention of Account Hijacking Based INCIDENTS in Cloud Environment. In: *2015 International Conference on Information Technology (ICIT)*. [online] IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/7437602 [Accessed 27 Oct. 2019].

Wang, Y. C., & Chen, S. (2011). Analysis of Informatization Construction for SMEs with SaaS model. In Advanced Materials Research (Vol. 187, pp. 652-657). Trans Tech Publications.

Winkler, J. & Meine, B. (2011). *Securing the cloud*. Waltham, MA: Syngress.

Wu, W. W., Lan, L. W., & Lee, Y. T. (2011). Exploring decisive factors affecting an organization's SaaS adoption: A case study. International Journal of Information Management, 31(6), 556-563.