Aalto-yliopisto
Perustieteiden korkeakoulu
Tietotekniikan tutkinto-ohjelma

Tietoturva julkisissa pilvipalveluissa

Kandidaatintyö

2. kesäkuuta 2011

Jussi-Pekka Erkkilä

Aalto-yliopisto
Perustieteiden korkeakoulu
Tietotekniikan tutkinto-ohjelma

KANDIDAATINTYÖN
TIIVISTELMÄ

Tekijä:	Jussi-Pekka Erkkilä
Työn nimi:	Tietoturva julkisissa pilvipalveluissa
Päiväys:	2. kesäkuuta 2011
Sivumäärä:	21
Pääaine:	Ohjelmistotekniikka
Koodi:	T3001
Vastuuopettaja:	Ma professori Tomi Janhunen
Työn ohjaaja(t):	TkL Sanna Suoranta (Tietotekniikan laitos)

Pilvilaskenta on uudehko konsepti, joka mahdollistaa palvelinten ja laskentainfrastruktuurin ulkoistamiseen Internetiin, niin sanottuihin pilvipalveluihin. Pilvipalvelut voivat monissa tapauksissa helpottaa IT-järjestelmän ylläpitoa ja vähentää ylläpitokuluja. Pilvipalveluiden merkittävin epävarmuustekijä on tietoturva.

Tässä tutkielmassa pyritään selvittämään pilvipalveluihin liittyvät tietoturvaongelmat ja -riskit, sekä esittämään joitakin vaihtoehtoja riskien minimoimiseksi. Erityisesti aiheeseen keskitytään julkista pilvipalvelua hyödyntävän asiakkaan näkökulmasta. Tutkielma perustuu muiden tutkimusten tarjoamiin tilastoihin ja johtopäätöksiin sekä pienehköön empiiriseen tutkimukseen, jossa tutustuttiin Amazon EC2-pilvipalveluun ja sen tietoturvaratkaisuihin.

Suurimmat ongelmat pilvipalveluiden käytössä liittyvät asiakkaan ja palveluntarjoajan väliseen luottamukseen sekä tiedon varastoinnin ja verkkoliikenteen turvallisuuteen. Ratkaisuna esitetään kaksi eri tietoturvamallia, jotka pyrkivät ratkaisemaan pilvipalveluihin liittyviä ongelmia. Tiedonsiirron turvaamiseksi ja tiedon eheyden varmistamiseksi ehdotetaan kryptografisia menetelmiä. Tutkielmassa myös esitellään myös pilvipalveluiden positiviisia vaikutuksia tietoturvaan.

Johtopäätöksenä todetaan, että pilvipalveluiden kohdalla järjestelmän ylläpitäjän on hyvä huomioida samat tietoturvauhat kuin minkä tahansa tietoteknisen järjestelmän kohdalla. Lisäksi pilvipalveluiden kohdalla täytyy tehdä kompromisseja: ovatko pilvipalveluiden tarjoamat hyödyt suuremmat kuin mahdolliset tietoturvariskit? Yksiselitteistä ratkaisua kysymykseen, ovatko pilvipalvelut turvallisia, ei ole. Kysymys vaatii aina tapauskohtaista arviointia.

Avainsanat:	tietoturva, pilvilaskenta, pilvipalvelut, IaaS, SaaS, luottamus
Kieli:	Suomi

Sisältö

1 Johdanto

Pilvilaskenta on uudehko konsepti, joka mahdollistaa laskennan ulkoistamisen Internetin yli niin sanottuun pilvipalveluun. Käytännössä pilvipalvelu voi olla esimerkiksi suuri joukko palvelimia, jotka tarjoavat tarpeen mukaan dynaamisesti skaalautuen laskentatehoa, tietoliikenneyhteyksiä tai levytilaa asiakkailleen.

Pilvipalveluiden suosio on kasvanut nopeasti viime vuosina ja niihin liittyen on tehty paljon tieteellistä tutkimusta. Yrityksille, organisaatioille ja muille tahoille voi olla houkuttelevaa ulkoistaa palvelinlaitteistonsa pilvessä toimiville virtuaalipalvelimille. Pilvipalveluiden etuja ovat muun muassa alhaiset aloituskustannukset ja resurssien skaalautuvuus. [7]

Pilvipalveluiden hyödyt ovat varsin ilmeisiä, mutta luonnollisesti niillä on myös negatiiviset puolensa. Suurimmat ongelmat pilvipalveluissa liittyvät tietoturvaan. Palveluntarjoaja myy omaa laitteistoaan asiakkaan käyttöön ja toisaalta asiakas käyttää palveluntarjoajan hallinnoimaa laitteistoa mahdollisesti luottamuksellisten tietojen käsittelyyn. Luottamus palveluntarjoajan ja asiakkaan välillä on siis ensiarvoisen tärkeää. Lisäksi pilvipalvelun käyttäjä joutuu lähettämään kaiken datansa useimmiten julkisen verkon kautta, jolloin salakuuntelun mahdollisuus täytyy huomioida.

Tässä tutkielmassa perehdytään nimenomaan pilvilaskentaan liittyviin tietoturvaongelmiin. Tutkielmassa pyritään selvittämään, millaisia erityisesti pilvipalveluihin liittyviä tietoturvaongelmia on olemassa ja miten niihin tulisi varautua. Lisäksi selvitetään, mistä tietoturvaongelmat johtuvat ja millaisia ratkaisuja niihin on kehitetty nimenomaan pilvipalveluita silmällä pitäen.

Tietoturvaa lähestytään erityisesti infrastuktuurinsa julkiseen pilveen siirtävän osapuolen näkökulmasta. Esimerkki tällaisesta on yritys tai organisaatio, joka on siirtänyt verkkopalvelujaan pilveen. Tutkielma sivuaa jonkin verran tietoturvaa myös infrastruktuuria tarjoavan palveluntarjoajan sekä yksittäisen loppukäyttäjän näkökulmasta, mutta näihin ei keskitytä yhtä syvällisesti.

Pilvipalveluiden tietoturvaongelmia pohditaan abstraktilla tasolla, kuten eheyden ja yksityisyyden näkökulmasta. Toisaalta asioita käydään läpi myös ohjelmistoteknisellä tasolla, esimerkiksi salausprotokollien ja perinteisten tietoturva-aukkojen kautta. Koko tutkielman tavoitteena on arvioida, onko pilvipalveluiden käyttö turvallista, mitä tietoturvaongelmia pilvipalveluihin liittyy ja miten tietoturvaongelmiin voisi varautua.

Lisäksi työhön kuuluu myös pienehkö kokeellinen osuus, jossa tarkastellaan erään pilvipalvelun tietoturvaa käyttäjän näkökulmasta. Tämä kokeellinen osuus ei kuitenkaan ole pääosa tutkielmaa, vaan ennemminkin kirjallisuustutkimusta tukeva esimerkki.

Lopputuloksena päädytään tosiasiaan, ettei pilvipalveluiden tietoturvaa voi aina selkeästi määritellä hyväksi tai huonoksi. Kyse on ennemminkin asiakkaan tietoturvavaatimuksista,

luottamuksesta palveluntarjoajan ja asiakkaan kesken sekä kompromissista hyötyjen ja haittojen välillä.

Työ jakautuu viiteen lukuun: johdannon jälkeen perehdytään tarvittavaan taustatietoon. Luvussa määritellään, mitä pilvilaskenta on, mihin se soveltuu sekä sen etuihin ja haittoihin. Tämän jälkeen luvussa 3 tutustutaan pilvipalveluiden tietoturvaan yleisellä tasolla ja arvioidaan niiden kriittisimpiä vaatimuksia ja riskejä. Neljäs luku keskittyy pilvipalveluissa käytettyihin tietoturvaratkaisuihin ja -malleihin, joilla ongelmia on pyritty selvittämään. Tässä myös käydään läpi perustoimenpiteitä, mitä käyttäjä voi tehdä parantaakseen tietoturvaa. Lisäksi esimerkkinä tarkastellaan Amazonin EC2-pilvilaskentapalvelua ja sitä miten tietoturva on huomioitu siinä käyttäjän näkökulmasta. Viimeisessä luvussa tehdään yhteenveto asioista, ja johtopäätöksenä pyritään arvioimaan, kannattaako pilvipalveluita ylipäätään käyttää.

2 Pilvilaskenta yleisesti

Pilvilaskenta ja pilvipalvelu ovat melko tuoreita käsitteitä. Vaikka niitä nykyisin arkikielessä käytetäänkin jonkin verran, ei ole olemassa yhtä yleisesti hyväksyttyä määritelmää sille, mitä pilvipalvelut ovat. Tässä luvussa esitetään, millaisia määritelmiä pilvilaskennalle on annettu ja mitä sillä yleensä käytännössä tarkoitetaan, sekä mitä pilvipalvelulla tarkoitetaan tässä tutkielmassa. Lisäksi pohditaan, mitä pilvilaskenta oikeastaan on: mitä se tarjoaa käyttäjille tai palveluntarjoajille sekä mitä hyötyä tai haittaa siitä on.

2.1 Pilvilaskenta ja pilvipalvelut

Pilvilaskenta viittaa palveluihin, joita suuret palvelinkeskukset tarjoavat Internetin yli asiakkailleen. Nämä palvelut voivat olla sovelluksia tai tietokonelaitteistoa, kuten laskentatehoa tai levytilaa, joita pilvipalveluntarjoajat tarjoavat asiakkailleen etäkäytettäväksi tarpeen mukaan [2]. Erilaiset palvelut pilvessä muodostavat palvelutyyppejä, joita esitellään tarkemmin alaluvussa 2.2. Sana “pilvi” viittaa palvelun abstraktiin sijaintiin Internetissä.

Lyhyesti voisi sanoa, että palvelinkeskuksen palvelimet ja ohjelmistot muodostavat pilven (engl. cloud). Mikäli pilvi on julkisessa käytössä ja kuka tahansa voi ostaa sieltä resursseja omaan käyttöönsä, kutsutaan sitä julkiseksi pilveksi (engl. public cloud) ja mikäli palvelinkeskus on rajoitetulle käyttäjäryhmälle tarkoitettu, puhutaan yksityisestä pilvestä (engl. private cloud). Armbrust et al. [1] määrittelevät kuitenkin vain julkiset pilvet pilvipalveluiksi ja erottaa yksityisen pilven omaksi, erilliseksi käsitteekseen. Näiden lisäksi joskus puhutaan yhteisöpilvestä (engl. community cloud) ja hybridipilvestä (engl. hybrid cloud), jotka sijoittuvat jonnekin julkisen ja yksityisen pilven välimaastoon - tai voivat olla kumpaakin [10]. Tässä tutkielmassa pilvellä tarkoitetaan kuitenkin ensisijaisesti julkista pilveä.

Pilvipalvelun määritelmään liitetään useimmiten seuraavat ominaispiirteet [10, 1]:

1. Palvelulla on näennäisesti rajaton määrä resursseja. Asiakas voi vuokrata pilvestä lisää resursseja tarpeen mukaan lähes rajattomasti.

2. Resurssien saanti on joustavaa, eli lisäresurssien käyttöönotto on nopeaa ja niitä pystyy vapauttamaan tai vuokraamaan lisää milloin tahansa ilman merkittävää viivettä. Resurssit voivat joissain tapauksissa skaalautua automaattisesti tarpeen mukaan.

3. Resurssien saatavuus on korkealla tasolla, eli asiakkaalla on pääsy resursseihin milloin tahansa ja mistä tahansa Internetin yli.

4. Hinnoittelu perustuu käyttöön. Asiakas voi maksaa palvelusta suoraan käyttämiensä CPU-tuntien tai siirrettyjen datamäärien perusteella.

5. Pilvipalvelun tilaajalla ei ole tarvetta suurelle alkupääomalle. Pilvestä saa käyttöön suuret resurssit ilman käynnistyskuluja.

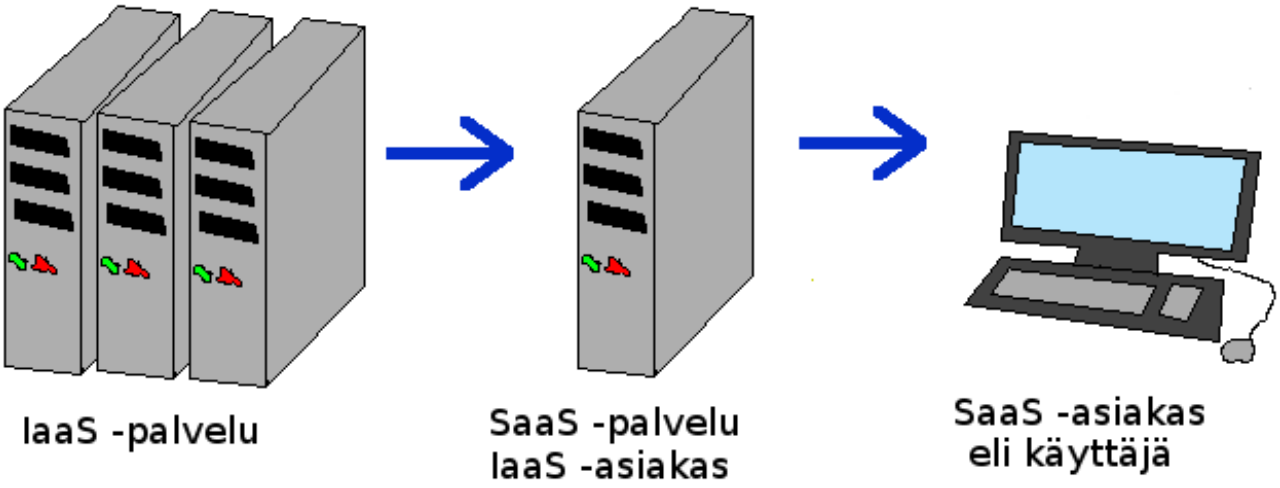
2.2 Palvelutyypit ja osapuolet

Pilvipalvelut voidaan jaotella useisiin eri palvelutyyppeihin. Sovelluspalveluista käytetään nimitystä *Software as a Service* eli SaaS ja laitteistopalveluista nimitystä *Infrastructure as a Service* eli IaaS. Pilvipalveluihin yhdistetään myös muita palvelumalleja, kuten *Platform as a Service*, joka sijoittuu hierarkiassa SaaS- ja IaaS-palveluiden välimaastoon tarjoten asiakkaalle sekä infrastruktuurin että ohjelmistoalustan palvelun tuottamista varten [2]. Koska palvelutyyppien erottelu ei ole aina yksiselitteistä, tässä työssä eritellään palvelut vain IaaS- ja SaaS-palveluiksi. IaaS-palvelu on käytännössä palvelu, jossa asiakas saa käyttöönsä laskentatehoa ja levytilaa verkon yli käytettäväksi. Käytännössä IaaS-palvelu toteutetaan useimmiten virtualisoinnin avulla [18]. Asiakas saa näennäisesti oman, erillisen tietokonelaitteiston käyttöönsä. SaaS-palvelussa asiakas voi käyttää jotakin sovellusta tai sovelluksia verkon yli aina tarvittaessa mistä päin maailmaa tahansa.

Eri osapuolet pilvipalveluliiketoiminnassa voidaan jakaa karkeasti kolmeen tahoon: IaaS-palveluntarjoajat, IaaS-asiakkaat ja SaaS-asiakkaat. Lisäksi IaaS-palveluntarjoajat sekä IaaS-asiakkaat toimivat usein myös SaaS-palveluntarjoajina, eli valjastavat fyysisen infrastruktuurin ohjelmistopalvelun tuottamiseen.

IaaS-palveluntarjoaja on palvelinkeskuksen omistava, hallinnoiva ja sitä ylläpitävä taho, usein suuryritys, esimerkiksi Amazon. IaaS-asiakas puolestaan on palvelinkeskuksen laitteistoa vuokraava osapuoli, esimerkiksi pienempi yritys, joka on ulkoistanut palvelimiensa fyysisen ylläpidon IaaS-palveluntarjojan vastuulle. SaaS-palveluntarjoaja on ohjelmistopalveluja loppukäyttäjille tarjoava taho. SaaS-palveluntarjoajien joukko on hyvin laaja: SaaS-palveluita tarjoavat sekä suuryritykset, yhteisöt että pienyritykset ja jopa yksityishenkilöt. SaaS-asiakas on usein yksittäinen loppukäyttäjä, joka käyttää jotakin verkkopalvelua. Esimerkkinä mainittakoon Google Docs joka on SaaS-palvelu ja jonka käyttäjät ovat usein yksityisiä henkilöitä.

Tämä jako ei kuitenkaan ole täysin ehdoton. SaaS-asiakas voi olla myös esimerkiksi yritys, joka ostaa SaaS-palvelun työntekijöidensä käyttöön. Tyypillistä on, että IaaS-asiakkaat hyödyntävät vuokraamaansa infrastruktuuria tarjoamalla edelleen ohjelmistopalveluita omille asiakkailleen, jolloin IaaS-asiakas on monesti samalla myös SaaS-palveluntarjoaja. Kuvassa 1 havainnollistetaan palveluntarjoaja–asiakas -hierarkiaa.



Kuva 1: Palvelutyyppien välinen hierarkia, nuolet osoittavat palveluntarjoajasta asiakkaaseen.

2.3 Edut ja haitat

Pilvipalveluiden edut ovat ilmeisiä: Palvelut skaalautuvat joustavasti suurillekin käyttäjämäärille. Ylläpitäjällä ei ole huolia fyysisen infrastruktuurin ylläpidosta tai päivittämisestä. Laskentatehoa on saatavilla lähes loputtomiin ja kulut nousevat vain lineaarisesti resurssien kasvaessa. IT-infrastruktuurin tarpeita ei arvioida kauaksi tulevaisuuteen, sillä kun palvelu tarvitsee lisää resursseja, niitä voidaan hankkia lisää hetkessä ilman palvelukatkoksia. Lisäksi aloituskustannukset ovat lähes olemattomat. [19]

Pilvipalvelut soveltuvatkin hyvin esimerkiksi startup-yrityksille tutkimus- ja kehitystyöhön nopeiden ratkaisujen ja pienten aloituskustannusten vuoksi. Ominaispiirteidensä vuoksi pilvipalvelut sopivat myös testaamiseen ja ohjelmistokehitykseen. Ne mahdollistavat myös helpon tavan kokeilla erilaisia palvelukonsepteja investoimatta suuria määriä rahaa. [12]

Luonnollisesti pilvipalveluiden käyttöön sisältyy myös ongelmia. Pilvipalveluntarjoajalla on pääsy käytännössä kaikkeen siihen tietoon, mitä asiakkaat pilvessä säilyttävät. Tämä on usein ongelma sekä asiakasyrityksen että loppukäyttäjän kannalta. Voiko pilvipalveluntarjoajaan luottaa?

Gens [5] osoittaa, että IT-alan johtohenkilöt pitävät tietoturvaa selvästi suurimpana huolenaiheena pilvipalveluissa. Samassa tutkimuksessa nähdään, että muita pilvipalveluasiakkaiden mielestä olennaisia seikkoja ovat saatavuus ja suorituskyky. IaaS-asiakkaan täytyy laskea sen varaan, että palveluntarjoaja pystyy tarjoamaan riittävän vakaan infrastruktuurin ja riittävästi suorituskykyä. Lisäksi jatkuvaan ja vaativaan käyttöön pilvipalveluiden laskutusmalli ei välttämättä ole edullisin mahdollinen. Ongelmaksi voi muodostua myös olemassaolevien palveluiden ja infrastruktuurin integroiminen pilvipalveluun,

pilvipalveluinfrastruktuurin rajoitettu muokattavuus sekä eri pilvipalveluiden yhteensopivuus mahdollinen palveluntarjoajan vaihtaminen huomioiden.

3 Pilvipalveluiden tietoturvavaatimukset ja -riskit

Tietoturva on kenties suurin yksittäinen ongelma pilvipalveluissa ja siihen liittyen on tehty paljon tutkimusta. Asiakkaan näkökulmasta ikävin yksityiskohta lienee se, että palveluntarjoajalla on täysin rajoittamaton pääsy asiakkaiden tietoihin. Lisäksi asiakkaan täytyy luottaa palveluntarjoajaan myös tiedon eheyden ja saatavuuden osalta, mistä kerrotaan lisää alaluvussa 3.2. Huomion arvoista on myös se, että pilvessä toimiva verkkopalvelu on korkeintaan yhtä turvallinen kuin itse pilvipalvelukin. Joissain tapauksissa asiakkaan tietoturvavaatimukset voivat olla jopa korkeammat kuin palveluntarjoajan. Tämän vuoksi onkin itsestään selvää, ettei esimerkiksi Suomen Poliisi voi missään nimessä siirtää infrastruktuuriaan julkiseen pilveen. Lisäksi ei tule unohtaa, että myös perinteiset tietoturvaongelmat ovat useimmiten olemassa myös pilvipalveluissa normaaliin tapaan.

Tässä luvussa tarkastellaan aluksi riskejä eri näkökulmista ja eri palvelutyypeissä. Sen jälkeen pohditaan asiaa tietoturvan perusvaatimuksia käsitteiden kautta, ja lopulta siirrytään konkreettisempiin asioihin, kuten löydettyihin tietoturvahaavoittuvuuksiin ja käytännön tietoturvakysymyksiin.

3.1 Riskit eri näkökulmista

Pilvipalveluiden palvelutyyppien hierarkia muodostaa useita käyttäjätasoja, joilla on erilaisia vaatimuksia ja prioriteettejä tietoturvan suhteen. Palvelutyyppejä koskee myös osin erilaiset tietoturvaongelmat. Tietoturvariskit voivat kuitenkin olla myös periytyviä: tietoturva-aukko IaaS-palveluntarjoajan järjestelmässä on riski myös IaaS-asiakkaille.

Pilvipalveluissa riskit voisi karkeasti jaotella kahteen osaan: ulkoiset riskit eli perinteiset tietoturvaongelmat, jotka koskettavat kaikkia verkossa olevia tietokoneita, sekä sisäiset riskit eli pilvipalvelusta itsestään johtuvat uhat. Ulkoiset riskit ovat yleisesti ottaen asiakkaan vastuulla ja sisäiset riskit palveluntarjoajan vastuulla. Asiakkaan täytyy esimerkiksi huolehtia, ettei vuoda salasanaansa tai omalla toiminnallaan aiheuta tietoturva-aukkoja. Palveluntarjoajan puolestaan täytyy huolehtia, ettei asiakkaan yksityiset tiedot vuoda heidän puoleltaan esimerkiksi ohjelmistovirheen tai epärehellisen työntekijän vuoksi.

SaaS-palveluita käytetään usein www-selaimen avulla. Tällöin huomionarvoisia asioita ovat useat web-sovelluksiin liittyvät seikat. Näitä ovat muun muassa tyypilliset web-sovellusten tietoturva-aukot, kuten SQL-injektiot ja XSS (Cross Site Scripting), sekä käyttäjän web-selaimen tietoturva [6]. Täytyy myös muistaa, että HTTP ei ole oletusar-

voisesti salattu protokolla, joten myös verkkoliikenteen turvallisuus täytyy huomioida [8]. Esimerkkinä palveluntarjoajan täytyy tarjota TLS-salattu web-yhteys verkkoliikenteen turvallisuuden takaamiseksi. Toisaalta käyttäjän vastuulla on huolehtia, että myös web-selain käyttää TLS-salausta.

Tämä työ keskittyy enemmän IaaS-palveluiden tietoturvavaatimuksiin ja -ongelmiin, joskin on hyvä huomata, että monia seikkoja voi soveltaa myös SaaS-palveluissa. IaaS-palveluiden kannalta huomionarvoisia asioita ovat esimerkiksi IaaS-asiakkaan infrastruktuurin hallintatyökalujen turvallisuus. Asiakkaan täytyy jotenkin pystyä varaamaan tai tuhoamaan hallinnoimiaan resursseja, kuten virtuaalipalvelimia tai verkkolevytilaa. Tämä hoidetaan usein web-käyttöliittymän kautta.

Palveluntarjoajat jakavat resurssit asiakkaille usein virtuaalikoneiden avulla. Virtualisoinnin toimivuus sekä turvallisuus ja virtuaalipalvelinten eristäminen muista samalla fyysisellä palvelimella suoritettavista prosesseista on eräs pilvipalveluiden merkittävistä haasteista [16]. Tämä on kriittinen seikka myös pilvipalveluntarjoajan oman järjestelmän tietoturvan vuoksi. Usein kuitenkin IaaS-asiakas on itse viimekädessä vastuussa tietoturvastaan ja mahdollisen tietoturva-aukon uhri on kuitenkin useimmiten käyttäjä - ei palveluntarjoaja. [17]

Virtuaalipalvelimen tietoturva perinteisessä mielessä on IaaS-asiakkaan eli virtuaalipalvelimen hallinnoijan vastuulla: virtuaalipalvelin on loogisesti tavallinen verkossa oleva tietokone, jota koskee samat ohjelmistopohjaiset tietoturvaongelmat kuin mitä tahansa tietokonetta. Näin ollen tietoturva-aukko virtuaalipalvelimelle asennetussa ohjelmistossa ei ole palveluntarjoajan ongelma.

IaaS-palveluita käytetään usein myös tiedostojen varastoimiseen esimerkiksi varmuuskopioina tai saatavuuden varmistamiseksi. Asiakkaan datan luottamuksellisuus, eheys ja saatavuus ovat perusvaatimuksia missä tahansa tietoturvallisessa järjestelmässä. Näiden ja pilvipalveluiden suhteeseen perehdytään seuraavaksi.

3.2 Tietoturvavaatimukset

Tässä alaluvussa käydään läpi vaatimuksia, joita tietoturvalliselta palvelulta edellytetään yleisellä tasolla. Vaatimukset huomioidaan erityisesti IaaS-palveluntarjoajien ja IaaS-asiakkaiden näkökulmasta.

Pilvipalveluissa tyypillisessä tapauksessa IaaS-asiakas siirtää vastuun fyysisen laitteiston ylläpidosta pilvipalveluntarjoajalle. Tämä on yksi pilvipalveluiden suurimmista eduista. Samalla se on myös yksi suurimmista riskeistä: asiakas menettää laitteistonsa fyysisen hallinnan, joutuu jakamaan saman fyysisen laitteiston muiden käyttäjien kanssa sekä joutuu luottamaan yksityisyytensä ja kaiken datansa pilvipalveluntarjoajan käsiin. Tämä

luo pilvipalveluille hieman normaalista poikkeavia tietoturvavaatimuksia.

Seuraavaksi tutustutaan tietoturvan vaatimukset määritteleviin käsitteisiin ja siihen, mikä niiden merkitys on pilvipalveluissa.

- **Saatavuus** on yksi pilvilaskennan peruselementtejä. Pilvipalveluita käytetään palvelumallista riippumatta poikkeuksetta jonkin verkon - yleensä Internetin - kautta, joten palvelusta ei ole mitään hyötyä, mikäli se ei ole saatavilla tarvittaessa. Saatavuuden vuoksi on myös tärkeää, että asiakas on tietoinen sopimuksestaan palveluntarjoajan kanssa. Mikäli kuukausimaksu myöhästyy tai käyttäjä rikkoo sopimusehtoja, on vaara että palvelu suljetaan ja asiakas menettää tiedostonsa [3]. Tyypillisesti sopimusehdoissa palveluntarjoaja takaa jonkin saatavuustason palvelulle, esimerkiksi 99,9%. Saatavuutta voidaan parantaa monistamalla palvelua eri maantietellisiin sijainteihin ja eri palveluntarjoajien verkkoihin.

- **Luottamuksellisuudella** tarkoitetaan asiakkaan tiedostojen salassapitoa tallennuksen ja siirron aikana. Luottamuksellisuus - tai sen puute - koetaan yhdeksi suurimmista ongelmista pilvipalveluissa [19]. Jokainen käyttäjä on vastuussa tiedostojensa turvallisuudelta omalta osaltaan itse, mutta myös palveluntarjoajalla on vastuu asiakkaidensa tiedostoista. Teknisesti palveluntarjoajan on helppo päästä käsiksi kenen tahansa asiakkaidensa tiedostoihin. Käyttäjän täytyy luottaa palveluntarjoajaan siinä, ettei palveluntarjoaja käytä mahdollisuuksiaan väärin. Lisäksi asiakkaan täytyy luottaa palveluntarjoajan turvatoimiin, ettei myöskään kolmas osapuoli pääse palveluntarjoajan oikeuksilla asiakkaan tietoihin käsiksi tarkoituksella tai vahingossa. Jos asiakas kuitenkin paljastaa salasanan itse tai omalla toiminnallaan aiheuttaa tietoturva-aukkoja, ei palveluntarjoaja ole näistä vastuussa. Tämä pätee sekä IaaS-palveluiden että SaaS-palveluiden palveluntarjoaja–asiakassuhteessa. Ratkaisuna luottamuksellisuuteen on salausmenetelmien käyttäminen sekä tiedonsiirrossa että varastoinnissa. Tällöin kryptografisia avaimia ei voi säilyttää samassa palvelussa.

- **Eheys** tarkoittaa tietoturvassa tiedon oikeellisuutta ja paikkansa pitävyyttä. Pilvipalveluissa tämä on huomionarvoinen asia, sillä kaikki tiedonsiirto tapahtuu oletusarvoisesti epäluotettavaa verkkoa pitkin. Asiakkaan täytyy luottaa siihen, ettei verkkoliikenteen epäluotettavuuden tai ohjelmistovirheen vuoksi tapahdu tiedostojen vioittumista. Tämän lisäksi täytyy varmistua siitä, ettei kolmas osapuoli oikeudettomasti pysty muuttamaan tiedostoja verkkolevyllä tai siirtovaiheessa. Palveluntarjoaja on tästä osaltaan vastuussa. Ratkaisuna eheyteen liittyviin ongelmiin ovat digitaaliset allekirjoitukset ja tiivistealgoritmit. [3].

- **Pääsynvalvontaa** tarvitaan palvelun käyttäjien käyttöoikeuksien hallinnoimiseen

ja käyttäjien tunnistamiseen. Usein eri käyttäjillä on omat henkilökohtaiset tiedostot ja lisäksi eri käyttäjillä voi olla eri käyttöoikeuksia. Palvelussa voi olla esimerkiksi peruskäyttäjiä ja ylläpitäjä-käyttäjiä. Pääsynvalvonta hoidetaan useimmiten joko käyttäjätunnuksen ja salasanan avulla (SaaS- ja web-palvelut) tai kryptografisten avainten avulla (IaaS-palvelut).

- **Hallinta** tarkoittaa mahdollisuutta säännöstellä palvelun käyttöä ja näkyvyyttä lyhyellä varoitusajalla. Asiakkaalla täytyy siis olla pääsy infrastruktuurinsa tilan hallitsemiseen reaaliajassa - esimerkiksi asiakkaan täytyy pystyä halutessaan ajamaan verkkopalvelunsa alas tai poistamaan tiedostoja verkosta. Käytännössä hallinta on toteutettu usein jonkinlaisen web-rajapinnan kautta.

- **Seuranta** on tärkeä ominaisuus asiakkaalle, jonka täytyy täytyy saada reaaliajassa yksityiskohtaista tietoa infrastruktuurin tilasta, kuten virtuaalipalvelinten ja verkon kuormituksesta ja levytilan käyttöasteesta. Lisäksi asiakkaalla täytyy olla mahdollisuus tarkastella logeja, eli mitä järjestelmässä on tapahtunut tiettynä ajankohtana.

3.3 Esimerkkejä toteutuneista tietoturvariskeistä

Ideaalisessa, luotettavassa ja turvallisessa pilvipalvelussa tietoturvavaatimusten tulisi täyttyä ilman ehtoja. Näin ei kuitenkaan käytännössä aina ole. Seuraavaksi esitellään lyhyesti muutamia tunnettuja tapauksia, missä pilvipalvelun tietoturva on pettänyt ja kaikki tietoturvavaatimukset eivät ole täyttyneet. Ongelmien ratkaisuja esitellään luvussa 4.

Merkittäviä palvelukatkoksia on ollut monilla suurilla palveluntarjoajilla, esimerkkinä Google Mail, Hotmail, Amazon S3 ja MobileME. Maaliskuussa 2009 Google Docs-palvelussa todettiin tietoturva-aukko, jonka seurauksena käyttäjien yksityisiä dokumentteja näkyi muille käyttäjille. [3]

Vuonna 2008 pilvipalveluiden luotettavuus kyseenalaistettiin, kun verkkolevytilaa tarjonnut yhtiö LinkUp tuhosi ylläpitäjän virheen vuoksi lähes puolet käyttäjiensä tiedostoista. Jotkut verkkolevytilaa tarjoavat palvelut puolestaan ovat pyrkineet ulkoistamaan varmuuskopioinnin ja vanhojen varmuuskopioiden säilyttämisen kolmansille osapuolille, joka osaltaan vähentää luottamusta ja lisää riskejä. [3]

Lokakuussa 2007 ohjelmisto- ja pilvipalveluliiketoimintaan erikoistuneen Salesforce.com -palvelun työntekijä todettiin syylliseksi niin sanottuihin phishing-hyökkäyksiin yrityksen asiakkaita vastaan. Työntekijä oli myös vuotanut asiakkaiden tietoja ulkopuolisille. [19]

Tietoturvavuodon sattuessa palveluntarjoaja on useimmiten korvausvelvollinen, mikäli hyökkäys on suoritettu palvelun sisältä käsin. Sen sijaan julkisesta verkosta tulleen tietomurron kohdalla näin ei aina ole.

4 Tietoturvaratkaisut pilvipalveluissa

Edellisessä luvussa esiteltiin tietoturvariskejä ja -ongelmia pilvipalveluihin liittyen. Näihin ongelmiin on kehitetty sekä teorian että käytännön tasolla erilaisia ratkaisuja, joihin tutustutaan seuraavaksi. Aluksi perehdytään pilvipalveluita varten kehitettyihin tietoturvamalleihin. Tämän jälkeen luetellaan käytännön tietoturvaongelmia ja niiden ratkaisuja. Lopuksi arvioidaan Amazon EC2-palvelun tietoturvaratkaisuja ja turvallisuutta käytännössä ja todetaan, että pilvipalveluilla voi olla myös positiivisia vaikutuksia tietoturvaan.

4.1 Pilvipalveluiden tietoturvamallit

Tässä luvussa esitellään pari teoreettista mallia, joiden tavoitteena on parantaa pilvipalveluiden tietoturvaa ja lisätä luottamuksellisuutta. Ensimmäiseksi esiteltävä TCCP (Trusted Cloud Computing Platform) on alusta, jonka tavoitteena on ratkaista palveluntarjoajan ja asiakkaan välinen luottamusongelma IaaS-palveluissa. Tämän jälkeen tutustutaan SecureCloud tietoturvamalliin, jonka tavoitteena on integroida useita pilvipalveluita yhdeksi loogiseksi järjestelmäksi.

TCCP-alustalle on tarkka ja yksityiskohtainen määritelmä, jonka perusteella voitaisiin tehdä myös ohjelmistototeutus. Sen sijaan SecureCloud on ainoastaan teoreettinen tietoturvamalli, ei spesifikaatio. SecureCloud-mallin toteuttamiseksi pitäisi asiaa tarkastella huomattavasti syvemmin. Tässä työssä ei kuitenkaan perehdytä kumpaankaan yksityiskohtaisesti, vaan ainoastaan selitetään toimintaperiaate ja vaikutukset yleisellä tasolla.

4.1.1 TCCP - Trusted Cloud Computing Platform

TCCP [13] eli Trusted Cloud Computing Platform on alusta, jonka tavoitteena on ratkaista IaaS-palvelumallissa asiakkaan ja palveluntarjoajan välinen luottamusongelma. Oletamus on, että palveluntarjoajan järjestelmäylläpitäjillä on teknisesti pääsy kaikille tietokoneille, joilla asiakkaiden virtuaalikoneita ajetaan. Näin ollen pahantahtoinen ylläpitäjä voisi kohtuullisen helposti käyttää väärin käyttöoikeuksiaan.

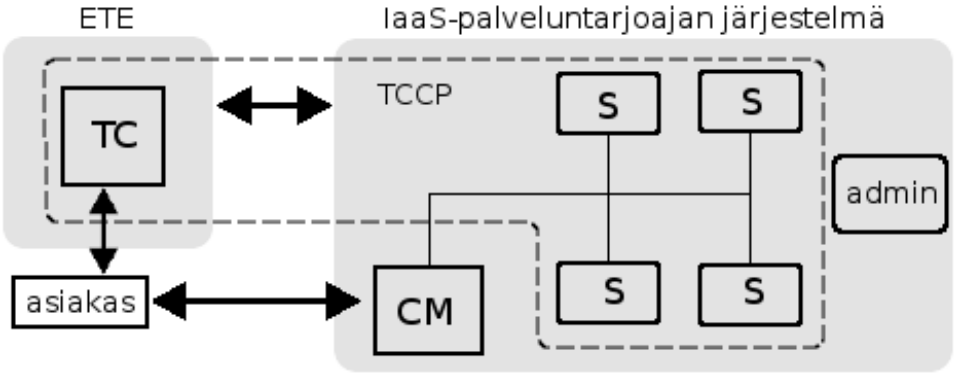
TCCP tarjoaa näennäisen niin sanotun suljetun laatikon ajoympäristön (engl. closed box execution envirnoment) asiakkaiden virtuaalikoneille. Tämän tarkoituksena on varmistaa, ettei järjestelmän ylläpitäjä pääse laajoilla käyttöoikeuksillaan tarkastelemaan tai muokkaamaan virtuaalikoneiden sisältöä. TCCP antaa asiakkaalle mahdollisuuden varmistaa, että palvelu todellakin käyttää luotettavaa TCCP-toteutusta ja on siten turvallinen.

TCCP-toteutuksen oleelliset komponentit ovat TVMM (trusted virtual machine monitor) sekä TC (trusted coordinator). Ajatus on, että jokaisella pilvipalvelun fyysisellä palvelimella on TVMM, jonka alaisuudessa asiakkaiden virtuaalikoneet ajetaan. TVMM-

monitorin tarkoitus on varmistaa virtuaalikoneiden paikallinen turvallisuus eli se, että fyysisesti kyseiselle koneelle pääsevä ylläpitäjä ei näe virtuaalikoneiden sisältöä. Jokainen palvelin sisältää myös TPM-sirun (trusted platform module), jonne on tallennettu uniikki kryptografinen avainpari.

TC puolestaan pitää kirjaa luotetuista palvelimista. TC varmistaa, että jokaisella palvelimella ajetaan asianmukaisesti TVMM-monitoria. Palvelinten yksilöintiin voidaan käyttää TPM-sirun sisältämää avainparia. TC voi dynaamisesti lisätä tai poistaa palvelimia luotettujen palvelinten listalta. Käyttäjät puolestaan voivat varmistaa TC:ltä, että palvelin, jolla heidän virtuaalikoneita ajetaan, on turvallinen ja luotettava.

TCCP määrittele vielä käsitteen ETE (external trusted entity), joka ylläpitää TC:tä. ETE on siis pilvipalveluntarjoajasta erillinen toimija, joka pystyy valvomaan IaaS-palvelun toimintaa riittävästi, jotta se voi varmistua siitä, että palvelun asiakkaiden virtuaalikoneet ovat asianmukaisesti suojattuja. Tärkein seikka koko TCCP-alustassa on se, ettei pilvipalveluntarjoajan henkilöstöllä ole pääsyä ETE-järjestelmään lainkaan, jolloin ETE yksin pystyy määrittelemään palvelinten turvallisuuden. Santos et al. [13] ehdottavat että ETE:ä hallinnoisivat erilliset luotetut tahot, kuten tietoturva-alan sertifioidut yritykset, joilla ei olisi motiivia liittoutua IaaS-palveluntarjoajan kanssa. TCCP käyttää eri tahojen väliseen kommunikointiin kryptografisia avaimia identiteetin ja turvallisuuden varmistamiseksi.



Kuva 2: TCCP-järjestelmän kaaviomalli. CM (cloud manager) eli IaaS-palveluntarjoaja hallinnoi palvelimia (S), joiden luotettavuuden TC (trusted coordinator) varmistaa. Nuolet kuvaavat eri tahojen välistä vuorovaikutusta.

TCCP:n idea lyhesti siis on, että pilvipalvelua suoritetaan sellaisella alustalla, että asiakas pystyy varmistumaan virtuaalikoneensa turvallisuudesta. Kolmas osapuoli koordinoi luotettuja palvelimia ja vahvistaa asiakkaalle palvelun luotettavuuden.

4.1.2 SecureCloud

SecureCloud [16] on tietoturvamalli, jossa on ideana integroida useita eri pilvipalveluja yhteen siten, että ne muodostavat yhtenäisen ja turvallisen järjestelmän. Lähtökohta on se, että organisaatio tai yritys tarvitsee järjestelmänsä toteuttamiseen palveluja monelta eri pilvipalveluntarjoajalta. Tarkoitus on kehittää malli, jonka avulla nämä eri pilvipalvelut muodostavat asiakasorganisaatiolle toimivan, yhtenäisen järjestelmän. Malli noudattaa palvelukeskeistä arkkitehtuuria (engl. service oriented architecture, SOA).

Ongelmakohtana nähdään pilvipalvelujen yhdistämisessä käyttäjien tunnistaminen, hallinta ja pääsynvalvonta. Ei ole käytännöllistä, että organisaation sisällä kullakin käyttäjällä on erilliset tunnukset kaikkiin järjestelmiin. Sen sijaan jokaisella käyttäjällä pitäisi olla yksi oma tunnus ja tämän perusteella käyttäjällä pitäisi olla automaattisesti pääsy niihin palveluihin, mihin käyttöoikeudet riittävät.

Toinen ongelma on eri palveluiden tietoturvapolitiikat, jotka eivät useimmiten ole yhteensopivia. Tätä varten tarvitaa komponentti, joka varmistaa, etteivät eri palveluiden tietoturvavaatimukset ole ristiriidassa ja että niitä noudatetaan. Lisäksi eri pilvipalvelut voivat joutua kommunikoimaan suoraan keskenään, jolloin jonkun tahon tulee huolehtia niiden välisestä turvallisesta viestinnästä.

Ratkaisuksi ehdotetaan järjestelmää, jossa jokaiselle palvelulle luodaan oma integrointikomponentti, nimeltään Service Integrator. Tämä komponentti tulkitsee palvelun käyttäjille näkyvään portaaliin siten, että palvelut ovat yhteneväisiä tietoturvaominaisuuksien puolesta ja pääsynhallinta toimii suoraan, eikä käyttäjien tarvitse huolehtia jokaisen järjestelmän turvallisuudesta erikseen. Integrointikomponentti sisältää moduulit palvelun hallintaan, luottamuksen hallintaan ja turvallisuuden hallintaan. Loogisesti vastaavat moduulit löytyvät myös jokaisesta pilvipalvelusta. Näiden avulla saadaan useasta pilvipalvelusta muodostettua yhtenäinen portaali.

SecureCloud on ainoastaan teoreettinen malli siitä, miten useita eri pilvipalveluita voisi hallita organisaation sisällä. Se pyrkii ratkaisemaan palveluiden eroavaisuuksista johtuvat integrointiongelmat.

4.2 Käytännön tietoturvaongelmia ja ratkaisuja

Tässä alaluvussa esitellään käytännön asioita, joita pilvipalvelua käyttävän tahon pitäisi huomioida tai tiedostaa. Jokainen asia käydään erikseen läpi, selvitetään miksi se on ongelma ja esitetään jokin mahdollinen ratkaisu ongelmaan yleisellä tasolla.

Lopuksi myös esitetään perustoimenpiteitä palvelun tai järjestelmän tietoturvan parantamiseksi. Nämä eivät välttämättä ole pilvipalveluihin erityisesti liittyviä seikkoja. On kuitenkin hyvä huomioida, että pilveen siirretty järjestelmä on useimmiten yhtä lailla

haavoittuva perinteisille tietoturvariskeille kuin muutkin järjestelmät.

4.2.1 Verkkoliikenteen turvallisuus

Pilven kanssa kommunikoidaan julkisen verkon kautta. Verkkoliikenteen salakuuntelu on tyypillinen ongelma verkkoturvallisuudessa. Salakuuntelu ei ole kovin yksinkertaista, mutta päätepisteiden välillä data kulkee salaamattomana reitittimien muistin läpi. Karkeasti ottaen siis kuka tahansa, jolla on pääsy reitin varrella olevaan reitittimeen, pystyy verrattain helposti kaappaamaan, estämään tai sotkemaan kaiken tietoliikenteen. Lisäksi myös monet langattomat lähiverkot ovat salaamattomia, jolloin kuuluvuusalueella oleva salakuuntelija pystyy kaappaamaan liikenteen.

Ratkaisuna tähän ovat kryptografiset menetelmät. Luottamuksellisuus saavutetaan verkkoliikenteen salaamisella, esimerkiksi SSL/TLS -protokollilla, ja eheys voidaan varmistaa digitaalisilla allekirjoituksilla, jossa voidaan hyödyntää esimerkiksi RSA-algoritmia [15].

4.2.2 Palvelun fyysinen sijainti

Asiakas ei välttämättä tiedä, missä maassa hänen hallinnoimansa infrastruktuuri, kuten virtuaalipalvelimet, tietokannat tai levytila, sijaitsevat. Pilvessä infrastruktuuri voi jopa olla hajautettu useaan paikkaan ympäri maapalloa. Tämä voi aiheuttaa muun muassa juridisia ongelmia eri maiden lainsäädäntöjen vuoksi [19]. Esimerkiksi joiden kryptografisten algoritmien käytössä on rajoituksia joissakin maissa [9]. Juridisten ongelmien lisäksi käyttäjä joutuu luottamaan palveluntarjoajan turvatoimiin fyysisen laitteiston suojauksessa ja ylläpidossa.

Tähän ongelmaan ei yksiselitteistä ratkaisua ole. Asiakkaan kannattaa näitä asioita silmällä pitäen lukea sopimusehdot ja tietoturvadokumentit sekä arvioida, onko palvelun fyysisen hallinnan puute merkittävä riski. Lisäksi sopimusehdoista kannattaa tarkistaa vahingonkorvausvastuu ja -ehdot riskien realisoituessa. Sopimusehdoista käy todennäköisesti myös ilmi, minkä maan lainsäädäntöä palvelussa noudatetaan.

4.2.3 Luottamus

Luottamus palveluntarjoajan ja asiakkaan välillä on yksi pilvipalveluiden suurimmista ongelmista. Asiakkaan täytyy muistaa, että palveluntarjoajalla on teknisesti mahdollisuus nähdä kaikki käyttäjän tiedostot. Vaikka palveluntarjoajan ja käyttäjän välillä on sopimus, joka takaa luotettavuuden, yksittäisen työntekijän luotettavuutta ei voi koskaan täysin taata.

Ratkaisuna asiakas voi salata itse tietoturvakriittisen sisällön siten, että salausavaimet

säilytetään pilven ulkopuolella. Myös ohjelmistopohjaisia tietoturvamalleja on kehitetty luottamuksen parantamiseksi. Näihin tutustuttiin luvussa 4.1.

4.2.4 Palvelun tilan seuranta

Infrastruktuuria pilvipalvelusta hankkiva asiakas on yleensä kiinnostunut laitteistonsa tilasta. Tyypillisiä mittareita ovat levytilan käyttöaste, prosessorin keskimääräinen kuormitus ja verkkoliikenteen määrä. Poikkeavat piikit esimerkiksi verkon kuormituksessa voivat viitata niin sanottuun brute force -hyökkäysyritykseen. Fyysisten mittarien lisäksi käyttäjän on hyvä pystyä keräämään dataa myös pilvessä suoritettavien ohjelmistojen tilasta.

Pilvipalveluntarjoajat tarjoavat usein myös fyysisen laitteiston seurantaominaisuutta muiden palvelujen ohella. Tämän lisäksi asiakas voi useimmiten IaaS-palveluissa ohjelmistopohjaisesti kerätä itse logeja järjestelmän käytöstä ja tilasta.

4.2.5 Sopimusehdot

Useimmat palvelut sisältävät jonkinlaiset sopimusehdot, jotka käyttäjän täytyy hyväksyä ennen kuin hän voi käyttää palvelua. Sopimusehdoissa asiakas voi kuitenkin antaa palveluntarjoajalle paljon laajempia juridisia oikeuksia kuin itse ymmärtää. Esimerkiksi Facebookin käyttäjät antavat palveluntarjoajalle oikeuden käyttää kaikkea palveluun lisäämäänsä sisältöä. [4]

Sopimusehdoista kannattaa olla ainakin sen verran selvillä, ettei tule ikäviä yllätyksiä. Harva jaksaa lukea monisivuista lakitekstiä sanasta sanaan, mutta yleisimpien palveluiden sopimusehdoista voi löytyä myös tiivistelmiä, missä käydään lyhyesti läpi ne asiat, jotka asiakasta todellisuudessa koskettavat.

4.2.6 Tyypillisiä tietoturvaratkaisuja

Tässä luvussa luetellaan käytännön tietoturvaratkaisuja, joita järjestelmän ylläpitäjä voi tehdä hyvän tietoturvatason saavuttamiseksi ja ylläpitämiseksi. Luetteloa voi soveltaa sekä IaaS-asiakkaan että SaaS- palveluntarjoajan järjestelmän kohdalla. Suurin osa mainituista seikoista ei liity erityisesti pilvipalveluihin, mutta on hyvä huomioida, että myös nämä niin sanotut perinteiset tietoturvariskit ovat olemassa myös pilvessä.

- Turhien palveluiden karsiminen. Ylimääräisiä taustaohjelmia ja tietoliikenneportteja ei ole syytä pitää auki palvelimella. Tämä pätee myös pilvessä olevien virtuaalipalvelinten kohdalla.

- Järjestelmän pitäminen ajan tasalla. Tietoturva on prosessi, joka edellyttää ylläpitäjältä ohjelmistojen päivittämistä ajan tasalle, mikäli tietoturva-aukkoja ilmenee.
- Tiedotteiden seuranta. Kaikkiin tietoturva-aukkoihin ei välttämättä saada korjausta välittömästi ongelman ilmaannuttua. Tällöin on hyvä olla tietoinen tietoturva-aukoista ja tarvittaessa ajaa haavoittuva palvelu alas, kunnes päivitys on saatavilla.
- Ohjelmakoodin auditointi. Erityisesti SaaS-palveluissa palveluntarjoajan täytyy tarjota käyttäjilleen turvallisia ohjelmistoja. Tällöin voidaan suorittaa ohjelmakoodin auditointi, eli ohjelman analysointi lähdekoodin tasolta lähtien ohjelman toiminnan oikeellisuuden varmistamiseksi ja virheiden havaitsemiseksi.
- Testaus. Perustoimenpiteenä voidaan pitää testausta, jossa tavoitteena on tietoisesti saada haavoittuminen aikaan järjestelmässä ja siten löytää tietoturva-aukko.
- Kriittisten palveluiden hajauttaminen. Tärkeitä palveluita ei kannata ajaa samalla palvelimella tai samassa loogisessa järjestelmässä. Mikäli yhdessä palveluista todetaan haavoittuvuus, seurauksena kaikki palvelut ovat potentiaalisesti haavoittuvia.
- Käyttöoikeuksien supistaminen. Joskus tietomurtoja sattuu, mutta tämä ei ole vakavaa, mikäli haavoittunutta palvelua on ajettu kapeilla käyttöoikeuksilla: näin ollen hyökkääjä ei todennäköisesti pysty hyödyntämään haavoittuvuutta juuri lainkaan.
- Käytettävyyden varmistaminen. Siirtyminen ylläpito-oikeuksien välillä tulee olla helppoa ja nopeaa siihen oikeutetuille käyttäjille, mutta se ei saa aiheuttaa ylimääräisiä tietoturvariskejä.
- Palveluiden monistaminen. Mikäli palvelun saatavuus on erityisen tärkeä kriteeri, palvelua voidaan monistaa usealle palvelimelle, mielellään eri maantieteellisiin sijainteihin. Pilvipalveluiden kohdalla oleellista olisi vielä palvelun monistaminen siten, ettei palvelu ole riippuvainen yhdestä pilvipalveluntarjoajasta.

4.3 Amazon EC2-palvelun turvallisuus

Tässä luvussa tarkastellaan Amazon EC2 (Amazon Elastic Computing Cloud)-palvelua tietoturvan kannalta. EC2 on osa Amazon Web Services -pilvipalvelujärjestelmää ja se tarjoaa joustavaa palvelinten virtualisointia asiakkaille.

Seuraavaksi arvioidaan palveluun rekisteröitymistä ja sen käyttöönottoa, tunnistautumista, verkkoturvallisuutta ja virtualisointia. Arviot perustuvat empiiriseen kokeiluun sekä Amazon Web Services -palvelun tietoturvadokumentteihin.

4.3.1 Rekisteröityminen ja käyttöönotto

Rekisteröityminen Amazon Web Services -palveluun tapahtuu TLS-salatun web-käyttöliittymän kautta. Käyttäjän täytyy antaa toimiva luottokortin numero ja puhelinnumero. Rekisteröityminen vahvistetaan siten, että käyttäjän puhelimeen soitetaan puhelu, jossa automaatti sanelee suojakoodin. Tämä suojakoodi tulee syöttää vahvistuslomakkeeseen.

Myös EC2-palvelun hallinta hoidetaan web-käyttöisen hallintapaneelin kautta. Käyttöliittymässä voi muutamassa minuutissa luoda virtuaalipalvelimen jollain Amazonin tietokannassa valmiina olevalla levykuvalla (engl. virtual machine image). Tietokannasta löytyy tuhansia levykuvia, lähinnä Windows- ja Linux-järjestelmistä eri jakelupaketteja ja versioita. Valittuaan haluamansa version käyttäjä määritelee kuinka tehokkaan palvelimen haluaa, jonka jälkeen virtuaalipalvelin luodaan ja se on valmis käytettäväksi muutamassa minuutissa.

4.3.2 Tunnistaminen ja varmennus

Luoduille virtuaalipalvelimille sisäänkirjautuminen tapahtuu kryptografisten avainparien avulla. Amazon EC2-palvelun hallintapaneelissa voi luoda avainpareja (engl. key pair). Luodessaan avainparin käyttäjä saa yksityisen avaimen. Julkinen avain puolestaan tallennetaan virtuaalipalvelimelle. Sen sijaan Amazon poistaa yksityisen avaimen järjestelmästään välittömästi, kun käyttäjä on saanut sen. Näin ollen mikäli käyttäjä kadottaa yksityisen avaimensa, sitä ei saa mistään takaisin, vaan joudutaan luomaan uusi avainpari.

Kirjautuminen sisään palvelimelle tapahtuu SSH-protokollalla siten, että kirjautumisavaimeksi annetaan yksityinen avain. Palvelin tarkistaa, että kirjautumisavain ja palvelimella oleva julkinen avain ovat toistensa pareja, jonka perusteella käyttäjä päästetään sisään. Kirjauduttuaan sisään käyttäjä voi sallia SSH-palvelimen asetuksista myös perinteisen salasanaan perustuvan varmennuksen.

4.3.3 Verkkoturvallisuus

Virtuaalipalvelimet ovat todellisuudessa Amazonin omassa sisäverkossa. Amazon on toteuttanut Internetin ja sisäverkon väliin rajapinnan, jonka kautta virtuaalipalvelimet kommunikoivat Internetiin.

Jokaisella palvelimella on myös oma julkinen IP-osoite. Virtuaalipalvelimet eivät kuitenkaan itse näe julkista IP-osoitettaan, vaan Amazonin tarjoama rajapinta muuntaa IP-osoitteet julkisen ja sisäisen verkon välillä. Sama rajapinta ei myöskään ohjaa kaikkea liikennettä ulkoverkosta sisäverkkoon: ainoastaan tiettyihin tietoliikenneportteihin tuleva

liikenne ohjataan palvelimelle. Käyttäjä voi itse hallintapaneelista avata portteja virtuaalipalvelimelleen. Näin rajapinta toteuttaa myös yksinkertaisen palomuurin.

Samalla fyysisellä alueella olevat virtuaalipalvelimet voivat kommunikoida keskenään myös suoraan sisäverkon IP-osoitteiden avulla. Tämä ei kuitenkaan mahdollista muihin kuin palomuurissa määriteltyihin portteihin yhdistämistä. Amazonin verkko estää IP-osoitteiden väärentämisen, ja havaitsee ja raportoi porttiskannausyrityksiä [14].

4.3.4 Virtualisointi

Virtualisointiin Amazon käyttää Xen Hypervisor -ohjelmistoa, joka on avoimen lähdekoodin alusta palvelinten virtualisointiin. Käyttäjillä ei ole suoraa pääsyä fyysiseen laitteistoon, kuten kiintolevyille, eivätkä käyttäjät näe muita samalla fyysisellä instanssilla ajettavia virtuaalikoneita. [14]

Amazonin oma massamuistin virtualisointikerros ylikirjoittaa ja puhdistaa käyttäjien poistamat tiedostot ja varmistaa, etteivät käyttäjien tiedostot voi sekoittua keskenään. Amazon kuitenkin mainitsee, että tiedostojensa turvallisuudesta huolissaan olevat käyttäjät voivat toteuttaa kryptatun tiedostojärjestelmän virtuaalilevyn päällä. [14]

4.3.5 Arvio Amazon EC2-palvelusta

Amazonin EC2-palvelun turvallisuus näyttäisi olevan melko korkealla tasolla. Tämän hetken standardien ja vaatimusten perusteella kriittistä huomauttamista ei löytynyt. Huomionarvoista kuitenkin on, että käyttäjä joutuu edelleen luottamaan täysin palveluntarjoajaan. Tietoturvadokumenttien ja selvitysten perusteella palveluntarjoaja on huolehtinut käyttäjän kannalta oleellisista tietoturvaseikoista varsin mallikkaasti [14]. Käyttäjällä ei kuitenkaan ole pääsyä palveluntarjoajan järjestelmään toteamaan, toimiiko järjestelmä todella niin kuin palveluntarjoaja väittää.

Kaikesta huolimatta palveluntarjoaja jättää käyttäjän vastuulle kuitenkin jonkin verran asioita. Käyttäjän tehtävä on huolehtia omista yksityisistä avaimistaan. Lisäksi virtuaalikoneiden sisällön varmuuskopiointi ja tietoturvakriittisen sisällön kryptaaminen on käyttäjän vastuulla [14].

4.4 Pilven positiiviset vaikutukset tietoturvaan

Pilvipalvelut eivät ominaispiirteistään huolimatta ole mustavalkoisesti aina huono asia tietoturvan kannalta. Monissa tapauksissa pilvellä voi olla positiivisia vaikutuksia tietoturvaan.

Luottamukseen liittyvistä riskeistä huolimatta käyttäjien tiedostot ovat usein todellisuudessa paremmassa tallessa pilvessä kuin käyttäjien tietokoneilla sekä saatavuuden että turvallisuuden kannalta [11]. Kannettava tietokone voidaan varastaa tai kovalevy voi rikkoutua. Pilvessä tiedostot ovat saatavilla aina ja kaikkialta, ja monet pilvipalvelut myös huolehtivat varmuuskopioista käyttäjän puolesta. Moni tavallinen käyttäjä ei huolehdi varmuuskopioista lainkaan. Pilvipalveluissa on yleensä myös kohtalaisen tason pääsynhallinta ja ainakin mahdollisuus salatulle yhteydelle.

Pilvipalveluissa tietoturvasta yleisellä tasolla huolehtivat tietoturva-alan ammattilaiset [11]. Monilla pienillä tai keskisuurilla yrityksillä ei välttämättä ole selkeää tietoturvapolitiikkaa tai turvallisuudesta vastaavaa henkilöä. Tällöin pilveen siirtyminen voi parantaa tietoturvaa.

Näiden asioiden lisäksi pilvipalvelut voivat sisältää ominaisuuksia, joiden tarkoitus on parantaat asiakkaan tietoturvaa. Kuten edellisessä alaluvussa todettiin, esimerkiksi Amazonin EC2-palvelussa asiakkaiden virtuaalipalvelimet ovat eräänlaisen palomuurin takana, jolloin ainoastaan määrätyistä tietoliikenneporteista pääsee liikennettä sisään. Tämä on lähtökohtaisesti parannus tyypilliseen tapaukseen, jossa palvelin näkyy suoraan verkkoon ja auki oleviin portteihin voi lähettää ulkoapäin dataa rajoituksetta.

5 Yhteenveto

Tämän tutkielman tarkoituksena oli selvittää pilvipalveluiden kriittisimmät tietoturvaongelmat ja esitellä ratkaisuja niihin. Lisäksi tutustuttiin erääseen pilvipalveluun ja arvioitiin sen tietoturvatasoa.

Yhteenvetona voidaan todeta, että pilvipalvelut ovat vielä uudehko, mutta kasvava osa Internet-palveluita. Tietoturvan kannalta ongelmia pilvipalveluissa ovat muun muassa asiakkaan luottamus palveluntarjoajaan, pilvipalvelun ja virtualisoinnin toteuttaminen turvallisesti sekä verkkoliikenteen turvallisuus. Näihin on kehitetty erilaisia ratkaisuja sekä teorian että käytännön tasolla. Esimerkiksi luottamukseen liittyviä tietoturvaratkaisuja ei kuitenkaan vielä sovelleta käytännössä. Nykyisissä pilvipalveluissa käyttäjä tai asiakas joutuu käytännössä luovuttamaan yksityisyytensä palveluntarjoajan käsiin.

Vaikka palveluntarjoajan tehtävä on vastata omalta osaltaan palvelun tietoturvasta, kuten esimerkiksi virtualisoinnin ja palvelun seurannan toimivuudesta, on asiakkaan hyvä huomioida, että toteutuessaan tietomurto kohdistuu luultavasti palvelun käyttäjiin. Näin ollen asiakkaan kannattaa huolehtia myös itse mahdollisen tietoturvakriittisen sisällön suojaamisesta ja käsittelystä.

Mikäli asiakkaan tietoturvavaatimukset eivät ole erityisen korkeat, esimerkiksi Amazon EC2-palvelun turvallisuus riittänee asiakkaalle. Tällöinkin on kuitenkin hyvä tutustua tietoturvadokumentteihin ja käyttää tervettä harkintaa, heikentääkö pilveen siirtyminen tietoturvaa - ja jos heikentää, ovatko pilvipalvelun tarjoamat edut riittävät, jotta kompromissi kannattaa tehdä. Tietoturvan perimmäinen tarkoitus on kuitenkin tasapainottaa kulut ja mahdollisista tietoturvavuodoista aiheutuvat vahingot. Mikäli pilvipalvelu vähentää järjestelmän ylläpitokuluja selvästi, mutta heikentää tietoturvaa vain vähän, pilveen siirtyminen lienee järkevä valinta. Sen sijaan jos tietoturvavaatimukset ovat korkeat, mutta pilvipalvelun tarjoamat edut marginaaliset, ei ole syytä siirtyä pilvipalveluihin.

Kaikissa tapauksissa asiakkaan kannattaa kuitenkin muistaa oma vastuunsa omista tiedostoistaan. Vaikka palveluntarjoaja kuinka vakuuttaisi palvelun tietoturvan toimivan, tietomurron sattuessa sillä ei ole mitään merkitystä. Mikäli asiakkaan tietoturvavaatimukset ovat suuremmat, kuin palveluntarjoajan tietoturvavaatimukset, niin vaatimukset luultavasti eivät täyty.

Koska tietoturvapuutteet ovat yksi pilvipalveluiden suurimmista ongelmista, palveluntarjoajat panostavat näiden puutteiden korjaamiseen aktiivisesti. Tämän vuoksi pilvipalvelut saattavat monissa tapauksissa myös parantaa tietoturvaa - erityisesti jos tietoturvasta ei ole aiemmin erityisemmin huolehdittu.

Lähteet

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica ja Matei Zaharia. Above the clouds: A berkeley view of cloud computing. Tekninen raportti UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009. URL `http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html`.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica ja Matei Zaharia. A view of cloud computing. *Commun. ACM*, 53:50–58, April 2010. ISSN 0001-0782. doi: http://doi.acm.org/10.1145/1721654.1721672. URL `http://doi.acm.org/10.1145/1721654.1721672`.

[3] Christian Cachin, Idit Keidar ja Alexander Shraer. Trusting the cloud. *SIGACT News*, 40:81–86, June 2009. ISSN 0163-5700. doi: http://doi.acm.org/10.1145/1556154.1556173. URL `http://doi.acm.org/10.1145/1556154.1556173`.

[4] Facebook. Statement of Rights and Responsibilities. 2010. URL `http://www.facebook.com/terms.php`.

[5] F. Gens. New IDC IT Cloud Services Survey: Top Benefits and Challenges. *IDC eXchange*, 2009. URL `http://blogs.idc.com/ie/?p=730`.

[6] M.W. Halton. Security issues and solutions in cloud computing. *Network Security News*, 2010. URL `http://wolfhalton.info/2010/06/25/security-issues-and-solutions-in-cloud-computing/`.

[7] Brian Hayes. Cloud computing. *Commun. ACM*, 51:9–11, July 2008. ISSN 0001-0782. doi: http://doi.acm.org/10.1145/1364782.1364786. URL `http://doi.acm.org/10.1145/1364782.1364786`.

[8] M. Jensen, J. Schwenk, N. Gruschka ja L.L. Iacono. On technical security issues in cloud computing. *Cloud Computing, 2009. CLOUD '09. IEEE International Conference on*, sivut 109 –116, 2009. doi: 10.1109/CLOUD.2009.60.

[9] Bert-Jaap Koops. Crypto Law Survey. 2010. URL `http://rechten.uvt.nl/koops/cryptolaw/`.

[10] P. Mell ja T. Grance. The NIST definition of cloud computing. *National Institute of Standards and Technology (NIST)*, 2009.

[11] N. Oza, K. Karppinen ja R. Savola. User experience and security in the cloud – an empirical study in the finnish cloud consortium. *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, sivut 621 –628, 2010. doi: 10.1109/CloudCom.2010.114.

[12] S. Ramgovind, M.M. Eloff ja E. Smith. The management of security in cloud computing. *Information Security for South Africa (ISSA), 2010*, sivut 1 –7, 2010. doi: 10.1109/ISSA.2010.5588290.

[13] Nuno Santos, Krishna P. Gummadi ja Rodrigo Rodrigues. Towards trusted cloud computing. *Proceedings of the 2009 conference on Hot topics in cloud computing*, HotCloud'09, sivut 3–3, Berkeley, CA, USA, 2009. USENIX Association. URL `http://portal.acm.org/citation.cfm?id=1855533.1855536`.

[14] Amazon Web Services. Amazon Web Services: Overview of Security Processes. 2010. URL `http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf`.

[15] U. Somani, K. Lakhani ja M. Mundra. Implementing digital signature with rsa encryption algorithm to enhance the data security of cloud in cloud computing. *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on*, sivut 211 –216, 2010. doi: 10.1109/PDGC.2010.5679895.

[16] H. Takabi, J.B.D. Joshi ja Gail-Joon Ahn. Securecloud: Towards a comprehensive security framework for cloud computing environments. *Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual*, sivut 393 –398, 2010. doi: 10.1109/COMPSACW.2010.74.

[17] Todd. Top 5 myths of cloud computing security. *Cloud Security Blog*, 2010. URL `http://cloudsecurity.trendmicro.com/top-5-myths-of-cloud-computing-security/`.

[18] L. Youseff, M. Butrico ja D. Da Silva. Toward a unified ontology of cloud computing. *Grid Computing Environments Workshop, 2008. GCE '08*, sivut 1 –10, 2008. doi: 10.1109/GCE.2008.4738443.

[19] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian ja Aoying Zhou. Security and privacy in cloud computing: A survey. *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*, sivut 105 –112, 2010. doi: 10.1109/SKG.2010.19.