Jami Jantunen

PILVIPALVELUIDEN LUOTTAMUKSELLISUUDEN TODENTAMINEN

Tietojenkäsittelyn koulutusohjelma

2016

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

PILVIPALVELUIDEN LUOTTAMUKSELLISUUDEN TODENTAMINEN

Jantunen, Jami
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Toukokuu 2016
Ohjaaja: Grönholm, Jukka
Sivumäärä: 45
Liitteitä: -

Asiasanat: pilvipalvelut, tietoturva, riskit, luottamus, auditointi

---

Luottamuksen syntyminen pilvipalveluntarjoajan ja pilvipalveluita käyttävän yrityksen välille on erittäin tärkeää. Oli pilvipalvelu, pilvipalveluntarjoaja tai pilvipalvelumalli mikä tahansa tarjolla olevista, liittyy pilvipalveluiden käyttöönottoon aina tietojen luovuttamista kolmannen osapuolen hallintaan. Tietojen luovuttaminen ulkopuoliselle osapuolelle on monelle yritykselle suuri askel, joten pilvipalveluita käyttöönottavalla yrityksellä tulisi olla ainakin hieman luottamusta pilvipalveluntarjoajaan.

Tämän työn tarkoituksena oli tutkia pilvipalveluiden luottamuksellisuuden merkitystä, sekä luottamuksen syntymisen eri vaiheita. Mitä pilvipalveluiden osapuolia pidetään luotettavina ja mitä pidetään suurimpina riskitekijöinä. Työssä arvioitiin myös pilvipalveluntarjoajien luottamuksellisuutta ja tekijöitä, jotka johtavat luottavaan asiakassuhteeseen.

Aluksi esiteltiin, mitä pilvi ja pilvipalvelut ovat ja mitä erilaisia palveluita pilvessä voidaan tuottaa, sekä käytiin läpi eri pilvipalvelumalleja ja pilvipalveluiden hankintamalleja. Tämän jälkeen arvioitiin pilvipalveluihin liittyviä merkittävimpiä riskejä ja niiden taustatekijöitä. Käytiin läpi tekijöitä, jotka tekevät pilvipalveluista luotettavia. Mitkä pilvipalveluiden ominaisuudet toimivat yhtä hyvin, tai paremmin, kuin vastaavissa perinteisissä tietojärjestelmissä. Samalla käytiin läpi miten aiemmin läpikäytyihin riskeihin voidaan varautua ja miten niiden toteutumista voidaan estää.

Lopuksi tutkittiin, miten pilvipalveluiden luottamuksellisuutta voidaan mitata, arvioida tai todentaa. Käytiin läpi eri tapoja saada tietoa pilvipalveluiden tai pilvipalveluntarjoajien sisäisestä toiminnasta, mukaan lukien tietoturva- ja yksityisyyskäytännöt, sekä mahdolliset sertifikaatit tai auditoinnit. Lopuksi tarjottiin myös esimerkkejä, mitä eri tilanteisiin sopivia arviointitapoja voidaan käyttää luottamuksellisuuden arvioinnissa.

AUTHENTICATING THE CONFINDENTIALITY OF CLOUD SERVICES

Jantunen, Jami
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
May 2016
Supervisor: Grönholm, Jukka
Number of pages: 45
Appendices: -

Keywords: cloud computing, information security, risks, confidentiality, audit

---

Creating a sound trust relationship between a cloud provider and a cloud user is extremely important. Using a cloud service always requires giving your own personal information for a third party organization regardless of the cloud services, cloud providers or cloud service models chosen. Giving away the management of your own files for a third party organization is always a big step for any company so there must be some amount of trust included in the use of cloud services.

The purpose of this thesis was to investigate the meaning of trust in using of cloud services and the basis of the trust relationship between a cloud user and a cloud service provider. What aspects of cloud services are considered trustworthy and what are considered to be the biggest risks. The thesis also evaluated the trustworthiness of cloud service providers and the attributes that lead to a healthy and trusting customer relationship.

At first the thesis opened the concepts of cloud, cloud services, cloud service providers and cloud acquisition models and presented examples of what cloud services could include. After the initial introduction the thesis evaluated the major risks, and their backgrounds, affiliated with the use of cloud services. Next the thesis went through the more trusted partitions of cloud computing and how a cloud user could by his best efforts avoid the previously mentioned risks.

In the end the thesis examined how a cloud user could measure, assess or authenticate the trustworthiness of cloud services. The thesis went through different ways to receive information on the internal workings of a cloud service or a cloud service provider including security and privacy policies and the possible certificates and audits performed on the cloud platform. Finally the thesis presented examples of different ways to assess and evaluate the different entities associated with cloud service.

SISÄLLYS

SANASTO

IaaS	Infrastructure as a Service, Infrastruktuuriresurssipalvelu. Infrastruktuuripalveluja pilvestä tarjoava pilvipalvelumalli.
PaaS	Platform as a Service, Alustaresurssipalvelu. Alustapalveluja pilvestä tarjoava pilvipalvelumalli.
SaaS	Software as a Service, Ohjelmistoresurssipalvelu. Sovelluspalveluja pilvestä tarjoava pilvipalvelumalli.
MaaS	Monitoring as a Service, Valvontapalvelu. Valvontapalveluja pilvestä tarjoava pilvipalvelumallit.
MBaaS	Mobile Backend as a Service. Pilvipalvelumalli, joka tarjoaa palveluja mobiilisovelluskehittämisen helpottamiseen pilvestä.
XaaS	'Anything' as a Service. Uusi pilvipalvelumalli, joka tarjoaa mitä tahansa palveluja pilvestä.
SLA	Service Level Agreement. Palvelutasosopimus. Käytetään kuvaamaan palveluihin liittyviä palvelutasotavoitteita.
CSA	Cloud Security Alliance. Voittoa tavoittelematon organisaatio, joka tarjoaa sertifikaatti- ja auditointipalveluja pilvipalveluille.
STAR	Security, Trust & Assurance Registry. CSA:n ylläpitämä rekisteri pilvipalveluntarjoajien tietoturvakäytännöistä.
CAIQ	Consensus Assesments Initiative Questionare. CSA:n ylläpitämä kysely pilvipalveluntarjoajien tietoturvakäytännöistä.
CCM	Cloud Controls Matrix. CSA:n ylläpitämä rekisteri, joka vertaa pilvipalveluntarjoajien tietoturvakäytäntöjä CSA:n tietoturvaoppaan ohjeisiin.
CTP	CloudTrust Protocol. CSA:n ylläpitämä rekisteri pilvipalveluiden sisäisestä toiminnasta.
RSA	EMC Corporationin tietoturvaosasto.
CTA	Cloud Trust Authority. Pilvipalvelu, joka tarjoaa tietoja pilvipalveluiden tietoturvasta.
TaaS	Trust as a Service. Pilvipalvelumalli, joka tarjoaa tietoja palveluiden tietoturvasta.

1 JOHDANTO

Luottamus on elintärkeä osuus pilvipalveluissa. Kaikkien pilvipalveluiden yhteinen tekijä on omien tietojen luovuttaminen ulkoisen kolmannen osapuolen hallinnan alaiseksi. Oli kyseessä sitten sähköposti, sovelluskehitysalusta, toimisto-ohjelmisto tai mikä muu tahansa pilvipalvelu, tiedot kulkevat jossain sen elinkaaren aikana pilvipalveluntarjoajan palvelinten läpi. Mikäli asiakkaalla ei ole tippaakaan luottamusta pilvipalveluntarjoajan toimintaan, voidaan olettaa, että tämä ei tule antamaan tietojaan pilvipalveluntarjoajan haltuun. Luottamuksen tason perusteella pilvipalveluiden asiakkaat voivat itse määritellä, mitä palveluita siirretään pilveen, ja mitä jätetään oman yrityksen paikalliseksi hallittavaksi. Mikäli luottamusta pilvipalveluntarjoajan toimintaan on vain vähäisesti, voi yritys ostaa pilvipalveluna vain esimerkiksi varmuuskopiointia tai testikäyttöön tarkoitettuja ympäristöjä. Jos luottamusta pilvipalveluntarjoajaan löytyy tarpeeksi, voi yritys ostaa lähes koko toimintansa, mukaan lukien työasemat, palvelimet ja verkkoyhteydet, pilvipalveluna.

Pilvipalveluiden luottamuksen kyseenalaistamiseen on monia syitä ja riskejä pilvipalveluiden käytössä on useita. Tulee kuitenkin muistaa, että mikään ihmisen rakentama ja käyttämä järjestelmä ei tule olemaan toiminnaltaan 100 prosenttisen varma kaikilla mittapuilla mitattuna. Myös perinteisillä järjestelmillä on omat ongelmansa, samoin kuin pilvipalveluillakin on omansa. Monilla on mielikuva, että pilvipalvelut ovat tietoturvaltaan heikompia kuin perinteiset palvelinsalit. Pilvipalveluiden data ei kuitenkaan sijaitse kirjaimellisesti pilvessä, vaan hyvinkin samanlaisessa palvelinsalissa, jotka vain sijaitsevat maantieteellisesti eri paikassa. Tulee myös huomioida, että perinteiset palvelinsalitkaan eivät historian aikana ole olleet turvassa tietomurroilta.

Pilvipalveluiden käytössä on myös monia hyviä puolia, jotka ovat omiaan parantamaan luottamusta pilvipalvelun toimintaan. Palveluiden varmuuskopiointi ja kahdentaminen varmistavat, että tietojen lopullinen katoaminen on lähes mahdotonta; palvelutasosopimusten avulla voidaan määritellä vasteajat, joiden puitteissa pilvipalvelun pitää toimia; ja pilvipalveluntarjoajat tekevät kaikkensa, että asiakas saa tilaamaansa palvelua, etteivät ne joutuisi maksamaan ylimääräisiä korvauksia tai joutuisi julkisen häpäisyn kohteeksi.

Pilvipalveluiden luottamuksen todentaminen voi olla asiakkaan näkökulmasta vaikeaa. Pilvipalveluntarjoajien tiloihin voi olla vaikeaa tai jopa mahdotonta päästä tutustumaan, eivätkä palveluntarjoajat voi paljastaa kaikkea pilvipalveluiden sisäiseen toimintaan liittyviä yksityiskohta. Luottamuksellisuuden arviointiin kuitenkin löytyy monia työkaluja. Eri pilvipalveluihin liittyvien osien tai organisaatioiden luottamuksellisuuden arviointiin tulee käyttää eri arviointimekanismeja. Oli kyseessä sitten niinkin yksinkertainen arviointitapa kuin pilvipalveluntarjoajan entisten tai nykyisten asiakkaiden kokemuksien tiedustelu, tai niinkin monimutkainen prosessi kuin pilvipalveluiden auditoijan virallinen akkreditointi, luottamuksellisuuden todentamiseen on keinonsa.

2 PILVIPALVELUT

Pilvipalvelut eli tietotekniikan resurssipalvelut ovat verkkoyhteyden välityksellä tarjottavia tietojenkäsittely- ja -tallennuspalveluita sekä tietoliikennepalveluita. Rajanveto pilvipalveluiden ja perinteisten etäkäytettävien tietoteknisten palveluiden välille on loppukäyttäjän näkökulmasta hankalaa, mutta palveluiden toteuttamisen, riskienhallinnan ja tietoturvallisuuden näkökulmasta on selviä eroja. (Viestintävirasto 2014)

Kuva 1. Esimerkkikuva erilaisista pilvipalveluista. (LE&AS Blog 2014)

Asiaa on helppo havainnollistaa meille kaikille tutun työkalun – sähköpostin – kautta. Monissa organisaatioissa työsähköposti oli pitkään tavoitettavissa ainoastaan omalta työkoneelta. Kaikki viestit sijaitsivat omalla päätelaitteella tai yrityksen tiloissa palvelimella, ja näin ollen työskentely toimiston ulkopuolella oli haastavaa. Yksityiselämässä käytössä olleet sähköpostipalvelut, kuten Gmail, Hotmail ja Luukku, sen sijaan olivat tavoitettavissa miltä tahansa koneelta. Tämä johtuu siitä, että kyseiset sähköpostiohjelmat toimivat keskitetyn pilvipalvelimen kautta. (Hanhirova, 2012)

Sähköpostin kohdalla tapahtunut ilmiö on siirtynyt viime vuosina nopeasti myös moniin muihin työssä käytettäviin sovelluksiin kuten kalenteriin ja tiedostonhallintaan. Pilvipalvelut poikkeavat perinteisistä ohjelmistoista ratkaisevasti siten, että ne toimivat missä tahansa ja millä laitteelta tahansa. Erillisiä laiteasennuksia jatkuvine päivityksineen ei enää tarvita – kaikki työntekoon tarvittavat sovellukset ovat käytettävissä selaimen kautta mobiilisti tai eri päätelaitteilta. (Hanhirova, 2012)

“Pilvi” tarkoittaa tässä yhteydessä datakeskuksista muodostuvaa palvelinten verkkoa, missä tieto liikkuu nopeasti ja varmuuskopioituu jatkuvasti. Käyttäjän ei tarvitse itse määrittää, mihin datakeskukseen tiedon tallentaa – kaikki tapahtuu automaattisesti ja silmänräpäyksessä. (Hanhirova, 2012)

Pilvipalveluilla tarkoitetaan palvelumallia, jossa helposti säädettäviä usean käyttäjän kesken jaettuja tietoteknisiä resursseja tarjotaan tietoverkkojen yli. Yhteydensaanti pilvipalveluun on tehty helpoksi. Palvelun toiminnallisuuksia voidaan kytkeä käyttöön ja pois käytöstä sekä yhdistää toisiin palveluihin nopeasti ja helposti käyttäjän tarpeen mukaan. Pilvipalveluiden käytön ja kuormituksen seuranta on tehty helpoksi ja läpinäkyväksi. Tämä yhdessä helpon resurssien hallinnan kanssa mahdollistaa toiminnan ja kulujen optimoinnin. Pilvipalvelut voidaan luokitella muun muassa sen mukaan, miten muotoiltua palvelua (palvelumallit) tarjotaan ja miten palvelun hankinta on järjestetty (hankintamallit). Pilvipalveluita voidaan tuottaa minä tahansa palvelu- ja hankintamallien yhdistelmänä. (Viestintävirasto 2014)

2.1 Pilvipalvelumallit

Pilvipalvelumallit jaotellaan tyypillisesti useampaan ryhmään ominaispiirteidensä mukaan. Yleisimmin käytetty on jako kolmeen:

- infrastruktuuri palveluna (IaaS),
- sovellusalusta palveluna (PaaS) ja
- sovellukset palveluna (SaaS).

Käytettiin palveluntarjoajien tarjoamista pilvipalveluista mitä hyvänsä, yhteisinä nimittäjinä niillä on edellä mainitut ominaispiirteet:

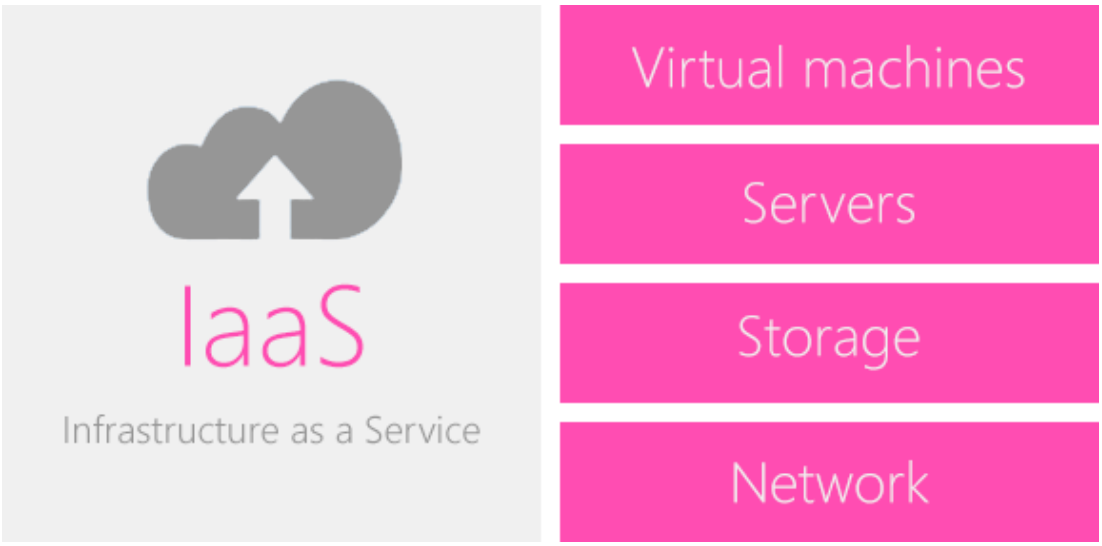
- itsepalvelullisuus,
- pääsy palveluihin eri päätelaitteilla,
- resurssien yhteiskäyttö,
- nopea joustavuus ja
- resurssien käytön tarkka mittaaminen.

Asiakkaan näkökulmasta palvelumalli on selkeä. Käyttäjä maksaa vain tarvitsemistaan skaalautuvista resursseista, joita on käytössä näennäisesti rajoittamaton määrä itsepalveluperiaatteella käyttöön otettavissa ja käytöstä poistettavissa. Ei investointeja, ei kiinteitä laitteistoon, sovelluksiin tai ylläpitoon liittyviä kustannuksia eikä kapasiteettitarpeen etukäteisarviointia tai kapasiteetin loppumisongelmaa. Asiakas maksaa vain siitä, mitä tarvitsee ja saa selkeät raportit resurssikäytöstään. (Salo 2012, 11)

Haasteena pilvipalvelumarkkinoiden palveluntarjoajilla on sama kuin uusien ratkaisujen kohdalla yleensä eli asiakaspotentiaalin vakuuttaminen uuden palvelun hyödyistä. Asiakkaita tällä hetkellä huolettavat tietoturva- ja luotettavuusriskit ovat myös todelliset, ja asiakkaat olisi saatava vakuuttamaan myös näiden asioiden olevan kunnossa. Säännöllisesti uutisoidut luottokortti-, salasana- ja muiden luottamuksellisten tietojen vuodot eivät ole omiaan herättämään luottamusta tietoturvalupauksiin, ja kansainvälisessä kilpailukentässä aiheellisia huolia ovat myös teollisuusvakoilu tai asiakastietojen menettäminen kilpailijoille. Vasta kun palveluiden toimivuus ja luotettavuus ovat riittävän korkealla tasolla, uskaltaa yritysten suuri massa luottaa liiketoimintakriittiset sovelluksensa ja tietonsa niiden haltuun. (Salo 2012, 14)

2.1.1 Infrastruktuuri palveluna (IaaS)

Suurimman toimintavapauden, mutta myös suurimman vastuun käyttäjälle tarjoaa infrastruktuuriresurssipalvelu (IaaS). Palveluntarjoaja yksinkertaisesti antaa asiakkaidensa käyttää laitteidensa laskentatehoa, tallennustilaa ja verkkoyhteyksiä. Asiakas saa itse valita tai toteuttaa kaikki ohjelmistot ja loogiset yhteydet päätelaitteiden käyttöjärjestelmistä lähtien. (Viestintävirasto 2014) IaaS-pilvipalvelussa asiakas ostaa palveluntarjoajan laitteiston resurssit käyttöönsä palveluna. Ostamisen ja omistamisen, tai pitkäkestoisen sitoutumisen, sijasta kapasiteettia voi ottaa jatkuvasti käyttöön tarpeen mukaan. Palveluntarjoajan resurssit ovat usein pitkälle virtualisoidut ja skaalautuminen sekä ylläpito mahdollisimman automatisoitu. Palvelun käyttöä mitataan tarkasti, jolloin laskutus perustuu käytettyihin resursseihin. (Salo 2012, 14)



Kuva 2. Esimerkkejä IaaS pilvipalveluista. (Edmonson 2012)

IaaS-tarjonnan liikkumavapaus ja käyttäjän kontrolli on pilvipalvelumalleista suurin. Asiakkaan mahdollisuudet säätää ja mukauttaa IaaS-pilvipalvelua tarpeidensa mukaisesti ovat suuret. Palveluntarjoaja vastaa resurssiensa toimivuudesta ja turvallisuudesta sekä takaa asiakkaidensa riippumattomuuden toisistaan yhteiskäytetyllä alustalla. Omien ratkaisujensa ja sovellustensa toimivuudesta, päivityksistä, skaalautuvuudesta, kuormantasauksesta ja tietoturvasta vastaa asiakas itse. (Salo 2012, 14)

2.1.2 Sovellusalusta palveluna (PaaS)

Alustaresurssipalvelussa (PaaS) palveluntarjoaja tarjoaa valitsemaansa apuohjelmien ja sovelluskehitysympäristön kokonaisuutta. Palvelun käyttäjä voi toteuttaa alustan päälle omat ohjelmistonsa ja niihin omat tietoturvaratkaisunsa. Palvelun toteuttavien fyysisten- tai virtuaalisten tietojärjestelmien käyttöjärjestelmiin käyttäjät eivät kuitenkaan voi vaikuttaa. (Viestintävirasto 2014)

Kehitystyöstä tulee yksinkertaisempaa, kun ei tarvitse huolehtia infrastruktuurista ja suuri määrä toiminnallisuuksista on saatavilla valmiina moduuleina ja ohjelmointirajapintoina. Lisäksi kolmansien osapuolten tuottamat maksulliset lisäosat tarjoavat laajennus- ja toiminnallisuusmahdollisuuksia. Alustoja käytettäessä kehitystyöstä tulee nopeampaa, kustannustehokkaampaa ja lopputulos skaalautuu massiivisiin käyttäjämääriin saakka ilman lisätyötä. (Salo 2012, 16)

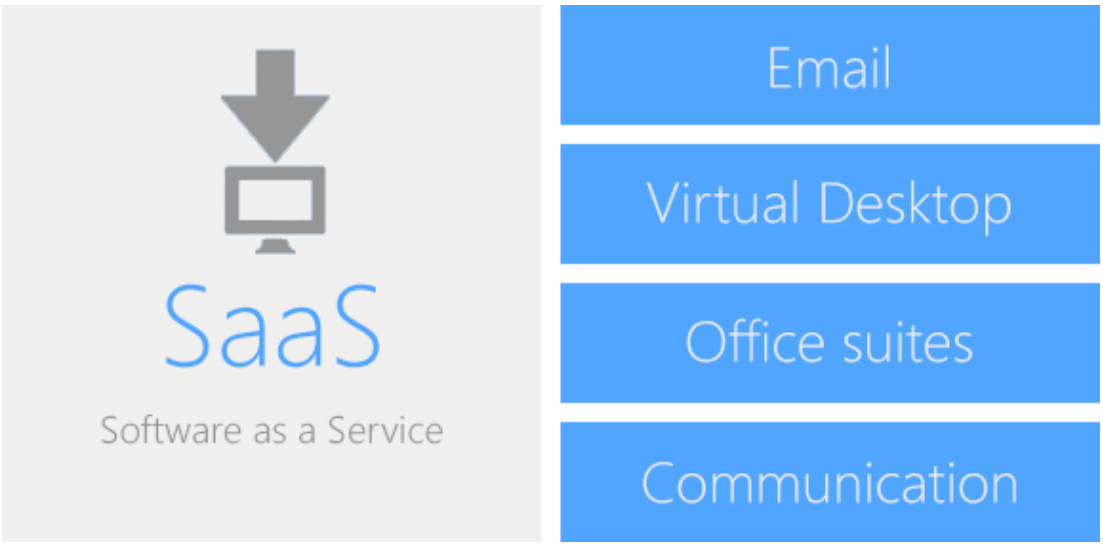
Välitön hyöty sovelluskehitysalustasta yrityksille koituu mahdollisuudesta kehittää omia sovelluksiaan kustannustehokkaasti, nopeasti ja tietoturvallisesti kapasiteettirajoitteesta huolimatta. Sovelluskehitystyön kustannustehokkuus PaaS-pilvipalveluiden avulla mahdollistaa myös pienten uusien toimijoiden saapumisen markkinoille. (Salo 2012, 16)

Kuva 3. Esimerkkejä PaaS pilvipalveluista. (Edmonson 2012)

Sovellusalustat pilvipalveluna muuttavat myös ajattelutapaa, joka sovelluskehitykseen liittyy. Toimintavarmuuteen, skaalautuvuuteen, alustan ylläpitoon ja päivityksiin liittyvät huolet ovat palveluntarjoajan vastuulla ja vain koodin tuottaminen jää yrityksen tehtäväksi. Ketterän sovelluskehityksen menetelmät ovat helposti sovellettavissa ja liikkeellelähtö, kehitystyö ja uusien ideoiden toteuttaminen on helppoa ja nopeaa. (Salo 2012, 16)

PaaS-pilvipalvelut tukevat luonnostaan modulaarista ajattelua, koska niissä tarjooman osa-alueet ovat valmiiksi palvelullistettuja sekä fyysiset resurssit ovat abstraktioiden takana. Käytännössä tämä tarkoittaa sitä, että käyttöön otettaviin SaaS-pilvipalveluihin voidaan helposti rakentaa omia laajennuksia tai kehittää jopa alusta loppuun asti omia sovelluksia kohtuullisin kustannuksin. (Salo 2012, 16)

2.1.3 Sovellukset palveluna (SaaS)



Kuva 4. Esimerkkejä SaaS pilvipalveluista. (Edmonson 2012)

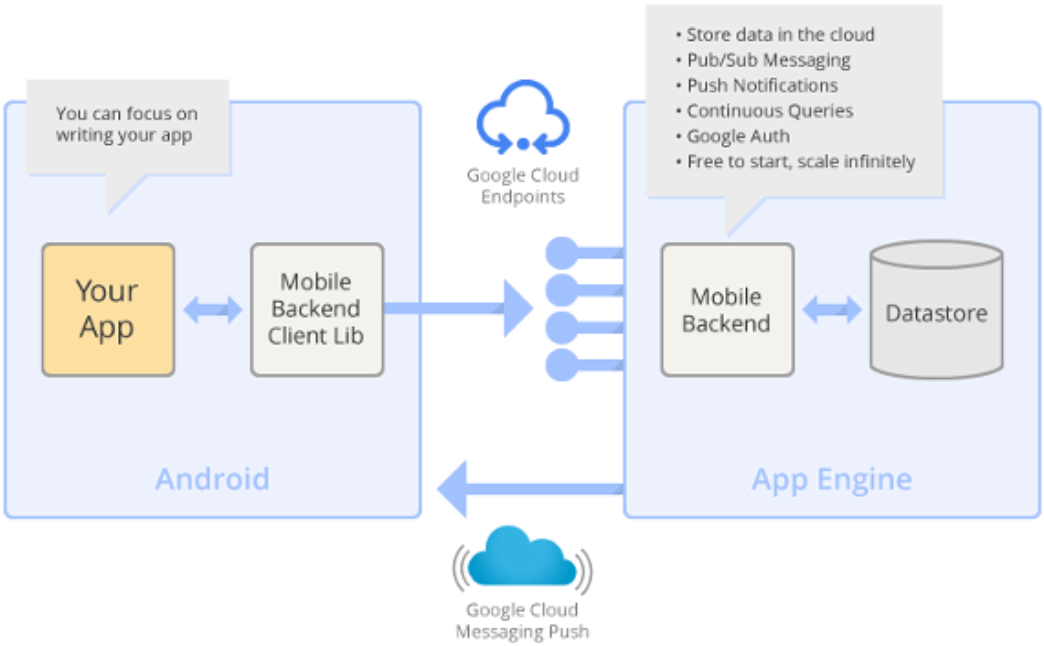
Ohjelmistoresurssi-palvelumalli (SaaS) on yksinkertaisin ottaa käyttöön, mutta toisaalta käyttäjällä on vähän mahdollisuuksia vaikuttaa palvelun toteutukseen ja erityisesti sen tekniseen tietoturvaan. Ohjelmistoresurssipalvelussa palvelun tuottaja antaa asiakkaidensa käyttöön valikoituja verkon yli käytettäviä ohjelmistoja. Tyypillisiä ohjelmistoresurssipalveluita ovat verkkoselaimella käytettävät toimisto-ohjelmistot ja tallennussovellukset. (Viestintävirasto 2014) Omistamisen, asentamisen, ylläpidon ja päivittämisen sijaan yritys ostaa sovellukset käyttönsä tarvittaessa. Perinteisen lisenssimaksun sijaan yritys maksaa esimerkiksi aikaperusteisen, käyttäjä- tai konekohtaisen maksun. Toimintamalli alentaa ohjelmistoihin ja niihin sijoitetun laitteiston pääoman määrää, poistaa ylläpidon ja päivitysten tarpeet ja vapauttaa henkilöresursseja yrityksen kannalta tuottavimpiin tehtäviin. (Salo 2012, 17)

Vaatimustaso palveluna hankittavalle sovellukselle on sitä korkeampi, mitä liiketoimintakriittisempi rooli sillä on. Kriittisimmät sovellukset ja arkaluonteisimmat tiedot ovat viimeiset pilveen siirrettävät, ja osa saattaa olla sellaisia, etteivät pilvipalvelut niiden kohdalla tule kysymykseen. Lisäksi yrityksellä saattaa olla itse tuotettuja tai hankittuja sovelluksia, joille ei löydy vastinetta SaaS-pilvipalveluista, eikä kaikkiin tarkoituksiin ratkaisua ole odotettavissakaan. Tällöin vaihtoehtona on PaaS- tai IaaS-alustalle sovelluksen tuottaminen tai sen pitäminen perinteisessä muodossaan yrityksen omissa tiloissa. (Salo 2012, 17)

2.1.4 Muita pilvipalvelumalleja

MaaS (Monitoring as a Service) on vielä toistaiseksi nouseva pilvipalvelumalli, mutta se on kuitenkin hyvin olennainen osa pilvipalveluiden tulevaisuutta. (Hendryx 2011) MaaS-pilvipalvelut tarjoavat valvontapalveluja, jotka perustuvat pilveen rakennettuun valvontainfrastruktuuriin. MaaS-palveluntarjoaja investoi valvontapuitteisiin, joihin lukeutuvat laitteisto, valvontasovellukset sekä erikoistuneet valvonta-asiantuntijat. Asiakkaan ei tarvitse sijoittaa suuria rahasummia rakentaakseen valvontakeskusta eikä palkata omia valvontaoperaattoreita, vaan kaikki hoituu palveluntarjoajan kautta. Asiakkaan tarvitsee vain maksaa palveluista, joita hän haluaa käyttää - samalla periaatteella kuin minkä tahansa SaaS palvelun kohdalla. Tilauksellaan asiakas saa käyttöönsä valvontakonsolin, johon pääsee käsiksi helposti internetselaimella tai esimerkiksi mobiilisovelluksen avulla. (Altnix 2014)

Mobiililaitteiden yleistymisen myötä on noussut myös mobiilisovellusten kehittämistä helpottava MBaaS (Mobile Backend as a Service, joskus myös pelkkä BaaS – Backend as a Service). MBaaS-pilvipalvelumalli on suhteellisen tuore pilvipalvelumalli, sitä on alettu kehittää vasta vuoden 2011 aikana. MBaaS-pilviapvelumalli on syntynyt ammattitaitoisten mobiilisovelluskehittäjien puutteesta verrattuna yllättävän suureen, erittäin laadukkaiden, mobiilisovellusten kysyntään. Yksinkertaistettuna, MBaaS on kehitetty helpottamaan sovelluskehittäjien työtä. MBaaS pilvipalvelun avulla sovelluskehittäjät voivat liittää tekemänsä sovellukset suoraan pilvipalveluna toimitettavaan tallennustilaan tai laskentatehoon, samalla tarjoten tavallisimpia toimintoja, kuten käyttäjänhallinta, ilmoitusten lähettäminen, sosiaaliseen mediaan yhdistyminen ja monet muut ominaisuudet, joita mobiilikäyttäjät jo suorastaan vaativat mobiilisovelluksiltaan. Jotkut MBaaS-pilvipalvelut tarjotaan asiakkaille suoraan ohjelmistopaketteina, jotka sisältävät MBaaS-palvelun perusominaisuudet, joiden päälle asiakas voi suoraan itse aloittaa oman sovelluksensa kehittämisen. MBaaS-pilvipalvelut jakavat paljon samoja ominaisuuksia PaaS-pilvipalvelumallin kanssa, sillä molemmat on tarkoitettu nopeuttamaan sovelluskehitysprosessia. MBaaS-pilvipalvelumalli on kuitenkin puhtaasti keskittynyt tarjoamaan sovellukselle infrastruktuurin, jossa skaalautuvuus ja optimointi toimii automaattisesti, ja jossa on mukana tärkeimmät mobiilisovellukseen kuuluvat ominaisuudet, joita mobiilisovelluksien kehittäjät ja käyttävät vaativat. (Lane 2013)



Kuva 5. Googlen tarjoama esimerkki Android sovelluskehityksestä käyttäen MBaaS ympäristöä. (Abrams 2013)

Uusimpana pilvipalvelumallina on nousemassa XaaS (Anything as a Service), jossa X tarkoittaa kirjaimellisesti ”mitä tahansa”. ”XaaS” voidaan myös tulkita tarkoittamaan ”Everything as a Service”, eli ”kaikki palveluna”. XaaS-pilvipalvelut yhdistävät normaalisti erikseen toimitettavat pilvipalvelut yhdeksi virtuaalipaketiksi. XaaS-pilvipalvelu voi sisältää yhden tai useamman pilvipalvelumallin tarjoomat samassa palvelussa. XaaS-pilvipalvelu voi esimerkiksi sisältää sovellukset (SaaS), infrastruktuurin (IaaS), sovellusalustan (PaaS) ja valvonnan (MaaS) yhdessä palvelussa. Asiakkaalle XaaS-pilvipalvelu on erittäin helppo ottaa käyttöön, sillä kaikki palvelut löytyvät saman sopimuksen ja palvelun alta. (Kiwaluk 2015)

2.2 Hankintamallit

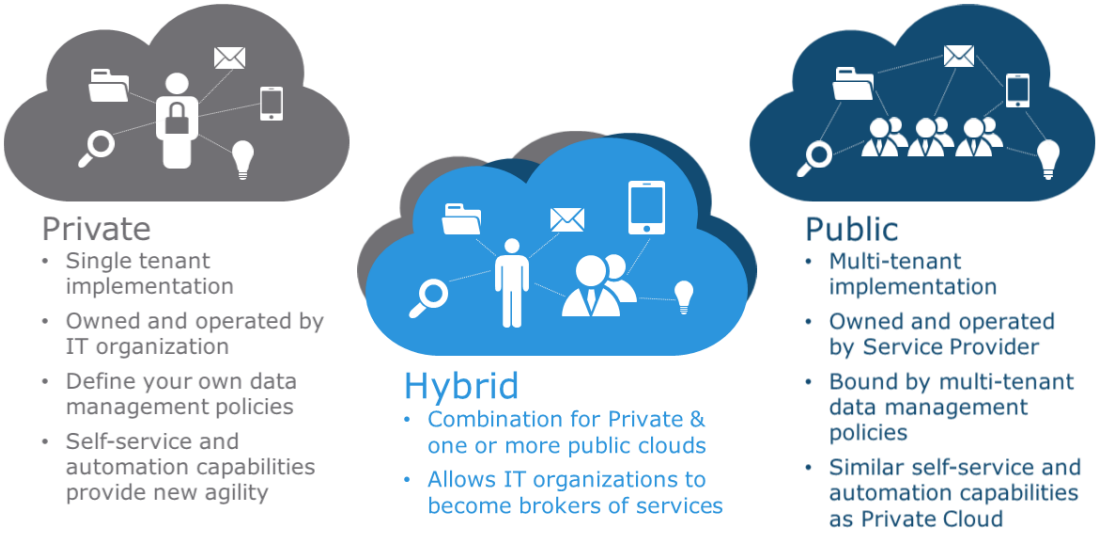
Pilvipalveluiden hankintatapa jaetaan yleensä neljään pääluokkaan:

- yksityinen,
- yhteisö,
- julkinen ja
- hybridi.

Yksityinen pilvipalvelu on tietyn organisaation vain omaan tarpeeseensa hankkima ja käyttämä. Yksityinenkin pilvipalvelu voi olla käyttäjäorganisaation ulkopuolelta hankittu ja tuotettu. Tällaisessa tapauksessa ulkoinen osapuoli tuottaa palvelun yksinomaan sen tilanneelle organisaatiolle. (Viestintävirasto 2014) Yksityisessä pilvessä pilvipalveluinfrastruktuuri on organisaation omistuksessa ja yksin sen käytössä. Hallinnoinnista voi vastata kolmas osapuoli ja laitteisto voi sijaita muuallakin kuin organisaation omissa tiloissa. (Salo 2012, 9)

Yhteisöpilvipalvelun infrastruktuuri on ennalta rajatun organisaatiojoukon omaan tarpeeseensa hankkima ja käyttämä. Käyttäjäyhteisöllä on tyypillisesti yhteisiä tavoitteita tai vaatimuksia pilviratkaisulle. Yhteisöpilvipalvelua voi tuottaa yksi tai useampi yhteisön jäsenistä, jokin kolmas osapuoli, tai näiden yhdistelmä. (Viestintävirasto 2014)

Julkisen pilvipalvelun käyttäjäjoukkoa ei ole ennalta rajattu. Palvelun tuottaja toteuttaa palvelun infrastruktuuria omissa tiloissaan. (Viestintävirasto 2014) Julkisessa pilvessä pilvipalvelut ovat halukkaiden saatavilla maksua vastaan palveluntarjoajan toimittamina. (Salo 2012, 9)



Kuva 6. Eri hankintamallien hyödyt ja haitat (Hybrid Cloud Solutions 2015)

Hybridipilvipalvelussa yhdistetään muilla hankintamalleilla tuotettuja pilvipalveluita käyttäen sovittuja rajapintoja. Osa arkkitehtuurista on yksityistä tai yhteisöllistä ja osa julkista. (Salo 2012, 9) Eräs tyypillinen tapa käyttää hybridipalvelua on yksityinen pilvipalvelu, jonka käsittelykapasiteetin hetkellisesti loppuessa lisäkapasiteettia otetaan käyttöön julkisestä pilvipalvelusta. (Viestintävirasto 2014)

3 PILVIPALVELUIDEN RISKIT

Tilastokeskuksen, vuoden 2015 keväällä, teettämän tutkimuksen mukaan 53 prosenttia suomalaisista yrityksistä käyttää jotain pilvipalvelua. Toimialoittain pilvipalveluita käytettiin eniten informaation ja viestinnän toimialoilla, joissa 84 prosentilla yrityksistä oli käytössä jokin pilvipalvelu. Harvimmin pilvipalveluita käyttivät vähittäiskaupan toimialla toimivat yritykset 34 prosentilla. Yleisimmät pilvipalvelut olivat sähköposti, joita käytti 37 prosenttia yrityksistä, ja tiedostojen tallennustila, joita käytti 30 prosenttia yrityksistä. (Tilastokeskus 2015)

Vuoden 2014 Tilastokeskuksen teettämässä tutkimuksessa yritykset, jotka eivät käytä pilvipalveluja, pitivät useimmin käytön esteenä liian vähäistä tietoa tai asiantuntemusta. Muiksi suurimmiksi syiksi kerrottiin tietoturvariskit, epävarmuudet tietojen sijainnista sekä epävarmuudet oikeudellisissa kysymyksissä. Ongelmaksi monelle yritykselle muodostui myös pilvipalveluiden korkea hinta. (Tilastokeskus 2014)

Taulukko 1. Pilvipalveluiden käytön esteet suomalaisyrityksissä. (Tilastokeskus 2014)

3.1 Pilveen tallennettava tieto

Kaikkiin pilvipalveluihin liittyy tavalla tai toisella datan tallentaminen, käsittely ja liikuttelu. Dataan ja sen säilyttämiseen liittyy myös olennaisia tietoturvahuolia. Käyttäjät haluavat, että tieto on varmassa tallessa siten, etteivät siihen pääse käsiksi tarpeettomasti palveluntarjoajan oma henkilöstö tai ulkopuoliset tahot. Lisäksi lainsäädännöllisistä ja muista syistä asiakkaalla on usein vaatimuksia tiedon säilyttämisen tavoista ja fyysisestä sijainnista. Esimerkiksi henkilötietoja ei haluta välttämättä säilyttää Suomen tai EU-alueen ulkopuolella eikä arkaluonteisia dokumentteja haluta säilyttää salaamattomina missään organisaation ulkopuolella. (Salo 2012, 25)

Pilvipalvelussa tieto on tallennettuna useassa paikassa samaan aikaan eri järjestelmien muistissa, ulkoisissa massamuisteissa tai tietokannoissa. Samaan aikaan se voi olla myös liikkeellä tietovirrassa. Pilvipalveluiden toiminta varmistetaan useimmiten varmuuskopioinnin tai palvelun kahdentamisen avulla. Varmuuskopiointi tarkoittaa yleensä sitä, että palveluiden tietosisältö kopioidaan turvalliseen paikkaan. Palvelun kahdentaminen tarkoittaa koko palvelun replikointia toiseen paikkaan siten, että palvelun on ajan tasalla ja käytettävissä eri paikoissa samanaikaisesti. Pilvipalveluiden varmuuskopiot tai kahdennukset voivat sijaita missä vain maapallolla, missä palveluntarjoajalla tai sen käyttämällä alihankkijalla on oma palvelinkeskus tai muuta siihen vaadittavaa kapasiteettia käytössään. Maantieteellistä hajautusta käytetään palvelun toiminnan varmistamiseksi sekä resurssien kohdentamiseksi. (Viestintävirasto 2014)

Wikileaksin tyyppiset esimerkit ovat osoittaneet, että mikään perinteinenkään järjestelmä ei ole tietosuojaltaan täydellinen ja että useimmiten ihminen on ketjun heikoin lenkki, johtuen joko heikosta salasanasta tai moraalisista kysymyksistä. Pilvipalveluiden kohdalla huoli datan säilymisestä ja turvallisesta säilyttämisestä on kuitenkin perinteisiin ratkaisuihin verrattuna suhteettoman paljon pinnalla. On paljon uutisotsikoihin asti päätyneitä esimerkkejä tapauksista, joissa tahattomasti tai tuottamuksellisesti on vaarannettu asiakkaiden tallentama data. Näkyvän uutisoinnin pitäisi tavallaan kuitenkin vahvistaa asiakkaiden luottamusta. Palveluntarjoajalla on vahva kannustin välttää kaikin keinoin epäonnistumisia, ja toisaalta jokainen epäonnistuminen päätyy suurella todennäköisyydellä julkiseksi referenssiksi kaikkien toimialan toimijoiden opiskeltavaksi. (Salo 2012, 25)

Tietoturvan lisäksi dataan liittyvät saavutettavuus- ja pysyvyyshuolet. Jos yhteyttä pilveen ei saada, ei päästä myöskään käyttämään siellä olevia tietoja. Oli sitten katkoksen syynä tekninen- tai inhimillinen virhe tai luonnonvoimien puuttuminen peliin, useimpien palveluntarjoajien sopimusehdoissa mainittu SLA eli palvelutasosopimus on tyypillisesti 99,95 ja 99,99 %:n välillä, eli se jättää tilaa pienille katkoksille. Yrityksen näkökulmasta pienikin katkos voi tulla kalliiksi. Kuten tietoturvankin kohdalla on saavutettavuuden suhteen hyvä miettiä, mikä on datan arvo ja kuinka suurella varmuudella sen on oltava käytettävissä. Jos minuutinkaan katkokseen ei ole varaa, ei pilvi välttämättä ole oikea paikka sen säilyttämiseen. (Salo 2012, 26)

Kun tietoa poistetaan tietojärjestelmästä tavanomaisin menetelmin, se ei yleensä vain lakkaa olemasta. Käyttöjärjestelmien yleinen toimintamalli on että, kun esimerkiksi tiedosto poistetaan tallennusmedialta, sitä ei pyyhitä pois vaan ainoastaan tieto siitä poistetaan järjestelmän kirjanpidosta. Tiedoston sijainti tallennusjärjestelmässä siis merkitään vapaaksi, jolloin järjestelmä voi käyttää tiedon käytössä olleen tilan muun tiedon tallentamiseen. Poistetuksi merkityn tiedoston sisällön voidaan kuitenkin lukea järjestelmästä niin kauan kuin sen kohdalle levypinnalle ei ole kirjoitettu jotain muuta tietoa. (Viestintävirasto 2014)

3.2 Sopimusehdot, lait ja säädökset

Yhä täsmällisemmin määriteltyjä palvelutaso- ja – sisältölupauksia kirjataan sopimuksiin. Tätä varsinkin suuremmat yritykset odottavat. Yrityskäytössä löyhät sopimukset johtavat sitä isompiin ongelmiin, mitä kriittisemmästä toiminnosta on kysymys. Yksittäisen pienemmän osaston tai yrityksen testikäyttöön tarkoitettu pilvipalvelualusta voi esimerkiksi toimia heikommalla suorituskyvyllä tai väljemmän palvelutasosopimuksen alaisena ja ajaa silti tarkoituksensa. Suuremman yrityksen asiakkuuksien hallinnan, taloushallinnon tai vaikka tuotekehityksen käyttöön tarkoitetut järjestelmät voivat olla liiketoiminnan ydin ja niiden kohdalla sopimustekniset seikat pienintä yksityiskohtaa myöden ovat tärkeitä. (Salo 2012, 32)

Sanktiot palvelutasosopimuksesta poikkeamisesta ovat usein palveluntarjoajalle kohtuullisen lieviä, mutta kirjattuna ne asettavat palvelulle näkyvän riman, jonka alittamisesta palveluntarjoajan liiketoiminta kärsii. Palvelutasosopimuksen rikkomisesta saadut laskuhyvitykset voivat olla asiakkaalle laiha lohtu, jos vahingosta on seurannut liiketoiminta- tai mainevahinkoa. Niiden olemassaolo itsessään kuitenkin lisää luottamusta ja parantaa ennakoitavuutta. (Salo 2012, 30)

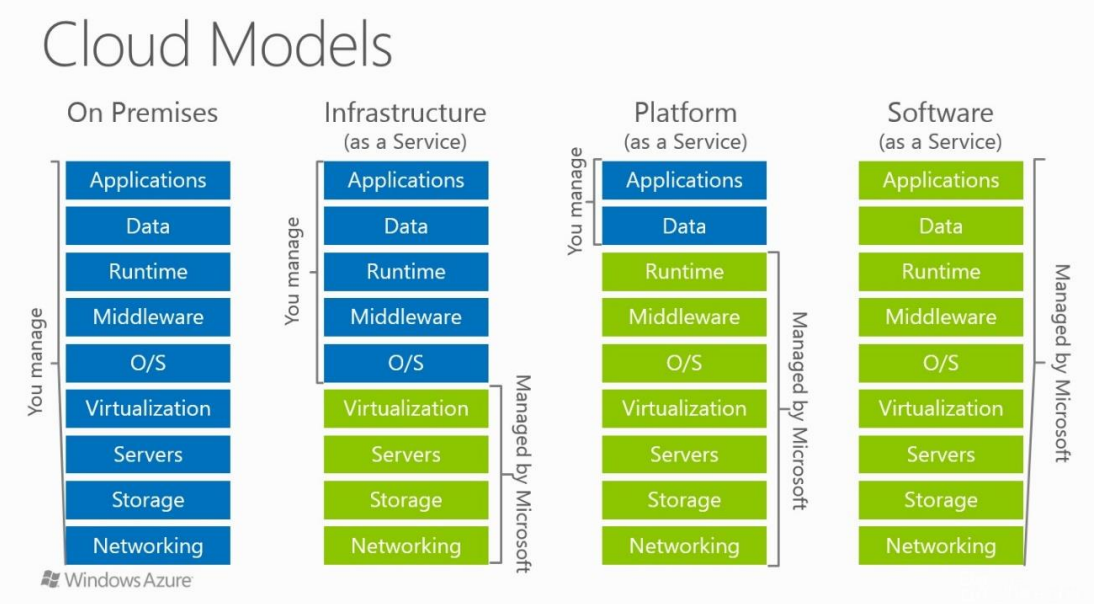
Tietoturvahuolten lisäksi toinen tyypillinen varauksella julkisiin pilvipalveluihin suhtautuvien argumentti ovat lait, asetukset ja erilaiset toimialakohtaiset suositukset ja totutut toimintatavat. Varsinkin henkilötietojen säilyttämistä säädellään tarkoin ja siihen liittyy myös suurta epävarmuutta. (Salo 2012) Jos pilveen tallennetaan henkilötietoja, tulee huomioida henkilötietojen käsittelyyn liittyvä säännöstely. Yleissääntö arkaluonteisen tiedon säilytykseen on, että rekisterinpitäjä ei voi ulkoistaa omaa vastuutaan. (Viestintävirasto 2014)

3.3 Pilvipalveluntarjoaja

Pilvipalveluiden houkuttavuus perustuu luottamukseen. Uutisoinnit käyttökatkoista ja tietoturvaongelmista ovat omiaan murentamaan sitä. Mikään inhimillinen järjestelmä ei ole eikä tule olemaan täysin toimintavarma, ja tämä pätee myös pilvipalveluihin. Virheetöntä vaihtoehtoa ei ole tarjolla ja täydelliseen riskittömyyteen ei liiketoiminnassa koskaan päästä. Pilvipalveluntarjoajat tiedostavat hyvin luottamuksen merkityksen ja pyrkivät markkinointi- ja kriisiviestinnälläänkin herättämään luottamusta, hälventämään epäluuloa ja pienentämään luottamukseen liittyvää riskiä. (Salo 2012, 30)

Pilvipalveluiden turvallisuuteen liittyy yllättävän monta tekijää, jotka eivät välttämättä näy loppukäyttäjälle. Palvelun turvallisuuteen vaikuttaa teknisen toteutuksen lisäksi myös sitä ympäröivä maailma. Esimerkiksi palvelun ylläpitohenkilöstöllä, tai jopa palveluntarjoajan alihankkijoilla saattaa olla pääsy käyttäjän tietoihin. Lisäksi turvallisuuteen vaikuttaa ohjelmistojen, laitteistojen ja fyysisen ympäristön huolto- ja toimittajaketjut. (Viestintävirasto 2014) Usein tietojärjestelmien heikoin lenkki on ihminen,

eivätkä pilvipalvelut poikkea tästä mitenkään. Käyttäjän huolimattomuus, pahantahtoisuus tai tietämättömyys aiheuttavat ongelmia, joihin on hankala varautua etukäteen. (Salo 2012, 28)



Kuva 7. Microsoftin esimerkki eri pilvipalvelumallien vastuualueista (Microsoft MSDN www-sivut)

Useimmiten palveluntarjoaja sanoutuu irti kaikesta vastuusta koskien palveluna käytön asiakkaalle aiheuttamaa välitöntä ja välillistä haittaa. Kärjistettynä tämä tarkoittaa sitä, että jos palvelu jonain päivänä ei enää olekaan olemassa, asiakas vastaa itse toiminnan jatkuvuudesta, eikä saa korvausta mistään menettämästään aineellisesta tai aineettomasta haitasta. Tämä ei luonnollisesti ole palveluntarjoajana liiketoimintaa tekevän tahon tahtotila, mutta heilläkään ei ole kontrollia kaikesta ja myös he kehittävät toimintaansa. Yritys saattaa esimerkiksi tulla ostetuksi ja uuden omistajan myötä toiminta voi muuttua. Palveluntarjoaja voi myös itse muuttaa toimintaansa tai ansaintalogiikkaansa. Mitä paremmin varaudutaan poikkeuksellisiin tilanteisiin, sitä paremmat mahdollisuudet on selviytyä tilanteen osuessa kohdalle. Jos kyseessä on kriittinen tieto, kannattaa siitä pitää varmuuskopio myös muualla kuin pilvessä. (Viestintävirasto 2014)

Palvelun käyttäjän omassa toiminnassa voi myös tapahtua ennakoituja tai ennakoimattomia muutoksia. On hyvä miettiä etukäteen, onnistuuko palveluntarjoajan vaihtaminen siten, ettei siitä koidu kohtuutonta haittaa. Tai jos palvelun käyttö halutaan lopettaa, saadaanko tietoaineisto talteen uudelleenkäytettävässä muodossa tai ylipäätään ollenkaan. Suuri osa palvelun jatkuvuuteen liittyvistä kysymyksistä selviää palvelun käyttöehdoista ja muista toiminnan kuvauksista. Niitä voidaan joissain tilanteissa tarkentaa tai jopa muuttaa palveluntarjoajan kanssa tehtävällä palvelusopimuksella. (Viestintävirasto 2014)

4 PILVIPALVELUIDEN LUOTETTAVUUS

4.1 Tiedon säilyvyys ja poisto

Yrityksen, joka on huolissaan datansa tuvallisuudesta tietosuojamielessä, kannattaa ennen tietojen pilveen siirtämistä arvioida, kuinka liiketoimintakriittisiä ne ovat ja mitä seuraisi, jos ne päätyisivät vääriin käsiin. (Salo 2012, 26) Riski-hyöty-arvioinnilla voidaan analysoida, mitä tietoja pilveen kannattaa siirtää ja mitkä tiedot olisi hyvä säilyttää organisaation omilla paikallisilla palvelimilla. Pilvipalveluiden käyttöönotto ja pilveen tallennettavien tietojen valinta tulisi aina perustua harkittuun päätökseen. Riskianalyysissä tulee ottaa huomioon, että pilvipaleluissa olevaa tietoa tallennetaan tai käsitellään jonkun muun ylläpitämässä palvelussa. Tällaisessa tilanteessa on mahdollista, että tietoa katoaa, vääristyy, tuhoutuu tai joutuu tuntemattoman kolmannen osapuolen haltuun. Organisaatioiden on hyvä harkita tapauskohtaisesti, kuinka suuria nämä riskit ovat ja mitä ne tarkoittaisivat omassa tilanteessa. Onko palvelun käytöstä saatu hyöty suurempi kuin tilanteeseen liittyvä riski? Ovatko kyseessä henkilökohtaiset tiedot vai oma liiketoiminta? Kolmanteen osapuoleen liittyvän riskin vuoksi ei kannata sokeasti laittaa kaikkea dataa ja laskentaa pilveen, vaikka se muutoin olisikin mahdollista. Pilvessä tietojen ja laskennan luottamuksellisuus, eheys, saatavuus tai kiistämättömyys eivät välttämättä ole yhtä hyvällä tasolla kuin tiettyä tarkoitusta varten rakennetuissa tietojärjestelmissä. On siis erittäin tärkeä valita ja rajata pilveen vietävä data ja laskenta, sillä läpikotaisesti ymmärrettyä ja loppuun asti harkittua tietojenkäsittelyä on helpompi hallita. (Viestintävirasto 2014)

Tieto liikkuu eri tallennuspaikkojen välillä varmuuskopioinnin tai muun palveluun liittyvän hallinnollisen toiminnan yhteydessä tai käyttäjän käsitellessä sitä. Tällöin tieto liikkuu valon nopeudella mantereiden välillä ja tietosisältö voi käydä matkansa varrella sijaitsevien tietoliikennelaitteiden välimuistissa. Yhä useammat pilvipalveluiden tarjoajat ovat kiinnostuneet asiakkaidensa tiedon turvaamisesta ja salauksen käyttö palveluiden ja palvelinkeskusten välisessä tietoliikenteessä on yleistymässä. Pilvipalvelun käyttäjän tuleekin varmistaa, missä hänen tallentamansa tieto sijaitsee koko sen elinkaaren aikana. Tiedon sijainnilla on vaikutusta muun muassa seuraavasti:

- Mitä tietoa kyseiseen palveluun saa tallentaa oman maan lakien puitteissa?
- Minkä maan lakia sovelletaan mahdollisissa poikkeustapauksissa?
- Onko jonkin maan viranomaisilla oikeus tutkia tätä tietoaineistoa?

Kuva 8. Googlen konesalien sijainnit kartalla. (Googlen www-sivut)

Jos tiedon maantieteellisellä sijainnilla on merkitystä käyttötarkoituksen kannalta, pitää sijainti selvittää palveluntarjoajan kanssa. Osa suurista palveluntarjoajista pyrkii keskittämän pilvipalveluidensa toiminnan maantieteellisesti siten, että eurooppalaisen käyttäjän tiedot pidetään Euroopassa sijaitsevissa palvelinkeskuksissa. Näissäkin tapauksissa palvelun ylläpitotyötä voidaan tehdä kyseisen maantieteellisen alueen ulkopuolelta. Myös joitain osia asiakkaan tiedoista saattaa tulla tallennetuksi tämän oman kotialueen ulkopuoliseen palvelinkeskukseen, jos asiakas esimerkiksi itse käyttää palvelua oman kotialueensa ulkopuolella. Palvelinkeskuksia sijoitetaan maantieteellisesti hajalle ja asiakkaiden tiedot kopioidaan useampaan kuin yhteen keskukseen erityisesti

siitä syystä, että jos yksi piste lakkaa toimimasta, palvelu voidaan keskeytyksettä tarjota toistaiseksi toisesta palvelinkeskuksesta. Samoin tällä voidaan jakaa tietoliikenteen kapasiteettia ja ratkaista varmuuskopiointiin liittyviä ongelmia. (Viestintävirasto 2014)

Palvelinkeskuksien sisällä eri asiakkaiden tiedot voidaan erottaa pilvipalveluissa toisistaan loogisesti tai fyysisesti. Erottelu voidaan tehdä niin asiakkaan käyttämälle palvelun toimintalogiikalle kuin siinä käsitetylle ja tallennetulle tiedollekin, jos ne ovat toisistaan erillä. Erottelua voidaan tehdä esimerkiksi seuraavin tavoin:

1. Usea asiakas käyttää samaa ohjelmistoa, mutta niiden käyttöympäristö on erotettu toisistaan ohjelmallisesti pääsynhallinnan avulla.
2. Jokaisella asiakkaalla on käytössä oma instanssi käytettävästä ohjelmasta ja ne toimivat samalla virtuaalisella tai fyysisellä palvelimella.
3. Jokaisella asiakkaalla on käytössä oma instanssi ohjelmasta, joka toimii omalla virtuaalisella tai fyysisellä palvelimella.

Fyysinen erottelu (kohta 3.) on näistä turvallisin. Loogisesti erotellussa ympäristössä on riski että asiakkaiden tietosisältö paljastuu toiselle asiakkaalle tai kolmannelle osapuolelle esimerkiksi ohjelmistovirheen, virheellisen asetuksen tai muun ylläpitotoimen johdosta. (Viestintävirasto 2014)

Tiedon poistamisen yhteydessä on hyvä varmistua tiedon todellisesta tuhoamisesta. Jotta tiedon poistamisesta voidaan varmistua, tieto pitää poistaa erillisellä ohjelmistolla, joka ylikirjoittaa poistettavan tiedon kohdan levypinnasta satunnaisilla merkeillä. Pilvipalveluissa noudatetaan erilaisia käytäntöjä asiakkaan tiedon tuhoamisen suhteen. Kannattaakin tarkistaa, mitä tiedolle oikeasti tapahtuu, jos asiakassuhde päättyy tai tapahtuu jokin muu poikkeuksellinen tapahtuma, joka vaikuttaa palveluntarjoajan toimintaan. Allokoidaanko asiakkaalta käyttöön vapautuneet resurssit seuraavalle käyttäjälle vai puhdistetaanko ne ensin vanhasta tiedosta ylikirjoittamalla tai muulla tavalla. Kannattaa selvittää, miten elinkaarensa päähän tullut pilvipalvelun fyysinen laitteisto, johon on tallennettu asiakkaan tietoja, poistetaan käytöstä: ylikirjoitetaanko laitteistojen tietosisällöt turvallisesti, tuhotaanko ne mekaanisesti vai laitetaanko ne suoraan kiertoon. (Viestintävirasto 2014)

4.2 Tiedon omistajuus ja käyttöoikeudet

Pääsääntö on, että tiedon omistajuus ja siihen liittyvät oikeudet ovat sillä henkilöllä tai organisaatiolla, joka on tuottanut tiedon alun perin esimerkiksi laatimalla pilveen tallennetun asiakirjan. Käyttöoikeudet määräytyvät sovellettavan lainsäädännön ja sopimusten perusteella. Palveluntarjoajan kanssa on hyvä sopia palveluehdoista tarkasti ja palvelun ehdot on hyvä lukea huolella. Erityisen tärkeää on huomioida tiedon hallintaan ja käsittelyoikeuteen liittyviä seikkoja. Jos yritys säilyttää pilvessä muun tiedon ohella myös liikesalaisuuksiaan, on varmistettava etteivät henkilöt, joilla ei ole oikeutta käsitellä näitä tietoja, pääse niihin käsiksi. Käsittelyoikeuksien säilyminen vain organisaatioilla itsellään on hyvä varmistaa sopimuksin. (Viestintävirasto 2014)

Turvallisen palvelun tärkeimpiä ohjelmistolle asetettavia vaatimuksia on, että käyttäjänhallinta on toteutettu luotettavasti. Tähän kuuluu palveluun rekisteröinti, rekisteröidyn käyttäjän tunnistaminen sekä käyttöoikeuksien hallinnointi. Käyttäjänhallinan tärkein tehtävä on jakaa palvelun, ja niin ikään tiedon, käyttöoikeuksia niille henkilöille, joille se kuuluu. Samalla se estää muita henkilöitä pääsemästä käsiksi tietoon, joka ei heille kuulu. Pääsynhallintaan sekä käyttöoikeuksien jakamiseen käytetään yleensä omaa käyttäjänhallintaan käytettävää tietokantaa tai järjestelmää tai käyttäjätunnukset luodaan paikallisesti itse pilvipalveluun. Molemmissa toimintamalleissa on tärkeää että tunnusten luominen ja käyttöoikeuksien jakaminen on mahdollista vai siihen erikseen valtuutetuilla henkilöillä. Näiden henkilöiden tulee tietää, millä perusteella oikeuksia jaetaan ja kuinka nämä henkilöt tulee tunnistaa ennen tunnusten tai oikeuksien aktivointia. (Viestintävirasto 2014)

Palvelua käyttöönottavan organisaation voi olla järkevää sisällyttää sopimukseen mahdollinen auditointioikeus sen tarkastamiseen, että yrityksen tietoja käsitellään laaditun palvelusopimuksen mukaisesti. Arkaluonteisen tai salassa pidettävän tiedon käsittelyyn tulee kiinnittää erityistä huomiota. Tällöin arvioitavaksi voi tulla myös se, pitääkö yrityksen ja palveluntarjoajan välillä solmia salassapitoon liittyvä oma salassapitosopimus. (Viestintävirasto 2014)

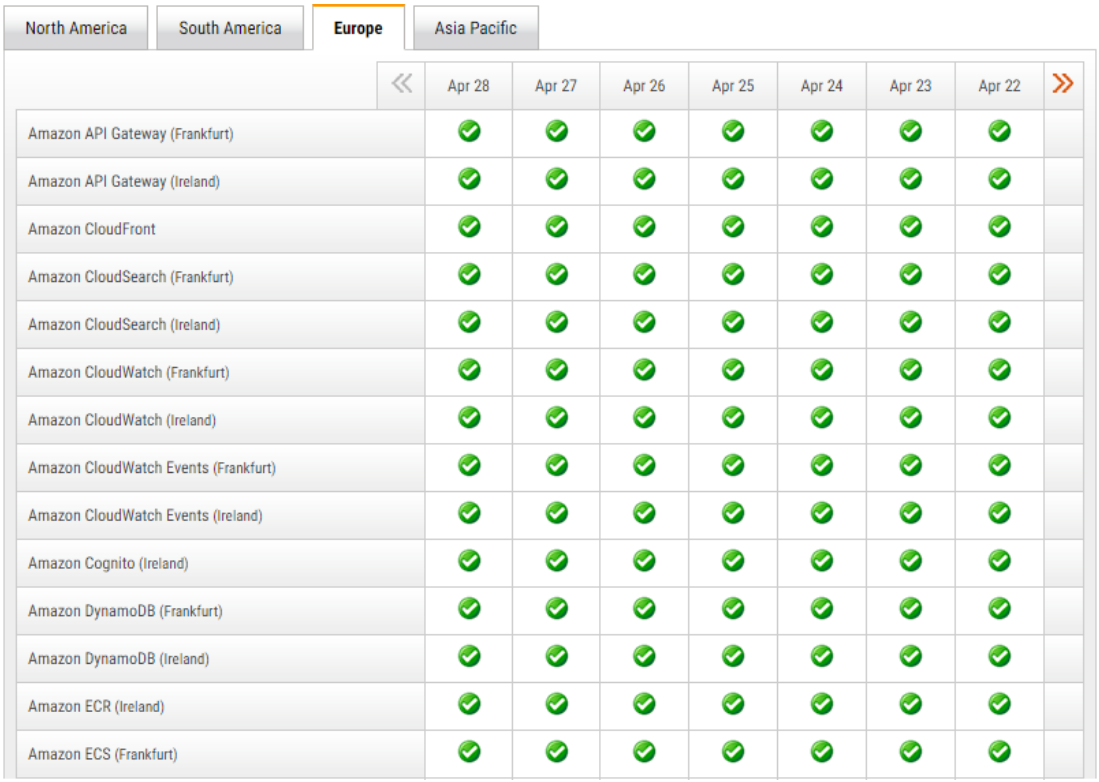
4.3 Sopimukset

Pilvipalvelun käyttöönotossa erilaisiin tilanteisiin voidaan varautua myös sopimuksilla. Palvelun riskiarviossa tunnistetut uhkat ja rajoitteet voidaan huomioida palvelun käyttöönottoon liittyvässä sopimuksessa. Palveluntarjoajan kanssa voidaan sopia esimerkiksi vaatimuksista ja mahdollisista sanktioista uhkatilanteisiin ja varautumiseen liittyen. (Viestintävirasto 2014)

Pilvipalveluihin voi tallentaa lähes rajattomasti ja mitä vain tietoa, kunhan tallennettu tietoaineisto ei loukkaa pilvipalveluntarjoajan sopimusehtoja, lainsäädäntöä tai muita sopimuksia, joihin pilvipalvelun käyttäjäorganisaatio on sitoutunut. Pilvipalveluiden tarjoajat asettavat palveluiden käytölle sääntöjä ja rajoituksia. Näitä ovat muun muassa kiellot käyttää palvelua laittomiin tai moraalittomiin tarkoituksiin sekä rajoitteet palvelun resurssien käyttöön. Säännöt ja rajoitukset ovat aina palvelukohtaisia. Niitä voidaan tarkentaa palvelusopimuksessa tai palvelun käyttäjä hyväksyy ne käyttöehtoina rekisteröityessään. Pilvipalveluiden käyttöä rajoittavat lähinnä sopimusehdot ja osaltaan myös lainsäädäntö. Näiden soveltuvuutta tulee arvioida kuitenkin aina tapauskohtaisesti. Pilvipalveluiden käyttöön ryhdyttäessä organisaation on hyvä varmistaa myös omat muut sopimusvelvoitteensa. Sopimukset voivat rajoittaa esimerkiksi tietojen siirtämistä ulkomaille. Jos käyttöön suunnitellun järjestelmän on toteutettava jonkin kriteeristön mukainen suojaus- tai turvallisuustaso, täytyy ensin tutkia täyttääkö käytettäväksi suunniteltu pilvipalvelu nämä vaatimukset. (Viestintävirasto 2014)

Pilveen tallennettuun tietoon liittyvät käsittely- ja käyttöoikeudet määräytyvät erityisesti sopimusten perusteella. Käsittely- ja käyttöoikeuksista on syytä varmistua siis sopimalla. Näin voidaan varmistaa käyttöoikeuksien pysyminen organisaatiossa, ja mahdollisesti palveluntarjoajankin puolella, vain tietyillä henkilöillä. Organisaation on syytä kiinnittää erityistä huomiota esimerkiksi salassa pidettävän ja arkaluonteisen tiedon käsittelyoikeuksiin. Palveluntarjoajan salassapitovelvollisuudesta voidaan laatia tarvittaessa myös oma salassapitosopimuksensa. Sopimusten avulla pyritään useimmiten varautumaan poikkeaviin tilanteisiin. Riskiarvioinnissa poikkeavat tilanteen tulee arvioida ja niihin varautuminen voidaan huomioida sopimuksellisin keinoin. Sopimuksissa on hyvä ottaa huomiin myös tilanteet, joissa palveluntarjoajan toiminta jostain syystä tulee epävarmaksi tai katkeaa. Pilvipalvelut käyttöönottavan yrityksen on hyvä

varmistaa, että heillä on pääsy pilvipalveluihin tilanteessa, jossa palveluntarjoajan toiminta syystä tai toisesta lakkaa. Tällöin tietojen siirrettävyyteen ja jatkuvuuden turvaamiseen on hyvä kiinnittää huomiota. (Viestintävirasto 2014)



Kuva 9. Amazon Web Services -palvelujen palvelutasohistoriaa voi seurata internetissä. (Amazon Web Services www-sivut, 2016)

Omat vaatimukset palvelun toiminnalle tulee myös huomioida. Nämä määritellään yleensä palvelutasosopimusten (englanniksi Service Level Agreement tai SLA) avulla. Palvelutasosopimuksessa voidaan kuvata paremmin palveluihin liittyvät palvelutasotavoitteet ja yksilöidä palveluntarjoajan ja asiakkaan vastuut. Palvelutasosopimuksessa voidaan määritellä erilaisia mittareita ja tavoitteita, joiden alittamisesta voi seurata sanktio. Tyypillisiä palvelutasosopimusten avulla määriteltäviä tavoitteita ovat esimerkiksi:

1. Kuinka suuren osan ajasta palvelun luvataan toimivan ja minkälaisilla vasteajoilla?
2. Minkä tasoista käyttäjätukea on saatavilla ja minkälaiset vasteajat ovat eri viikonpäivinä ja vuorokaudenaikoina?
3. Missä tietoa säilytetään ja mistä sitä voidaan ylläpitää? (Viestintävirasto 2014)

4.4 Lainsäädäntö

Kotimaistenkin pilvipalveluiden osalta on hyvä varmistaa palvelinten sijaintimaa. Jos palvelu on osittain tai kokonaan toteutettu ulkomailla siihen saattaa kohdistua myös ulkomaisten lainsäädännön asettamia vaatimuksia. Ulkomaiset palveluntarjoajat luonnollisesti suosivat oman maansa lainsäädäntöä myös riitatilanteissa. Pilvipalveluita käyttöönottavan organisaation näkökulmasta helpointa on laatia palvelusopimukseen lauseke, jolla sovellettavaksi lainsäädännöksi asetetaan oma kansallinen lainsäädäntö ja riitatilanteiden varalle toimintavaltainen tuomioistuin on määritelty sopimuksessa. Organisaatioiden ja palveluntarjoajien välisissä sopimuksissa tällaisesta voidaan mahdollisesti jopa sopia. Tilanne on hankalampi kuluttajapalvelusopimukissa, joissa sopimusten ehdot on useimmiten ennakkoon määritelty, eikä niihin voi ehdottaa muutoksia. Suuremmat palveluntarjoajat käyttävät useimmiten vakiosopimuksia, kun taas pienemmät palveluntarjoajat voivat olla palveluissaan ja sopimusehdoissaan joustavampia. (Viestintävirasto 2014)

4.4.1 Henkilötietoja koskeva lainsäädäntö

Henkilötietoja voidaan siirtää toiseen Euroopan unionin jäsenvaltion tai Euroopan talousalueeseen (ETA) kuuluvaan maahan samoilla perusteilla kuin niitä saa Suomessa luovuttaa tai käsitellä. Henkilötietoja voidaan siirtää EU:n tai ETA:n ulkopuolelle ainoastaan jos kyseisessä maassa taataan tietosuojan riittävä taso. EU:n komissio voi päättää, että joku unionin ulkopuolinen valtio takaa riittävän tietosuojan tason, jolloin henkilötietojen siirto on sallittua. Euroopan unionin ja Yhdysvaltojen välillä henkilötietojen siirtoon Yhdysvaltoihin sijoittautuneelle organisaatiolle sovellettavaksi puolestaan tulee niin sanottu Safe Harbor -järjestelmä. Euroopan yhteisöjen komissio on päätöksellään todennut Safe Harbor -järjestelmän varmistavan riittävän henkilötietojensuojan tason henkilötietojen siirroissa Yhdysvaltoihin sijoittautuneille organisaatioille. Muussa tapauksessa henkilötietojen siirto edellyttää suostumusta, elintärkeää etua tai EU:n komission hyväksymien mallisopimusten käyttämistä, jolloin vastuu henkilötietojen oikeanlaisesta käytöstä muuttuu sopimuskysymykseksi. (Viestintävirasto 2014)

4.5 Pilvipalveluntarjoajan turvallisuus

Kun arvioidaan pilvipalvelun turvallisuutta, on syytä arvioida myös palvelun toteutusta sekä palveluntarjoajan toimintaa. Vakavasti otettavat pilvipalveluiden tarjoajat ymmärtävät nykyään käyttäjien tarpeen varmistaa toiminnan turvallisuus ja usein ne pyrkivätkin tekemään toiminnastaan mahdollisimman läpinäkyvää. Kannattaa tutustua mahdollisiin sertifiointeihin tai kolmannen osapuolen tekemiin auditointeihin, sekä palvelintarjoajan itse toimittamiin dokumentteihin palvelun käytännön toimista ja teknistä toteutuksista. Kaikkia yksityiskohtia palveluntarjoajat eivät voi kuitenkaan paljastaa kilpailukyvyn säilyttämiseksi ja turvallisuuden ylläpitämiseksi. (Viestintävirasto 2014)

Palvelua ostaessa joutuu punnitsemaan monia kysymyksiä. Onko esimerkiksi suuren ja tunnetun monikansallisen yrityksen tarjoama palvelu luotettavampi kuin pienen paikallisen toimijan? Suuren yrityksen tarjoamassa palvelussa on useita hyviä puolia. Näillä on useimmiten vakaa talouspohja, eikä toiminnan pitäisi kaatua ainakaan ennakoimattomaan taloudelliseen tilanteeseen. Maineriski epäonnistuessa on sellainen, että toimintaan panostetaan asianmukaisesti. Suuri toimija voi rakentaa ison ja tehokkaan infrastruktuurin ja näin ollen tarjota hyvää palvelua kilpailukykyiseen hintaan. Eri maissa toimivat palvelinkeskukset turvaavat toiminnan jatkuvuuden, vaikka yksittäisessä maassa tai sinne johtavassa runkoverkossa olisi ongelmia. Toisaalta isossa palveluympäristössä yksittäisen asiakkaan tarpeet saattavat hautautua massan alle. Suuressa ympäristössä on paljon eritasoisia toimijoita tuottamassa ja käyttämässä palvelua, minkä seurauksena riski väärinkäyttöön tai tahattomaan haitan aiheuttamiseen kasvaa. Samoin suuri ympäristö voi olla houkuttelevampi maali haitantekijöille. Lisäksi eri maissa sijaitsevat palvelinkeskukset ovat alisteisia paikalliselle lainsäädännölle. (Viestintävirasto 2014)

Kuva 10. Pilvipalveluntarjoajia. (Iyoob 2012)

Pienemmällä paikallisella toimijalla on koosta ja toiminnan laajuudesta aiheutuvat hyvät ja huonot puolensa. Pienen toimijan kanssa voi usein neuvotella useimmista palveluun liittyvistä asioista ja räätälöidä itselle sopivamman paketin. Pienempi palveluntarjoaja saattaa myös esimerkiksi räätälöidä halutun kaltaisen rajapinnan asiakkaan tietojärjestelmää varten. Paikallinen toimija voi myös näyttää asiakkaalle palvelun fyysisen ympäristön, jolloin asiakas voi varmistua missä ja minkälaisissa olosuhteissa hänen tietonsa sijaitsee. Paikallista toimijaa veloittavat samat lait ja määräykset, joten toiminnan säännöt ovat kaikille osapuolille samat. (Viestintävirasto 2014)

Pilvipalvelun fyysisellä ympäristöllä on suuri merkitys palvelun turvallisuuteen ja jatkuvuuteen. Hyvin suojattu ja valvottu ympäristö on vähemmän altis tahallisille ja tahattomille vahingoille. Kulunvalvonnalla varmistetaan, että vain asianomaiset henkilöt asioivat alueella. Näin voidaan suojautua palveluun kohdistuvalta ilkivallalta ja minimoida muutenkin turhat vahingot. Tavanomaisiin poikkeustilanteisiin, kuten sähkön jakelun keskeytykseen, voidaan varautua varavoimalla. Vastaavasti verkkoliikenteen katkeamiseen voidaan varautua käyttämällä kahta erillistä tietoliikenneyhteyttä. Palveluiden kahdentaminen takaa yleensä palvelun jatkuvuuden poikkeustilanteiden aikana. Jos esimerkiksi koko palvelinkeskuksen toiminta keskeytyy luonnonmullistuksen vuoksi, voidaan palvelua edelleen tarjota toisesta sijainnista. (Viestintävirasto 2014)

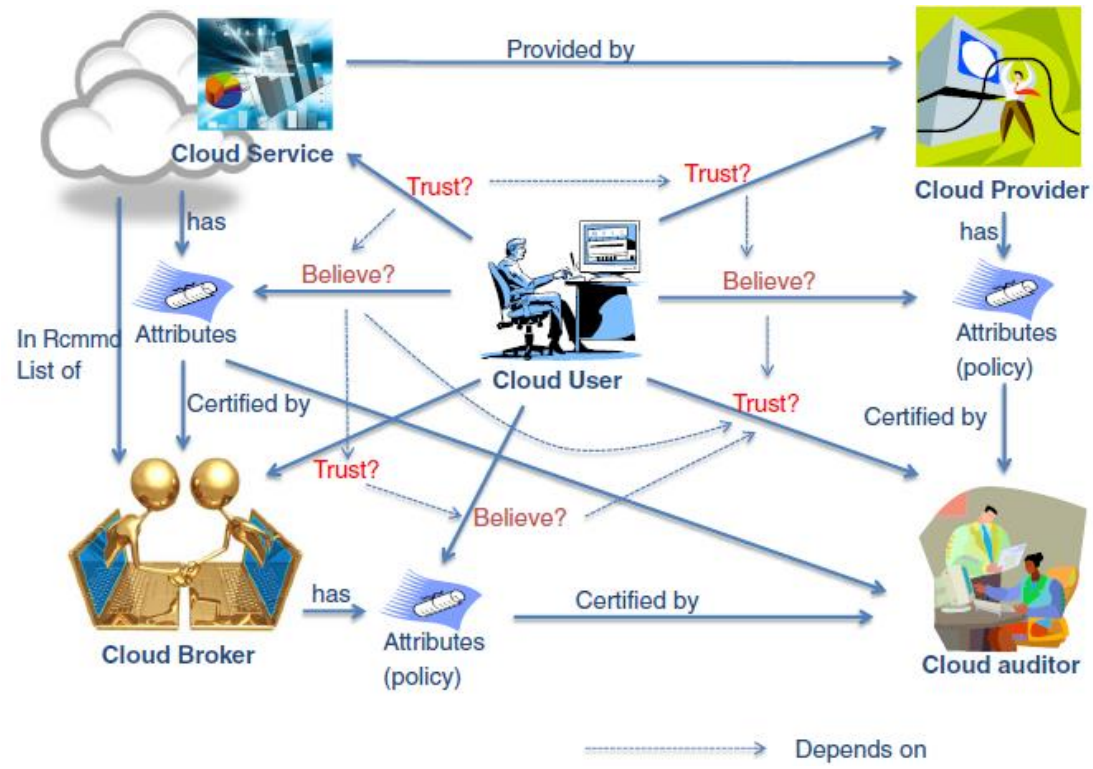
Henkilökunnalla sekä heidän työtavoillaan ja työkaluillaan on merkittävä rooli. Palvelun turvallisuutta arvioitaessa on tärkeää selvittää, minkälainen palveluntarjoajan henkilöstöpolitiikka on, ja noudatetaanko työnteon prosesseissa alan parhaita käytäntöjä. Tehdäänkö kriittisissä toiminnoissa toimiville henkilöille turvallisuusselvityksiä ja seurataanko käytännön toiminnoissa hyväksi havaittuja alan standardeja? Palveluntarjoajan tulisi vaatia sama turvallisuuden taso soveltuvin osin kaikilta alihankintaketjuilta ja niiden työntekijöiltä. Henkilöstöllä, erityisesti ylläpitäjillä ja kehittäjillä, on suora pääsy palvelun toiminnallisuuteen. Järjestelmäylläpitäjät huolehtivat palvelun päivittäisestä toiminnasta ja korjaavat mahdollisia vikatilanteita. Usein heillä on myös pääsy asiakkaan tietosisältöön. Järjestelmän kehittäjät ovat alun alkaen rakentaneet palvelun toiminnallisuuden ja tuntevat sen yksityiskohtia myöten. Useimmiten samat toimijat toimittavat myös päivityksiä ja muita korjauksia kyseisiin ohjelmistoihin. On myös paljon muuta ylläpitohenkilöstöä, jotka toimivat välillisesti tai välittömästi palveluun kuuluvien tietojärjestelmien parissa tai läheisyydessä, ja joilla on mahdollisuus vaikuttaa palvelun toimintaan. (Viestintävirasto 2014)

Pilvipalvelun teknisen turvallisuuden kannalta olennaisia asioita ovat käytettävät teknologiat, toimintamallit ja periaatteet. Pilvipalvelun syvällisempää toimintaa voi olla mahdotonta tutkia, mutta jonkinlaisen kuvan saa palveluntarjoajan toimittamien teknisten tietojen avulla, mahdollisten sertifiointien tai kolmannen osapuolien tekemien auditointien tulosten perusteella sekä tutkimalla palvelua käyttäjälle näkyviltä osilta. Varovaisia johtopäätöksiä voidaan myös tehdä palveluntarjoajan muiden tuotteiden, toimintakulttuurin ja maineen perusteella. (Viestintävirasto 2014)

Pilvipalveluntarjoajan ohjelmistojen päivityskäytännöt on myös hyvä selvittää. Yleensä etenkin suurilla pilvipalveluntarjoajilla ohjelmistopäivitysten käytännöt on hyvin järjestetty ja resursoitu. Asiakkaan tulee kuitenkin itse varmistaa, että päivitysmenettely toimii halutulla tavalla. Lisäksi pilvipalvelussa, kuten missä tahansa verkkoyhteyttä hyödyntävässä ohjelmistossa, on syytä varmistaa että käytettävät yhteydet on salattu. Näin tiedon liikkuminen oman päätelaitteen ja pilvipalvelun välillä on ainakin teoreettisesti suojattu. Selainpohjaista käyttöliittymää käytettäessä salauksen päällä olosta voidaan varmistua protokollan määrittävän osoitteen etuliitteellä ’https://’ tai lukon kuvasta koko osoitekentän edessä. (Viestintävirasto 2014)

5 LUOTTAMUKSELLISUUDEN TODENTAMINEN

Pilvipalvelun tai pilvipalveluntarjoajan luottamusta arvioidessa, tulee myös ottaa huomioon saatavilla olevien tietojen luotettavuus. Tietojen tulee olla luotettavia sekä luotettavasta lähteestä. Arvioitavat tiedot voivat olla useasta eri lähteestä: pilvipalvelua aiemmin käyttäneeltä asiakkaalta, vertaiskäyttäjältä kuultuna, pilvipalveluntarjoajalta itseltään, pilvipalveluiden auditoijalta tai erikseen palkatulta pilvipalveluiden välittäjältä. (Huang & Nicol 2013, 6)



Kuva 11. Kuvaus pilvipalvelun käyttäjän ja pilvipalveluihin liittyvien yksiköiden välisistä luottamussuhteista. (Huang & Nicol 2013, 12)

Jos käyttäjä on aiemmin ollut tietyn pilvipalvelun tai palveluntarjoajan asiakkaana, tulee tuosta asiakaskokemuksesta automaattisesti perusta kyseessä olevan henkilön mielipiteelle palveluntarjoajasta. Aikaisemmat kokemukset ovat olennainen tekijä luottamuksen arvioinnissa. Suorasta asiakaskokemuksesta saatu kokemus on arvokasta, mutta samalla tulee muistaa, että kyseessä on kuitenkin vain yksittäisen käyttäjän kokemus pilvipalvelusta ja kokemukset saattavat olla eri käyttäjien kesken hyvinkin erilaisia. (Huang & Nicol 2013, 6)

Yhden käyttäjän kokemuksen ollessa riittämätön, voi yrittää etsiä tietoa muilta vertaisilta, joilla on kokemusta tietystä pilvipalvelusta tai pilvipalveluntarjoajasta. Ongelmat käyttäjäryhmää laajentaessa ovat kuitenkin edelleen samat kuin yksittäiseltä käyttäjältä kysyttäessä. Miten voi luottaa juuri kyseisen henkilön mielipiteeseen asiasta? Usein käyttäjien kokemus pilvipalvelusta on myös melko rajoittunut, eikä kata pilvipalvelun kaikkia puolia. Kun tarpeeksi monen vertaisen mielipide on mukana pilvipalvelua arvioimassa, tulee yhdistetyistä mielipiteistä yhdessä pilvipalvelun maine. (Huang & Nicol 2013, 6)

Yhdistettyjen mielipiteiden, eli maineen, käyttäminen pilvipalvelun arvioimisessa kattaa usein monia eri tilanteita laajalla aikavälillä. Käyttämällä mainetta pilvipalvelun luotettavuuden arviointivälineenä saadaan palvelusta huomattavasti laajempi kuva kuin kysymällä yksittäiseltä tai yksittäisiltä käyttäjiltä. Mainetta käytettäessä tulee kuitenkin huomioida seuraavat asiat:

- palvelun arvioijien määrän tulee olla tarpeeksi suuri, jotta arviosta tulee merkittävä ja objektiivinen,
- palvelun arvioijilla ja käyttäjillä tulee olla yhteiset parametrit palvelun arvioinnissa sekä samalla tasolla oleva ymmärrys palvelun toiminnasta,
- mainetta käyttämällä saadaan hyvä yleiskuva palvelun toiminnasta, mutta tarkat tiedot yksityiskohdista jäävät usein vähemmälle huomiolle,
- yksittäisen arvioijan luotettavuus tulee kyseenalaistaa ja
- palveluntarjoajat saattavat yrittää vaikuttaa tulokseen manipuloimalla joitain osa-alueita palvelussaan näkyvien arviointiperusteiden mukaisiksi. (Huang & Nicol 2013, 6)

Luottamus ja maine ovat lähellä toisiaan, mutta ne ovat kuitenkin hyvin erilaisia. Yksinkertaistettuna luottamus on olemassa kahden yksilön välillä, kun taas maine on monien korostettu mielipide yksilöstä. Yleensä palveluntarjoajalla, jolla on hyvä maine, on myös monien asiakkaidensa luottamus. Asiakas voi käyttää palveluntarjoajan mainetta yhtenä kriteerinä arvioidessaan tämän luotettavuutta. Pilvipalvelun tai pilvipalveluntarjoajan maine vaikuttaa väkisinkin asiakkaiden mielipiteeseen näiden valitessa käyttöön otettavaa pilvipalvelua. Näin ollen palveluntarjoajat yrittävät rakentaa ja ylläpitää mahdollisimman hyvää ja puhdasta mainetta. Pilvipalveluntarjoajan maine kuvastaa yhteisön kokonaiskuvaa palveluntarjoajasta ja täten on hyödyllisempi lähinnä

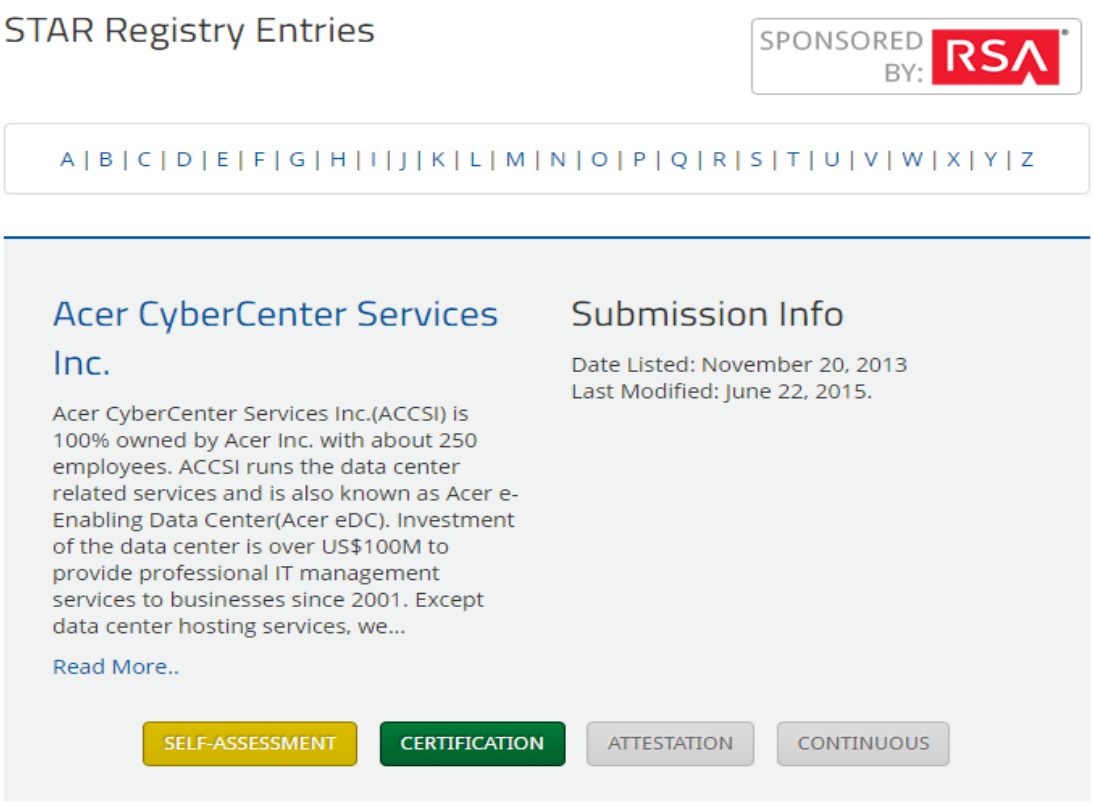
yksityisille käyttäjille, jotka etsivät uutta pilvipalvelua ja joilla ei ole erityisiä vaatimuksia pilvipalvelulta. Maine saattaa olla hyödyllinen parametri, kun pilvipalvelua valitaan, mutta jälkeenpäin pelkkä maine ei enää riitä perustelemaan luottamusta. (Huang & Nicol 2013, 2)

Pilvipalveluntarjoajan asiakkaan tulisi luottaa palveluntarjoajaan, mutta myös varmistaa, että palveluntarjoajan toimii luottamuksen arvoisesti jatkossakin. Alustavan luottamussuhteen luomisen jälkeen asiakkaan pitää varmistaa ja uudelleen arvioida luottamus. Palvelutasosopimus on lainalainen sopimus palveluntarjoajan ja asiakkaan välillä. Palvelun laadun ja tason seuranta on tärkeä perusta pilvipalveluiden luottamuksen hallinnalle. Palvelutasosopimuksiin perustuvassa tarkkailussa merkittäväksi ongelmaksi muodostuu kuitenkin sen keskittyminen ”näkyviin” elementteihin pilvipalvelun toiminnassa, jättäen ”näkymättömät” elementit, kuten tietoturvan ja yksityisyyden, huomioimatta. Asiakkaalla ei myöskään aina välttämättä ole tarpeeksi resursseja mittaamaan palvelun laatua ja -tasoa tarvittavalla tarkkuudella. On kuitenkin olemassa kolmannen osapuolen asiantuntijoita, jotka tarjoavat näitä palveluita. Jos kyseessä on yksityinen pilvi, voidaan palkata ulkopuolinen luotettava osapuoli, jolle uskotaan pääsy yksityisen pilven domainiin. Näin kyseinen ulkopuolinen osapuoli voi tuottaa asiakkaalle raportteja palveluntarjoajan tuottamasta palvelun tasosta ja -laadusta. (Huang & Nicol 2013, 3)

5.1 Auditointi

Kun luottamusta pilvipalveluntarjoajaan rakennetaan, läpinäkyvyys ja vastuullisuus ovat sen perustana. Parantaakseen pilvipalveluiden läpinäkyvyyttä, Cloud Security Alliance (CSA) julkaisi Security, Trust & Assurance Registry (STAR) ohjelman. STAR on ilmainen, julkisesti saatavilla oleva, rekisteri, joka sallii pilvipalveluntarjoajien julkistaa itsearvioita omista tietoturvakäytännöistään. Tiedot voi julkaista joko Consensus Assesments Initiative Questionareen (CAIQ) tai Cloud Controls Matrixiin (CCM), jotka molemmat perustuvat CSA:n määrittelemiin alan parhaisiin käytäntöihin. CAIQ-kysely sisältää yli 140 kysymystä, joita pilvipalveluiden käyttäjät tai auditoijat saattaisivat kysyä. CCM-rekisterin avulla voi verrata kuinka hyvin pilvipalveluntarjoaja nou-

dattaa CSA:n julkaiseman tietoturvaoppaan ohjeita. STAR-rekisteri on erittäin hyödyllinen työkalu, kun yritetään etsiä uutta pilvipalveluntarjoajaa. Esimerkkejä pilvipalveluntarjoajien itsearvioinneista voi nähdä CSA:n STAR www-sivuilla. Pitää kuitenkin muistaa, että STAR-rekisteri pitää sisällään vain pilvipalveluntarjoajan itse ilmoittamia tietoja. (Huang & Nicol 2013, 3)



Kuva 12. Kuvakaappaus CSA:n STAR-rekisteristä. (CSA:n www-sivut)

CloudTrust Protocol (CTP) on toinen CSA:n ylläpitämä ohjelma. CTP:n ensisijainen tarkoitus on luoda todisteisiin perustuvaa varmuutta siihen, että kaikki, jota pilvessä väitetään tapahtuvan, oikeasti tapahtuu niin kuin on väitetty tapahtuvan, ilman mitään ylimääräisiä toimintoja. CTP tarjoaa mielenkiintoisen kanavan pilvipalveluntarjoajan ja asiakkaan välille, jonka kautta asiakkaan on mahdollista tarkastella pilvipalvelun sisäistä toimintaa. Tulee kuitenkin muistaa, että samoin kuin STAR-rekisterin, CTP:n olennainen heikkous on, että sen tarjoama informaatio tulee suoraan pilvipalveluntarjoajalta itseltään. Epärehelliset palveluntarjoajat voivat yrittää käyttää tätä hyväkseen ja yrittää suodattaa niille epäsuotuisat tiedot pois rekisteristä. (Huang & Nicol 2013, 3)

RSA on julkaissut Cloud Trust Authorityn (CTA) pilvipalveluna, jota kutsutaan luottamukseksi palveluna (englanniksi Trust as a Service, TaaS). TaaS-pilvipalvelun tarkoituksena on tarjota yksi palvelu turvallisen pilvipalvelun konfigurointiin ja hallintaan. CTA on suunniteltu toimimaan useiden eri pilvipalveluntarjoajien palveluiden kanssa. CTA:n alustava julkaisu sisältää identiteettipalvelun, joka mahdollistaa kirjautumisen useaan pilvipalveluun yhdellä sisäänkirjautumisella, sekä säännösten valvontapalvelun, jonka avulla käyttäjä näkee useiden pilvipalveluntarjoajien tietoturvaprofiilit, jotka on arvioitu keskenään samalla suorituskykytestillä. CTA työkaluna on erikoistunut pilvipalveluiden luottamuksen hallintaan ja se on kehitetty RSA:n filosofian ”luottamus = näkyvyys + hallinta” mukaisesti. Pilveen perustuvana palveluna CTA voi yksinkertaistaa käyttäjien luottamuksen hallinnan. Käyttäjän tulee kuitenkin edelleen tehdä päätös CTA:n sisältävien tietojen luotettavuudesta, sillä tiedot ovat pilvipalveluntarjoajien itse syöttämiä. Käyttäjän tulee myös päättää luottaako itse CTA:n rooliin välikätenä. (Huang & Nicol 2013, 3)

Koska itsearvioinneissa palveluntarjoajat voivat olla epärehellisiä, on väitetty että viralliset auditoinnit ovat välttämättömiä terveellisen pilvipalvelumarkkinoiden saavuttamiseksi. Yleiseen käyttöön tarkoitettuja ulkopuolisia auditointeja, todistuksia ja sertifikaatteja on käytetty myös pilvipalveluihin, mutta niitä ei ole suunniteltu juuri pilvipalveluiden arviointiin. Esimerkkejä näistä ovat:

- ISO/IEC 27000 - kansainvälisen tietoturvan hallinnan standardeja
- SSAE 16 - standardi palveluorganisaatioiden sisäisestä valvonnasta
- ISAE 3402 - varmuusraportointi palveluorganisaatioiden sisäisestä valvonnasta

CTP:n ja STAR:n lisäksi, CSA julkaisi myös juuri pilvipalveluille suunnatun CloudAudit initiativen. CloudAudit tarjoaa yhteisen rajapinnan kaikille pilvipalveluntarjoajille, jotka haluavat julkistaa auditointituloksia ja sallii palvelun käyttäjien automatisoida näiden tietojen käytön omissa auditointiprosesseissaan. CloudAuditiin voi julkaista tuloksia pilvipalveluntarjoajien itsearvioista, pilvipalvelun asiakkaiden teettämistä arvioinneista sekä virallisia kolmannen osapuolen suorittamista auditoinneista. (Huang & Nicol 2013, 4)

5.2 Auditoijat

National Institute of Standards and Technologyn (NIST) mukaan auditoija on “puolue, joka voi suorittaa itsenäisiä arviointeja pilvipalveluista, tietojärjestelmän toiminnoista, suorituskyvystä sekä pilvitoteutuksen tietoturvasta.” Pilvipalveluiden auditointi on tärkeä työkalu pilvipalveluiden ominaisuuksien luotettavuuden arvioinnissa. Auditoijan arvioita pilvipalvelusta pidetään yleisesti erittäin luotettavana tiedon lähteenä. Useimmille pilvipalveluiden asiakkaille ulkoisen kolmannen osapuolen auditointi riittää hyvin perustamaan luottamussuhteen pilvipalveluntarjoajaan. Vaativimmat asiakkaat voivat vaatia, että myös itse auditoijan toimintaa tulee tarkkailla ja valvoa. (Huang & Nicol 2013, 7)

Virallisessa akkreditoinnissa, ammattimaista standardointia, auditointia tai arviointia teettävä yritys saa sertifikaatin pätevyydestään, auktoriteetistaan ja uskottavuudestaan. Sertifikaatin myöntää itsenäinen valtuutettu akkreditointiorganisaatio, joka voi itsekin olla akkreditoitu kansainvälisen standardointielimen tai virallisen yhdistyksen toimesta. Akkreditointi on paljolti verrattavissa auditointiin, mutta eroja kuitenkin löytyy. Molemmissa itsenäinen ulkopuolinen kolmas osapuoli arvioi palvelua tai palveluntarjoajaa. Akkreditointi kuitenkin keskittyy enemmän arvioitavan yksikön pätevyyteen suorittaa tietynlaisia ammatillisia palveluja, kun taas auditointi taas keskittyy arvioimaan palvelun tai palveluntarjoajan suorituskykyä, verraten sitä yhteisesti sovittuihin standardeihin. Tämän lisäksi auditointi suoritetaan normaalisti vuosittain, tai jopa puolivuosittain, kun taas akkreditointi käydään läpi huomattavasti harvemmin, esimerkiksi viiden vuoden välein. (Huang & Nicol 2013, 7)

5.3 Pilvivälittäjät

Pilvivälittäjät ovat myös tärkeässä roolissa pilvipalvelumarkkinoilla. NIST:n määrityksen mukaan pilvivälittäjä on ”osapuoli, joka hallinnoi pilvipalveluiden käyttöä, suorituskykyä ja toimitusta, sekä toimii välikätenä pilvipalveluntarjoajan ja asiakkaan välillä.” Pilvivälittäjän teettämät havainnot voivat olla tärkeitä luotettavuuden arvioinnin tiedonlähteitä. Pilvivälittäjän palveluihin kuuluu esimerkiksi pilvipalveluiden välittäminen sekä pilvipalveluiden yhdistäminen. Pilvipalveluiden välittämisen kautta

pilvivälittäjä voi tarjota lisäpalveluina esimerkiksi suorituskyvyn seurantaa tai tietoturvan hallinnointia. Pilvipalveluiden yhdistäminen voi tarkoittaa esimerkiksi pilvivälittäjän itse kokoamaa pakettia monista eri pilvipalveluntarjoajien pilvipalveluista.

Pilvivälittäjän käytön etuihin lukeutuvat esimerkiksi pilvipalveluiden suorituskyvyn reaaliaikainen mittaaminen, vertaiskäyttäjien palautteen huomioiminen palvelun valinnassa ja kyky valvoa ja arvioida monia eri samaan kategoriaan kuuluvia pilvipalveluja eri palveluntarjoajilta. Pilvivälittäjällä voi olla erittäin hyvä kuva pilvipalvelumaailman nykytilasta, ja osaa käyttää tätä suositellessaan eri pilvipalveluita asiakkaansa käyttöön. Kuitenkin jälleen nousee kysymys pilvivälittäjän luotettavuudesta. Pilvivälittäjän luotettavuus ja kyky arvioida eri pilvipalveluiden ominaisuuksia voidaan asettaa kysymyksen alaiseksi. Tiheään ylläpidetyt bisnessuhteet voivat vaikuttaa pilvivälittäjän toimintaan ja mielipiteisiin, eikä tämä välttämättä pysty toimimaan yhtä objektiivisesti kuin viralliset auditoijat tai akkreditoijat. (Huang & Nicol 2013, 7)

Voidaan kuvitella, että jos pilvivälittäjä edustaa yhtä tiettyä pilvipalveluntarjoajaa, voivat pilvivälittäjän tiedot suosia tuota tiettyä palveluntarjoajaa. Pilvivälittäjän ollessa itsenäinen toimija, ja tämän liiketoiminnan perustuen suurilta osin tämän omien asiakassuhteiden luottamukseen, on todennäköistä, että pilvivälittäjä on motivoitunut pitämään omat asiakkaansa tyytyväisinä tarjoten heille luotettavaa ja mahdollisimman hyödyllistä palvelua. Pilvivälittäjän palveluiden sisältäessä useampien pilvipalveluntarjoajien pilvipalveluita, on todennäköisempää, että pilvivälittäjä todella on tietoinen eri pilvipalveluiden eroista, hyödyistä ja haitoista. (Huang & Nicol 2013, 8)

Varmistaakseen, että pilvivälittäjä toimii luotettavana pilvipalveluiden arvioijana, tulee käyttäjien saada tietää tarkemmin kuinka pilvivälittäjä toimii. Onko pilvivälittäjä neutraali, mitä käytäntöjä pilvivälittäjä noudattaa ja onko pilvivälittäjällä todisteita tämän luotettavuudesta. Näiden kysymysten noustessa pintaan voidaan ajatella, että myös pilvivälittäjiä tulisi auditoija tai akkreditoida. (Huang & Nicol 2013, 8)

6 LUOTTAMUSARVIOINTI

6.1 Auditoijan luottamuksen arviointi

Auditoijan tulisi yhdenmukaistaa toimintansa ammatillisten toimintamallien ja standardien mukaiseksi. Pilvipalveluiden auditoijat itse tulisi myös auditoida säännöllisin väliajoin, jotta voidaan varmistua niiden toimintamallien noudattavan asetettuja toimintatapoja ja standardeja. Yksi pilvipalveluiden asiakas saattaa pitää auditoijaa luottamuksellisuuden lähteenä, samalla kun toinen asiakas vaatii myös auditoijan todistavan olevansa luottamuksen arvoinen. Pilvipalveluiden asiakas odottaa, että auditoijan arvio pilvipalvelusta on objektiivinen, asiantunteva sekä asiaankuuluvien standardien mukainen. Oletus auditoijan luottamuksellisuudesta perustuu yleensä jonkinlaisiin todisteisiin auditoijan pätevyydestä, hyväntahtoisuudesta ja johdonmukaisuudesta. Auditoijan luottamuksellisuuden arvioinnin perusteina voidaan pitää yhtä tai useampaa seuraavista asioista:

Akkreditointi: Pilvipalvelun asiakas voi tarkistaa onko pilvipalveluiden auditoijalle suoritettu virallista akkreditointia ammattitaitoisen auditointiorganisaation tai pilvipalveluihin erikoistuneen organisaation toimesta. Ammattitaitoisia auditointiorganisaatioita ovat esimerkiksi Auditing Standards Board ASB ja American Institute of Certified Public Accountants AICPA.

Standardit: Auditoijan tulisi noudattaa ammatillisia käytäntöjä ja standardeja auditoinneissaan. Esimerkkejä tällaisista standardeista ovat SAS 70, SSAE 16 ja ISAE 3402. Auditoijan tulisi arvioida pilvipalvelua yleisesti hyväksyttyjen käytäntöjen mukaisesti.

Sertifioinnit ja arvioinnit: Akkreditoinnin ja käytäntöauditoinnin lisäksi pilvipalvelun asiakas voi haluta tarkastaa auditoijan muita attribuutteja, kuten auditoijan historiatietoja, edellisten auditoitujen kokemuksia auditoijasta ja auditoijan auditointien historiaa. Jotkut tiedot voivat sisältyä auditointidokumentteihin, toiset saattavat sisältyä erilaisiin sertifikaatteihin tai vertaiskäyttäjien arviointeihin. (Huang & Nicol 2013, 10)

6.2 Pilvivälittäjän luottamuksen arviointi

Mitä tahansa yritystä, joka tarjoaa välitettyjä pilvipalveluita, voidaan pitää pilvivälittäjänä. Esimerkkeinä voidaan pitää pilvipalvelukauppapaikkana toimivaa SpotCloudia tai TaaS-pilvipalvelua kuten CTA. Pilvivälittäjien palveluilta odotetaan muun muassa luottamuksen arvoisia lisäpalveluita, kuten palveluiden yhdistämistä, tietoturvan hallintapalveluja ja objektiivista ja tarkkaa arviointia eri pilvipalveluista ja pilvipalveluntarjoajista. Pilvivälittäjän luottamuksellisuuden arvioinnin perusteina voidaan pitää yhtä tai useampaa seuraavista asioista:

Akkreditointi: Samoin kuin pilvipalveluiden auditoijien, myös pilvivälittäjien tulisi olla todistetusti päteviä tarjoamaan palveluitaan. Virallinen akkreditointi tulisi suorittaa ammattitaitoisen auditointiorganisaation tai pilvipalveluihin erikoistuneen organisaation toimesta.

Standardit: Pilvivälittäjän tulisi noudattaa tiettyjä käytäntöjä ja yleisesti hyväksyttyjä alan standardeja toiminnassaan. Pilvivälittäjän toimintaa tulisi auditoida säännöllisin väliajoin.

Sertifioinnit ja arvioinnit: Pilvivälittäjän pätevyys, hyväntahtoisuus ja johdonmukaisuus ovat tärkeitä todisteita pilvivälittäjän luottamusta arvioidessa. Standardien noudattamisen lisäksi, tulee arvioinnissa ottaa huomioon myös arvioitavan tahon suorituskyky, tietoturva ja yksityisyyskäytännöt. Arviointeja pilvivälittäjän käytöstä voi ottaa huomioon myös toisilta pilvivälittäjiltä tai pilvivälittäjän entisiltä tai nykyisiltä asiakkailta.

Läpinäkyvyys ja itsearviointi: Pilvivälittäjien toiminnan tulisi olla myös mahdollisimman läpinäkyvää asiakkaalle. Ohjeita palveluntarjoajien läpinäkyvyyteen on saatavilla esimerkiksi CSA:n toimintaohjeissa. Myös itsearviointi on hyvä pitää pilvivälittäjän toiminnassa mukana. Pilvivälittäjä voi suorittaa itsearvioinnin esimerkiksi täyttämällä CSA:n CAIQ-kyselyn tai täyttämällä pilvivälittäjän tiedot CCM-rekisteriin. Itsearvioinnissa julkistetut tiedot voidaan mahdollisuuksien mukaan varmentaa virallisella auditoinnilla.

Maine ja suositukset: Vertaiskäyttäjien ja edellisten tai nykyisten asiakkaiden mielipiteet, tai luotettavien osapuolien suositukset pilvivälittäjästä voivat olla tärkeä tiedon lähde pilvivälittäjän toiminnan luotettavuudesta. (Huang & Nicol 2013, 10)

6.3 Pilvipalveluntarjoajan luottamuksen arviointi

Pilvipalveluiden asiakkaat odottavat saavansa pilvipalveluntarjoajalta luotettavaa palvelua. Monet pilvipalveluntarjoajat antavat julkisuuteen tietoja tarjoamansa pilvipalvelun sisäisistä toiminnoista. Kaikille asiakkaille pelkkä palveluntarjoajan sana ei kuitenkaan ole riittävä peruste pilvipalveluntarjoajan luottamuksellisuuden todentamiseksi. Pilvipalveluntarjoajan luottamuksen arviontiin voidaan käyttää monessa kohdassa samoja menetelmiä kuin aikaisemmin käytettiin pilvivälittäjien kohdalla. Pilvipalveluntarjoajan luottamuksellisuuden arvioinnin perusteina voidaan pitää yhtä tai useampaa seuraavista asioista:

Akkreditointi: Samoin kuin pilvipalveluiden auditoijien ja pilvivälittäjien, myös pilvipalveluntarjoajien tulisi olla todistetusti päteviä tarjoamaan palveluitaan. Virallinen akkreditointi tulisi suorittaa ammattitaitoisen auditointiorganisaation tai pilvipalveluihin erikoistuneen organisaation toimesta.

Standardit: Pilvipalveluntarjoajan tulisi noudattaa tiettyjä käytäntöjä ja yleisesti hyväksyttyjä alan standardeja toiminnassaan. Pilvipalveluntarjoajan toimintaa tulisi auditoida säännöllisin väliajoin.

Sertifioinnit ja arvioinnit: Pilvipalveluntarjoajan pätevyys, hyväntahtoisuus ja johdonmukaisuus ovat tärkeitä todisteita pilvipalveluntarjoajan luottamusta arvioidessa. Standardien noudattamisen lisäksi, tulee arvioinnissa ottaa huomioon myös pilvipalveluntarjoajan suorituskyky, tietoturva ja yksityisyyskäytännöt. Arviointeja pilvipalveluntarjoajan toiminnasta voi ottaa huomioon myös pilvivälittäjiltä tai pilvipalveluntarjoajan entisiltä tai nykyisiltä asiakkailta.

Läpinäkyvyys ja itsearviointi: Pilvipalveluntarjoajien toiminnan tulisi olla mahdollisimman läpinäkyvää asiakkaalle. Ohjeita pilvipalveluntarjoajien läpinäkyvyyteen on saatavilla esimerkiksi CSA:n toimintaohjeissa. Myös itsearviointi on tärkeä osa pilvipalveluntarjoajan läpinäkyvyyttä. Pilvipalveluntarjoaja voi suorittaa itsearvioinnin esimerkiksi täyttämällä CSA:n CAIQ-kyselyn tai täyttämällä pilvivälittäjän tiedot CCM-rekisteriin. Itsearvioinnissa julkistetut tiedot voidaan mahdollisuuksien mukaan varmentaa virallisella auditoinnilla.

Maine ja suositukset: Vertaiskäyttäjien ja edellisten tai nykyisten asiakkaiden mielipiteet, tai luotettavien osapuolien suositukset pilvipalveluntarjoajasta voivat olla tärkeä tiedon lähde pilvipalveluntarjoajan toiminnan luotettavuudesta. (Huang & Nicol 2013, 11)

6.4 Pilvipalvelun luottamuksen arviointi

Pilvipalvelun tasoa voidaan mitata esimerkiksi perustuen sen luotettavuuteen, saatavuuteen, johdonmukaisuuteen, tietoturvaan tai yksityisyyteen. Pilvipalveluiden luottamuksellisuutta arvioidessa, on hyvä myös ottaa huomioon aikaisemmin arvioitujen auditoijien, pilvivälittäjien ja pilvipalveluntarjoajien arviointien tulokset. Pilvipalvelun luottamuksellisuuden arvioinnin perusteina voidaan pitää yhtä tai useampaa seuraavista asioista:

Luottamus pilvipalveluntarjoajaan: Jos asiakas luottaa pilvipalveluntarjoajaan voidaan suoraan olettaa, että myös tarjottu pilvipalvelu on luottamuksen arvoinen.

Standardit: Pilvipalvelun asiakas voi tutkia mitä käytäntöjä pilvipalvelu käyttää tai mitä standardeja se toteuttaa. Voidaan myös tutkia pilvipalveluntarjoajan auditointien tuloksia.

Sertifioinnit ja arvioinnit: Asiakas voi tutkia pilvipalvelun suorituskykyyn, tietoturvaan ja yksityisyyskäytäntöihin liittyviä ominaisuuksia. Edellä mainittuja ominaisuuksia on voitu arvioida auditoijan, pilvivälittäjän tai pilvipalvelun käyttäjien toimesta.

Läpinäkyvyys ja itsearviointi: Asiakas voi tutkia pilvipalveluntarjoajan itsearvioinneissa tarjoamia tietoja pilvipalvelusta tai käyttää esimerkiksi CTA:n tarjoamia palveluita tutkiakseen pilvipalvelun sisäistä toimintaa.

Palvelutasoseuranta: Palvelun laadun ja tason seuranta on tärkeä lähde luottamuksen todentamiseen.

Maine ja suositukset: Suosituksen pilvipalvelusta voi saada esimerkiksi pilvivälittäjältä tai palvelua ennen tai nyt käyttävältä asiakkaalta tai muulta vertaiskäyttäjältä. Suosituksien kohdalla tulee aina pitää mielessä suosittelijan luotettavuuden taso. (Huang & Nicol 2013, 11)

LÄHTEET

Viestintävirasto. 2014. Organisaation pilvipalveluiden tietoturva. Viitattu 14.4.2016. https://www.viestintavirasto.fi/

LE&AS. 'Take the financial risk out of cloud computing with SaaS escrow'. Escrow news 2.9.2014. Viitattu 21.4.2016. http://www.leaas.co.uk/blog/take-the-financial-risk-out-of-cloud-computing-with-saas-escrow/

Hanhirova. 'Mitä pilvipalvelu tarkoittaa käytännössä – esimerkkinä sähköposti'. Gapps Blogi. 27.9.2012. Viitattu 8.3.2016. http://gapps.fi/mita-pilvipalvelu-tarkoittaa-kaytannossa-esimerkkina-sahkoposti/

Salo, I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo.

Edmonson, C. 2012. Jumpstart: Windows Azure. Introduction to Windows Azure. Viitattu 30.4.2016.

Hendryx, A. 2011. Cloudy Concepts: IaaS, PaaS, SaaS, MaaS, CaaS & XaaS. Viitattu 10.4.2016. http://www.zdnet.com/

Altnix. 2014. Monitoring as a Service (MaaS) in the Cloud – Does it Work? Viitattu 10.4.2016. http://www.altnix.com/resources/white-paper/monitoring-as-a-service-maas-does-it-work

Lane, K. 2013. Overview Of The Backend as a Service (BaaS) Space. Viitattu 10.4.2016. https://s3.amazonaws.com/kinlane-productions/whitepapers/API+Evangelist+-+Overview+of+the+Backend+as+a+Service+Space.pdf

Abrams. 'Get your mobile application backed by the cloud with the Mobile Backend Starter'. Google Cloud Platform Blog. 3.6.2013. Viitattu 10.4.2016. https://cloudplatform.googleblog.com/2013/06/get-your-mobile-application-in-the-cloud-with-mobile-backend-starter.html

Kiwaluk. 'What is 'Everything as a Service'?'. RevenueWire Blog. 2.10.2015. Viitattu 10.4.2015. https://www.revenuewire.com/blog/what-is-everything-as-a-service/

Hybrid Cloud Solutions. 2015. Hybrid Cloud's Security Issues and Benefits. Viitattu 21.4.2016. http://hybridcloudsolutions.info/hybrid-clouds-security-issues-and-benefits/

Tilastokeskus. 2014. Puolet yrityksistä käyttää pilvipalveluja. Viitattu 6.5.2016. http://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_tie_001_fi.html

Tilastokeskus. 2015. Pilvipalveluiden käyttö yleistyy yrityksissä. Viitattu 6.5.2015. http://www.stat.fi/til/icte/2015/icte_2015_2015-11-26_tie_001_fi.html

Microsoft MSDN www-sivut. Viitattu 21.4.2016. https://msdn.microsoft.com/es-es/library/dn194478.aspx

Googlen www-sivut. Viitattu 29.4.2016. https://www.google.com/about/datacenters/inside/locations/index.html

Amazon Web Services www-sivut. 2016. Viitattu 29.4.2016. http://status.aws.amazon.com/

Iyoob. 'Cloud Technology Spectrum'. Cloud Navigator. 27.7.2012. Viitattu 21.4.2016. http://blog.gravitant.com/2012/07/27/cloud-technology-spectrum/

Huang, J & Nicol, D. 2013. Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications. 2:9. Viitattu 3.5.2016. doi:10.1186/2192-113X-2-9

Cloud Security Alliancen www-sivut. Viitattu 29.4.2016. https://cloudsecurityalliance.org/