SÄKERHETSRISKER I MOLNTJÄNSTER

Kandidatuppsats i Informatik

Julia Kjellberg
Felix Angtorp

VT 2022:KANI23

HÖGSKOLAN
I BORÅS

Svensk titel: Säkerhetsrisker i molntjänster

Engelsk titel: Security risks in Cloud services

Utgivningsår: 2022

Författare: Felix Angtorp & Julia Kjellberg

Handledare: Gideon Mbiydzenyuy

Abstract

The use of cloud services is widespread among companies today, where the flexibility and availability offered in cloud services has sped up the transition from local data storage and software. The application of a third-party provider for data storage and the use of services in the cloud has created some concerns about security and associated risks. Therefore, this thesis aims to increase knowledge about cyber security and associated risks in cloud services for users and service providers. To achieve the stated aim the following research question was raised: What are the security risks in cloud services today, is there a difference between cloud service users and cloud service providers in perceived security risks?

To answer the research question, the thesis predominantly made use of thematic analysis of data collected via semi-structured interviews and email-interviews. The interviews were conducted on a sample of cloud service providers (two companies) and end-users of cloud services (two companies). From the analysis of the collected empirical data, the thesis found out that cloud service users and providers perceive insider risk as the most critical security risk. For cloud service users, data leakage, particularly related to customer data, was considered to be the highest risk. This differs from cloud service providers; they are worried about the consequences of a data leakage.

For cloud service providers, it is about being able to demonstrate that you take an insider attack as a major security risk and work against it in a preventive way in order to increase the trust of the companies that choose to use cloud services. At the same time, continued focus is needed on the development of security against various types of hacker attacks and intrusion attempts addressed in the study in order not to neglect the security risks that should still be taken seriously.

Keywords: Cloud services, service users, service-provider, Cyber security, cyber risk

Sammanfattning

Användningen av molntjänster är utbredd bland företag idag, där den flexibilitet och tillgänglighet som erbjuds i molntjänster har påskyndat övergången från lokal datalagring och mjukvara. Tillämpningen av en tredjepartsleverantör för datalagring och användning av tjänster i molnet har skapat vissa farhågor om säkerhet och tillhörande risker. Därför syftar denna uppsats till att öka kunskapen om cybersäkerhet och tillhörande risker i molntjänster för användare och tjänsteleverantörer. För att uppnå det uttalade målet ställdes följande forskningsfråga: Vilka är säkerhetsriskerna i molntjänster idag, är det skillnad mellan molntjänstanvändare och molntjänstleverantörer i upplevda säkerhetsrisker?

För att besvara forskningsfrågan har avhandlingen framför allt använt sig av tematisk analys av data som samlats in via semistrukturerade intervjuer och mailintervjuer. Intervjuerna har genomförts på ett urval av molntjänstleverantörer (två företag) och slutanvändare av molntjänster (två företag). Utifrån analysen av den insamlade empiriska datan fann avhandlingen att användare och leverantörer av molntjänster uppfattar insiderrisk som den mest kritiska säkerhetsrisken. För användare av molntjänster ansågs dataläckage, särskilt relaterat till kunddata, vara den högsta risken. Detta skiljer sig från molntjänstleverantörer, de är oroliga för konsekvenserna av ett dataläckage.

För molntjänstleverantörer handlar det om att kunna visa att man tar en insider attack som en stor säkerhetsrisk och motarbetar den på ett förebyggande sätt för att öka förtroendet hos de företag som väljer att använda molntjänster. Samtidigt behövs fortsatt fokus på utvecklingen av säkerheten mot olika typer av hackerattacker och intrångsförsök som tas upp i studien för att inte försumma de säkerhetsrisker som ändå bör tas på allvar.

Nyckelord: Molntjänster, användare, leverantör, säkerhet, säkerhetsrisker

Innehållsförteckning

1 Inledning

I detta avsnitt avses en introduktion samt bakgrund till ämnesområdet molntjänster. Med hjälp av bakgrund och tidigare forskning kommer en problemdiskussion och problemformulering formuleras för att sedan landa i ett syfte med tillhörande forskningsfråga för uppsatsen.

1.1 Bakgrund

Allt fler företag går idag över till användning av molntjänster eller molnlösningar för lagring av data och tillgång till beräkningsresurser. Utifrån Bu, Xiao och Qian (2017) artikel beskriver de hur molnlösningar utför möjligheten att data kan bli portabel och därmed kan användare få tillgång till ett moln vart de än befinner sig så länge det finns en internetuppkoppling. Via en molntjänst har man också möjligheten till att använda IT-tjänster utan att besitta någon specifik kunskap om de bakomliggande modeller och tillhörande komplexitet. Med ökad andel företag som använder sig av molntjänster för att hantera sin data och information så berättar Beckers et al. (2013) att det ligger i molntjänsters natur att ha bristande förtroende för säkerheten eftersom lagring och hantering av data, samt känsliga IT-processer sker utanför företag och organisationers kontroll. Molntjänstleverantörer är därav i behov att kunna illustrera att säkerheten är allvarsam nog för att säkerhetsställa att användarna känner sig trygga med molnlösning. GDPR (*eng. General Data Protection Regulation*) dataskyddsförordningen är en EU lag som trädde i kraft 25 maj 2018, som togs fram för att reglera insamlingen och hanteringen av personuppgifter (IMY, 2021). Molnleverantörer måste säkerhetsställa att dataskyddsförordningen efterföljs genom att upprätthålla en fullständig dokumentation av de personuppgifter som lagras skriver Georgiopoulou, Makri & Lambrinoudakis (2020). Skyldigheterna som kommer med dataskyddsförordningen är omfattande och utmanande vilket ställer höga krav på molntjänstleverantörer eftersom konsekvenserna av att inte följa dataskyddsförordningen kan bli kostsamma.

Molntjänster beskrivs av Iqbal et al (2016) som en banbrytande process för hur företag idag alltmer arbetar med distribution och hantering av företagsapplikationer samt datalagring över internet. Detta bidrar dels med tidsbesparing för företag, men också stora besparingar i form av att inte behöva hantera en egen infrastruktur för hårdvara. Iqbal et al. (2016) tar också upp frågetecknet kring hur integritet och säkerhet ses som kritiska faktorer när molntjänster ska levereras som modeller. Flertalet säkerhetsfrågor bör överses som relateras till datasäkerhet, nätverkssäkerhet och webbapplikationssäkerhet för att säkerhetsställa att integritet och säkerhet inte blir bristande och därmed utgöra en sårbarhet. Sajid et al. (2021) förklarar hur molntjänster är en hoppfylld teknik till följd av de genomgripande funktioner som hög skalbarhet, online lagring och den sömnlösa tillgängligheten som lockar företag till att bedriva sin verksamhet. Detta utgör en viktig del i arbetet kring att minska på kapitalkostnaden och arbetskraften genom att bedriva tjänster via molnet. Men trots innovationsaspekten av molntjänster där datoranvändning med enkel åtkomst är en grundpelare så bidrar den ökande användningen av molntjänster till en proportionell ökning av säkerhetsproblem förklarar Sajid et al. (2021).

En transparens och medvetenhet om vilka risker som finns med molntjänster bör finnas hos alla molnanvändare. Singh och Chatterjee (2017) tar upp att alla molnanvändare borde vara väl medvetna om de risker, sårbarheter och attacker som förekommer i molntjänster. För att företag ska kunna snabbt adaptera sig till molnen är en medvetenhet om attacker och säkerhetsrisker en nyckel till en snabb adaption. Genom att belysa molntjänsters teknologier och den växande

tekniken, hur den kan skapa specifika säkerhetsproblem i molnet, så behövs dessa belysas för att företag ska öka möjligheten till säker användning av molntjänster (Singh & Chatterjee 2017).

1.2 Forskningsöversikt

Molntjänster är ett relativt brett område och därmed har tidigare forskning genomförts. I stora drag diskuteras molntjänsters utvecklingspotential tillsammans med de tillkommande säkerhetsutmaningarna och lösningar. Iqbal et al. (2016) undersöker i sin studie två viktiga begrepp inom molntjänstleveransmodeller som är integritet och säkerhet, vilket dessutom är kritiska faktorer vid anpassningen av molntjänster. Syftet är att presentera säkerhetshoten i förhållande till molntjänstleveransmodellerna och de olika nivåerna i modellerna. Författarna undersöker molntjänster och hur de i första hand använder sig av leveransmodeller för att kunna erbjuda molnbaserad mjukvara, infrastruktur och plattform som tjänst. Det är viktigt att kunna överta tidigare potentiella säkerhetshot/brister till framtida leveransmodeller, eftersom alla företagsapplikationer skiljer sig åt och kräver olika typer av åtgärder (Iqbal et al. 2016).

Många företag lockas idag av att använda sig av molntjänster då de erbjuder online lagring, lätt och sömlös tillgänglighet samt hög skalbarhet. Även om många företag väljer att bedriva sin verksamhet med hjälp av molnet och att innovationen av lättillgängligt ligger i framkant finns det nackdelar som kan leda till en del säkerhetsproblem. Sajid et al. (2021) förklarar och undersöker i sin studie att med en ökad användning av molntjänster ökar dessutom säkerhetsproblemen. För att lösa de problemen som uppstått i samband med utvecklingen av molnet har Internet of Things (IoT) tillämpats i undersökningen. IoT står för att objekten i fråga ska vara anslutna till internet för att kunna tillhandahålla tjänster som exempelvis resurshantering, datalagring och elasticitet (Sajid et al. 2021).

Det finns ett flertal leveransmodeller av molntjänster som krävs då ”Big data Cloud computing” ständigt utvecklas. På grund av IoT ökar möjligheterna successivt för molnet och finns idag tre stora tjänstemodeller. Singh, Jeong och Park (2016) undersöker i sin studie de tre stora tjänstemodellerna och vad de representerar. Infrastructure as a service (IaaS) hanterar hårdvara för datorer genom exempelvis nätverkslagring och minne. Plattform as a service (PaaS) används som ett utvecklingsverktyg, en arkitektur eller som ett program. Detta innebär att kunden på egen hand kan kontrollera sina applikationer, dock kan kunden ej hantera den rådande infrastrukturen. Software as a service (SaaS) är fjärrdatortjänster och gör det möjligt för applikationer att på distans kunna distribueras av tredjepartsleverantörer. SaaS innebär dessutom att kunden kan använda molntjänsters CSP:s (content security policy) applikationer som används via internet som en webbläsare. En diskussion om de tre modellerna har genomförts med utgångspunkt om att förstå de rådande säkerhetskoncepten med hjälp av de tre olika nivåerna och hur kraven för säkerhetshanteringen ska förbättras (Singh, Jeong & Park 2016).

Vidare finns det en del grundläggande komponenter vid molntjänster förklarar Singh, Jeong och Park (2016) som används över hela internet som ett utbud av tjänster. Första komponenten är virtualisering som har en stor roll när det gäller att distribuera molnet på en strategisk nivå. Virtualiseringen möjliggör instansen av en enhet eller resurs såsom ett operativsystem. Den andra komponenten är multi-tenancy vilket innebär att kunder kan dela exekveringsmiljö eller resurser mellan varandra även om de inte tillhör samma organisation. Molnlagring är en komponent som möjliggör tillgänglighet över nätverk att kunna säkerhetskopiera, hantera och underhålla data på distans. Även workstation clusters är en viktig komponent, den kan driva

tusentals servrar som ett datacenter vilket gör den till en säker nätverksinfrastruktur som kan hantera och på ett effektivt sätt konstruera lagringar för molnet. Sista komponenten är hypervisorn som är en nyckelmodul för virtualisering, denna kan köra flera virtuella maskiner på en hårdvaruvärd. Hypervisorn hanterar dessutom olika operativsystem som delar på ett fysiskt system (Singh, Jeong & Park 2016).

Privat moln är en av fyra modeller som används för att distribuera molnlösningars infrastruktur där ingår offentliga moln, gemenskapsmoln och hybridmoln. Mazhar, Samee och Athanasios (2015) granskar i sin studie de olika typerna av moln och hur säkerhetsproblemen uppstår i samband med dem. Ett privat moln används endast vid en enskild organisation och de tillhörande resurserna används ej av någon annan kund. Här är de företaget eller tredje part som äger och kan hantera infrastrukturen. Offentliga moln och det ägs av CSP, det är den fysiska infrastrukturen för molnet och är öppen för alla. Kunden betalar för att få använda tjänsten och de tillhörande resurserna. Gemenskapsmolnet består av fler organisationer eller kunder som tillsammans bildar ett community där alla gemensamt har samma säkerhetskrav, policy och uppdrag osv. Hybridmolnet är en blandning av flera moln av de ovannämnda med samma unika egenskaper dock i kombination med andra typer av moln. Undersökningen resulterade i att förklara de senaste lösningarna mot säkerhetsproblemen med hjälp av de olika typerna av moln, genom exempelvis sårbarheter (Mazhar, Samee & Athanasios 2015).

Säkerhet är den största utmaningen vad gäller användningen av molnlösningar och här finns också den största oron från användarna för den så kallade känsliga datan. Coppolino, D'Antonio, Mazzeo och Romano (2017) undersöker i sin studie de största säkerhetsutmaningarna idag och att de bland annat är sårbarhet i delade data, dataintrång, samt Denial of Service. Undersökningen visar hur man ska arbeta för att uppnå molnsäkerhet och hur man ska ta sig an de övriga säkerhetsutmaningarna med hjälp av molntjänstleverantörerna (Coppolino, D'Antonio, Mazzeo & Romano 2017).

1.3 Problemdiskussion

Med utgångspunkt av ovanstående forskning finns de en del utmaningar med användandet av molntjänster och de kan medföra en del risker inom informationssäkerheten för många företag. Utvecklingen av tekniken samt molntjänster ökar dels säkerheten men medför också ny ovisshet kring hur pålitlig säkerheten är. Människan är den så kallade svaga länken när det gäller informationssäkerheten, där misstag lätt kan inträffa som kan äventyra hela hanteringsprocessen. Organisationer måste genomgå många faser med sin information där den ska genereras, bearbetas, lagras och distribueras. Det resulterar i fler kritiska lägen där informationssäkerheten blir allt mer viktig och står i fokus.

Övergången till molntjänster är lockande för flera företag idag. Fördelarna och besparingarna ekonomiskt som företag gör är en stor del av anledning till val av molntjänster. Men trots alla säkerhetsåtgärder som finns tillgängliga nu för tiden för att arbeta mot säkerhetsproblem och risker bör företag vara medvetna om att det inte finns något system som är 100 % säkert skriver Singh, Jeong och Park (2016). Den mänskliga faktorn är ofta den bakomliggande orsaken till, att oavsett vilken typ av ny teknik som uppfinns är det inte självklart att den är mer säker än tidigare på grund av potentiella mänskliga misstag (Singh, Jeong & Park 2016). I och med ökningen av onlinenätverksapplikationer ökar också den digitala brottsligheten i samma takt vilket ställer ännu högre krav på säkerheten hos molntjänster. Det är den här osäkerheten som

finns hos molnanvändare, de har inte kontroll över hur deras data kan användas och missbrukas av datacenterägare förklarar Singh, Jeong och Park (2016).

Även Mazhar, Samee och Athanasios (2015) tar upp att just säkerheten är ett av de största hindrena som motverkar en större utbredning av användningen av molntjänster. Företag har en tendens att inte helt lita på att molntjänster som en tredjepartsleverantör ska ta hand om ens digitala tillgångar. Vidare förklarar Mazhar, Samee och Athanasios (2015) att många företag än idag upplever att den konventionella IT-infrastrukturen håller de digitala tillgångarna inom företagets administrativa domän där bearbetning, förflyttning och hantering av data upplevs som säkrare. Att säkerheten hos molntjänstleverantörerna i flera fall är transparenta och närvaron av ett stort antal användare som inte är relaterade till företaget ökar oron ännu mer berättar Mazhar, Samee och Athanasios (2015). Summeringen är att säkerheten är just något som upplevs vara en stor faktor till att molntjänster i allmänhet inte används i större utsträckning och därmed bör det undersökas hur molntjänstleverantörer och molntjänstanvändare ska förhålla sig till säkerheten samt vilka åtgärder mot risker finns och bör det finnas för att öka förtroendet för sina molntjänster.

1.4 Problemformulering

Utifrån tidigare forskning (Beckers et al. 2013) och information som finns kring molntjänster kan det konstateras att det kvarstår stora utmaningar kring säkerheten inom molntjänster. Den ständiga utvecklingen av tekniken inom molntjänster är en faktor som också gör att säkerheten och specifikt pålitligheten problematiseras. Med tanke på ökningen av informationsflöden blir det viktigt att förhindra att andra kan komma åt och utnyttja den information som organisationen hanterar. Att förhindra olovligt intrång är av stor vikt eftersom att det kan finnas företagshemligheter som är viktigt att skydda från att utnyttjas i olagliga syften, det finns personuppgifter som måste säkras och det finns information som inte får hamna hos fel person. En stor anledning till orolighet går att koppla till GDPR, konsekvensen av att data missbrukas och därmed att dataskyddsförordningen inte följs kan idag bli mycket kostsamma för företag. Den tidigare forskningen som gjorts visar Singh, Jeong och Park (2016) att det finns en del tveksamheter hos företag när det gäller tredjepartsleverantörer som molntjänster, därför är en undersökning i hur man på ett bättre sätt som molntjänstleverantör ska ta sig an detta för att förtroendet för säkra teknologiska lösningar avseende molntjänster ska öka.

1.5 Syfte och forskningsfråga

I denna uppsats är syftet att utöka kunskapen om säkerhetsrisker inom molntjänster för användare och medvetenheten hos molntjänstleverantörer om hur företag som använder molntjänster ser på säkerhet. Med hjälp av detta kan molntjänstleverantörer öka förtroendet för de företag som använder sig av molntjänster genom att kunna se vilka säkerhetsrisker som användarna är mest bekymrade över. Uppsatsen kommer undersöka vilka säkerhetsrisker som uppfattas vara mest kritiska för molntjänstanvändare respektive molntjänstleverantör samt om det är skillnad sinsemellan.

Forskningsfråga genom arbetet:

- Vilka är säkerhetsriskerna inom molntjänster idag, är det skillnad mellan molntjänstanvändare och molntjänstleverantörer i upplevda säkerhetsrisker?

1.6 Målgrupp för arbetet

Målgruppen för denna studie är i första hand företag eller organisationer som klassificeras som molntjänsteleverantörer som erbjuder molntjänster till företag som lagrar information och dagligen använder molntjänster. Som tidigare nämnt är syftet med undersökningen att ta reda på vilka säkerhetsriskerna är vid användningen av molntjänster och jämföra om det finns en skillnad på molntjänstanvändare respektive molntjänstleverantörernas syn på vilka risker som är mest kritiska. Det förväntade resultatet från denna studie ska kunna ge molntjänstleverantörerna en inblick om vilka säkerhetsrisker deras användare ställs inför. I andra hand är denna studie riktad mot företag som använder sig av molntjänster i sitt dagliga arbete för att kunna förstå molntjänsleverantörers perspektiv vid säkerhetsrisker i molnet.

2 Metod

I detta avsnitt avses att redogöra för de metoder som använts vid undersökningen för att kunna besvara forskningsfrågan. Metodvalet kommer redovisas genom datainsamling och analys av data tillsammans med urvalsmetoder och etiska överväganden som har använts vid utformningen av studiens genomförande. Avslutningsvis kommer en metodreflektion redogöras.

2.1 Forskningsstrategi

Denna uppsats består av ett undersökande arbete som kopplar tillbaka syftet att se vilka säkerhetsrisker som finns inom molntjänster idag. Jacobsen (2017) beskriver tre olika synsätt inom området, vilka är induktion, deduktion och abduktion som är olika forskningsansatser, de är olika metoder för hur man tar sig an en forskningsansats. Induktion handlar om att utgå från observationer och genom de komma fram till en teori som grundar sig i generalisering, medan deduktion är motsatsen där man istället utgår ifrån teorin och hädanefter skapar en teori utefter det. Jacobsen (2017) förklarar att det är svårt att rikta in sig enbart mot induktion eller deduktion eftersom det inte går att enbart förhålla sig till teori till följd av att teori härstammar från observationer som gjorts tidigare. Samtidigt är det svårt att observera utan att ha några antaganden om det man observerar, därav är ett pragmatiskt synsätt som grundar sig i abduktion, som innebär att det vetenskapliga tänkandet börjar med observationer där man ser ett fenomen som vill undersökas. Det leder sedan till en fråga eller problem som ska granskas där hypoteser skapas, undersöks och sammanförs med empiri. Därav av blir abduktion en fortlöpande interaktion mellan empiri och teori, vilket gör den till en kombination av induktion och deduktion berättar Jacobsen (2017).

Undersökningen har bestått av en explorativ undersökningsdesign, vilket innebär att författarna har haft för lite av tidigare kunskaper inom ämnet för att skapa en tydlig problemställning för studien. Därmed har det erfordrats en mer öppen metodik som tillåter flexibilitet menar Jacobsen (2017). Den använda forskningsstrategin i undersökningen har därmed varit en kvalitativ strategi, denna form är öppen och flexibel för forskningsprocessen där forskningsansatsen abduktion kommer att tillämpas. Fördelar med denna typ av forskningsstrategi är att man kan få en bredare förståelse för respondenternas resonemang och ett resultat som är genomgripande, samt där en helhet kan skapas med tydliga mönster. En kvalitativ forskningsstrategi består av en djupgående undersökning på en högre detaljnivå, eftersom antalet respondenter är färre till skillnad från en kvantitativ strategi (Jacobsen 2017).

2.2 Urval av respondenter

Studien är till för att bilda en bättre förståelse för författarna om de undersökta problemområde vilket består av säkerhetsrisker i molntjänster för både molntjänstanvändare och molntjänstleverantörer. Därmed har ett ändamålsenligt urval genomörts eftersom tillgängligheten av information och respondenter har varit ett avgörande kriterium för studien (Jacobsen 2017). Ett av de viktigaste kriterierna för urvalet har varit personernas relevans till forskningsfrågan. Av de respondenter som kontaktades var det viktigt att personen arbetade med molntjänster i sitt dagliga arbete och skulle ha god kunskap inom säkerhetsrisker i molntjänster.

Undersökningen har genomförts på fyra olika företag med fyra olika respondenter, varav två stycken tillhör ett företag som använder sig av molntjänster i sitt dagliga arbete och två stycken molntjänstleverantörer. Detta för att få ett varierande perspektiv på hur de olika företagen ser på informationssäkerheten hos molntjänster samt de risker som upplevs infinna sig i användning av molntjänster, vilket dessutom också har varit ett av de kriterierna som har uppfyllts vid undersökning. Ett kriterium som har varit mycket avgörande för studiens urval har varit att respondenterna ska ha varit tillgängliga eftersom tiden för undersökningen var knapp. Det var ett flertal företag/personer som kontaktades, dock var de många som tackade nej på grund av säkerhet för verksamheten eller resursbrist. Många av de kontaktade företagen har inte visat något intresse alls och valde därmed att inte svara vid förfrågan om intervju.

Därmed består urvalet av fyra utvalda företag som har en koppling till informationssäkerhet hos molntjänster med respondenter som är väl medvetna om säkerhetsrisker i samband med molntjänster. Urvalet för denna studie har också varit ett strategiskt urval, där författarna på egen hand valt ut och kontaktat de personer/företag som var möjliga respondenter för undersökningen. Med ett strategiskt urval för en kvalitativ ansats blir variationen av erfarenheter kring fenomenet rimlig och övergripande för en bra datainsamling (infovoice 2020). Alla respondenter för studien har uppfyllt de kriterierna som har krävts av författarna för att kunna genomföra undersökningen och uppnå syfte med tillhörande forskningsfråga.

Tabell 1: Respondenter

Respondent/verksamhet	Befattning	Typ av respondent
A	CDO (Cheif Digital Officer)	Molntjänstanvändare
B	Enterprise IT Security Compliance Awareness	Molntjänstanvändare
C	IT- ansvarig	Molntjänstleverantör
D	People Manager Cloud	Molntjänstleverantör

2.3 Datainsamling med hjälp av kvalitativa intervjuer

Undersökningens datainsamling bestod av primärdata som har förts samman från respondenternas intervjuer. Den kvalitativa primärdatan har samlats in genom intervjuer där respondenterna har besvarat frågor angående deras verksamhet kopplat till synen på informationssäkerheten hos molntjänster och dess säkerhetsrisker. Primärdata har skräddarsytts för specifikt denna undersökningen. Syftet med intervjuerna är att undersöka företagen som molntjänstanvändare och molntjänstleverantör, hur deras nuvarande värderingar och kunskaper gällande informationssäkerheten ser ut hos molntjänster. I intervjuerna är frågorna anpassade efter urvalet och knyter samman till studiens forskningsfråga samt syfte (Jacobsen 2017).

Intervjufrågorna grundar sig i en semistrukturerad intervjuform med fördefinierade kategorier som utgår ifrån studiens forskningsfråga och tidigare forskning gällande säkerhet samt säkerhetsrisker i molntjänster. Detta har sin utgångspunkt ur två olika perspektiv som har ställts mot varandra för att en diskussion om skillnader samt likheter om molntjänstanvändare och

molntjänstleverantör skulle vara möjlig. Därmed skiljer sig intervjufrågorna som ställts till respondenterna beroende av vad för typ av perspektiv som ligger i grund för underlaget.

För att besvara syfte och forskningsfråga för undersökningen har en semistrukturerad intervju och tre mejl intervjuer genomförts, vilket är en del av den kvalitativa metodiken. Intervjuer har fullbordats eftersom undersökningen kräver primärdata i och med att utgångspunkten är att molntjänstanvändare och molntjänstleverantörer syns skall framhävas i uppsatsen. Deras inblick är värdefull för ämnet då undersökningen ska ge stöd för framtida arbete kring informationssäkerhet i molntjänster. Med intervjuerna kommer man in på djupet av ämnet och kan analysera i flera steg. Eftersom syftet är specificerat mot vilka säkerhetsrisker företag som molntjänstanvändare och molntjänstleverantörer upplever är kritiska idag är intervjuer ett bra sätt att kunna vidareutveckla de svar som företagen ger. Intervjuerna har genomförts på distans via zoom och mejl för att lättare kunna återkoppla om nya frågetecken eller kompletterande frågor som uppstått efter intervjuerna (Jacobsen 2017).

Undersökningen har bestått av fyra intervjuer med fyra olika respondenter, en semistrukturerad och tre mejl-intervjuer genomfördes. Av respondenterna var det tre män och en kvinna som deltog. Innan genomförandet av varje intervju tillfrågades respondenterna om hur de ville besvara intervjun, författarna erbjöd respondenterna en semistrukturerad intervju via videomöte, men tre av fyra respondenter valde att avböja detta och istället svara på frågorna via mejl, då de inte ville bli inspelade. Efter de planerade intervjumomenten har en bearbetning av data genomförts i form av en transkribering och bearbetning av det insamlade materialet.

2.4 Innehållsanalys av data

Efter insamlingen av data börjar den kvalitativa ansatsen där det handlar om att använda en öppen metod för att inte styra den insamlade datan för mycket (Jacobsen, 2017). Här har en innehållsanalys använts där den insamlade datan struktureras in i kategorier som sedan kan kopplas till varandra. Enligt Jacobsen (2017) är forskaren mycket viktig i den kvalitativa metoden eftersom de gäller att strukturera informationen på rätt sätt för att kunna tolka den efter insamlingstillfället. Fördelen av att använda sig av en kvalitativ metod är att man får respondentens uppfattning indirekt via personens egna ord, därav är öppenhet viktigt eftersom syftet är att respondentens egna perception ska komma fram. Samtidigt är det av stor vikt att författarna innan har satt ut vissa riktlinjer kring vad som efterfrågas i intervjuerna utan att skapa standardiserade frågor med svarsalternativ som blir för fasta.

För att få ut något av intervjuerna är det bra att reducera komplexiteten ner till en nivå som gör det enklare att strukturera så en överblick kan bildas. Trots att syftet med en kvalitativ ansats är att få ut flera perspektiv och synvinklar så skriver Jacobsen (2017) för att den kvalitativa analysen ska tillföra något behöver det finnas gränser för nyanser. Blir det för många så finns risken att det blir svårt att tolka och därmed göra det svårt att förstå något alls. Sammanställning av intervjuer och tidigare forskning gör det möjligt att analysera mönster, avvikelser och regelbundenheter vilket enligt Jacobsen (2017) är det centrala delarna för att skapa förståelse för i en situation eller ett fenomen. Därav har författarna använt sig av en innehållsanalys för att analysera de intervjuer som har genomförts. Här har det som respondenterna sagt och som författarna observerat reducerats till mer övergripande samt väsentliga kategorier.

Utformningen av teman har gjorts utifrån problemställningen där de senare brutits upp i mindre enheter. Därefter har kategorier bildats där data har splittrats upp i mindre antal grupper i den

öppna kodningen. I den öppna kodningen har data som liknar varandra och processar samma sak delats in i kategorier för att föras samman till ett fåtal kategorier istället för att använda sig av den totala datamängden (Jacobsen, 2017). Vidare har det genomförts en annan form av kategorisering som heter axial kodning där kategorier formats som inte uppenbart finns i data utan som är kategorier som författarna upprättat efter att den första analysen var utförd. Den axiala kodningen handlar om att bilda en förståelse för samband mellan data där fler underkategorier bildar en större grupp av kategorier. Utifrån kategorierna som bildats har analys av likheter och skillnader gjorts mellan enheter som kopplats till kategorierna, samt att författarna letat efter samband för att kunna jämföra molntjänstleverantör perspektivet mot molntjänstanvändarnas.

2.5 Validitet och reliabilitet

Det finns väsentliga faktorer som påvisar hur kvaliteten på en studie är, Jacobsen (2017) förklarar tre stycken faktorer. De tre faktorerna är extern-, intern validitet och reliabilitet är viktiga begrepp för att undersöka hur studiens kvalité ser ut, samt hur tillförlitlig eller trovärdig studien har varit. Den interna validiteten syftar på studiens trovärdighet, om resultaten uppfattas som giltiga eller inte, menar Jacobsen (2017). För att se till att skapa en intern validitet i studien har författarna granskat sitt val av metod genom att ifrågasätta de val som gjorts för att se om studievalen ger en sann representation av verkligheten. Granskning av respondenter har gjorts för att säkerhetsställa att källorna gav ifrån sig riktig information om det som studien faktiskt studerar. I analysen har strävan efter objektivitet i revideringen av data bidragit till att öka den interna validiteten.

Den externa validiteten syftar på huruvida studiens resultat kan generaliseras till andra än de som varit med i undersökningen (Jacobsen 2017). En kvalitativ undersökning har generellt sett svårare att generaliseras kontra kvantitativa undersökningar. För att stärka den externa validiteten i studien har respondenterna som deltagit bestått av personer från olika stora företag, men också innehaft varierande roller vilket anses öka bredden på forskningen och därmed stärka överförbarheten i studien. Reliabiliteten står för tillförlitligheten i studien och innebär om undersökningens design och undersökaren har någon påverkan samt effekt på de som undersöks (Jacobsen 2017). För att stärka reliabiliteten i studien har författarna skickat transkribering av den semistrukturerade intervju som genomfördes till respondenterna för att säkerhetsställa att rätt tolkningen gjorts av respondentens svar och därmed försökt stärka empirins reliabilitet.

2.6 Etiska överväganden

Vid utformningen av denna studie har författarna utgått från Vetenskapsrådets fyra forskningsetiska krav för att kunna försäkra sig om en god informationssäkerhet för de respondenter som deltagit. De fyra kraven är informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. Dessa resulterar i att uppfylla det grundläggande individskyddskravet (Vetenskapsrådet, 2002). För att uppfylla informationskravet har författarna informerat varje respondent om syftet med studien och vad det innebär för respondenten att delta i undersökningen. Dessutom att det är frivilligt om respondenten anser att det är okej för författarna att spela in intervjun. Det har meddelats att de insamlade materialet endast kommer att användas till studien och ingen obehörig kommer ha åtkomst till det. Författarna har belyst för respondenterna att uppsatsen kommer att offentliggöras på DIVA portal och att de inspelade materialet endast är till för en transkribering. Detta har genomförts

innan påbörjad intervju och alla respondenter har informerats om att deltagandet är frivilligt och kan avbrytas om det önskas.

Alla respondenter i undersökningen är över femton år och därmed har de på egen hand kunnat ge ut sitt samtycke för att delta i studien, det har även getts möjligheten för deltagaren att eventuellt se transkriberingen för att innehållet av intervjun. På så sätt har samtyckeskravet uppfyllts. För att uppfylla konfidentialitetskravet har varje respondent fått förfrågan om de vill vara anonyma eller inte. Majoriteten av respondenterna valde att vara anonyma och med detta som utgångspunkt gjordes en utvärdering av författarna som resulterade i att alla respondenter fick förbli anonyma och tilldelades istället en individuell bokstav i form av A,B,C,D. Som tidigare nämndes kommer det insamlade materialet endast användas till det förmedlade ändamålet och här uppfylls nyttjandekravet, då inga obehöriga kommer ha tillgång till materialet och inget material kommer lånas ut (Vetenskapsrådet, 2002).

2.7 Metodreflektion

I denna studie var en kvalitativ metod i form av intervjuer bäst lämpad som datainsamlingsmetod. Som tidigare underrubriker har redogjort så bedöms en kvalitativ datainsamlingsmetod i form av semistrukturerade intervjuer vara ett synnerligen bra tillvägagångssätt för att skapa ökad förståelse för nuvarande upplevda säkerhetsrisker av molntjänstanvändare och molntjänstleverantör. För att kunna besvara frågeställningen har det behövts företag med rätt personer och rätt kompetens, som har intervjuats för att få ut så bra svar som möjligt från en semistrukturerad intervju.

En nackdel med semistrukturerade intervjuer är att respondenterna är mindre objektiva vilket innebär att det framförs mer subjektiva svar och därmed personliga åsikter. Vilket kan resultera i mindre trovärdiga och mindre nyanserade svar. Det är också viktigt att den som leder intervjun har rätt fokus och leder intervjun i rätt riktning för att inte sväva iväg och skapa oklarheter. Studiens uppsatta mål var att inkludera fem stycken respondenter, men på grund av tidsbrist och avhopp från respondenter uppnåddes inte detta mål. Men studien anses ändå upprätthålla en god kvalitet då respondenterna som deltog ansågs besitta ansenligt goda kunskaper inom ämnet samt inneha betydande erfarenheter.

En annan typ av metod som skulle kunna ha används är en kvantitativ insamlingsmetod i form av formulär som fylls i digitalt där en jämförelse mellan olika företags arbete med informationssäkerheten hade kunnat genomföras med de svar formuläret genererat. Utifrån frågeställningen anses semistrukturerade intervjuer vara bäst lämpade för att få in rätt typ av data och säkerhetsställa att rätt person med rätt kompetens erlägger studien med material. Därav anses intervjuer passa ändamålet med denna studie bäst. För att höja kvalitetssäkrandet i denna studie är det viktigt att författarna är öppna och reflekterar mellan den forskning som gjorts samt de resultat som kommer att presenteras. Reflexivitet är betydande gällande kvalitetssäkring då författarna arbetar med flera infallsvinklar för att öka trovärdigheten, förklarar Jacobsen (2017).

3 Litteratur

I detta avsnitt avses att redogöra samt presentera den använda litteraturen i arbetet. Målet är att kunna utveckla läsarens förståelse för molntjänster och dess olika delar, hur det funkar i förhållande till olika typer av modeller och med de tillkommande säkerhetsrisker osv.

3.1 Vad är en Molntjänst?

Termen molntjänst är bred och kan definieras som en form av behållare som innehåller olika tjänster, hårdvara och mjukvara som kan användas och kommas åt när som helst och var som helst via internet (Singh, 2016). Det finns flertal stora företag som Google, Amazon och Microsoft som erbjuder molntjänster där de sitter på resurser som hårdvara i form av servrar och mjukvara som finns tillgänglig att sälja som "pay per use". Det funkar på det viset att det finns en datainfrastruktur som finns redo att användas via webben som enkelt går att komma åt där datalager, programvara och tjänster finns tillgängliga. Den höga flexibiliteten och att det är lättillgängligt medför låga kostnader för användare eftersom en egen datainfrastruktur inte behövs (Singh, 2016).

Det finns olika typer av moln där indelning sker i fyra olika kategorier. Den första typen heter Public Cloud som är ett offentligt moln. Det offentliga molnet kan alla abonnenter komma åt med en internetuppkoppling och tillgång till molnet där företag eller statliga organisationer äger offentliga molnmiljöer (Singh, Jeong & Park 2016). Den andra typen heter private Cloud och innebär att ett moln etableras för en specifik organisation eller grupp, där åtkomsten är begränsad till enbart gruppen eller organisationen. Tredje typen av moln är Community Cloud där molnet delas mellan flera organisationer som har likartade molnkrav. Den fjärde och sista molntypen heter hybrid Cloud som är en sammankoppling av flera moln som är privata, offentliga eller gemensamma (Mazhar, Samee & Athanasios 2015).

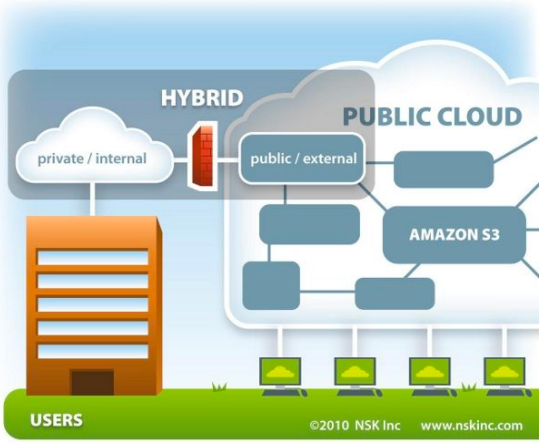

Bild 1 - illustration av de olika typerna av moln (NSK Inc. 2010)

Det finns olika kännetecken för molntjänster där några nyckelegenskaper förekommer som hjälper till att bygga en bild av molntjänster. Ett av kännetecknen är att som kund behöver man inte veta hur mycket kapacitet man behöver som mest, utan hos molntjänster finns möjligheten att skala upp kapaciteten efter hand. Ett annat kännetecken och nyckelegenskap hos molntjänster är att kunden enbart betalar för det man använder. Eftersom man inte behöver köpa

servrar för en maximal kapacitet kan man spara pengar genom att bara behöva betala för den kapaciteten man behöver använda sig av. En annan egenskap hos molntjänster är att molnet jobbar automatiskt med att fördela processorkraft, lagring och nätverksbandbredd på begäran. Det innebär att när ett mindre antal användare befinner sig på webbplatsen anpassar molnet sig och kapaciteten som används blir låg, tvärtom när många användare är inne (Singh, 2016).

3.2 Molntjänst leveransmodeller

Det finns olika typer av tjänstemodeller som bidrar med att kunna leverera molntjänster och med hjälp av Internet of Things ökar man molnets möjligheter till utveckling. Genom utvecklingen av molntjänster krävs det tjänstemodeller med god funktionalitet och en väl fungerande tjänstetillhandahållande kapacitet. Det finns tre stora huvudkategorier inom tjänstemodeller och dessa är **IaaS**, **PaaS** och **SaaS**. Där varje kategori är en generell del av en leveransmodell (Singh, Jeong & Park 2016).

3.2.1 Infrastructure as a service (IaaS)

Infrastructure as a service (IaaS) hanteras av den nedre delen av modellen och behandlar datorhårdvara bestående av minne, nätverkslagring, datacenter, processor samt virtuell server. Förtydligande är det en virtuell dataresurs för bland annat nätverks- och lagringstjänster. Med hjälp av IaaS behöver inte kunden på egen hand hantera infrastrukturen för molnet och delar istället sin data genom en entreprenad. IaaS som tjänst kontrollerar och betalar för de resurserna som efterfrågas av kunderna, vilket är en av de fördelarna som denna kategori erhåller. Man kan säga att IaaS är en kombination av hårdvara och mjukvara (Iqbal et al.2016). IaaS har också ett fokus på några säkerhetsområden som intrångsdetektering och brandväggar (Singh, Jeong & Park 2016).

3.2.2 Platform as a Service (PaaS)

Platform as a service (PaaS) är en typ av metod för att kunna hyra olika molntjänster som exempelvis ett operativsystem, hårdvara eller lagring. Denna typ av tjänst skapar möjligheter för kunderna att på egen hand testa, utveckla och distribuera olika typer av IT-tjänster över till plattformen för molnet, men utan att ha kontroll över den underliggande strukturen (Singh, Jeong & Park 2016). Med andra ord är PaaS ett molnprogram som möjliggör en snabb och effektiv utveckling av webbapplikationer över internet genom att bortse från infrastrukturen och programvarans komplexitet, det kan underlätta om flera olika utvecklare befinner sig på olika platser och behöver samarbeta (Singh, Jeong & Park 2016). Modellen är ett hjälpmedel för företag som hyr virtuella IT-tjänster för att bevara eller skapa nya applikationer samt utveckla tjänster. PaaS är dessutom mellanprogrammet som levererar tjänsterna i form av utvecklingsverktyg (Iqbal et al.2016). PaaS säkerheten kan också äventyras där framförallt tiden då applikationen körs är mest kritisk och i kundens applikationsdistribution.

3.2.3 Software as a Service (SaaS)

Software as a service (SaaS) är en samling av flera fjärrdatortjänster (Singh, Jeong & Park 2016). Det är toppmodellen bland de tre tjänstemodellerna och denna etablerar applikationer samt affärsprocesser som bidrar till att kunder får tillgång till de molntjänster som återfinns i molninfrastrukturen. Denna typ av tjänst nås via exempelvis en webbläsare och installationer

som innefattar mjuk/hårdvara uppdateras regelbundet av dess leverantörer så att molntjänstanvändarna inte behöver hantera infrastrukturs designen.

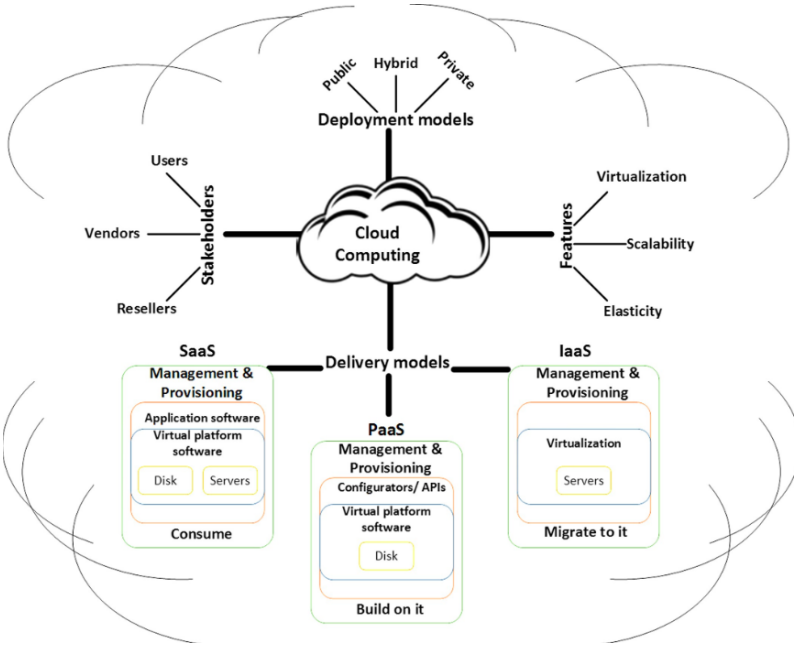

Bild 2 - illustration av Cloud computings koppling till leveransmodellerna (Iqbal et al. 2016)

3.3 Säkerhetskoncept

3.3.1 "CIA Triaden"

CIA triaden är ett uttryck när man talar om informationssäkerhet för att kunna hantera värdefulla informationstillgångar såsom hårdvara, data, information och resurser. CIA triaden innefattar att säkerhetsställa konfidentialitet, tillgänglighet och integritet (Warkentin & Orgeron 2020). Albuquerque et al. (2014) förklarar att konfidentialitet är informationssäkerhetens tillhörighet och bär ansvaret för att motverka oberättigat uppdagande av information. Det är en typ av process för att ge åtkomst till auktoriserade personer eller system i organisationer. Den applicerar olika principer för att säkerhetsställa sekretess för att tillgången till viktig information begränsas till endast de som behöver tillgång till den informationen. Konfidentialitet är den del av organisationens förmåga att tillhandahålla sin data, information och kunskap skyddade från obehöriga.

Tillgänglighet handlar om att varje del av informationen har ett specifikt värde eller användning och för att ett informationssystem ska tjäna sitt syfte bör information finnas tillgänglig vid behov. Albuquerque et al (2014) skriver att alla nätverk, databaser, informationssystem och andra informationstillgångar måste vara tillgängliga och ha godkänd åtkomst för att kunna hanteras när det behövs. Förlorad eller förstörd information är inte den enda informationen som är otillgänglig, om tillgång nekas för de som är behöriga att använda den, brister tillgängligheten och dess syfte. För att garantera tillgänglighet bör olika kommunikationskanaler användas för att få tillgång till information oavsett vart man befinner sig och dessutom ställer det krav på att det fungerar på ett korrekt sätt efter informationssäkerhetspolicyer berättar Albuquerque et al. (2014).

Integritet är den tredje och sista delen i CIA triaden, det handlar om färdigheten att kunna garantera att information och data är konsistens samt har en exakthet under hela livscykeln. Det innebär att information eller data inte på ett otillåtet sätt elimineras alternativt modifieras för att på så sätt stävja dess upptäckt. Det handlar också om garantin att informationen ska vara korrekt och därmed tillförlitlig, den får inte omarbetas av en obehörig part skriver Albuquerque et al. (2014). Integritet kan sammanfattas som den del av CIA triaden för hur information ska hanteras på ett säkert sätt, utan att de grundläggande egenskaperna hos informationen går förlorad.

3.3.2 Infrastruktursäkerhet

För att möjliggöra en stabil och säker infrastruktur för molntjänster krävs det att molnets fysiska och virtuella infrastruktur i första hand går att lita på. Som en molntjänstleverantör av tredje part är det nödvändigt att infrastrukturen intygas på de företag som använder dess tjänster, dock är detta inte tillräckligt för den kritiska affärsprocessen. Företag som erbjuder molntjänster måste på egen hand kunna verifiera affärskrav för att dess infrastruktur ska vara säker (Singh, Jeong & Park 2016). Enligt Kiraz (2016) måste de företag som tillhandahåller molntjänster till en början säkerhetsställa den så kallade fysiska hårdvaran samt se till att den berörda personalen är involverad i arbetet med den övergripande molnuppsättningen. Företagets uppgift som molnleverantör är dessutom att säkerhetsställa att det finns en begränsad åtkomst mot hårdvaran och data.

3.3.3 GDPR

GDPR (The General Data Protection Regulation) även kallat dataskyddsförordningen är en lagstiftning för att skydda enskilda personers friheter och rättigheter samt ett sätt att ställa hårdare krav på hantering av personuppgifter. Det bygger på sex rättsliga grunder som används inte endast används för behandling av personuppgifter utan också samtycke, avtalsskäl (bekräftelse av betalning) och legitima intressen (Harris, Samuel & Probert 2018). Enligt PWC (2022) ställs det idag högre krav för processer och rutiner gällande en säker hantering av register och krav som täcker ansvarig ledningsnivå. Den uppdaterade versionen av dataskyddsförordningen ska gälla för alla företag som hanterar eller sparar känslig eller personlig information om sina kunder eller anställda. Om ett företag ej skulle följa de riktlinjer som GDPR står för kan de riskera stora avgifter som en typ av böter mot brott. Under åren har kraven ökat, vilket innefattar anpassningsåtgärder som exempelvis krav på genomförande av konsekvensbedömningar, incidentrapporteringsrutiner och att samma hanteringsregler ska gälla för alla typer av personuppgifter som är ostrukturerade. Det innebär att de ska skapas ordning samt god kontroll över dessa och dessutom ett ändamålsenligt dataskydd. Med ett ändamålsenligt dataskydd kan man öka förtroendet hos sina kunder med en ökad transparens mot vilken information som hanteras (PWC 2022). Georgiopoulou, Makri och Lambrinoudakis (2020) förklarar att som molnleverantörer måste man kunna säkerhetsställa alla GDPR-principer gällande bland annat integritet, ansvarighet, lagringsbegränsning och många fler efterföljs. Därmed måste molnleverantörer följa alla de krav som principerna innebär för att få lagra känsliga eller personliga uppgifter, då det dessutom krävs att uppgifterna behandlas enlighet med lagkraven för att inte begå misstag som kan bli kostsamma för företaget.

3.3.4 Integritet

Dataintegritet blir allt mer viktigt i samband med molnlagringstjänster krävs det att man garanterar tillgängligheten och korrektheten hos den outsourcade data. Molnlagringstjänster har ett flertal säkerhetsproblem som gör molnet sårbart genom att äventyra dess integritet, konfidentialitet och tillgänglighet för data. Människor är medvetna om säkerhetsproblemen med att använda sig av molnet som en lagringstjänst och datasäkerheten är en av de faktorer som gör folk ovilliga att använda just den typ av tjänst. Integritet är en viktig del av datasäkerheten menar Alshaimaa, Nagwa och M.F (2016).

3.4 Fördelar med molntjänster

Enligt Baltatescu (2014) finns det flertalet fördelar med att använda sig av molntjänster istället för traditionella IT-tjänster som att hantera infrastruktur, system och nätverk på egen hand. Baltatescu (2014) tar upp följande fördelar:

- Skalbarhet, där tillgång till obegränsade datorresurser finns efter behov till exempel oändligt lagringsutrymme.
- Nytta, pay as you go modell där resurser matchas med behov på en löpande basis vilket innebär reducerade kostnader eftersom man enbart behöver betala för det som används.
- Snabb elasticitet/elasticitet, där förmågan att anpassa de rätta resurserna i rätt storlek efter behov samt att de sker snabbt och elastiskt.
- On demand-tjänster, att man kan komma åt molntjänster utan att ständigt behöva integrera med molntjänstleverantörerna.
- Tredjepartsleverantör, alla uppdateringar hanteras av tredjepartsleverantören, vilket innebär att företag inte behöver tänka på några installationer av hårdvara och mjukvara.
- Lätt åtkomst, tillgång till resurser i molnet är tillgängligt oavsett vart man befinner sig via internet.
- Tillgång till ett brett utbud av applikationer, man behöver inte ladda ner eller installera något på egen hand.

Utifrån dessa punkter som Baltatescu (2014) tar upp kan molntjänster sammanfattas som mer flexibla än traditionella IT-tjänster eftersom användarna endast betalar för de resurser som används, förmågan att anpassa resurser efter behov samt att uppdateringar hanteras av tredjepartsleverantör som medför en bekymmerslös användning av IT-tjänster.

3.5 Nackdelar med molntjänster

Enligt Grossman (2009) finns det inte bara fördelar med molntjänster utan det finns också nackdelar med att använda sig av molntjänster. Grossman (2009) tar upp följande nackdelar:

- Uppkoppling, eftersom molntjänster är en fjärrapplikation som behöver uppkoppling mot ett nätverk för åtkomst, kan de orsaka att åtkomstproblem om nätverksuppkoppling saknas.
- Flera användare samtidigt, kan skapa problem eftersom flera användare använder samma plattform vilket gör att ifall det blir problem med plattformen så påverkar det många användare samtidigt.

- Tredjepartsleverantör, att lagra data hos en molntjänstleverantör som blir en tredjepartsleverantör kan medföra säkerhetsrisker, svagheter och regelbundna problem som prestandaproblem.

Det är inte konstigt att det finns nackdelar med molntjänster eftersom det inte finns något som är perfekt och utan problem och brister. Flera användare samtidigt bidrar till att risken för problem är högre, eftersom en uppkoppling mot internet alltid krävs ställer det höga krav på att användarna har tillgång till säkra nätverksuppkopplingar. Att låta en tredjepartsleverantör vara ansvarig för hantering av data som till exempel viktiga uppgifter, är en av de största anledningarna till att inte använda sig av molntjänster och en av de viktigaste faktorerna som vägs in när övergång till molntjänster är de potentiella säkerhetsriskerna som finns.

3.6 Säkerhetsrisker i molnet

Det finns många säkerhetsrisker med att använda sig av molntjänster och ständigt hotas säkerheten för både företag som använder sig av molntjänster samt egna molntjänstleverantörer. Trots de flertalet säkerhetsåtgärder som finns för att motverka säkerhetsrisker mot molntjänster så ska det alltid tas i beaktning att ett system inte kan vara hundra procent säkert. Flertalet händelser och säkerhetsundersökningar har visat på att, trots nyuppfunnen teknik, så finns risken alltid att den kan vara felaktig på grund av mänskliga fel, menar Singh, Jeong och Park (2016). Enligt Patel och Alabisi (2019) är de vanligaste säkerhetsriskerna hos molntjänstanvändare generellt sett avslöjande av kommersiella hemligheter och potentiella driftstopp med inverkan på verksamheten, dessa risker går ej att undvika helt och det finns alltid en risk att det inträffar. Dessutom finns det alltid en risk att behörighetsstatusen för molntjänstleverantörerna ger upphov till oro över frågor som berör eliminering av företagsmigrering, skadeersättning och allmänna fel.

De vanligaste säkerhetsriskerna som molntjänstleverantörer har är försäkran om en långsiktig drift av molndatacentret, vilket innebär att man ska isolera de potentiella felen för att kunna minska/ minimera dess inflytande. En mycket vanlig säkerhetsrisk är de så kallade nätverkshackarna och molntjänstleverantörerna behöver skydd mot dessa då de kan vara många men också mycket aggressiva. Kundernas krav är viktiga för leverantörerna och därmed är behovet av effektivitet och säkerhet viktigt (Patel & Alabisi 2019).

3.6.1 DoS (Denial of Service) & DDoS attacker

Denial of service (DoS) eller distribuerade denial of service (DDoS) attack är ett säkerhetshot som förhindrar ett molns kapacitet från att kunna utföra de tjänster och funktioner de är menat för, detta framkommer genom ett skadligt beteende som hindrar molnet från sin fulla kapacitet. Syftet med dessa attacker är att attackera ett datasystem och blockera den normala användningen av själva systemet. Detta är en av de största säkerhetsriskerna då attackerna ofta kan påverka stora datasystem och alla anslutna datorer som är kopplade till de nätverket. Det sker många gånger att det blockeras data och dataöverföring samt att tillgängligheten av exempelvis molntjänster äventyras (Mohammad & Marzie 2016).

3.6.2 SQL- injection

SQL-injectionsattacker är enligt Masri och Sleiman (2015) ett sätt att kunna utnyttja sårbarheter i webbapplikationer för att kunna utföra skadliga SQL-kommandon. Detta sker genom en kodinjekttionsteknik som kan förstöra en hel databas och därmed klassas de som en av de vanligaste teknikerna för webbhackning samt en av de största säkerhetsriskerna mot en molntjänst. För att man ska kunna förstöra en databas krävs det att man infogar en skadlig SQL-sats i inmatningsfältet för exekvering och måste därmed utnyttja en säkerhetsspårbarhet i en programvara för en applikation som använder sig av en SQL-databas för att lyckas. Med en SQL-injektion kan hackern komma åt resurser för att kunna manipulera data, vilket innebär att personen i fråga kan få tillgång till känslig information som är viktig för företagen (Masri & Sleiman 2015).

3.6.3 Insider risker

Ofta när ett system utsätts för någon form av intrång eller attack brukar det många gånger anses vara någon från utsidan som hackar sig in berättar Duncan, Creese och Goldsmith (2014). Men det är inte så ovanligt att det visar sig vara någon som är betrodd av företaget, som företaget förlitar sig på, detta är en insider attack. En insider klassificeras som en nuvarande eller tidigare anställd som har eller har haft tillgång till en organisations system, nätverk eller data. Personen ska avsiktligt ha missbrukat denna åtkomst på ett sådant sätt att de har haft en negativt påverkande effekt på integritet eller tillgänglighet för organisationens information och informationssystem berättar författarna. En attack från insidan är oftast svårare att upptäcka och kan därmed vara betydligt skadligare än en attack från utsidan eftersom att insidern vet hur man ska göra för att risken att bli påkommen ska vara så liten som möjligt. De har koll på vilka säkerhetsåtgärder som finns och hur de ser ut, vilka motåtgärder som görs, vart allt känsligt material finns, medvetna om vilka tillfällen som är bäst att genomföra attacken och framförallt hur man ska ta sig ut. Duncan, Creese och Goldsmith (2014) förklarar att en insider attack är annorlunda eftersom de inte behöver attackera för att komma åt och få tillgång till systemen, de har redan full tillgång.

4 Resultat

I detta avsnitt avses att presentera en redogörelse för resultatet av den insamlade empirin från datainsamlingen. Resultatet kommer att delas upp i molntjänstleverantör och molntjänstanvändare.

4.1 Molntjänstanvändares perspektiv på säkerhet & risker

4.1.1 Respondent A

Respondent A tillhör ett stort företag som består av 13 olika bolag och i grunden är ett bolag som jobbar med IT och digitalisering, företaget har över 1500 anställda i hela koncernen. Respondenten som kontaktades och intervjuades är företagets CDO (Cheif digital officer). Verksamheten använder sig av till stor del av molntjänster i det dagliga arbetet och har flera olika system för företagets olika tjänster. Respondenten förklarade att i princip i hela koncernen använder sig av Microsoft 365 för att lagra sin information i molnet. CDO förklarar att molntjänster används till större del i bolagen där man bland annat använder sig av molntjänster för ärendehanteringssystem, rekryteringssystem, avtalshantering, kundundersökningar, fakturering och learning managementsystem. De använder sig även av Azure för att lägga upp servrar och liknande i molnet samt system som är baserade på Azure DevOps.

Enligt respondenten är den främsta anledningen till användningen av molntjänster är leveransmodellen, köper man en molntjänst har man alltid en uppdaterad produkt. Eftersom i molntjänsten har man alltid någon som ser till att man har kör senaste versionen, man har någon som är expert på den mjukvaran och driften, vilket gör att de troligtvis kommer vara tio gånger bättre än vad företaget själva någonsin kommer att kunna bli för att kunna driva deras egna applikation. Om det uppstår fel eller problem i något system så kommer någon att upptäcka detta och reagera väldigt fort, samt fixa det eventuella felet säkert istället för att respondenten själv behöver fixa det.

CDO fortsätter med att förklara att de till viss del har koll på säkerheten i företaget när de gäller molntjänster. Till exempel så kopplar de alla sina molntjänster till deras användarkatalog Azure active directory för att säkerhetsställa inloggning och utloggning. En annan del är att det inte går att veta vem som jobbar på andra sidan molntjänsten därför skrivs alltid avtal med leverantörerna om personuppgiftshantering enligt GDPR, men det går inte att veta att det följs fullt ut. Det kan ske hackerattacker på molntjänstens tjänst men gissningsvis kan leverantörerna paketera sin egen tjänst på ett säkrare sätt än om respondenten på egen hand skulle starta upp en drift av tjänsten, så totalt sett ser respondenten det som säkrare än att driva det i egen regi, men de kan aldrig bli hundra procent säkert.

Respondenten berättar att de ställer krav på sina molntjänstleverantörer att få skydd mot olika typer av intrång. Ifall till exempel någon försöker kryptera respondentens data så skall leverantörerna se till att det finns backups för att kunna återställa data. Däremot om det skulle ske att någon får tag i personuppgifter eller annan känslig information som skulle komma på drift så finns det en krishanteringsplan beroende på karaktären på krisen. CDO berättar att vissa saker inte går att reparera utan det handlar i så fall om att försöka minimera skadan så mycket som möjligt. Den första typen av händelse kan vara att informationen i systemet ändras och det är inte självklart att man ser detta eftersom data manipuleras som inte syns eller saknar åtkomstskydd vilket kan bli dumt. Till exempel om intressenter har medarbetarundersökningar

och någon fipplat med uppgifterna vilket gör att de inte blir pålitliga samt att förtroendet kan bli bristande vilket inte är bra.

Om något inträffar gällande säkerheten i molntjänsterna som respondenten använder så ska de enligt avtal bli informerade av leverantör. Det ser lite olika ut från leverantör till leverantör när det gäller hur respondenten blir informerad, till exempel de större leverantörer som Microsoft så skickas det ut ett standardmail som är opersonligt, medan med mindre molntjänstleverantörer sker kommunikationen mellan person till personkontakt.

CDO anser att de största säkerhetsriskerna med molntjänster är läckage av personuppgifter då de kan orsaka höga böter både för molntjänstleverantören och för respondenten. Dessutom är finansiellt känslig information dåligt att tappa dock beror allt på tjänsten av vad som är hög och låg risk, men att tappa data som inte går att återskapa och att personuppgifter sprids är de största riskerna med molntjänster. När det gäller åtgärder mot säkerhetsrisker i molntjänster förklarar CDO att de granskar leverantörerna innan de tar ombord dem och använder sig också av säkerhets premisser där de kollar hur de punkterna granskas och följs upp. Skulle det vara riktigt känslig information ser de till att ta backup av själva molntjänsten och även i vissa fall ta de separata backups till exempel om en leverantör skulle gå i konkurs.

Det skiljer sig mellan större och mindre leverantörer av molntjänster kring planen om något inträffar där till exempel Microsoft och Google arbetar med schemalagda procedurer vilket gör att respondenten har en liten påverkan på hur man ska arbeta. Däremot hos de mindre molntjänstleverantörerna har man en större påverkan, mer flexibilitet och det finns en bättre möjlighet till att få sin egen information upp prioriterad vid ett eventuellt läckage berättar respondenten. Säkerheten ligger högt i prioritet när det gäller molntjänster som hanterar känslig information men det är alltid en avvägning mellan säkerhet och funktionalitet. Respondenten förklarar att vissa system väljer de att inte ha molntjänster för att det inte är förenligt med den risken som finns, exempelvis deras lönesystem, som de lagrar informationen i egna lokala servrar.

En annan viktig sak som är relaterad till säkerheten när man skaffar molntjänster är det viktigt att koppla de mot en gemensam katalog av användare som behörighetstjänst berättar respondenten. Detta för att undvika problem med att när folk slutar på företaget så behöver man inte avaktivera konton i alla olika molntjänster, vilket är lätt att missa när någon slutar. Annars finns risken att personer sitter på behörigheter som de inte bör ha, vilket är en viktig faktor att tänka på för att se till att man har kontroll på behörigheten till systemen.

4.1.2 Respondent B

Respondent B tillhör ett stort företag som har cirka 100 000 anställda inom produktion, försäljning och finansiella tjänster. Respondenten som kontaktades och intervjuades arbetar på företaget som Enterprise IT Security Compliance Awareness. Verksamheten som respondent B arbetar på använder molntjänster i omfattande drag, dels som ersättning för gamla tjänster och nya behov och i stora drag inom alla typer av verksamhetsområden. Respondenten förklarar att företaget arbetar med molntjänster för att de anser att det dels är billigare men också effektivare än att etablera egna tjänster med tillkommande infrastruktur.

Respondenten berättar att företaget använder sig av alla typer av molntjänster där Software as a service, Infrastructure as a service och Platform as a service används genom ett hundratal

olika molntjänstleverantörer. Vidare förklarar respondenten när det gäller insyn kring säkerheten att företaget anser att de har en bra insyn i molntjänsternas säkerhet. Vidare berättar respondenten att de ställer olika höga krav på molntjänsterna de använder beroende på hur högt informationsvärdet är som de lagrar i molntjänsten. Desto högre värde av informationen, desto högre krav ställs på säkerheten i molntjänsten. Om det inträffar något som äventyrar säkerheten i molntjänsterna som de använder styrs åtgärder av de avtal man skrivit med molntjänstleverantören.

Om något inträffar med företagets uppgifter eller liknande i molntjänsterna så står det alltid i avtalet när och hur de vill bli informerade av molntjänstleverantören berättar respondenten. Beroende på naturen av känslighet på informationen som molntjänstleverantörerna hanterar så varierar sättet som de blir informerade på förklarar respondenten. När det kommer till säkerhetsrisker så berättar respondenten att de anser att säkerhetsriskerna i stort sett är detsamma som om man hanterar informationen själv, men att de inte har samma fulla kontroll vid användande av molntjänster. Säkerhetsriskerna varierar beroende på vad för typ av information som molntjänsten hanterar. Respondenten berättar också att det kan vara olika typ av känslighetsgrad på uppgifterna som lagras i molntjänsten, men att information som innehåller känsliga uppgifter om företaget eller till exempel kunder är inte alls bra om det skulle äventyras.

När det kommer till åtgärder kring säkerhetsriskerna handlar det om att försäkra sig om att leverantörerna följer de krav som respondenten har. Det försäkrar sig om detta via att använda sig av frågeformulär, utvärderingar och tillslut via avtalsformulär för att försäkra sig om att leverantören har förstått och har intentionen att följa de krav som respondenten ställer. Det lägger också stor vikt vid att de molntjänstleverantörer som används är säkerhetscertifierade berättar respondenten. Respondenten berättar också att alla tillgängliga åtgärder utförs när det kommer till säkerhetsrisker, men att det samtidigt inte innebär att alla tänkbara åtgärder tilltas. Det finns fall då leverantören inte går med på alla tänkbara åtgärder och det kan innebära för respondenten att acceptera säkerhetsluckor i molntjänsten för att uppnå funktionella fördelar som lösningen ger.

Respondenten förklarar att de kräver att molntjänstleverantörerna har en plan ifall något skulle inträffa i någon form av intrång eller läckage och att det kräver det för att teckna avtal med en leverantör. Men samtidigt berättar respondenten att det inte i samtliga fall kan visa att de har en fungerande plan i praktiken, om leverantören inte har en tredje part som kan bevisa detta i form av exempel en certifiering som är en viktig faktor. Kraven på planen ser olika ut beroende på vilken tillgänglighet som respondenten behöver, men att de arbetar enligt de avtal som skrivs med leverantören. Respondenten berättar att säkerheten är mycket viktig men att planer kring åtgärder inte lämnas ut på grund av säkerhet, samt erfarenhet kring intrång inte är officiell information.

4.2 Molntjänstleverantörers perspektiv på säkerhet & risker

4.2.1 Respondent C

Respondent C tillhör ett medelstort företag i Sverige som arbetar som molntjänstleverantör genom att tillhandahålla molnlagring och arkivering av filer samt data på ett säkert sätt i servrar placerade i Sverige. Bolaget inriktar sig på svenska företag och lyder under svensk lagstiftning, vilket gör de enklare för svenska företag när de gäller bland annat GDPR. Först kontaktades företagets VD som vidarebefordrade frågorna som ställdes till den IT-ansvarige på företaget. Respondenten började med att förklara att de utvecklar all programvara på egen hand som körs på deras backend och i utvecklingsarbetet där säkerhetsaspekten är av högsta prioritet. Respondenten berättar att driften och produktionsmiljön har en så begränsad åtkomst till som möjligt där endast tre personer på företaget har åtkomst och de har genomgått en noga bakgrundskontroll med bland annat utdrag ut brottsregistret.

IT-ansvarig på företaget förklarar att det finns en plan om något skulle inträffa eller störa säkerheten, dock är detta sekretessbelagt och de delar ej med sig kring dess detaljer. Däremot känner de ett enormt ansvar för den data som deras kunder valt att anförtro att lagra i dess molntjänster hos företaget. Företagets lägger störst vikt på dess kunder och att de ska kunna känna sig helt säkra med sin lagring av data hos företaget berättar respondenten. För att uppnå integritet hos sina kunder anpassar företaget sitt arbetssätt utifrån GDPR och har en utpekad Data Protection Officer som ansvarar för att bevaka kundernas uppgifter samt hantera dem på ett korrekt sätt med full integritet.

Respondenten påstår att de största säkerhetsriskerna som de upplever som molntjänstleverantör är att personalen som jobbar med de olika tjänsterna om de skulle utsättas för påtryckningar av olika slag, genom exempelvis hot riktad mot den lagrade informationen. DDoS-attacker är en annan säkerhetsrisk företaget står inför, då de påverkar tillgängligheten av data. Företaget hanterar på egen hand all sin infrastruktur, inklusive brandväggar så att de kan ha full kontroll på tillgången av deras miljö, menar IT-ansvarig. De åtgärder som vidtas av molntjänstleverantörer inför de olika säkerhetsriskerna är regelbunden testning och årliga säkerhetstester av dess tjänster av extern part. Om testerna visar några risker eller brister så åtgärdas de direkt, där åtgärden beror på naturen av risken.

Respondenten berättar att kunderna hanterar sin lagrade information via företagets webbgränssnitt eller via någon av företagets klienter. Kunderna har full kontroll på sin lagrade information, men bär inte ansvar för säkerheten. Respondenten förklarar att det är CTO på företaget som är ansvarig för säkerheten, men att det yttersta ansvaret bärs av företagets VD. Respondenten berättar att den största utmaningen ur säkerhetssynpunkt är intrångsförsök och de kommer förmodligen att öka i framtiden, vilket gör att där kommer det krävas att vara extra vaksam framöver.

4.2.2 Respondent D

Respondent D tillhör ett stort företag i Norden med över 600 anställda som arbetar med digitaliserings- och molnlösningar i Sverige, Norge, Danmark och Finland. De arbetar med att digitalisera och utveckla affärsprocesser via databaserat beslutsfattande och säkra molntjänster. Respondenten började med att förklara att de är 100% Microsoft partner och att de levererar tjänster inom alla de tre molndelarna inom Microsoft som är Azure, Modern Workplace och Dynamics. Respondenten arbetar i en affärsenhet med tre fokusområden som är Data & Analytics, Cyber Security och Cloud Infrastructure. Respondenten förklarar att företaget har en specifik säkerhetsavdelning som arbetar internt på företaget, men också externt ute hos deras kunder. Vidare förklarar respondenten att de utnyttjar Microsofts molnteknik, men har ett eget security operation center som sitter och övervakar i realtid ifall det sker incidenter som stör säkerheten.

Vidare berättar respondenten om hur deras arbete med integritet gentemot deras kunder ser ut, där deras mål är att agera trusted advisor för deras kunder genom att utgå ifrån kundernas behov och därigenom föreslå lösningar som åstadkommer så högt värde som möjligt för de. Arbetet kring säkerhetsrisker som leverantör innebär att den rätta tekniken måste finnas på plats som hjälper, men enligt respondenten handlar de till största delar att den egna personalen utgör den största säkerhetsrisken. Därför anses utbildning inom säkerhetsfrågor hos personalen på företaget vara något av det viktigaste som de prioriterar. När det gäller åtgärder mot säkerhetsrisker så förklarar respondenten att de rekommenderar sina kunder att använda Microsofts flora av produkter för att ha bästa möjliga förutsättningar som rör åtgärder mot säkerhetsrisker framåt.

Åtgärder som företaget gör mot säkerhetsrisker är att de arbetar med security assessments för att göra så kallade genomlysningar av kundföretagens status och ger rekommendationer utifrån dessa genomlysningar. Respondenten förklarar också att dialogen med leverantören är viktig för att säkerhetsställa att de produkter som finns för åtgärder mot säkerhetsrisker används i full utsträckning. Vidare lyfter respondenten fram hur kundernas kontroll av molnet ser ut där landskapet är komplext och därav finns många aspekter att se över som kund. Därför får kunderna som företaget hanterar en inbyggd governance, säkerhetsstruktur med tillhörande processer berättar respondenten. När det avser vem som bär ansvaret för brister i säkerheten i molntjänsterna så säger respondenten att det företag som tillhandahåller infrastrukturen bär det största ansvaret kring säkerheten. Till exempel om man outsourcar sin miljö ligger oftast huvudansvaret hos den leverantören förklarar respondenten.

5 Analys

I detta avsnitt avses att analysera data från den insamlade empirin tillsammans med teori (litteratur) för att finna samband mellan säkerhet och säkerhetsrisker.

5.1 Öppen kodning av molntjänstanvändare

5.1.1 Användandet av molntjänster

Både respondent A och B använder sig av molntjänster i sitt dagliga arbete och det används i hela verksamheten, dock förklarar de på olika sätt hur arbetet med molntjänsterna ser ut. I verksamhet A använder man sig av flera olika system för företagets olika tjänster där i princip hela koncernen använder sig av Microsoft 365 för att lagra sin information i molnet. De använder också molntjänster för att lägga upp servrar och liknande, men även till större del av sina system som till exempel ärendehanteringssystem, fakturering och rekryteringssystem använder sig av molntjänster. Respondent B använder sig av alla typer av molntjänster där Saas, Iaas och Paas används via ett hundratal olika molntjänstleverantörer. Enligt respondent B använder de sig av molntjänster dels för att ersätta gamla tjänster, men också för nya behov inom alla typer av verksamhetsområden. Motivering till användning av molntjänster är att det framförallt är effektivare än att etablera egna tjänster, men samtidigt anses det också vara billigare. Verksamhet A förklarar att den främsta anledningen till användning av molntjänster är leveransmodellen som innebär att man alltid har en uppdaterad produkt. I molntjänsten finns det alltid någon som sköter uppdatering för att alltid köra senaste versionen, men också någon som är expert på mjukvaran och driften, vilket förhoppningsvis kommer vara tio gånger bättre än vad verksamhet A någonsin kommer kunna bli för att driva sin egen applikation.

5.1.2 Krav på säkerheten

Respondent A skriver avtal med sina molntjänstleverantörer om personuppgiftshantering enligt GDPR, eftersom man aldrig vet vem det är som jobbar på andra sidan av molntjänsten. Detta är ett av de kraven som ställs mot leverantörerna. Respondent A ställer krav på sina leverantörer för att få skydd mot olika typer av intrång, exempelvis mot kryptering av data så ska leverantörerna ha backups för att kunna ersätta data. Verksamheten har en så kallad krishanteringsplan utifall att någon skulle få tag i personuppgifter eller annan känslig information och denna plan är beroende av karaktären på krisen. Verksamheten för respondent B arbetar istället genom att ställa olika höga krav på molntjänsterna som de använder och detta grundar sig i hur högt informationsvärdet är på den lagrade informationen i tjänsten. Om informationsvärdet är högre ställs högre krav på säkerheten och om något skulle äventyra säkerheten finns det avtal med molntjänstleverantören.

5.1.3 Säkerhetsrisker för molntjänstanvändare

Respondent A anser att de största säkerhetsriskerna för verksamhet A är att läckage av personuppgifter skulle ske och föra med sig höga böter både för verksamhet A och molntjänstleverantören. Även finansiellt känslig information är viktigt att det inte läcker ut och att förlora data som inte skulle kunna gå att återskapa eller få tillbaka på något sätt är också en stor säkerhetsrisk. Respondent A lyfter dessutom hackerattacker, insider risker eftersom man aldrig kan veta vem som arbetar på andra sidan av molntjänsten samt felaktig behörighet vid till exempel avslutad tjänst som möjliga säkerhetsrisker för verksamheten. Respondent B anser att de gäller säkerhetsrisker för verksamhet B så är det i stort sett samma som om Verksamhet B skulle hantera informationen själva, men att det dock tappar den fulla kontrollen vid användandet av molntjänster. Säkerhetsriskerna varierar för vilken typ av information som den specifika molntjänsten hanterar och för verksamhet B varierar känslighetsgraden på den informationen som lagras i molntjänsterna, men att känslig information om kunder eller om företaget skulle läcka ut anses vara en av de största säkerhetsriskerna

5.1.4 Åtgärder mot säkerhetsrisker

Respondent A förklarar att de åtgärder de vidtar mot säkerhetsrisker är till en början en granskning av deras leverantörer och sedan ett flertal säkerhets premisser. För att förebygga arbetet mot säkerhetsrisker är en åtgärd att ta backup på känslig information, både för molntjänstleverantören och separata backups för företaget själva utifall leverantören skulle gå i konkurs. Respondent B arbetar istället med kraven mot leverantörerna där det handlar om att försäkra sig att de följs genom frågeformulär, utvärderingar och avtalsformulär. För det första måste molntjänstleverantörerna vara säkerhetscertifierade. Här menar respondent B att man i förtid måste bestämma vad för tillgängliga åtgärder som ska vidtas vid inträffandet av säkerhetsrisker för molntjänster. Dock innebär detta inte att alla tänkbara åtgärder kommer vidtas på grund av molntjänstleverantören, då respondenten menar att man får acceptera säkerhetsluckor för molntjänsten för att kunna uppnå funktionella fördelar för åtgärden.

5.1.5 Plan för säkerheten

Planen för om något skulle inträffa kring säkerheten i molntjänster för respondent A beskrivs skilja sig mellan större och mindre leverantörer, där de större leverantörerna har schemalagda procedurer som verksamhet A har liten påverkan på. Hos de mindre molntjänstleverantörerna arbetar man mer nära inpå och där finns en större flexibilitet och möjlighet till att få verksamhet A information upp prioriterad vid eventuella läckage eller intrång. Hos verksamhet A ligger säkerheten som en hög prioritet hos de molntjänster som hanterar den mest känsliga informationen, men det är alltid en avvägning mot funktionaliteten för att hitta den lämpligaste lösningen. Respondent B förklarar att de använder sig av tecknade avtal mellan de som verksamhet och molntjänstleverantören. Planen står för om något skulle inträffa med säkerheten för molntjänsten, såsom intrång eller läckage. Respondenten menar att planen nästan aldrig fungerar i praktiken om leverantören inte har en tredje part som kan bevisa detta i form av en certifiering, som är en viktig faktor. Kraven på en fungerande plan varierar beroende på tillgängligheten av informationen i molntjänsten och detta står också i deras avtal hur det ska fungera.

5.2 Öppen kodning av molntjänstleverantör

5.2.1 Hur ser arbetet ut som molntjänstleverantör

Både respondent C och D är molntjänstleverantörer, men de arbetar på två olika sätt. Respondent C utvecklar sin egen programvara som körs via deras backend och i deras utvecklingsarbete är alltid säkerhetsaspekten prioritet ett. Medan respondent D är en 100% Microsoft partner och levererar tjänster via Microsofts tre molndelar som är Azure, Modern Workplace och Dynamics.

5.2.2 Plan för säkerheten

Respondent C har en egen plan för om något skulle störa säkerheten som de själva tagit fram och utgår ifrån men inga specifika detaljer utelämnades. De känner ett enormt ansvar för den data som deras kunder anförtror de med och är därmed viktigt att deras kunder ska kunna känna sig helt säkra med att sin data hos respondent C. Medan respondent D har en egen säkerhetsavdelning som jobbar internt med säkerhet och externt hos kunder. De använder sig av Microsofts molnteknik men har en egen Security Operation Center som sitter och övervakar incidenter i realtid.

5.2.3 Arbetet med integritet

Det skiljer sig hur de två olika företagen arbetar med integritet för deras kunder. Respondent C arbetar mot GDPR och anpassar sitt arbetssätt utifrån de förhållningsregler som finns. De har också en vald person som ansvarar för att bevaka kundernas uppgifter så att de hanteras korrekt med full integritet och denna personen kallas för Data Protection Officer. Respondent D arbetar som en trusted advisor till sina kunder och istället utgår från kundens behov samt föreslår olika lösningar som skapar värde för kunderna på bästa sätt.

5.2.4 Säkerhetsrisker som molnleverantör

Den största säkerhetsrisken som molntjänstleverantör står inför är enligt båda respondenterna den personal som arbetar på företaget. Respondenterna berättar att personal kan utsättas för påtryckningar utifrån när någon vill komma åt lagrad information i deras molntjänster. Utbildning av personal inom säkerhetsfrågor anses vara viktigt av respondent D, medan respondent C arbetar med att så få personer som möjligt ska ha tillgång till alla data som företaget hanterar i deras molntjänster. Respondent D säger att teknik mot säkerhetsrisker också måste vara på plats för att kunna säkerhetsställa säkerheten. Respondent C förklarar att risken att bli utsatt för olika typer av hackerattacker är stor exempelvis DDoS-attacker, eftersom de på egen hand hanterar all infrastruktur, inklusive deras brandväggar, så att de får full kontroll på tillgången av deras miljö. Respondent C berättar att de i framtiden kommer att vara med tanke på världsläget, intrångsförsök som kommer att öka och att där måste man vara extra vaksam framöver som molntjänstleverantör.

5.2.5 Åtgärder mot säkerhetsrisker

Respondent C berättar att de regelbundet själva bedriver tester mot säkerhetsrisker och årligen utförs säkerhetstester av en extern part. Skulle några risker mot säkerheten framkomma under dessa tester åtgärdas de direkt och åtgärden beror på naturen av risken, men respondenten vill inte gå in på några detaljer. Medan Respondent D använder sig av Microsofts flora av säkerhetsprodukter som de sedan rekommenderar till sina kunder att använda för att ha bästa möjliga förutsättningar mot säkerhetsrisker. De har även en dialog mellan sig och Microsoft för att säkerhetsställa att alla tjänster mot säkerhetsrisker används. Respondent D arbetar även med något som de kallar security assessments för att kunna genomföra analyser av företags säkerhetsstatus och ger rekommendationer på åtgärder utifrån de.

5.2.6 Kundernas kontroll i molnet

Kundernas kontroll skiljer sig mellan molntjänstleverantörerna där respondent C berättar att kunderna kan hantera all sin lagrade information via webbgränssnittet eller via någon av deras klienter. Kunden får därmed full kontroll på sin lagrade information säger respondent C. Medan Respondent D förklarar att det är svårt att svara i kundens vägnar eftersom landskapet i molnet är komplext och många aspekter behöver ses över. Men kunderna får en inbyggd governance och säkerhetsstruktur med tillhörande processer.

5.2.7 Ansvaret för säkerheten

Ansvaret för om brister sker i säkerheten konstaterar både respondent C och D att det är företaget som äger infrastrukturen som står som ansvarig ifall det händer något. Respondent specificerat sig och påstår att chief technology officer (CTO) på företaget är ansvarig för säkerheten men att de i första hand alltid är VD.

5.3 Axial kodning säkerhet molntjänster

5.3.1 Molntjänstanvändare

Respondent A förklarar att samarbetet med molntjänstleverantörer kan ibland vara komplicerat eftersom man inte vet vem som befinner sig på andra sidan “skärmen”. Därmed använder verksamheten avtal utifrån GDPR om uppgiftshantering och det är ett av de krav företaget ställer på leverantören. Enligt Harris, Samuel och Probert (2018) har kraven för uppgiftshantering ökat och ett ändamålsenligt dataskydd har införts för att kunna öka förtroendet för sina kunder, vilket respondent A kräver av sin leverantör. Respondent A menar att detta också ska skydda mot möjliga hot och att dessa avtal existerar på grund av att det alltid ska finnas backups och leverantörerna måste följa dataskyddslagen utifrån GDPR för att kunna hantera alla typer av känsliga eller personliga uppgifter (PWC 2022).

Grossman (2009) uppskattar det som respondent A menar att relationen till molntjänstleverantören kan vara komplicerad. Eftersom en tredjepartsleverantör som ansvarar för lagrade data kan medföra säkerhetsrisker, regelbundna problem för prestandan och generella svagheter för företaget, vilket respondent B ser på annorlunda. Respondent B menar att om leverantören har en certifiering som tredjeparts bör leverantören kunna leverera en fungerande

plan för säkerheten och att detta varierar beroende på tillgängligheten av informationen i molntjänsten. De säkerhetsproblem i molntjänster som kan orsakas av tredjepartsleverantörer kan göra molnet sårbart genom att äventyra dess integritet, konfidentialitet och tillgänglighet för data och datasäkerheten kan saboteras (Alshaimaa, Nagwa & M.F 2016).

Respondent B arbetar genom att ställa krav utifrån hur högt informationsvärde informationen har som de vill lagra i molntjänsten. Det innebär att lägre informationsvärde kan få till följd att funktioner och tillgänglighet i molntjänsten prioriteras högre än säkerheten hos respondent B. Enligt CIA triaden är tillgänglighet en av de viktiga aspekterna när det kommer till informationssäkerhet (Albuquerque et al. 2014). Det handlar om att informationen har ett specifikt värde eller användning och därmed för att molntjänsten ska tjäna sitt syfte krävs att informationen finns tillgänglig vid behov. För respondent A prioriteras också säkerheten högre hos de molntjänster som hanterar känslig information, medan en avvägning görs mot funktionalitet för att hitta den bästa lösningen när säkerheten inte har lika hög prioritet. Enligt CIA triaden är inte bara förlorad eller förstörd information den enda information som är otillgänglig, utan det handlar också om att informationssystem och informationstillgångar ska finnas tillgängliga med godkänd åtkomst för att ha möjlighet att hanteras när det behövs. Detta lägger både respondent A och B vikt vid när avtal med en ny molntjänstleverantör ska skrivas, avvägning mellan säkerhet och tillgänglighet är något som blir en vågskål när molntjänstleverantör ska väljas.

5.3.2 Molntjänstleverantör

Det skiljer sig hur de två olika företagen arbetar med integritet för deras kunder. Integritet är enligt Alshaimaa, Nagwa och M.F (2016) mycket viktigt i samband med molnlagringstjänster och det krävs att man garanterar tillgängligheten och korrektheten hos den outsourcade datan. För att uppnå detta arbetar respondent C företag mot GDPR och anpassar sitt arbetssätt utifrån de förhållningsregler som finns. Harris, Samuel och Probert (2018) skriver att GDPR är en lagstiftning som har tagits i bruk för att kunna skydda personuppgifter, i detta fall för kunder och anställda på företag. Respondent C har därför tillsatt en person som de kallar för Data Protection Officer som har ansvaret att se till så deras kunders personuppgifter hanteras på ett korrekt sätt med full integritet för att följa de riktlinjer som GDPR står för. Eftersom GDPR är en lag där företag som sparar eller hanterar känslig eller personlig information om sina anställda och kunder, så är det viktigt att göra det på ett korrekt sätt för att inte riskera att bryta mot lagen och därmed löpa fara för stora böter. Respondent D arbetar istället med att rådgiva sina kunder efter deras behov för att bygga lösningar som skapar det högsta värdet för kunden, detta eftersom företaget är en partner till Microsoft och i detta fall är det Microsoft som bär ansvaret för säkerheten, GDPR samt integriteten för kunder och anställda.

Båda respondenterna som representerar molntjänstleverantörer redogör att ansvaret för de brister som inträffar med säkerheten är det företaget själva som ansvarar ifall det händer något, eftersom de äger infrastrukturen och är därmed ansvariga. För att företagen ska kunna uppnå en säker infrastruktur krävs det enligt Singh, Jeong och Park (2016) att man kan lita på den virtuella och fysiska infrastrukturen samt intyga detta för användarna, vilket båda respondenterna ständigt arbetar med att uppnå. Respondenterna C och D är tredjepartsleverantörer inom bland annat molntjänster och deras uppgift enligt Kiraz (2016) är att säkerhetsställa att åtkomsten är begränsad mot data och hårdvara, exempelvis så är det endast tre personer på respondent C företag som har åtkomst till detta.

5.4 Axial kodning säkerhetsrisker

5.4.1 Molntjänstanvändare

Både respondent A och B anser att den största säkerhetsrisken vid användningen av molntjänster är läckage av personuppgifter, information och känsliga företagsuppgifter, samt insider risker. Eftersom det inte går att veta vilka de anställda hos molntjänstleverantören är, kan man inte veta vilka som jobbar på andra sidan och därmed finns risken för att någon på insidan utnyttjar tillgången till känslig information. Som Patel och Alabisi (2019) skriver så är en av de vanligaste säkerhetsriskerna för molntjänstanvändare att kommersiella hemligheter blir avslöjade. Denna risk är något som aldrig går att undvika helt för molntjänstanvändare, som respondent A och B säger är det just insider risken som är den svåraste att kontrollera och därför är behörighetskontroll något som är viktigt. Respondent A menar på att det är viktigt att kontrollera behörigheten till molntjänsterna som företaget använder. Om en anställd slutar till exempel är det viktigt att följa upp så att den personen inte längre har behörighet till att komma åt känslig information.

Duncan, Creese och Goldsmith (2014) pratar om insider risker där det handlar om att en person avsiktligt har missbrukat sin åtkomst som sedan påverkar integriteten eller åtkomst av molntjänstanvändarnas information och informationssystem. Insiderattacker är annorlunda mot andra säkerhetsrisker eftersom en attack för att komma åt och få tillgång till system inte behövs, de har redan full tillgång vilket gör att det är svårare att försvara sig mot samt upptäcka en insiderattack. Därmed är det svårt för företag som respondent A och B tillhör att vara medvetna om vad som pågår och vad de egentligen utsätts för. Den mänskliga faktorn är det som påpekas då vara den största risken som respondent A och B nämner, men även Singh, Jeong och Park (2016) rapporterar om att flertalet händelser och säkerhetsundersökningar har visat på att även om tekniken utvecklas och blir bättre, så kommer det alltid att finnas en risk att den är felaktig på grund av mänskliga misstag.

Respondent A påpekar också säkerhetsrisken för att drabbas av andra hackerattacker, dock via molntjänstleverantören där de lagrar information. Singh, Jeong och Park (2016) förklarar att dessa typer av hackerattacker mot de tjänster som företaget använder begränsar användningen av dem och att det ständigt hotar säkerheten. Därmed är det viktigt för företag som använder sig av molntjänster från en tredje part att skriva avtal, då man ännu en gång aldrig vet vem som arbetar på andra sidan av molntjänsten, menar respondent A. Respondent B påstås inte se detta som en stor säkerhetsrisk för verksamheten, då respondenten litar på de certifierade tredje part leverantörerna på grund av avtalen och anser att företaget på egen hand inte hade kunnat hantera molntjänsterna bättre än vad molntjänstleverantörerna gör.

5.4.2 Molntjänstleverantör

Patel och Alabisi (2019) menar att den vanligaste säkerhetsrisken som molntjänstleverantör står inför är försäkran om en långsiktig drift i molncentret eller nätverkshackarna som molntjänstleverantörerna är i behov av ett stabilt skydd från. Enligt båda respondenterna är den största säkerhetsrisken som en molntjänstleverantör står inför, personalen på deras respektive företag. Respondenterna berättar att personal kan utsättas för påtryckningar utifrån när någon vill komma åt lagrad information i deras molntjänster. Teorin stämmer här inte överens med hur det fungerar på respondenternas företag, dock menar Singh, Jeong och Park (2016) att ett flertal av de säkerhetsrisker som generellt sätt gäller för molntjänster är grundade av mänskliga

fel. Respondent C förklarar också att risken att bli utsatt för olika typer av hackerattacker är stor där DDoS-attacker tas upp. Eftersom företaget som respondent C arbetar på, hanterar på egen hand all infrastruktur och brandväggar, så skapar de full kontroll på tillgången av deras miljö. Enligt Mohammad och Marzie (2016) är en DDoS en attack som ska förhindra ett molns kapacitet för att kunna utföra de tjänster som finns. Med denna typ av attack kan personen i fråga påverka hela datasystemet och blockera en hel del data och för företag såsom respondent C arbetar på är detta en stor säkerhetsrisk då de hanterar allt inom systemet och datamiljön på egen hand.

Respondent C berättar också om framtiden hur säkerhetsrisker kommer att se ut med tanke på världsläget, där nämns att intrångsförsök kommer att öka och man kommer behöva vara extra vaksam där framöver som molntjänstleverantör. SQL-injectionsattack är en sån form av intrångsförsök som är och kommer vara av de största säkerhetsriskerna mot molntjänster berättar Masri och Aleiman (2015). Genom en SQL-injektion kan man komma åt resurser för att kunna manipulera data och därmed också få tag i känslig information som är viktig för företagen. Även tidigare nämnda DoS/DDoS- attacker, där syftet är att skada och blockera den normala användningen av molntjänster. Detta är också en form av intrångsförsök som respondent C och andra molntjänstleverantörer behöver vara vaksam inför.

6 Diskussion

I detta avsnitt avses att diskutera och reflektera kring den analys som gjorts bestående av insamlad empiri och tidigare forskning.

Beckers et al. (2013) beskriver i sin tidigare studie att molntjänster har en benägenhet att ha lägre förtroende för säkerheten eftersom företag utelämnar kontrollen av lagring och hantering av data till ett utomstående företag. Därav finns ett stort behov hos molntjänstleverantörer att försäkra sina kunder att det är säkert att utelämna hantering av data, lagring samt känsliga IT-processer till en molntjänstleverantör. Även Iqbal et al. (2016) lyfter fram i sin studie att integritet och säkerhet ses som kritiska delar inom molntjänster, där flertalet säkerhetsfrågor kring datasäkerhet bör belysas. Detta är en uppfattning som den insamlade empirin också delar med den tidigare forskningen som gjorts. Empirin visar på att säkerheten hos molntjänstanvändare och molntjänstleverantörer är en av de mest kritiska faktorerna som de arbetar med, där molntjänstanvändarna beskriver att säkerheten är av komplex karaktär. Som molntjänstanvändare vet man aldrig vem som jobbar på andra sidan molntjänsten och i empirin framkommer det att molntjänstanvändarna därav ser till att skriva avtal som följer GDPR för att säkerhetsställa att all hantering av känsliga eller personliga uppgifter sker på ett korrekt sätt. Komplexiteten ligger i att hela tiden avgöra hur mycket säkerheten ska prioriteras kontra funktionaliteten och tillgänglighet i molntjänsten, där visar empirin att detta blir en vågskål när val av molntjänstleverantör ska göras. Just tillgängligheten är också en säkerhetsaspekt där Albuquerque et al. (2014) förklarar att tillgänglighet är en viktig del i informationssäkerheten för molntjänster, eftersom information som lagras i molntjänsten kan inneha ett värde eller användning som för att kunna tjäna sitt syfte krävs det att tillgängligheten alltid är befintlig.

Empirin visar att molntjänstleverantörerna arbetar med att anpassa sitt arbetssätt utefter de förhållningsregler som finns där GDPR är en av de viktigaste att förhålla sig till. De skyldigheter som kommer med dataskyddsförordningen är både utmanande och omfattande, kraven på molntjänstleverantörerna blir också höga på grund av de konsekvenser och följder som kan inträffa om lagen inte följs. Empirin visar att det är mycket viktigt för molntjänstleverantörerna att följa den för att inte riskera att bryta mot lagen och därmed påföljderna av det. Vidare visar empirin också att som molntjänstleverantör hamnar allt ansvar för säkerheten hos de, vilket gör att åtkomsten mot data och infrastruktur försöker begränsas i så hög mån som möjligt. Detta innebär att åtkomsten också är en viktig säkerhetsaspekt vad gäller säkerhetsrisker i molntjänster.

Enligt den tidigare forskningen som gjorts av bland annat Singh, Jeong och Park (2016) visar att det finns flertalet olika säkerhetsrisker som uppstår i användning och distribuering av molntjänster. Den tidigare forskningen visar att de största säkerhetsriskerna som molntjänstleverantörerna står inför är de olika typer av hackerattacker som förekommer, där Dos attacker som Mohammad och Marzie (2016) skriver om och SQL-injektioner som Masri och Sleiman (2015) berättar om, är vanligt förekommande säkerhetsrisker som leverantörerna står inför. Empirin visar på att dessa typer av attacker är något som molntjänstleverantörer är orolig för. Eftersom en av molntjänstleverantörerna hanterar hela infrastrukturen på egen hand så har de full kontroll på tillgången till deras miljö, men samtidigt är det upp till de att se till att ingen kan ta sig in och därmed att molnet hela tiden fungerar. För de är det viktigt att kunna stå emot dessa typer av attacker för att säkerhetsställa att molnet inte utsätts för några störningar som skulle kunna påverka användningen av molnet. Men ett system kan aldrig vara hundra procent säkert, där empirin visar att den största säkerhetsrisken är den mänskliga faktorn.

Människan är enligt empirin den största säkerhetsrisken hos molntjänstleverantörerna där deras egen personal kan få påtryckningar utifrån som kan ske när någon vill komma åt information som personal har tillgång till. Så kallade insider attacker är något som är svårt att skydda sig från och mycket svårt att upptäcka då den som genomför attacken redan kan ha tillgång till alla system. Empirin beskriver att den största säkerhetsrisken för molntjänstanvändare är läckage av personuppgifter och känsliga företagsuppgifter, likaså här återkommer insider risker. Det som oroar molntjänstanvändarna är att man inte vet vad det är för typ av människor som jobbar på andra sidan molntjänsten där risken finns att någon som arbetar på molntjänsten utnyttjar tillgången till känslig information. Denna risk är något som aldrig går att undvika helt för molntjänstanvändarna, därav anser empirin att det är mycket viktigt att arbeta med behörighetskontroll. Men det handlar inte bara om att se till att behörighetskontroll fungerar korrekt för de som tillhandahåller känslig information, empirin tar också upp att det är viktigt att se till att personer som avslutar sin tjänst blir av med sin behörighet för att behålla kontrollen. Det är lätt hänt att de faller mellan stolarna vilket kan leda till att personer har behörighet som de längre inte ska ha.

En jämförelse mellan vad molntjänstanvändarna och molntjänstleverantörerna upplever som de mest kritiska säkerhetsriskerna visar att det finns en viss skillnad, där användarna är mest oroliga för att läckage av personliga och känsliga uppgifter. Detta främst via insider risker där personal hos leverantören som har access till dessa uppgifter på något sätt skulle läcka ut det för egen vinning eller om de uppstår påtryckningar utifrån som skulle göra att personalen känner sig hotat att lämna ut uppgifter. Leverantörerna är mest oroliga för hackerattacker, intrångsförsök och personalen som arbetar hos leverantören. Här är det betydligt fler variabler som visar sig vara kritiska säkerhetsrisker jämfört med användarna. Detta kan anses bero på att användarna litar på att säkerheten mot hackerattacker och intrångsförsök från utsidan är något som molntjänstleverantörerna ska kunna stå emot. Medans en insider attack aldrig går att förhindra, bara minska risken mot med hjälp av behörighetskontroller och att ett lågt antal personer i personalen som har access. Leverantörerna måste däremot kunna stå emot alla typer av intrångsförsök eller hackerattacker vilket skapar bekymmer hos leverantörerna, det blir viktigt att hela tiden utveckla säkerhetslösningar i takt med den tekniska utvecklingen av molntjänsterna.

Likheten mellan användarna och leverantörerna vad gäller säkerhetsriskerna är personalen som arbetar hos leverantörerna. Men de ser det från olika perspektiv genom att användarna ser risken i att utsättas för läckage av uppgifter på grund av leverantörerna. Medan leverantörerna ser risken i att personalen ska utsättas för någon form av hot eller påtryckningar från någon utomstående person som vill komma åt uppgifter eller data som användarna lagrar hos leverantörerna. Likheten grundar sig i att människan är den säkerhetsrisken som är svårast att kontrollera, det är svårt att se till att den mänskliga faktorn inte gör något fel. Det är viktigt att användare och leverantör inte missuppfattar varandra här, eftersom de har olika perspektiv på samma säkerhetsrisk. Konsekvensen av att missförstå varandra skulle kunna innebära att de säkerhetslösningar man kommit överens om inte fungerar som de var tänkt från båda sidor. Här anser författarna att det handlar om att se till att personal som arbetar hos molntjänstleverantör är rätt utbildade inom säkerhet, göra en noggrann bakgrundskoll när man anställer nya medarbetare och fortlöpande kontroller samt utbildningar som förebygger risken för insider attacker.

7 Slutsatser & Vidare forskning

I detta avsnitt avses att redogöra de framtagna slutsatserna för den genomförda undersökningen. Dessutom kommer en värdering av vidare forskning göras för att presentera för framtida forskning samt utveckling av studien.

7.1 Slutsatser

Syftet med studien har varit att utöka kunskapen om säkerhetsrisker inom molntjänster för användare och medvetenheten hos molntjänstleverantörer om hur företag som använder molntjänster ser på säkerhet. Även undersöka vilka säkerhetsrisker som uppfattas vara mest kritiska för molntjänstanvändare respektive molntjänstleverantör samt om det är skillnad sinsemellan. Utefter syftet och den problemställning som tagits fram har följande forskningsfråga tagits fram;

- Vilka är säkerhetsriskerna inom molntjänster idag, är det skillnad mellan molntjänstanvändare och molntjänstleverantörer i upplevda säkerhetsrisker?

Efter att ha genomfört undersökningen i denna studie framgick det att molntjänstanvändarna upplever att den största säkerhetsrisken är insider attacker. Personal som jobbar hos molntjänstleverantören och har access till personliga eller känsliga uppgifter på något sätt skulle kunna orsaka skada för molntjänstanvändarna genom att läcka ut dessa uppgifter eftersom det inte går att reparera när det väl har hänt. Hos molntjänstleverantörerna framgick det också att läckage av uppgifter är den största säkerhetsrisken. Men för leverantörerna handlar det om vad ett sådant läckage kan leda till, det skulle kunna innebär att leverantören blir bestraffade med böter, tappar kunder, får dålig publicitet och i värsta fall kan dessa faktorer leda till en konkurs. För molntjänstleverantörerna handlar det om att kunna påvisa att man tar insider attack som en stor säkerhetsrisk och arbetar mot det på ett förebyggande sätt för att förtroendet hos de företag som väljer att använda molntjänster ska öka. Samtidigt som de är i behov av att själva inte sätta sig i en situation där läckage av uppgifter sker. Samtidigt krävs det fortsatt fokus på utveckling av säkerhet mot olika typer av hackerattacker och intrångsförsök som tagits upp i studien för att inte försumma de säkerhetsriskerna som fortfarande bör tas på allvar.

En annan slutsats som författarna kom fram till var att trots alla säkerhetsrisker som finns är empirin i denna studie enade i att molntjänster som levereras av tredjepart idag är ett bättre och säkrare sätt för företag att hantera data och information än att utföra det på egen hand. Empirin påvisar att de avtal man skriver med en molntjänstleverantör ska vara tillräckligt för att överväga de säkerhetsriskerna som finns med molntjänster. Molntjänstleverantörerna anses kunna hantera molntjänsterna bättre än molntjänstanvändarna skulle kunna göra eftersom de är nischade inom det området och därmed har man överseende med de säkerhetsrisker som finns.

Efter slutförd undersökning anses syftet och forskningsfrågan vara besvarad genom insamlad empiri där det har kunnat påvisas vilka säkerhetsriskerna inom molntjänster är idag samt att det fanns skillnader mellan molntjänstanvändare och molntjänstleverantörer i upplevda säkerhetsrisker. Med hjälp av denna uppsats kan kunskapen om säkerhetsrisker i molntjänster utökas för både användare och leverantörer av molntjänster.

7.2 Vidare forskning

Vidare forskning inom området anses vara intressant, där en liknande undersökningen med fler respondenter för att möjliggöra ett mer generaliserbart resultat kan genomföras. Därmed skulle det vara relevant att intervjua fler verksamheter för att kunna generalisera inom molntjänstanvändare och molntjänstleverantörer i stora drag för att se om säkerhetsriskerna är en trend eller om det var slumpmässigt för denna undersökning. Vidare hade en större undersökning kunnat genomföras där det inte begränsas till Sverige, eftersom användningen av molntjänster är global skulle det vara intressant att se om det är skillnader mellan olika länder.

För att bygga vidare på syftet och forskningsfrågan för undersökningen hade ett tillägg av att undersöka lösningar och åtgärder för säkerhetsriskerna vara en spännande infallsvinkel att se över, då det också utgör en stor roll inom säkerhet i molntjänster idag. Det skulle dessutom finnas en möjlighet att göra en jämförelse med säkerhetsåtgärderna och lösningarna för de två perspektiven, molntjänstleverantör och molntjänstanvändare, för att se skillnaden sinsemellan.

Referenser

Abo alian, Alshaimaa., Badr, Nagwa L., Tolba, M. F. (2017) Integrity as a service for replicated data on the cloud. *Concurrency and computation*, 2017-02-25, Vol.29 (4), p.e3883-n/a

Albuquerque, R. d. O., Villalba, L. J. G., Orozco, A. L. S., Buiati, F., & Kim, T. (2014). A layered trust information security architecture. *Sensors, Vol 14*(12),

Ali, Mazhar., Khan, Samee U., Vasilakos, Athanasios V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, 2015-06-01, Vol.305, p.357-383

Baltatescu, I., PhD. (2014). Cloud computing services: Benefits, risks and intellectual property issues. *Global Economic Observer,* Vol.2 (1), p.230-242

Beckers, K., Côté, I., Faßbender, S., Heisel, M., & Hofbauer, S. (2013). A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance. *Requirements Engineering*, 18(4), 343-395.

Bu, Kai., Xiao, Bin., Qian, Yi. (2017). High performance and security in cloud computing: Editorial: High Performance and Security in Cloud Computing. *Concurrency and computation*, 2017-10-10, Vol.29 (19) p.e4241

Coppolino, Luigi., D'Antonio, Salvatore., Mazzeo, Giovanni., Romano, Luigi. (2017). Cloud security: Emerging threats and current solutions. *Computers & electrical engineering*, 2017-04, Vol.59, p.126-140

Duncan, A., Creese, S., and Goldsmith, M. (2015) An overview of insider attacks in cloud computing. *Concurrency Computat.*: Pract. Exper., Vol.27: 2964-2981. doi: 10.1002/cpe.3243.

Georgiopoulou, Z., Makri, E., & Lambrinoudakis, C. (2020). GDPR compliance: Proposed technical and organizational measures for cloud provider. *Information and Computer Security,* Vol. 28 Iss. 5, p.665-680.

Grossman, R. L. (2009). The case for cloud computing. *IT Professional Magazine*, Vol. 11, Iss. 2, (Mar/Apr 2009): p.23-27.

Harris, D., Samuel, S., & Probert, E. (2018). GDPR confusion. *The Veterinary Record,* Vol. 183, Iss. 12, (Sep 29, 2018): 388.

Integritetsskydds Myndigheten (2021) Introduktion till dataskyddsförordningen https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/ [Hämtad 2022-05-25]

Iqbal, Salman., Kiah, Miss Laiha Mat., Anuar, Nor Badrul., Daghighi, Babak., Wahab, Ainuddin Wahid Abdul., Khan, Suleman. (2016) Service delivery models of cloud computing: security issues and open challenges: Cloud computing security *Security and communication networks*, 2016-11-25, Vol.9, Iss. 17, p.4726-4750

Jacobsen, D. J. (2017) Hur genomför man undersökningar? Introduktion till samhällsvetenskapliga metoder. Lund: Studentlitteratur.

Kiraz, Mehmet Sabır. (2016). A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing. *Journal of ambient intelligence and humanized computing*, 2016-06-18, Vol.7, Iss. 5, p.731-760

Masdari, M., & Jalali, M. (2016). A survey and taxonomy of DoS attacks in cloud computing. *Security and Communication Networks*, Vol. 9, Iss. 16, (Nov 2016): 3724-3751.

Masri, W., & Sleiman, S. (2015). SQLPIL: SQL injection prevention by input labeling. *Security and Communication Networks,* Vol. 8, Iss. 15, (Oct 2015): 2545-2560.

NSK Inc. (2010). Hybrid Clouds - The best of both World. Boston: NSK Inc

Patel, K., & Alabisi, A. (2019). Cloud computing security risks: Identification and assessment. *The Journal of New Business Ideas & Trends*, Vol. 17, Iss. 2, (2019): 11-19.

PricewaterhouseCoopers International Limited (PWC) (2022). GDPR (dataskyddsförordningen) påverkar alla branscher, företag och organisationer som hanterar personuppgifter. https://www.pwc.se/gdpr [2022-05-03]

Ronny Gunnarsson (2020). Urvalsstrategier och datainsamling. https://infovoice.se/urvalsstrategier-och-datainsamling/. [2022-05-03].

Singh, A. Chatterjee, K (2017) Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, Vol. 79, February 2017, p.88-115

Singh, G. (2016). Cloud computing: New paradigm of internet services. *International Journal of Advanced Research in Computer Science*, Vol. 7, Iss. 6, (Nov 2016).

Singh, Saurabh., Jeong, Young-Sik., Park, Jong Hyuk. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of network and computer applications,* 2016-11-01, Vol.75, p.200-222

Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., . . . Ki-Il, K. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. *Electronics*, Vol.10, Iss. 15, p. 1811.

Vetenskapsrådet (2002) *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Stockholm: Vetenskapsrådet

Warkentina, M., Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management* Volume 52, June 2020, 102090.

Bilagor

A Intervjufrågor molntjänstanvändare

Vill du vara anonym?
Är det okej om vi spelar in dig?

Vill du börja med att berätta lite generellt om hur ni använder er av molntjänster i företaget?

Varför använder ni molntjänster?
Vilken molntjänstleverantör använder ni? Och vilka typer av molntjänster?
Anser du att ert företag har koll på säkerheten när de gäller molntjänster?

Vad händer om det inträffar något med säkerheten i molntjänsterna?
Blir du informerad om något händer med era uppgifter?
Hur blir ni informerade?

Vad finns det för säkerhetsrisker i molntjänster?
Vad finns det för åtgärder när det gäller säkerhetsrisker i molntjänster?
Vilka åtgärder görs?

Har molntjänstleverantörer en plan ifall något inträffar?
Hur ser den planen ut?
Hur ser lösningen ut om någon kommer åt er info?
Hur viktigt är säkerheten för er?

Har ni någon erfarenhet av intrång eller liknande inom användning av molntjänster?
Hur gick det till i så fall? Och hur löste ni det?

B Intervjufrågor molntjänstleverantör

Vill du vara anonym?
Är det okej om vi spelar in dig?

Hur arbetar ni som molntjänstleverantör? Kan du berätta lite kort
Har ni någon plan ifall något stör säkerheten?
Hur ser planen ut?

Hur känner ni över ert ansvar för säkerheten hos era molntjänstanvändare?
Hur arbetar ni för att uppnå integritet hos era kunder?
Vad är de största säkerhetsrisker enligt er som leverantör?
Vad finns det för åtgärder när det gäller säkerhetsrisker i molntjänster?
Vilka åtgärder görs?

Har kunderna någon kontroll över molnet?
Vem bär egentligen ansvaret för bristerna i säkerheten?

Vilka är de största säkerhetsutmaningarna som en molntjänstleverantör?

HÖGSKOLAN
I BORÅS

Besöksadress: Allégatan 1 · Postadress: 501 90 Borås · Tfn: 033-435 40 00 · E-post: registrator@hb.se · Webb: www.hb.se