

**Pilvipalvelujen
hyödyntämismahdollisuudet
vakuutusyhtiössä**

Cloud Services in Insurance Company

Kandidaatintyö

TIIVISTELMÄ

Tekijä: Pyry Peura

Työn nimi: Pilvipalvelujen hyödyntämismahdollisuudet vakuutusyhtiössä

Vuosi: 2019

Paikka: Lappeenranta

Kandidaatintyö. LUT-yliopisto, tuotantotalous.

34 sivua, 5 kuvaa ja 1 liite

Tarkastaja(t): Lasse Metso

Hakusanat: Pilvipalvelut, Vakuutusyhtiö

Keywords: Cloud services, Insurance

Tutkimus on toteutettu pohjoismaisen vakuutusyhtiön toimeksiannosta. Työn tavoitteena on havainnollistaa pilvipalvelujen hyödyntämisen etuja ja haasteita sekä vakuutusyhtiön erityispiirteitä pilvipalvelujen hyödyntämisessä.

Kirjallisuuden avulla käydään läpi yleisiä pilvipalvelun etuja ja riskejä ja vakuutusyhtiöiden erityispiirteitä vakuutusyhtiössä. Vakuutusyhtiön erityispiirteistä pilvipalvelujen käytöstä erityisen huomion kohteena on sensitiivinen data, jota vakuutusyhtiöiden sovellukset sisältävät huomattavasti enemmän kuin monien muiden alojen yhtiöiden sovellukset. Lisäksi vakuutusyhtiöiden erityispiirteitä on tutkittu myös haastattelututkimuksen ja case-tapauksen avulla.

Pilvipalvelujen avulla voidaan ratkaista monenlaisia liiketoiminnan ongelmia, mutta ratkaisujen hyödyt riippuvat usein yrityksen kyvystä implementoida ne nykyisiin järjestelmiinsä. Pilvipalvelujen edut korostuvat runsaasti laskentatehoa vaativissa ympäristöissä, jolloin pilvipalvelujen hyödyntäminen muodostuu huomattavan paljon tehokkaammaksi kuin oman laskentakapasiteetin ylläpitäminen.

SISÄLLYSLUETTELO

1	Johdanto	3
1.1	Tausta ja tutkimusongelma	3
1.2	Työn tavoitteet, rajaukset ja rakenne	4
2	Pilvipalvelut	5
2.1	Edut	8
2.2	Haasteet	10
2.3	Sensitiivinen data pilvipalvelussa	12
2.4	Tietoturva pilvipalveluissa	13
2.5	Pilvipalvelujen tarjoajat	14
3	Pilvipalvelujen käyttöönotto	17
3.1	Uudet sovellukset pilviympäristössä	18
3.2	Vanhat sovellukset pilviympäristössä	19
4	Pilvipalvelut vakuutusyhtiössä	23
5	Case: katre	25
6	Johtopäätökset	28
	Lähteet	30
	Liite	

KÄSITE- JA LYHENNELUETTELO

IaaS – Infrastructure as a Service, infrastruktuuri palveluna

IT – Informaatio teknologia

PaaS – Platform as a Service, alusta palveluna

SaaS – Software as a Service, sovellus palveluna

1 JOHDANTO

Pilvipalvelut ovat olleet jo vuosia yritysten tiedossa ja monessa yrityksessä myös käytössä. Niiden hyödyntäminen yleistyy jatkuvasti ja pilvipalvelut mahdollistavat monille yrityksille resurssien hyödyntämisen aikaisempaa tehokkaammin. Yrityksen siirtyessä itse hallinnoiduista servereistä pilvipalvelujen hyödyntämiseen yritykselle vapautuu paljon resursseja kalliista serverien hallinnasta muihin asioihin, joissa resursseja voidaan hyödyntää tukemaan paremmin yrityksen ydinosaa. Yrityksen siirtyessä pilvipalveluihin ulkopuolisen serverienhallinta palvelun hyödyntämisestä syntyy yrityksellä taas uusi vastuu pilvipalvelun hallinnasta, jota aikaisemmin on vastannut ulkopuolisen palveluntarjoajan serverinhallintapalvelut. (Heino, 2010)

Pilvipalvelut tarjoavat kuitenkin monia muitakin sovelluksia, kuin servereitä ja virtuaalikoneita, mitkä voivat mahdollistaa yritykselle uusien ratkaisujen hyödyntämisen liiketoiminnassaan. Pilvipalvelut tarjoavat esimerkiksi valmiita konenäkö- ja koneoppimissovelluksia. Yritys voi hyödyntää liiketoiminnassaan näitä sovelluksia, vaikka yrityksen omat resurssit eivät riittäisi konenäkö tai koneoppimis sovellusten tuottamiseen. Näin ollen siirtyminen servereiden ja virtuaalikoneiden tehokkaamman käytön vuoksi voi samalla avata uusia mahdollisuuksia, joita yrityksellä ei aikaisemmin ole ollut käytössään. (Heino, 2010)

1.1 Tausta ja tutkimusongelma

Työ on toteutettu toimeksiantona pohjoismaiselle vakuutusyhtiölle, joka toimii yritysasiakkaiden ja yksityisasiakkaiden parissa. Työlle syntyi tarve, kun yrityksessä siirrytään jatkuvasti kasvavalla tahdilla pilvipalvelujen hyödyntämiseen. Pilvipalveluista tärkeimmät palvelut yhtiölle ovat erilaiset virtuaalikoneet ja serverit, joilla voidaan hallita yhtiön käyttämiä verkkosovelluksia. Tämän työn tutkimuskysymykset ovat:

1. Mitä hyötyjä ja haasteita pilvipalvelujen hyödyntämisestä syntyy?
2. Mitkä ovat vakuutusyhtiön erityispiirteet pilvipalvelujen hyödyntämisessä?

Työssä tehdään myös havaintoja pilvipalveluun toteutettavan kansallisen tulorekisterin (Katre) hyödyntämiseen tarkoitetun sovelluksen kehityksestä ja toteutuksesta.

1.2 Työn tavoitteet, rajaukset ja rakenne

Työ jakaantuu kahteen osaan: kirjallisuuskatsaukseen ja Katren toteutusta tutkivaan osaan. Kirjallisuuskatsauksessa tutkitaan yleisesti pilvipalveluja, pilvipalvelujen toimittajia ja pilvipalvelujen etuja ja riskejä. Käyttöönottoon liittyvässä osiossa käydään läpi uusien ja vanhojen sovellusten käyttöönottoa pilviympäristössä. Vakuutusyhtiöitä koskevassa kappaleessa kerrotaan pilvipalvelujen käytön erityispiirteistä vakuutusyhtiöissä.

Tutkimusmenetelmät ovat kirjallisuuskatsaus ja haastattelututkimus. Kirjallisuuskatsauksessa on keskitytty pilvipalveluilta eri näkökulmista käsittelevään kirjallisuuteen. Haastattelut toteutettiin puolistrukturoituna haastatteluna, jossa kysymykset olivat valmiiksi määriteltyjä, mutta vastauksia ei oltu sidottu vastausvaihtoehtoihin (Hirsjärvi & Hurme 2015).

Työn tavoitteena on, että lukija ymmärtää paremmin pilvipalvelujen toimintaa ja vakuutusyhtiöiden erityispiirteitä pilvipalvelujen hyödyntämisessä. Työssä pilvipalveluita tutkitaan lähinnä strategisten ja liiketoiminnan kannalta oleellisten asioiden kannalta ja tekninen toteutus on työssä sivuutettu siltä osin kuin se työn tavoitteiden kannalta on mahdollista. Palvelun tarjoajista on keskitytty pääosin kahteen suurimpaan Azureen ja Amazon Web Serviceen (AWS). Suurin mielenkiinto palvelun tarjoajista kohdistuu kuitenkin työssä Azureen, koska Azure on Tutkimuksen toimeksiantajayrityksen organisaation valitsema pilvipalvelujen tarjoaja, jonka ratkaisuja hyödynnetään yrityksen hyödyntäessä pilvipalveluita.

Työn kannalta tärkeää on pilvipalvelujen tietoturva näkökulma. Vakuutusyhtiöiden tietojärjestelmissä on paljon sensitiivistä dataa, jonka tietosuojan takaaminen on tärkeää pilvipalveluihin siirryttäessä.

2 PILVIPALVELUT

Pilvipalvelut termillä on erilaisia määritelmiä. Tietyt analyytikot ja palveluntarjoajat määrittelevät pilvipalvelut kapeasti tarkoittamaan ainoastaan virtuaalisten servereiden tarjoamista internetin välityksellä. Toisten mukaan pilvipalvelut tarkoittavat kaikkea mitä tehdään palomuurin ulkopuolella sisältäen tavanomaisen tietotekniikka infrastruktuurin ulkoistamisen. (Knorr & Gruman 2008) Yhdysvaltalaisen The National Institute of Standards and Technologyn mukaan pilvipalvelu on malli, jossa mahdollistetaan kaikkialla saatavissa oleva tarvittaessa käytettävä pääsy jaettuun joukkoon määriteltäviä laskentaresursseja, jotka ovat nopeasti käyttöönotettavissa pienellä vaivalla ja palveluntarjoajan kanssa toimimisen kanssa. (Mell & Grance 2011) Heinon (2010) mukaan pilvipalvelut ovat toimintamalli, jonka avulla voidaan luopua fyysisistä konesaleista.

Tärkeimmät pilvipalvelujen palvelumallit ovat Software as a Service (SaaS), Platform as a Service (PaaS) ja Infrastructure as a Service (IaaS) (Mell & Grance 2011). SaaS mallissa sovellus on tarjoajan datakeskuksessa ja asiakkaalla on täysi hallinta sovelluksen käytössä, mutta tarjoajalle jää täysi vastuu sovelluksen ylläpidosta, kehityksestä ja servereistä vapauttaen asiakkaan näistä asioista (Waters 2005). IaaS mallissa tarjotaan asiakkaalle infrastruktuuria esimerkiksi virtuaalikoneiden muodossa. Usein pilvipalvelut liittyvät web-sovelluksiin, mutta IaaS mahdollistaa suuren määrän erilaisia sovelluksia, kuten median koodauksesta ja dekodeuksesta sovellusten etänä tehtävän toimituksen ja datan louhintaan. PaaS mallissa asiakkaan ei tarvitse ladata sovelluksia ja palveluita vaan ne ovat käytettävissä internetin välityksellä. PaaS ja IaaS palveluiden välillä on vaikea tehdä selkeää rajausta, koska yhtiöt jotka tarjoavat IaaS palveluita tarjoavat usein myös PaaS palveluita. (Velte, Velte & Elsenpeter 2009) Kuvassa 1 näkyvät eri palvelumallien osiot, joista asiakas vastaa ja mistä osiosta toimittaja vastaa. Kuvan 1 mukaisesti omien palvelinten mallissa yritys vastaa täysin omasta ympäristöstään ja vastaavasti SaaS mallissa yrityksellä ei ole enää ollenkaan hallintaa sovellukseen tai sen ympäristöön vaan toimii ainoastaan sovelluksen käyttäjänä.



Kuva 1 Pilvipalvelu mallit (mukaillen Mell & Grance 2011)

Hinnoittelun määrittelystä on muodostumassa pilvipalvelujen tarjoajille kriittinen tekijä, koska markkinoille on tullut useampia palveluntarjoajia. Hinnoittelumallit voidaan jakaa kiinteän hinnan ja dynaamisen hinnan malleihin. Kiinteän hinnoittelun mallissa voi olla tilausmaksu tai käyttömukainen hinnoittelu. Käyttömukaisessa hinnoittelussa asiakas maksaa ainoastaan käyttämistään palveluista useimmiten käyttöajan ja käytetyn palvelun perusteella. Dynaamisessa hinnoittelussa palveluiden hinnat muuttuvat kysynnän ja tarjonnan perusteella. Esimerkiksi Amazon Web Services on esitellyt Amazon Spot Instances palvelun, jossa asiakkaat voivat tarjota haluamaansa hintaa käyttämättömästä kapasiteetista. Hinnat pysyvät tarjousten mukaisina niin kauan, kun tarjoukset ovat korkeammat kuin Amazonin määrittämä alaraja. Dynaamisella hinnoittelulla voidaan saavuttaa taloudellisesti kannattavampi resurssien allokointi ja matalammat hinnat arvokkaille palveluille. Kiinteän hinnan malli on asiakkaalle selkeämpi, vaikka käytön mukaan maksettava malli voi olla vaikea hyväksyä asiakkaille, jotka haluavat pitää tiukan kontrollin budjetistaan. (Chun & Choi 2013)

Pilvipalveluja on mahdollista tuottaa muutamalla eri tavalla ja nämä pilvityypit ovat yksityinen pilvi (private cloud), julkinen pilvi (public cloud), hybridipilvi (hybrid cloud) ja yhteisöpilvi

(community cloud). (Mell & Grance 2011) Pilvityypeillä on erilaisia vaatimuksia ja ne sopivat erilaisiin tilanteisiin. Seuraavaksi käydään läpi eri pilvityypit.

Yksityinen pilvi

Yksityinen pilvi on yrityksen luoma pilvipalvelu, johon ulkopuolisilla ei ole pääsyä. Yksityinen pilvi on LAN-lähiverkon tai muun järjestetyn luotetun verkon kautta käytettävä pilvipalvelukoneisto. Yrityksen Informaatio teknologia (IT) infrastruktuuri tarpeen ollessa tarpeeksi suuri kannattaa sen harkita yksityisen pilven perustamista. Yksityisessä pilvessä yrityksen sovellukset voisivat jakaa samoja infrastruktuuri resursseja. Näin infrastruktuurille on mahdollista saavuttaa suurempi käyttöäestä. Tarpeeksi suuressa yrityksessä yksityinen pilvi voi toimia julkisen pilven tavalla, joskin pienemmässä mittakaavassa. Nykyisistä pilvipalveluista esimerkiksi AWS on ollut aluksi yksityinen pilvi, josta Amazon on alkanut myymän ylimääräistä kapasiteettia julkisesti, jolloin yksityinen pilvi on muuttunut julkiseksi pilveksi (Rosenber & Mateos 2011)

Julkinen pilvi

Julkinen pilvi on internetyhteyden kautta käytettävä pilvipalvelu, joka on julkisessa käytössä. Usein julkisessa pilvipalvelussa asiakas saa kapasiteettia jaetusta ympäristöstä ilman asiakkaalle itselleen osoitettua laitteistoa tai kapasiteettia, mutta se ei ole julkisen pilven edellytys, eikä sitä rajaava seikka. Julkisessa pilvessä palvelun tarjoaja vastaa pilvipalvelukoneistossa olevien laitteiden ylläpidosta ja omistamisen kustannuksista, jolloin asiakas vapautuu näistä asioista hyödyntäessään julkista pilveä. (Heino 2008)

Yhteisöpilvi

Yhteisöpilvi on useamman järjestön tai yrityksen yhdessä käyttämä pilvipalvelu, joka ei ole kuitenkaan julkisessa käytössä. Yhteisöpilveä voivat käyttää esimerkiksi yritykset, joilla on jotain yhteistä, kuten toiminta, turvallisuusvaatimukset tai muuta vastaavaa. (Mell & Grace 2011)

Hybridipilvi

Hybridipilvessä infrastruktuuri muodostuu kahden tai useamman pilvityypin (yksityinen, julkinen tai yhteisö) yhdistelmästä, jossa pilvet pysyvät erillisenä, mutta niiden välille on rakennettu teknologia, jonka avulla dataa ja sovelluksia voidaan siirtää niiden välillä. (Mell & Grance 2011) Yleinen hybridipilvipalvelun hyödyntämisen tapa on yksityisen pilven ja julkisen pilven yhdistelmä. Hybridipilvessä julkisella pilvellä voidaan tasata suurissa kuormituksissa tulevia kapasiteetin riittävyys ongelmia. (Heino 2010)

2.1 Edut

Pilvipalvelujen hyödyntäminen luo yritykselle monenlaisia etuja kuten tehokkaamman toimintaympäristön, kustannussäästöt, tehokkaamman toiminnan mahdollistamisen ja tarpeiden mukaan ostamisen. Tässä luvussa tutkitaan pilvipalvelujen hyödyntämisen etuja.

Pilvipalveluun siirtyminen on paradigman muutos, jota seuraa siirtyminen omista omistetuista IT-infrastruktuurista asiakas servereille. Yksityiskohtat pilvipalvelussa on yksinkertaistettu, eikä asiakkaan tarvitse omata asiantuntemusta teknologia infrastruktuurista. IaaS palvelussa monet asiakkaat näkevät suurimpana hyötynä hinnoittelun joustavuuden, koska asiakkaan tarvitsee maksaa vain resursseista, joita toimitettava sovellus tarvitsee. IaaS on erittäin joustava malli ja paras valinta sovellusten siirtämiseen pilvipalveluun, kun ei ole aikaa uudelleen työstää sovelluksen koodia pilviympäristöä varten. (Bhardwaj et al. 2010)

Pilvipalvelu voidaan nähdä edullisena. Microsoft Azuren perustason A2 Linux serveri, jossa on 1 GB:n keskusmuisti ja 32 GB paikallista levykapasiteettia kustantaa 7,43 euroa kuukaudessa ilman sitoumusta käytön pituudesta. Instanssilla tarkoitetaan tässä kohtaa laskentayksikköä, jota voidaan käyttää virtuaalikoneena. Tämän instanssin yritys voi ottaa käyttöönsä välittömästi tarpeensa mukaan ja luopua siitä, kun sen tarve loppuu. Jos instanssi on käytössä kokonaisen vuoden yhtäjaksoisesti, niin sen kustannukseksi syntyy 89,16 euroa. Omaan palvelimeen verrattuna käytön mukaan maksaminen on erittäin suuri. Jos oma palvelin on hankittu ja asennettu, ei siitä pääse eroon, vaikka palvelinta ei enää tarvittaisikaan ja palvelimesta syntyy

kustannuksia ainakin poistojen muodossa elinkaarensa loppuun asti. Pilvipalvelusta hankittu palvelin pystytään lopettamaan välittömästi, kun tarve sen käytölle päättyy ja kustannukset myös päättyvät tähän hetkeen. Jos sama Azuren serveri sitouduttaisiin ottamaan kolmeksi vuodeksi tippuisi kuukausihinta 2,83 euroon ja vuosihinnaksi muodostuisi 33,96 euroa, mutta tällöin menetettäisiin mahdollisuus instanssin sulkemiseen kolmen vuoden ajanjakson aikana. Kolmen vuoden sitoumuksella kolme vuotta instanssin käyttöä kustantaa kuitenkin vain muutaman euron enemmän kuin vuosi käyttöä ilman sitoutumista, joten jos palvelimen tarvitseva sovellus tiedetään pitkäikäiseksi, on sitoutuminen pidemmäksi ajaksi kustannusten kannalta järkevää. (Azure 2019a)

Pilvipalvelut tarjoavat monia houkuttelevia säästöjä liittyen IT-kustannuksiin kuten alhaisemmat implementointi- ja ylläpitokulut, pienemmät raudanhankinta ja ylläpitokulut, sähkön kulutuksesta maksun poistumisen, säilytystilan vapautuminen, kun resurssit siirtyvät palveluntarjoajan tiloihin, pienemmät operointikulut ja maksaminen vain käytetyistä resursseista. Pilvipalvelu mahdollistaa IT-organisaatioiden korkeamman kilpailukyvyyn tarjoamalla joustavia ja ketteriä IT-alustoja, skaalautuvia ja korkeatehoisia resursseja ja erittäin luotettavia ja helposti saatavilla olevia sovelluksia ja dataa. Pilvipalvelun avulla IT-osastot säästävät myös sovelluskehityksessä, turvallisuus ja ylläpitoajassa ja kustannuksissa hyötyen samalla mittakaavaedusta. (Carrol et al. 2011)

Pilvipalvelut muuttavat myös IT-investointien kustannusrakennetta verrattuna perinteiseen omien palvelinten omistamiseen. Omien palvelinten strategialla IT-investoinnit ovat olleet vahvasti etupainotteisia, kun suurimmat kustannukset ovat syntyneet palvelinten hankinnasta niiden elinkaaren alkuosassa. Pilvipalvelut taas jakavat investointeja tasaisemmin niiden käytön koko elinajalle. (Lin et al. 2009)

2.2 Haasteet

Pilvipalvelujen hyötyjen lisäksi niiden käyttöönotto ja käyttäminen sisältävät haasteita, joita tulee ottaa huomioon pilvipalveluita käyttävässä yrityksessä. Tässä luvussa käsitellään pilvipalveluiden hyödyntämisen haasteita.

Heiser & Nicolett (2008) määrittelevät seitsemän pilvipalveluihin liittyvää merkittävintä riskiä jotka ovat etuoikeutettu käyttöoikeus, valvontaan liittyvät riskit, datan sijaintiin liittyvät riskit, datan eristämiseen liittyvät riskit, saatavuuteen liittyvät riskit, palautumiseen liittyvät riskit, tutkinnan tukeen liittyvät riskit ja pitkäaikaiseen toimintakelpoisuuteen liittyvät riskit. Heiser & Nicolett (2008) mukaan käytännöllisin tapa arvioida pilvipalvelun käyttämiseen liittyviä riskejä on antaa se kolmannen osapuolen tehtäväksi. Suuressa yrityksessä kolmas osapuoli voidaan korvata erillisellä osastolla, joka arvioi eri sovellusten riskejä pilvipalvelujen käytössä.

Kun yrityksen sensitiivistä dataa pääsevät käsittelemään yrityksen ulkopuoliset ihmiset, yrityksen johtajien mahdollisuudet datan turvallisuuden käsittelyyn vähenevät. Mikä tahansa ulkopuolelta hankittu IT-palvelu ohittaa kaikki fyysiset, loogiset ja henkilökontrolliin pohjautuvat turvakeinot, joita IT normaalisti tarjoaa talon sisäisille sovelluksille. (Heiser & Nicolett 2008) Pilvipalveluita hyödynnettäessä luottamus palveluntarjoajaan onkin erittäin tärkeää.

Valvonta ja auditointi on ollut aina IT-osastoilla tärkeää ja pilvipalveluiden hyödyntäminen vaatii erityisesti ulkopuolisten palveluntarjoajien auditoinnin suorittamista entistä tarkemmin. Valvonnassa muita tärkeitä valvottavia asioita ovat sisäinen valvonta ja lainmäärittämät valvonnat. (Mather et al. 2009)

Pilvipalvelun ostava yritys ei aina tiedä datansa sijaintia. Jos datan sijainti on yrityksen kannalta tärkeää, tulee datan sijainti varmistaa pilvipalveluntarjoajalta sopimuksella. Palvelujen tarjoajilta tulee varmistaa, että he sitoutuvat säilyttämään ja prosessoivat dataa tietyn lainsäädännön mukaan ja tekevätkö he sopimuksia paikallisen lainsäädännön noudattamisesta asiakas yrityksen puolesta. (Kandukuri et al. 2009)

Pilvipalveluiden rakenteen vuoksi monien asiakkaiden data voi sijaita fyysisesti samassa paikassa. Tässä ympäristössä on mahdollisuus siihen, että asiakkaan dataan tunkeutuu toisen asiakkaan dataa, jos palveluntarjoaja ei ole huolehtinut datojen eristämisestä. Tunkeutuminen voidaan suorittaa hyökkäämällä tietoturva aukkoihin tai injektoimalla haitallista koodia SaaS-sovellukseen. Asiakas voi kirjoittaa peitettyä haittakoodia ja injektoida sen SaaS-sovellukseen, jos sovellus suorittaa koodin ilman verifiointia on suuri riski tunkeutumisesta toisen asiakkaan dataan. Pilvipalvelun tarjoajan pitää varmistaa selkeät rajat asiakkaiden datoissa niin fyysisellä puolella, kuin myös sovellus puolella. (Subashini & Kavitha 2011)

Luotettavuus on yksi pilvipalvelumallien tärkeimmistä eduista. Kuitenkaan kovin monet pilvipalvelujen tarjoajat eivät tarjoa palvelutasosopimuksia, jotka ovat tyypillisesti tärkeitä liiketoimintaprosesseissa. Saatavuuden luottamisen lisäksi on tärkeää tietää, miten pilvipalvelujen tarjoaja varautuu palautumaan totaalisen vahingon sattuessa. Mikä tahansa tarjoaja, jolla ei ole replikoitua dataa ja sovellus infrastruktuuria useassa sijainnissa on haavoittuvainen totaaliselle vahingolle. Totaalisessa vahingossa kaikki data ja sovellus infrastruktuuri häviävät. Pilvipalvelun tarjoajalta on tärkeää varmistaa replikoinnin olemassaolo ja onko tarjoajalla mahdollisuus täydelliseen palauttamiseen ja kuinka kauan se vahingon sattuessa kestää. (Heiser & Nicolett 2008) Pilvipalveluiden jatkuvuudesta on tehty tutkimusta, mutta dataa tämän tutkimiseen ei ole vielä kovinkaan paljon (Johnson & Qu 2012). Asiakkaalle on kuitenkin tärkeää kyky luottaa pilvipalvelun jatkuvuuteen ja valittujen ratkaisujen saatavuuteen tulevaisuudessakin. Asiakkaan on kannattamatonta sijoittaa resurssejaan liiketoimintansa rakentamiseen epävarmuuden alla oleviin ratkaisuihin, jos asiakas ei kykene luottamaan pilvipalvelun jatkuvuuteen.

Sisäiset tutkinnat sopimattomasta tai laittomasta toiminnasta ovat haastavia ja kalliita, jopa silloin kun tämä on tapahtunut yrityksen itse hallinnoimassa infrastruktuurissa. Pilvipalveluissa tällainen tutkinta on erityisen haastavaa, koska tapahtumakirjaukset ja data voivat sijaita useilla asiakkailla samassa sijainnissa ja näiden sijainti voi myös vaihdella eri datakeskuksissa. (Heiser & Nicolett 2008)

Park et al. (2015) mukaan turvallisuuteen liittyvät riskit ovat merkittävimmät esteet, jotka hidastavat pilvipalveluihin siirtymistä, mutta suurin osa pilvipalveluihin liittyvistä tutkimuksista ovat käsitelleet pilvipalveluita trendinä tai niiden teknologista kehittämistä, joten ei ole olemassa paljon tutkimuksia negatiivista vaikutuksista ja turvallisuusriskeistä. Kiinalaiset käyttäjät pitävät pilvipalveluissa informaatiovuotojen ja sääntöjen mukaisuuden riskit vaikuttavat negatiivisesti pilvipalvelujen käyttöönottohalukkuuteen. Korealaisilla internetin käyttäjillä on suuri usko tietoturvalle ja pienempi pelko informaatiovuodoista pilvipalveluiden käytössä. Korealaisten pilvipalvelujen käyttöönottoon pelko tietoturva riskeistä vaikuttaa huomattavasti vähemmän kuin kiinalaisilla (Park et al 2015).

Pilvipalveluihin on tehty onnistuneita hyökkäyksiä ja riskiä niistä pilvipalveluiden käyttäjä ei voi sulkea pois. Dropbox jakamispalveluun onnistuttiin pääsemään sisään linkkien jakoon jäänestä tietoturva aukosta ja hyökkääjät myös jakoivat saamiaan tietoja eteenpäin. Amazon Web Services on kaatunut hetkellisesti useamman kerran ja Code Spaces, joka on arvostettu lähdekoodin tallennus repositorio, joka on rakennettu Amazon Web Servicen fasiliteeteillä onnistuttiin tuhoamaan kokonaan lunnaita vaatineella hyökkäyksellä. (Neumann 2014)

2.3 Sensitiivinen data pilvipalvelussa

Sensitiivistä dataa on rodun tai etnisen alkuperän, poliittisen mielipiteen, uskonnollisten tai filosofisten uskomusten paljastava data, ammattiliiton jäsenyys, data biometrinen data, jolla ihminen voidaan tunnistaa, terveyteen liittyvä data ja data, joka liittyy henkilön seksuaaliseen suuntautumiseen. Sensitiivisen datan käsittelyä koskee tiukemmat säännöt ja yritys saa käyttää niitä ainoastaan, jos ne ovat välttämättömiä liiketoiminnan kannalta. Data ei saa myöskään poistua EU alueelta. (EU asetus 2016/679) Vakuutusyhtiössä sensitiivistä dataa on erityisesti terveyteen liittyvää dataa, joka on henkilövakuutuksien käsittelyä varten välttämätöntä ja dataa ammattiliittojen jäsenyydestä, jotka voivat vaikuttaa vakuutusten hintoihin erilaisten alennusten kautta.

Pilvipalveluita käytettäessä sensitiivistä dataa sisältävät sovellukset vaativat huomattavasti suurempaa tietoturva huomiointia kuin sovellukset, jotka eivät sisällä sensitiivistä dataa. Helpomman tietoturvan hallinnan vuoksi isot toimijat sijoittavat 100% datastaan yhdelle

pilvipalvelun tarjoajalle. Suurilla pilvipalvelun tarjoajilla on olemassa infrastruktuurit hyökkäysten estämiseen ja niistä selviytymiseen, joten data on luultavasti pilvipalvelun tarjoajalla paremmin suojeltua kuin omilla palvelimilla ollessa, mutta pilvipalvelujen luonteen vuoksi ne asettavat suuremman houkutuksen hyökkääjille ja data onkin suuremman hyökkäys vaaran alla pilvipalvelussa kuin itse hallinnoitussa konesalissa. (Kaufmman 2009)

2.4 Tietoturva pilvipalveluissa

Pilvipalveluilla on erilaisia arkkitehtuureja riippuen siitä, millaisia palveluja palvelu tarjoaa. Dataa prosessoidaan pilvipalvelun tarjoajan konesaleissa, jossain muualla kuin asiakkaan omissa konesaleissa, joten asiakkaan tulee luottaa tarjoajaan tietoturvassa niin kuin se luottaa tarjoajaan myös palveluiden saatavuudessa. Palvelutaso sopimus on ainut asiakkaan ja palveluntarjoajan suhdetta määrittävä asia, joten luottamuksen saavuttamiseksi palvelutasosopimusten täytyy olla standardisoituja ja tarjota asiakkaalle riittävä selvitys tietoturvaan liittyvistä asioista, jotta asiakkaalla on mahdollisuus luottaa pilvipalvelun tarjoajaan tietoturvan osalta. (Kandukuri et al. 2009)

Sovellusten tietoturva

Sovellusten tietoturvaan vaikuttavat suoraan tunnistaminen, oikeuksien valvonta, seuranta ja seurattavuus. Tunnistamisella tarkoitetaan, että varmistetaan, että sovelluksen käyttäjä on se, kuka kertoo olevansa. Tunnistaminen voidaan suorittaa esimerkiksi SAML tunnistamisella, joka tarkistaa active directoryn avulla, kuka käyttäjä on kirjautuneena tietokoneelle sisään (Lewis & Lewis 2009). Oikeuksien valvonnalla tarkoitetaan, että sovellukset tarkistavat onko käyttäjällä oikeuksia käyttää tietokone resurssia ja tietoa, jota yrittää käyttää. Kun käyttäjä on tunnistettu määrittävät oikeus tasot voiko käyttäjä käyttää resurssia. (Krutz & Vines 2010)

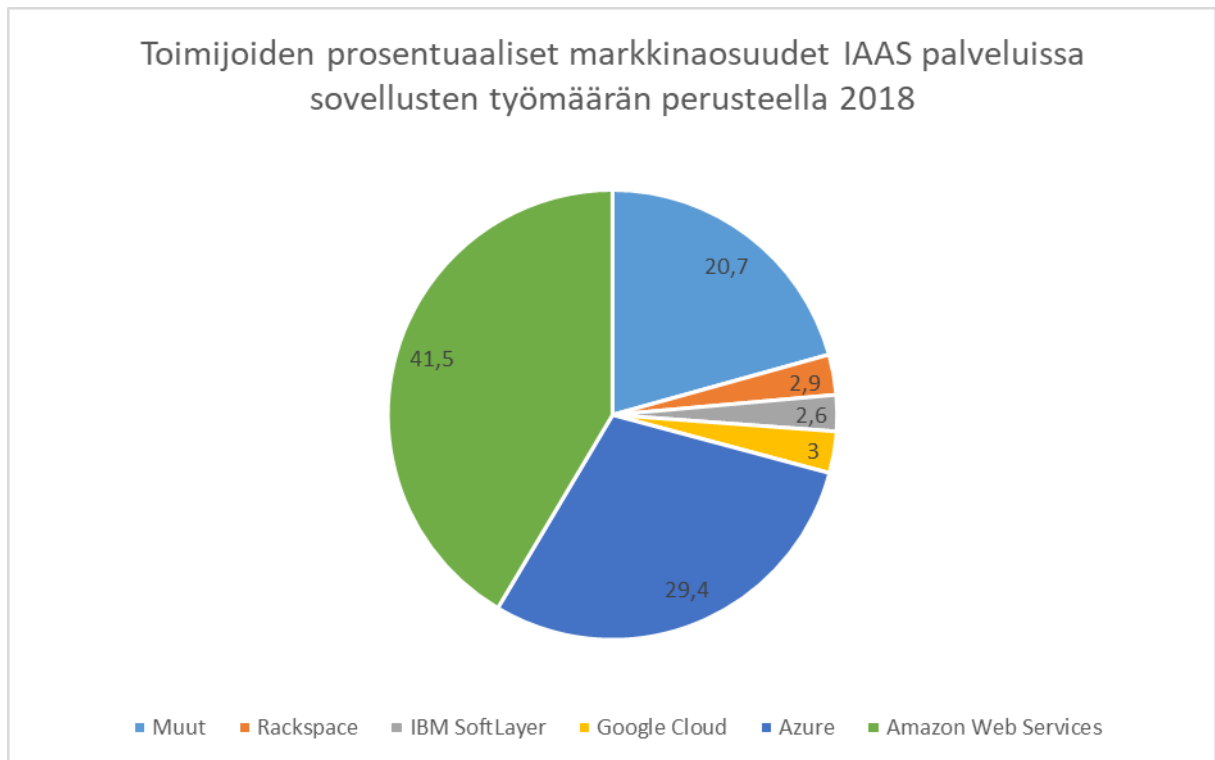
Varmuuden säilyttämiseksi organisaatiot käyttävät sovelluksissa usein kahta valvonta tapaa: jaksoittaista auditointia ja jatkuvaa monitorointia. Näitä valvonnan tapoja voidaan käyttää yhdessä tai erikseen. Seuranta on monilta osin laissa määritetty, etenkin sensitiivisen dataan liittyvissä sovelluksissa. Valvonnan suurimpana tarkoituksena on valvoa, että organisaation toiminta ja johtaminen seuraavat asetettuja ohjeita ja ulkopuolelta tulleita määräyksiä.

Valvonnan ensimmäinen seurannan osa on valvonnan suunnittelu. Suunnittelu vaiheessa päätetään, miten valvontaa varten tarvittava informaatio kerätään, mitkä ovat valvottavat IT prosessit, miten sisäistä valvontaa suoritetaan ja potentiaaliset riskit tulee miettiä jo ennen valvonnan aloittamista. Valvonnan toinen vaihe on kontrollien testaaminen. Tutkitaan valittujen prosessien sisäisiä kontrollointeja ja toimintaa. Kolmas vaihe on laaja testaus, jossa tutkitaan niin IT osastojen, kuin sovellusten käyttäjien toimintaa. Näiden lisäksi tarkistetaan myös IT operaatioiden finanssi puoli ja valvotaan, että IT operaatioiden kustannukset jakautuvat oikein ja niille annettujen ohjeiden mukaan. Valvonta on tärkeässä osassa tietoturva pilvipalveluiden käytössä, koska sen avulla voidaan havaita väärinkäytöksiä ja osia prosesseissa, joissa tietoturvavuotojen riski on suurimpia. Valvonnan avulla järjestelmän heikot kohdat voidaan paikantaa ja löydetty ongelma kohdat voidaan paikata. (Chou 2015)

Seurattavuudella tarkoitetaan, että pilvipalvelun käyttö on jäljitettävissä. Jokaisen yksittäisen käyttäjän haut ja sovellusten käyttö tulee olla analysoitavissa. Seuranta on erittäin tärkeää sensitiivisen datan kohdalla, koska dataa koskevalla henkilöllä on oikeus saada tietoonsa, ketkä hänen tietojansa ovat tutkineet ja yrityksen tulee kyetä tämä tieto henkilölle tarjoamaan. Myös väärinkäytös tilanteissa yhtiölle on tärkeää, että väärinkäytöksiä toteuttaneet henkilöt pystytään tunnistamaan. (Krutz & Vines 2010)

2.5 Pilvipalvelujen tarjoajat

Pilvipalvelujen palvelujen tarjoajista Amazon Web Servicesillä ja Microsoftin Azure palvelulla on hallussaan noin 60 prosenttia pilvipalveluissa mitattuna IaaS-palveluiden työmäärällä vuonna 2018 kuvan 2 mukaisesti. Tässä luvussa tutustutaan Amazon Web Serviceen, Microsoftin Azureen.



Kuva 2 Pilvipalvelun tarjoajien markkinaosuudet 2018 (Coles, 2018)

Azure

Microsoftin Azure pilvipalvelu on marraskuussa 2008 aloitettu skaalautuva pilvipalvelu. Azure pyrkii mahdollisimman suureen johdonmukaisuuteen ja Calder et al. (2011) mukaan Azure tarjoaa kolme asiaa, jotka ovat CAP teorian mukaan vaikea saavuttaa samaan aikaan: suuri johdonmukaisuus, suuri saatavuus ja paloittelun sietäminen. Azurella on panostettu myös vikatilanteista palautumiseen ja asiakkaiden data replikoidaan aina useisiin datakeskuksiin useiden satojen kilometrien päähän toisistaan. Kuvan 2 mukaisesti Azurella on hallussaan noin 21 % markkinaosuus pilvipalveluista. Azurella on palveluissaan laajasti ISO- ja CSA-sertifikaatteja, jotka mahdollistavat asiakkaille ISO-standardien mukaisten pilvipalvelu sovellusten rakentamisen (Rison 2017).

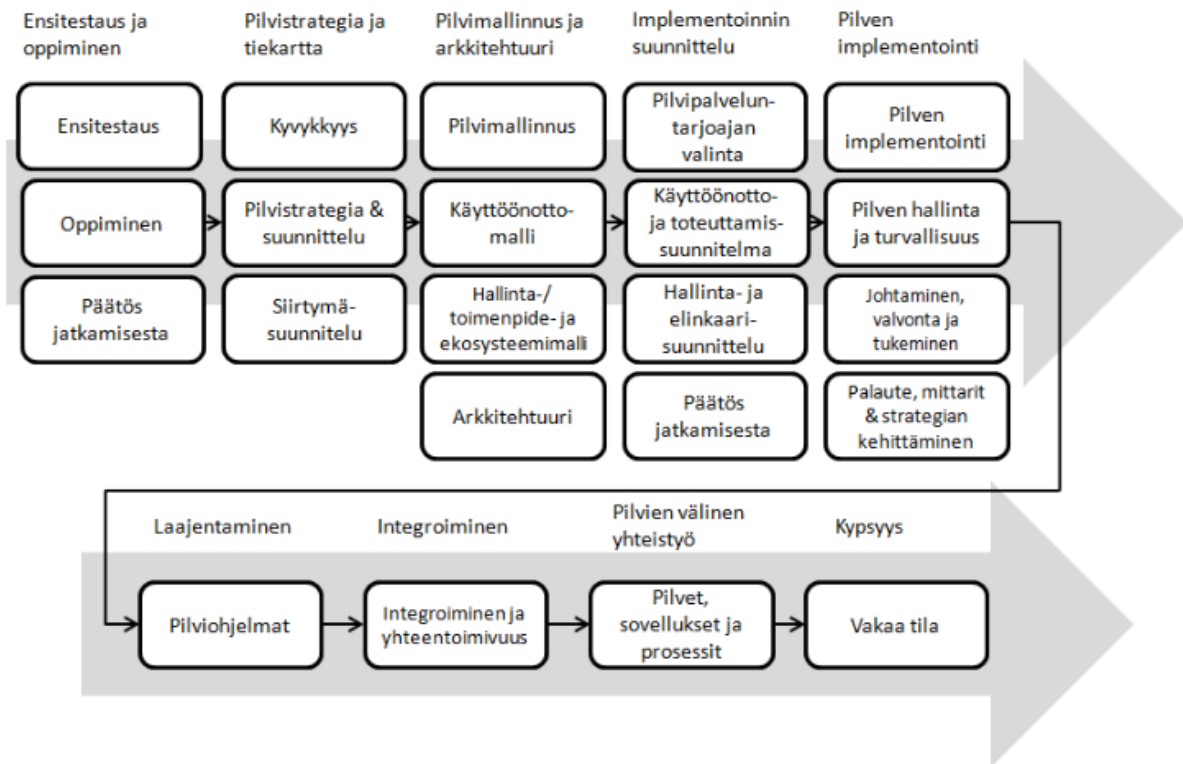
Amazon Web Services (AWS)

AWS on alun perin 2002 käynnistynyt pilvipalvelu, jonka keskiössä ovat Elastic Compute Cloud (EC2) virtuaalisten palvelimien palvelu. Nimekkäistä palveluista ainakin Twitter ja Second Life käyttämätä AWS:n palveluita. (Heino 2010) AWS:n datakeskukset sijaitsevat maantieteellisesti useissa eri sijainneissa, joista asiakkaalla on mahdollisuus valita missä datakeskuksissa haluaa datansa sijaitsevan. AWS käyttää käytönmukaista hinnoittelua. (Gulabani 2017)

3 PILVIPALVELUJEN KÄYTTÖÖNOTTO

Uusissa IT-innovaatioita käyttöönotettaessa on tärkeää, että innovaatiolla on myös liiketoiminnan tuki, koska usein innovaatiot ilman liiketoiminnan tukea jäävät tärkeysjärjestyksessä heikoille tai peruutetaan kokonaan. Teknologiat, joilla on suuri potentiaali nopeaan investoinnin kustannusten takaisin maksuun ovat usein myös liiketoiminnan suosiossa ja alkavat ja niiden tavoittelua jatketaan. Pilvipalvelujen hyödyntämisellä on usein suuri potentiaali investointihinnan takaisin maksuun ja saavat usein tämän vuoksi myös suuren tuen liiketoiminnan puolelta. (Marks & Lozano 2010)

Pilvipalveluiden luominen kehittyy jatkuvasti suoraviivaisemmaksi ja nopeammaksi. Jos yrityksen johtajilla on kokemusta ulkoistamisesta IT-palveluissa helpottaa tämä myös pilvipalveluihin siirtymistä, sillä organisaatio tasolla pilvipalveluiden hyödyntäminen muistuttaa ulkoistamista. (Géczy et al. 2012)



Kuva 3 Pilvipalvelun käyttöönoton vaiheet (Marks & Lozano 2010)

Pilvipalvelujen käyttöönotto on monivaiheinen prosessi, joista jokainen vaihe tulee suorittaa huolellisesti. Kuvassa 3 on esitetty pilvipalvelujen vaiheet aina ensitestauksesta vakaaseen tilaan asti. Vaiheita on paljon ja niiden läpikäyminen ei ole yrityksessä nopea prosessi. Prosessia varten yrityksen kannattaa luoda selkeä suunnitelma, jota toteutetaan ja seurataan monissa eri prosessin kohdissa.

3.1 Uudet sovellukset pilviympäristössä

Pilvinatiivit sovellukset ovat pilvipalveluihin suunniteltu ja optimoituja sovelluksia, jotka ovat yleensä suunniteltu alun perin pilvipalvelu ympäristössä käytettäväksi. Pilvinatiiveista sovelluksista puhutaan, koska on erilaista luoda sovelluksia perinteisiin datakeskuksiin kuin pilviympäristöön. Tämä aiheuttaa myös tietynlaista osaamisen päivittämisen tarvetta, koska sovelluksia ei voida enää suunnitella samalla tavalla kuin aikaisemmin suurimpien hyötyjen saavuttamiseksi pilvipalvelujen käytöstä. Pilvinatiiville sovellukselle tyypillistä seuraavat asiat: käytetään kertakäyttöistä infrastruktuuria, muodostuu rajatuista erillään olevista palasista,

skaalautuvat globaalisti, hyödyntää arvoa lisääviä pilvipalveluita, työllistää itseohjautuvia full-stack tiimejä ja ajaa kulttuurillista muutosta. Full-stack tiimillä tarkoitetaan tiimiä joka hyödyntää kaikkia teknologiatasoja sovellusten kehittämiseen. (Gilbert 2018)

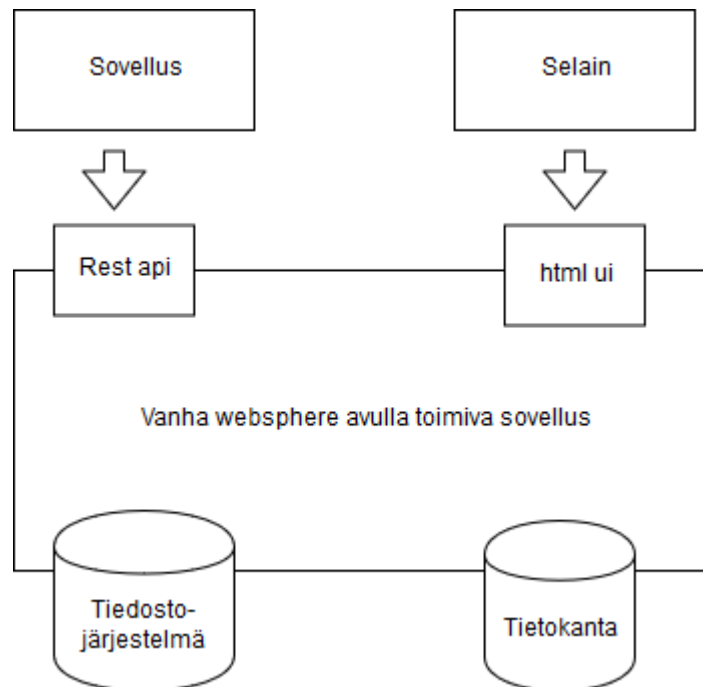
Pilvinatiivit sovellukset täytyy rakentaa vikasietoisemmiksi kuin perinteiset yhdessä konesalissa toimivat sovellukset ja tämä muokkaa tapaa millä sovellukset tulee suunnitella. Pilvinatiiveille sovelluksille onkin tyypillistä, että ne muodostuvat useista mikropalveluista, jotka huolehtivat yhdestä pienestä osasta sovellusta. Mikropalvelut rakennetaan toisistaan riippumattomiksi ja ne suunnitellaan vikasietoisiksi. Pilvipalveluissa usein sovelluksia julkaistaan jonkin orkestraattorin kuten Kubernetesen avulla. Orkestraattori huolehtii, että mikropalvelusta ja sovelluksesta on sopivasti kapasiteettia sovelluksenhallitsijan määritysten mukaisissa rajoissa. Orkestraattori myös luo automaattisesti uusia instansseja mahdollisesti vikatilaa ajautuneiden instanssien tilalle huolehtien näin siitä, että sovellus on jatkuvasti käytettävissä, vaikka yksi instanssi ajautuisikin vikatilaan. Myöskin sovellusten ensimmäinen julkaisu tehdään orkestraattorin avulla, jolloin orkestraattori luo automaattisesti määritysten mukaisia instansseja ilman käyttäjän tarvetta luoda samaa instanssia moneen kertaan. (Tofetti et al. 2017)

3.2 Vanhat sovellukset pilviympäristössä

Sovelluksien uudelleensuunnittelu ja kehittäminen niiden toimimiseksi pilvipalvelussa voi vaatia erittäin paljon työtä. (Zhong et al. 2010). Vanhoille sovelluksille on myös mahdollista käyttää Gladinet ohjelmistoa. Gladinetin avulla vanhaa sovellusta voidaan käyttää samalla tavalla kuin aikaisemminkin, mutta sen data voidaan pitää pilvipalvelussa. Gladinet luo pilvipalvelun näkymään tietokoneella samalla tavalla kuin USB-aseman tai ulkoisen kovalevyn ja näin ollen pilvipalvelun tietovarastot ovat vanhojenkin sovellusten käytettävissä helposti. (Sarna 2011)

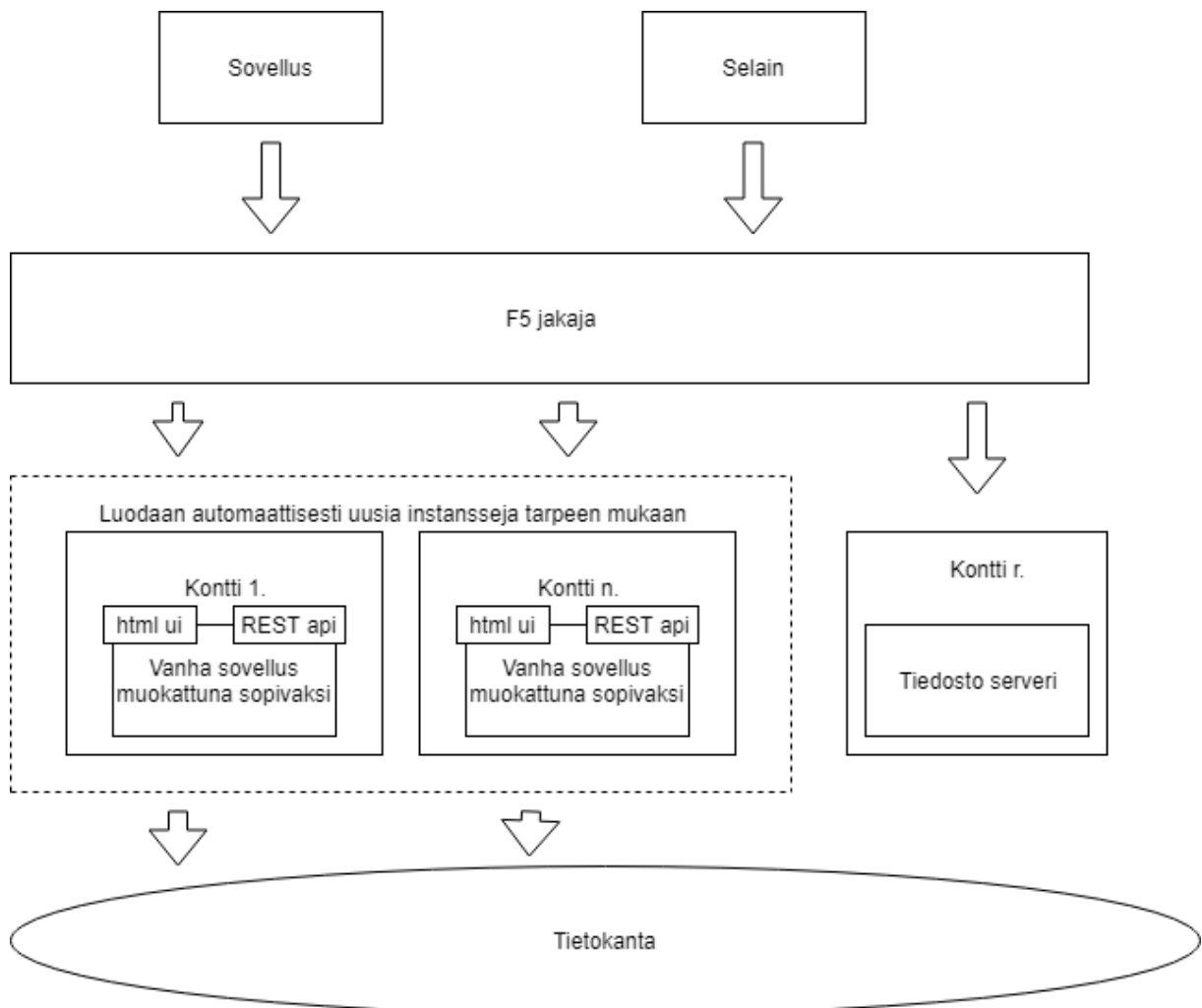
Docker sovellus mahdollistaa vanhojen sovellusten siirtämisen pilvipalvelun pienillä muutoksilla, itse ohjelmaan. Vanhaa ohjelmaa konvertoidessa Dockeriin kannattaa se pilkkoa

pienempiin palasiin, jotka toimivat toisistaan riippumattomissa Docker konteissa, jotka ovat helposti siirrettäviä riippumattomia ympäristöjä. Docker kontti luo isäntäkoneestaan riippumattoman ajoympäristön sovellukselle. Tämän ominaisuuden avulla Docker kontissa oleva sovellus voidaan siirtää täysin erilaisille isäntäkoneilla, koska ympäristö on riippumaton isäntäkoneen käyttöjärjestelmästä. (Slominski et al. 2015)



Kuva 4 Vanhan sovelluksen yhteydet (mukailien Slominski et al. 2015)

Vanhalla teknologialla tehty sovellus omaa kaksi rajapintaa. Graafinen html:n avulla toteutettu rajapinta käyttäjiä varten ja REST api rajapinta muita sovelluksia varten. Sovellus voisi toimia esimerkiksi yhdellä websphereä hyödyntävällä serverillä, jolla olisi oma tietokanta ja tiedostojärjestelmä. Kuvan 4 Sovellus ei ole skaalautuva vaan yhden serverin täytyisi olla mitoitettu kestäämään kuormitusta suurimpien mahdollisten kuormitustilanteiden mukaan, vaikka sitä ei aina tarvittaisikaan.



Kuva 5 Vanhan sovelluksen yhteydet pilvipalveluun siirrettynä (mukaillen Slominski et al. 2015)

Kuvan 5 mukaisesti pilvipalveluun toteutettuna samalla sovelluksella olisi edelleen html pohjainen graafinen käyttöliittymä käyttäjiä varten ja REST api rajapinta sovelluksia varten. Sovellus toimii kontti instansseina, joista jokainen sovelluksen kontti olisi eristetty toisistaan. Kontit olisivat yhteydessä pilvipalvelussa olevaan tietokantaan ja jokainen instanssi tallentaa tietonsa samaan tietokantaan, vaikka tulevatkin eri lähteistä. Käyttäjät tavoittavat kontit F5 jakajan kautta, joka ohjaa aina yhden käyttäjän pyynnöt samalla instanssille kuin käyttäjä oli saman istunnon kautta käyttänyt. Näin istuntoon liittyvät tiedot eivät katoa, eikä istuntoon liittyviä tietoja tarvitse jakaa konttien välillä. Kontitettua sovellusta on helppo skaalata tarpeen mukaan. Skaalaus voitaisiin suorittaa esimerkiksi Kubernetesin avulla orkestroimalla. Orkestroinnin avulla instansseja käynnistyisi tarpeen mukaan käyttökuorman lisääntyessä ja

tarpeettomat instanssit sulkeutuisivat käyttökuorman vähentyessä. Näin pilvipalvelussa voidaan saada huomattavia kustannussäästöjä skaalautuvuuden lisääntymisellä. Kuvan 4 mukaisessa tilanteessa palvelimen pitäisi olla suhteettoman suuri moniin tilanteisiin suhteutettuna harvinaisempien maksimikuormitus tilanteiden varalta, kun kuvan 5 mukaisessa tilanteessa instanssien määrää voitaisiin muokata kuormituksen mukaan. Skaalautuvuus voisi olla hyödyllistä esimerkiksi vakuutuskorvauksiin liittyvässä sovelluksessa, jossa käyttö voi olla päiväsaikaan huomattavasti suurempaa kuin ilta- ja yöaikaan. Vakuutuskorvauksiin liittyvässä sovelluksessa voisi olla iltaisin vain muutama instanssi käytössä ja päiväsaikaan kuormituksen ollessa suurimmillaan voisi instanssien määrä kasvaa suuremmaksi kuormasta selviytymiseksi. Ilta- ja yöaikaan instansseja sulkemalla voidaan saada aikaan kustannussäästöjä verrattuna vanhaan tapaan, jossa laskentateholtaan suuri palvelin on käynnissä kellon ympäri.

4 PILVIPALVELUT VAKUUTUSYHTIÖSSÄ

Vakuutusyhtiöiden erityispiirteitä pilvipalvelujen hyödyntämisessä kartoitettiin haastattelututkimuksella. Haastattelukysymykset on esitetty liitteessä 1. Työtä varten haastateltiin yritys X:n suomen liiketoimintaa varten toteutettavista sovelluksista vastaavan osaston esimiestä.

Vakuutusyhtiön erityispiirteet

Vakuutusyhtiöillä on monia it-yhtiölle tyypillisiä piirteitä, kuten paljon sovelluksia ja paljon it-työntekijöitä ja liiketoiminta on riippuvainen sovelluksien toiminnasta. Haastattelun perusteella merkittävimmät erityispiirteet vakuutusyhtiöillä pilvipalvelujen käytössä korkeat tietoturva-vaatimukset sovelluksien sisältämän sensitiivisen datan vuoksi.

Haastattelun perusteella tietoturva vaatimukset otetaan yrityksessä hyvin huomioon ja pilvipalveluita varten on luotu selkeä prosessi tietoturvan varmistamiseksi. Prosessin osana uudet pilvipalveluun luotavat sovellukset ja pilvipalvelut käyvät läpi tietoturva tarkistuksen. SaaS-sovellusten osalta käydään lävitse riskiarviointi ja DPIA-prosessi. Riskiarvioinnista arvioidaan sovelluksen käytöstä aiheutuvat uhat ja luodaan mahdollinen irtautumisstrategia, jos sovelluksesta halutaan irtautua. DPIA-prosessissa arvioidaan sovelluksen luotettavuutta sensitiivisen datan käsittelyn osalta. Yrityksen itse tuottamille sovelluksille prosessi sisältää samat osat kuin SaaS-sovelluksella ja niiden lisäksi sovellus tulee julkaista uusimpaan mahdolliseen ympäristöön ja tulevaisuudessa prosessiin lisätään uhkamallinnus. Uhkamallinnuksessa analysoidaan sovelluksen tietoturvallisuutta ja strukturoidulla prosessilla pyritään paikantamaan sovelluksen tietoturvariskit.

Odotukset pilvipalveluista

Haastattelun perusteella suurimmat toiveet pilvipalveluiden hyödyntämisen eduista liittyvät ohjelmistokehityksen prosessien tehostumiseen ja sovellusten skaalautuvuuteen. Myös kustannussäästöt nousivat esiin haastattelussa. Haastattelun perusteella yrityksessä on ymmärretty pilvipalvelujen hyödyntämisen vaativan yritykseltä selkeää suunnitelmaa

henkilöstön kouluttamisesta. Henkilöstön koulutuksessa pilvipalveluiden käyttöön voidaan hyödyntää yrityksen erillistä osastoa, joka on keskittynyt pilvipalveluiden hyödyntämisen mahdollistamiseen yhtiössä. Pilvipalvelujen odotetaan mahdollistavan joustavampi sovelluskehitys, kun tarvittavat palvelimet voidaan luoda muutamalla klikkauksella tarvittaessa. Uusien palvelimien luonnin helppous myös herätti huolta haastattelussa, koska näillä voidaan aiheuttaa myös suuria kustannuksia. Palvelimien luonnin ja sulkemisen kouluttaminen asianmukaisesti nousi selkeäksi tarpeeksi.

5 CASE: KATRE

Katre on kansallista tulorekisteriä varten toteutettava sovellus. Sovelluksen on tarkoitus toimittaa työntekijöiden palkkatiedot ja tuloina huomioitavien vakuutuskorvausten tiedot kansalliselle tulorekisterille. Katre on toimeksiantaja yrityksen suomen organisaatiota varten sovelluksia kehittävän osaston ensimmäinen pilvipalveluun toteutettava sovellus. Tässä luvussa käydään läpi sovelluksessa hyödynnettäviä palveluita.

Sovelluksen rakentamiseen käytetään Microsoftin Azuresta seuraavia palveluita: App Services Web App, App Services Function apps, Azure Blob Storage, CosmosDB, Service Bus Queues ja Azure Active Directory. Seuraavaksi käydään läpi käytettyjä työkaluja ja niistä saatavia hyötyjä.

App Services Web App

App Services Web App on PaaS-palvelu, jonka avulla on helppo suorittaa eri kielillä toteutettuja sovelluksia Linux ja Windows ympäristöissä. Web App sisältää kaikki sovelluksen käyttämiseen vaadittavat osat eli käyttöjärjestelmän, kapasiteetin ja serverit ja kuorman jaon. Web App on myös autoskaalautuva eli se luo uusia laskentayksiköitä kuormituksen lisääntyessä ja sulkee niitä kuormituksen vähentyessä. Web App -palvelu vapauttaa sovelluksenkehitykseen paljon resursseja muille osa-alueille, kun kehittäjän ei tarvitse huolehtia palvelun valmiiksi tarjoamista osista. (Azure 2019b) Web App palvelu toimii Katren päätepineenä. Web Appin sisällä toimivat sovelluksen muut osat, jotka vastaavat tiedon tallentamisesta ja ohjelman toiminnallisuudesta.

App Services Function app

App Services Function app -palvelu on tarkoitettu funktioiden rakentamiseen tarkoitettu PaaS-palvelu. Function app-palvelulla rakennetaan funktioita hyödyntäen Web App-alustaa. Function appilla voidaan sovellusta varten rakentaa erillään olevia funktioita joiden päivittäminen voidaan suorittaa täysin ilman sovelluksen alhaalla olo aikaa. Function app huolehtii automaattisesti funktion päivittämisestä uusien määritysten mukaiseksi, eikä

kehittäjän tarvitse huolehtia päivittämisestä. (Azure 2019c) Katren pääasiallinen sovelluslogiikka on rakennettu Function app funktioiden avulla. Funktiot kuuntelevat saapuvia viestejä ja käsittelevät ne halutulla tavalla.

Cosmos Db

Cosmos Db on Azuren tarjoama tietokantapalvelu. CosmosDb on joustava ja automaattisesti skaalautuva tietokantapalvelu, joka tarjoaa suuren 99.999% saatavuuden. CosmosDbn käyttöliittymä tarjoaa käyttäjälle mahdollisuuden valita käytettävien konesalien sijainnin muutamalla klikkauksella. Vakuutusyhtiössä konesalin valinnan mahdollisuus on tärkeä, koska data ei saa poistua EU-alueelta. CosmosDb huolehtii automaattisesti varmuuskopioiden luomisesta ja sijoittaa ne eri konesaleihin, joten datan säilyminen ongelma tilanteissa on varmistettu suurella todennäköisyydellä. CosmosDb tietokannat sijaitsevat usein myös samoissa konesaleissa kuin itse sovellus, joten vasteajat tietokantakutsuille pysyvät lyhyinä. (Azure 2019d) Katressa kaikki sovelluksen tarvitsema metatieto tallennetaan Cosmos Db:seen. CosmosDb mahdollistaa sovellukselle tehokkaan jonojen hallinnan ja on tehokas metatiedon tallentamiseen.

Service Bus Queues

Service Bus Queues on viestienpohjainen väliohjelmisto. Service Bus Queues -palvelun avulla voidaan hallita sovellusten sisäisiä viestiketjuja ja sovelluksen käyttäjän toimintoja. Sovelluksen lähettämät viestit kulkevat Service Bus Queues-jonojen kautta ja ja jonot hallitsevat viestien tilatietoja. Service Bus Queues-jonojen avulla viestin lähettäjän ja vastaanottajan ei tarvitse lähettää viestejä samaan aikaan. Jonot mahdollistavat sen, että sovelluksen ei tarvitse odottaa käyttäjän vastausta vaan voi jatkaa prosessiaan eteenpäin ennen vastauksen saamista. Jonojen avulla on myös mahdollista tehdä myös kuormantasausta kun käyttäjien viestejä voidaan asettaa jonoon odottamaan vuoroaan, kun sovelluksen kapasiteetti on äärimmillään. Näin sovelluksen käyttämän ympäristön laskentatehoa ei tarvitse lisätä vaan viestejä voidaan käsitellä jonosta siinä järjestyksessä, kun ne ovat saapuneet kapasiteetin sallimissa rajoissa. (Azure 2019e) Kaikki Katren viestintä tehdään Service Bus Queue jonojen

avulle. Jokainen jonon toimii erillisenä välitalennustilana, joka säilöö sen hetkisen viestin prosessin tilaa.

Azure Blob Storage

Azure Blob Storage on rakenteettoman datan tallentamiseen tarkoitettu palvelu. Azure BloB Storagea voidaan hyödyntämään monen eri sovelluksen tai yhden sovelluksen eri ilmentymien yhteisenä tallennuspaikkana. Blob Storage on erillään oleva tallennustila, johon on mahdollista saada yhteys ulkopuolelta. Näin ollen jokaiselle sovellukselle tai sovelluksen ilmentymällä ei tarvitse rakentaa omaa tallennuspaikkaa vaan ne voivat hyödyntää yhteistä Blob Storagea. (Azure 2019f) Katressa Blob Storage käytetään tallentamaan kaikki sovelluksen transaktiot, jolloin transaktioita on mahdollista tarkistella jälkikäteen erillisellä sovelluksella.

Azure Active Directory

Azure Active Directory on Microsoftin pilvipalvelu pohjainen käyttäjätietojen hallinta ja oikeuksienhallinta palvelu. Active Directoryn kautta voidaan hallita käyttäjien pääsyä sovellukseen ja tunnistaa sovelluksen käyttäjä. Active Directory mahdollistaa sen, että käyttäjän ei tarvitse kirjautua sisään sovellukseen vaan sovellus voi tunnistaa käyttäjän tämän tietokoneen kirjautumistiedoista. (Azure 2019g) Katressa Active Directorya käytetään käyttäjien tunnistamiseen ja näiden oikeuksien tarkistamiseen. Näin käyttäjän ei tarvitse erikseen kirjautua sovellukseen ja käyttäjäkokemus on parempi.

6 JOHTOPÄÄTÖKSET

Työn tavoitteena oli vastata kysymyksiin ”Mitä hyötyjä ja haasteita pilvipalvelujen hyödyntämisestä syntyy?” ja ”Mitkä ovat vakuutusyhtiö erityispiirteet pilvipalvelujen hyödyntämisessä?”. Vastaus etsittiin kirjallisuuskatsauksen, haastattelun ja case-tutkimuksen avulla.

Pilvipalvelut ovat vakuutusyhtiölle suuri mahdollisuus. Pilvipalvelut mahdollistavat vakuutusyhtiön IT-osastoille paremman resurssien hyödyntämisen monin eri tavoin. Pilvipalvelujen hyödyntäminen mahdollistavat resurssien hankkimisen tarpeen mukaan, eikä ole tarvetta ylläpitää suurta kapasiteettia harvinaisten maksimikuormitustilanteiden kannalta. Myös uusien resurssien käyttöönotto tehostuu huomattavasti, kun niitä ei tarvitse hankkia omaan konesaliin tai odottaa, että palveluntarjoaja luo uudet resurssit yrityksen käyttöön vaan ne saadaan helposti käyttöön pilvipalvelusta heti tarpeen tullen.

Case Katressa hyödynnettiin monia Azuren valmiita toiminnollisuuksia. Valmiit toiminnot nopeuttavat sovelluksenkehitystä huomattavasti, kun monista sovelluksen osa-alueista on olemassa valmis toiminto, jota sovellus hyödyntää. Katren osalta sovelluskehitys on myös ketterää kun Azuren palvelut huolehtivat sovellusten päivittämisestä määritellyllä tavalla ja päivitysten saaminen palvelimille on nopeaa ja helppoa.

Vakuutusyhtiöissä sensitiivinen datan suuri määrä luo kuitenkin paineita korkeatasoiseen tietoturvaan käytetään sitten omaa konesalia, perinteistä palveluntarjoajaa tai pilvipalvelua. Pilvipalvelut on kuitenkin rakennettu niin, että asiakkaat pystyvät luottamaan infrastruktuurin tietoturvaan. Esimerkiksi Microsoftin Azure pilvipalvelulla on erittäin kattavat tietoturva sertifikaatit joiden tietoturva tasoon omalla konesalilla olisi erittäin vaikea päästä. Pilvipalvelut mahdollistavat siis oikein käytettynä myös tietoturvallisemman ympäristön kuin omat konesalit, mutta sovellusten ja järjestelmien tietoturva-arkkitehtuurin luonne muuttuu pilvipalveluissa, joten tietoturvaan yrityksen tulee kuitenkin paneutua pilvipalveluita käyttöönotettaessa. Sensitiivinen data on otettava myös palvelutasosopimusta tehdessä

huomioon, koska sensitiivinen data ei saa poistua EU-alueen ulkopuolella oleviin konesaleihin ja tästä tulee sopiva pilvipalveluntarjoajan kanssa erikseen.

Pilvipalveluiden käytössä haastavimpia osia on käyttöönotto ja yrityksen tuleekin käyttää käyttöönotto vaiheessa huomattavasti resursseja muun muassa henkilöstön kouluttamiseen, jotta henkilöstö osaa hyödyntää pilvipalveluita parhaalla mahdollisella tavalla. Myös vanhojen sovellusten arkkitehtuuria joudutaan mahdollisesti muokkaamaan niitä siirrettäessä pilvipalveluita. Myös uusia sovelluksia kehittäville ohjelmoijille tulee tarjota koulutuksia, joiden avulla he osaavat hyödyntää pilvipalveluiden tarjoamia mahdollisuuksia mahdollisimman tehokkaasti sovellusten kehityksessä.

Pilvipalveluiden suurimpina hyötyinä ovat siis ohjelmistotuotantoprosessien tehostuminen ja resurssien käytön tehostuminen kun niitä voidaan ostaa tarpeen mukaan joustavasti. Suurimpia haasteita ovat käyttöönotto ja tietoturvallisuudesta huolehtiminen. Vakuutusyhtiölle erityispiirteitä pilvipalveluiden käytössä luo sensitiivisen datan suuri määrä, minkä vuoksi tietoturvasta täytyy huolehtia erityisen huolellisesti.

LÄHTEET

Azure. 2019a. Pricing calculator. [WWW-dokumentti]. [viitattu 14.3.2019]. Saatavissa: <https://azure.microsoft.com/en-us/pricing/calculator/#virtual-machines43c3b0fc-b6ec-4e07-986e-37f3951dc033>.

Azure. 2019b. App Service. [WWW-dokumentti]. [viitattu 10.4.2019]. Saatavissa: <https://azure.microsoft.com/en-us/services/app-service/>.

Azure. 2019c. Create a function app from the azure Azure portal. [WWW-dokumentti]. [viitattu 10.4.2019]. Saatavissa: <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-function-app-portal>.

Azure. 2019d. Welcome to Azure Cosmos DB. [WWW-dokumentti]. [viitattu 10.4.2019]. Saatavissa: <https://docs.microsoft.com/en-us/azure/cosmos-db/introduction>.

Azure. 2019e. Service Bus queues, topics and subscriptions. [WWW-dokumentti]. [viitattu 10.4.2019]. Saatavissa: <https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions>.

Azure. 2019f. Azure Blob Storage. [WWW-dokumentti]. [viitattu 10.4.2019]. Saatavissa: <https://docs.azuredatabricks.net/spark/latest/data-sources/azure/azure-storage.html>.

Azure. 2019g. What is Azure Active Directory? [WWW-dokumentti]. [viitattu 10.4.2019]. Saatavissa: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>.

Bhardwaj, S., Jain, L. & Jain, S. 2010. Cloud Computing: A Study of Infrastructure as a Service (IaaS). *International Journal of Engineering and Information Technology*. Vol. 2 nro. 1, s. 60-63.

Calder, B., Wang, J., Aaron, O., Nilakantan, N., Skjolsvold, A., McKelvie, S., Yikang, X., Shaswat, S., Wu, J., Simitci, H., Haridas, J., Uddaraju C., Khatri, H., Edwards, A., Bedekar, V., Mainali, S., Abbasi, S., Agarwal, A., Fahim ul Haq, M., Ikram ul Haq M, Bhardwaj, D., Dayanand, S., Adusumili, A., McNett, M., Sriram, S., Kavitha, M. & Leonidas R. 2011. Windows Azure Storage, a highly available cloud storage service with strong consistency. *SOSP '11 Proceeding of the Twenty-Third ACM Symposium on Operating Systems Principles*. S. 143-157.

Carrol, M., van der Merwe, A. & Kotzé, P. 2011. Secure cloud computing: Benefits, risks and controls. *Information Security for South Africa*.

Chou, D. 2015. Cloud computing risk and audit issues. *Computer Standards & Interfaces*. Vol. 42, s. 137-142.

Chun, S-H- & Choi, B-S. 2013. Service models and pricing schemes for cloud computing. *Cluster Computing*. Vol. 14, nro 2, s. 529-535.

Coles, C. 2018. Cloud Market in 2018 and Predictions for 2021. [WWW-dokumentti]. [viitattu 15.2.2019]. Saatavissa: <https://www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/>.

Euroopan parlamentin ja neuvoston asetus 2016/679. 2016

Geczy, P., Izumi, N. & Hasida K. 2012. Cloudsourcing: Managing Cloud Adoption. *Global Journal of Business Research*. Vol.6, nro. 2, s.57-70.

Gilbert, J. 2018. Cloud Native Development Patterns and Best Practices. *Packt Publishing*. 297 s.

Gulabani, S. 2017. Practical Amazon EC2, SQS, Kinesis and S3. *Apress*. 312 s.

Heino, P. 2010. Pilvipalvelut. *Talentum Media*. 267 s.

Heiser, J. & Nicolett, M. 2008. Assessing the Security Risks of Cloud Computing. *Gartner*. 6 s.

Hirsjärvi, S. & Hurme, H. 2015. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. *Gaudeamus*. 213 s.

Johnson, B. & Qu, Y. 2012. A Holistic modern for Making Cloud Migration Decision: A Consideration of Security, Architecture and Business Economics. *2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications*.

Kandukuri, B., Paturi, R. & Rakshit, A. 2009. Cloud Security Issues. *2009 IEEE International Conference on Services Computing*.

Kaufmann, L. 2009. Data Security in the World of Cloud Computing. *IEEE Security & Privacy*. Vol. 7, nro. 4, s61-64.

Krutz, R. & Vines, R. 2010. Cloud Security. *Wiley*. 384 s.

Henkilö X. 2019. Pilvipalvelujen erityispiirteet vakuutusyhtiössä haastattelututkimuksen tulokset. Yritys X. Haastattelu 19.3.2019.

Lewis, K. & Lewis, J. 2009. Web Single Sign-On Authentication using SAML. *International Journal of Computer Science Issues*. Vol. 2, s.41-48

Knorr, E. & Gruman, G. 2018. What Cloud Computing Really Means. *InfoWorld*. Vol. 42, nro. 2, s. 52-54.

Lin, G., Fu D., Zhu J. & Dasmalchi, G. 2009. Cloud Computing: It as a Service. *IT Professional*. Vol. 11, nro. 2, s. 10-13.

Marks, E. & Lozano B. 2010. Executive's Guide to Cloud Computing. *John Wiley & Sons*. 285 s.

Mather, T., Kumaraswamy, S. and Latif, S. Cloud Security and Privacy. *O'reilly Media*. 299 s.

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing. *NIST Special Publication 800-145*. 3 s.

Neumann, P. 2014. Risks and myths of cloud computing and cloud storage. *Communications of the ACM*. Vol. 57, nro 10, s. 25-27.

Park, S-T., Park, E-M., Seo, J-H. & Li, Q. 2015. Factors affecting the continuous use of cloud service: focused on security risks. *Cluster Computing*. Vol. 19, nro. 1, s.485-945

Rison, A. 2017. Microsoft Azure leads the industry in ISO certifications. [www-dokumentti]. [viitattu 15.3.2019]. Saatavissa: <https://azure.microsoft.com/en-us/blog/microsoft-azure-leads-the-industry-in-iso-certifications/>

Rosenberg J. & Mateos, A. 2011. The cloud at Your Service. *Manning*. 272 s.

Sarna, D. 2011. Implementing and Developing Cloud Computing Applications. *CRC Press*. 308 s.

Subashini, S. & Kavitha, V. 2011. A surve on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*. Vol. 34, nro. 1, s.1-11.

Slominski, A., Muthusamy, K. 2015. Building a Multi-tenant Cloud Service from Legacy code with Docker Containers. *2015 IEEE International Conference on Cloud Engineering*.

Toffetti, G., Brunner, S., Blöchlinger, M., Spillner, J., Bohnert, T-. 2017. Self-managing cloud-native applications: Design, implementation, and experience. *Future Generation Computer Systems*. Vol. 72, nro. 1, s. 165-179.

Velte T., Velte A., Elsenpeter R. 2009. Cloud Computing, A Practical Approach. *McGraw-Hill Osborne Media*. 333 s.

Waters, B. 2005. Software as a service: A look at the customer's benefits. *Journal of Digital Asset Management*. Vol. 1 nro 1. S. 32-39.

Zhong, L., Wo, T., Li, J., Li, B. 2010. A Virtualization-Based SaaS Enabling Architecture for Cloud Computing. *2010 Sixth Internal Conference on Autonomic and Autonomous Systems*.

Liite 1. Haastattelututkimuksen haastattelukysymykset

- 1. Mikä on edustamasi osasto? Mikä on edustamasi osaston toiminnoista tärkeimpiä ja mitkä vähiten arvoa luovia.*
- 2. Millaista ohjelmistokehitysprosessi osastollasi on tällä hetkellä?*
- 3. Mitkä ovat ohjelmistokehitysprosessin haastavimmat osiot?*
- 4. Miksi pilvipalveluihin halutaan siirtyä?*
- 5. Mitä erityispiirteitä uskot vakuutusyhtiöillä pilvipalvelujen käytössä olevan?*
- 6. Mitä hyötyjä pilvipalveluista uskot syntyvän?*
- 7. Mikä pilvipalveluihin siirtymisessä huolettaa eniten?*
- 8. Miten ohjelmistokehitysprosessi on muuttunut viime vuosina osastollasi?*
- 9. Miten uskot pilvipalvelujen muuttavan ohjelmistokehitysprosesseja osastollasi?*
- 10. Mitä pilvipalvelujen onnistunut integraatio osaksi yrityksen toimintamalleja ja henkilöstön arkea edellyttää?*