LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Säkerhetsutmaningar i molnet

Hur verksamheter hanterar säkerhetsmässiga utmaningar med cloud computing

Kandidatuppsats 15 HP, kurs SYSK16 i Informatik

Författare:
Sören Ljunggren
Victor El Bishti

Handledare:
Björn Svensson

Rättande lärare:
Umberto Fiaccadori
Nicklas Holmberg

Säkerhetsutmaningar i molnet: Hur verksamheter hanterar säkerhetsmässiga utmaningar med cloud computing

ENGELSK TITEL: Security challenges within the cloud: How businesses handle security challenges with cloud computing

FÖRFATTARE: Victor El Bishti, Sören Ljunggren

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Christina Keller, Professor

FRAMLAGD: maj, 2020

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 99

NYCKELORD: Cloud computing, molntjänster, säkerhetsutmaningar, informationssäkerhet, datakontroll, mjukvaruutveckling, mjukvarudistribution

SAMMANFATTNING (MAX. 200 ORD): Cloud computing har drivit fram ett nytt paradigm för mjukvaruutveckling och -distribution. Nya teknologier används för att leverera infrastruktur och plattformar som tjänst, vilket innebär särskilda utmaningar. I den här studien tittar vi på utmaningar i kategorierna (1) informations- och datasäkerhet, baserat på CIA-triaden och (2) datakontroll och ansvar. Vi har genomfört semistrukturerade intervjuer för att undersöka hur verksamheter hanterar utmaningar och fastslår att de gör det med preventiva åtgärder, såsom kryptering och åtkomstbehörigheter; att de använder moderna utvecklingsmetoder och ramverk, såsom mikrotjänstarkitektur, vars sekundära effekter bemöter utmaningarna. Vi kommer fram till att delar av säkerhetsansvar ligger hos molnleverantörerna, att överlappet i säkerhetsansvar är försumbart och att användare har stor tillit till att leverantörer tar ansvar för säkerhet i sina tjänster.

Innehåll

Tabeller

1 Introduktion

Cloud computing, eller molntjänster, beskriver mjukvarutjänster som levereras till kund över nätverk oberoende av plats eller enhet (Mell & Grance, 2011; Liu, Chan, Yang & Niu, 2018; Iyer & Henderson, 2010; Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica & Zaharia, 2010) och har kommit att bli en dominant affärsmodell för att leverera IT-resurser, t.ex. nätverk, servrar eller lagring, på ett globalt och distribuerat sätt (Benlian, Kettinger, Sunyaev & Winkler, 2018; Harris, 2002). Molntjänsterna har blivit ett nytt paradigm för utveckling, drift och distribution av mjukvara över internet och utvecklats till ett attraktivt alternativ för verksamheter som eftersöker skalbar och elastisk IT-infrastruktur utan stora initiala investeringar (Zhang, Cheng & Boutaba, 2010). Den globala marknaden för cloud computing-lösningar, *cloud infrastructure services*, värderades till ca 23.5 miljarder USD 2017 och förväntas växa i en takt på mer än 22,3% per år under perioden 2018–2025, vilket har fått stora aktörer som Amazon, Microsoft och Google att tävla om marknadsandelar (MarketWatch, 2019).

1.1 Problembakgrund

Tillväxten av cloud computing innebär att fler och fler verksamheter går från att hantera sina egna IT-resurser på plats inom verksamheten (traditionell IT), till att ge över hanteringen till molnleverantören. Denna outsourcing av IT-resurser och datacenter innebär att användarna måste förlita sig på att leverantören uppnår full datasäkerhet (Meiyan, 2013), samtidigt som de förlorar väsentlig kontroll över data och tjänster till den utomstående leverantören (Géczy, Izumi & Hasida, 2012). Detta framgick inte minst i med fallet WikiLeaks, som exponerade inneboende risker med förflyttning av kontroll (Sternstein, 2011). WikiLeaks fick sina tjänster avslutade och sin data borttagen från Amazon till följd av en förfrågan från en amerikansk federal åklagare (MacAskill, 2010). WikiLeaks är förvisso inte en mönsterverksamhet; de har en tämligen antagonistisk relation till amerikanska staten, men förfarandet belös ändå den kontrollförlust som hade skett. Detta upprörde hela branschen och lärdomen var tydlig: organisationer kan inte med full tillit anförtro sina kritiska tjänster och data till molnleverantörer (Géczy, Izumi & Hasida, 2012).

Trots att kontroll förflyttas blir organisationer inte av med ansvaret för den data och de program som de lagrar och distribuerar (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka & Molina, 2009; Vithayathil, 2018). Detta utgör en stor utmaning för användare av molntjänster - att uppnå samma IT-säkerhet som de önskar samtidigt som de måste förhålla sig till ett nytt säkerhetslandskap (Venters & Whitley, 2012). Tekniska fel, *distributed denial-of-service*-attacker och dataförlust är säkerhetsrisker som molnleverantörer står inför eller har blivit utsatta för (Tchernykh, Schwiegelsohn, Talbi & Babenko, 2019) och användarna måste förhålla sig till att det kan inträffa. Cloud computing har övertygande fördelar, men det nya paradigmet innebär att verksamheter ställs inför nya säkerhetsutmaningar (Chen, Paxson & Katz, 2010).

I den här studien behandlar vi säkerhetsutmaningar i två kategorier. *Information- och datasäkerhet* innebär utmaningar som följer av att uppnå och garantera godtagbara nivåer av konfidentialitet, integritet och tillgänglighet, både för egen räkning och gentemot sina kunder.

Datakontroll och ansvar handlar om utmaningar som följer av att man lagrar och processar data på infrastruktur som man inte äger och därmed förlorar kontroll till den som äger infrastrukturen.

1.2 Problemområde

Tidigare litteratur visar på utmaningar inom information- och datasäkerhet (t.ex. Whitman & Mattord, 2011; Samonas & Coss, 2014) och användning av öppna molnlösningar (t.ex. Zissis & Lekkas, 2012; Popović & Hocenski, 2010; Rizwan & Zubair, 2019; Chow et al. 2009; Meiyan, 2013). Därtill finns litteratur om utmaningar relaterade till datakontroll och ansvar i samband med användning av cloud computing (t.ex. Davidovic, Ilijevic, Luk & Pogarcic, 2014; Venters & Whitley, 2012; Shivpuriya, 2017; Chow et al. 2009; Beslic, Bendraou, Sopenal & Rigolet, 2013). Vi kan därmed förvänta oss att verksamheter är medvetna om utmaningarna och att de hanterar dem, men hur de bär sig åt är inte fastställt i litteraturen. Företag praktiserar inte alltid vad litteraturen säger, vilket kan förklaras av verksamheters komplexa sammanhang och att akademin är för generell eller specifik för att vara tillämpbar (Ward & Griffiths, 1996). Det kan också bero på att forskningsfältet i sig, informationsteknik, i hög grad är dynamisk vilket (1) adderar komplexitet och osäkerhet, (2) resulterar i att akademiker jagar praktiken snarare än att leda den och (3) vanligtvis leder till att resultat rapporteras från studier som innehåller ny teknik år efter att tekniken accepteras eller förkastas av praktiker (Benbasat & Zmud, 1999).

För att göra förändringar i verksamheter är det nödvändigt att ha en bild av var verksamheten står, en målbild att röra sig mot och en metod för att röra sig dit. Genom att utreda hur verksamheter hanterar säkerhetsutmaningar är det möjligt att skapa en bild av var verksamheten står. Av denna anledning och givet den forskning som vi har tittat på anser vi att nämnda säkerhetsutmaningar i nämnda sammanhang är ett relevant problemområde att undersöka.

1.3 Frågeställning

Hur hanterar verksamheter säkerhetsutmaningarna (1) information- och datasäkerhet och (2) datakontroll och ansvar, i samband med att de använder cloud computing för mjukvaruutveckling och -distribution?

1.4 Syfte

Syftet med den här studien är att beskriva hur verksamheter hanterar olika säkerhetsutmaningar gällande *information- och datasäkerhet* och *datakontroll och ansvar*. Beskrivningen utgår från verksamhetens arbete med mjukvaruutveckling och -distribution med hjälp av cloud computing-tjänster.

1.5 Avgränsningar

Vi behandlar ämnet cloud computing, som innehåller tre tjänstemodeller: Software as a Service, Platform as a Service och Infrastructure as a Service (Mell & Grance, 2011). Software as a Service (SaaS) beskriver tjänster och applikationer som körs på en molninfrastruktur men där konsument varken hanterar eller kontrollerar den underliggande molninfrastrukturen, inkluderat nätverk, servrar eller operativsystem (Mell & Grance, 2011), t.ex. Gmail eller Dropbox. Den här uppsatsen behandlar inte SaaS eftersom vi undersöker verksamheter som utvecklar och distribuerar sin egen mjukvara ovanpå en molninfrastruktur.

Det finns fyra distributionsmodeller av cloud computing: *private*, *public*, *community* och *hybrid cloud* (Mell & Grance, 2011). Community cloud är avsedd för exklusiv användning av en specifik grupp av konsumenter med delade angelägenheter och särskilda krav, t.ex. policies eller säkerhetskrav (Mell & Grance, 2011). Den här studien bortser från distributionsmodellen *community cloud* eftersom vi inte ställer några särskilda krav på verksamheternas användning av cloud computing eller undersöker någon specifik bransch där särskilda krav ingår.

Det finns möjliga fall av on-premise cloud computing, men i den här studien undersöker vi fall där leverantören och användare av en molntjänst är separata organisationer. Detta, dels för att det är så det vanligen ser ut i verkligheten, dels för att en on-premise molnlösning i mångt och mycket kan betraktas som en traditionell IT-lösning, där verksamheten själv hanterar de fysiska komponenterna av IT-infrastrukturen (se t.ex. Vithayathil, 2018).

2 Litteraturgenomgång

2.1 Cloud computing

Cloud computing, eller molntjänster, är ett samlingsbegrepp för hårdvaru- och mjukvarutjänster som levereras över nätverk till kund med hjälp av självbetjäning, oberoende av plats och enhet (Mell & Grance, 2011; Liu et al. 2018; Iyer & Henderson, 2010). Cloud computing är en evolution av datorteknologi som har blivit en dominant affärsmodell för att leverera IT-infrastruktur (t.ex. nätverk, servrar, lagring), komponenter och applikationer på ett globalt, distribuerat och service-centrerat vis (Benlian et al. 2018; Harris, 2002).

Cloud computing som koncept är väl definierat; Mell & Grance (2011) står för definitionen som används av väldigt många artiklar, bland andra Armburst et al. (2010) om fördelar och möjligheter, Venters & Whitley (2012) om vad cloud computing-användare vill ha ut av det, Choudhary & Vithayathil (2013) om hur cloud computing påverkar synen på IT-avdelningen, Schneider & Sunayaev (2016) om vad som avgör beslut om IT-outsourcing till molntjänster, Battleson, West, Kim, Ramesh & Robinson (2016) om hur man når framgång med cloud computing och Vithayathil (2018) om huruvida cloud computing kommer göra den traditionella IT-avdelningen förlegad: alla *Basket of Eight*-artiklar om cloud computing per Mell & Grance (2011) definition. Det finns forskning om tekniska aspekter och utmaningar om cloud computing (t.ex. Wang et al. 2008; Kumar & Goudar, 2012; Jadeja & Modi, 2012), men forskning om cloud computings organisatoriska påverkan är ännu ett fält i sin vagga (Vithayathil, 2018).

Vi använder amerikanska NIST:s, National Institute of Standards and Technology, väletablerade definition av cloud computing. Mell & Grance (2011) och till viss del Armbrust et al. (2010) är välciterade artiklar från ansedda publikationer som beskriver cloud computings struktur och karaktäristik. Choudhary & Vithayathil (2013) och Vithayathil (2018) konstaterar detsamma. Wang, Tao, Kunze, Castellanos, Kramer & Karl (2008) beskriver cloud computing och ger en lösare definition där de redogör för de tekniska förutsättningarna för cloud computing, men deras definition är inte ett alternativ till Mell & Grance (2011) eftersom den är konceptuellt lik men mindre specifik. NIST:s definition av Cloud Computing omfattar fem grundläggande egenskaper (Mell & Grance, 2011):

- *On-demand self-service* innebär att en konsument kan fördela resurser och kapacitet utan att interagera med handläggare hos leverantören.
- *Broad network access* innebär att tjänsterna finns tillgängliga över nätverk och kan tillgås genom varierade klienter.
- *Resource pooling* innebär att konsumenten ingår i en resurspool där kapaciteter och resurser fördelas automatiskt till de konsumenter som behöver resurserna för stunden.
- *Rapid elasticity* innebär att resurser och kapaciteter kan fördelas snabbt efter behov; för konsumenten kan de tillgängliga resurserna ofta upplevas som obegränsade.
- *Measured service* innebär att molnsystemen automatiskt kontrollerar och optimerar resursanvändning Därmed finns det någon slags mätning som kan tjäna som övervakning och generell transparens för både leverantörer och konsumenter.

2.1.1 Tjänstemodeller

Cloud computing kommer i tre tjänstemodeller: *Software as a Service, Platform as a Service* (PaaS) och *Infrastructure as a Service* (IaaS) (Mell & Grance, 2011). Medan de olika tjänstemodellerna är konceptuellt distinkta är de tillgängliga tjänsterna inte alltid enkla att placera i någon av kategorierna eftersom de ofta erbjuder både IaaS- och PaaS-funktionalitet (Armbrust et al. 2010). Man kan därför se det som att olika tjänster ligger på olika platser i ett abstraktionsspektrum. Låg abstraktionsnivå ger användaren större kontroll över exempelvis system- och serverkonfiguration, applikation- och infrastruktursäkerhet, belastningsbalans och upp-/nedskalning (Armbrust et al. 2010). Med hög abstraktionsnivå kan mycket av det hanteras automatiskt, vilket erbjuder användaren större stöd för applikationsdesign och implementering (Armbrust et al. 2010). De två överlägsna aktörerna på marknaden för cloud computing är Amazon och Microsoft medan Google, Alibaba och IBM har nämnvärda marknadsandelar (Synergy Research Group, 2020). Alla tillhandahåller tjänster i hela eller stora delar av abstraktionsspektrumet (Amazon Web Services, 2020a; Microsoft Azure, 2020a; Google Cloud, 2020a; IBM Cloud, 2020; Alibaba Cloud, 2020a).

Infrastructure as a Service är en tjänstemodell av cloud computing som tillhandahåller infrastruktur och IT-resurser, oftast i form av virtuella maskiner (Mell & Grance, 2011; Zhang, Cheng & Boutaba, 2010). IT-resurserna som tillhandahålls är bearbetningskapacitet, lagring, nätverk och andra fundamentala IT-resurser där kund kan distribuera och köra mjukvara (Walraven, Truyen & Joosen, 2014; Mell & Grance, 2011). Virtualiseringsteknik har en omfattande roll i IaaS-molnet: att integrera/bryta ned fysiska resurser för att möta en ökad eller minskad efterfrågan av IT-resurser (Kumar & Goudar, 2012; Wang et al. 2008). IaaS-kunder hanterar eller kontrollerar inte den underliggande molninfrastrukturen men har kontroll över operativsystem, lagring, distribuerade applikationer och i vissa fall begränsad kontroll över utvalda nätverkskomponenter såsom brandvägg (Mell & Grance, 2011).

Platform as a Service är ett begrepp som beskriver molntjänster som förser användare med en virtuell plattform för mjukvaruutveckling och -distribution av program och applikationer (Mell & Grance, 2011; Lawton, 2008; Walraven, Truyen & Joosen, 2014). Den primära användaren av denna typ av tjänst är utvecklingsteam - PaaS-tjänster tillåter dem att snabbt sätta upp applikationsmiljöer, enkelt lansera kod till dessa miljöer och omedelbart skala upp eller ned (Krancher, Luther & Jost, 2018). PaaS-lösningarnas utvecklingsmodell låter utvecklaren specificera verksamhetens processflöden och applikationslogik utan att behöva referera till de underliggande fysiska datorsystemen eller nätverksgränssnitten och gömmer således komplexiteten i att köra mellan en klient och en virtuell server (Armbrust et al. 2010; Lawton, 2008).

2.1.2 Distributionsmodeller

Det finns fyra olika distributionsmodeller av molntjänster av cloud computing: *Private cloud, Public cloud, Community cloud* och *Hybrid cloud* (Mell & Grance, 2011). Alternativen för distribuering ger liknande fördelar i förhållande till prestanda, tillförlitlighet, skalbarhet och lastbalansering - men vilken distributionsmodell en organisation bör använda beror på verksamhetens behov (Vithayathil, 2018).

Private cloud innebär ett moln avsatt för exklusivt användande av en enskild organisation (Mell & Grance, 2011). Det kan ägas och förvaltas av den konsumerande organisationen, en

tredje part eller en kombination och kan existera on- eller off-premise (Orakwue, 2010; Mell & Grance, 2011). I ett privat moln hanteras tjänster och infrastruktur alltid på ett privat nätverk med dedikerad hård- och mjukvara (Microsoft Azure, 2020b).

Public cloud innebär ett moln som är avsatt för öppen användning av allmänheten (Mell & Grance, 2011). Ett publikt moln ägs och förvaltas av ett företag eller akademisk eller offentlig organisation och den fysiska infrastrukturen existerar hos leverantören (Mell & Grance, 2011). Amazon, Azure och Google m.fl. erbjuder molntjänster av den här typen (Amazon Web Services, 2020a; Microsoft Azure, 2020a; Google Cloud, 2020a; IBM Cloud, 2020; Alibaba, 2020).

Hybrid cloud är en hybrid komposition av två eller fler distinkta sammanlänkade moln, varav ett (eller flera) kan vara publika (Mell & Grance, 2011). Molnen sammanlänkas av standardiserad eller proprietär teknologi som gör data och applikationer portabla mellan dem (Mell & Grance, 2011). Det innebär att en verksamhet kan ha delar av sin verksamhet i ett privat moln och delar i ett publikt moln, där de olika molnen interagerar med varandra.

2.1.3 Virtualiseringsteknik

Skalbarhet är en kritisk framgångsfaktor för många verksamheter som är verksamma över internet eftersom deras efterfrågan och belastning kan variera drastiskt över tid - i vissa perioder kan en verksamhet behöva serverkapacitet i nivå med superdatorer medan i andra perioder näst intill ingen alls (Chieu, Mohindra, Karve & Segal, 2009; Wang et al. 2008; Armbrust et al. 2010). Cloud computing-modellen har utvecklats för att kunna tillgodose de varierande behoven; den serverkapacitet och processorkraft som cloud computing erbjuder möjliggörs till stora delar av distribuerade, storskaliga datorkluster, i allmänhet med hjälp av hårdvaruvirtualisering (Chieu et al. 2009; Wang et al. 2008; Armbrust et al. 2010).

Virtualiseringsteknik är i grunden en abstraktion av fysiska IT-resurser och fungerar i princip på så vis att fysiska datorresurser omvandlas till virtuella gästmaskiner som kan flyttas omkring på olika fysiska IT-resurser (Benlian et al. 2018; Wang et al. 2008). Eftersom de kan flyttas bryts det direkta beroendet mellan maskin och hårdvara som är associerat med icke virtualiserade maskiner (Chieu et al. 2009; Wang et al. 2008). Därmed kan gästmaskinen bli isolerad och automatisk förflyttad mellan hårdvarumaskiner, i fall där hårdvara går sönder, bryts upp eller når sin belastningsgräns (Chieu et al. 2009; Wang et al. 2008). Tekniken gör att IT-resurser kan bli allokerade på begäran och således kan upp-/nedskalning i perioder av hög eller låg efterfrågan och belastning göras automatiskt (Benlian et al. 2018; Chieu et al. 2009). I och med cloud computings utformning har användare till synes oändliga resurser tillgängliga på begäran och betalar bara för det arbete (beräkning, lagring, bearbetning) som de faktiskt använder (Armbrust et al. 2010).

2.1.4 Cloud native

När en webbtjänst- eller applikation är både utvecklad och distribuerad med hjälp av en molntjänst av en verksamhet som har helt outsourcat sin infrastruktur kallas den *Cloud Native* (Foster & Gannon, 2017). Cloud Native-applikationer är distribuerade, elastiska och horisontellt skalbara system som följer designmönster som minimerar antalet *stateful*-komponenter och är designade för att köras på elastiska plattformar (Kratzke & Quint, 2017).

Eftersom applikationerna är uppbyggda av många små, fördelade komponenter måste säkerhet vara inbyggt i applikationerna och i arkitekturen (Gannon, Barga & Sundaresan, 2017). Cloud native är ett nytt fenomen och förekommer därmed vanligen på nyare företag (Patrizio, 2018).

2.2 Mjukvaruutveckling och -distribution med cloud computing

I den här studien tittar vi på säkerhetsutmaningar som uppstår i samband med att användning av cloud computing specifikt för mjukvaruutveckling och –distribution. I följande avsnitt redogör vi för innebörden av just utveckling och distribution av mjukvara. Vi använder *Software Development Life Cycle* (SDLC) som teoretisk referenspunkt i våra undersökningar och senare delar av studien.

Mjukvara är numera både en produkt och ett verktyg för att leverera produkter (Pressman, 2005). Mjukvaruutveckling involverar inte bara flera hårdvaruteknologier utan flera olika parter, såsom kunder, slutanvändare och utvecklare, vilket gör det till en komplex procedur (Guha & Al-Dabass, 2010). Inom mjukvaruutveckling finns flera olika metodologiska ansatser (Boehm, 1988). SDLC är en kategori av flera olika metoder (Ragunath, Velmourougan, Davachelvan, Kayalvizhi & Ravimohan, 2010; Wikipedia, 2020; Boehm, 1988) som används av både stora och små organisationer (ProductPlan, u.å.) och omfattar flera modeller såsom *agile*, *lean* och vattenfallsmodellen (Ragunath et al. 2010). Vi har valt SDLC som metodologisk modell eftersom den omfattar olika storlekar av verksamheter och processmodeller för mjukvaruutveckling, som täcker upp för ämnet och dess faser i sin helhet.

SDLC består av ett antal faser eller aktiviteter: kravinsamling, planering, design, programmering, testning, distribution och underhåll (Khari & Kumar, 2016; Guha & Al-Dabass, 2010). Vilka faser som ingår i SDLC varierar beroende på källa men innehållet är sällan olikt. Valacich & George (2017) använder SDLC för att beskriva systemutveckling med faserna: planering, analys, design, implementation och underhåll. Kulkarni & Gulvani (2016) räknar upp de traditionella faserna design, programmering, testning och distribution och menar att dessa är samma inom alla områden av mjukvaruutveckling medan Ruparelia (2010) helt enkelt förklarar att livscykeln täcker alla faser från kravinsamling till underhåll. Det som skiljer SDLC åt är hur det tillämpas, vilka parter som är involverade och vilka verktyg som parterna har tillgång till (Guha & Al-Dabass, 2010).

2.2.1 Molntjänsters inverkan på SDLC

Under kravinsamlingsfasen bör verksamheter ta hänsyn till och utvärdera sina molnleverantörer eftersom de tillhandahåller och underhåller IT-infrastrukturen (Kulkarni & Gulvani, 2016; Guha & Al-Dabass, 2010). Molnleverantören ska även inkluderas i planerings-, och designfasen, då de har information om arkitektoniska detaljer, virtualiseringsstrategier och hur de resurser som erbjuds bäst nyttjas: t.ex. rådgivning om antal mjukvaruutvecklare, kostnadsestimering, riskhantering, konfigurationshantering eller kvalitetsförsäkran (Guha & Al-Dabass, 2010).

Programmering och testning kan i många fall genomföras på molnplattformen, vilket underlättar tillgången till den mjukvara som utvecklats (Guha & Al-Dabass, 2010). Med traditionell mjukvaruutveckling skrivs hela applikationens mjukvara *in-house*, från början till slut, men idag används vanligen flera olika källor av mjukvara (Valacich & George, 2017). Delar och komponenter kombineras för att producera produkter och tjänster (Valacich & George, 2017). Mjukvaruutvecklare använder sig ofta av webbtjänster och öppen källkod från molnet, vilket kräver en förmåga att utveckla och återanvända mjukvara från tillgängliga komponenter och befintliga applikationer (Guha & Al-Dabass, 2010).

Disitribution (*deployment*) är en aktivitet som innefattar tre åtgärder: *leverans*, *support* och *underhåll* (Pressman, 2005). I och med modernare distribution, med cloud computing, sker inte distributionen en gång, utan ett antal gånger där varje iteration av åtgärderna förser kunden och slutanvändaren leverans av ny funktionalitet och förbättringar, dokumentation och assistans för den nya funktionaliteten (Khari & Kumar, 2016; Pressman, 2005).

2.2.2 Secure Software Development Life Cycle

Det finns en utökning till livscykeln som heter *Secure Software Development Life Cycle* (SecSDLC eller SSDLC), som adderar till SDLC identifikation av specifika hot och risker, följt av design och implementation av specifika kontroller för att bemöta dessa hot och hantera de risker som organisationen och/eller dess kunder står inför (Rittinghouse & Ransome, 2016).

Identifikation av hot och risker kan ske med hjälp av testning, som är en vital fas för säkerhet, och ska innehålla säkerhetstester baserat på attackmönster och hotmodeller med tekniker såsom penetrationstester (Khari & Kumar, 2016). Testningsfasen innefattar även att moduler testas utförligt för att upptäcka säkerhetsproblem innan implementation och kontinuerligt genom hela livscykeln (Rittinghouse & Ransome, 2016). Kravinsamling ämnar till att identifiera säkerhetskrav och att tillhandahålla fullständig säkerhet med hjälp av grundläggande säkerhetsfunktionalitet (Khari & Kumar, 2016). Med SecSDLC skrivs kod på ett konsekvent sätt som enkelt kan granskas och förbättras; applikationens kärntjänster tillhandahålls på ett gemensamt, strukturerat och upprepningsbart vis (Rittinghouse & Ransome, 2016).

2.3 Säkerhetsutmaningar med cloud computing

IT och datorer har historisk sett hanterats centraliserat av ett få antal kunniga yrkesverksamma och där fysisk säkerhet haft den yttersta betydelsen (Loch, Carr & Warkentin, 1992). I takt med att den tekniska inträdesbarriären för användare sjunker blir tjänster tillgängliga för många fler, vilket skapar nya, sårbara miljöer (Loch, Carr & Warkentin, 1992). Verksamheter som har sin data på molnet möts av utmaningar såsom data- och nätverksintrång, malware-injektioner, osäkra API:er, DDoS-attacker, sårbarheter i molnlösningarnas system, phising-attacker m.m. (Rizwan & Zubair, 2019), utmaningar som är större på molnet än i traditionella system (Armbrust et al. 2010; Chow et al. 2009) eller som inte kan bemötas med traditionella medel (Zissis & Lekkas**,** 2012)

Ju mer information om personer och verksamheter placeras i molnet, desto mer växer oron om hur säker molnmiljön är (Popović & Hocenski, 2010). Det råder generell oro över molnsäkerhet (Vithayathil, 2018) vilket har gjort att det har blivit en av de mest citerade invändningarna mot cloud computing (Armbrust et al. 2010). Till skillnad från traditionell IT finns en inneboende risk med cloud computing då det kringgår fysiska-, logiska- och personalkontroller (Brodkin, 2008). Säkerhet är en signifikant utmaning för verksamhet på molnet och ämnet dominerar litteraturen om utmaningar (Venters & Whitley, 2012).

I och med att cloud computing använder sig av virtualiseringsteknik kan användarnas data bli spridd till olika datacenter istället för att stanna på samma fysiska plats (Kumar & Goudar, 2012). Till följd av att moln-resurser poolas, med hjälp av virtualisering och bred nätverksåtkomst, finns det bekymmer med attacker mot virtuella maskiner och attacker mot en ökad nätverksyta som användarna delar (Chow et al. 2009). Med cloud computing-modellen förlorar användare kontroll och kunskap över fysisk säkerhet och var de fysiska IT-resurserna befinner sig, vilket kan utsätta verksamheten för risk att direkt eller indirekt utsättas för beslag eller förstörelse av data (Popović & Hocenski, 2010).

2.3.1 Information- och datasäkerhet

Information- och datasäkerhet syftar till att skydda informationstillgångar som lagras, bearbetas eller överförs med hjälp av policys, utbildning, träning, medvetenhet och teknologi (Whitman & Mattord, 2011; Harris, 2002). Konfidentialitet, integritet och tillgänglighet är sedan länge den etablerade triaden för informationssäkerhet (se tabell 1: CIA-triaden) (Harris, 2002) och är inom militären, där modellen först utvecklades, mål som måste uppnås fullständigt, oavsett pris (Samonas & Coss, 2014). Inom kommersiell verksamhet måste däremot målen bara uppnås i förhållande till förlustrisken relativt till investeringen i informationssäkerhet (Samonas & Coss, 2014).

Vi använder CIA-triaden (ibland *AIC-triaden*) som modell för informationssäkerhet. De tre principerna i CIA är *confidenciality* - konfidentialitet, *integrity* - integritet och *availability* - tillgänglighet; dessa utgör informationssäkerhetens fundamentala principer (Harris, 2002). Även om triaden framstår som simpel är arbetet med att få sin verksamhet och sitt system att uppfylla de tre principerna ovedersägligt en utmaning (Harris, 2002).

Ett alternativ till CIA-triaden är Parkers Hexad (Andress, 2011). Parkers hexad innefattar, utöver de tre pelarna i CIA, *posession of controll* - kontrollinnehav, *authenticity* - autenticitet och *utility* - användbarhet (Andress, 2011). Parker-modellen har en avvikande syn på principen om integritet, som gör autenticitet en nödvändig utökning av triaden (Andress, 2011). Vi använder integritet i den bredare bemärkelsen och autenticitet innefattas därav i vår användning av principen. Kontrollinnehav tar vi upp i avsnitt 2.3.2. Den sista principen, användbarhet, kan vara intressant att beakta, exempelvis hur användbar information är för någon som otillbörligen kommer över information, men principen är icke-binär, något abstrakt (Andress, 2011) och tillför därför inte till den säkerhetsbild på ett sätt som gör det relevant för oss att undersöka i den här studien.

Tabell 1: CIA-triaden

Begrepp	**Beskrivning**
Confidentiality (konfidentialitet)	Information har konfidentialitet när den är skyddad från avslöjande eller exponering till icke-auktoriserade individer eller system (Whitman & Mattord, 2011; Harris, 2002). Informationen berör både data och metadata, t.ex. information om datatrafik (Samonas & Coss, 2014). Konfidentialitet säkerställer att endast de med rättigheter och privilegier att få tillgång till information kan göra det och när någon obehörig kan visa informationen så har konfidentialiteten blivit bruten (Whitman & Mattord, 2011; Harris, 2002).
Integrity (integritet)	Information har integritet när den är hel, komplett och icke-korrupt (Whitman & Mattord, 2011; Harris, 2002). Integriteten hos information är hotad när den exponeras för korruption, skada, förstörelse eller annan störning från sitt äkta tillstånd (Samonas & Coss, 2014; Whitman & Mattord, 2011; Harris, 2002). Sabotage av information utgör ett hot för integriteten och en förövare behöver således inte se informationen för att orsaka ett integritetsbrott (Samonas & Coss, 2014).
Availability (tillgänglighet)	Tillgänglighet innebär graden av att auktoriserade användare, personer, roller eller datorsystem har tillgång till information utan störningar eller hinder och att kunna ta emot det i önskat format (Whitman & Mattord, 2011; Harris, 2002).

Konfidentialitet syftar till att bara auktoriserade parter eller system har tillgång till skyddade data (Zissis & Lekkas, 2012; Tchernykh et al. 2019). Hotet att data blir äventyrad ökar i molnet eftersom det ökade antalet aktörer, enheter och applikationer som är involverade leder till en ökning i antalet som har tillgång till molnet som lagrar data (Zissis & Lekkas, 2012). *Multitenancy* innebär egenskapen hos molnlösningar att dela på resurser såsom minne, program, nätverk och data mellan användare (Zissis & Lekkas, 2012; Mell & Grance, 2011). Trots att användare separeras på en virtuell nivå så separeras inte hårdvara vilket, om det inte hanteras varsamt, skapar en allvarlig sårbarhet med att datakonfidentialitet bryts oavsiktligt (Zissis & Lekkas, 2012). Vanliga metoder för att säkerställa konfidentialitet är datakryptering, dokumentering av åtkomstbehörigheter, lösenord och andra metoder för autentisering (Tchernykh et al. 2019).

Verksamheter är varsamma om hur *integritet* kan bibehållas med cloud computing och ser det som en stor risk att placera kritiska applikationer och känsliga data i en publik molnmiljö utanför deras egna datacenters nätverk (Popović & Hocenski, 2010; Brodkin, 2008). Data som lagras i molnet kan drabbas av skada vid överföring till/från molndatalagring (Aldossary & Allen, 2016). Integriteten bör kontrolleras på data- och beräkningsnivå och alla typer av avvikelser som förlust eller manipulation av data eller icke betrodda fjärrservrar som utför beräkningar bör kontrolleras och rapporteras (Aldossary & Allen, 2016).

Tillgänglighet avser egenskapen hos ett system och tjänster att vara åtkomlig och användbar (Géczy, Izumi & Hasida, 2012) på begäran av en auktoriserad enhet och fortsätta sina operationer även vid risk för säkerhetsintrång (Zissis & Lekkas, 2012; Tchernykh et al.

2019). Det kan betraktas i två bemärkelser: dels molntjänstens-/plattformens tillgänglighet, dels den distribuerade mjukvarans tillgänglighet. Det är viktigt att tjänsterna har hög nätverksäkerhet och beredskap; om nätverket är oåtkomligt kan användare inte komma åt kritiska tjänster och data (Géczy, Izumi & Hasida, 2012).

2.3.2 Datakontroll och ansvar

Det finns en upplevd trygghet med att ha datacenter i egna lokaler (Venters & Whitley, 2012) men i praktiken finns det inte nödvändigtvis säkerhetsmässiga skillnader på traditionella datacenter och datacenter i molnet, även privata, om de är tillgängliga genom internet (McAfee, 2012; Munk, 2019).

När verksamheter använder molntjänster istället för traditionella datacenter förändras ansvars- och kontrollfördelningen, i och med att en ny part blandas in: molnleverantören. Molnleverantören är ett separat företag med eget vinstintresse som därmed kommer de sträva efter att tillhandahålla tjänster som håller en säkerhetsnivå som återspeglar sina kunders samlade eller genomsnittliga förväntningar, för att maximera sin egen omsättning och vinst (Vithayathil, 2018). Molnleverantörer är givetvis ansvariga för *molnets* säkerhet, men de som utvecklar och distribuerar från molnet måste själva ansvara för säkerhet *inom molnet* och inom sina applikationer och tjänster (Shivpuriya, 2017).

Informationstjänster har fram till nyligen alltid försökt behålla full kontroll över information och/eller datorsystem inom det tillhörande affärssystemet (Davidovic et al. 2014). Det sker en utveckling från traditionell klient/server-arkitektur till arkitektur med många komponenter och lager, vilket innebär att kontroll och inflytande över säkerhet distribueras (Davidovic et al. 2014). Molnanvändarna har egentligen samma säkerhetsansvar som i en traditionell miljö, i förhållande till sin egen verksamhet, samtidigt som de förlorar kontroll och inflytande (Chow et al. 2009).

Förvaltning och kontroll av data och tjänster är en av de viktigaste frågorna för verksamheter och användare (Julisch & Hall, 2010). Förvaltning syftar till att ha en kraftfull övervakning över organisationens data och tjänster, vilket inkluderar datakryptering, uppdateringar och säkerhetskopior medan datakontroll syftar till att behålla åtkomstkontrollen över data och tjänster (Géczy, Izumi & Hasida, 2012). En finfördelad kontroll över åtkomstbehörigheter är nödvändigt för att minimera skada ifall någon oönskad entitet tar kontroll; samtidigt bör kontrollen återställas snabbt och säkert vilket kan ske med flera säkerhetslager hos molnleverantören (Géczy, Izumi & Hasida, 2012).

På grund av den förflyttning av kontroll som följer med bruk av cloud computing har förlorad förmåga att migrera data och mjukvara kommit att bli en stor utmaning, ibland kallat v*endor lock-in* (Beslic et al. 2013) eller *data lock-in* (Armbrust et al. 2010) När en verksamhet väl har anlitat en leverantör kan de tendera att fastna och leverantören har egentligen inget incitament att motverka tendensen (Armbrust et al. 2010; Beslic et al. 2013; Vithayathil, 2018). Det innebär en risk, i och med att verksamheten kan bli låst till en leverantör som plötsligt ändrar sina säkerhetspolicies (Vithayathil, 2018). Leverantörsbyte och datamigrering är inte standardiserat och kan kräva oerhörda ansträngningar med *re-engineering*, som kan vara både kostsamma och tidskrävande (Vithayathil, 2018).

2.4 Litteratursammanställning

Tabell 2: Litteratursammanställning

Kategori	Aspekt	Författare
Cloud computing	● Grundläggande egenskaper med cloud computing ● Distributionsmodeller ● Tjänstemodeller ● Virtualiseringsteknik ● Cloud native	Alibaba Cloud (2020a) Amazon Web Services (2020a) Armburst et al. (2010) Battleson et al. (2016) Benlian et al. (2018) Chieu et al. (2009) Choudhary & Vithayathil (2013) Foster & Gannon (2017) Gannon, Barga & Sundaresan (2017) Google Cloud (2020a) Harris (2002) IBM Cloud (2020) Iyer & Henderson (2010) Jadeja & Modi (2012) Krancher, Luther & Jost (2018) Kratzke & Quint (2017) Kumar & Goudar (2012) Lawton (2008) Liu et al. (2018) Mell & Grance (2011) Microsoft Azure (2020a) Microsoft Azure (2020b) Patrizio (2018) Schneider & Sunayaev (2016) Synergy Research Group (2020) Orakwue (2010) Venters & Whitley (2012) Vithayathil (2018) Walraven, Truyen & Joosen (2014) Wang et al. (2008) Zhang, Cheng & Boutaba (2010)
Mjukvaruutveckling och distribution med cloud computing	● Software Development Life Cycle ● Secure Software Development Life Cycle	Boehm (1988) Guha & Al-Dabass (2010) Kulkarni & Gulvani (2016) Pressman (2005) ProductPlan (u.å.) Ragunath et al. (2010) Rittinghouse & Ransome (2016) Wikipedia (2020)
Säkerhetsutmaningar med cloud computing	● Information- of datasäkerhet ○ Konfidentialitet ○ Integritet	Aldossary & Allen (2016) Andress (2011) Armbrust et al. (2010)

	○ Tillgänglighet ● Datakontroll och ansvar	Beslic et al. (2013) Brodkin (2008) Chow et al. (2009) Davidovic et al. (2014) Géczy, Izumi & Hasida (2012) Harris (2002) Julisch & Hall (2010) Kumar & Goudar (2012) Loch, Carr & Warkentin (1992) McAfee (2012) Mell & Grance (2011) Munk (2019) Popović & Hocenski (2010) Rizwan & Zubair (2019) Samonas & Coss (2014) Shivpuriya (2017) Tchernykh et al. (2019) Venters & Whitley (2012) Vithayathil (2018) Whitman & Mattord (2011) Zissis & Lekkas (2012)

3 Metod

I den här studien samlar vi in kvalitativa data för att besvara vår forskningsfråga om hur verksamheter hanterar specifika säkerhetsutmaningar i samband med att de använder cloud computing för att utveckla och distribuera mjukvara. Kvalitativa metoder lämpar sig mer för meningar och innebörder än statistisk verifierbara sammanhang och fenomen (Alvehus, 2013; Jacobsen, 2002) och metoden tar, som grund för empiri, fram respondenternas unika betraktelsesätt (Ryen, 2004). Därmed lämpar sig en intervjuundersökning för vår studie. En kvalitativ undersökning ger deskriptiva svar på *hur* och *varför* någon gör eller tänker något (Rienecker & Stray Jörgensen, 2014; Alvehus, 2013). En kvalitativ undersökning kan gå djupet, eftersom respondenterna får utrymme att nyansera sina svar, ge förtydliganden där det behövs och ge exempel eller fallbeskrivningar (Rienecker & Stray Jörgensen, 2014). Givet utformningen av vår forskningsfråga är kvalitativa data lämpliga att besvara den, eftersom den efterlyser en deskriptiv beskrivning och innebörder av hur verksamheter en uppsättning specifika utmaningar.

En kvantitativ studie riskerar att ge mindre granulär data från ett större antal respondenter (Jacobsen, 2002; Bryman, 2013), men vi anser att de förlorade detaljerna är avgörande stora för att göra en kvantitativ undersökning relevant för den här studien. Det är tänkbart att utforma enkätfrågor som informerar vår forskningsfråga, men insatsen som krävs av respondenten i form av längre utläggningar i en enkät gör att vi riskerar att få icke-uttömmande och icke-satisfierande svar, eller helt enkelt uteblivna svar. Det finns en inneboende risk med kvalitativa studier, i det att de data som samlas in är otillräckliga för att underbygga slutsatserna (Oates, 2006). Däremot är en av metodens största fördelar att arbetssättet skapar en djup struktur (Ryen, 2004).

Vi har valt att använda oss av semistrukturerade intervjuer eftersom vi bedömer det sannolikt att intervjuobjekten har en del att säga inom ämnet och relaterat till forskningsfrågan, givet att de får utrymme att uttrycka sig. Semistrukturerade intervjuer är lämpliga för relativt outforskade områden (Jacobsen, 2002) och är den vanligast förekommande intervjuformen (Alvehus, 2013). Vi måste inte tvunget ha svar på de frågor vi har tagit fram; frågorna är snarare en guide genom samtalsämnen som anknyter till forskningsfrågan. I en kvalitativ studie med semistrukturerade intervjuer kan intervjudispositionen ändras allteftersom studien fortskrider (Jacobsen, 2002) eller inom den enskilda intervjun (Oates, 2006). Genom att använda semistrukturerade intervjuer är det möjligt att ställa följdfrågor och utforska ett ämne som kommer upp under intervjun, snarare än att vara tvugna av metodval att gå vidare till nästa fråga (Alvehus, 2013). En alltför strukturerad intervju tar bort en stor del av poängen med att använda intervjuer, nämligen det interaktiva elementet (Alvehus, 2013). Semistrukturerade intervjuer kräver att intervjuvärdarna lyssnar aktivt och ställer följdfrågor som är relaterade till de svar som intervjuobjektet ger (Alvehus, 2013). Till följd av detta lämpar sig semistrukturerade intervjuer för vår studie.

I planerade intervjuer ges vanligen intervjufrågor ut i förväg och det avsätts tid för intervjun i god tid före intervjun, medan i överraskande intervjuer görs varken eller (Jacobsen, 2002). Överraskande intervjuer ger utrymme för spontana och impulsiva åsikter medan planerade intervjuer ger möjlighet för intervjuobjekten att förbereda sina svar (Jacobsen, 2002). Vi har valt att inte skicka ut intervjuguide eller frågor i förväg för att se till att intervjuobjekten svarar utifrån sin erfarenhet och för att undvika att ge intervjuobjekten en möjlighet att ‘läsa

på' och ge teoretiskt grundade 'rätt svar', men intervjuerna i sig bekräftade vi i god tid förväg. Varje intervjurespondent fick själv möjlighet att inverka på datum och tid för intervjuer och vi bokade slutliga intervjutider med minst en veckas varsel.

Vi tagit fram en kort intervjupresentation som vi använder under intervjun för att ge intervjuobjekten en översiktsbild av intervjuns upplägg och för att kort presentera de teoretiska områden vi berör. Detta för att bekräfta att vi och intervjuobjektet har samma förståelse för de begrepp som vi använder och för att väga upp för att vi inte skickar ut intervjufrågor i förväg (se bilaga 2: Intervjupresentation). Intervjupresentationen presenterar studiens syfte, de metoder vi använder för att bearbeta data och de principer vi fastslagit för att studien ska uppnå de etiska värden vi eftersträvar.

Vi har hållit intervjuerna enskilt och vi har inte behövt göra ändringar i intervjuguiden mellan intervjuer. En risk med semistrukturerade intervjuer är avvikelser från ämnet (Ryen, 2004). Vi har inte råkat ut för det; lärdomen vi tog med oss från tidigare intervjuer till senare är att det är lätt att fastna vid en viss aspekt av studien och därmed måste vi, i egenskap av intervjuvärdar, se till att gå vidare till nästa ämne för att hinna med alla aspekter på avsatt tid. Intervjupresentationen hjälpte oss att inte glida ifrån ämnet och tjänade som påminnelse om vilket material som behöver behandlas.

3.1 Urval

Intervjuer med personer som är bekanta kallas bekvämlighetsurval (Jacobsen, 2002). Om de bekanta istället hänvisar till en annan person kallas det snöbollsurval (Jacobsen, 2002). Vi har mailat och ringt i våra sociala och professionella kontaktnät för att få tag på intervjuobjekt som lämpar sig för vår studie. Vi har tillfrågat åtta personer varav fyra accepterade och en hänvisade till en, i sin mening, mer lämplig kollega. Därmed utgör vårt urval lite av båda typer.

Ett strategiskt urval innebär att det utformas specifikt utifrån de undersökningsfrågor som ställs (Alvehus, 2013; Ekengren & Hinnfors, 2006). Vårt urval har ett strategiskt element i sig - det består av nyckelpersoner i verksamheter som utvecklar och distribuerar mjukvara med hjälp av cloud computing, eller personer som konsulterar och rådgör i tekniska och säkerhetsmässiga frågor åt sådana företag (se tabell 3: Urval- och intervjuprotokoll). Med nyckelpersoner menar vi personer som har insikt i verksamhetens IT-infrastruktur och hur verksamheten påverkas eller kan påverkas av olika säkerhetsaspekter. Exempel på roller i verksamheterna vi har intervjuat är IT-chef (CTO), backend-utvecklare och informationssäkerhetskonsult.

Vi har adderat dimensionen "konsulterar och rådgör" är för att få en mer nyanserad bild av hur verksamheter hanterar utmaningarna. *Outsiders* kan ibland ge en väl så insatt bild som *insiders* (Alvehus, 2013) och det är viktigt med en variation bland urvalet (Ekengren & Hinnfors, 2006). Vi kompletterade därför vårt urval med en person, en outsider, som inte är anställd eller delägare av verksamheterna den beskriver men trots det har god insyn i verksamheternas hantering av de ämnen som ingår i vårt forskningsområde.

3.1.1 Presentation av intervjuobjekt

Nedan presenterar vi de utvalda inrervjuobjekten. En sammanställning presenteras i tabell 3: Urval- och intervjuprotokoll.

Intervjuobjekt 1 arbetar på ett litet bolag med tio anställda, varav åtta är mjukvaruutvecklare och två jobbar med sälj och marknad. Verksamhetens tonvikt ligger på teknikutveckling, där de utvecklar och distribuerar en plattform i vilken deras kunder kan bygga digitala processer, med stort fokus på meddelandehantering. Intervjuobjektet beskriver att verksamheten primärt använder Amazon som molnleverantör och de har över fem års erfarenhet av att jobba med Amazon Web Services (AWS), men har även viss erfarenhet av Microsoft Azure. Intervjuobjekt 1 är delägare av företaget, är utvecklingschef och har mångårig erfarenhet av att jobba med mjukvaruutveckling och cloud computing.

Intervjuobjekt 2 arbetar på en liten konsultbyrå med cirka tio anställda. Verksamheten utvecklar moderna webblösningar, ofta med hjälp av serverlösa tjänster eller molntjänster, internt och externt mot kund. De använder sig främst av Amazon för infrastruktur men har även erfarenhet av Azure som PaaS-tjänst. Intervjuobjekt 2 är grundare, är utvecklingschef på företaget och har mångårig erfarenhet av att jobba med utveckling och cloud computing.

Intervjuobjekt 3 arbetar på ett några år gammalt startup-bolag som utvecklar och distribuerar en plattform och handelsplats för branschspecifika produkter. Bolaget har tio anställda varav fyra är mjukvaruutvecklare. Intervjuobjekt 3 är grundare och utvecklingschef av företaget och har tidigare arbetat som Cloud Solution Architect på Google. Den molnleverantör som de använder för att driva sina tjänster med är Google Cloud Platform (GCP).

Intervjuobjekt 4 arbetar på en verksamhet som utvecklar mjuk- och hårdvara för dataanalys och -processering som sedan presenteras i olika gränssnitt och applikationer. Det har varit så många som 47 anställda i företaget, allt från utvecklare till produkt- och säljteam - men på grund av ett uppköp så är de idag endast elva anställda kvar i verksamheten, varav de flesta är utvecklare. De använder sig av och har ett nära samarbete med Amazon som primär molnleverantör, men använder sig även av många andra leverantörer efter behov och behag. Intervjuobjekt 4 har rollen som backend-utvecklare sedan tre år tillbaka.

Intervjuobjekt 5 jobbar på ett globalt konsultföretag som hjälper andra företag att granska att de efterlever lagar och regler och hjälper med att vidta rätt åtgärder. Intervjuobjekt 5 har arbetat med information- och IT-säkerhet i närmare 20 år, med erfarenhet av både privat och offentlig sektor, både som konsult och i linjeroller. Intervjuobjekt 5 arbetar inte själv med mjukvaruutveckling men konsulterar och rådgör till många utvecklande företag.

Tabell 3: Urval- och intervjuprotokoll

Intervjuobjekt	Roll	Storlek på företag	Datum och tid	Appendix
Intervjuobjekt 1	Delägare och utvecklingschef	10 anställda	22 april 2020 10:00-10:30, 16:00-16:30	3.1
Intervjuobjekt 2	Grundare och utvecklingschef	~ 10 anställda	21 april 2020 10:30-11:30	3.2
Intervjuobjekt 3	Grundare och utvecklingschef	10 anställda	21 april 2020 14:00-15:00	3.3
Intervjuobjekt 4	Backend-utvecklare och IT-infrastrukturarkitekt	11 anställda	22 april 2020 15:30-16:30	3.4
Intervjuobjekt 5	Information- och IT-säkerhetskonsult	> 150 000 anställda	28 april 2020 12:30-14:00	3.5

3.2 Insamling av empiriskt material

Samtliga intervjuer genomfördes i form av videosamtal med den digitala tjänsten Zoom. Vi valde videosamtal framförallt på grund av den rådande situationen med Coronavirusepidemien och COVID-19-sjukan som råder under 2020. Videosamtal ger oss andra fördelar, såsom att vi undviker att vi eller intervjuobjekten behöva resa till och besöka den andres arbetsplats, boka och hitta till mötesrum och dylikt. Detta är särskilt smidigt för oss, eftersom våra intervjuobjekt har sina arbetsplatser utspridda i flera delar av landet. Att träffa människor i sin egen miljö är till fördel eftersom deras beteende kan påverkas av omgivningen (Jacobsen, 2002). Verktyget (Zoom) tillåter oss att spela in ljud och bild, med redundans. Inspelning och transkription är nödvändigt för att inte missa något som sägs (Bryman, 2013). Under intervjuerna var även vi som intervjuvärdar på olika platser och på olika enheter. Därmed kunde vi skapa en säkerhet för att klara av risken att ett tekniskt fel skulle uppstå i en av enheterna eller inspelningarna.

Att sitta ansikte mot ansikte underlättar för människor att öppna upp sig, vilket är särskilt lämpligt för semistrukturerade intervjuer. (Jacobsen, 2002). Med Zoom är det möjligt att samtala både med och utan video (Zoom, 2020). Vi har alltid haft video påslaget och de vi intervjuat har haft det när de haft möjlighet till det. Vi har upplevt att det skapas en smärre samtalsbarriär i samband med videosamtal; en del av sömlösheten som finns i en vanlig konversation försvinner till följd av att kroppsspråk inte uppfattas lika väl som i vanliga möten. Här framkom en fördel med separerade intervjuvärdar; det skapades ingen samtalsasymmetri under intervjuerna. Kommunikation mellan intervjuarvärdarna gick inte smidigare eller enklare än med intervjuobjektet och därigenom hamnade fokus på intervjuobjektet.

3.2.1 Transkribering och bearbetning

Transkribering och reflektion är nödvändigt och underlättar för intervjuvärdar att identifiera viktig information från intervjuer (Jacobsen, 2002). Transkriptionen utgör dessutom första steget i empirisk analys (Alvehus, 2013).

Vi har strävat efter att transkribera intervjuerna ordagrant och kort inpå att intervjun har genomförts för att inte gå miste om något som intervjuobjekten uttalar sig om. Vi har utelämnat att transkribera vissa utfyllnadsord och ofullständiga meningar som inte tillför något till samtalet eller skadar läsbarheten i transkripten. Vid en psykologisk intervjustudie kan det tänkas att det är nödvändigt att skriva ut varje paus för eftertanke och varje stavelse som intervjupersonen uttalar, eftersom det är önskvärt att fånga även sådant som är osagt eller sägs mellan raderna eller andra samtalsmässiga undertoner. Inom vår studie anser vi det osannolikt och orimligt att utgå ifrån att våra intervjurespondenter har anledning att dölja åsikter eller att de har svårt att uttrycka sig om frågorna; de ska bara uttrycka sig om ett förfarande som de är delaktiga i. Det finns ingen nämnvärd laddning eller känslomässiga undertoner som vi behöver fånga upp och därför kan vi utelämna intervjuobjektens rättelser av sina egna felsägningar, utfyllnadsord och dylikt. Även de delar av intervjuerna som består av att vi som intervjuvärdar presenterar oss själva, teoretisk bakgrund till frågeavsnitt, intervjulogistiska diskussioner eller övrig diskussion som inte hör till intervjun har utelämnats. Till intervjuerna avsatte vi 60 minuter, inklusive beskrivning och presentation av begrepp och förhållanden kring anonymisering och lov att spela in.

Bearbetningen av data genomförs i ett antal steg: först transkribering och reflektion, sedan kortfattad beskrivning av data och slutligen kategorisering och tolkning av data (Jacobsen, 2002). Vi har gjort det i enighet med intervjuguidens teman. Omedelbart efter intervjuerna höll vi ett internt möte där vi diskuterade ämnen som kom upp under intervjun. Vi transkriberade intervjuerna så kort inpå detta som möjligt. Sedan sammanfattade vi intervjuerna, passade in utsagor efter litteraturgenomgångens struktur och letade efter uppkomna, lämpliga teman för diskussion. Efter att intervjuerna hade sammanfattats, kategoriseras sammanfattningarna och placeras under respektive kategori eller aspekt. Slutligen tolkas de kategoriserade sammanfattningarna och skrevs om till löptext i vårt resultatavsnitt.

3.2.2 Intervjuguide

Våra intervjuer följde en struktur med fem kategorier, ett antal aspekter inom varje kategori och ett antal frågor inom varje aspekt. De första tre kategorierna ger en bakgrund till forskningsområdet medan de två sista ger svar på utmaningarna för vår studie. Tabell 4: Intervjuguide visar kategorierna, aspekterna och referens till intervjufrågorna som går att hitta i bilaga 1: Intervjuunderlag.

Tabell 4: Intervjuguide

Kategori	**Aspekt**	**Intervjufrågor**
Bakgrund	Övergripande, verksamhet	1.1, 2.2, 2.3
	Molnleverantör	2.1

Cloud computing	Tjänstemodell och abstraktionsnivå	2.1
	Distributionsmodell	2.1, 2.4
Mjukvaruutveckling och -distribution	SDLC, SecSDLC	3.1, 3.2, 3.3, 3.7
	Leverans-/ distributionssätt	3.6
	Organisatorisk påverkan från molnleverantör	3.3, 3.4, 3.5, 3.7
	Teknisk påverkan från molnleverantör	3.1, 3.3, 3.4
	Interaktion med molnleverantör	3.2
Information- och datasäkerhet	Konfidentialitet	4.1, 4.2, 4.3
	Integritet	4.4, 4.5, 4.6, 4.7
	Tillgänglighet	4.8, 4.9, 4.10
Datakontroll och ansvar	Vendor Lock-in	5.1, 5.2
	Motsättning i intressen mellan användare och leverantör	5.2
	Förtroende och tillit	5.2, 5.3, 5.4
	Inflytande, kontroll och ansvar	5.4, 5.5, 5.6

3.3 Reliabilitet

Reliabilitet avser huruvida forskningsresultat är upprepningsbara, det vill säga att metoden visar samma resultat varje gång (Alvehus, 2013; Rienecker & Stray Jörgensen, 2014). Eriksson och Wiedersheim-Paul (2008) menar att det inte är meningsfullt att tala om reliabilitet i kvalitativa studier och hävdar att många metodutvecklare menar att kvalitativa undersökningar bör utvecklas enligt egna principer. Den empiriska data vi samlat in baseras på en uppsättning intervjuobjekt och verksamheter som är unika i sig, varför vår studies resultat har färgats av deras åsikter och erfarenheter. Vid analys är det viktigt att skilja på person- och ämnescentrerad analys (Jacobsen, 2002). För att undvika en personcentrerad analys av intervjuerna har vi noga utformat intervjufrågorna till att avhandla problemområdet, strukturerat intervjun på upprepningsbart vis och satt upp tydliga kriterier för vårt urval. Vi har försökt att uppnå reliabilitet i vår studie genom att tydligt förklara bakgrund och syfte till

studien för intervjuobjekten. Det har vi gjort med hjälp av en intervjupresentation (se bilaga 2: Intervjupresentation) i vilken vi på ett identiskt vis gett en bakgrund till de begrepp och ämnen vi senare ställer frågor kring för att ge samtliga intervjuobjekt samma förståelse för studien och vad vi ämnar undersöka.

3.4 Validitet

Validitet avser huruvida det som undersöks eller mäts är det som var avsett att undersökas eller mätas (Alvehus, 2013; Rienecker & Stray Jörgensen, 2014). I en undersökning som har hög validitet bör det finnas en god överensstämmelse mellan de teoretiska begreppen och operationella indikationerna (Ekengren & Hinnfors, 2006). Vi har försökt uppnå detta genom att ge bakgrund till samtliga intervjuobjekt på ett identiskt vis.

En fördel med kvalitativa studier med semistrukturerade intervjuer är att det underlättar att säkra hög intern validitet (Jacobsen, 2002), men det finns svårigheter med att mäta validitet i kvalitativa undersökningar i och med att tolkningsprocesser baseras på att vi aktivt väljer ut delar av verkligheten och sätter in dem i specifika sammanhang (Alvehus, 2013). I intervjuundersökningar har intervjuvärdarna, jämfört med många andra metoder, möjlighet att påverka hur materialet som sedan ska analyseras faktiskt ser ut (Ekengren & Hinnfors, 2006).

Två huvudsakliga kategorier av validitet är *intern* och *extern* validitet, där intern validitet beskriver hur pass väl författarna mäter det som är avsett att mäta och extern validitet beskriver i vilken grad en studie kan generaliseras (Bryman & Bell, 2011). I brist på extern validitet kan studien råka ut för ett fenomen som kallas generaliseringsproblemet, det vill säga att den data som samlats in är från så pass specifika fall att det inte går att generalisera på andra fall (Jacobsen, 2002; Bryman & Bell, 2011). Vi försöker uppnå intern validitet genom att dela in intervjufrågorna i kategorier och aspekter som går i linje med vår forskningsfråga (se tabell 4: Intervjuguide) och ge samtliga intervjuobjekt en förklaring och definition av begrepp och ämnen som vi använder för att undvika missförstånd. Vi försöker uppnå extern validitet genom att ha tydliga urvalskriterier och använda breda och generellt applicerbara begrepp och teorier som är tillämpbara på många olika typer av verksamheter, t.ex. mjukvaruutveckling inom den breda kategorin av utvecklingsprocesser (SDLC) eller samtliga distributionsmodeller inom cloud computing, med undantag för community cloud.

Alvehus (2013) beskriver tre alternativa begrepp för validitet: *hantverksvaliditet*, *kommunikativ validitet* och *pragmatisk validitet*. Hantverksvaliditet grundas på metodiskt arbete med datainsamling och analyser (Alvehus, 2013) vilket vi i vår studie försöker uppnå genom att strukturera våra intervjuer enligt en intervjuguide (se tabell 4: Intervjuguide) och transkribera intervjuerna i efterhand för att läsa av det intervjuobjekten säger ordagrant. Kommunikativ validitet handlar om att testa de kunskapsanspråk som görs i dialog (Alvehus, 2013). Detta testas under våra seminarier, där vi får försvara vår datainsamling, urval och vår analysprocess. Slutligen handlar pragmatisk validitet om att kunskapen blir relevant i det den är avsedd att vara relevant för (Alvehus, 2013). Vår studie undersöker aktuella fenomen som uppstår i samband med att verksamheter använder modern teknologi; därmed anser vi att kan anses pragmatisk och relevant för såväl akademiker som praktiker.

3.5 Etik

I en undersökning bör intervjuvärdarna informera om vilka de är, studiens syfte och vad empirin ska användas till (Oates, 2006). Detta gör vi först övergripande, i samband att vi först kontaktar möjliga intervjuobjekt och i detalj i början av intervjun. Intervjun fortskrider och spelas in, endast om intervjuobjekten accepterar de villkor som vi föreslår. I våra intervjuer har vi bett om samtycke, både för att spela in intervjun för transkribering och för att använda det empiriska material vi samlade in under intervjun till vår studie. Detta utgör uppfyllt krav på intervjuobjektens informerade samtycke, som utgör ett av Jacobsens (2002) etiska grundkrav. Vi anonymiserar de insamlade data och kommer varken att exponera personen i fråga eller verksamheten personen är delaktig i, i vår studie. Alla ska erbjudas förbli anonyma (Oates, 2006). För att undvika exponering av verksamheter har vi gjort beskrivningarna av verksamheterna i vår presentation av empiriska data specifika nog att det tillför sammanhanget, men så generaliserade att det inte går att identifiera vare sig företag eller intervjuobjekt. På så vis uppfylla Jacobsens (2002) krav på intervjuobjektens respekterade privatliv. Vår analysmetod underbygger intervjuobjektens rätt att bli korrekt återgivna.

4 Empiriskt resultat

4.1 Mjukvaruutveckling med cloud computing

I de initiala faserna inför ett projekt - kravinsamling, planering och design - fick vi intrycket att molnleverantören inte var särskilt inblandad förutom i planering av kapacitet och hårdvarukrav. Intervjuobjekt 2 beskrev att de använder sig av en kostnadskalkylator från Amazon för att uppskatta kostnader. Intervjuobjekt 4 beskrev hur Amazon aktivt analyserar och ger tips på bättre lösningar för att få ner kostnader eller förbättra prestanda. Intervjuobjekt 1 beskrev att de inte jobbar särskilt projektorienterat och behöver således sällan genomföra ett kravinsamlingsarbete men att de däremot kontinuerligt arbetar med säkerhetsplanering. På liknande sätt beskrev intervjuobjekt 3 att de inte genomför någon strukturerad säkerhetsanalys och att kravinsamling sker kontinuerligt.

De flesta av verksamheterna använde sig av olika typer av kontroller och tester försedda av molnleverantören för att övervaka sin trafik, kapacitet, prestanda och kostnad. Intervjuobjekt 2 beskrev hur de finns olika nivåer av övervakning. Den första nivån är program och script de själva skrivit för att övervaka vissa tröskelvärden och funktioner, t.ex. e-posthantering eller prestandakostnad. Den andra nivån är molnleverantörens egna regler och tröskelvärden som automatiskt kan stänga ner och stoppa tjänster om de utsätts för missbruk. Ett sådant exempel är Amazon Cloud Watch, som innehåller små övervakningsprogram över interna program och hårdvara.

Intervjuobjekt 4 beskrev vikten av att kontrollera all kod som publiceras och att de hade en kontroll för att minst fyra ögon ska kolla på varje kodrad innan den distribueras medan intervjuobjekt 1 beskrev hur de diskuterar scenariobeskrivningar internt i verksamheten för att komma fram till vad som kan missbrukas. Intervjurespondenterna från de utvecklande verksamheterna, intervjuobjekt 1–4, lägger mycket vikt vid säkerhetsarbetet i sin egen ände - i sin kod, arkitektur och i sina applikationer. Intervjuobjekt 3 lägger tonvikt i att när de rekryterar ser till att ta in anställda som är säkerhetsmässigt kunniga och har ett säkerhetstänk i vad de gör. Säkerhetsriskerna som verksamheterna identifierar och arbetar med att motverka ligger i den egna verksamheten och sällan i, eller i överlapp med, det som anses vara molnleverantörens verksamhet.

I frågan om intervjuobjekten kände att deras verksamheter är begränsade av sin molnleverantör i förhållande till kompabilitet mellan ramverk och språk så svarade de flesta att de inte gjorde det. Tjänsteutbudet beskrevs som så stort (hos Amazon) att det snarare var svårt att navigera. Intervjuobjekt 5 beskrev utbudet som i praktiken obegränsat. Däremot beskrev intervjuobjekt 2 det stora utbudet som en utmaning, eftersom man blir låst till molnleverantörens sätt att tänka och göra saker på och att de därför tar höjd för det redan i utvecklingen med användning av öppna ramverk. Intervjuobjekt 3 beskrev att de använder sig av det öppna ramverket Kubernetes och därmed har möjlighet att på ett snabbt och smidigt sätt flytta applikationer mellan leverantörer. Intervjuobjekt 4 menar att molnleverantörerna gör ett väl genomfört arbete i att förutspå och följa efterfrågan av språk och ramverk, samt att det historiskt sett har visat sig att de språk och ramverk som de har förutspått ska växa har gjort det.

Vid frågan om de ansåg att deras utvecklingsprocesser har förändrats/anpassats vid användning av molnleverantörer så var svaret genomgående att den har förändrats i den mån att molnleverantören gett nya möjligheter. Molnleverantörer har gett verksamheterna möjlighet att snabbt komma igång med projekt och starta igång instanser av virtuella maskiner och samtidigt tvingat distributionen att bli automatiserad eftersom det är "svårt att administrera hundratals servrar manuellt" (Intervjuobjekt 1). Intervjuobjekt 3 beskriver hur molnleverantörerna har låtit företaget fokusera på sin kärnverksamhet (mjukvaruutveckling) istället för att lägga resurser på infrastruktur. Intervjuobjekt 5 menar att det snarare är så att en verksamhet flyttar till molnet för att verksamheten använder moderna utvecklingsmetoder med krav på infrastruktur som den interna IT-avdelningen inte kan tillgodose, än att verksamheten först flyttar till molnet och sedan ändrar sin utvecklingsprocess.

4.2 Hantering av information- och datasäkerhet

Information- och datasäkerhet utgörs av tre grundpelare: *konfidentialitet*, *integritet* och *tillgänglighet*. Intervjuobjekten beskrev hanteringen av information- och datasäkerhet i flera olika nivåer: säkerhetsarbete med mjukvaruutveckling av egna tjänster och applikationer, säkerhetsarbete för att skydda den infrastruktur de använder hos molnleverantörer samt molnleverantörenas säkerhetsarbete med att skydda plattformen.

4.2.1 Konfidentialitet

Intervjuerna gav oss intrycket att de flesta verksamheter arbetar aktivt med att skydda konfidentialiteten av information med hjälp av kryptering, åtkomstbehörigheter och andra typer av inloggningsskydd som tvåfaktorsautentisering på kritiska tjänster (t.ex. AWS-kontot). Intervjuobjekt 1 beskrev hur de hade arbetat och sett över sina användarroller; tagit bort de som inte borde ha åtkomst eller gett nya behörigheter till användare som borde ha mindre åtkomst. Samtidigt övervakar de sina användare för att kontrollera oönskat eller avvikande beteende, såsom hur ofta de är inloggade eller när senast de ändrade lösenord. Intervjuobjekt 2 ansåg att deras känsligaste punkt var det fysiska rummet och hade därför sett till att alla anställdas enheter, såsom datorer och telefoner, är krypterade så att informationen inuti enheterna är svårtillgängligt. De delar dessutom anonymiserade data från sina databaser för att ge vissa användare möjlighet att arbeta med data utan att avslöja verkliga data, t.ex. känsliga kunddata.

Intervjuobjekt 3 och 4 beskrev hur de inom sina företag är varsamma med vilka tjänster de ansluter mot molntjänsten och att de använder en mikrotjänstarkitektur, vilket minimerar antalet tjänster och delar av deras system som har åtkomst till olika informationskanaler. Intervjuobjekt 5 nyanserar verksamheters ansvar för att skydda konfidentialitet genom att ge exempel på hur myndigheter hanterar molntjänster; myndigheten för digital förvaltning (DIGG) säger att information anses röjd om den ligger på en molntjänst och därför får myndigheter inte använda molnleverantörer från utlandet som har lagar som säger att staten får hämta information utan att informera kunderna. Intervjuobjekt 5 menar att det enda sättet att kringgå konfidentialitetsbrott eller industrispionage från främmande makter är att kryptera allting med en öppen och godkänd krypteringsstandard som endast verksamheten själva har nyckeln till, vilket enligt intervjuobjektet onekligen är en krävande och komplicerad process.

4.2.2 Integritet

Verksamheterna hanterar information- dataintegritet genom att övervaka sina system och sin data med hjälp av diverse interna övervakningssystem och verktyg som tillhandahålls från molnleverantören. Intervjuobjekt 1 beskrev hur de kontinuerligt tittar på loggar för att upptäcka dataförlust eller -manipulation och Amazon Cloud Watch för att varna om vissa saker, särskilt hur system är anslutna till varandra. Intervjuobjekt 2 beskrev ett av deras mest avancerade system för att skapa redundans som ett skydd mot dataförlust och -manipulation; tre databaser i synk, två hos molnleverantören och en lokalt som håller en kopia i realtid, en daglig säkerhetskopia och en månatlig säkerhetskopia. Denna uppsättning ger, enligt intervjuobjekt 2, företaget ett skydd mot akut dataförlust men också möjlighet att jämföra data mot andra perioder för att upptäcka avvikelser.

Intervjuobjekt 4 berättade att företaget har flera olika versioner av sina databaser och att de använder många tjänster, hos sin molnleverantör och andra leverantörer, för att övervaka allt i systemen, bland annat övervakar de transaktioner för att upptäcka avvikelser. Vidare förklarar intervjuobjekt 4 att det är upp till dem själva att aktivt avgöra vad de vill övervaka mer noggrant, men att molnleverantören generellt sett är bra på att upptäcka och meddela om avvikande beteende. Intervjuobjekt 3 beskriver att de gör säkerhetskopior men inte har något system för att upptäcka om deras data går förlorad eller manipuleras. De hade gärna velat ha det, men de har ännu inte funnit tid att implementera något system för det.

Intervjuobjekt 5 förklarar att det är svårt för verksamheter att veta om molnleverantörerna själva lever upp till den säkerhet de påstår eftersom utomstående egentligen inte får testa deras säkerhet med egna tester (t.ex. penetrationstester). Det utgör ett regelbrott mot plattformen och det är upp till molnleverantörerna själva att försäkra säkerheten genom att testa och publicera rapporter. Vidare påpekar intervjuobjekt 5 att det finns en stor integritetsproblematik med molntjänster som ägs av amerikanska och kinesiska bolag. De är mål för lagar och regler som säger att de måste lämna ut information och data, dekrypterad om de kan, till myndigheter och säkerhetsorganisationer som kräver det, utan att berätta det för sina kunder.

4.2.3 Tillgänglighet

Utmaningen med tillgänglighet upplevdes framförallt i form av driftstörningar eller överbelastningsattacker i och mot molnleverantören. De flesta intervjuobjekten underströk att det är ett sällsynt problem och att både de och molnleverantören aktivt arbetar med olika typer av skydd mot attacker som påverkar tillgängligheten. Däremot underströk intervjuobjekt 3 att molnleverantörenas SLA (Service Level Agreement) inte garanterar 100% upptid. Intervjuobjekt 5 påpekar att det finns tjänstenivåer, där man i någon mån får den tillgänglighet man betalar för. Intervjuobjekt 2 kunde minnas ett tillfälle omkring 2014–2015 där Amazon utsattes för en krasch som orsakade flera veckors nedtid för vissa kunder och tog i samband beslutet att alltid ha en lokal säkerhetskopia utanför molnleverantören för att ha möjlighet att starta upp tjänsterna hos en ny leverantör. Intervjuobjekt 1 beskrev att de upplevde tillfälliga driftstörningar under en längre period, vilket de åtgärdade genom att gå över till en hybridlösning hos molnleverantören med dedikerad hårdvara för vissa delar av den påverkade infrastrukturen.

Intervjuobjekt 5 beskriver att molnleverantörer generellt är mer tillgängliga och har bättre upptider än outsourcade serverhallar samt att de är duktiga på att hantera överbelastningsattacker eftersom de har olika nivåer av skydd som kan förhindra avvikande trafik från att nå nätverksnivå. Ett verktyg för att hantera överbelastningsattacker och som används av verksamheter med Amazon som molnleverantör är Amazon Shield. Intervjuobjekt 1 förklarar sin verksamhets strategi för ifall systemen ligger nere: inom fem minuter ska de ha börjat reagera och arbeta för att åtgärda problemet; om det inte är löst inom tjugo minuter så startas en ny instans hos molnleverantören; om problemet kvarstår efter en timme så ska de försöka få igång de mest kritiska tjänsterna hos en ny leverantör inom fyra timmar. De har dock inte gjort tester för att se hur väl de efterlever de tider som de har satt upp i sin strategi. Intervjuobjekt 4 uppger att de aldrig har upplevt någon nämnvärd driftstörning som har påverkat slutanvändaren och har heller ingen uttalad strategi för att bemöta utmaningen om det sker.

4.3 Synen på molnleverantörer, datakontroll och ansvar

Synen på molnleverantörerna är något tudelad beroende på vad som frågas efter. Om frågan är ifall de anser att molnleverantören tar ett säkerhetsansvar så är svaren enade bland intervjuobjekten från de utvecklande verksamheterna (intervjuobjekt 1–4): ja, det gör de. Samtliga beskriver att det ligger i molnleverantörens intresse likväl som verksamheterna att beakta säkerheten på plattformen och över infrastrukturen. Intervjuobjekt 1 säger att för att vara så stor som Amazon ställs det krav att hålla koll på sin integritet och säkerhet mot kunderna. Vidare förklarar intervjuobjekt 1 "*Skulle det visa sig att t.ex. amerikanska myndigheter har en bakdörr rätt in i alla system som kör hos Amazon, då skulle Amazon få väldigt stora problem.*". Intervjuobjekt 2 vittnar om samma sak och förklarar att de har stor tillit till att molnleverantören tar säkerhetsansvar och förklarar att om det skulle brista i säkerhet så hade molnleverantören själva förlorat pengar.

Däremot finns det en oro över den data- och tjänstekontroll molnleverantören har och vilken förmåga de har att migrera sin data och sina applikationer ifall de blir illa tvungna. Intervjuobjekt 2 beskriver att de ofta accepterar problematiken för att de anser att fördelarna väger tyngre, men förklarar vidare att det går med ganska små verktyg komma runt delar av det genom att använda olika oberoende ramverk. Intervjuobjekt 4 anser att alla tjänster bör fokusera på portabilitet och att det är en nyckelfaktor de tittar efter hos leverantörer. Intervjuobjekt 4 beskriver även att portabilitet eller flytthjälp är något som leverantörer erbjuder nya kunder. Intervjuobjekt 3 beskriver att de med relativ enkelhet kan migrera sina tjänster till en ny leverantör, men uttrycker även en viss riskmedvetenhet om de inte skulle ha tillgång till sin data. På liknande sätt beskriver intervjuobjekt 1 att databaserna är det mest kritiska för dem och det som hade varit viktigast att ha tillgänglig vid en migrering. Intervjuobjekt 5 påpekar att det givetvis är möjligt att göra sig leverantör-ambivalent, men om det visar sig att det inte längre går att lita på amerikanska eller kinesiska leverantörer av molntjänster har man inte mycket val och många verksamheter som är i molnet sitter fast i molnet - de kan röra sig mellan leverantörer, men de kan inte lämna molnet.

Intervjuobjekt 5 håller med om att molnleverantören tar ett säkerhetsansvar men menar samtidigt att alldeles för många verksamheter har ett osunt högt förtroende för molnleverantörerna. De verksamheter som har rört sig ut i molnet eller byggt sin verksamhet från grunden i molnet är redan där och har enligt intervjuobjekt 5 inget val - de måste helt

enkelt lita på leverantörerna. Den essentiella skillnaden, enligt intervjuobjekt 5, är att man har mindre att säga till om och svårare att ställa krav. Leverantörerna har stort intresse för kundernas informationssäkerhet för sina kunders räkning och är duktiga på det, men när myndigheter ber om åtkomst finns det inte så mycket de kan göra.

Alla intervjuobjekt från de utvecklande verksamheterna (intervjuobjekt 1–4) svarar på frågan om vilket säkerhetsansvar de tar, att de tar ansvar för säkerhet inom de applikationer och kod de själva producerar och säkerhet för infrastrukturen för tjänsterna som de nyttjar ligger helt hos leverantören. Det framgår att det finns en tydlig skiljelinje mellan vilket ansvar som ligger hos leverantören och vilket som ligger hos de utvecklande verksamheterna.

5 Diskussion

Utmaningen med information- och datasäkerhet växer allteftersom informationstillgångar blivit mer tillgängliga och värdefulla än tidigare. Molntjänsters inverkan på information- och datasäkerhet är delvis att det fysiska skyddet helt har blivit outsourcat och distribuerat. Delvis är det att nya tekniker och arkitektoniska mönster förändrar säkerhetsbilden. Användare vet i regel inte ens var deras tillgångar befinner sig, rent geografiskt - möjligtvis vet de vilken region eller land, men sällan mer än så. Molntjänsterna har många användare och skryter med hög tillgänglighet, men det innebär att data existerar på platser med större inneboende nätverksyta. Med traditionell IT behövde en attack av något slag, t.ex. en överbelastningsattack, vara riktad direkt mot verksamhetens egna datacenter för att verksamheten skulle påverkas. Till följd av molntjänsters stora utbredning kan verksamheter som använder molntjänster påverkas indirekt av en attack, riktad mot en för dem helt okänd användare, som befinner sig på samma nätverksyta.

Molntjänsters och dess leverantörers inverkan på datakontroll är stor och betydelsefull. Hela företags digitala verksamheter ligger ofta i molnleverantörenas händer. Molnleverantörerna väljer sällan, i vilket fall inte på ett öppet vis, att utöva denna kontroll men i praktiken sitter de på alla sina kunders *kill switch*. Ett fullgott alternativ, att nyttja molntjänsterna och samtidigt behålla full kontroll, finns inte tillgängligt för en bred publik och många verksamheter väljer att förbise eller acceptera vissa av de inneboende säkerhetsproblemen med att använda molntjänster.

5.1 Mjukvaruutveckling och -distribution i molnet

Faserna i SDLC kan upplevas som flytande, och även om de flesta verksamheter genomgår faserna i någon form kan det vara mer eller mindre medvetet eller avsiktligt. Molnleverantören blandas in på olika sätt i faserna, t.ex. med kostnadskalkyler i planeringsfasen eller övervakningsprogram i test- och underhållningsfasen. Många av de metoder och verktyg som verksamheter använder för att hantera säkerhet - intern kodgranskning, säkerhetskopior, tvåfaktorsautentisering eller mikrotjänstarkitektur - är inte unika eller annorlunda till följd av användning av molntjänster. Dessa används likväl av verksamheter som driver egna datacenter vilket tyder på att säkerhetshantering i samband med mjukvaruutveckling med molntjänster inte skiljer sig nämnvärt mot traditionellt säkerhetsarbete. Det är vanligt att molnleverantörerna tillhandahåller övervakningsverktyg som är inbyggda i plattformen. Molnleverantörer vill givetvis leverera de mjukvarutjänster som deras kunder vill använda och när de kommer från den egna plattformen underlättar det för användarna, men det bidrar också till att man byggs in i ett ekosystem.

I vår studie framkom det att verksamheter vidtar säkerhetsåtgärder och har säkerhet i åtanke under alla faser av utveckling och distribution. Det talas generellt om ett säkerhetstänk och -medvetenhet i hela processen, oavsett i vilken grad de anser att deras utvecklingsprocess går i linje med SDLC eller SecSDLC. Exempel på preventiva åtgärder är kodgranskning, testning och att slå fast regler och standarder för arkitektur och kod.

Det har framkommit att utvecklingsprocessen inte påverkas nämnvärt i sin struktur i och med användning av molntjänster. Däremot anses molnleverantören ge nya möjligheter och

tillhandahålla verktyg som underlättar processen. Användarna slipper hantera administration av infrastruktur, då mycket sköts automatiskt och molnleverantören förser användarna med övervakningsverktyg och olika nivåer av säkerhet, t.ex. på nätverksnivå.

De stora molnleverantörena förser i regel användarna med en så stor katalog av tjänster och ramverk att de beskrivs som “svåra att navigera i” eller “obegränsade”. Enligt våra data blir företag inte begränsade av molnleverantören i förhållande till mjukvarukompabilitet.

5.1.1 Molnleverantörens roll

Mjukvaruutveckling involverar en mängd parter, bland andra kunder, slutanvändare, testare och utvecklare, vilket gör proceduren komplex. När mjukvaruutveckling sker mot molntjänster blandas ytterligare en part in: molnleverantören. Molnleverantörens roll skiljer sig för olika verksamheter. I vår studie har det framkommit att för vissa företag är molnleverantörens roll passiv medan andra beskriver den som delaktig. När molnleverantören är delaktig hjälper de till att hantera optimeringar av mjukvara, arkitektur och infrastruktur för att minska belastning och kostnad. Det är givetvis så att molnleverantören förlorar intäkter på att bidra med tips för optimering, men alternativet att kunden flyttar till en annan leverantör är en större intäktsförlust - det ligger i molnleverantörens intresse att leverera bra tjänster, och inte bara mjukvarutjänster. Hur mycket molnleverantören aktivt deltar i utvecklingsprocessen beror på hur engagerad användaren är att inkludera molnleverantören och vilken maktposition eller inflytande användaren har, det vill säga hur stora de är och hur mycket de spenderar på plattformen.

5.2 Hantering av information- och datasäkerhet

I litteraturen beskrivs det hur hotet mot informationssäkerhet i samband med att användning av molntjänster. Data blir äventyrat på grund av en ökad exponering mot aktörer såsom användare, enheter eller applikationer. I vår undersökning framkom det att verksamheter delar den bilden och att de går varsamt fram när de ansluter olika mjukvarutjänster till sina system i molntjänster. De använder mikrotjänstarkitektur och i vissa fall öppna ramverk såsom Kubernetes, vilket ökar sammanhållning och minskar koppling i systemen och minimerar antalet åtkomstpunkter till information i systemen. Detta görs inte nödvändigtvis med informationssäkerhet som primärt syfte, men det har sekundära effekter till informationssäkerhetens fördel.

Den ökade exponeringen gäller även användare. Där vi har upptäckt att verksamheter i allmänhet tar till säkerhetsåtgärder i form av att använda olika autentiseringsskydd och åtkomstbehörigheter. Denna typ av skydd används även vid utveckling och distribution med traditionella tillvägagångssätt, men de är i högre grad nödvändiga i samband med den ökade exponeringen.

Flera av åtgärderna som verksamheter använder sig av för att styrka informationssäkerhet överlappar mellan de tre benen i CIA-triaden. Användarbehörigheter, kryptering och autentiseringsverktyg är åtgärder som bemöter både konfidentialitets- och integritetsutmaningar. Övervakning av system kan ske på olika sätt, så att det bemöter utmaningar i alla tre aspekter.

En preventiv säkerhetsåtgärd som vi har upptäckt att verksamheter använder sig av är säkerhetskopior utanför molntjänsten. Lokalt lagrade säkerhetskopior har å ena sidan fördelen att förbli opåverkat ifall molntjänsten blir korrupt eller otillgänglig men utgör å andra sidan en risk att bli konfiskerad eller förstörd i det fysiska rummet. I vår studie har det framkommit att vissa verksamheter betraktar just det fysiska rummet som den största säkerhetsrisken, i form av att någon utomstående kommer över en av deras enheter, såsom en bärbar dator eller mobiltelefon. Att ett lösenord eller enhet blir exponerad så att någon annan kommer åt delar av ett system är i första hand ett konfidentialitetsbrott, men lösenordet kan sedan användas till att manipulera eller sabotera data och eventuellt påverka systemets och delar av molntjänstens tillgänglighet för företaget.

5.2.1 Hantering av konfidentialitetsutmaningar

Datakryptering är en etablerad och specifik metod för att säkerställa konfidentialitet i information. Verksamheter krypterar särskilt känsliga data, såsom lösenord, för att skydda användarna i sina egna system. Molnleverantörer tillhandahåller ofta krypteringstjänster men för att uppnå fullständig konfidentialitet bör man använda öppna och godkända krypteringsstandarder och spara krypteringsnycklarna säkert och avskilt från molnleverantören. För att garantera den nivå av konfidentialitet som beskrivs ovan behöver dessutom all information och data som går in i molntjänsten vara krypterad innan den hamnar i molnet, vilket onekligen är ett omständligt förfarande.

Vårt sista intervjuobjekt talade om osunda tillitsnivåer bland praktiker och lyfte problematik kring statligt industrispionage från främmande makter och konstaterade detta som ett faktum. Samtidigt påpekade andra att om så vore fallet, skulle leverantörerna förlora kunder. Därmed råder det en nämnvärd klyfta i hur man betraktar verkligheten, i det avseendet. I efterhand hade vi gärna utforskat detta i samtliga intervjuer. Soghoian (2010) beskriver att stater har historiskt tvingat leverantörer att installera bakdörrar in av flera olika typer av mjukvaror och mjukvarutjänster, med varierat lagligt underlag, och bekräftar därmed denna risk. Risken för konfidentialitetsbrott genom industrispionage kan delvis bekräftas av formuleringar i integritetspolicies hos alla stora leverantörer; Amazon Web Services (2020b), Microsoft Azure (2020c) Google Cloud (2020b) och Alibaba Cloud (2020b) är alla är mål för lagar och regler i de länder som de är verksamma i. Därigenom kan molnleverantörerna inte garantera att information inte kan eller kommer lämnas ut till den stat och myndighet som reglerar molnleverantören - oftast USA eller Kina - och ofta utan kundens vetskap. Konfidentialitetsbrott från främmande makter är därmed svåra att upptäcka. Av denna orsak råder det het diskussion om huruvida svenska myndigheter kan använda sig av dessa tjänster (Barzey, 2019; Malmqvist, 2019; Kolsjö, 2019). Vi spekulerar att utvecklande verksamheter antingen inte är medvetna om denna bakdörr eller inte betraktar detta som en risk eller utmaning som är sannolik eller konsekventiell nog att bemöta.

5.2.2 Hantering av integritetsutmaningar

En utmaning och risk med cloud computing är integritetsskyddet för kritiska tjänster och känsliga data i en publik och delad molnmiljö. Vår studie har visat att verksamheter hanterar dataförlust eller avvikelser i data genom att alltid lagra en kopia av databaser på en server utanför molnplattformen, ibland i flera tidsintervaller. Det kan användas för att jämföra data och upptäcka avvikelser men även som en säkerhetsåtgärd för att försäkra tillgång till data.

Det finns ett antal övervakningstjänster hos molnleverantören som verksamheterna använder för att hantera integritetsbrott mot information och data. I vår studie framkom att verksamheter övervakar sina system med lösningar som tillhandahålls i och utanför molntjänsten de använder för att upptäcka avvikelser. Det har även framkommit att verksamheter använder sig av loggar och statistik försedda av molnleverantören för att se hur systemen används och att de inte missbrukas. Även missbruk av bearbetningskapacitet, dvs. serveranvändning, är ett integritetsbrott. Det förhindrar verksamheter genom att sätta upp övervakningssystem och tröskelvärden som varnar när de upptäcker avvikelser eller missbruk i användning. Övervakning är en preventiv åtgärd för att upptäcka avvikelser, likt många andra åtgärder för att skydda information- och datasäkerhet, som påvisar förmåga hos verksamheterna att resonera kring hoten.

Överlag uppfattar vi att verksamheter har relativt gedigen och adekvat hantering av säkerhet i förhållande till integritet. Verksamheter lär sig av verkligheten och vidtar åtgärder som återspeglar både riskernas sannolikhet och konsekvens. Det blir så av nödvändighet; verksamheter måste vidta åtgärder, men det tar tid och resurser; därmed får verksamheter helt enkelt göra en avvägning.

5.2.3 Hantering av tillgänglighetsutmaningar

Det har framkommit, i vår studie, att god tillgängligheten hos molnleverantören är en av de stora anledningarna till att verksamheterna använder molntjänster. Samtidigt utgör det en utmaning som består i att verksamheter behöver hantera oväntade tillgänglighetsavbrott, som exempelvis driftstörningar eller överbelastningsattacker.

Tillgängligheten kan påverkas indirekt på grund av molntjänsterna har väldigt stor nätverksyta, vilket är en följd av att infrastrukturens resurser poolas. Den tekniska lösningen för att möjliggöra resurs-poolning, virtualiseringsteknik, är också det som gör det möjligt för molnleverantörer att tillhandahålla god tillgänglighet över lag. I och med att de bryter den direkta kopplingen mellan hårdvara och instans/maskin kan molnleverantören flytta omkring maskiner, ifall en viss hårdvara skulle gå sönder eller ifall ett specifikt datacenter blir otillgängligt. Detta är även grunden för de till synes oändliga resurserna och molntjänsters generellt höga tillgänglighet.

Verksamheter väljer distributionsmodell baserat på sina behov, varav tillförlitlighet är en parameter. Den mest förekommande distributionsmodellen är *public*, som i regel är ett fullgott alternativ. Om verksamheten har ett högre säkerhets- och tillförlitlighetskrav är *private* eller åtminstone *hybrid* distributionsmodeller att föredra. Molnleverantörerna skriver ut i sina avtal (SLA) att de inte garanterar 100% upptid, men de erbjuder även olika nivåer av avtal. En verksamhet kan förhandla om att bli högre prioriterad, dvs. betala ett högre pris för ett SLA som garanterar bättre tillgänglighet.

Det har framkommit att vissa verksamheter har brottats med driftstörningar och löst det genom att använda mer dedikerad hårdvara hos molnleverantören, dvs. gå mer mot en hybridlösning. Andra har vid driftstörningar erbjudits att uppgradera till ett SLA med högre grad av tillgänglighet.

En annan strategi för att hantera tillgänglighetsutmaningar är att vara förberedd på att behöva flytta till en ny leverantör på kort tid. Det är en så åtråvärd lösning att leverantörer både

skryter med sin egen portabilitet och erbjuder flytthjälp till sina egna plattformar som tjänst, till förmånliga priser. Detta kan anses försvaga den inlåsningseffekt som kan uppstå i tekniska ekosystem.

Det framkom att vissa verksamheter inte har någon särskild strategi för att hantera otillgänglighet hos molnleverantörer, vilket delvis beror på att molnleverantörer generellt sett har hög tillgänglighet - bättre än traditionella serverhallar. Vissa verksamheter har inga egna nämnvärda upplevelser av tillgänglighetsavbrott och därför ingen formaliserad strategi gör att hantera det.

5.3 Hantering av datakontroll och ansvar

Att en viss typ av kontroll går förlorad när en verksamhet flyttar sin mjukvara till molnet råder inget tvivel om. Användarna förlorar kontroll över den fysiska säkerheten och hårdvaran, som länge har präglat informationssäkerhet. Ett visst inflytande över infrastrukturen förloras också. Verksamheter kan till mångt och mycket konfigurera infrastrukturen efter sina behov, lite beroende var på abstraktionsspektrumet molntjänsten de använder befinner sig, men vissa skydd och viss säkerhet som molnleverantören har implementerat har användaren lite att säga till om. I vår studie har det framkommit att kontrollförlusten inte betraktas som ett stort problem och det anses ligga i molnleverantörens intresse, likväl som användarnas, att beakta säkerheten på plattformen. Användare tar vissa preventiva åtgärder för att hantera kontrollförlust över data och tjänster, exempelvis att aktivt göra sina system plattformsoberoende, i den grad det är möjligt. Det har framkommit att portabilitet är en nyckelfaktor vid val av molntjänster och att verksamheter använder öppna ramverk som gör sina applikationer och lösningar portabla.

5.3.1 Tillit till molnleverantören

I och med den oundvikliga kontrollförlusten som kommer med användning av molntjänster behöver användarna i någon mån ha tillit för den leverantör de använder - vilket det också visat sig att de har. Molntjänster betraktas som en möjliggörande faktor, framförallt för verksamheter i startup-fasen, där de ofta är djupt investerade i molntjänster och ofta driver hela verksamhetens infrastruktur i molnet - de är s.k. *cloud native*-företag.

Det framkommer att utvecklande verksamheter överlag har närmast fullständig tillit till sina molnleverantörer, och av utomstående säkerhetskonsulter beskrivs det som närmast ohälsosam tillit. Det finns flera möjliga orsaker till att molnleverantörer har detta förtroendekapital; en av dem är att användare står i ett slags beroendeställning, om inte till sin molnleverantör så till molninfrastruktur i sig. Det antyds att många verksamheter väljer att helt enkelt hantera sin brist på inflytande och kontroll genom att blunda för de risker och hot som tillkommer i samband med användning av molntjänster, eller att betrakta konsekvensen som försumbar.

5.3.3 Överlapp i säkerhetsansvar

Litteraturen beskriver hur molnleverantörerna är ansvariga för *molnets* säkerhet men att användarna är ansvariga för säkerheten *inom molnet*, det vill säga de applikationer och tjänster som de distribuerar på molnplattformar. I vår studie framkommer det att verksamheter är medvetna om detta ansvar och att de tar det. Det överlappande säkerhetsarbetet är litet och ansvarsområden är tydligt separerade - det är därför ingen överraskning att verksamheter inte ser det som en stor utmaning. Verksamheter ser sig i stort som fullt ansvariga, förutsatt att det inte finns stora säkerhetsbrister hos leverantören.

Det har framkommit att säkerhetsarbete mellan mjukvaruutvecklare som använder molntjänster och molnleverantörer inte bara är väl separerade utan i praktiken inte *kan* spilla över till varandra, i varje fall inte från mjukvaruutvecklarnas sida. Vi har fått indikationer på att verktyg i molnplattformar kan ge tips och feedback på hur väl en databas är uppbyggd och därav är det tänkbart att mer generell, eventuellt automatisk, granskning av kod skulle kunna erbjudas som tjänst från molnleverantören. Däremot finns det inget utrymme för en kund till molnleverantören att testa leverantörens säkerhet - det betraktas som otillåtet och ett villkorsbrott mot tjänsten. Molnleverantören hanterar denna testning själv eller hyr in externa parter att testa säkerhet och publicerar sedan säkerhetsrapporter, som är upp till användare och kunder att läsa och lita på.

5.4 Metoddiskussion

Fyra av våra intervjuer var med nyckelpersoner på utvecklande verksamheter. Dessa fyra företag är också små företag. Detta utgör inte en del av vårt urval och vi betraktar det inte som förödande för studiens generalisering, men vi anser också att våra fynd och slutsatser med större reliabilitet kan appliceras på små företag än på stora företag. Den femte intervjun, med en säkerhetskonsult från ett globalt företag, anser vi breddar området som vi kan applicera våra fynd på. Det är trots det värt att påpeka denna omständighet och att vi betraktar det som sannolikt att det finns andra faktorer som spelar in på medelstora och särskilt på stora företag.

Små och särskilt unga verksamheter har förvisso enklare att vara *cloud native*, i och med att deras "bagage" är lättare, medan större verksamheter troligtvis sitter på ett *legacy* som inte lika enkelt går att flytta till molntjänster. Med det sagt undersöker vi inte utmaningar i samband med *flytten* till molntjänster, utan utmaningar i samband med *användning* av molntjänster. Vi kan därför endast hållas till svars på frågan om större verksamheter har andra förutsättningar än mindre verksamheter i sin hantering av utmaningar i samband med användning av molntjänster. Vi anser att förutsättningarna skiljer sig på två plan: (1) större verksamheter är troligtvis också en större och viktigare kund för molnleverantören än mindre verksamheter och har således en annan förhandlingsposition gentemot dem och (2) den exponering och den position de besitter gör troligtvis att de är i större grad utsatta för säkerhetshot och behöver lägga större resurser på säkerhet än mindre verksamheter. Vi anser våra fynd inte uteslutningsbara för medelstora, stora och gamla företag, men studiens underlag för att dra slutsatser om dessa kan betraktas som begränsat.

6 Slutsats

I vår studie har vi identifierat två huvudsakliga kategorier av åtgärder som verksamheter tar för att hantera (1) information- och datasäkerhet och (2) datakontroll och ansvar. De två kategorierna är (i) preventiva åtgärder vars huvudsakliga syfte är att hantera specifika säkerhetsutmaningar och (ii) val och beslut de gör i sin mjukvaruutveckling och -distribution som har ett andra primära syften, men som har sekundära effekter som utgör ett stöd gentemot säkerhetsutmaningarna.

Hantering av information- och datasäkerhet skiljer sig inte avsevärt, i princip, från säkerhetsarbete i system som inte bygger på molntjänster. Detta inkluderar att verksamheter formellt eller informellt förhåller sig till utvecklingsprocesser där säkerhetstänk får utrymme i alla processens delar. Verksamheter använder testning, precis som i utveckling utanför molntjänster, men molnleverantörer stödjer viss testning på sina plattformar. Verksamheter har kodgranskning inbyggt i sina utvecklings- och distributionsprocesser och letar efter utvecklare med säkerhetskompetens när det rekryterar.

Verksamheters primära hantering av information- och datasäkerhetsutmaningar är med preventiva åtgärder. Dessa innefattar bland andra säkerhetskopiering av data, både inom och utom sin primära molnleverantör, systematisk kryptering, övervakning och principer för autentisering och användarroller. Saker som verksamheter gör som har som sekundär effekt är att använda moderna ramverk och arkitektoniska mönster, såsom Kubernetes och mikrotjänstarkitektur. Ytterligare potentiella preventiva åtgärder är att välja en distributionsmodell med dedikerad hårdvara, förhandla om serviceavtal, som ger verksamheten större kontroll och ökad tillgänglighet, eller bygga sina system plattformsoberoende, så att de kan flytta mellan leverantörer om det skulle visa sig vara nödvändigt. Detta kan vara av direkt intresse för att bemöta utmaningarna eller av andra anledningar; det kan exempelvis vara en kostnads- eller prestandafråga.

Det finns i praktiken inget överlapp i säkerhetsansvar, så när infrastruktur väl är outsourcad hamnar allt säkerhetsfokus i det egna systemen, tjänsterna och applikationerna.

Verksamheter hanterar framförallt en minskad datakontroll med förtroende och tillit. Utvecklande verksamheter har ett mycket stort förtroende för säkerheten hos molnleverantörerna, ibland större än om de hade stått för infrastrukturen själva. Det beror dels på att de outsourcar infrastrukturen och därmed inte har lika mycket intern kompetens för infrastruktursäkerhet, dels för att de stora leverantörerna har oerhörda resurser och kompetenser inom infrastruktursäkerhet. Slutligen beror det stora förtroendet på att verksamheter ser stora fördelar med att använda molntjänster, och att de eventuellt inte har möjlighet sluta använda dem.

Bilagor

1. Intervjuunderlag

R: Hur hanterar verksamheter säkerhetsutmaningarna *information- och datasäkerhet* och *datakontroll och ansvar* i samband med att de använder cloud computing för att utveckla och distribuera webbtjänster och -applikationer?

Syfte: Vi vill få en överskådlig bild av vilka CC-lösningar intervjuobjektet använder och hur det påverkar deras utveckling och distribution för att få en grundlig bild av hur de hanterar säkerhetsutmaninagrna *information- och datasäkerhet* och *datakontroll och ansvar*.

Kategori	**Aspekt**	**Intervjufrågor**
Bakgrund	Övergripande, verksamhet	1.1, 2.2, 2.3
	Molnleverantör	2.1
Cloud computing	Tjänstemodell och abstraktionsnivå	2.1
	Distributionsmodell	2.1, 2.4
Mjukvaruutveckling och -distribution	SDLC, SecSDLC	3.1, 3.2, 3.3, 3.7
	Leverans-/ distributionssätt	3.6
	Organisatorisk påverkan från molnleverantör	3.3, 3.4, 3.5, 3.7
	Teknisk påverkan från molnleverantör	3.1, 3.3, 3.4
	Interaktion med molnleverantör	3.2
Information- och datasäkerhet	Konfidentialitet	4.1, 4.2, 4.3
	Integritet	4.4, 4.5, 4.6, 4.7
	Tillgänglighet	4.8, 4.9, 4.10
Datakontroll och ansvar	Vendor Lock-in	5.1, 5.2
	Motsättning i intressen mellan användare	5.2

	och leverantör	
	Förtroende och tillit	5.2, 5.3, 5.4
	Inflytande, kontroll och ansvar	5.4, 5.5, 5.6

1. Bakgrund

1. (Bakgrund) Beskriv er verksamhet.
    a. Hur många anställda? Hur många kontor? Vilka delar av landet och världen?

2. Cloud computing (CC)

Bakgrund: Cloud computing är en modell som möjliggör nätverkstillgång *on-demand* till en delad pool av konfigurerbara IT-resurser (t.ex. nätverk, servrar, lagring) som snabbt kan fördelas och släppas med minimal hantering eller ingripande från molnleverantör.

1. (Bakgrund/Avgränsning) Vilken/vilka CC-lösning(ar) använder ni er av för utveckling och distribution?
    a. Vid val av leverantör: genomförde ni en analys och/eller jämförelse av de olika molnlösningarnas datasäkerhet?
    b. Identifiera abstraktionsnivå
    c. Identifiera tjänstemodell
2. (Bakgrund) Hur lång erfarenhet har er verksamhet av att jobba med Cloud computing?
3. (Bakgrund) Beskriv vilka typer av mjukvaruapplikationer eller -tjänster ni utvecklar och distribuerar med hjälp av Cloud Computing.
    a. Vilken typ av säkerhetskrav finns för de tjänster och applikationer som ni utvecklar?
4. (Avgränsning) Använder ni er av CC-lösningar där ni delar resurser med andra (public), en CC-lösning där resurserna är dedikerade till er verksamhet (private) eller en kombination (hybrid)?

3. Mjukvaruutveckling och -distribution med CC
Bakgrund: Plattformar tillhandahåller miljöer att utveckla i och därför kan det finnas begränsningar i vilka ramverk och språk som är möjliga att utveckla och distribuera i.

Det finns ett antal faser (kravinsamling, planering, design, programmering, testning, distribution, underhåll och nedstängning) som ett utvecklingsprojekt genomgår, en livscykel som kallas SDLC. En utökning av SDLC som kallas SecSDLC och adderar identifikation av specifika hot och risker, följt av design och implementation av specifika kontroller för att bemöta dessa hot och hantera de risker som organisationen och/eller kunderna står inför. Alla utvecklare följer den här cykeln i någon mening.

1. (Bakgrund) Vilka verktyg och vilken information tar ni del av vid kravinsamling, planering och design av ett projekt från er molnleverantör?

2. (Preventiva åtgärder) Vid start av ett nytt projekt: genomgår ni något arbete för att identifiera och planera för eventuella säkerhetsrisker och hot?
    a. Om ja, beskriv hur detta förarbete ser ut och vilka aktiviteter ni gör.
    b. På vilket sätt är CC-leverantören inblandad?
3. (Preventiva åtgärder) Har ni någon kontroll och/eller testning för att upptäcka säkerhetshot och -risker?
    a. Tillhandahålls dessa av CC-lev.?
    b. Om ja, beskriv hur dessa kontroller och tester fungerar.
4. (Utmaning) Upplever ni er begränsade av er CC-leverantör, i förhållande till kompabilitet med språk och ramverk?
5. (Utmaning) Upplever ni att organisatoriska beslut påverkas av kompatibilitet hos leverantören?
6. (Utmaning) Upplever ni att det finns säkerhetsutmaningar med att distribuera (*deploy*) webbtjänster eller -applikationer med cloud computing?
    a. Om ja, hur hanterar och bemöter er verksamhet dessa brister/risker?
7. Påverkas era utvecklingsprocesser, till exempel genom att det tillhandahålls verktyg, av er CC-lev?

4. Information- och datasäkerhet:

Bakgrund: om man arbetar mot molnet finns det en ökad inneboende risk för attacker mot eller obehöriga intrång i ens tjänster eller applikationer. Cloud computing underlättar åtkomsten för en verksamhet att utveckla och distribuera tjänster och applikationer på olika platser och med olika enheter.

1. (Utmaning) Upplever ni att det finns en risk eller utmaning med att obehöriga får tillgång till känsliga data och kritiska applikationer?
    a. Om ja, hur hanterar ni den risken?
2. (Preventiv åtgärd) Har ni en strategi för att hantera och motverka ett intrång av en obehörig i er tjänst eller applikation?
3. (Utmaning) Har ni blivit utsatta för ett intrång av en obehörig i er tjänst eller applikation?
    a. Är det en utmaning för er?
    b. Om ja, beskriv vad som hände och hur ni hanterade det - ge exempel.
    c. Om nej, beskriv hur ni hade hanterad en sådan situation.
4. (Preventiv åtgärd) Har ni en strategi för att hantera och motverka en attack mot er tjänst eller applikation?
    a. Vad är er strategi?
5. (Utmaning) Har ni direkt eller indirekt utsatts för en attack mot er tjänst eller applikation?
    a. Om ja, beskriv vad som hände och hur ni hanterade det.
        i. Har det varit svårt att hantera?
        ii. Kommer ni ändra något i hur ni hanterade det till framtiden?
    b. Om nej, beskriv hur ni hade hanterad en sådan situation.
6. (Utmaning) Utför ni någon form av kontroll för att upptäcka avvikelser såsom dataförlust eller -manipulation?
7. (Utmaning) Gör ni kontroller för att upptäcka avvikelser i er tjänsteanvändning, såsom att någon annan utför beräkningar på er bekostnad? Av t.ex. icke-betrodda användare eller fjärrservrar.

8. (Utmaning) Har ni upplevt att er tjänst eller applikation inte varit tillgänglig, dvs. legat nere?
    a. Om ja, förklara vem som bar ansvaret och hur länge det pågick?
    b. Hur hanterade ni eller skulle ni hanterat en sådan situation?
9. (Utmaning) Har ni upplevt att den plattform och de verktyg ni arbetar med för mjukvaruutveckling och -distribution inte varit tillgänglig?
    a. Om ja, förklara mer ingående vad som inte var tillgängligt och hur länge det pågick?
    b. Hur hanterade ni eller skulle ni hanterat en sådan situation?
10. (Utmaning) Har ni upplevt att data och information som ni arbetar med inte varit tillgänglig?
    a. Om ja, förklara mer ingående vad som inte var tillgängligt och hur länge det pågick?
    b. Hur hanterade ni eller skulle ni hanterat en sådan situation?
11. (Utmaning) Är det någon kring er hantering av information- och datasäkerhet med användning av cloud computing som du vill tillägga?

5. Datakontroll och ansvar (tredje part):

Bakgrund: En viss kontroll går förlorad vid användning av en tredje part molnleverantör, däremot kvarstår det ansvar som ligger hos verksamheten i hur de säkerställer och hanterar information och data.

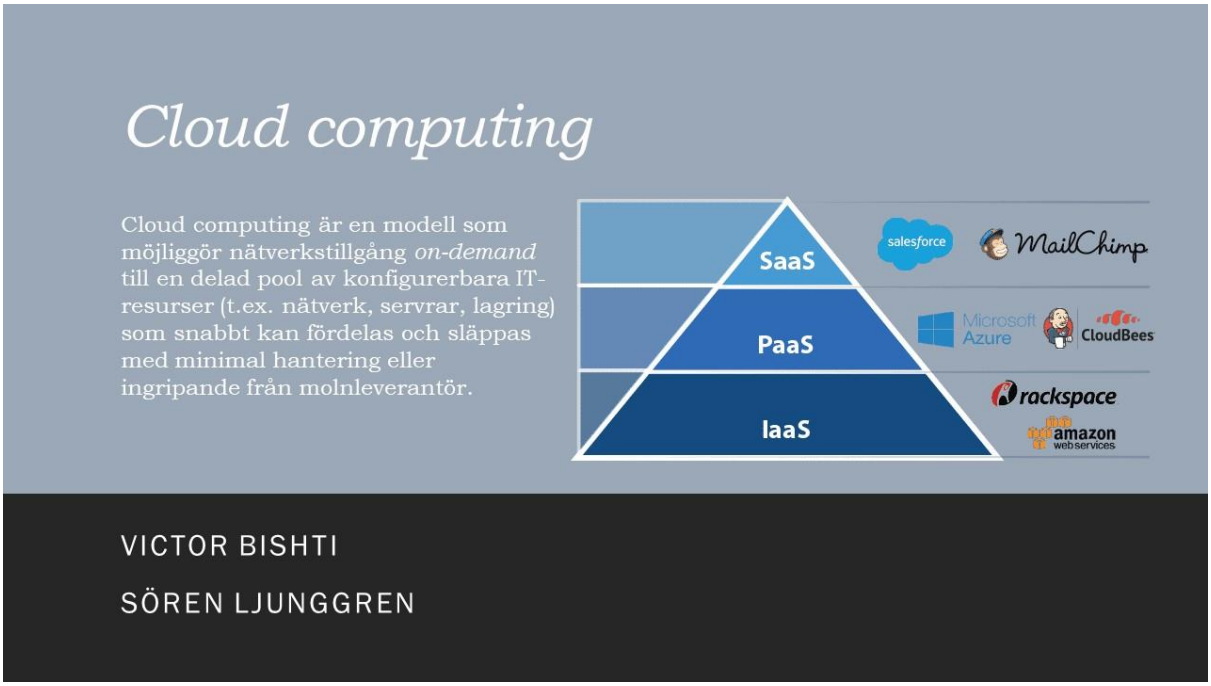
1. (Utmaning) Vendor Lock-in beskriver problematiken att flytta sina applikationer och data mellan leverantörer. Har ni upplevt den problematiken?
    a. Om ja, beskriv hur ni hanterade det - ge exempel.
2. (Utmaning) Molnleverantörer kan byta policies som de själva önskar.
    a. Har det någonsin skett förändringar i de molntjänster ni använder som har påverkat er verksamhet?
    b. Har ni en plan för migration, ifall er molnleverantör ändrar sina policies på ett sätt som gör att de inte längre är i linje med era egna?
3. (Utmaning) Hur är ert förtroende och tillit till er CC-leverantör? Litar ni på att de värnar om era intressen?
4. (Utmaning) Hur stor tillit har ni till att CC-leverantören tar säkerhetsansvar?
    a. Tar ni ansvar för säkerhetsaspekter som överlappar, utifall att det skulle visa sig att de inte tar det ansvar som de borde?
5. (Utmaning) Hur hanterar ni att inte ha fullständig kontroll över data, tjänster och säkerhet?
6. (Utmaning) Vilket ansvar tar ni för att hantera dataförlust eller -manipulation till följd av en attack eller intrång mot CC-leverantören?
7. (Utmaning) Är det något kring er hantering av datakontroll och ansvar med cloud computing som du vill tillägga?

2. Intervjupresentation

Presentationsbild 1: Inledning

Presentationsbild 2: Översikt

Presentationsbild 3: Anonymitet och reliabilitet



Presentationsbild 4: Bakgrund - Cloud computing

Presentationsbild 5: Bakgrund - Mjukvaruutveckling och -distribution med cloud computing

Presentationsbild 6: Bakgrund - Information- och datasäkerhet

Presentationsbild 7: Bakgrund - Datakontroll och ansvar

3. Transkript från intervjuer

V: Victor; **S**: Sören; **I-n**: Intervjuobjekt-n

3.1 Intervjuobjekt 1

[Inledning och bakgrund till cloud computing]

V: Beskriv er verksamhet, hur många anställda är ni och vad gör ni för något?

I1: Vi är 10 personer i huvudsak, vi har några som jobbar lite som resurser runt omkring oss men i bolaget är vi 10. Vi har en tonvikt på teknikutveckling, vi är åtta på utveckling och två på sälj och marknad. Ganska litet företag men med väldigt stort fokus på teknik, och vi levererar en plattform som skulle kunna ses som en Software as a Service-tjänst. Vi levererar den helt och hållet via nätet. Vi har en plattform för att bygga digitala om Low-Code idag vilket kan innebära lite vad som helst men det är en del av vad vi gör. Vi hanterar allt från infrastruktur, och all applikationsutveckling och all gränssnittsutveckling även ut i appar och så vidare. Det är ganska stort fokus på meddelandehantering: SMS, mail, push osv.

V: Vad är det för molnlösningar ni använder er av? Både tjänstemodell och leverantör.

I1: Egentligen använder vi Amazon primärt till väldigt mycket, och flera olika delar av deras tjänst. Sen har vi i flera olika omgångar testat olika andra leverantörer, vi har haft Rackspace före Amazon men vi använder inte det längre. Vi använde Rackspace i apputveckling tidigt i det vi gjorde. Vi har även tittat på Azure, framförallt i sammanhang där vi börjat titta på IoT-lösningar. Vi har jobbat lite ihop med Microsoft kring andra delar så var lite där. Egentligen kan man säga att det vi använder är Amazon och flera utav deras tjänster. Vi har allting där, vi hade tidigare en lokal leverantör som heter Glecius som också levererade mycket av de här cloud-tjänsterna men i ett mer lokalt perspektiv eftersom vi visste att de hade servrarna här i närheten. Vi hade en blandad konfiguration där vi hade en del fysiska servrar som vi placerade där och sen använda vi även deras VMware och så vidare.

V: Ni använder Amazon för hela spektrumet, både för infrastruktur och som plattform för utveckling?

I1: Ja, när man tänker utvecklingsmässigt så är det att vi använder Microsoft .NET för själva applikationsutvecklingen. För webbgränssnitten kör vi Angular som bas. Annars är det C# och .NET som vi kör primärt.

V: Hur lång erfarenhet har ni av att jobba med cloud computing?

I1: Ska man titta tillbaka till när vi började med Rackspace, så var det något vi använde för filhantering och avlastning för ganska länge sedan. Då tänkte vi inte så mycket utifrån vad vi tänker på cloud computing idag, utan det var väl Amazon för ett antal år sedan som vi började med. Säg att det var 2015 kanske.

V: När ni valde leverantör, eller när ni flyttade från Rackspace till AWS, gjorde ni någon typ av jämförelse eller analys av datasäkerheten för molnlösningarna?

I1: Just då, var det inte supermycket fokus på säkerhet utan då var det mycket mer utifrån vad de kan lösa tekniskt i form av vilka servertyper de har, hur man startar servrar, hur lätt är det att jobba med infrastrukturen. Säkerheten var inte på samma sätt top-of-mind då som det är idag. Nu förutsätter man att, oavsett vilken leverantör, så kan man göra ganska mycket och då börjar man titta mer på detaljer idag än vad vi gjorde då. Just då kände vi främst, att Amazon är mest kraftfull och smidig att jobba med. Sen har de andra frågorna utvärderats kontinuerligt efteråt.

V: Så det var mer de tekniska möjligheterna och tillgängligheten som lockade då?

I1: Ja precis.

V: I era tjänster som ni utvecklar, har ni några speciella säkerhetskrav i form av vilken data ni lagrar?

I1: Ja det gör det absolut. Vi har lite olika typer av avtal, vi säljer på lite olika sätt. Ibland direkt mot kund och ibland via återförsäljare. Det ser lite olika ut, men i grund och botten har vi ett krav på oss att hantera personuppgifter på ett säkert sätt och se till att följa GDPR och de här bitarna. Det finns absolut krav på hur vi lagrar data, vilken data vi lagrar och hur länge det lagras. Det är någonting som har blivit mer och mer diskussion kring. Det började någonstans kring GDPR när det trädde i kraft, men det blir mer och mer aktuellt för varje dag. Generellt sätt är det framförallt kring personuppgifter som det pratas mycket om, loggar och personuppgifter. Hur lagrar vi dem och hur länge lagrar vi dem, är de krypterade, vilken åtkomst har de och så vidare.

V: Det finns olika distributionsmodeller av molnlösningar: public, private och hybrid. Vad använder ni för distributionsmodell?

I1: Vi har vad vi brukar kalla en multitenant-lösning. Vi hanterar hela infrastruktur och hårdvaru-delen åt kunden. Alla kunder är i samma infrastruktur, vi spinner inte upp några nya egna servrar när en kund behöver utan det är en delad lösning och vi ser till att distribuera funktionerna som de ska men vi har full kontroll över infrastruktur.

V: Era kunder befinner sig i en slags pool av IT-resurser, men befinner ni er i delad pool av IT-resurser med andra Amazon-användare?

I1: Där är det lite olika för olika delar. Man kan explicit gå in och välja att en viss del ska vara dedikerad hårdvara för oss. Det har vi gjort på några ställen vet jag, men inte överallt. Vi hade för ett par år sedan, lite knepiga driftstörningar som vi inte visste vad det berodde på. I samband med det misstänkte vi att störningarna kunde bero på att det var att vi påverkades av någon annans belastning som vi delad hårdvara med. Då gick vi in på ett antal ställen och såg till att vi hade vår exklusive hårdvara. Det beror lite på vilka tjänster, men inte genomgående.

V: Man skulle kunna säga att ni har någon typ av hybridlösning, vissa delar är dedikerade och andra är delade med andra användare?

I1: Ja, precis.

[Bakgrund för mjukvaruutveckling och –distribution]

V: Använder ni några verktyg eller information när ni gör en kravinsamling eller planerar ett nytt projekt från er molnleverantör?

I1: Ja, till viss del men det styr inte vad vi gör speciellt mycket. Vi tänker oftast utifrån att vi vill lösa uppgiften; vi behöver en viss funktion för det vi utvecklar och sen ser vi till att infrastrukturen anpassar sig till det. Till viss del kan vi tänka: är det här en process som kommer att skapa väldigt mycket transaktioner eller ställa väldigt höga hårdvarukrav, då förstår vi att det ganska snabbt kommer bli ganska dyrt. Vi pratar en del om kapacitet, det finns en burst-kapacitet och en slags medel-kapacitet och där blir det lite att fundera på: hur beter sig de olika systemen och vad är det egentligen de behöver? Jag skulle säga, att om vi backar tillbaka till mjukvaruutveckling så tänker vi inte så mycket på vad molnleverantören kan leverera utan det blir ett steg senare. I distribution då måste vi tänka på vad det ska köras på och hela den biten. Vi har det till viss del i form av att våra maskiner kan både köras på Windows och Linux. Det är något vi måste ta hänsyn till när vi utvecklar, vad kommer det kunna köras och vilka ramverk används. Till viss del, själva distributionen och deployment utav det vi har skapat ställer någon typ av krav på plattformen. Det påverkar inte så mycket vilken molnleverantör vi använder. Vi har inte någon riktig avstämning där vi säger: vad gör vi med detta hos Amazon? Det ska upp på en server, det är ett API, en applikation eller anant. De bitarna körs på ett visst sätt och då använder vi en viss molnleverantör. Där har vi tänkt att vi helst inte vill låsa in oss mot Amazon därför kör vi primärt på en Linux-instans hos en annan leverantör om allt skulle gå åt skogen för Amazon, vilket kanske inte är jättetroligt men det kan hända, då kan vi köra igång en instans hos Azure istället. Det är en del av vad vi har i bakhuvudet på många utav tjänsterna, att vi har en kontroll över det och inte sitter fast i Amazons lösningar.

V: Gör ni något arbete innan ett projekt för att identifiera och planera för eventuella säkerhetsrisker?

I1: Ja, det tycker jag absolut. Vi har med det som en del att tänka vilka risker det finns. Säkerhetsmässigt är det... Pratar man om hur man autentiserar mot olika tjänster vilket är en grundsten eftersom vi ofta exponerar ut saker via API:er och via olika typer av gränssnitt. Då tänker vi; kan någon annan komma åt det här? Kan någon missbruka det här på något sätt? Den biten finns med absolut.

V: Är molnleverantören inblandad på något vis i den planeringen?

I1: Inte så ofta, det finns en tanke om att... Vi har en situation där vi har ett privat nät hos vår molnleverantör, där innanför finns våra resurser och in dit har vi våra väggar som vi kommer åt via VPN osv. Sen finns en annan del där vi vill dela ut API:er, och hur delar vi ut de från vårt nät så att de är isolerade från andra delar av vår infrastruktur som databaser. Där har vi gjort ett arbete i hur den strukturen är uppbyggd. Eftersom vi har den strukturen... Vi jobbar primärt på en plattform, hade man jobbat mer projektorienterat och från olika situationer varje gång man levererar ett projekt så hade det varit mycket mer en löpande grej. Här har vi gjort ett antal beslut ganska tidigt, sen hamnar vår utveckling i något av de här facken. Är det en viss leverans som kanske är helt och hållet innanför våra väggar och då har vi en tanke om att man kommer åt det. Annars är det en funktion som ska upp på ett gränssnitt och då

levereras den på ett annat sätt och då finns det en tanke att vårt authentication system tar över och ger dig rättigheter baserat på ditt konto och din token. Det kanske är främst för att vi gjort det tankearbetet på en mer övergripande nivå, sen när vi gör utvecklingsarbete så hamnar det i en redan uttänkt folla.

V: Gör ni någon kontroll eller testning för att upptäcka säkerhetshot?

I1: Det är ett område vi tänker att vi vill göra mer i. Vi försöker framförallt internt diskutera och bolla lite scenariobeskrivning om vad som kan hända och vad som kan missbrukas. Det gör vi i samband... Det sker ganska tidigt i tanken. Om vi behöver en viss funktion så funderar vi över vad det finns för tekniska utmaningar men också vilka risker som finns med att exponera ut något på ett visst sätt. Framförallt har vi pratat om att genomföra penetrationstester eller att ha någon extern som gör tester på våra system. Dit har vi inte kommit än, det är generellt sätt vi själva som testar och funderar med våra resurser internt vad vi kan göra för åtgärder för att hålla det säkert.

V: Vill du beskriva vad ett penentrationstest är?

I1: Det finns tjänster för det. I grund och botten handlar det om att man utifrån försöker ta sig in och komma åt data på något sätt. T.ex. om jag inte känner till något innanför men jag kan hitta att jag kan få ett konto och token, hur kan jag förändra den token så att jag kommer åt mer information. Med mål att t.ex. komma åt en databasserver. Ofta pratar man om white hackers som man kan ge uppdrag att försöka ta sig in i våra system på något sätt och då kan man se var säkerhetsbristerna finns. Ett vanligt scenario är att man säger: testa se om du kan ge dig själv förhöjda rättigheter i systemet. Den typen av tester. Det finns lite olika certifieringar och e-säkerhetsramverk, men inget av det är speciellt väl typeat så det görs nog ganska godtyckligt. Man dokumenterar vilka tester som har gjort, t.ex. försökt överbelasta authentication, eller brute force-hacka lösenord. Sen kan man se vilka delar som har lyckats och inte. En sårbarhet kan ju vara att man vet att vi använder Amazon, då kan det vara någon som är expert på Amazon som.. De har ju CLI:er för att komma åt och scripta. Om man är lite händig där, så kanske man vet att det finns en sårbarhet - om jag har ett annat konto kan jag komma åt resurser. Lite det vi pratade om en delade hårdvaruresurser. Kan jag på något sätt genom att manipulera något komma åt något från ett annat konto.

V: Alla molnlösningar skyltar med olika programmeringsspråk och ramverk. Har ni upplevt någon begränsning i förhållande till kompabilitet av språk och ramverk?

I1: Nej det tycker jag inte. Det är snarare svårt att navigera för Amazon har så himla mycket. Vi vill ha någon kontroll att vi inte är helt låst mot Amazon så vi kör ofta vanliga Linux- eller Windowsservrar, och där konkluderar vi våra applikationer så att vi kan sätta upp det någon annanstans också. Vi använder Amazons gränssnitt mycket för att på automatik sätta upp och starta de här servrarna. Amazon har lamdas och ett antal olika tjänster där man mer programmerar i deras miljö, men det har vi valt att inte använda i någon större utsträckning för att inte låsa in oss. Vi behöver dessutom sätta in oss i något som är osäkert om vi kommer att ha så mycket nytta av.

V: När ni utvecklar någon ny funktion och ska distribuera det, upplever du att det finns några säkerhetsrisker med den delen av distribution?

I1: Nej, vi använder ganska mycket olika tjänster där Amazon är en del men t.ex. för deployment så bygger vi i en annan tjänst som heter AtLayer som är vår continuous

integration-plattform. Sen har vi koden hos BitBucket. Vi comittar vår kod mot BitBucket sen plockar vi från AtLayer och bygger där, sen plockar vi från AtLayer över till Amazon via terraform som är en annan produkt som hämtar färdigbyggda paket hos AtLayer och installerar de på servrar.

V: Anser du att den kopplingen, och den automatiska synkningen är säker?

I1: Ja det tycker jag. Man har ett antal olika certifkat mellan de olika delarna och de ansluter till varandra. Det tycker jag känns säkert.

V: Har era utvecklingsprocesser påverkats av den molnleverantör ni använder och de verkktyg som tillhandahålls?

I1: Ja, de har gett oss möjligheter som vi inte hade när vi hade fysiska servrar. Framförallt tanken om att enkelt kunna dra upp flera instanser av saker och ting, och att vi generellt sätt gärna gör det. Det är bättre att vi startar en viss tjänst i flera olika instaner som kan avlasta varandra, om det blir fel eller vi vill uppdatera. Det är något som hade varit mycket, mycket svårare om man inte hade haft en molntjänst bakom. Vi har kanske lite tvingats skapa den här kedjan av deployment, och hur vår struktur ser ut på ett annat sätt. Har man en server som man alltid går in och installerar sin programvara på så är det inte så mycket att göra. I det här fallet vill vi automatisera det här, vi har ett hundratals servrar och då är det inte vettigt att vi sitter och administrerar dem en och en. Då behöver andra tankar kring hur vi jobbar med vår distribution med programvara. Absolut, det påverkar men i huvudsak är det på ett positivt sätt för det ger oss andra möjligheter än vad vi hade haft annars.

[Bakgrund för data- och informationssäkerhet]

V: Upplever du att det finns någon risk eller utmaning med att obehöriga får tillgång till känslig data eller kritiska applikationer?

I1: Det är alltid en oro, skulle jag säga. Sen har vi gjort ganska nyligen en hel del åtgärder för att förbättra det. Vi har sett över så att vi får bättre kontroll över de olika servrar vi har, de olika tjänster vi använder. Vi tittade även över våra användarroller för att vara säkra att det inte läcker. Användare vi inte har kontroll över eller användare som har för mycket behörighet. Det är absolut något vi tänker på och som är viktigt sen finns det ganska många olika nivåer av det här. Vår data är en del, kundens data är en annan del.. sen är det en del att förstöra data, eller förstöra system eller komma åt eller få tillgång till saker som man inte ska ha tillgång till. Hur känslig är den datan som man kommer åt. Vi har funderat mycket kring vad är den känsliga datan vi har och vad skulle man åstadkomma med den.

V: Det finns olika lager som du säger. Har ni någon strategi för att motverka att intrång sker?

I1: Ja, absolut. Det är många olika lager och de är olika för vilken tjänst vi pratar om. Inom infrastrukturen handlar det om att kapsla in. Vi har ett antal olika nät i vårt nät där olika servrar placeras och dem är ju till viss del avskilda från varanda. Det gör att man behöver ta sig in i flera nivåer för att komma åt saker, t.ex. en databasserver. Den ligger inte i samma nät som en API-server eller liknande. Det är en del utav det och på det så har vi dels det som Amazon har, IM-roller, där man definierar upp personliga inloggningar för alla oss här som ska tillgång till saker och ting. Där har man sin egen användare och den kan vi ju jobba med vilka behörigheter den ska ha, och vi kan även se lite vad som har hänt, hur länge sedan man uppdaterade lösenord osv. Sen finns den andra delen att komma åt infrastruktur via VPN,

man anslutar med en VPN in till en server hos oss som sen ger dig tillgång till nätverket. Där finns det också nyckelfiler och en autentisering som vi också roterar och jobbar med. Vi vill ju faktiskt exponera rätt mycket data, eftersom det är det vår tjänst gör. Det handlar om att göra en avvägning där.. Ska du t.ex. skicka ett meddelande till en person så behöver den meddelandetexten och till vem du skickade till lagras någonstans. Du som användare vill ju gärna kunna se det och följa det, men du vill vara säker på att ingen annan gör det. Då handlar det om hur du hämtar ut och låser resurser till just din användare och då är det ofta vårt eget autentiseringssystem som hanterar den läsbarheten,

V: Det är en del att ni har flera lager för att skydda från att obehöriga ska läsa och få insyn i er data, men har ni någon strategi för att hantera attacker?

I1: Där finns det ju dels som ett yttre lager Amazon Shield som är ett verktyg som de har och jobbar primärt mot DDoS-attack och överbelastningsattacker. Med det kan man få hjälp om de ser sådan aktivitet, då kan de på nätverksnivå gå in och stoppa trafik. Där får man hjälp från Amazon och det ligger i deras intresse också. Sen finns det en annan del av attacker som sker mot oss. Då får vi fundera över vad vi har för säkerhet på nycklar och på autentiseringssystem osv. Sen har vi möjligheten med molnsystemen att starta upp andra instanser, så vi har en tanke att om det skulle hända något på ett ställe så kan vi starta upp en ny instans, vi kan starta upp på en ny domän - vi kan röra oss ganska fritt i hur vi distribuerar vår plattform. Där har man hjälp av molntjänsterna i det.

V: Har ni själva blivit direkt eller indirekt attackerade?

I1: De tillfällen som vi har upplevt driftstörningar så fick vi uppfattningen att de var slumpmässiga. Det råkade nog vara så att vi delade resurser med någon som hade hög belastning. Vi har inte riktigt sett någon överbelastning, ingen medveten. Vi har haft påverkan av kunder, t.ex. använt ett annat system som är konfiguerat att göra något mot oss och så börjar det systemet göra väldigt många anrop. Inte för att det är fel utan för att det är felkonfiguerat, och det är klart att det blir en slags överbelastningsattack om det kommer tusentals anrop i sekunden. Det är en misstag snarare än en medveten åtgärd. Nej, vi har inte blivit överbelastningsattackerade på det sättet. Tidigare innan vi hade molntjänster däremot så hade vi en situation där vår hostingleverantör hade andra kunder som fick problem, de blev DDoS:ade, och då satt vi innanför deras brandvägg vilket gjorde att vår trafik också påverkades. Vi har varit med om situationer men inte pågrund utav oss men vi blev påverkade. Det var en av anledningarna till att man kände att det var svårt med en sån leverantör där man sitter fast fysiskt, det kändes inte bra. Det är ett äldre problem på det sättet.

V: Det var en av anledningarna till att ni flyttade så småningom?

I1: Ja, precis. I första läget flyttade vi till en annan leverantör och det var Glecius för att de erbjöd en hybridlösning med fysiska och virtuella servrar. Sen klarade inte de av att leverera det vi ville och då tittade vi på alternativ och då kändes Amazon kraftfullast.

V: Gör ni någon typ kontroll eller test för att se att det inte sker några avvikelser i data, dataförlust eller datamanipulation?

I1: Vi tittar kontinuerligt på våra loggar, mer statistik över hur vårt system används. Det är nog lite svårt att.. Vi har inget system som tittar på datamanipulation på det sättet. Vi tittar mer på om det kommer in mycket anrop av en viss typ, eller felaktiga eller stor mängd. Att

det skapar effekter i vårt system. Vi har något som heter Kebana där man kan agregera massa loggar och information från olika system och få upp dashboards och grafer på det. Där kan vi se om t.ex. om det plötsligt börjar ske väldigt många anrop mot våra API:er, ofta om man försöker göra brute force så skulle det generera en väldigt massa unauthorized anrop. Då skulle vi se det som peakar på en graf.

V: Är det också någon typ av kontroll för att upptäcka avvikelser i tjänsteanvändning, hur mycket beräkningar som sker på er bekostnad?

I1: Lite så är det. Man ser när saker och ting förändras. Det är också ett område som man behöver fundera lite på. Hur kan vi upptäcka de här; vi har ju så mycket trafik i våra system, det är miljontals transaktion som flödar runt så det är klart att om det kommer en process som ligger på en specifik del i en inte allt för stor utsträckning så skulle den vara svår för oss att upptäcka om den inte påverkar något annat system så att det blir instabilt. Det är väl något vi har tittat på, hur skulle vi kunna upptäcka när något är fel - snarare än att det resulterar i en incident från kund. Det är mer utifrån ett driftperspektiv än ett säkerhetsperspektiv.

V: Det finns inbyggda verktyg, t.ex. med Amazon heter det Cloud Watch, där man kan övervaka trafik och kostnader. Använder ni av de för att övervaka era system?

I1: Absolut, Cloud Watch använder vi till en hel del. Det är mycket som landar där. Det kan larma på vissa saker, och vi har egna program som larmar på andra delar i framförallt hur saker är anslutna till varandra - om det tappar kontakten och så. Vi använder en uppsättning av grejer men Cloud Watch är absolut en tjänst som vi på automatik integrerade då vi använder flera av deras tjänster.

V: Har er tjänst eller delar av tjänsten legat nere någon gång?

I1: Ja, det har den. Det är någon vi jobbar på att minimera, men det har generellt sätt varit.. Vi hade en situation där vår databas kraschade hela tiden och till slut gjorde vi den ändringen att vi hade hårdvara för alla läs- och skriv storageenheter. Det tog bort problemet. Det kan väldigt random, och det var förmodligen att någon annan använde samma delade hårdvara på en så pass hög nivå att det påverkade vår stabilitet.

V: Hur lång tid kunde det som mest ligga nere?

I1: Under en månads tid så hade vi ganska många avbrott. Sen var inte avbrotten alltid så jättelånga, utan vi fick stänga ner och göra saker - flytta runt. Men vi var påverkade under en ganska lång tid totalt sett men sen kom det stötvis. Det låg väl nere timmar kanske i olika omgångar. Vi har en plan kring vad vi gör när ett system går ner. Då vill vi att det är vi som upptäcker det så snart som möjligt och inom fem minuter bör vi ha reagerat och börjat göra saker kring det. Om vi inte har fått igång det på 20 minuter så bör vi se till att ha startat en kopia, en ny instans. I de allra flesta fall vi får problem är det en del utav ett system som går sönder, sen beroende på vilken del det är så får det olika stor påverkan. T.ex. om en primär databasserver - då har vi ofta redundans att vi har ett replikaset så att vi kan en annan som blir master isället. Felen kan flytta runt ganska mycket, i de flesta fallen kan vi starta upp en ny instans. Ta bort det som är dåligt, starta upp en ny, göra en ny kopia eller något. Där har vi lite olika återställningstid men vi tänker att inom en tjugo minuter, kanske en timme så bör vi kunna ha upp i princip alla delar utav vårt system. Sen har vi pratat om att försöka göra ett test där vi ser hur väl vi matchar de tiderna. T.ex. att inom en timme ska allt vara igång, eller fyra timmar om allt ligger nere och vi behöver flytta från Amazon. Hur skulle vi kunna få

igång någoting någon annanstans, vi kanske är något begränsade i prestanda eller antalet tjänster men att man åtminstone kan få igång kärnverksamheten ganska snabbt på ett annat ställe. Vi håller på att jobba en del där och har kommit en bra bit men vi jobbar med det kontinuerligt.

V: Har Amazon eller den molnleverantör ni använt någonsin legat nere för er?

I1: Inte generellt, nej det skulle jag inte säga.

[Bakgrund för datakontroll och ansvar]

V: Vendor Lock-in beskriver en problematik att flytta applikationer och data mellan olika leverantörer. Har ni upplevt den problematiken?

I1: Nej inte på det sättet att vi haft problem med det än. Som sagt, vi ser det som ett hot. Om vi tycker att det är smidigt att ha en databas hos en molnleverantör, vad händer om vi inte kommer åt den längre? Vad gör vi då? När backuper och allting ligger i deras tjänst. Till viss del har vi ingen tydligt åtgärd för att flytta information eller data. Vi gör inte det aktivt idag vilket skulle bli ett problem om Amazon som helhet försvinner.

V: Vad tror du skulle vara det svåraste att flytta? Vilken del av er tjänst?

I1: Det beror på hur man ser det. Å ena sidan har vi en hel del som är låst till Amazons lastbalanserare, IP-nätverksstruktur. Där har vi inpekat olika delar och att det är lite låst mot det. T.ex. att vi har en del domäner som är reggade där. De ligger i Amazons namnservrar och körs via deras tjänster. Det är klart att det blir svårt att flytta ut det. Den mest kritiska informationen ligger primärt i våra databaser. Därför skulle det vara att ta en databasdump och flytta ut den och få med den till en annan plats. Där finns det ytterligare delar där vi har vissa databaser där vi egentligen kör, MongoDB t.ex. kör vi själv som en instans och då skulle vi kunna flytta den. Men vi använder också Amazons IBS-tjänster, och att flytta ut en kopia ifrån en utav deras databaser är nog lite knepigare. Det finns nog utmaningar där, men databaserna är det som skulle vara nyckeln för oss att.. om vi skulle starta upp någon annanstans skulle vi behöva få ut den informationen för där ligger mycket av det vi behöver för att kunna starta upp på en annan plats. Det viktigaste skulle vara det: databaserna.

V: Molnleverantören är ett eget bolag med eget vinstintresse. De kan ju ändra policies eller priser helt plötsligt. Har ni någonsin upplevt att det skett förändringar i en molntjänst som har påverkat er verksamhet?

I1: Nej inte på det sättet.

V: Har ni ett förtroende och tillit till er molnleverantör? Litar ni på att de värnar om era intressen?

I1: Ja det tycker jag. Vi ställer oss ofta frågan, t.ex. med Googles "Dont be evil"-slogan. Jag förstår att de har sina vinstintressen och på något sätt är det lite det som skyddar oss också. Skulle det visa sig att t.ex. amerikanska myndigheter har en bakdörr rätt in i alla system som kör hos Amazon. Då skulle Amazon få väldigt stora problem. Deras tanke om att överleva och bli stora ställer också krav på att hålla koll sin integritet och säkerhet för kunderna.

V: Du skulle säga att de tar ett säkerhetsansvar eftersom det är i deras intresse?

I1: Ja, precis. Dem vet att om de gör dumma grejer så kommer det exponeras och då får de väldigt stora problem.

V: Det finns vissa säkerhetsaspekter som överlappar där det kan vara svårt att veta vem som bör ta ansvar. Är det Amazon eller företaget själva. Har du upplevt någon problematik med det?

I1: Vi förutsätter att vi måste ta ansvaret, vi måste vara säkra på vad vi sätter upp. Sen såklart förutsätter vi att det inte finns massa bakdörrar och andra problem kopplat till det. Vi utgår från att vi behöver ta ansvar för det i mångt och mycket.

V: Är det något som skaver med tanken på att ni inte har full kontroll över data eller säkerhet?

I1: Vi tänker mycket på olika scenarion. Vad kan hända och vad gör vi om vissa saker inträffar. Det är orosmoment och funderar en del över. Samtidigt tycker jag.. vi har inte haft några leveransproblem direkt från Amazon, och i den stora mängden som använder det så hade vi funnit de här stora problemen och det hade bubblat upp till ytan. Jag känner att vi har förtroende för dem i det avseendet. Jag funderar mer om vi använder det på ett bra sätt mer än om det är ett grundläggande problem hos Amazon.

V: Är det något vi inte har tagit upp med datakontroll eller datasäkerhet som du vill lyfta som den största utmaningen?

I1: Jag tycker den största frågan just nu är från t.ex. svenska myndigheter. Om vi har data där (Amazon), vad är det som säger att inte andra kommer åt det? Den tryggheten i att.. om jag har en fysisk server som står i ett rum så kan jag kontrollera vilka som har tillgång till den. Hur kan ni säkerställa att det är på det sättet. Hur kan vi visa för en kund att data är säker. Det går ju så pass långt att myndigheter säger att ni får absolut inte.. den här tjänsten får absolut inte levereras via en molntjänst. Framförallt en molntjänst utanför Sveriges gränser. Det tycker jag är den svåraste frågan. Hur kan vi angripa det och hur kan vi svara på de frågorna och jobba med det? För det är det som verksamheterna utanför oss kommer till oss med.

V: Någon slags vattenstämpel på att data hanteras säkert?

I1: Ja lite så. Vad finns det för system.. vi skulle gärna vilja säga att vi använder Amazon på det här sättet, alltså är det ingen fara. Men det finns inget sånt utan det är väldigt godtyckligt idag.

[Intervjun avslutas]

3.2 Intervjuobjekt 2

[Inledning och bakgrund till cloud computing]

S: Hur ser er verksamhet ut, hur många anställda är ni, var jobbar ni och vad utvecklar ni för tjänster och produkter?

I2: Vi är cirka 10 anställda. Vi jobbar med att ta fram nya och moderna webblösningar och vi använder ofta serverlösa tjänster eller molntjänster för att leverera det vi bygger. En del gör vi

internt för eget bruk men vi hjälper också en hel del kunder med deras hostinglösningar och sätter upp tjänster åt dem, som de hostar i molnet.

S: Vilka cloud computing-tjänster och -lösningar använder ni för att utveckla och distribuera?

I2: Menar du specifika tjänster hos Amazon eller på vilken nivå?

S: Både vem som levererar dem och sen vill vi kanske identifiera var i abstraktionsspektrumet. Är det PaaS-tjänster eller är det bara infrastruktur?

I2: Vi utnyttjar alla: Infrastructure as a Service och Platform as a Service och Software as a Service, kan man säga i olika avseenden. Vid IaaS använder vi ju för hosting av maskiner som körs för speciella ändamål. Det kan vara virtuella maskiner som vi programmerar mot. Sen använder vi PaaS t.ex. när man hyr in sig på en produkt som t.ex. från Microsoft. Vid PaaS ingår väl även MySQL, och RDS-tjänster i AWS dvs. när man får tillgång till en plattform och inte till den underliggande hårdvaran. SaaS använder vi ju både som konsument av tjänsterna själva till olika syften och sen så erbjuder vi också i vissa fall SaaS gentemot kunder kan man säga. Vi jobbar egentligen i hela spektrumet.

V: Vilka leverantörer använder ni då?

I2: Vi använder främst Amazon för infrastruktur sen använder vi en del Azure, men det är inte speciellt mycket. Där har vi någon PaaS-tjänst och hjälper någon kund med det. SaaS där är vi konsumt och där kan det vara alla möjliga, t.ex. Google Docs, Fortnox ligger väl också i det lagret. Om man säger ur ert perspektiv med PaaS och IaaS så är det ju Amazon framförallt men lite Azure.

S: Okej, har ni lång erfarenhet av att jobba med dem?

I2: Framförallt Amazon har vi jobbat med sex år, tror jag att det är.

V: Jag tänkte höra när ni valde leverantör för molntjänster, gjorde ni någon typ av analys eller jämförelse över hur duktiga de var på datasäkerhet? Vilken nivå av datasäkerhet de hade, jämförde ni leverantörerna?

I2: Då fanns det ju inte så många som konkurrerade med Amazon på det sättet. Amazon hade byggt ut sin tjänst, det är först några år efter det som egentliga Microsoft med Azure och Google Cloud kom ifatt med IaaS-tjänster. Där fanns ju andra som Rackspace och det fanns några lokala här i Sverige också men de var liksom på en helt annan nivå. Det vi lockades till dem var inte några säkerhetsaspekter, utan det var ren tillgänglighet och enkelhet. Sen gjorde vi väl ingen explicit analys av deras säkerhet, däremot så gjorde vi antagandet med hur stora de är och så många som använder dem så måste de ha, för oss, en tillräcklig bra säkerhet.

S: Så då betraktade ni det inte som att ni har några extraordinära säkerhetskrav eller så på grund av hur er verksamhet ser ut? Om det är så för alla andra borde det räcka för er?

I2: Ja, lite så var det inledningsvis i alla fall. Sen har vi ju tagit höjd för säkerhetsaspekter i efterhand men i frågan inför valet av det så hade vi nog inga tankar på säkerhetsaspekter utöver att det såklart ska anses vara säkert. Men det var nog en allmän tanka att Amazon var överlag säkra, sen det som gjorde de osäkra var om man själv gjorde något som gjorde de osäkra men det har vi ganska bra koll på själva för själva säkerheten runt en server och hur

man sätter upp den, för det är ju oberoende av tjänsten. Det kan vara en fysisk maskin som har samma problem som en virtuell maskin i Amazon. Så de säkerhetsaspekterna hade vi själva lite koll på. Sen har vi haft genomgående funderingar över säkerheten steg för steg och men det har blivit mer aktuellt på senare tid. Som t.ex. att använda Zoom som är ett hett ämne.

S: Okej, du nämner att man kan ha egna servrar - traditionell IT och egen serverhall. Man kan också ha, i praktiken och teorin, virtuella maskiner på sina egna nätverk som finns on-premise. Man kan i någon mening hosta sin egen IaaS och ha en molnmiljö som är helt sluten till er verksamhet. Man kan arbeta i en molnmiljö som ligger i helt och hållet i en molnmiljö som ligger helt och hållet hos en leverantör som Amazon och sen kan man ha någon slags hybridlösning där emellan där man har lite av varje. Har ni någon egen molninfrastruktur, eller är all er molninfrastruktur och era molnplattformar hos externa leverantörer?

I2: Vi har ju lokala virtuella miljöer också, sen om man får in dem som IaaS eller PaaS definitionsmässigt vet jag inte. Men vi har lokala servrar med ett gäng virtuella maskiner som vi kör på den. Det är mest utvecklingsmaskiner, testmaskiner. Det är ju ibland när vi har t.ex. kunders data hos så lägger vi inte upp det i molnet utan deras medgivande i alla fall. Det har vi lokalt hos oss. Sen har jag omvänt haft fundering om säkerhetsaspekten där. Jag tycker att vårt kontor borde ju rimligen ha sämre säkerhet än vad Amazons serverhall har och därför borde det egentligen vara säkrare att ha det hos dem än att ha det hos oss, även om det känns säkrare att ha det innanför egna dörrar. Det åtgärder vi har tagit är t.ex. att ha krypterade hårddiskar, så skulle en dator bli stulen så får de en dator som fysisk fungerar men själva innehållet är inte kvar på den eller mycket svårt att komma åt. Det jag anser är den största risken för datastöld är egentligen att någon fysiskt bryter sig in på vårt kontor och själv våra maskiner. Så därför har vi egentligen sett det som att det är bättre att vi trycker upp det i Amazon, för där går det inte att fysiskt stjäla sakerna. Förutsatt såklart att man har en bra säkerhet på det som ligger där uppe.

S: Victor, jag kommer att avvika lite från vår intervjuguide för vi har kommit in på några ämnen som vi kommer komma in på senare i vilket fall. Du nämner här att man får jämföra säkerhetsnivåerna mellan att ha egna resurser och att ha resurser hos Amazon. Amazon är givetvis en jättestor spelare som har råd att investera i både mjuk- och hårdvara för säkerhet, som ingen liten spelare kan göra. Men samtidigt så är man en del av en delad resurspool, så man kan föreställa sig att det finns aspekter där er data utsätts för andra typer av säkerhetsrisker som DDoS-attack, mot Amazon, som gör att Amazons tjänster inte är tillgängliga för er. Amazon löper större risk, eftersom ni delar de resurserna med andra som ni inte gör med era egna lokala resurser. Har du något på det Victor?

V: Hur har tänkt kring det att ni utsätts för indirekta säkerhetsrisker, genom att ni befinner er i en delad pool av IT-resurser?

I2: Jo, det har vi faktiskt beaktat i den mån att jag var med, 2014-2015, när Amazon blev utsatt för någon form av krasch som gjorde att det var flera veckors nedtid för vissa kunder och det var stort problem för Apoteket i sverige tror jag och någon annan som hade gått ut där. Men i alla fall, då visste jag att det här kunde ske. Vi upplevde det, våra kunder drabbades inte men jag har en bekant som drabbades och deras kunder. Och då tog jag beslutet, som vi har följt sedan dess, att vi har andra sorts miljöer. Vi anser att Amazon är säkert men vi ser till att ha en lokal kopia av det mest väsentliga, eller det mest viktiga för oss. Det är också ett råd vi ger till våra kunder att de kan köra i molnet och lita på molnet men

om det väl smäller ordentligt i Amazon eller Azure så är man rätt liten i deras värld, de bryr sig inte om oss i första hand utan de tar hand om sina riktigt stora kunder i första hand och så kommer man själv att hamna på efterkälken långt, långt efter. Och då måste man kanske ha tillgång till sin data under den tiden, för annars har man själv ett bekymmer gentemot sin egna kunder. Så jag har alltid haft det som rekommendation till våra kunder, de kan köra i Amazon och ha det säkert där uppe men dra ut en backup eller liknande en gång per dygn så att de har en katastrofplan. Det kanske inte är Amazon som försvinner, det skulle kunna vara någon bekymmer med internet eller tillgänglighet över lag, eller något annat som orsakar det. Det kan vara väldigt trevligt att ha en lokal kopia över det absolut viktigaste. Det har vi och det rekommenderar vi alla våra kunder.

V: När ni använder AWS och Azure. Det finns lite olika lösningar, det finns något som heter private cloud, public cloud och sen finns det en hybrid mellan dem. Med private får man dedikerade resurser för ens egna verksamhet, och public delar man dem - så man kan hantera och konfiguera lite mer med private och hybrid är en mellanväg. Vad använder ni i era tjänster?

I2: Vi själva använder public, den delen med private anser jag är för dem verksamheter som har ett speciellt säkerhetsbehov t.ex. vissa myndigheter i Sverige. Eller sjukvård som har vissa andra regler om hur och var man får lov att lagra data. Jag anser annars att för de allra flesta som en vanlig e-handel eller vanliga e-tjänster så behövs inte den nivån av säkerhet som tvunget behöver dedikerad hårdvara. Då kanske man ska använda en annan leverantör eller ha hårdvaran själv. Sen är det ju väldigt liten risk att det delas någon data mellan maskiner, du får ha rätt så duktiga hackare som är efter dig för att det ska vara någon risk med en sån sak egentligen.

V: De olika tjänster och applikationer som ni utvecklar för er själva och kunder, anser ni att ni har något speciellt säkerhetskrav på de eller går ni som en i mängden på vilka säkerhetskrav ni har?

I2: Det vi gör anser vi att vi går som en i mängden, vår känsligaste data är kunduppgifter. Vi håller oss undan från alla andra känsliga uppgifter som kreditkortsnummer eller liknande som är åtråvärda att hacka sig till. Det känsligaste vi har är personuppgifter och de ska självklart skyddas, men de behöver inte skyddas som nationell hemlighet. De ska skyddas på ett rimligt sätt och då anser jag att de tjänster som finns i Amazon lagrar dessa på ett vettigt sätt. Det behöver inte vara större säkerhet utöver det.

[Bakgrund till mjukvaruutveckling och -distribution]

S: Vilka verktyg och information tar ni del av vid kravinsamling, planering och design vid projekt?

I2: Vilka verktyg vi använder?

S: Och vilken inforrmation ni tar del av från er molnleverantör?

V: När man använder sig av PaaS och IaaS då har molnleverantören en mängd olika verktyg och information som kan underlätta arbetet för kravinsamling och hur man ska planera och designa ett projekt. Beskriv några av de verktyg eller någon specifik information som ni använder från er molnleverantör innan ett projekt.

I2: Jag kan inte komma på något specifikt verktyg vi använder för kravinsamling. Vi jobbar ju inte jättemycket med krav. Ofta är det kunden eller någon annan som har gjort en kravinsamling innan oss. Vi kommer kanske in på planeringsstadiet men framförallt programmering, testning och distribution. Vi är sällan med under underhåll och nedstängning. Jag känner inte till några konkreta verktyg vi använder, de är de vanliga: excel, word och powerpoint. Det jag vet kommer från Amazon specifikt är t.ex. ikonbibliotek för deras olika tjänster som vi använder när man ska rita server-/tjäntekartor. Det är ett ikonbibliotek som de har bestämt att en EC2-instans ser ut så här, så att det ska vara ett gemensamt språk när man visar för varandra hur man har byggt upp en tjänst.

V: Är det någon speciell information ni behöver ta del av innan ett projekt från er molnleverantör? T.ex. kostnad, säkerhet eller utvecklingstid.

I2: Amazon har en kostnadskalkulator som vi använder ibland när vi ska ge kunden en uppskattning av vad det kostar. Ofta är den typen av beräkningar så låg att den inte har någon effekt på projektet. Där är egentligen övervakning och uppsättning mycket högre än vad själva kostnaden för plattformen är. Därför är det småpengar i sammanhanget för det mesta. Vissa kunder har behov av extrem kapacitet, det kan vara t.ex. att man vill distribuera en stor video till en stor mängd besökare. Då kan en sån kostnadskalkylator vara användbar, dvs. vilken metod ska vi använda för att leverera och vad kostar det. Så man kan ge de en vettig prisbild av vad de kan förvänta sig.

S: Nu är säkert era kundprojekt mycket större än era interna projekt. När ni gör interna projekt är ni delaktiga i kravinsamling och planering av projekt. Är det något ni använder då?

I2: Vi har ju inte jättemånga interna projekt, de är ett fåtal vi driver själva. Där har vi nog aldrig använt några verktyg för det. Det är väldigt ad-hoc, det är ju inte vår expertis egentligen och därför har vi inte det.

[Tillfällig paus]

V: Innan ni startar ett nytt projekt, genomför ni något arbete för att identifiera och planera för eventuella säkerhetsrisker och hot?

I2: Ja, det gör man ju. Man gör någon form av bakgrundskontroll medvetet eller omedvetet. Vi kanske inte har någon formell punkt som heter så men jag har ganska god erfaranhet av säkerhetsarbete så därför gör jag intuitivt vissa saker på ett visst sätt. Sen kanske det hade varit bättre att formalisera så att man inte missar något. Vi gör en bedömning av säkerhetsrisker.

V: Är er molnleveratör inblandad i den bedömningen?

I2: Bara i form av att vi använder deras dokumentation. Att vi läser om det är något undrar, som hur något sparas, hur det överförs eller vem som kan ha tillgång till informationen. Dem är inte aktiva. Nästan alla molnleverantörer är väldigt passiva tjänster, det är "man-får-sköta-sig-själv"-tjänst.

V: Ni tar ändå del av någon form av information från dem för att se var riskerna finns?

I2: Vi kollar deras dokumentation där de skriver om vilken säkerhet de tillämpar, hur de hanterar nycklar. Sen kanske man också gör sökningar på deras forum och kollar vad andra

har sagt om vissa säkerhetsaspekter. Själv har jag upplevt att t.ex. Amazon har väldigt hög säkerhet. I början, för fem sex år sedan, var jag förvånad över hur pass nedlåst en ny dator var. Man fick själv öppna upp varenda liten tjänst man ville skulle vara tillgänglig utåt. Man fick en låst svart låda och öppna upp tjänst efter tjänst till skillnad från hur det var på vissa lokala, mindre webbhotell som även tillhandahåller virtuella servrar. Där köpte man en virtuell server så var den väldigt öppen med många tjänster igång när man fick den. Då kände jag att Amazon hade ett mycket högre säkerhetstänkt över vad jag förväntade mig.

V: Har ni någon typ av kontroll eller test för att upptäcka olika säkerhetshot?

I2: Vi bevakar servrarna, t.ex. kapaciteten. En sån tjänst som vi bevakar som är hacker-benägen är e-posthanteringen, utgående e-posthantering. Den hackas i spam-syfte. Där har vi program som övervakar utgående trafik, och om den passerar vissa av våra tröskelvärde så stänger vi ner tjänsten. Där finns säkerhet i två nivåer, om inte vi stänger ner tjänsten när den börjar anmälas för spam så stänger Amazon ner tjänsten när den börjar användas för spam. Då har vi ett bekymmer för då kan inte vi återstarta tjänsten utan att be Amazon om lov. Det har hänt någon kund att de fått sina nycklar stulna för hur man skickar utgående e-post och det har utnyttjas som en spamleverantör i storleksordningen 50.000 spam. Det slår i taken för AWS och de stänger ner tjänsten. Där har vi skrivit egna regler för att varna vid mycket lägre tröskelvärden eftersom vi kan bedöma vad en tjänst normalt ska skicka iväg. T.ex. om den övergår ett tröskelvärde på 1000 mail om dagen så ska den stänga tjänsten.

V: De verkyg och gränserna ni sätter upp gör ni inne hos molnleverantören?

I2: Ja, det är egentligen små övervakningsprogram. I AWS finns det en stor tjänst som heter Cloud Watch som har massor av olika övervakningsverktyg för att övervaka alla möjliga typer av tjänster internt. De kan man knyta ihop och programmera mot. Man kan skriva script som säger "när den här nivån överstigs under den här tiden så ska du göra så och så". Jag vet att Amazon har sånna regler själva för att stoppa, reglera och stänga ner. En liknande gräns som finns är en varning om kostnaden för AWS börjar skjuta i höjden, om vi förbrukar pengar i en snabbare takt än vi förväntar oss. Kör man igång 10 instanser får man betala för alla medan de är där. Om vi inte förväntar oss att de ska vara där så blir vi förvånade att det kostar massa pengar. Då kan man t.ex. sätta in en varning om förbrukningsnivån överstiger en förbestämd takt innan det blir en för stor kostnad.

V: Ni använder framförallt AWS. Har ni någonsin upplevt att ni är begränsade av er molnleverantör i förhållande till programmeringsspråk, ramverk och kompabiliteten dem emellan?

I2: Ja, lite. Vissa molnleverantörer gör vissa språk mer tillgängliga. AWS har väldigt stort tjänsteutbud vilket gör att man blir låst till deras sätt att tänka och göra saker på. Det begränsar både innan i vad som finns och efter i vår möjlighet att flytta runt tjänster, t.ex. till Azure eller Google eftersom de har lite annorlunda sätt att se på det.

V: Anpassar ni er då eller försöker ni hitta någon väg runt det?

I2: Oftast gör vi så att vi tar höjd för det redan när vi utvecklar. Vi ger oss möjlighet att ändra om vi vill, om det är relevant. Ibland vet man att det är så liten risk att ändra så då gör man det specifikt för molnleverantören, Amazon.

V: Det påverkar på något sätt organisatoriska beslut också, vad det finns för kompabilitet hos leverantören?

I2: Ja, det gör det.

V: Anser du att molnleverantörerna ger den här informationen tydligt innan?

I2: Det är lite olika. Vissa saker upptäcker man längst vägen och anpassar sig efter det.

V: När ni kommer med en ny uppdatering och distribuerar det mot er molnleverantör, upplever du att det finns någon säkerhetsutmaning med själva distributionen?

I2: Nej, inte mer än att ha de där överhuvudtaget.

V: Påverkas era utvecklingsprocesser av er molnleverantör och de verktyg de tillhandahåller?

I2: Ja framförallt i form av möjligheter. Man ser att molnleverantören erbjuder en tjänst som underlättar, t.ex. den mest basala och enkla som finns AWS är köhantering: hanteirng av saker som ska utföras i en kö. Ett jobb som är tungt som man inte vill köra direkt, då har man en maskin som tuggar av på de jobben så ofta den har möjlighet men det finns för många jobb i kön för att köra hela jobbet direkt. Istället för att själv bygga en databas som håller reda på vad som finns i kön, och en databas som hämtar ut och lämnar in värden där och ser till vad som blir gjort så finns det en tjänst färdig för det.

[Bakgrund för information- och datasäkerhet]

V: Upplever ni att det finns en risk eller utmaning med att obehöriga får tillgång till känslig data eller kritiska applikationer? Era egna eller kunders tjänster och data.

I2: Ja det är något som ligger i bakhuvudet hela tiden, var man än sparar data oavsett om det är i molnet eller en dator på kontoret.

V: Hur hanterar ni den risken att någon som inte ska ha tillgång till viss information får tillgång till den?

I2: Vi hanterar rätt så mycket känslig data, det kan vara källkoden till en kunds system som kan utnyttjas. Av den anledningen har vi ganska hög säkerhet vad det gäller hur vi hanterar data. Alla datorer och laptops krypterar vi så att om de blir stulna så är det det fysiska värdet vi blir av med men inte innehåll. Krypteringen hade kanske inte hållt för NSA men en vanlig hobbyhacker kommer inte förbi det i alla fall. Samma sak gäller telefoner som också är en känslig punkt. Det svåraste är egentligen att komma åt information som finns i e-post, eller konton som är kopplade till ens e-post t.ex. AWS-kontot. Får de tillgång till AWS kommer de tillgång till allt, därför kräver vi att alla konton till e-post och AWS ska ha två-steg-auktorisering. Det är för att säkra upp så att man inte kommer åt informationen bakvägen vilket är den största risken till skillnad från den publika delen av webbtjänster där användare loggar in.

V: Ni har någon typ av strategi för att förhindra intrång?

I2: Nu är det t.ex. en praktikant som ska göra ett visst arbete som ska komma åt viss kunddata och då har vi sett till att den data som vi har tillgänglig skickar vi över anonymiserat. Det är

rätt innehåll för att utföra uppdraget men den är anonymiserad och på det sättet ser man inte vem den faktiska kunden är i databasen. Vi tar alltid sånna beslut oavsett om det är moln eller inte. Sen försöker vi alltid tänka igenom vilka senarion som kan uppkomma.

V: Har ni någon gång blivit utsatta för ett intrång av en obehörig?

I2: Inte vad vi känner till. Inte vi direkt, däremot har vi varit med och städat upp hos kunder där det har skett.

V: Hur hanterade ni den situationen?

I2: Där var vi först rädda att det var vi som hade haft säkerhetsintrånget. Efter ett tag visade det sig att det var en kunds data som var infekterad med ett virus och det viruset och det hade skvallrat om flera inloggningsuppgifter som den datorn hade haft tillgång till. Så allt var begränsat till vad just den kunden hade kommit åt och det var så vi upptäckte det. Vi försöker lista ut vad det har kommit ifrån och utesluta. Beroende vilken information som har blivit kompromissad och vilka system det har passerat igenom kan man lista ut var det läcker.

V: Har ni någon strategi för att motverka attacker? T.ex. DDoS-attacker.

I2: Mot DDoS-attacker har Amazon olika försvar som man kan bygga in så att DDoS-attacker inte når slutservern. Man kan blockera ut trafik. Det har vi varit med om ett antal gånger. Ibland arbetar vi aktivt med det och ibland hanterar Amazon det automatiskt.

V: När ni befinner er på en publik molnlösning kan man också utsättas indirekt för en attack. Vi talade senast om att AWS låg nere en viss tid. Har ni blivit utsatta för en indirekt attack?

S: Det behöver inte nödvändigtvis vara på grund av en attack, utan kan vara en anledning som Amazon varit otillgänglig.

I2: Det har vi säkert vid några tillfällen, men inte så att vi har lidit stort av det. Det har varit driftstörning på servrar som har varit utanför vår kontroll. I vissa fall har man hört att det varit angrepp. Så länge vi har använt Amazon så har vi inte haft det bekymret. Däremot har vi haft bekymmer när vi låg hos svenska leverantörer, där vi indirekt har påverkats.

V: Hur har ni hanterat den situationen när ni indirekt skadats?

I2: Det är ju lite därför vi har flyttat till Amazon. I AWS är det svårare att göra den typen av attacken. Sen är de ett större mål, så de som verkligen vill kan anfalla Amazon och göra mycket mer skada då och för många fler. Antagandet är att Amazon är en starkare part och därför är risken mindre men det är lite som att höja insatsen, när det väl händer så händer ordentligt. Precis som det gjorde 2015.

V: Om det hade hänt i framtiden, hur hade ni hanterat det?

I2: Det beror på vad som händer och hur AWS hanterar det. Det beror också på om andra leverantörer hade hanterat det bättre. Det är ju därför vi har flyttat till Amazon en gång i tiden, för att de känns stabilare och stora nog att hantera det. När det väl händer, har vi inte en stor plan för det. Då sitter vi och får snällt vänta. Om hela AWS skulle ligga nere, vi har domäner, databaser och innehåll där vilket inte är oersättligt - vi kan bygga upp det igen - men det skulle ta tid och vi skulle lida under en period när vi flyttade. Vi ser till att försöka ha

en kopia offline, så har vi har en säkerhetskopia utanför AWS. Det är den enda försäkringen vi har egentligen. Annars är vi utelämnade till deras säkerhet i mångt och mycket.

V: Har ni någon typ av kontroll för att upptäcka avvikelser i hur er data och kapacitet används?

I2: Vi har kontroller för hur mycket vi förbrukar per dag. Den har vi satt till ungefär 25% över vad vi förväntar oss att den ska vara. Det är en ganska jämn kostnad hela tiden, vi har inga bursts utan jämn förbrukning. Om den överstiger 25% av förväntad debitering så mailar den till oss och säger att något händer. Då kan vi gå in och kolla, ibland är det helt förväntat t.ex. en ovanligt stor besökarstorm men annars blir vi rätt tidigt varse att det är något fel så att vi kan gå in och stänga ner det som behövs.

V: Ni tar backups varje dag, så att ni kan rulla tillbaka till gårdagen. Har ni någon typ av kontroll för att upptcäka om det finns avvikelser i dataförlust eller -manipulation?

I2: Det är olika för olika system. Det är inte bara daglig backup, i de mest avancerade system vi har så är det för det första tre databaser i synk där två är i molnet och den tredje är on-premise och som håller en aktuell kopia av allt hela tiden i realtid. Utöver det så görs det en daglig backup av en av servrarna och hela tiden har senaste dygnet kopierat. Utöver det så finns det en månatlig backup som körs på sidan. Detta är en av våra mest avancerade uppsättningar för de som verkligen inte vill förlora någon data. Fördelen med den här uppsättningen är att det finns olika typer av återställning från en backup. När man pratar backup är det ibland lite slarvigt för det finns många olika typer. Här kan man se dataförlust eftersom man kan jämföra hur det ser för exempelvis en månad sedan mot hur det ser ut idag. Har man bara den senaste backupen hela tiden är det svårt att avgöra när eller om något har skett.

V: Om data eller information inte hade varit tillgänglig hos molnleverantören har ni alltid er lokala backup som ni kan hämta ifrån?

I2: Vi har alltid en lokal kopia också av just den anledningen. Vi vet att vi kan påverkas.

V: Har själva plattformen hos molnleverantören varit otillgänglig?

I2: Nej, vi har aldrig haft det bekymret att t.ex. AWS varit otillgänglig i sig.

V: Om det hade skett, kan du tänka dig in i hur ni hade hanterat det?

I2: Jag misstänker att vi inte hade kunnat göra så mycket än att lägga ett supportärende och sitta och vänta.

[Bakgrund för datakontroll och ansvar]

V: Vendor Lock-in beskriver problematiken att flytta sina tjänster och data mellan leverantörer. Har ni upplevt den problematiken?

I2: Ja det har vi. Ibland väljer vi att medvetet att gå med på det, eftersom deras tjänst är så bra eller att det inte finns någon motsvarighet och då accepterar vi den problematiken Vendor Lock-in ger i utbyte mot de fördelar de ger.

V: Ni accepterar problematiken som finns i vissa fall?

I2: Ja, precis. Man får beakta den då, för i vissa fall kan man med ganska små medel komma runt den. Det finns ett oberende ramverk, Kubernetes, som hanterar små mikrotjänster. Det kanske är bättre att använda det ramverket då som stödjs av fler leverantörer än att använda någon specifik. Jag nämnde kötjänsten som finns i AWS, om jag bygger allting runt den tjänsten så är jag ju låst till AWS. Men om jag istället själv bygger en Kubernetes som driver en kötjänst kan jag ju uttnyttja den överallt, t.ex. Amazon eller Microsoft.

V: Molnleverantörer är ett eget bolag med eget vinstintresse som kan ändra policies eller priser. Har ni upplevt en förändring hos molnleverantören som har påverkat er verksamhet?

I2: Nej, inte direkt. De har ändrat priser så att det har blivit billigare men inte så att vi haft bekymmer med det.

V: Om det skulle ske något förändring som får er att rynka på näsan, har ni då en plan för hur ni ska migrera eller flytta till en annan leverantör?

I2: Nej det har vi ingen plan för alls, det tar vi om vi får problemet.

V: Har du förtroende och tillit för er molnleverantör?

I2: Ja, stort.

V: Har ni också tillit att molnleverantören tar ett säkerhetsansvar?

I2: Ja, stort. Hela deras tjänst bygger på att de tar ansvar för det så jag antar att de har mycket bättre kunskap om säkerhet än vad jag har. Så länge baserar det på deras tjänster och gör som de har tänkt så bör det vara säkert. Det är ett grundantagande jag har.

V: Är det något som skaver med att ni inte har fullständigt kontroll över data, tjänster eller säkerhet?

I2: Inte för oss. Vi hanterar inte nationell säkerhet precis. Jag förstår att man måste ha större kontroll om det t.ex. är ritningar till ett kärnkraftverk eller liknande. Då är det andra aspekter som spelar in, främande makter och allt möjligt. För vår del känner jag inte att det är något bekymmer.

V: Vad tar ni för ansvar för att hantera dataförlust mot själva molnleverantören?

I2: Vi tar egentligen inget ansvar alls. Vi är mest med i utvecklingsfasen och inte i underhållsfasen och de senare delarna. Vi överlåter ofta det på kunden. Vi har en del större kunder som har sina egna IT-avdelningar. Vad vi gör är att hjälpa dem att sätta upp ett AWS-konto och hjälper dem att hantera kontot, men det är deras konto och då är villkoren mellan Amazon och kunden direkt - inte via oss. Sen förklarar vi lite hur det fungerar vilket ger oss ett litet ansvar, men vi försöker vara tydliga med att vi hjälper dem att sätta upp tjänsten och ansvarar inte för den.

S: Tror ni att molnleverantören värnar om era intressen?

I2: Jag tror absolut inte att de värnar om våra intressen, däremot ser de oss som en kund. De tjänar pengar och om de skulle ha säkerhetsproblem så förlorar dem pengar. De är

intresserade av oss specifikt men däremot måste de ha en viss nivå av säkerhet för att vara så stora som de är. Vi är små och obetydliga för dem men de måste ha en policy som täcker allt och alla.

[Slut på intervju]

3.3 Intervjuobjekt 3

V - [Bakgrund ---]

V: ... så tänkte jag börja med att fråga lite om dig och den verksamhet du jobbar på, om du skulle kunna beskriva den; hur många som är anställda, hur många kontor har ni, vad för typer av tjänster utvecklar ni?

I3: det är ett kontor som är liksom fast, vi är ungefär tio anställda, more or less

V: vad är det för tjänster ni utvecklar och distribuerar?

I3: en handelsplats för [branschprodukter] med tillhörande värdegivande tjänster, såsom analys av [produkt]-marknaden och verktyg för att lyckas som handlare, både köpare och säljare av [produkt]

V: okej. vilken eller vilka molnlösningar använder ni av när ni utvecklar och distribuerar?

I3: men då är ni inte intresserade av SaaS, alltså?

V: nej, precis. Så om ni använder gmail eller google docs; det är vi inte intresserade av, utan både liksom vilka leverantörer...

I3: då är det typ bara GCP, alltså google cloud platform, om ni tänker IaaS och PaaS,

S: vi är dels intresserade av infrastruktur som mjukvarutjänst. sen är det ganska vanligt, om man har infrastruktur hos amazon eller google att man har vissa andra utvecklingsverktyg ovanpå det och då blir det en plattformstjänst och det är i det spannet vi tittar på. Så det vi vill identifiera är nog vilken infrastrukturtjänst använder ni och vilka ytterligare plattformstjänster använder ni, ovanpå det. Så det är nog helt i rätt spår där, att ni använder google cloud platform sa du, va?

V: ja, GCP. Sen har vi ju dedikerat oss ganska mycket till det, men plattformen är i princip infrastrukturagnostisk. Vi har byggt det via kubernetes i GCP.

V: just det. Hur lång erfarenhet har ni av att jobba med cloud computing och gcp?

I3: jag började jobba med gcp i slutet på 2017, så 2,5 år ungefär.

V: när ni valde google som leverantör, gjorde ni någon typ av jämförelse mellan de olika leverantörerna baserat på datasäkerhet?

I3: baserat på datasäkerhet tror jag inte att jag la in så mycket, men jag jobbade ju på google tidigare, som cloud solutions architect, och det blev ju oundvikligen så att jag skaffade mig ett bias i frågan, i och med att jag lärde mig väldigt väl hur gcp funkar. Sen har jag satt upp motsvarande plattformar både i Azure och AWS. Det är väl de stora, de är ju också helhetslösningar. Tidigare jobbade vi med mindre distributörer, framförallt IaaS, vi hade virtuella servrar och fysiska servrar både hos mishosting, 05:44, godaddy, men det är ju ett tag sedan, det är några år sedan. Men utifrån ett säkerhetsperspektiv så var det ungefär så att vi fick 100 000 dollar att göra vad vi ville för i GCP och

då valde vi det av de anledningarna. Jag tror att, vad gäller just infrastruktursäkerhet så är de väldigt stabila. De stora säkerhetsriskerna ligger snarare i den egna implementationen hos bolaget. Jag ser inte ett så stort problem, säkerhetsmässigt i GCP, utan det är handhavandeproblem från vår sida, i så fall, som är den stora problemfaktorn.

V: du beskrev era tjänster som ni utvecklar. Anser du att ni har några speciella säkerhetskrav i den tjänsten? Vilka olika typer av säkerhetskrav har ni när ni utvecklar eran tjänst?

V: Vi har gjort ett arbete nu, sedan november har vi jobbat en del med IT-säkerhet och vi har öppnat upp lite mer av plattformen, men det är fortfarande så att vi släpper bara in användare som har företagskonton kopplade till sig, så när man skapar ett användarkonto i vår plattform måste du både ge ett legitimt personnummer och ett legitimt organisationsnummer, vilket gör att vår plattform i dess fundamentala form inte kommer ringa in en ohygglig mängd användare. Våra bekymmer kommer snarare dyka upp om ett tag, när vi har tagit in en automatisk lösning för betalningar. Våra transaktioner snittar i nuläget på 160 000 kr per transaktion och då är det viktigt att sånt blir rätt, men... det är ju en SaaS-tjänst som vi kommer använda oss av där. I själva utvecklingen är vi väldigt noga med hur man hanterar olika sorters token. Vi har använt lite olika tjänster för att göra pen-tester, framförallt automatiserade pen-tester, som egentligen inte är tillräckligt bra. Vi skulle vilja investera, under det kommande året kanske, i att hyra in någon som gör pen-tester därför att de automatiserade är inte tillräckligt bra. Vi jobbar också med GraphQL-api:er istället för REST-api:er, vilket många av de automatiserade inte klarar av, enligt min åsikt.

V: Sören, har du någon följdfråga på det?

S: Nej.

I3: vi är väldigt noga med att ha uppdaterade SSL-certifikat....

S: det vi egentligen är nyfikna på... jag tror att vi har fått svar på det vi undrar egentligen. Det vi undrar är om er verksamhet eller er bransch i sig har specifika krav. Om i hade pratat med någon som jobbar, låt säga på KRY eller någon tjänst som hanterar känsliga persondata, då vill vi höra om särskilda säkerhetskrav som är unika för vår verksamhet och bransch. Vad de tekniska detaljerna i dem är detaljer, men det vi är nyfikna på är om det finns särskilda säkerhetsutmaningar för er bransch.

I3: det är en pågående diskussion inom lantbruk och livsmedelskedjor om jordbrukets data. Vi har byggt plattformen så att allt går att härleda till olika entiteter så att i samband med att GDPR trädde i kraft byggde vi om hela vår databas. Vi har inte jättekänsliga data egentligen. Vi har personnummer, vi har personinformation...

S: och i och med att det går under GDPR är det egentligen precis samma som alla verksamheter som hanterar personuppgifter.

I3: Där löser GCP det bra för oss. En gång om dygnet gör vi back-ups av databasen och GCP tar hand om att radera data i tidigare versioner. Det hade varit ett mäck annars, att sätta upp själv.

S: det här är lite bakgrundsfrågor, så vi kommer in mer specifikt på det senare.

V: [bakgrund om distributionsmodeller ---] vad är det för variant ni använder?

I3: Vi kör kubernetes... vet ni vad det är för något?

S: övergripligt

I3: grundkonceptet med kubernetes, som det gäller att förstå, är poddar. Och poddar har en livslängd. Så på sätt och vis har vi inte en enda server som lever särskilt länge. De startar upp och dödas hela tiden, så vi har inte dedikerade egna servrar. Det flyttas runt ganska konstant.

V: [bakgrund om utveckling och distribution ---] Använder ni några verktyg eller någon information från er molnleverantör GCP för kravinsamling och planering?

I3: nej. Vi använder Asana. Det liknar trello och är en SaaS-tjänst.

V: Använder ni någon information från GCP om hur stor kostnaden kommer bli, hur lång utveckling, hur många maskiner ni behöver eller så?

I3: nej, det kan jag inte säga. Det är google compute engine som vårt kuberneteskluster ligger och där vet vi vad det kostar, hur många noder kan vi ha, hur många poddar vi kan ha uppe per nod. Då får man räkna på; hur mycket CPU kan vi allokera, hur mycket för olika enskilda applikationer men i mångt och mycket kan vi lägga ganska många poddar på en nod, innan det blir ett problem. Vi har ett kuberneteskluster med olika namespaces. För att beräkna, kvarinsamling, planering... SDLC är en typisk vattenfallsmetod och man kan absolut abstrahera det och trycka i agila metoder, men kravinsamling pågår under hela processen fram tills att vi är i produktion.

V: innan ni startar ett projekt, gör ni någon slags analys för att se vad det finns för säkerhetsrisker- och hot?

I3: inte strukturerat, men vi gör alltid en säkerhetsanalys. Jag gissar att om man har ett bolag som har hundratalsutvecklare så behövs det ett ramverk, men vi är just nu fyra och en halv utvecklare och då får vi lita på [anställda]. Det viktigaste vi kan göra för säkerhet är rekrytering. Vi måste se till att varje person funderar över detta. Vi produktionssatte en ny stor funktion nyligen och då är det så att man måste fundera; när man signerar, vad skulle hända om de signerar flera gånger? Men det finns inte en strukturerar process och definitivt inte i samband med [molntjänsten]. Hela den här infrastrukturbiten; varför vi valde just GCP är för att lägga minimalt med tid på infrastruktur. Vi har satt upp på ett sätt så att jag kan ha en ny applikation med en ny URL som är SSL-hanterad och lastbalanserad på 15 minuter.

V: Har ni någon kontroll eller testning för att upptäcka säkerhetshot eller -risker?

I3: inte säkerhetsrisker. däremot använder vi cloud build... Vi använder oss av secrets, som är en kubernetesentitet.

V: vill du beskriva lite, vad det är för något?

I3: ... miljövariabler är en säkerhetsfråga i de flesta IT-applikationer och med kubernetes kan vi ha krypterade secrets som bara koms åt om det är inuti samma kluster och har getts tillgång till en viss pod. Våra miljövariabler är ju… om de kommer åt dem har vi riktigt stora problem, för då kommer de åt allt annat. Vi har inga integrationstester utan vår teststrategi är lagd på enhetstester, så vi testar ganska extensiv enhetstestning men har en infrastruktur där integrationstester inte tar så stor plats.

V: Upplever ni er begränsade av er molnleverantör i förhållande till vilka språk eller ramverk ni kan använda?

I3: nej. Vi har byggt det så att allt är dockifierat med kubernetes så det är samma sak där. Vi har provat att flytta hela vår applikation [till en annan leverantör], det kan vi göra på någon timme. Allt är dockifierat, så vi har abstraherat bort allt vad gäller server-delen.

S: Är det något ni har gjort avsiktligt? Har GCP underlättat? Har ni blivit styrda dit av någon annan orsak?

I3: Kubernetes behöver ju lite infrastruktur bakom för att funka men det finns i både GCP, AWS och Azure. Men även, låt säga att vi inte skulle använda oss av kubernetes; alla våra applikationer ligger fortfarande i docker-containers för sig. Det blir lite jobb med att introducera lastbalansering och någon form av intern nätverkshantering, men den är inte överdrivet stor. Det är länge sedan jag hade problem i form av "det funkar på min dator, men inte på din". Det är några år sedan.

V: när man ska distribuera och deploya ny kod, finns det några säkerhetsrisker där? Med molnleverantör, som du känner till. Hur hanterar ni det?

I3: så som den fungerar i nuläget; varje enskild person har fått lägga en nyckel på sin dator kopplat… vårt kodhotell är github och vi jobbar strikt med git och då är det så att nya utvecklare som kommer in behöver inte veta någonting om vår infrastruktur, utan det enda de behöver göra är att pusha kod och så sköts allt i bakgrunden. Det sker via autentisering mellan github och GCP och den är väldigt stabil. Och då är det mer en strategi för vem man ger tillgång till. Återigen, handhavandefel; om man ger fel autentiseringsbefogenheter i respektive plattform, men då är det som om "om jag ger min plånbok till dig så kan du gå och köpa vad du vill". Men inte va du vill… jag har inte så mycket pengar.

V: du var inte lite kort på att ni jobbar agilt. Påverkas er utvecklingsprocess av verktygen som finns hos er molnleverantör? Är det något som underlättar en viss process framför en annan?

I3: ja det tycker jag absolut. Jag rekommenderar... alla som börjar bygga något från scratch uppmuntrar jag att använda någon form av molnhantering för det är annars en massa extrajobb, om du inte explicit håller på att utveckla något som ska underlätta för någon form av infrastruktur. Då är det ju en del av din kärnprodukt, men man ska fokusera all din tid på din kärnprodukt. Om det inte är att bygga en perfekt lastbalanserade servrar ska du inte hålla på med det heller. Det gör att vi kan lägga minimalt med tid på infrastruktur. Vi ändå lite tid på det tidigare. Nu får jag ta upp privatprojekt för att få leka med servrar ens, jag får inte göra det längre.

V: Vi går vidare till information- och datasäkerhet. [bakgrund om information- och datasäkerhet ---]

V: Upplever du att det finns en risk eller utmaning med att obehöriga får tillgång till känsliga data eller kritiska data från era applikationer?

I3: Kopplat just till IaaS och PaaS känner jag mig ganska lugn. Det är snarare i implementationen, när man producerar mycket kod, som man kan missa grundläggande säkerhetskoncept. Det är mer kodrelaterat, sånt som jag är orolig över, vad gäller säkerhet.

V: Man kan luta sig tillbaka lite när allt hanteras i bakgrunden, med infrastruktur och så, finns det en risk att man utsätter sig själv för onödiga säkerhetsrisker när man ignorerar hur bakgrunden körs?

I3: [funderar]

V: har du upplevt att ni har gjort det någon gång?

I3: jo, på sätt och vis. Speciellt så som vi har byggt vår plattform nu. Låt säga att vi skulle få en [mycket större trafik], av någon anledning går hela Sveriges befolkning in på vår hemsida. Då kan, beroende på hur man har satt upp applikationen... vår applikation skulle krascha då. Men du kan ju konfigurera, i de här molnplattformarna, så att de skalar automatisk, horisontellt, genom att lägga till fler [maskiner, enheter, mer kapacitet]. De har ju väldigt starka lastbalanserare generellt. Så länge det inte handlar om att ha en väl uppdaterad databas så kan du föda väldigt mycket trafik och det blir ju snarare en risk för en väldigt stor kostnad; det kan kosta mycket pengar. När du då kan göra allt i en plattform så kan man också göra allt. Låt säga: "oj, nu råkade jag skapa 20 replikas av den här", som sitter och skickar 1000 requests i sekunden till något ställe... det hade vi några studenter som gjorde [av misstag]. "With great power...".

V: exakt

I3: ... Inte för dataintrång på det viset. Då är det mer en risk att det skenar iväg. Det är till och med så att spotify sitter och har problem med budgetar på deras molnplattform; de har också dedikerat sig ganska mycket till GCP och har problem med att folk [utvecklare] skapar en massa [instanser] och leker runt och så kommer det en räkning i slutet på månaden som är jäkligt stor. Men inte i form av datasäkerhet.

V: har ni någon typ av strategi för att hantera ifall någon som inte är behörig gör ett intrång i era tjänster eller applikationer?

I3: nej, jag tror inte det. Jag kan bara ge mitt logiska svar: att jag skulle förmodligen bara stänga ner hela applikationen. Vi har ingen strukturerad lösning.

V: det kan ju vara både att de kommer åt er molnplattform, men också vara era tjänster som ni har utvecklat.

I3: ja, kommer de in i vår molnplattform så är det ju jobbigt, onekligen. Vi försöker, med alla tjänster vi har, att jobba med två-faktors-autentisering. Så när du kommer in som ny användare i våra system får du sätta upp, om det så är för slack eller gmail eller vad det nu är, att alla delar där det faktiskt går att använda tvåfaktorsautentisering ska du göra det. Så det är väl lite av en process.

V: Det låter på dig som att ni inte har råkat ut för ett intrång i era tjänster.

I3: Inte vad jag vet.

V: Har ni någon strategi för andra typer av attacker mot era tjänster? Har ni någon strategi för hur ni ska hantera det? Det kan vara en DDoS-attack eller virus eller andra typer av attacker.

I3: Kul att du nämner det! Vi fejkade en DDoS-attack nu för tre veckor sedan, på våra egna system. Eller då tog vi ju våra staging-system. Vi lyckades krascha applikationen, så det var ju bra. Vi lyckades krasch:a den på flera sätt. Men då var det just för att kika på om vi, låt säga får väldigt mycket trafik, hur hanterar vi det då? Så vi har en process och strategi för att hantera väldigt mycket trafik. Och då hjälper definitivt GCP. Då är det jättebra att ha det, eller någon annan molnhanterare.

V: Så ni hanterar det genom att koppla på automatisk upp- och nedskalning, eller?

I3: nej, jag vill inte ha automatiskt. Det vi har satt istället är notiser, som vi får när trafiken ökar. Så du kan använda dig av olika former av loggning. Med GCP använder vi oss av stack driver för att få notiser om när någonting går över det normala, och det kan vara allt från CPU-hantering till nätverkstrafik, [som den] ska varna för. Då kan vi bara trycka på plusknappen, vilket hade varit väldigt jobbigt om vi hade haft egna servrar.

V: Har ni någon gång utsatts för en indirekt attack? Ni delar ju resurser, på en ökad nätverksyta. Googles servrar kanske ligger nere och då påverkas ni indirekt. Har ni blivit utsatta för någon sån attack tidigare?

I3: Det är ju som du säger, en indirekt eller ofrivillig attack. Jag tror inte att det var en attack, utan vi ett tillfälle så… i GCP jobbar man i olika zoner, var man har sin infrastruktur någonstans, och då var det just att vid något tillfälle sommaren 2018 så var vi i början på juli, då gick våran applikation då och då upp och ner och när man gick in och kollade så var det som att "jag har ingen aning om vad som händer" därför att allt verkade okej. Då var vi en av de första som upptäckte det här, måste vi ha varit, därför att då hörde vi av oss till dem [GCP] och sa det: "det här är ju kaos" och då fick vi, i och med att vi jobbar med olika docker-containers, de sa då att vi får köra upp en basal engine X-server och när inte den funkade då så triggade det "ah, vi [GCP] får kolla mer på det här" och då kom det

sen; då basunerade dom ut, lite senare då, att "alla de här zonerna har just nu problem, vi jobbar på att fixa det". Jag har inte koll på vad den exakta SLA:n är, men det är inte 100% upp-tid.

V: Ändrade det här ert sätt att arbeta på något vis?

I3: Ja, till viss del. Det var ju… Det som vi fick göra då var att vi fick spinna upp ett nytt kluster i en annan zon. Det gjorde vi ju inte lika snabbt då som om vi skulle göra det nu.

V: Ni lärde er att distribuera det?

I3: Vi inledde lite arbete just med att göra den näst intill moln-agnostisk. Vi skulle kunna få upp den väldigt snabbt, som sagt, i till exempel Amazon. Vi skulle inte ha alla CICD-pipelines på plats lika fort, men att bara få upp applikationen går fort. Och sen så kan man, för en vanlig dag så deployar vi kanske fyra-fem gånger och det är väl bara att vi får skjuta på lite deployments någon dag för att få ordning på CICD. Men akuta lösningar, det löser vi fort numera och det gjorde vi inte på samma sätt då.

V: Har ni något sätt upptäcka att data går förlorad ofrivilligt, eller att data blir manipulerad på något vänster?

I3: Tyvärr inte. Men det skulle jag gärna vilja ha. Det är tidsbrist som är enda anledningen till att vi inte har det.

V: Gör ni någon...

I3: Jo, för katten, vi gör ju back-ups, en gång om dygnet. Men det är ju en gång om dygnet, men i realtid... man kan ju ha check:ar på databasen och vi har inte någonting sånt i realtid och det är inget integralt heller.

V: Du beskrev lite tidigare att ett par studenter fick använda eran tjänst och att de drev på kostnaden lite i hur de använde kapacitet. Gör ni någon form av kontroll för att upptäcka om det är avvikelser i hur tjänsten används?

I3: numera gör vi det.

V: så ni har koll på vilka beräkningar som görs och hur stor kostnad ni har?

I3: det hade varit naivt av mig att säga att jag har koll på allihop, men vi har koll på fler och fler. Det är just, typ en sån här sak, vi vet det nu att i GCP kan man enkelt koppla på olika API:er. Du kan enkelt koppla på om du vill hålla på med Google maps eller google translate eller google vision eller någon sån här och nu vet vi att varje gång du vill koppla på så måste du sätta en budget. Då kan man sätta budget allerts. I det här fallet med studenterna, det som var bra då var att där hade vi ändå satt en budget allert, så jag vaknade ju upp på morgonen och så stod det, du har nått 50% av budget och jag kunde då gå in och [imiterar att trycka på en knapp och gör ett prutt-ljud] stoppa allting. Men det var ju ändå så att det kostade oss 5–6000 och det var ju halvkul. Då satt de och skickade hur många requests som helst. De hade använt ett kronjobb som bara gick och pumpade. Det var lite spännande.

V: har eran tjänst inte varit tillgänglig vid något tillfälle? Eller molnleverantören, vid ett annat tillfälle?

I3: under tider som vår tjänst inte har varit tillgänglig, det har ju varit många. Det är ju titt som tätt. Men det är ingen som märker. Ofta när vi gör, kanske, bakåtinkompatibla förändringar så gör vi det på udda tider. Det är inte långa perioder. För ett tag sedan gjorde vi en väldigt stor uppdatering där vi i princip bytte ut, stor infrastrukturellt, ackordmässig stor skillnad när vi deployade och då låg applikationen nere i en halvtimme. Men det var också kl 02:30 på natten och vi har då

lantbruksinriktade kunder så jag är ganska säker på att vi inte hade i princip någon användare inne över huvud taget. Det är nog det längsta vi har haft. Sen att det händer några sekunder lite då och då, det händer någon gång i veckan. Då är det helt och hållet för att vi... eller, inte nere, det är väl mer att... Vi jobbar ju med microservices-arkitektur och då är det så att man kan få API-förändringar som den inte känner igen på en gång, mellan de olika microservice:arna och då kan det var någon som klient som försöker anropa en icke existerande end point. Men vad gäller just molnplattformen är det den enda gången som jag jag vet att de verkligen har triggat att det har legat nere, som jag vet om. Annars är det helt och hållet handhavande.

V: Har själva molntjänsten i sig legat nere någon gång, att den inte har varit tillgänglig för er att komma in på?

I3: inte som jag minns.

V: om det skulle vara så att den ligger nere under en viss tid, hur hade ni hanterat det då? Vad hade ni gjort för att lösa det?

I3: jag vet inte. Jag skulle nog ha... Jag vet inte hur snabbfotad man är. Men låt säga att det är på dagen och att man märker att man inte kommer in. Då kommer man varken in på deras plattform eller på deras hemsida. Om jag inte kan göra det, då skulle jag nog ta action inom... inte superfort, inte i den fasen som vi är nu. Vi gör då som sagt ganska stora transaktioner, men vi gör då kanske, nu har vi ungefär en transaktion om dagen. Och vi har ganska nära kontakt, så då hade vi.. Jag tror inte vi hade förlorat så mycket pengar på om det hade legat nere ens några timmar. Då kan vi bara återkomma sen och säga att vi hade trubbel och mejla ut. Efter en timme skulle vi ta action. Det går ju att skapa ett test-konto på amazon eller microsoft med någon fejk-adress och få upp den ganska fort. Bara som en temporär lösning. Sen blir det liksom nästa lösning och nästa lösning, men det är ju en rejäl eskalation.

V: har ni någon status page för att kommunicera ut till era kunder ifall någon del av tjänsten ligger nere?

I3: ja, vi har sync:at med, det heter zengrid, som är en SaaS-tjänst. Den är konstant up to date med vilka kontakter vi har i vår interna kontaktdatabas, så då kan vi trigga mail till alla våra användare därifrån.

V: slutligen tänkte jag bara kolla, vi har varit inne på molnleverantören, vi har varit inne på er tjänst och så där, är det någon gång ni har upplevt att data eller någon annan information som ni behöver inte har varit tillgänglig i ert arbete?

I3: Har du något exempel?

V: Det kan väl vara att ni inte kommer åt vissa API:er eller att ni inte kommer åt någon databas...

I3: Jo men det har vi. Vi har haft trubbel med mer än ett tillfälle faktiskt, två gånger har det hänt. Vid registreringen så skriver du in både organisationsnummer och personnummer. Organisationsnummer hämtar vi ut från allabolag, som strikt sett ska vara en direktkoppling till bolagsverket. Vid något tillfälle har det legat nere, ett tillfälle, och vid ett tillfälle har vi blivit nekade felaktigt.

V: så det är mer på deras håll än på ert?

I3: Ja, i och för sig. Sen kan det vara någon gång som vi har gjort fel, men då är det för att vi har gjort fel på vår sida. Att man någon gång skickar requests till fel ställen, det har ju hänt. BankID, i början, när vi implementerade det, så var det inte superstabilt. Men då är det mer på den egna sidan och de är väldigt hårda med sin felhantering så då blir det att folk inte kan använda vår applikation.

V: vi har en avslutande öppen fråga, om det är något du vill tillägga till er hantering av information- och datasäkerhet; är det något du vill tillägga eller ska vi gå vidare till den sista delen?

V: [bakgrund om datakontroll och ansvar ---]

V: [förklarar vendor lock-in ---] du var inne på att ni snabbt och enkelt kan flytta er tjänst till till exempel amazon. Har ni upplevt den problematiken? Ni är ju i och för sig trogna till Google där. Hur tänker ni kring den problematiken?

I3: ja, det är väl databaserna, har vi inte en backup på utanför GCP. Kodmässigt så är det inget problem, men databaserna är ett problem. För där har vi bara tagit sporadiskt. Det är inget stort problem för oss att faktiskt fixa det. Enda anledningen till att vi inte har gjort det är tidsbrist. Där skulle man kunna ha en sync med någon annan plattform så att man lägger databasen någon annanstans. Det är ingen dum idé! Jag får kolla på det.

V: Det låter på dig som att ni blir tvungna att byta leverantör så skulle det gå ganska smärtfritt.

I3: Ja, men det är ett problem med data. Låt säga då, i det sjuka eventet, att de raderar all vår data, då är vi kokt i bajs.

S: Det är ju en ganska extrem situation, med wikileaks, men låt säga att er leverantör annonserar att om två veckor kommer vi ändra policies och detaljerna gör att ni upplever att "det här kanske inte är så bra för oss", skulle ni kunna flytta med databaser på en vecka eller en månad eller så där?

I3: alltså, det är ett kommando per databas som jag gör lokalt på min dator så har jag all data.

s- så, i praktiken låter det som att ni inte upplever vendor-lock in särskilt starkt alls, så att det är ett hinder för er om ni skulle vilja byta.

I3: nej, det tycker jag inte. Däremot så är de ju, som jag sa innan, ska man bygga ett företag helt utan pengar då är det en annan fråga. Det kostar ju en del med molnleverantörerna, men fasen vad skönt det är. Det som jag tyckte var skönt är... det här är en personlig åsikt: vi funderade ett tag på att byta till amazon om de kunde ge oss en bra deal, men så gav google oss en bättre deal och så stannade vi på google, och sen så känns det bara som att vi kan ju byta ut de olika API:erna mot någon annan, men det är jävligt soft att ha allt på samma ställe. Och där inser jag ju mycket väl att vi Google leder oss i hur vi ska beteende, men det köper jag för de gör [det de gör] så jävla bra och det är inte en del av vår kärnverksamhet, så då betalar vi gärna. Dessutom är det så att en faktor i att vi vill använda molnleverantör är rekrytering; det är väldigt hett. Det är ballt, många tycker det är kul. För ett bolag med tio anställda är det lättare att hitta duktiga utvecklare om man har state of the art-miljöer och då är det alla de hippa, coola bolagen jobbar med antingen AWS, azure, GCP därför då får du laborera med mycket. Det kostar extra men du vinner igen det många gånger om genom att du får in duktiga personer.

V: du var inne på det lite, Sören, att molnleverantören kan helt plötsligt byta policys eller ändra priser eller något annat. Har ni det någonsin hänt för er [Intervjuobjektet], att de har ändrat någon policy som har fått er att rynka på näsan?

I3: Nej, de skickar ut lite ibland. Men om ärligheten ska fram där så är det många av dem, om det kommer ut en stor policyuppdatering så skummar jag den, max. Det är nog en statistiskt sett överlagd risk jag tar, med tanke på att vi inte i allmänhet har otroligt känsliga data att hantera. De gånger jag tittar på meddelanden från GCP är det snarare så att de har bytt version av en mjukvara. Då kikar jag lite bättre så jag vet att vår funkar. Policys på data har skett någon gång, men jag kan inte säga att jag kan minnas någon del av det.

V: skulle du säga att du har stort förtroende för er leverantör? Litar du på att de värnar om era intressen?

I3: Det är ingen fråga jag någonsin har ställt mig. Men ja, det tror jag. Tillräckligt!

V: Känner du att du har tillit till att de tar sitt säkerhetsansvar?

I3: ja.

V: Ett visst ansvar av säkerhetsaspekter kan överlappa. Ni behöver ta ansvar kring er applikation och ni tar kring sina datacenter och så. Utifall att det skulle visa sig att de inte tar de ansvar som... nu kom jag av mig lite. Sören, har du något?

S: Ja, jag tror att jag ser vart frågan är på väg. Har ni tagit på er något säkerhetsansvar som överlappar med ansvar som egentligen ligger hos Google?

I3: nej, det tror jag inte.

S: Är det redundant i någon mening att göra det eller tänka så? Är det möjligt att göra det eller jobbar ni i olika världar?

I3: I de aspekter som gäller säkerhet som google säger att de hanterar så litar vi väldigt mycket på att de gör det väldigt väl.

V: det var faktiskt vår sista fråga. Tack för att du ställer upp!

[intervjun avslutas]

3.4 Intervjuobjekt 4

V: [inleder mötet]

V: [cloud computing bakgrund]

I4: ... det är det vi säljer

s- precis, men sen använder ni kanske Amazon eller Azure till...

I4: exakt, vi har inte egna servrar

s- precis, och det är det vi tittar på.

[mer bakgrund]

V: ...och det här med PaaS och IaaS kan vara otydligt vad som är vad

I4: jag tror att alla gör någon slags, att de blandar och ger lite; man gör förmodligen inte allt utan man tar vissa delar. Om Amazon tar fram tekniker och services som man annars behöver bygga själv så finns det ingen anledning, om det inte är snordyrt.

V: jag tycker vi kör igång och jag skulle vilja börja med om du kan beskriva verksamheten: hur många anställda ni är och vad ni gör för något?

I4: ja, vi är lite speciella, vi var ju, vi gjorde och gör fortfarande en full stack-lösning för att [anonymiserad detalj], så vi har hårdvara som kopplas in i [anonymiserat], som vi samlar in data från. Sen laddar vi upp data till vår plattform där vi processar data med hjälp av amazon-tjänster, egentligen, för att presentera på appar och sidor och diverse, beroende på vad kunden vill använda sin data till.

V: hur många är ni som jobbar med det?

I4: när vi byggde hela [produkten], när vi gick för att ta över hela världen inom uppkopplade [anonymiserat] var vi 47 personer, men då var det också produktteam och säljteam och diverse. Men sen hade vi otur och en ägare köpte upp oss och gjorde att vi kånkade på två månader för att de inte hade några pengar. Men då köpte våra två största kunder upp oss. Nu är vi 11 personer med egentligen bara utveckling och vi ska förmodligen göra något försök att bygga upp teamet igen så vi blir... vi vill ha en produktavdelning också. Det är tråkigt att ha en produkt när man bara har utvecklat den. Den blir inte totalt shape:ad för marknaden som finns om man bara går på det som känns bäst ur utvecklingssynpunkt. Så nu är vi elva personer varav sju rena utvecklare och två testare och en produktchef.

V: vet du vilka molnlösningar ni använder för att utveckla och distrubera?

I4: Vi använder Amazon till största del. Sen har vi databaser, vi testar lite olika databastjänster. Amazon har de flesta olika sorters databaserna men stöder inte direkt allt som vi behöver, så vi kör lite olika när det gäller databashantering och det finns ju ganska många olika. Vi är väldigt öppna när det gäller saker; vi testar nya saker om det finns alternativ och sen ser vi om det funkar bra, om det är billigare eller dyrare och migrerar över databaser någon annanstans. Det är en öppen utveckling där om folk har förslag så får man använda det som [de önskar] används. Så vi är inte totalt fokuserade på amazon, när det finns andra alternativ som är intressanta. Men huvudsakligen använder vi tjänster från amazon för det är väldigt dumt att ha, eller, ofta är det väldigt svårt att bygga en tjänst som är totalt fristående, som man kan plugga in i amazon eller azure eller google. Det går och folk försöker det men om man läser på diverse forum och så så är det väldigt få som lyckas göra en stabil plattform där man faktiskt kan fortsätta bygga på om man vill göra den helt hosting-neutral. Vi har kollat på det men kom fram till att det inte riktigt är värt det, så då har vi anpassat oss till amazon till stor del. Det är inte omöjligt att köra flera samtidigt, men för produktionshastighet är det alltid enklare att hålla sig till ett sätt att utveckla.

V: vi kommer komma in på de mer med just hur inlåst man är till en leverantör. Men jag tänkte först kolla, när ni först valde amazon, gjorde ni någon typ av analys eller jämförelse för att kolla hur duktiga de är på datasäkerhet?

I4: Jag var inte med från början, jag har jobbat på företaget i två år och det har varit ganska bra ruljans på folk så alla har inte varit med och satt upp allting. Men vi har haft väldigt fokus på säkerhet överlag genom allt vi har gjort och vi har anlitat firmor, det är folk som har gjort arbeten på våra system och testat. Vi har alltid varit väldigt måna om säkerhet på alla plan. Vi försöker använda de senaste teknikerna inom Amazon också; om det kommer en ny teknik, som är kopplad till säkerhet så kollar vi vad den ger för fördelar och om den är säkrare om det vi har innan och än så länge har vi inte stött på något, eller något som vi har ifrågasatt, när det gäller amazons säkerhetslösningar.

V: du har jobbat där i två år, vet du hur lång erfarenhet verksamheten i sig har av att jobba med cloud computing?

I4: företaget kickades igång 2013. Första connected car-plattformen satets upp och lanserdes 2016-2017 så det var första gången det lanserades på riktigt...

[kort avbrott]

I4: ... så jag skulle säga att lanseringen är väl då, där vi faktiskt har processad data och att det har varit känslig data som vi har processat var hösten 2016.

V: [bakgrund om distributionsmodeller] vad använder ni?

I4: det är en ren kostnadsmodell. Att köra dedikerad hårdvara är otroligt mycket dyrare än att faktiskt rida på resurser som är lediga. Där har vi också läst på tillräckligt mycket för att förstå att datasäkerheten ska inte vara ett hot. Nånstans litar man på AWS. Jag vet att det finns företag som kör dedikerad hårdvara och det känns lite mer... i mitt huvud är et nästan en konspirationsteori att det finns stora risker med att dela resurser, att man inte kan ha data sparad på samma server. Sen kommer Amazon fram till massa snygga lösningar, vilket i ett miljöperspektiv och effektiviseringsperspektiv är sjukt smart. Det finns extremt mycket resurser, både databaser och servrar och allting som ligger och kör på halvfart eller 10% eller 2% eller 0,2%. Istället för att de ska hogga upp en hel server kan man ju ta all CPU och minne som finns över och effektivisera. Det har vi kollat jättemycket på och där tjänar man både pengar och energi och miljö och allting. Det är amazon duktiga på och det kommer nya saker hela tiden.

V: [bakgrund om utveckling och distribution] ...gör ni någon kravinsamling inför ett projekt och i så fall, tar ni del av information eller använder ni verktyg från er molnleverantör?

I4: alltså, när vi använder nya tekniker?

V: när ni börjar, inför ett nytt projekt, det kan vara av olika storlekar kanske ni behöver planera, kravinsamla och designa projektet. Hämtar ni information från molnleverantören då? Jag vet till exempel att amazon har någon slags kostnadskalkylator för att se hur dyrt det blir att köra x antal instanser.

I4: För det första har amazon ganska mycket verktyg i deras konsol som analyserar och ger tips på bättre lösningar. De på amazon sitter och kikar på sina kunder, vilka som spenderar pengar. De har en såpass stor del av kakan och tjänar så pass stora pengar så de hör ofta av sig till sina kunder och ger tips på sätt man kan förbättra sitt system och sätt man kan spara pengar på för att de är så pass måna om att man inte ska byta leverantör. Det är inget de tjänar på direkt, hos den kunden, utan de tjänar förtroende.

V: har du erfarenhet av att de har hört av sig till er verksamhet?

I4: ja, vi har haft dem hos oss flera gånger och diskuterat olika saker och gått igenom hela systemet och frågat. Vi vill ju veta, hur står vårt system mot andra liknande system och så har man tagit in två arkitekter från amazon och frågat "hej, hur ser vårt system ut? vad kan vi göra och vad skulle det ge för resultat?" och det är ju jättebra. Både att man kan få ganska mycket [bekräftelse] på att det är rätt och att det ligger i tiden och det är inte utdaterat, det vi gör, och vad det finns för nya möjligheter och vad skulle det ge för kostnadspåslag och vad

skulle det kunna ge för hastighet eller säkerhet eller vad det nu ger för fördelar. Det är skitkul och det är något de levererar på väldigt bra, tycker jag.

V: kommer de ut fysiskt till er arbetsplats eller...

I4: både och. Men inte nu [på grund av Corona/COVID-19-krisen].

V: innan ett projekt, gör ni något arbete för att se vilka hot som finns, säkerhetshot och säkerhetsrisker?

I4: Ofta är det inte en säkerhetsrisk mer än att... De största riskerna som vi ser... Vi litar på att vårt system mycket. Det är att det kan göra en förändring som kan påverka kunderna till slutprodukten, att tjänsten inte funkar såpass bra som den gör och sånt. Vi jobbar mycket med prem(?)14:14 och pre mortem - före- och efterstudier, så man lägger upp en lista med saker som kan hända i värsta fall. VI listar upp saker som att det här kan hända, det här kan hända... då är det mycket worst case scenarios och så läger man upp taktiker på hur man kan göra allt för att förutse dem så de inte händer och om de händer att man sparar så mycket information som möjligt om vad som händer och att man snabbt har action en action plan. Sen om det har hänt något som man inte har förutsatt har man ett möte där man gör nästan exakt samma sak: vad var det här, vad skulle vi kunna ha gjort, vad kan vi göra så det inte händer igen, vad kan vi göra så det inte uppstår igen. Designmodeller är något vi gör också: diskuterar hur vi kan bygga något som vi inte behöver ändra, som kan vara future proof, så det funkar för alla framtida sorters implementationer. Man bygger inte något som ska fungera för en sak utan man ser alltid om det kommer återanvändas och hur man kan använda det till det, eller om det är något som kommer försvinna eller något som man måste uppdatera ofta, så är det något man måste ta med i bilden.

V: är molnleverantören inblandad på något sätt att identifiera de här riskerna eller åtgärderna?

I4: nej, det skulle jag inte säga. Vi har mest använt molnleverantören är så bra den kan vara och vad vi kan förbättra. Sen har, om man kollar på databas, det finns ju flera leverantörer av databaser, det finns IBM, det finns Compose, det finns atlas, det finns många stora som hostar databaser. Och många av dem har gjort många verktyg där man kan söka igenom alla sina databaser och ser till att ens indexeringar, hur man har satt upp hela databasen, att allt är 100% och om det finns risker så brukar de automatiskt säga det till en. Det är ju väldigt bra, hur de informerar om risker. Det är ju mer risker för, det är väldigt sällan de pratar om security, det är mer downtime och oeffektivitet i diverse olika tjänster.

V: det låter som en slags kontroll eller testning för att upptäcka säkerhetshot. Har du ett annat exempel på eller gör ni andra tester för att täcka andra säkerhetsrisker?

I4: Nej. Vi har väldigt mycket regler och kodstandarder för hur man hanterar data och det är det vi trycker på. Sen är det så klart, vi är väldigt hårda med att man kontrollerar varandras kod, det ska vara minst fyra ögon på varje kodrad som skickas ut. Vi har väldigt tydliga stadgar för hur vi skriver kod, hur man hanterar känslig data, hur man hanterar lösenord, allt sånt, så att vi har de bästa tjänsterna som finns för tillfället och hanterar dem på absolut bästa sätt. Man får väldigt mycket gratis från början om man är noga och håller sina egna regler. Då blir det mindre säkerhetshot och mindre som andra kan trycka på när de kollar på ens system.

V: du beskrev att ni försöker vara lättfotade om ni behöver migrera. Har det hänt att ni har upplevt er begränsade, i förhållande till programeringsspråk eller ramverk som finns hos er molnleverantör?

I4: nej, men när de utformade mycket av plattformen för sex år sedan gjorde de bra undersökningar om vilka ramverk som kändes mest relevanta för tillvället och det är också de som har växt och blivit [de väl etablerade] under tiden, så det är viss del tur. Vissa grejer har inte gått lika bra i tiden och då har vi bytt ut mycket saker. Om man märker att saker inte blir de facto vissa grejer så är det värt att gå mot någonting som känns mer aktuellt. Det är viktigt att utveckla plattformen konstant och hänga med och inte fastna, vilket många företag gör: att de har mycket kod som de inte orkar ändra och då är det bättre att ha ta den bajsmackan och bara ändra det så fort som möjligt.

V: när ni ska pusha ny kod, någon ny funktion som ni har utvecklat, upplever du att det finns några säkerhetsutmaningar med att distribuera koden till molnleverantören?

I4: nej. Vi försöker automatisera så mycket som möjligt och använder de tekniker som finns. Vi vill att om du är inne i ett projekt och pushar upp kod till nätet så vill vi att den, så fort den är godkänd, så vill du att allting ska distribueras så fort som möjligt efter de tekniker som finns. Säkerhetsmässigt har vi aldrig sett någonting utan vi har mycket lyssnat på det som rekommenderas och det som används, till största del.

V: med säkerhet så menar jag även tillgänglighet. Har den här automatiska syncningen någon gång fallerat så att ni har påverkats av det?

I4: man använder ju verktyg för att få upp saker, oftast; du har ju en versionshanterare där du versionshanterar din kod och sen måste du använda ett verktyg för att få den koden till amazon. Där har vi kollat på olika, det finns många olika sätt att faktiskt få den till amazon. Där har vi kollat på olika sätt och sett fördelar och nackdelar med dem. Så det är är också under utveckling och vi testar nya versioner och nya program och lösningar för att det ska bli så enkelt som möjligt. Det är under progress och det är något man lär sig hela tiden och det man vill är att det ska gå så snabbt som möjligt ut i produktion. Det är det vi satsar mycket på i företaget också, att vi ska kunna gå från ide till produktion på väldigt kort tid och då är det viktigt att man har lösningar som gör det möjligt.

V: Intressant att du säger det [videokonferensverktyget laggar] påverkats av den molnleverantör ni använder?

I4: våra slutkunder, sa du det?

S: det laggar lite, hos Victor, gör det det för dig också, [Intervjurespondenten]?

I4: Ja, det laggar lite.

V: jag slår av min video så kanske det går bättre. Har era utvecklingsprocesser påverkats något av er molnleverantör och de verktyg som finns tillgängliga hos dem?

I4: Det går ju inte att undvika att saker måste uppdaterats och alla företag som håller på med mjukvarutjänster kommer ha downtime och det kommer behöva uppdateras och allt och det är inget unikt. Amazon är skitduktiga men de har så klart saker som inte funkar 100% och

man måste uppdatera vissa saker och det finns problem när saker ska uppdateras och det är inget som gör dem unika mot någon annan, men det är väldigt sällan skulle jag säga.

V: bra, vi ska hoppa vidare till informaitons- och datasäkerhet. [bakgrund]

V: upplever du att det finns en risk eller utmaning med att obehöriga får tillgång till känsliga data eller kritiska applikationer?

I4: nej, verkligen inte. Det är ju en risk att bygga ett system, så klart, Vi hade väldig tur på gamla företaget, att vi hade en dedikerad advokat som bara jobbade med GDPR och datasäkerhet så de flesta nya funktionaliteten i systemet gick en runda via henne om det man hade minsta fundering på om det hade något med GDPR eller säkerhet eller någonting [att göra] så kontaktade man henne så fick hon gå igenom hela och sen satte hon en checkmark om det var okej eller en fundering eller om man fick boka ett möte eller bara strikt nej. Så vi har jobbat extremt mycket för att hålla både GDPR-mässigt rätt och säkerhetsmässigt och att ingen känslig data någonsin ska komma i el händer. Så det är väldigt skönt. När GDPR kom och när de släppte GDPR-lagen gjorde vi inga förändringar över huvud taget i vårt system.

V: vad gör ni för att motverka att information hamnar i fel händer?

I4: det är mycket anonymiserade identifierare. vi krypterar den data som behöver krypteras. Alla lösenord, all känslig data som används i kod krypteras och hämtas från amazon och sen, all data som finns är nycklad på en anonym identifierare som i sin tur, någon annanstans, är kopplad till en specifik kund. Huvudsaken är att ha identifierare som inte säger någon utomstående någonting, som inte går att använda i något sammanhang om man inte har hela bilden. Det gäller att ha en central identifierare som är fastklistrad på all data om är kopplad till en viss kund och sen att den inte går att hämta om man inte är just den kunden. Alla känsliga uppgifter som används i kod: github är inte hundraprocentigt, man ska inte lägga upp saker på github som är känsligt, eller på någon annan versionshanterare. All känslig information som används ska hämtas från någon annan säkerhetstjänst som man använder från sin cloud-leverantör. Så det är det man håller väldigt hårt på också, att det inte exponeras några nycklar eller tokens eller lösenord eller användarnamn.

S: det låter som att det är ganska mycket i er ände och i er kod och i er applikation som säkerhet och säkerhetsarbete ligger. Rådgör amazon något i det här eller tar ni allt det här ansvaret?

I4: vi använder ju deras tjänster till att kryptera och dekryptera saker. Vi använder deras databaser för att spara känslig information och hämtar från deras databaser på ett smidigt och enkelt sätt, så på så sätt tar vi hjälp av dem. Men när det gäller att hålla sig GDPR-riktiga: om man ska bygga en stor cloud-plattform som ska vara funktionell och samtidigt väldigt säker gäller det att ha ett genomgående tänk genom hela. Att använda tjänster, så klart, det hjälper till viss del, men det är helhetslösningen som gör det säkert, oftast. Sen är det också hur man hanterar... man gör en stor, som vi kör, skyffling av data överallt så att all auktorisering för olika tjänster görs på ett genomtänkt och bra sätt också. Vi kör microservice-tänk där vi har extremt mycket services som pratar med varandra och det är viktigt att bara de som får prata med den de ska få prata med får göra det. Ingen annan får prata med just den eller hämta information just där, det är bara vissa användare som får göra det. Om man minimerar den skara som får hämta saker så minskar man ju säkerhetsrisk och sånt också.

V: har ni någonsin själva blivit utsatta för intrång?

I4: Inte medan jag har jobbat här.

V: kan du tänka dig in i hur ni hade hanterat en sån situation?

I4: Då får man ha en diskussion och både ett sätta att täppa igen och göra framtiden mer säker. Det blir så som jag sa om mortem-möten där man diskuterar varför och hur det kunde bli som det blev, vad hade vi kunna gjort, skulle vi ha gjort någonting, vad kan vi göra i framtiden för att det inte ska hända och om det händer, vad kan vi göra för att ta så lite skada möjligt. Det är det som är viktigast. Man kan inte förutse allt, det är omöjligt. Inget system är 100% säkert och det är bara att jobba så mycket som möjligt för att det inte ska hända och arbeta aktivt för att identifiera vad som skulle kunna vara. Om det finns en minsta risk eller om det finns ett sätt att göra det lite säkrare på och om det inte tar för mycket tid, då kanske det är värt att göra det, även fanns det finns extremt liten risk att det skulle exponeras på något sätt.

V: du pratade tidigare om att det nästan var en konspirationsteori att man blir utsatt för attacker vid delade IT-resurser. Det behöver inte bara vara en attack, det kan vara en hög belastning som gör att det blir driftstörningar. Har ni någonsin blivit direkt eller indirekt utsatta för en DDoS-attack eller driftstörning?

I4: nej, aldrig. Inte sedan jag började i alla fall och inget jag har hört om.

V: Har ni någon kontroll eller testar ni på något sätt för att ni inte utsätts för avvikelser i data, alltså dataförluster? Gör ni några säkerhetskopior eller liknande?

I4: Absolut. Mycket av våra databaser har vi flera versioner av. Sen har vi extremt mycket, både hos amazon och andra, tjänster som övervakar allt i systemet, där vi ser alla transaktioner som händer, alla sorters avvikelser. Sen finns det grundfunktionalitet för hur övervakningsverktyg funkar och det är ju inpluggat, så att säga. Sen är det mycket på eget bevåg, hur mycket man övervakar. Vi måste ju på något sätt aktivt säga att "här vill vi hålla extra koll; om vi har det minsta avvikande beteende häromkring så måste vi larma det", då skickar vi det dit vi behöver det. Sen är ju många leverantörer bra på att upptäcka onormalt beteende. Det är extremt viktigt för deras produkt, om det finns minsta möjlighet att upptäcka avvikelser i deras produkter så hjälper de till med det. Det är delat ansvar på leverantör och en själv att hålla koll på det.

V: Då kan jag tänka mig också att den här övervakningen även går ut över beräkningar och datakapacitet, hur mycket den används på er bekostnad?

I4: Ja, det går också att effektivisera väldigt mycket så att det blir försumbart i princip.

V: Har er tjänst någonsin legat nere, eller molnleverantörens plattform?

I4: det är ju saker som händer hela tiden men downtime är väl också en definition av hur länge det är. Om slutkunder faktiskt påverkas i deras användning av produkten är det då det blir faktiskt crucial. Om man bygger en modern plattform har man fallback:s för det mesta och att ingen data gås miste om. Om någonting går ner så sparas all processering av data. Om det är data som ska processas och den inte lyckas av någon anledning för att någonting ligger nere måste man försöka igen tills det går. Det är så vi bygger mycket av vårt system. Vi ser ju att nu är det massa saker som inte gör vad de ska göra, nu ligger det och väntar ett tag. Det är så man får bygga. De här väntköerna kan ju vara igång en hel dag om det är så, tills man

hittar en lösning på problemet. Det ska mycket till att kunden blir påverkad i slutändan. Den kanske inte ser den mest aktuella datan, men ingen data gås miste om om man bygger på rätt sätt. Och det är viktigt.

V: Sören, har du något du vill tillägg här?

S: Nej.

V: Vi har en öppen fråga om det är något du vill tillägga om information- och datasäkerhet med molnleverantören?

I4: Nej. Det är väl intressant med GDPR, hur olika företag ser på GDPR, både att hämta ut [data]. Vi har börjat med det, det är kunder som har hört av sig att hämta ut [sin] data och det ska alltid vara möjligt och det ska alltid ta två veckor eller vad det är, det finns någon lagstandard på det. Så det är något som jag tror att inte så många företag faktiskt har möjligt att göra. Sen är det att hålla det GDPR-riktigt också. Man stöter på konstant, företag som har missuppfattat eller inte riktigt håller sig.

V: [bakgrund om datakontroll och ansvar]... har ni själva upplevt den problematiken [med vendor lock-in]?

I4: att flytta leverantörer?

V: ja, det kan vara databaser eller hela tjänster

I4: grejen är att det är så extremt hög konkurrens och det är så extremt mycket pengar att tjäna så om det är någonting som utvecklas och blir bättre så är det migrering av data. Om man hör av sig till leverantörer angående om det är svårt att migrera så svarar de att "vi löser allting åt er". Det är långt ifrån perfekt nu, men jag tror att det verkligen är någonting som kommer utvecklas ännu mer. Att ta en vecka eller så att få ett stort företag att byta från en tjänst till en annan ligger så sjukt mycket pengar i så att göra bra tjänster för att migrera data eller migrera tjänster eller kod eller vad som helst från en tjänst till en annan är någonting som alla, om de inte gör det, som de borde satsa på för alla kollar på nya alternativ, att spara pengar eller säkerhet eller som wikileaks eller vad som helst, att de inte litar på sin leverantör till 100%. Det är något vi har märkt, att det känns otroligt smidigt att byta vissa saker i alla fall.

V: Jag försvann där en sekund, Sören har du några följdfrågor på det [intervjuobjektet] sa?

S: Nej

V: Molnleverantören i sig är ju ett eget företag och de har eget vinstintresse och kan ändra policies eller ändra priser när de själva önskar. Har det någonsin skett någon förändring i en molntjänst ni använder som har påverkat er verksamhet?

I4: nej, inte molntjänst skulle jag säga. Vi har ju väldigt många externa parter där vi betalar olika saker, så vi har ju sett saker som har gått upp som vi har behövt strukturera om. Men det är så här, när det gäller IT-utveckling finns det så sjukt mycket konkurrens och vissa är för stora för att bry sig om att de höjer priser på vissa saker och vissa är på väg uppåt och gör allt för att landa nya. Det är mycket vilken position olika företag har. Vi har helt klart stött på att folk har bytt prismodeller för tjänster vi har använt. Det är saker som händer hela tiden och

man får anpassa sig, men det är det som är roligt att jobba med arkitektur också. Det finns aldrig ett rätt och det finns aldrig ett sätt att göra det på - det finns extremt många olika sätt att göra det på och själva kostnaden för saker är inte alltid... det går oftast att göra en snygg och bra lösning som blir ganska billig, men man kanske måste ha lite mer insikt i det och bygga lite grejer själv. Sen kanske det finns någonting där man inte behöver göra någonting alls själv och då betalar man tre gånger så mycket. Så det är alltid en avvägning av hur mycket kompetens man har på företaget och hur mycket tid man kan och vill lägga ner.

V: Skulle du säga att du har förtroende och tillit till er molnleverantör? Litar ni på att de tar ett säkerhetsansvar?

I4: Säkerhetsmässigt har jag nog aldrig riktigt funderat på det. Jag har bara tänkt på att jag hoppas och tror att de gör så bra de kan för att det ska vara säkert. Det är det de säger att de gör och då litar man på att de gör det. Sen är det så klart, om man litar bättre eller ser att det finns bättre alternativ så vill man ju gå över till det och det är sådana saker som vi tittar på hela tiden; om det finns bättre alternativt är det klart vi ska försöka gå över till det. Att bara avvakta och inte orkar göra saker kommer bara skjuta en i foten ju längre fram man går. Om man är det minsta osäker på att man kontraktet eller att man litar på företaget så är det ju mycket bättre att gå till någonting man litar på bättre.

V: Är det någonting som skaver med att inte ha fullständig kontroll över data eller säkerheten eller är det skönt att överlåta den delen?

I4: Det är egentligen bara en kostnadsfråga skulle jag säga. Och en resursfråga. Om alla skulle få välja så skulle man ha ett eget serverrum och ett eget ops-team och allting på plats, men det har man oftast varken pengar eller tid till att sätta upp. Om du har tillräckligt stort system och tillräckligt många anställda så blir det väl i långa loppet billigare att serva allting själv och då tar du över all säkerhet också. Det är drömscenariot. Men om man är 11 personer och bygger en extremt stor plattform så finns det inga resurser för att göra det och då är amazons modell jättedröm på det sättet, och alla andra cloud-lösningar, för det går mycket snabbare och är så extremt mycket billigare än att sätta upp allting själv.

S: Hur ballpark-stor är smärtgränsen för att det ska vara intressant att ens överväga att ha servrar och resurser själv? Handlar det om 100 eller 1000 anställda?

I4: Det borde ligga någonstans där mitt emellan. Och det beror det på hur avancerat system man har. Om man använder många av ens cloud-leverantörs tjänster så blir det någonstans... det är klart det finns open source-projekt för liknande saker och det går att anpassa på ett visst antal olika servrar. Men det är mycket det som behöver sättas upp också. Jag har dålig insikt i exakt hur man sätter upp ett sånt system, mest mjukvarumässigt. Man kan köpa olika sorters servrar och sånt men exakt hur man sätter upp allting så att man kan spegla de resurser man har från en cloud-leverantör vet jag inte exakt hur man gör men jag tänker att många företag gör det, så det finns nog företag som säljer den mjukvaran också, eller att det finns open source-projekt och rekommendationer för hur man gör det.

V: Vilket ansvar tar ni själva för om molnleverantören blir utsatta för ett intrång eller en attack? Vilket ansvar tar ni gentemot era kunder?

I4: Vi har ju våra avtal. Jag kan inte till punkt och pricka vad det står i kundavtalen. Det är mer att vi informerar vilka data vi sparar och vilka som tar del av data. Om något annat än det som står i kontraktet blir vi ansvariga för då är det något vi har gått emot kontraktet som vi

har skrivit med kunden och det gör vi allt för att undvika. Men det är omöjligt att vara 100%:ig. Exakt hur det skulle gå till får man väl dra med en advokat i sådant fall. Vi har avtal med alla kunder om all data som vi sparar. Vi informerar om all data vi sparar och vad vi gör med datan. Sen ska inte vi göra något annat och vi eftersträvar till 100% att inte göra något annat än det som står i avtalet.

V: Sören, har du något du vill tillägga här kring det avsnittet?

S: Ja, jag funderar på, i och med att vi har spekulerat lite om det redan: vi har en artikel i vår referenslista som heter typ "will cloud computing be the death of internal IT", kan du spekulera kring det? Tror du att det kommer bli mindre och mindre intern IT och att det här är det nya sättet att jobba på, eller kommer företag ändå vilja ha sina egna datacenter, eller måste man vara Facebook-stor för att vilja ha det?

I4: Det är väl både och. Man kan se det tvådelat: det har funnits en viss tid och kommer finnas en lång tid framöver och att det kommer bli billigare känns mer troligt än att det kommer bli dyrare. Den här smärtgränsen som vi pratade om förut, när det finns argument för att sätta upp en egen serverhall kommer öka hela tiden, tror jag i alla fall, så länge som det är så populärt som det är nu. Sen är det också att till viss del blir det lättare och lättare att automatisera saker; automatisera kod, generera kod, det är någonting som är på jätteframkant också. Amazon skapar services som är lite mer plug and play-aktigt, många tjänster, vilket gör att man kanske inte kommer behöva lika många utvecklare på ett företag. Sen är det skillnad på operations och server-anställda och faktiska mjukvaruutvecklare men jag tror att båda kommer minska i framtiden och att de stora bolagen kommer få större makt. De är såpass duktiga och har såpass mycket pengar.

V: [avslutar mötet]

3.5 Intervjuobjekt 5

[Bakgrund om cloud computing, kommer fram till hur djupt på tekniska detaljer vi går in på ---]

I5: ... det som är skillnaden är ju egentligen, när det kommer till cloud computing, om man hårdrar ett infosec-perspektiv så är det bara att du har mindre att säga till om och svårare att ställa krav.

[mer bakgrund och introduktion ---]

V: det var lite bakgrund till cloud computing, så jag tänkte börja med att ställa en liten bakgrundsfråga, om du kan beskriva verksamheten du jobbar på, vad du gör och hur stort företaget är och så vidare?

I5: mm.. det kan jag göra. Jag är konsult på [företaget] och [företaget] är ett stort globalt företag men jag har jobbat i både offentlig sektor och privat sektor i både linjeroller och som konsult. Jag har jobbat med informationssäkerhet och även IT-säkerhet när jag var tekniker, jag har en teknisk bakgrund, så jag har jobbat med det i 18-19 år. Det vi gör på [företaget] är att vi hjälper andra företag att granska att de efterlever lagar och regler och hjälpa dem att vidta rätt åtgärder till stora delar, men vi gör även annan konsulting. Men vi som företag är

väl 200 000 anställda tror jag ungefär, globalt, och jag jobbar då på den svenska delen som även omfattar Estland, Lettland och Litauen numera.

V: Vad använder ni för molnlösingar i er utveckling och distribution? Och då när jag säger ni och er så hänvisar jag både till [företaget] och de verksamheter ni har varit hos.

S: och om er verksamhet inte omfattar utveckling så kanske det är: vilka leverantörer eller verktyg jobbar de som ni rådgör och konsultar hos?

I5: Det blir lite lurigt att svara så som ni har ställt frågorna. Det blir konstigt för mig att svara ur ett [företaget]-perspektiv, inte av något annat skäl än att jag inte har haft till jobb att försöka fundera över hur vi gör. Jag vet ju ungefär hur vi gör därför att jag är nyfiken, men jag har lättare att svara för hur det ser ut hos kunder, men då blir istället problemet att våra kunder gör allt det här. En del har egen utveckling i egna lokaler som driftas och förvaltas i egen regi. En del har outsourcade tjänster och en del har hybrider där de köper in antingen infrastruktur eller platform as a service och nästan alla har dessutom SaaS:tjänster till det. Många kör kanske ekonomin som en SaaS:tjänst eller... Salesforce hade ni som exempel, det har säljavdelningen; HR-systemet kanske rullar som en PaaS:tjänst hos en sourcing-partner och de kan ha ett core-system som de säljer och utvecklar på som de lever på, där de använder sin egen knoI5:how och utveklingsmetodik och sitter och utvecklar på kontoret men de använder AWS eller Azure eller någonting som infrastructure as a service för att bygga och leverera detta. Är allt ett bra svar eller blir det bara jobbigt då?

S: Det är ett bra svar tror jag och då kanske det blir, när vi kommer till mer detaljfrågor så kan du göra... i andra fall har det varit att "vi använder aws" och då gör de exempel med awS:grejer, men då kanske du har flera exempel eller får specificera vid exempel, om det är relevant. Det är ett bra svar, för då vi ett hum om vilken sfär vi rör oss i.

V: Jag får försöka ställa lite mer generella frågor utifrån de vi har förberett då. Av erfarenheten du har, har det generellt sett genomförts en analys eller någon slags jämförelse när man väljer olika molnlösningar i förhållande till datasäkerhet?

I5: Det beror ju lite på verksamheten, men generellt sett, när vi är ute och tittar, så har det gjorts för lite sådan. Man har utgått ifrån, både när man väljer leveransmodell eller när man väljer leverantör, så är det väldigt få som har gjort en analys av vad som behövs ur ett säkerhets perspektiv när de väljer vare sig lösning eller något annat utan det är andra skäl som har avgör att man har gått in i molnet. Ett fåtal kunder som har haft en, om man tittar på kanske den vanligaste tjänsten är office365. Där finns väl ett fåtal kunder som har valt att köra office365 för att det finns säkerhetsfeatures som de vill åt eller inte har kompetens att leverera i sin egen miljö. Däremot så är det också så att det är väldigt få som lyckas dra nytta utav de de köper, när det kommer till säkerhetskomponenter. De underskattar i regel det jobb de behöver göra för att få ut den nyttan de eftersträvade när de fattade beslutet. Men de flesta har valt att gå ut i molnet av helt andra skäl än säkerhetsskäl och ibland visar det sig då att det inte var ett helt genomtänkt beslut.

V: skulle du säga att det är de tekniska möjligheterna och tillgängligheten som lockar mer?

I5: ja. Och tillgängligheten är ju en av tre kritiska perspektiv när du jobbar med säkerhet. Det är ju konfidentialitet och riktighet också. Men tillgängligheten och enkelheten, man ser det som att man minskar risk för problem i sina egna datahallar och kanske upprätthålla kompetens hos egna tekniker för att förvalta en plattform när det man egentligen vill åt är

funktionalitet. Så då väljer man att göra det, gå ut i molnet på olika sätt. När det gäller infrastructure as a service så skulle jag säga att de som är duktigast på att verkligen utnyttja den, i alla fall när man inte fokar på säkerhet så är ju det start-ups som inte har en massa gammal legacy. Många har ju gått ut i molnet och haft en stor förhoppning om att allt ska ut i molnet, men även de brukar underskatta den resan och sitter ofta kvar med en hybridmiljö och ganska dyra kostnader. Men det är ju bara kostnader, det kan ju skapa möjligheter åt dem också. Det gör ofta det, när man börjar prata säkerhet.

V: vi har en fråga, för avgränsningens skull, om vilken typ av distributionsmodell som används: om det är public, private eller hybrid. Då menar du att lite större verksamheter som har ett stort legacy och vill ut i molnet, där blir det lätt en hybridlösning, medan nya mer lättfotade verksamheter kanske kan helt gå ut i molnet?

I5: Ja. De börjar där och har inget annat. Företag som utvecklar och levererar olika typer av tjänster idag, som började för mindre än 10 år sedan, de kör i regel allting ute i molnet. Det i sin tur skapar affärsmässiga utmaningar för dem. Det gör ju att det är svårt för visas myndigheter och så vidare att köpa deras tjänster om de inte vill ut i molnet. Men de har valt att gå den vägen. Ganska många i offentlig sektor har tidigt velat använda molnet men står nu och tvekar om de verkligen får.

V: Hur lång erfarenhet har [företaget] och du av att jobba med cloud computing?

I5: [företaget] är jättestort och vi har nog varit med från början och jobbat med cloud computing i olika former, men i Sverige har vi varit ganska sena på. Vi har en egen IT-avdelning som levererar egna saker, men ska jag vara ärlig så tror jag inte heller att vi har gjort vår analys ur ett säkerhetsperspektiv över huvud taget. Vi har nog trott att... kanske har vi valt att hålla kvar länge därför att vi har haft en bild av att det är säkrare eller att vi har mer under kontroll. Men de besluten där vi lyfter ut saker i molnet, de har inte föregåtts av någon säkerhetsmässig analys, utan det är helt andra skäl.

V: har [företaget] några särskilda säkerhetskrav?

S: [diskussion om huruvida frågan är relevant]

[bakgrund om mjukvaruutveckling, SDLC, SecSDLC ---]

V: vi ska se hur vi kan formulera de här [frågorna]. Generellt sett, tar verksamheter del av verktyg eller infotmation från molnleverantören när de gör en kravinsamling för att planera och designa utvecklingsprojekt?

I5: nu vet jag inte om jag förstod frågan, menar de att de skulle använda molnverktyg för att ta fram krav?

V: precis - inför planering och kravinsamling. Jag kan ge ett exempel. I en av våra intervjuer kom det fram att de använder, det finns, kostnadskalkylatorer i AWS för att räkna på hur mycket hårdvara kommer kosta när de kör igång x antal instanser. Sådana typer av verktyg och dokumentation från leverantören om hur de implementerar säkerhetsarbete i vissa funktioner.

I5: okej. Nu vet jag inte. Är frågan hur mycket de egentligen nyttjar möjliga verktyg som skulle kunna underlätta för dem?

V: ja, precis, hos molnleverantören, i förarbetet.

I5: är det innan de väljer att gå ut i molnet? Tänker du att de redan har något att jämföra med, eller är det inför ett start av ett projekt, sådär, att "vad kommer det här kosta oss? oj, titta, det kommer bli dyrare än vi trodde för det kommer vara oerhört mycket transaktioner eller det kommer vara en stor databas" eller något åt det hållet?

V: ja, exakt, det är när de använder en molnleverantör redan och sen inför ett nytt projekt så använder de olika verktyg hos leverantören för att planera projektet. Känner du till att några sådana typer av verktyg används, hos molnleverantören?

I5: jag ska se, jag måste ju se till att det blir ett ärligt svar. Jag känner till att de finns och jag vet att en del använder dem, naturligtvis, men oftast har de ändå redan beslutat sig för... har de väl valt att gå ut i molnet, om vi tittar på de här som inte har något annat, som inte har en hybridlösning, de har ju egentligen inget val längre. De sitter där de sitter. Det kommer aldrig bli ett alternativ för dem, om de ska köra ett projekt, att de helt plötsligt börjar teckna avtal med någon som levererar en datahall och börjar ställa dit fysiska servrar för det har de inte kompetens till. De kommer nog ändra sitt beslut i ett projekt, bara för att de ser att det blir väldigt dyrt utan de sitter är de sitter och tänker att de får ta igen det på något annat sätt. Jag är helt övertygad om att de som är duktiga på molntjänster använder de stöd som finns för att lista ut vad det här kommer kosta innan, det är jag övertygad om. Men det kommer aldrig påverka deras beslut utan det kommer bara ge en hint om kanske vad de behöver ta betalt i slutänden. Det är kanske mer för tjänsteberäkning som det används i så fall, än som ett beslutsunderlag.

V: känner du till om de genomför några kontroller och tester för att upptäcka säkerhetshot i molntjänsten?

I5: det är väldigt, väldigt olika. Det är extremt olika. Det beror på vilka typer av tjänsteleveranser. På SaaS:tjänster gör de det i regel aldrig. Men det var ju inte det vi skulle prata om. En mogen organisation som har höga säkerhetskrav gör ibland [ohörbart]-tester 19:34 på sina lösningar som finns i molnet, men oftast är det man testar det de själva har utvecklat. Det är sällan man angriper och hittar hål i själva tjänsten, för det får man inte i regel. Det brukar inte uppskattas av leverantören, utan de gör egna tester och tredjepartstester och så publicerar de rapporter och säger att "så här sköter vi säkerheten". Sen får du gilla det eller inte gilla det. Du kan ju dra upp en windowS:server i azure eller aws eller något åt det håller och du liksom rattar hela windowS:servern, om vi pratar ren infrastructure-aS:a-service, och då är det ju alltid klokt att testa att du har satt upp den på ett bra sätt. Det är samma risk ute i molnet som om du hade den i din datahall. Det handlar ju om hur den är konfigurerad, inte om hur själva tjänsten.. Där är ju du som kan förstöra... Infrastrukturen och tjänsten i sig den får man nog lov att välja att anse att den är säker nog. Men du kan ju göra override på den genom att öppna en massa hål in till din infrastruktur, det kan du ju göra.

V: Varje molnleverantör erbjuder sin uppsättning av ramverk och språk som stöds på deras plattform. Har du upplevt att det har varit begränsningar där, med val av molnleverantör, i förhållande till kompabilitet mellan språk och ramverk?

I5: Näe, där skulle jag nog säga att man är medveten som kund. Jag menar, antingen går folk all-inn-google, men annars när du tittar på aws och azure så finns det inga sådana begränsningar. Du kan dra upp vilken typ av miljö du vill och köra dem, både de verktyg för

provisionering, om man tittar på infrastruktur, eller de ramverk du vill ha för utveckling eller de programspråk. Det väljer du själv. Det är egentligen inget hinder, eller missförstår jag frågan? Tänker ni på någon speciell, någon PaaS:lösning eller någogot åt det hållet?

S: Jag tycker det är rätt tänkt.

V: Vissa väljer ju att gå efter lite mer oberoende ramverk som kubernetes och så för att undvika att vara inlåst till en viss leverantör. Har du upplevt att kunder resonerar på det sättet?

I5: Ja men okej, då tror jag att jag fattar lite mer. Jag har faktiskt sett flera kunder som väljer att gå den vägen, att göra sig oberoende, för att kunna flytta mellan, om vi tar till exempel, azure och aws. Och det gör de av flera skäl - de gör det lite av konkurrenssjäl, de gör det utav, kanske driftsäkerhetssjäl också, att om den ena är borta så ska det funka på den andra. Det ser jag flera som gör, men de som gör det är de som är duktiga och medvetna. Jag ser nog fler som bara har gått... var de windowS:tunga från början så valde de azure och så började de trycka grejer ut i molnet och så hoppas de att det ska funka. De är nog fler än de som gör det medvetna valet. Men de som lever på att sälja tjänster i slutändan, sådana som, deras business... De använder Infrastructure-aS:a-service för att kunna sälja software as a service till tredje part. Eller PaaS eller SaaS och nästa steg. De brukar vara bättre på att, nu pratar jag om ganska unga företag, de är också bättre på att hela tiden jobba med oberoende, alltså, att försöka vara plattformsoberoende. Men det finns företag som gör även internt, även om de inte alls använder molntjänster. De vill helt enkelt kunna flytta, om deras datahall brinner upp vill de kunna fortsätta köra i molnet. Då flyttar de upp det i molnet. Så det finns ingen direkt koppling till molntjänster, skulle jag säga, där, utan det handlar mer om strategi, vad du har för strategi och hur viktigt det är för dig att alltid kunna vara tillgänglig på något sätt. Och att inte binda in dig till en leverantör. Men jag vet inte om ni hör det själva, ni kanske inte har hunnit vara ute och jobba så mycket, men, det är ju inget roligt att sitta... men det är samma... det har inget med molntjänster att göra det heller, om du tittar på hur man gjorde förr, i sin egen organisation, då kanske man började - man valde IBM-servrar för att de var dyrare men ingen kunde säga att man hade gjort fel och ovanpå det installerade man HP UX och då vart man tvungen att välja... tvungen, men mer eller mindre tvungen kanske att välja Oracle, och sen Java ovanpå det och helt plötsligt sitter du i ett läge där du är beroende utav... dumt exempel kanske med HP UX och IBM-servrar... men att du försätter dig i ett läge där du.. om du ska välja att byta hårdvaruplattform så behöver du göra om hela din applikationsflora. Då sitter du ju fast hos den leverantören.

V: Vi kommer komma in på det lite mer i ett senare avsnitt om amen just den problematiken med vendor lock-in.

I5: Det är ju ett skäl till att jobba med kubernetes och mycket annat, att det ska vara transparent, mobilt, mot andra infrastructure as a service-leverantörer.

V: vi tänkte avsluta det här avsnittet med, har du märkt av att verksamheter har påverkat sina utvecklingsprocesser när de har flyttat till molnet eller när de använder molnet? Jag kan ge ett exempel från en tidigare intervju där de beskrev att de lite har blivit tvugna att automatisera sina 26:52 [uppkoppling bryts]

S: nu tappade vi Viktor lite där tror jag. Eller tappade ni mig?

I5: jag tror att jag hörde honom

S: okej då var det jag som...

V: i en tidigare intervju beskrev e att det är omöjligt att sitta och administrera hundratals servrar och därför har man blivit tvungen att automatisera hela distributionskedjorna. Har du upplevt att utvecklingsprocessen har ändrats i verksamheter från att de har börjat använda molntjänster?

I5: usch, nu vet jag inte vad jag ska svara... Jag bara blir så här, men herregud, vem har ni pratat med? Det låter som att de inte gjorde en analys innan de gick ut i molnet i alla fall... Man kanske har missat det och underskattat den kostnaden för den investeringen för att kunna göra det jobbet i vissa fall men det är ju en förutsättning, men det är samma om du börjar bygga interna molntjänster, om vi nu pratar provisionering av maskiner. Det största problemet du i regel får när du börjar köra internt är att du upptäcker att det går jättefort att spinna upp nya miljöer åt utvecklare och så vidare, och till och med, du kan disponera och låta dem göra det själv och helt plötsligt tar disken slut, så går det inte att spinna upp några fler. Och så har du dålig koll, det kommer till livscykelhantering, då vet du inte längre vilka som är viktiga eller vilka du kan ta bort, du låter det helt enkelt bli vildvuxet. Det problemet är ett av själen till att man löser det genom att flytta ut i molnet. Vad händer då? Går inte disk åt då? Jo, den går åt, men vi får en faktura istället för att vi måste köpa ny disk och installera nya disk-skåp. Men du har fortfarande det här att du får en helt ohanterlig miljö om du inte kan hålla ihop den från en central punkt med provisionering utav nya maskiner och avveckling och patchning och underhåll. Då hamnar du i en vedervärdig vardag. Jag har inte sett så många som inte har... Inga stora, som inte har förstått det, utan de har provisioneringsverktyg för att de måste ha det. Men återigen, det är ingen skillnad på det på molntjänster internt eller externt, så att säga, egentligen. Det är inte kopplat till de leverantörerna. Skulle jag säga, om jag inte missförstår din fråga.

V: jag tror jag menade lite mer, i hur kanske agilt de utvecklar. Den typen av utvecklingsprocess, att de har behövt ställa om deras utvecklingsarbete.

S: det behöver inte vara så att man gör en stor omställning, utan det kan vara, finns det någon förändring överhuvud taget, i utvecklingsprocesses, till följd av att man utvecklar och distribuerar till molnet istället.

I5: Nej, jag skulle egentligen säga att de två inte hänger ihop, eller snarare omvänt, om vi tittar på infrastructrure as a service i alla fall, så är det snarare så att de moderna utvecklingsmetodikerna, där du helt enkelt vill vara snabbare i time to market och så vidare, när du börjar köra mer agila metoder, då kommer du behöva fler miljöer, och då har molnet skapat massa goda förutsättningar för det för det går fort att få upp nya miljöer. Så det här beror nog på om ni pratar med en IT-chef eller en utvecklingschef, på något sätt, hur de upplever det och de kommer nog säga lite olika saker. Men det finns ingenting som säger att "oj, nu har vi flyttat ut den här servern i molnet, nu måste vi börja planera våra utvecklingsprojekt på ett annat sätt". Det finns ingenting sånt. Däremot är det nog många som har gjort det i samma veva, men det är nog egentligen mer en slump att de moderna utvecklingsmetodikerna, typ scrum och kanban och hela det köret har blivit heta samtidigt som molnet har blivit hett. Alltså, att det är två coola grejer att göra. Jag skulle nog säga att det är nog vanligare att om de har varit tidiga på med moderna utvecklingsmetoder så har de insett att "vår interna IT-avdelning kan inte leverera det vi behöver". Snarare så, att de har behövt utveckla IT-infrastrukturen och då valt att gå till molnet för att kunna bli snabbare eftersom det tog för lång tid att styra om den interna IT-verksamheten att leverera IT-

infrastruktur på ett sätt som man behöver för moderna utvecklingsprojekt. Sen om det är bra eller dåligt, det kan vi faktiskt diskutera i ett helt annat möte för att allt det här har ju enorma för- och nackdelar, inte minst ur ett säkerhetsperspektiv.

V: det är jättespännande. Vi ska gå vidare till lite mera utmaningarna

[bakgrund och diskussion om CIA ---]

I5: då måste jag bara ställa en fråga för skojs skull, har ni läst på lite så ni vet vad DIGG och de här säger och vad som gör att det här är jobbigt för myndigheter?

S: vad vem säger om det här?

I5: de heter väl DIGG nu.. nu står det still. De gick ut hårt, och flaggade. De sa en sak som gjorde att myndigheter får jävligt svårt att använda molnet. Det de säger är att information som är klassificerad eller classified, alltså känslig information, då, ska anses vara röjd om du lägger den i en molntjänst.

V: för att det inte är inte är innanför nationella gränser?

I5: nej, inte för att det inte är innanför nationella gränser utan det här kopplar till cloud act och de sakerna. De stora molntjänsterna som finns på marknaden idag, det är ju två amerikanska och sen är det kinesiska Alibaba och alla de har lagstiftning som säger att staten kan begära ut den här informationen utan att de får berätta för dig som kund att de har lämnat ut den. Och i och med att den lagen finns, så länge den lagen finns, så ska du anses att informationen är röjd.

S: myndigheten för digital förvaltning, är det, om den myndigheten eller en annan myndighet skulle spinna upp ett eget moln, som är avsett för offentlig verksamhet i sverige, då kan väl de se till att det följer DIGGs krav på molnet. Det är inte molnet i sig, som gör det, utan det är utbudet av molntjänster som gör att myndigheter inte får jobba i molnet just nu.

I5: ja, precis. Skulle vi utveckla en svensk tjänst, och i Sverige skulle det bli försäkringskassan som fick göra det, som det ser ut just nu, då skulle försäkringskassan bygga ett moln där de hade all disklagring och allting hos sig och de upplevs då som en molntjänst som vilken som helst för myndigheterna. Då skulle de få använda det, i det här fallet. De tjänsterna finns inte idag, men jag vet att försäkringskassan vill det och de har också skrivit lite bra saker ni kan läsa om sen, om ni vill.

V: spännande. Jag tänkte försöka forma de här så det blir lite mer generella frågor. Upplever du att det finns en ökad risk med att obehöriga får tillgång till känslig data i molnet?

I5: ja, kopplat till det jag just sa.

V: Det är att myndigheter [utländska stater] kan komma åt data, för att det står i lagtexterna

I5: ja, egentligen är det, ja, eftersom molnleverantörerna är skyldiga enligt lagar, som de lyder under, att lämna ut information på begäran, till sina statliga organ, utan att du känner till det. Du kan inte välja att säga nej för att du är svensk.

V: finns det några andra obehöriga än myndigheter som det finns en ökad risk mot?

I5: alltså, generellt sett så är det ju... men det är samma, det är ingen skillnad på molntjänster eller outsourcing i allmänhet, heller. Det är ju inte dina anställda som har tillgång till informationen, utan det är någon annans anställda som har tillgång till informationen, så är den klassiska risken: vem är lättast att muta eller angripa? Om du väljer att göra bakgrundskontroller på dina anställda så hjälper det inte så mycket om inte din leverantör gör samma motsvarande bakgrundskontroller på sina anställda. Och det kan du aldrig få microsoft och dem att göra. De gör säkert det, däremot, men du styr inte det. Det är inte du som väljer. Så ja, risken ökar på samma sätt, utöver det första jag sa, kopplat till att du överlåter informationen i händer som du inte styr över.

V: finns det någon strategi för att hantera och motverka det här, förutom det att svenska myndigheter gör: att de helt enkelt inte använder det?

I5: Det finns svenska myndigheter som gör det, det är många myndigheter som kör office 365 och så vidare, de små. De sitter och svettas just nu. Om du ska motverka det här så är egentligen enda sättet... det finns två sätt. Du kan använda molntjänster för data som du har klassificerat so matt det inte gör någonting om det hamnar i deras händer. Då kan man använda molntjänster, men då har du hamnat i läget att du inte kan gå all-in-cloud. Det är därför du kan hamna i hybrid-lösningar. Det var det jag sa tidigare, att ibland är det bra, det skapar möjligheter också, om du har kvar din gamla datahall. Det är det ena du kan göra, men om du nu behöver få ut data så är tyvärr det enda som finns att göra, som jag känner till, är att kryptera all information, det innebär att du även får kryptera databaser och så vidare, med en godkänd, liksom en bra, vedertagen standard, där du äger nycklarna och det bara är du som har tillgång till nycklarna. Jag tror att molnleverantörerna kommer tillslut tillhandahålla sådana här tjänster, men de jag har tittat på hittills, och nu är det något halvår sedan jag har tittat på något sånt i detalj, eller ett år sedan. Där är det ändå så att man kan betala massvis med pengar för att få tillgång till en HSM, men då är det ju leverantören som tillhandahåller HSM:en och så säger de att "jag lovar att inte titta på de här nycklarna utan att fråga dig först", men de har ju fortfarande tillgång till dem. Och skulle då, om vi pratar azure eller amazon, de är ju skyldiga att lämna ut informationen till sina myndigheter och om de kan dekryptera den så är de skyldiga att dekryptera den. Men om du skulle använda till exempel PGP... är ni bevandrade med vanlig kryptostandard?

V: det är en oberoende kryptostandard, eller?

I5: ja, om vi säger så här att förenklar det och säger att om du kan bevisa för dig själv att du äger nycklarna, det vill säga att om du krypterar någonting med PGP till exempel, då har du en publik och en privat nyckel. Om du har både den publika och privata nyckeln och aldrig visar den för molnet, alltså för molnleverantören, eller ger dem möjlighet att använda den, då är det bara du som kan dekryptera informationen. Om du skulle ta kvalificerad eller känslig information på något sätt som du egentligen inte får ha i molnet, men om du först krypterar den och sen lägger upp den i molnet, då skulle den anses inte vara röjd, egentligen. Problemet är att det inte funkar så bra med molntjänster. Det går att göra, men det blir otroligt krångligt, tekniskt, och det slutar i regel med att ja... det är svårt att göra. Det tillhandahålls inte utav leverantörerna på ett sätt som är... För att förenkla det: du måste välja att lita på leverantörerna. Det är likadant om du outsourcar. När du har valt att lita på leverantören och säga "jag litar på dig, oavsett vad som sägs", då får du anse att det är en risk du har valt att ta, att det även hamnar hos FBI eller vad det nu kan vara. Ingen aning. Men till saken hör att den som tror att inte stater sysslar med industrispionage, vilket har varit deras uppdrag de senaste 300 åren, de tar ganska stora risker utan att de vet om det.

V: Har någon verksamhet du har jobbat för blivit utsatt för ett intrång och i sådana fall, hur hanterade den verksamheten det?

I5: Hur ska jag svara på det här då... ja, det har de.

S: jag tänker mig att du har varit med om ganska många situationer, men vi är redan ganska mycket inne på vårt sista avsnitt och vi ska inte hålla dig alltför länge till. Jag funderar på om vi ska gå till sista avsnittet, som handlar mer om datakontroll, vendor lock in, ansvar, som vi redan är inne på ganska mycket och se om det är något vi kan få mer på, eftersom du inte är utvecklare.

V: Jag har några frågor till på det här, som jag skulle vilja ställa.

I5: [diskuterar tid och annat]

V: Gör verksamheter någon kontroll för att upptäcka avvikelser i data? Alltså dataförlust eller datamanipulation?

I5: Ja. Återigen, har ingenting med molntjänster att göra, men mer än det jag sa innan. Det som jag beskrev om en stat skulle begära ut det, det är inte relevant för det kommer du aldrig upptäcka. Det går inte att upptäcka. Eller, det går att dölja så lätta att du kommer inte upptäcka det, om det inte läcker ut från dem sen, vilket har hänt, om de har stulit information. I alla fall, det är väldigt varierande, och jag skulle säga att svenska kunder är lite sämre på att försöka upptäcka saker. På nätsidan är de ganska bra på att upptäcka saker, för det har man gjort länge, kopplat till saker som har utvecklats från antiviruS:tiden eller vad vi ska kalla det. Du börjar sätta upp saker som kan monitorera på näteverksnivå om det verkar ske anamolier eller så.

V: Överlastningsattacker och så där?

I5: ja. Det är nog ganska många ganska bra på av det skälet att antingen så kan de det själva och har byggt det själva och gjort det själva, eller så köper de tjänster som omfattas utav den typen av funktionalitet. Tyvärr är inte de sakerna så värdefulla, för de är lite för lätta att kringgå. Sättet du angriper, oavsett om det är en molntjänst eller inte, så är sättet du angriper en organisation på idag är mer att du angriper en person eller flera personer med phishing, spear phishing(?) eller annat som du kan göra olika saker med och då avgörs allt av hur skyddad deras klient är. För kan jag ta över deras klient, då är de ju, beroende på hur de sen har jobbat med behörigheter och annat och segmentering och så, så är de ganska rökta, för jag kommer till och börja med åt allting som den individen. Och då spelar det ingen roll var du har datan, om det är en molntjänst eller om det är hemma i en källare eller vart det än er. Allting du kommer åt, kommer du åt.

V: jag tänker att det underlättar, med molntjänsterna, att förhindra sån typ av dataförlust, med hjälp av olika automatiska säkerhetskopior och sådana typer av skydd.

I5: okej men nu frågar du om dataförlust som att data bara råkade bli förstörd och gå bort. Du tänkte inte dataförlust som i att data har hamnat i andras händer.

V: nej, precis

I5: backup, restore, alltså disaster recovery och ur det perspektivet att ha data, där är molntjänsterna i regel mycket bättre därför att du får så mycket mer backup utan att du har bett om det, i och med att du tar snappshots och så vidare. När det kommer till det så är problemet oftast att om du har speciella krav så kan du inte införa dem utan du får det leverantören ger. Så du kan fortfarande, om du har data som du behöver spara väldigt, väldigt länge, som du kan upptäcka väldigt sent att den har blivit förstörd eller något åt det hållet, då behöver du ändå ha separat backup-hantering i form utav backup-lösningar som du tankar ner data till och sparar utanför produktionsmiljön. Så det kommer du behöva sådana lösningar till i alla fall. Det här med snapshots och det, det gör att man är snabbare igång, men det är oftast tekniska lösningar. Det är väldigt sällan; du kan ju upptäcka att data du ska arkivera på olika sätt eller ha tillgång till i kanske 10 år - bokföringslagen eller någonting annat - det finns ju inga garantier att det finns kvar bara för att du använder en molntjänst, utan du får ju vad du betalar för på något sätt.

V: med public cloud delar man ju IT-resurser med andra, till exempel, amazonanvändare och då finns det en risk för att man kan utsättas för driftstörningar eller överbelastningsattacker, indirekt. Har du upplevt den problematiken någonting i verksamheter du har jobbat på?

I5: Inte så att den har uttalats på det sättet, utan det är snarare så att det som händer är att de har en incident och sen så inser man att den incidenten är en följdverkan av något som har hänt hos någon annan. Det händer, det du säger, men det händer mindre i molnet, för de är faktiskt bättre på det än de är i outsourcade miljöer och så vidare.

V: webbhotell och så vidare?

I5: ja, fast det vet jag inte om det är, det kanske det kan vara. Jag tänker mer om du anlitar CGI och har deras datahall. De är liksom sämst... nu ska jag inte hänga ut någon leverantör, det spelar ingen roll vilken det är. Men molntjänstleverantörerna är ganska bra på att hålla isär de här miljöerna och skydda dina miljöer, men framförallt så kan du köpa olika nivåer för det mesta. När det här har hänt visar det sig oftast att det hade kunnat undvikas om du hade betalat mer, men det är då du upptäcker också att molntjänster kan vara bättre för dig, men det blir inte billigare.

[diskussion om avsnittet och att få vidare]

[bakgrund om datakontroll och vendor lock-in ---]

V: ... skulle du säga att det är en problematik för verksamheterna du är ute hos, att vara portabla?

I5: Det här är egentligen två frågor, skulle jag säga, igen, därför att om vi tittar på just wikileakS:problemet att någon annan bestämmer att det du har ska stängas ner, det problemet är ett potentiellt jätteproblem, men nu börjar vi prata kris och kanske krig och annat, så är ju det ett jätteproblem då, att skulle vi hamna i krig med USA, då har de all information och de kan sabba vår tillgänglighet till informationen. I övrigt är det fråga mer om vad du själv sysslar med. Ur perspektivet att det är en risk, att det finns en risk att någon inte vill att jag ska finnas kvar längre och kan styra min leverantör, ja, den risken finns alltid. Men det är väldigt få verksamheter som har just det problemet. Där är ju wikilieaks, där amerikanska staten tycker att de kan styra amerikanska leverantörer, de väljer att göra det, wikileaks hade valt att ligga i molnet. Tråkigt! Sen tror jag ju att just wikileaks inte var dummare än att de faktiskt hade backuper för rätt mycket av den där datan fick faktiskt kvar, så de hade ju på

andra ställen också. De använder ju lite hängslen och livrem. Ja, det här är ett potentiellt problem, du behöver ha med det här i din riskanalys, att det är inte du som bestämmer längre om informationen ska få finnas där. Men där får du göra en riskbaserad bedömning. Jag skulle inte säga att det är ett jätteproblem. Det är ett större problem för offentlig sektor än vad det är för privata sektorn som kan fatta sina egna beslut. Men sen sa du någonting mer...

I5: just det, för det jag menar är att just det här problemet med wikileaks: vilka molntjänster har du att välja på idag? Det hade inte gjort någon skillnad om de låg på både Azure eller AWS. Lyckas de styra den ena så blir det prejudicerande och då styr de den andra också och då plockar de bort båda två. Då får wikileaks välja att använda kinesisk, typ använda alibaba, det skulle kunnat vara smart utav dem, och ha backup på alibaba för de kan ge sig sjutton på att om kineserna väljer att ta ner någonting så kommer amerikanerna älska att göra reklam för det och tvärt om. Så det är ett sätt att fortfarande kunna lösa det, förutsatt att du vill ha informationen på en kinesisk molntjänst vilket jag tror inte att wikileaks skulle vilja, för då skulle de definitivt bli dömda för spioneri och annat. Men okej, vendor lock-in är mer, för de flesta av mina kunder, ett ekonomiskt problem, alltså en ekonomisk risk. Om mina tjänster bara funkar på azure och de väljer att höja priserna så är jag rökt - jag har inte kvar min datahall, jag kan inte flytta det här hur jag än gör. Och det är därför man jobbar med kubernetes och sådana grejer, för att kunna säga hela tiden till azure att om ni höjer priserna så flyttar jag till amazon och vice versa. Det är ett ekonomiskt problem, tycker jag, för de flesta kunder. Det handlar om datakontroll på något sätt, men den ekonomiska sidan handlar inte om datakontroll och datakontroll handlar om att du har kvar ansvaret men du kan inte längre styra den när du är i en molntjänst. Däremot så behöver inte det hindra dig utan det är en risk du kan välja att ta beroende på vilken typ av verksamhet och vilken information du har. Risken att det USA skulle välja att stänga ner CDON för att det inte ska konkurrera med Amazon, den finns nästan inte så länge det är fred på jorden. Det skulle de inte kunna göra. Och där kan man väl tycka att det skulle vara en större risk att köra allting i sina egna datahallar, för det skulle kunna vara problem för dem.

V: du var inne det lite, på att azure kan höja priserna. Molnleverantörerna är ju ett eget företag med ett eget vinstintresse och de kan ändra policies och priser hur de önskar. Har du någonsin märkt av att det skett förändringar i molntjänster som har påverkat en verksamhet?

I5: Jag är helt övertygad om att det har skett men det har inte jag följt. Det största problemet som jag har sett, kopplat till avtal och förändringar i förutsättningar som du inte längre styr, det gäller naturligtvis privacy, där jag skulle säga att det är under utveckling. Använder du några google-tjänster, och det gör ni ju, så ser du att du får uppdateringar hela tiden och väldigt mycket av det rör privacy. Tyvärr så handlar det mer om omformuleringar. Vi kan ta exemplet, nu kör vi ju Zoom. Vet ni vad Wire är? Wire är en väldigt bra tjänst som konkurrerar med Zoom, ungefär som signal, för säkra chattmeddelanden och du kan även ringa säkert och sådana saker. Det är helt open source, det är skitbra på alla sätt. Sverige skulle kunna leverera en svensk tjänst om du vill, men det säljs också som en tjänst på internet och det är den som är mest spridd. Den tjänsten har nu köpts upp av ett amerikanskt bolag för att användas av amerikanska staten och helt plötsligt så flyr ju alla europeiska kunder som är säkerhetsmedvetna från den tjänsten för "nu kan vi absolut inte använda det här med". Det blir konsekvensen av det, därför de har teknisk förmåga att kunna lyssna av det här videosamtalet eller någonting annat och det är ju tråkigt. De har ändrat i sin privacy-policy också, förut stod det, när det var levererat från europa, att vi kommer inte lämna in information till någon myndighet. Och så kommer det ut en liten liten uppdatering långt ner där det står att vi kan komma att lämna ut det här på begäran utav legala myndigheter eller

myndigheter som har rätta att göra det. De måste uppdatera det för att följa sin nya lagstiftning och så gör de den uppdateringen och helt plötsligt är det helt värdelöst ur ett privacy-perspektiv, att kunna lita på den här. Så nu flyr alla en bra tjänst och så väljer de att använda teams eller något annat och så gör de samma sak och hamnar i samma läge. Men det är en annan fråga...

V: jag skulle vilja gå in och prata lite om förtroende och tillit. Skulle du generellt säga att verksamheter är så skeptiska som du beskriver i det exemplet eller har de ett förtroende och en tillit till sin molnleverantör, att det tar ett säkerhetsansvar liksom?

I5: Alla kunder som jag träffar har ett osunt högt förtroende till sina leverantörer ur ett informaitonssäkerhet- och privacy-perspektiv. De vill inte höra att de inte kan lita riktigt på sina molntjänster. De vill inte det. Så de har nästan ett medvetet osunt förhållande till de risker de tar, tycker jag.

V: är det för att det skulle bli så krångligt, om det inte funkar?

I5: det går inte att gå tillbaka längre! De har redan sagt upp sina datahallar och allt sitt eget. Du har ju massor med företag som faktiskt livnär sig på, som tjänar vansinnigt mycket pengar idag, små företag, men som tjänar massor med pengar, men man pratar inte ens om dem, som är superduktiga, som har liksom sjukt vassa idéer och lösningar och kod som är hela deras existens. Det är det ena, och de kör i molntjänster - de kör sin utveckling där, de kör sin kod där. Allting är liksom tillgängligt för någon som skulle vilja stjäla det. Jag tycker inte att de är tillräckligt riskmedvetna, men om de säger att de känner till risken och säger att de har valt att ta risken, fine. Då är det deras val. Men framförallt kanske ur ett privacy-perspektiv. Jag tar ett exempel: den lilla ekonomibyrån, som är 15 personer, de kör allt i molnet, de har ingen information direkt som är värd att stjäla - de är inget mål. De har inte tillräckligt med personuppgifter och alltihop men sen har de ju kunder och så förvaltar de alla sina kunders information. Helt plötsligt kan de sitta på information som är reglerad enligt lag därför att deras kunder är börsnoterade och deras bokslut och deras siffror där kan vara kursdrivande information. Då behöver de ju skydda den informationen på samma sätt som kunden skulle ha skyddat den om de körde det själva och det gör de inte. Då kan man fråga sig, vem har gjort del. Då är det egentligen kunden som har fel för kunden har ju lämnat över ansvaret till ett företag helt utan att styra hur de får göra. Så det är kunden som fortfarande är ansvarig. Ur ett privacy-perspektiv är det solklart, att om den här organisationen, om de sköter löner åt det här bolaget, så har de massvis med känsliga personuppgifter om Erikssons anställda. Eriksson skulle inte anställa Nisses ekonomibyrå... men bara för att ta ett exempel. Så det är Eriksson som samlar in uppgifter om sina anställda och de är alltså personuppgiftsansvariga. Sen tycker de ut det här till en leverantör som behandlar uppgifterna så att de ska få ut sin lön, som i sin tur trycker ut det här till en molntjänst där de har sitt system, där de processar all data, de är alltså data processor. Eriksson i det fallet är ju skyldig att säkerställa att data processorn längst bak efterlever deras förväntningar på vad du får och inte får göra med de här personuppgifterna. Det blir väldigt svårt. Frågan var egentligen om de har högt förtroende - ja, de har extremt högt förtroende för sina leverantörer. Det är av helt olika skäl. Ibland väljer de att blunda för att de inte kan och ibland har de inte tänkt och ibland så, i ett fåtal fall, har de ett högt förtroende därför att de har gjort research och bedömt att risken för att det här ska hända är något vi kan leva med. Men de flesta har ett högre förtroende än vad leverantören faktiskt förtjänar, om vi säger så.

V: Det finns vissa säkerhetsaspekter som kan överlappa mellan verksamheter och molnleverantören. Känner du att verksamheter tar ett ansvar för det överlappande säkerhetsaspekterna?

I5: Tänker du då lite governance? Eller vad tänker du?

V: Delvis det, men också kanske hur man säkrar upp sin egen applikation och sin egna tjänst kanske litar lite blint på att det ska funka hos molnleverantören och inte ta fullt ansvar för sin egna säkerhet i sina applikationer.

V: Ja, det är nog vanligt att man brister där. Det skiljer sig ganska mycket globalt, utav det jag har sett. I USA är man bättre på att ställa krav men man är sämre på att se till att det faktiskt är bra. I Sverige kan man oftast ha gjort lite tekniska granskningar och tycka att det är ganska bra rent tekniskt, men man är dålig på att ställa krav och följa upp det. I Sverige litar vi betydligt mer på våra leverantörer i allmänhet och verksamheten, när du säger verksamheten, bara föra att vara tydlig, då skiljer jag mellan core business för ett företag och sen kan ju de ha en IT-avdelning som ibland är en beställarorganisation eller pytteliten eller en utvecklingsorganisation, men de är IT-avdelningen i det fallet är inte verksamheten utan verksamheten kanske är de som säljer försäkringar eller har en bank eller något åt det hållet. De flesta av mina kunder skulle jag säga har för lite inblandning från verksamhetssidan - verksamheten tar för lite ansvar för säkerheten och informationssäkerheten. Mindre ansvar än de behöver.

[sista öppna frågan, inget svar, intervjun avslutas ---]

Referenser

Aldossary, S. & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions, *International Journal of Advanced Computer Science and Applications,* vol. 7, no. 4, pp. 485-498

Alibaba Cloud. (2020a). Alibaba Cloud Products & Services, Tillgänglig online: https://www.alibabacloud.com/product [Hämtad 9 april 2020]

Alibaba Cloud. (2020b). Alibaba Cloud International Website Privacy Policy, Tillgänglig online: https://www.alibabacloud.com/help/faq-detail/42425.htm [Hämtad 13 maj 2020]

Alvehus, J. (2013). Skriva uppsats med kvalitativ metod: en handbok

Amazon Web Services. (2020a). AWS Service Catalog, Tillgängllig online: https://aws.amazon.com/servicecatalog/?aws-service-catalog.sort-by=item.additionalFields.createdDate&aws-service-catalog.sort-order=desc [Hämtad 9 april 2020]

Amazon Web Services. (2020b). Privacy Notice, Tillgänglig online: https://aws.amazon.com/privacy/ [Hämtad 13 maj 2020]

Andress, J. (2011). The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice, Waltham, MA: Syngress Media

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM,* vol. 53, no.4, pp. 50-58

Barzey, N. (2019). Myndigheters användning av molntjänster – överväganden gällande dataskydd och sekretess, Advokaten, Tillgänglig online: https://www.advokaten.se/Tidningsnummer/2019/nr-3-2019-argang-85/myndigheters-anvandning-av-molntjanster-overvaganden-gallande-dataskydd-och-sekretess/ [Hämtad 13 maj 2020]

Battleson, D. A., West, B. C., Kim, J., Ramesh, B. & Robinson, P. S. (2016). Achieving dynamic capabilities with cloud computing: An empirical investigation, *European Journal of Information Systems*, vol. 25, no. 3, pp. 209-230

Benbasat, I. & Zmud, R. W. (1999). Empirical research in information systems: the practice of relevance, *MIS quarterly*, vol. 23, no. 1, pp. 3-16

Benlian, A., Kettinger, W. J., Sunyaev, A., Winkler, T. J. & Guest Editors. (2018). The transformative value of cloud computing: a decoupling, platformization, and recombination theoretical framework, *Journal of management information systems*, vol. 35, no. 3, pp. 719-739

Beslic, A., Bendraou, R., Sopenal, J. & Rigolet, J. Y. (2013). Towards a solution avoiding Vendor Lock-in to enable Migration Between Cloud Platforms, *MDHPCL@ MoDELS*, pp. 5-14

Boehm, B. W. (1988). A spiral model of software development and enhancement, *Computer*, vol. 21, no. 5, pp. 61-72

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks, *Infoworld, 2008*, pp. 1-3

Bryman, A. (2013). Samhällsvetenskapliga Metoder (2002), Malmö: Liber AB, vol. 2, no. 4

Bryman, A. & Bell, E. (2011). Business research methods, 3rd ed, Oxford: Oxford University Press

Chen, Y., Paxson, V. & Katz, R. H. (2010). What's new about cloud computing security?. *University of California, Berkeley Report No. UCB/EECS-2010-5, 20(2010)*, 2010-5

Chieu, T. C., Mohindra, A., Karve, A. A. & Segal, A. (2009). Dynamic scaling of web applications in a virtualized cloud computing environment, *International Conference on e-Business Engineering*, pp. 281-286

Choudhary, V. & Vithayathil, J. (2013). The impact of cloud computing: Should the IT department be organized as a cost center or a profit center?, *Journal of Management Information Systems*, vol. 30, no. 2, pp. 67-100

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control, *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 85-90

Davidovic, V., Ilijevic, D., Luk, V. & Pogarcic, I. (2014). Private Cloud Computing and Delegation of Control, *Annals of DAAAM & Proceedings*, vol. 25, no. 1, pp. 196-205

Ekengren, A. M. & Hinnfors, J. (2006). Uppsatshandbok: hur du lyckas med din uppsats, Lund: Studentlitteratur

Eriksson, L. T. & Wiedersheim-Paul, F. (2008). Rapportboken: hur man skriver uppsatser, artiklar och examensarbeten, Malmö: Liber

Foster, I. & Gannon, D. B. (2017). Cloud Computing for Science and Engineering, *MIT Press*

Gannon, D., Barga, R. & Sundaresan, N. (2017). Cloud-native applications, *Cloud Computing*, vol. 4, no. 5, pp. 16-21

Géczy, P., Izumi, N. & Hasida, K. (2012). Cloudsourcing: managing cloud adoption, *Global Journal of Business Research*, vol. 6, no. 2, pp. 57-70

Google Cloud. (2020a). Google Cloud Solutions, Tillgänglig online: https://cloud.google.com [Hämtad 9 april 2020]

Google Cloud. (2020b). Government requests for cloud customer data, Tillgänglig online: https://cloud.google.com/security/transparency/govt-requests [Hämtad 13 maj 2020]

Guha, R. & Al-Dabass, D. (2010). Impact of web 2.0 and cloud computing platform on software engineering. *2010 International Symposium on Electronic System Design*, pp. 213-218

Harris, S. (2002). CISSP All-in-one Certification Exam Guide, New York: McGraw-Hill/Osborne

IBM Cloud. (2020). Catalog - IBM cloud, Tillgänglig online: https://cloud.ibm.com [Hämtad 9 april 2020]

Iyer, B. & Henderson, J. C. (2010). Preparing for the future: Understanding the seven capabilities cloud computing, *MIS Quarterly Executive*, vol. 9, no. 2, pp. 117-131

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

Jadeja, Y. & Modi, K. (2012). Cloud computing-concepts, architecture and challenges, *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pp. 877-880

Julisch, K. & Hall, M. (2010). Security and control in the cloud, *Information Security Journal: A Global Perspective*, vol. 19, no. 6, pp. 299-309

Khari, M. & Kumar, P. (2016). Embedding security in software development life cycle (sdlc), *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 2182-2186

Kolsjö, M. (2019). Molntjänster flyttar makt över svenska myndigheter till USA, ST-Bloggen, Tillgänglig online: https://stbloggen.se/molntjanster-flyttar-makt-over-svenska-myndigheter-till-usa/ [Hämtad 14 maj 2020]

Krancher, O., Luther, P. & Jost, M. (2018). Key affordances of platform-as-a-service: Self-organization and continuous feedback, *Journal of Management Information Systems*, vol. 35, no. 3, pp. 776-812

Kratzke, N. & Quint, P. C. (2017). Understanding cloud-native applications after 10 years of cloud computing-a systematic mapping study, *Journal of Systems and Software*, vol. 126, pp. 1-16

Kulkarni, M. A. & Gulvani, S. S. (2016). Software Development Life Cycle for Developing Cloud Based Software Suit, *The International Journal Research Publication's*, vol. 06, no. 02, pp. 31-35

Kumar, S. & Goudar, R. H. (2012). Cloud computing-research issues, challenges, architecture, platforms and applications: a survey, *International Journal of Future Computer and Communication*, vol. 1, no. 4, pp. 356-360

Lawton, G. (2008). Developing software online with platform-as-a-service technology, *Computer*, vol. 41, no. 6, pp. 13-15

Liu, S., Chan, F. T., Yang, J. & Niu, B. (2018). Understanding the effect of cloud computing on organizational agility: An empirical examination, *International Journal of Information Management*, vol. 43, pp. 98-111

Loch, K. D., Carr, H. H. & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding, *Mis Quarterly*, vol. 16, no. 2, pp. 73-186

MacAskill, E. (2010). WikiLeaks Website Pulled by Amazon After US Political Pressure, The Guardian, 2 december, Tillgänglig online: http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon [20 April 2020]

Malmqvist, M. (2019). Myndigheterna fast i molnlimbo. Hur ska de nu ta sig vidare?, Computer Sweden, 7 mars, Tillgänglig online: https://computersweden.idg.se/2.2683/1.715718/myndigheter-moln-ta-sig-vidare [Hämtad 15 maj 2020]

MarketWatch. (2019). Cloud Infrastructure Services Market: Industry Outlook, Size & Forecast 2018-2025, 26 september, Tillgänglig online: https://www.marketwatch.com/press-release/cloud-infrastructure-services-market-industry-outlook-size-forecast-2018-2025-2019-09-26 [Hämtad 9 april 2020]

McAfee, A. (2012). What every CEO needs to know about the cloud, *Harvard business review*, vol. 89, no. 11, pp. 124-132

Meiyan, W. (2013). Analysis to the Weaknesses and Safety in Cloud Computing, *2013 Third International Conference on Intelligent System Design and Engineering Applications*, pp. 358-361

Mell, P. & Grance, T. (2011). The NIST definition of cloud computing.

Microsoft Azure. (2020a). Azure-produkter, Tillgänglig online: https://azure.microsoft.com/sv-se/services/ [Hämtad 9 april 2020]

Microsoft Azure. (2020b). What are public, private, and hybrid clouds? Understanding your options, Tillgänglig online: https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/ [Hämtad 14 april 2020]

Microsoft Azure. (2020c). Law Enforcement Requests Report, Tillgänglig online: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report [Hämtad 13 maj 2020]

Munk, D. (2019). Cloud-Based Vs. On-Premise Servers, 22 mars, Tillgänglig online: https://www.forbes.com/sites/forbestechcouncil/2019/03/22/cloud-based-vs-on-premise-servers/#699989ca79e2 [Hämtad 3 april 2020]

Oates, B. J. (2006). Researching information systems and computing, London: SAGE.

Orakwue, E. (2010). Private clouds: secure managed services, *Information Security Journal: A Global Perspective*, vol. 19 no. 6, pp. 295-298

Patrizio, A. (2018). What is cloud-native? The modern way to develop software, InfoWorld, 14 juni, Tillgänglig online: https://www.infoworld.com/article/3281046/what-is-cloud-native-the-modern-way-to-develop-software.html [Hämtad 4 maj 2020]

Popović, K. & Hocenski, Ž. (2010). Cloud computing security issues and challenges, *The 33rd international convention MIPRO*, pp. 344-349

Pressman, R. S. (2005). Software engineering: a practitioner's approach, 6th ed., New York: Palgrave macmillan

ProductPlan. (u.å.). What is the Software Development Lifecycle?, Tillgänglig online: https://www.productplan.com/software-development-lifecycle/ [Hämtad 27 april 2020]

Ragunath, P. K., Velmourougan, S., Davachelvan, P., Kayalvizhi, S. & Ravimohan, R. (2010). Evolving a new model (SDLC Model-2010) for software development life cycle (SDLC), *International Journal of Computer Science and Network Security*, vol. 10, no. 1, pp. 112-119

Rienecker, L. & Stray Jörgensen, P. (2014). Att skriva en bra uppsats. 4th ed., Malmö: Liber

Rittinghouse, J. W. & Ransome, J. F. (2016). Cloud computing: implementation, management, and security, Boca Raton: CRC Press

Rizwan, S. & Zubair, M. (2019). Basic Security Challenges in Cloud Computing, *2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, pp. 1-4

Ruparelia, N. B. (2010). Software development lifecycle models, *ACM SIGSOFT Software Engineering Notes*, vol. 35, no. 3, pp. 8-13

Ryen, A. (2004). Kvalitativ intervju: från vetenskapsteori till fältstudier, 1st ed., Malmö: Liber ekonomi

Samonas, S. & Coss, D. (2014). The Cia Strikes Back: Redefining Confidentiality, Integrity And Availability In Security, *Journal Of Information System Security*, vol. 10, no. 3, pp. 21-45

Shivpuriya, V. (2017). Security in a cloud-native environment, InfoWorld, 26 juni, Tillgänglig online: https://www.infoworld.com/article/3203265/security-in-a-cloud-native-environment.html [Hämtad 6 april 2020]

Schneider, S. & Sunyaev, A. (2016). Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing, *Journal of Information Technology*, vol. 31, no. 1, pp. 1-31

Soghoian, C. (2010). Caught in the cloud: Privacy, encryption, and government back doors in the web 2.0 era, *J. on Telecomm. & High Tech. L.*, vol. 8, pp. 359

Sternstein, A. (2011). Service interrupted: WikiLeaks fiasco reinforces push to set security standards for cloud services, *Government Executive*, vol. 43, no. 2, pp. 13-14.

Synergy Research Group. (2020). Incremental Growth in Cloud Spending Hits a New High while Amazon and Microsoft Maintain a Clear Lead, 4 februari, Tillgänglig online: https://www.srgresearch.com/articles/incremental-growth-cloud-spending-hits-new-high-while-amazon-and-microsoft-maintain-clear-lead-reno-nv-february-4-2020 [Hämtat 9 april 2020]

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G. & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability, *Journal of Computational Science*, vol. 36, 100581

Valacich, J. S. & George, J. F. (2017). Modern systems analysis and design, Boston: Pearson

Venters, W. & Whitley, E. A. (2012). A critical review of cloud computing: researching desires and realities, *Journal of Information Technology*, vol. 27, no. 3, pp. 179-197

Vithayathil, J. (2018). Will cloud computing make the Information Technology (IT) department obsolete?, *Information Systems Journal*, vol. 28, no. 4, pp. 634-649

Walraven, S., Truyen, E. & Joosen, W. (2014). Comparing PaaS offerings in light of SaaS development, *Computing*, vol. 96, no. 8, pp. 669-724

Wang, L., Tao, J., Kunze, M., Castellanos, A. C., Kramer, D. & Karl, W. (2008). Scientific cloud computing: Early definition and experience, *2008 10th ieee international conference on high performance computing and communications*, pp. 825-830

Ward, J. M. & Griffiths, P. M. (1996). Strategic planning for information systems, New York: John Wiley & Sons, Inc.

Whitman, M. E. & Mattord, H. J. (2011). Principles of information security, 4th ed., Boston: Cengage Learning

Wikipedia. (2020). Software Development Process, Tillgänglig online: https://en.wikipedia.org/wiki/Software_development_process [Hämtad 27 april 2020]

Zhang, Q., Cheng, L. & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges, *Journal of internet services and applications*, vol. 1, no. 1, pp. 7-18

Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues, *Future Generation computer systems*, vol. 28, no. 3, pp. 583-592

Zoom (2020). Zoom Meetings & Chat, Tillgänglig online: https://zoom.us/meetings [Hämtad 13 maj 2020]