Atte Herttala

Pilvipalvelut ja niiden suosion syitä

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Atte Herttala

Yhteystiedot: atte.a.herttala@student.jyu.fi

Ohjaaja: Sanna Juutinen

Työn nimi: Pilvipalvelut ja niiden suosion syitä

Title in English: Cloud computing and reasons for cloud popularity

Työ: Kandidaatintutkielma

Sivumäärä: 20+0

Tiivistelmä: Tutkielman aiheena on pilvipalveluiden ominaisuudet, palvelu- ja käyttöönottomallit sekä pilvipalvelujen vertausta klassisiin yrityksien omilla palvelimella oleviin palveluihin ja järjestelmiin. Tutkielmassa käydään läpi esimerkiksi pilvipalveluiden hinnoittelua, saatavuutta sekä turvallisuusnäkökulmaa. Tutkielmassa avataan myös pilvipalveluiden korkean suosion takana olevia syitä

Avainsanat: Pilvi, pilviteknologiat, pilvipalvelu, AWS, Azure

Abstract: This thesis is about characteristics of cloud computing services and different cloud service models and deployment models, and pros and cons of cloud services when comparing to on premise services. Thesis includes pricing, security and availability of cloud services. Thesis also includes finds on why the cloud computing services are so popular nowadays.

Keywords: Cloud, cloud computing, cloud service, AWS, Azure

Kuviot

Sisällys

1 Johdanto

Pilvipalvelut ovat 2000 luvun jälkeen pinnalle nousseita ja suuren suosion keränneitä IT-alan palveluita, joissa osa palvelun vastuusta on siirretty palveluntarjoajalle. Perinteisessä ohjelmistoratkaisussa on itse yritys vastuussa kaikista ohjelmiston fyysisistä ja virtuaalisista osista. Tämä tarkoittaa palvelimena käytettävien resurssien ostamista sekä ylläpitoa (Kavis 2014).

Tässä tutkielmassa selitetään aluksi käsitteitä ja määritelmiä, jotka liittyvät pilvipalveluihin tai niiden ominaisuuksiin. Tämän lisäksi tutkielmassa käsitellään eri tapoja jolla pilvipalveluita voidaan luokitella. Palvelumalleihin jako on yleisin luokittelutapa pilvipalveluille. Palvelumalleja ovat infrastruktuuri palveluna, palvelualusta palveluna sekä sovellus palveluna. Tutkielmassa käsitellään myös käyttöönottomalleja, joita ovat julkinen pilvi, yksityinen pilvi sekä hybridipilvi (Shrivastwa 2018).

Tutkielmassa vertaillaan myös pilvipalveluiden ja on-premise-ratkaisujen ominaisuuksia. Tämän jälkeen tarkastellaan asioita, jotka tekevät pilvipalveluista suosittuja, kuten hinnoittelu ja saatavuus. Tutkielmassa käydään läpi myös pilvipalveluiden turvallisuusnäkökulmaa. Pilvipalveluiden turvallisuus on monelle kysymyksiä herättävä aihe, sillä suuret tietomurrot nousevat mediassa pinnalle ja ihmiset saattavatkin pitää pilvipalveluita tämän takia epäturvallisena. Tutkielmassa päätavoitteena on selvittää pilvipalveluiden suosion syitä ja selvittää ovatko pilvipalvelut turvallisia. Tutkielma on kirjallisuuskartoitus.

2 Pilvipalveluiden rakenne ja ominaisuudet

Pilvipalvelu on internetin kautta tarjottavia palveluita, joissa käyttäjä ostaa palveluntarjoajalta heidän palvelimien resursseja, laskentatehoa, tai tallennuskapasiteettia, kun taas klassisessa mallissa yritys käyttää heidän omassa datakeskuksessa olevia resursseja ohjelmiston pyörittämiseen. Yleisimpiä pilvipalvelun palveluntarjoajia ovat: AWS (Amazon Web Services), Microsoft Azure sekä Google Cloud. Klassisessa konesaliratkaisussa yritys itse ylläpitää ja omistaa kaiken laitteiston ja siihen kuuluvat osat, joilla ohjelmiston käyttöönotto on mahdollista. Pilvipalvelussa kaikki tai osa näistä laitteistoista, infrastruktuureista sekä ohjelmistoista ja väliojelmistoista on palvelutarjoajan omistamia ja ne sijaitsevat palveluntarjoajan omistamassa datakeskuksessa.

Grance ja Mell (2011) kirjoittaman NIST (National Institute of Standards and Technology) dokumentin The NIST Definition of Cloud Computing mukaan pilvipalveluiden viisi tärkeintä ominaisuutta ovat:

Itsepalvelullisuus resursseja tarvittaessa (on-demand self-service). Resurssit ovat heti saatavilla ja käytettävissä ilman vuorovaikutusta toisen ihmisen kanssa. Vastaesimerkkinä Grance ja Mell (2011) käyttävät lankapuhelinta, jolla pitkän matkan puhelua soitettaessa täytyi soittaa toiselle ihmiselle eli teleoperaattorille, joka yhdisti puhelun käyttäjän puolesta. Konesaliratkaisuissa myös resurssien varaaminen täytyy hoitaa viikkoja tai kuukausia etukäteen, ennen ohjelmiston käyttöönottoa. Pilvipalveluratkaisussa taas palvelinresurssit ovat välittömästi saatavilla.

Laaja saatavuus internetin välityksellä (broad network access). Resurssit ovat käytettävissä esimerkiksi normaaleilla matkapuhelimilla sekä tietokoneilla. Resurssien saatavuus ei ole siis riippuvainen käyttäjän fyysisestä sijainnista, vaan hänen internettiin pääsystä. Nykypäivänä myös ihmiset odottavat että hyvälaatuinen internet on saatavilla fyysisestä sijainnista riippumatta (Grance ja Mell 2011). Pilvipalvelu on siis saatavilla langattoman, tai langallisen verkon kautta.

Resurssien yhdistäminen (resource pooling). Palveluntarjoajan resurssien fyysiset sijainnit ovat hajautettuja, mutta kaikkia instansseja tai resursseja voi käyttää useampi henkilö sa-

maan aikaan (Grance ja Mell 2011). Tätä kutsutaan multi-tenant malliksi. Multi-tenant mallilla voidaan luoda kustannustehokkaasti useille asiakkaille tarkoitettuja sovelluksia, jotka kuitenkin ovat eristettyjä keskenään. Asiakkaat eivät näe muiden asiakkaiden dataa, mutta kaikki käyttävät samoja resursseja (Pearson 2013). Eri resurssien käyttöä voidaan myös muuttaa liikenteen mukaan. Käyttäjällä voi olla rajoitettu hallinta palvelevan resurssin sijainnin muuttamisesta (Grance ja Mell 2011). Toissijaisia resursseja voidaan myös automaattisesti allokoida vikatilanteiden sattuessa (Bauer ja Adams 2012).

Nopea joustavuus (rapid elasticity). Resursseja voidaan joustavasti provisioida sekä vapauttaa. Resurssien määrää siis voidaan muuttaa kuorman perusteella. Tämä toimenpide tapahtuu useimmissa pilvipalveluissa automaattisesti. Tästä käytetään myös termiä skaalautuvuus (Grance ja Mell 2011). Pilvi-infrastruktuurin osia voidaan skaalata vaaka- ja pystysuunnassa. Saman suorituskyvyn resurssien määrän lisäämistä kutsutaan vaakasuuntaiseksi skaalautumiseksi. Pystysuuntainen skaalautuminen tarkoittaa resurssien suorituskyvyn tai kapasiteetin lisäämistä (Kumar ja Vidhyalakshmi 2018).

Palveluiden mitattavuus (measured service) Pilvijärjestelmät automaattisesti hallitsevat, raportoivat sekä mittaavat eri resurssien käyttöä. Mitattavia asioita voi olla esimerkiksi tallennustila, kaistanleveys, käyttäjien määrä tai resurssien käyttöstatistiikat. Nämä tuovat rehellisyyttä palveluntarjoajan sekä asiakkaan välille (Grance ja Mell 2011). Esimerkiksi Amazon Web Services (2022) tarjoaa eri palveluita resurssien käytöstä, kuten suorituskyvyn käytöstä, kustannuksista sekä käyttäjien tekemistä operaatioista pilvipalveluissa.

2.1 Pilvipalveluiden palvelumallit

Pilvipalvelut voidaan jakaa karkeasti kolmeen eri palvelumalliin niiden vastuiden mukaan: infrastruktuuri palveluna (IaaS, Infrastructure as a Service), palvelualusta palveluna (PaaS, Platform as a Service) sekä ohjelmisto palveluna (SaaS, Software as a Service) (Grance ja Mell 2011). Palvelumalleja on kuitenkin useampia, mutta edellä mainitut ovat yleisimmin käytössä olevia malleja. Eri palvelumalleissa palveluntarjoajat tarjoavat yhden tai useamman järjestelmään kuuluvista kerroksista (Pearson 2013). Verrattuna yrityksen täysin itse ylläpitämään ja omistamaan palveluun on IaaS-malli lähimpänä vastuiden suhteen. Tässä mal-

lissa palveluntarjoaja on vastuussa laitteistosta, PaaS-mallissa laitteiston lisäksi palveluntarjoaja on myös vastuussa palvelun käyttöjärjestelmästä ja väliohjelmistosta, ja SaaS-mallissa on palveluntarjoaja vastuussa edellä mainittujen lisäksi myös tarjottavasta sovelluksesta tai ohjelmistosta. SaaS on siis valmis tai lähes valmis tuotepaketti (Kavis 2014). On-premise-ratkaisuista siirtyessä IaaS-, PaaS- ja SaaS-ratkaisuihin kyky muokata ohjelmistoa pienenee (Shrivastwa 2018). Palvelumallien valinta on hyvin tärkeä osa pilvipohjaisten järjestelmien käyttöönotossa, minkä takia on myös erittäin tärkeää, että mallit ymmärtää ennen kuin yritys valitsee sopivan palvelumallin (Kavis 2014).

On-premise-ratkaisuissa yritys on itse vastuussa kaiken laitteiston omistuksesta, ylläpidosta, turvallisuudesta ja huollosta. Netflixin siirtyessä on-premise-ratkaisusta AWS-pilvipalveluihin, kertoi Netflix suurimmaksi haasteeksi on-premise-ratkaisussa liikenteen suuren määrän sekä ennalta-arvaamattomuuden. Yrityksellä täytyi olla enemmän kapasiteettiä kuin keskivertoliikenne vaatii, jotta liikennepiikkien haitat saatiin minimoitua. Tämä on suuri haaste klassisissa ratkaisuissa. AWS:n tuomat palvelut toivatkin automaattisesti skaalautuvia resursseja. Netflix myös pystyi käyttämään miehistöresurssejansa enemmän sovelluskehitykseen, sillä pilvipalveluihin siirryttäessä ei tarvitse käyttää niin paljoa resursseja infrastruktuurin rakentamiseen ja ylläpitoon (Kavis 2014).

Infrastruktuuri palveluna -mallissa pilvipalveluntarjoajan resurssit ovat prosessointiteho, tallennuskapasiteetti, tietoverkot sekä muut resurssit joilla käyttäjä voi suorittaa ja käyttöönottaa ohjelmistoja, jotka koostuvat sovelluksista ja järjestelmistä (Kumar ja Vidhyalakshmi 2018). IaaS toimittaa siis ulkoistetun tietokoneinfrastruktuurin (Kavis 2014). Kuluttajalla ei ole täyttä hallintaa kaikista infrastruktuurin osista, mutta hän hallitsee esimerkiksi käyttöjärjestelmää, sovellusta ja tallennuskapasiteettiä sekä mahdollisesti joitain tietoverkon komponentteja. Palveluntarjoaja voi myös suorittaa varmuuskopiointia sekä järjestelmäpäivityksiä (Kumar ja Vidhyalakshmi 2018). Tässä palvelumallissa tietokoneinfrastuktuurin muokkaaminen tapahtuu komentorivityökaluilla, selainpohjaisella käyttöliittymällä tai molemmilla (Kavis 2014). Esimerkkinä IaaS-palvelusta on AWS EC2-instanssit ja S3 sekä Open Stack (Grance ja Mell 2011).

Palvelualusta palveluna -mallissa käyttäjällä on mahdollisuus julkaista ja käyttöönottaa sovelluksia IaaS-mallia rajoitetummalla infrastruktuurin hallintamahdollisuuksilla (Grance ja

Mell 2011). Kuluttajat julkaisevat palveluntarjoajan tarjoamalle pilvi-infrastruktuurille ohjelmointikielillä sekä palveluntarjoajan tarjoamilla työkaluilla tuotettuja sovelluksia (Pearson 2013). Korkeasti skaalautuvien järjestelmien kehittämisessä kehittäjät joutuvat ohjelmoimaan paljon välimuistiin, asynkroniseen viestintään ja tietokannan skaalautumiseen liittyviä ominaisuuksia. Monet PaaS-ratkaisut tarjoavat näitä ominaisuuksia palveluina, jolloin kehittäjät voivat keskittyä muun sovelluslogiikan kehittämiseen (Kavis 2014). Esimerkkinä PaaS-palvelusta on AWS Lambda ja force.com.

Sovellus palveluna -mallissa kuluttaja käyttää palvelutarjoajan infrastruktuurissa olevaa ohjelmistoa, joka on käytettävissä esimerkiksi web-selaimella. Käyttäjällä on hyvin rajoitetut hallintamahdollisuudet infrastruktuurin muokkaamiseen (Grance ja Mell 2011). Muokkausominaisuuksia saattaa olla sovelluskohtaisiin asioihin ja parametreihin. SaaS-mallissa hyödynnetään paljon multi-tenant-mallia, jossa samaa palvelinresurssia voi hyödyntää useat eri asiakkaat, yritykset ja sovellukset. Sovellukset jotka ovat luotu eri asiakkaille, saattavat erota hieman keskenään. Nämä sovellukset kuitenkin käyttävät samaa palvelinresurssia. Single-tenant-mallissa taas jokaiselle erilliselle sovellukselle on varattu oma palvelinresurssi. Multi-tenant-malli mahdollistaa tehokkaan resurssienkäytön, joten ne ovatkin tarkoitettu erittäin monen henkilön samaan aikaan käytettäväksi. (Kavis 2014). Palvelun ostajan ei tarvitse kuin hallita käyttäjiä, ja palveluntarjoaja vastaa sovelluksesta, käyttöönotosta, infrastruktuureista sekä päivityksistä. Yrityksen täytyy vain maksaa ennakkoon määrätyt kulut sovelluksen käytöstä (Kavis 2014). Esimerkkeinä SaaS palveluista on Google Docs, Microsoft Office ja erilaiset asiakkuudenhallinta- ja toiminnanohjausjärjestelmät (Bauer ja Adams 2012).

Kuvio 1. Pilvipalveluiden palvelumallien eroja vastuiden suhteen Kavis (2014) ja Grance ja Mell (2011) mukaisesti. Kuvan tekijä Atte Herttala

2.2 Pilvipalveluiden käyttöönottomallit

Yksi tapa luokitella pilvipalveluita on käyttöönottomalleihin lajittelu (deployment model). Eri käyttöönottomalleja ovat yksityinen pilvi (private cloud) julkinen pilvi (public cloud), hybridipilvi (hybrid cloud) sekä yhteisöpilvi (community cloud). (Grance ja Mell 2011) Nämä mallit jakavat pilvipalvelut niiden käyttäjien perusteella.

Yksityinen pilvi on tarkoitettu yhden organisaation käyttöä varten. Toinen termi yksityiselle pilvelle on sisäinen pilvi (internal cloud) (Kumar ja Vidhyalakshmi 2018). Yksityinen pilvi voi olla ulkoisen toimijan, itse organisaation tai molempien ylläpitämä. Se voi fyysisesti sijaita itse organisaation tai pilvipalveluntarjoajan tiloissa (Grance ja Mell 2011). Yksityistä pilveä suosivat suuret organisaatiot, joilla on vahva IT-jäsenistö, jotka voivat järjestää ja ylläpitää toimintoja. Tämän käyttöönottomallin etuna on vahva tietoturva, joustavuus ja yksityisyys (Kumar ja Vidhyalakshmi 2018).

Yhteisöpilvi on tarkoitettu tietyn yhteisön käyttöä varten. Yhteisö voi koostua esimerkiksi organisaatioista kenellä on yhteisiä turvallisuusvaatimuksia pilvipalveluille, tiettyjä ohjeistuksia (compliance) tai muita vaatimuksia. Se voi olla kolmannen osapuolen, itse yhteisön

tai molempien omistuksessa (Grance ja Mell 2011). Yhteisöpilven etuina on vahva tietoturva ja yksityisyys kuten yksityisessäkin pilvessä, mutta se voi olla paljon kustannustehokkaampi jaettavien käyttöomaisuusinvestointien takia (Kumar ja Vidhyalakshmi 2018).

Julkinen pilvi on julkisesti käytettävissä. Se voi olla jonkun yrityksen tai koulutusyhteisön omistama ja ylläpitämä (Grance ja Mell 2011). Keskisuuret ja pienemmät yritykset valitsevat yleensä tämän mallisen pilviratkaisun. Julkinen pilvi koostuu tuhansista palvelimista jotka sijaitsevat fyysisesti eri puolilla maapalloa. Datakeskuksen sijainnin valitsemisen vapaus mahdollistaa läheisen sijainnin asiakkaasta, jolloin viive palveluntarjoamisessakin pienenee (Kumar ja Vidhyalakshmi 2018).

Hybridipilvessä infrastruktuuri on yhdistelmä edellä mainittujen käyttöönottomallien infrastruktuureja. Hybiridipilvessä nämä infrastruktuurit pysyvät itsenäisinä, mutta ovat keskenään sidottuja erilaisten teknologioiden avulla joka mahdollistaa tiedon ja sovelluksen siirrettävyyden (Grance ja Mell 2011). Hybridipilveä käytetään tapauksissa, jossa täytyy yhdistellä mallien eri ominaisuuksia. Etuina on esimerkiksi tietoturvan ja vaatimusten saavuttaminen matalalla kustannuksella. Organisaatiot voivat hyödyntää julkisen pilven skaalautuvuutta ja kustannustehokkuutta paljastamatta arkoja tietoja ja sovelluksia erilaisille tietoturvauhkille (Kumar ja Vidhyalakshmi 2018). Datan lokalisaaatioon liittyvät lait tai vaatimukset saattavat olla yksi syy valita hybridipilvi, sillä pilvipalveluiden datakeskuksia ei ole tällä hetkellä kaikissa maissa. Datan tallentamiseen voidaan käyttää yksityistä pilveä, ja järjestelmän muiden osien suorittamiseen käyttää julkisen pilven resursseja (Shrivastwa 2018). Pilvipurske (cloud bursting) on myös yksi tärkeä skaalautuvuuden mahdollistava hybridipilven käyttötapaus. Yksityisessä pilvessä pyörivä sovellus voi liikenteen kasvaessa käyttää apunaan julkisen pilven resursseja. Tämänkaltaisen hybridipilven käyttöönottaminen saattaa vaatia hankalaa sovelluksen suunnittelua, mutta se on yksi tapa pidentää yrityksen omistaman konesalin käyttöikää (Hirway 2018).

3 Pilvipalveluiden suosion syitä

Eri pilvipalveluille on yleistä on-demand-malli, jossa käyttäjä maksaa vain tarvittavasta palvelimen käytöstä (Amazon Web Services 2022). Palvelut ovat yleensä myös hyvin skaalautuvia, jolloin niiden suorituskykyä ja tehoa voidaan muuttaa lähes milloin vain. Näin hintaluokkaankin voidaan itse vaikuttaa tehovaatimusten myötä. Käytön mukainen laskutus (Pay-as-you-go) on yleinen hinnoittelumalli pilvipalveluille, joten ne ovat myös yrityksille myös yleensä halvempia kuin konesaliratkaisut. Matalat kustannukset ovat tärkeä ominaisuus ja ne johtuvat monista eri tekijöistä. Pilvipalvelut myös parantavat liiketoiminnan ketteryyttä ja antavat yrityksille ketteryyttä mukautua asiakkaan tarpeisiin. Teknologiapäivitykset tulevat ajallaan ja ilman- tai pienellä ihmisinteraktiolla (Kumar ja Vidhyalakshmi 2018).

3.1 Hinnoittelu

Pilvipalveluissa on yleistä kolme erilaista hinnoittelumallia: käytön mukaan maksettavat palvelut, on-demand-hinnoittelumalli sekä spot-hinnoitellut palvelut (Nicola 2020). Käytön mukaan maksettavissa (Pay-as-you-go) palveluissa yritys maksaa käytetyistä resursseista vain ajankäytön tai resurssien määrän ja kuorman mukaisesti (Kumar ja Vidhyalakshmi 2018). Yleisin AWS:n käyttämä hinnoittelumenetelmä koostuu vakiohinnasta, johon lisätään ajankäyttöön perustuva hinta (Nicola 2020). On-demand hinnoittelumallissa hinnoittelu koostuu ajankäytöstä ja vakiohinnasta, mutta kokonaisajankäyttö on pienempi, sillä resurssit otetaan käyttöön vain tarvittaessa, jonka jälkeen ne luovutetaan. Tämän niistä ei tarvitse enää maksaa (Nicola 2020). Kolmas hinnoittelumalli on spot-hinnoittelu, jossa resurssit hyödyntävät muiden käyttäjien käyttämättömien resurssien suorituskykyä. Tässä mallissa hinnat ovat mukautuvia ja tarjoavat jopa 90 % säästön normaaleihin instansseihin verrattuna (Amazon Web Services 2022). Tämänlaiset maksutavat mahdollistavat yrityksen keskittyvän muuhun liiketoimintaan kuin IT-infrastruktuurin kuluihin. Käytön mukaan maksettavat palvelut myös parantavat kulujen ennustamista (Kumar ja Vidhyalakshmi 2018). Rahallinen riski pilvipalveluhankinnassa on myös huomattavasti pienempi on-premise-ratkaisuihin verrattuna (Bauer ja Adams 2012).

Pääomamenot pienentyvät. Klassisen mallin ohjelmiston käyttöönottoon kuuluu laitteistojen osto, asennus, ylläpito ja päivitykset. Ostotapahtumiin menee paljon kuluja, joten ostajan täytyy myös huomioida esimerkiksi fyysisten tilojen turvallisuus. Pilvipalveluiden kanssa täytyy vain käyttää web-selainta (Grance ja Mell 2011). Kulut tulevat käytetyistä palveluista. Jos yritys kuitenkin jo omistaa konesalin tai resurssien käyttö on tasaisen vaativaa voi joissain tapauksissa olla oma konesaliratkaisu halvempi kuin pilvipalveluiden käyttäminen. Palveluiden resursseissa on myös parempi hyötysuhde (Kumar ja Vidhyalakshmi 2018). Klassisissa vaihtoehdoissa suurin osa resursseista on käyttämättöminä ja arvioitu palvelinresurssien käyttö on n. 5-15 % niiden kokonaiskapasiteetistä. Amazon Web Services (2022) tarjoaa myös spot-instansseja, jotka ovat halvempia, mutta ne ovat tarkoitettu käyttöön, jossa sovelluksen suoritusajankohta voi olla joustava ja mahdollisesti keskeytyvä. Tämä parantaa resurssien hyötysuhdetta.

Liiketoiminnan jatkuvuus on myös parempi. Pilvipalvelun tarjoajilla on käytössä katastrofista palautumisprosessit. Varmuuskopiointeja suoritetaan eri aikavälein riippuen tietojen tärkeydestä ja palvelutasosopimuksesta (Carstensen, Morgenthal ja Golden 2012). Automaattiset vikatilanteiden korjausprosessit parantavat myös liiketoiminnan jatkuvuutta pienennetyin kustannuksin. Palvelut ovat myös hyvin luotettavia varmuuskopioiden ja automatisoitujen prosessien takia (Kumar ja Vidhyalakshmi 2018). Liiketoiminnan jatkuvuuden varmistamiseksi pilvipalveluita valittaessa ei kuitenkaan tule valita automaattisesti suurinta palveluntarjoajaa. Palvelutasosopimus ja sen sopiminen yritykselle on varmistettava. Yleensä pienemmät pilvipalveluntarjoajat ovat mukautuvampia ja mahdollistavat enemmän räätälöintiä liiketoiminnan jatkuvuuden varmistamiseksi (Carstensen, Morgenthal ja Golden 2012). Tämä on tärkeää, sillä pilvipalveluihin siirryttäessä on yrityksen riippuvuus palveluntarjoajasta hyvin suuri.

Pilvipalvelut pienentävät myös hiilijalanjälkeä. Klassisissa vaihtoehdoissa resurssien jaettavuus on huonompaa ja jäähdytysjärjestelmät on yleensä kovin raskaita. Pilvipalveluiden useampikäyttöisten resurssien ja luonnollisten jäähdytyskeinojen takia ne ovat paljon ekologisempia ratkaisuja (Kumar ja Vidhyalakshmi 2018). Amazon Web Services (2022) kertoo pilvipalveluihin siirtymisen pienentävän hiilijalanjälkeä 88 % klassisiin ratkaisuihin verrattuna. Pilvipalveluntarjoajat saattavat käyttää esimerkiksi pelkästään uusiutuvia energianläh-

teitä palveluiden ylläpitoon.

3.2 Saatavuus ja luotettavuus

Luotettavuus tarkoittaa mukaan toimintavarmuutta ja tasaista suorituskykyä. (Kumar ja Vidhyalakshmi 2018) Luotettavuus ja saatavuus ovat termejä, jotka usein kulkevat käsi kädessä. Saatavuutta voidaan mitata ajallisesti jakamalla saatavilla ollut aika kokonaisajalla. Tässä tavassa käytetään yksikkönä yleensä kuukautta tai vuotta. Saatavuutta voidaan myös mitata kutsujen ja vastausten perusteella. Esimerkiksi 99,99 % saatavuus tarkoittaa maksimissaan 52 minuutin häiriöaikaa vuodessa. Bauer ja Adams (2012) kertoo kaksi yleisintä redundanssin lisäämistapaa: kuormanjakaminen (load sharing) sekä aktiivisen valmiustilan (active-standby) lisääminen. Kuormanjakamista yleensä kutsutaan "N + K" kuormanjakamiseksi. "N" kertoo pienimmän resurssien määrän, jolla kuormaa pystytään palvella, kun taas "K" kertoo redundanssiresurssien määrän, jotka ovat lisäresursseina. Esimerkiksi useiden suurien lentokoneiden moottorit ovat suunniteltu N + 1 redundanssilla. Jos yksi moottori sammuu, voi lentokone vielä lentää. Tällaista kuormanjakamista, jossa redundanssiresurssit "K" ovat koko ajan päällä, kutsutaan active-active-malliksi (Bauer ja Adams 2012). Redundanssiresurssi "K" voidaan myös käynnistää vasta ensimmäisen "N" resurssin vioittuessa, jolloin palautumisaika on hieman pidempi. Tämä vaihtoehto on kuitenkin muita malleja halvempi. Active-standby-mallissa redundanssiresurssit eivät aktiivisesti palvele käyttäjiä, mutta ovat osittain käynnissä. Resurssien käyttöönoton nopeutta kuvataan yleensä termeillä "hot standby" "warm standby" sekä "cold standby" (Bauer ja Adams 2012).

Saatavuutta voidaan parantaa myös jakamalla resurssit eri saatavuusalueille (Amazon Web Services 2022). Saatavuusalue tarkoittaa alueen (region) sisällä fyysisesti eri sijainnissa sijaitsevaa datakeskusta (Microsoft 2022). Fyysisesti eri sijainneissa olevat datakeskukset mahdollistavat sen, että samaan aikaan tapahtuvien häiriöiden todennäköisyys on hyvin pieni. Saatavuusalueita voi olla useita yhden alueen sisällä. Amazon Web Services (2022) palvelutasosopimus lupaa AWS:n alueille 99,99 % saatavuuden. Pilvijärjestelmän resurssit voidaan jakaa usealle saatavuusalueelle, ja jotkin pilvipalveluntarjoavat saattavat tehdä niin automaattisesti esimerkiksi tallennetussa datassa sen saatavuuden varmistamiseksi (Pearson 2013). Jos kaksi resurssia jolla on 99,9 % saatavuus sijoittaa kahdelle eri saatavuusalueel-

le niin että molemmissa saatavuusalueissa on yksi resurssi, on näiden yhteinen saatavuus 99,9999 % (Amazon Web Services 2022). Useammalle resurssille liikenteen jakamista kutsutaan kuormantasaamiseksi (load balancing).

Microsoft (2022) mukaan Azure-pilvipalveluiden sisäiset saatavuusalueet ovat keskenään yhdistettyinä erittäin nopealla verkolla, jossa edestakainen viive on alle 2ms. Tämä mahdollistaa nopean tietojen synkronoinnin ja saatavuuden, jos jokin vika ilmenee. Skaalautuvuus myös parantaa saatavuutta, pienentämällä viivettä mahdollisten liikennepiikkien takia. 500 millisekunnin viiveen lisäys pienentää Googlen liikennettä 20 % ja 100 millisekunnin viiveen lisäys Amazonille pienentää myyntiä 1 % (Bauer ja Adams 2012). Saatavuusalueet ja alueet mahdollistavat myös nopean ohjelmiston käyttöönoton globaalisti eri sijainteihin. Eri sovellusversioita voidaan tarjota eri puolille maailmaa ja esimerkiksi maanosakohtaisten sovelluksversioiden viive pysyy pienenä. Varmuuskopioita voidaan myös säilyttää eri saatavuusalueilla, tai jopa alueilla, jotta saadaan parannettua palautumisprosessia vikojen ilmentyessä (Amazon Web Services 2022). Häiriöistä palautumisprosessista käytetään termiä disaster recovery.

Laitteiston hajoamisen syitä ovat ihmislähtöiset vahingot, laitteiston tuotannossa satunnaiset normaalia heikommat kohdat, kuten juotokset, kuluminen, ruoste, osien vahingoittuminen kuljetuksen aikana, tai liian korkeasta lämpötilasta johtuva rikkoutuminen (Bauer ja Adams 2012). Virtuaalisia vikoja voi myös tulla ohjelmavirheiden myötä (Kumar ja Vidhyalakshmi 2018). Mahdollisia käytännön vikoja laitteistoille ovat suorittimen viat jotka yleensä johtuvat lämpötilasta, HDD-kovalevyt, jotka hajoavat fyysisen levyn pyörimisen takia, muuntajaviat, muistiviat sekä verkkoviat. Laitteiston rikkoutumiselle on siis monia syitä ja niiltä on mahdoton välttyä (Bauer ja Adams 2012).

4 Turvallisuus

Yleisimpiä huolenaiheita pilvipalveluihin liittyen ovat datan säilyttämisen sijaintiin ja turvallisuuteen liittyvät asiat, datan suojeleminen pilvipalveluntarjoajan työntekijöiltä, yrityksen sisäinen käyttäjänhallinta pilvessä sekä toimintakelpoisuusajan varmistaminen (Carstensen, Morgenthal ja Golden 2012). Suuret tietomurrotkin herättävät epäilystä pilvipalveluihin. Palvelu- ja käyttöönottomalleista riippuen on kuitenkin vastuu osittain palveluntarjoajalla ja osittain palveluita käyttävällä asiakkaalla. Tätä pilvipalveluiden vastuun jakamista kutsutaan jaetun vastuun malliksi (shared responsibility model). Pilvipalveluiden turvallisuus ei siis ole pelkästään palveluntarjoajasta kiinni. Itse palveluiden käyttäjillä on suuri rooli turvallisen ympäristön luomisessa. Käyttäjillä tulee olla vahvat salasanat itse pilvipalveluiden käyttäjätunnuksissa, sähköposteissa sekä kaksivaiheiset tunnistautumiset. Myös käyttäjien koulutuksella on suuri merkitys, sillä pilvipalveluiden käyttäjiltä saattaa puuttua osaamista ja tietämystä turvallisesta pilvipalveluiden käyttöönotosta. (Pearson 2013)

Amazon Web Services (2022) kuvailee jaetun vastuun mallia jakamalla turvallisuuden kahteen osaan. Pilven turvallisuus (security of the cloud) ja turvallisuus pilvessä (security in the cloud). Pilven turvallisuus on tässä palveluntarjoajan vastuulla. Tämä koskee laitteistoinfrastruktuuria, verkkoa, sovelluksia ja laitoksia joissa pilvipalvelut pyörivät. Pilvessä oleva turvallisuus taas on asiakkaan vastuulla. Amazon Web Services (2022) käyttää tästä esimerkkinä EC2-instanssia, joka on IaaS-palvelu. Kehittäjät vastaavat EC2-instanssien käyttöjärjestelmistä ja ovat myös vastuussa niiden päivityksistä. Myös käyttöoikeusryhmien määrittely on asiakkaan vastuulla. Microsoft (2022) mukaan Azuren pilvipalveluissa käyttäjien vastuulla on aina data, päätepisteet, käyttäjät ja käyttövaltuuksien hallinta. Turvallisuus ei siis ole pelkästään palveluntarjoajan käsissä, vaan myös asiakkaalla on roolinsa turvallisen pilvijärjestelmän kehittämisessä ja tämä on tärkeä tietää pilvipalveluita käyttäessä.

Yleisen tietosuoja-asetuksen GDPR artiklan 32 mukaan täytyy henkilökohtaista dataa käsitellessä toteuttaa asianmukaiset salaukset, mutta ei anna tarkkoja määritelmiä salauksen toteuttamiselle. McAfee Cloud BU (2015) kertoo että 81,8 % pilvipalveluntarjoajista salaavat datan joka liikkuu käyttäjän ja pilvipalvelun välillä, mutta vain 9,4 % palveluntarjoajista salaavat datan kun se on tallennettuna pilvipalvelussa. Näistä datan eri muodoista käytetään

termejä data in transit sekä data at rest. Tallennetun datan kryptaus jää siis usein asiakkaan vastuulle. Eri asiakasryhmät kuitenkin vaativat tietynlaisia standardeja, säännöksiä ja lakeja. Yksi tällaisista on HIPAA (Health Insurance Portability and Accountability Act), joka määrää potilastietojen ja henkilötietojen käsittelyn liittyviä asioita, kuten kryptausvaatimuksia liikkuvalle ja tallennetulle datalle. Amazon Web Services (2022) ja Microsoft (2022) tarjoavat dokumentteja, jotka kertovat kaikki standardit ja säännökset joita niiden palvelut tukevat sekä ohjeita säännöstenmukaiseen palveluiden käyttämiseen. Näissä ohjeissa kuvaillaan myös mahdolliset auditoinnin, varmuuskopioinnin sekä häiriöstä palautumisprosessin vaatimukset ja käyttöönotto-ohjeet. Näiden dokumenttien myötä on säännöksien käyttöönotto helppoa. Säännöstenmukainenmukainen järjestelmän rakentaminen parantaa pilvijärjestelmän tietoturvaa ja vähentää tietomurtojen riskiä, mutta ei kuitenkaan riitä takamaan turvallisuutta pilvessä.

Datan tallentamiseen pilvessä liittyy myös paljon luottamuskysymyksiä. Esimerkiksi henkilötietojen poistaminen, joka on yleisen tietoturva-asetuksen mukainen oikeus. Pilvipalveluntarjoajat saattavat kopioida dataa useisiin datakeskuksiin saatavuuden varmistamiseksi. On vaikeaa taata, että kopiot sekä varmuuskopiot datasta eri datakeskuksissa varmasti poistetaan (Pearson 2013). Esimerkiksi hybridipilven käyttöönottaminen pienentää luottamukseen liittyviä riskejä datan tallennukseen liittyvissä asioissa (Hirway 2018). Palveluntarjoaja voi myös käyttää tai luovuttaa esimerkiksi henkilötietoja laittomasti asiakkaan tietämättä (Ames 2018). Tallennetun datan salauksen käyttöönotto on yksi keinoista vähentää tietojen väärinkäyttöä. Multi-tenant-malli myös lisää henkilökohtaisten tietojen vuotamisen uhkaa, sillä mallin asiakkuuksien erottavat suojaukset ja salaukset voivat vioittua, jolloin data saattaa olla laajemmin saatavilla kuin yhden asiakkuuden sisällä (Pearson 2013). Virtualisaation myötä voidaan laitteiston resursseja hyödyntää parhaiten käyttämällä virtuaalikoneita. Virtuaalikoneet pyörivät hiekkalaatikoidusti, joka luo eristyksen niiden välille ja siten parantaa laitteiston sisäistä tietoturvaa. Tämä kuitenkin saattaa tuoda uusia turvallisuusriskejä, sillä hyökkääjät voivat purkaa nämä virtuaalikoneiden väliset eristykset ja päästä käsiksi muiden laitteistolla pyörivien virtuaalikoneiden dataan (Ristenpart ym. 2009).

5 Yhteenveto

Tutkimuksessa käsiteltiin pilvipalveluita, niiden ominaisuuksia ja erilaisia tapoja niiden luokitteluun. Pilvipalvelut ovat tapa tuoda ja myydä internetin välityksellä olevia mahdollisesti hajautettuja ja skaalautuvia resursseja. Yksi käsitellyistä luokitustavoista oli palvelumallit: IaaS, PaaS, ja SaaS, jotka ovat tarkoitettu eri tarpeisiin. Nämä mallit jakavat eri tavalla järjestelmän infrastruktuurin osia asiakkaan ja palveluntarjoajan välille ja näin tuovat myös eritasoisia mukauttamismahdollisuuksia. Toisena luokittelutapana on käyttöönottomalli, joka kuvailee tapaa jolla palvelut ovat saatavilla sen käyttäjille ja mahdollistaa kohderyhmien rajauksen. Eri mallien ymmärtäminen onkin kovin tärkeää ennen migraatiota pilvipalveluihin. Tämä ja liiketoiminnan jatkuvuussuunnittelu ovatkin riskikohtia pilvipalveluihin siirryttäessä (Kumar ja Vidhyalakshmi 2018). Esimerkiksi sovelluksen turvallisuustarpeet täytyy tietää, ja käyttöönottomallit ymmärtää jotta palvelut voidaan valita vastaamaan sovelluksen tarpeita. Palvelumalleja valittaessa myös työntekijöiden tietotaito täytyy ottaa huomioon, sillä IaaS-palveluiden käyttöönottaminen vaatii enemmän osaamista ja koulutusta kun PaaS- tai SaaS-palveluiden. Näiden tietotaitojen mittareina voidaan käyttää esimerkiksi palveluntarjoajien omia sertifikaatteja, jotta järjestelmiä pystyy kehittämään tehokkaasti ja turvallisesti.

Seuraavaksi tutkimuksessa esiteltiin syitä, jotka ovat tehneet tällä vuosituhannella pilvipalveluista niin suosittuja. Hinnoittelu on yksi tärkeimmistä syistä siirtyä pilvipalveluihin. Käytön mukaan laskuttaminen, resurssien on-demand-malli, skaalautuvuus ja spot-hinnoitellut palvelut tekevät käytöstä halvempaa, erityisesti jos liikenteen määrä on epätasaista ja ennalta määrittelemätöntä. Jaettujen datakeskuksien myötä myös hiilijalanjälki pienenee. Suosion toisena suurena syynä on niiden saatavuus ja luotettavuus. Pilvipalveluiden suuret ja jaetut datakeskukset mahdollistavat hyvän saatavuuden mahdollistamisen ympäri maailmaa. Myös kuormantasaus mahdollistaa hyvän saatavuuden ja luotettavuuden. Nopea käyttöönotto on hyvin yleistä pilvipalveluille, joten ne soveltuvatkin hyvin esimerkiksi ketterien menetelmien käyttöönottoon. CI/CD putket ovat yksi tapa automatisoida testausta ja mahdollistaa nopea käyttöönotto pilvipalveluissa.

Lopuksi tutkielmassa esiteltiin pilvipalveluiden turvallisuusnäkökulmia. Suurten yritysten tietomurrot ja tietovuodot ovat herättäneet epäilystä pilvipalveluiden luotettavuuteen. Pilvi-

palveluissa on käytössä jaetun vastuun malli, joka jakaa vastuuta palveluiden eri osista asiakkaan ja palveluntarjoajan välille. Pilvipalveluiden turvattomuus johtuukin siis usein niiden käyttäjien tietämättömyydestä. Käyttäjien koulutus ja jaetun vastuun mallin ymmärtäminen on tärkeä osa turvallisen pilviympäristön luomista. Tallennetun datan kryptauksen puute vaatii käyttäjiä ymmärtämään palveluista, jotta kryptaus saadaan käyttöön liikkeessä olevan datan lisäksi, joka oli vakiona suurimmassa osaa pilvipalveluista.

Pilvipalveluissa on hyvät dokumentaatiot eri säädöksien ja standardien käyttöönotosta, joka helpottaa niiden mukaisten järjestelmien käyttöönottoa. Näissä dokumenteissa myös kuvaillaan mahdollisia varmuuskopiointi, auditointi sekä häiriöstä palautumisprosessien vaatimuksia. Varmuuskopiointien ja päivityksien helppous tekevät myös tietoturvan vahvistamisesta helpomman. Tämä on myös yhtenä syynä pilvipalveluiden suosiolle. Nämä kaikki ovatkin ominaisuuksia jotka vähentävät käyttäjien vaivaa, joilla toimintoja saadaan suoritettua. Pilvipalveluiden dataan liittyvät asiat ovat kuitenkin eräänlaisia riskikohtia, sillä ne perustuvat täysin luottamukseen, eikä niitä voi täysin itse hallita. Datan ja sen mahdollisten varmuuskopioiden poistaminen sekä sen laiton käyttö ja luovuttaminen perustuvat täysin luottamukseen, joten julkisen pilven käyttö henkilötietojen tallentamiseen ei välttämättä sovi nollan luoton strategian omaavalle yrityksille. Tällaisissa tapauksissa voidaan käyttää esimerkiksi hybridipilveä, mutta kustannukset luonnollisesti kasvavat.

Pilvipalveluiden suosio tulee todennäköisesti jatkumaan, joten migraatio on-premise-ratkaisuista pilvipalveluihin tulee varmasti olemaan monella yrityksellä edessä, ellei yrityksellä ole esimerkiksi jotain turvallisuuteen liittyvää syytä pysyä omassa konesaliratkaisussa. IT-alan pilvipalvelukoulutuksen, ja mahdollisesti palveluntarjoajien sertifikaattien merkitys täten kasvaa IT-alan henkilöstön kesken. Toivottavasti tämä tulee ainakin osittain tulevaisuudessa koulutukseen osaksi, jotta pilvipalveluiden kehittäminen ja käyttäminen olisi turvallista.

Lähteet

Amazon Web Services, Inc. or its affiliates. 2022. *AWS Documentation.* Viitattu 26. helmikuuta 2022. https://docs.aws.amazon.com/.

Ames, Forrest. 2018. *Data security in cloud computing.* Momentum Press.

Art. 32 GDPR Security of processing. 2016. Viitattu 10. huhtikuuta 2022. https://gdpr-info.eu/art-32-gdpr/.

Bauer, Eric, ja Randee Adams. 2012. *Reliability and availability of cloud computing.*

Carstensen, Jared, JP Morgenthal ja Bernard Golden. 2012. *Cloud Computing : Assessing the Risks.*

Grance, Timothy, ja Peter Mell. 2011. *The NIST Definition of Cloud Computing, SP 800-145.*

Hirway, Manoj. 2018. *Hybrid Cloud for Developers.*

Kavis, Michael J. 2014. *Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS).* John Wiley Sons, Incorporated.

Kumar, Vikas, ja R Vidhyalakshmi. 2018. *Reliability Aspect of Cloud Computing Environment.* Springer Singapore.

McAfee Cloud BU. 2015. “Only 9.4% of Cloud Providers Are Encrypting Data at Rest”.

Microsoft. 2022. *Microsoft Azure documentation.* Viitattu 24. maaliskuuta 2022. https://docs.microsoft.com/en-us/azure/availability-zones/az-overview.

Nicola, Dimitri. 2020. *Pricing cloud IaaS computing services.*

Pearson, Siani, toimittanut. 2013. *Privacy and Security for Cloud Computing.* Computer Communications and Networks.

Ristenpart, Thomas, Eran Tromer, Hovav Shacham ja Stefan Savage. 2009. “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds”. Teoksessa *Proceedings of the 16th ACM conference on Computer and communications security.*

Shrivastwa, Alok. 2018. *Hybrid Cloud for Architects.* Packt Publishing, Limited.