Pilvipalveluiden haavoittuvuudet IaaS -palvelumuodossa

Oulun Yliopisto
Tietojenkäsittelytieteiden laitos
Kandidaatintyö
Joni Kerkelä
9.1.2016

Tiivistelmä

Tässä työssä käydään läpi pilvipalveluiden "infrastructure as a service" eli IaaS -palvelumuodon keskeisiä haavoittuvuuksia. Haavoittuvuuksia tarkastellaan IaaS -palvelumuodon ulkoisten sekä sisäisten haavoittuvuuksien kautta. Ulkoiset haavoittuvuudet aiheutuvat erityisesti palvelun ulkopuolisten pahantahtoisten käyttäjien toiminnasta palvelua vastaan ja sisäiset haavoittuvuudet palvelun teknisestä toteutuksesta. Kyseisen aiheen tutkiminen on relevanttia, sillä IaaS -palvelut ovat laajasti käytetty palvelu, jonka suosio on edelleen nopeassa kasvussa. Palveluiden suosio johtuu niiden organisaatioiden tarpeisiin soveltuvista helposti käyttöön otettavista ja edullisista resursseista. Hyötyjen vastapainona ovat kuitenkin IaaS -palveluissa esiintyvät haavoittuvuudet, joiden huomioiminen on kriittistä haavoittuvuuksien vaikutusten vuoksi.

Tutkimuskysymyksenä on mitkä ovat IaaS -palvelumuodon keskeiset ulkopuolisista hyökkäyksistä johtuvat haavoittuvuudet ja palvelun teknisestä toteutuksesta johtuvat sisäiset haavoittuvuudet. Tutkimuskysymyksen avulla työn aihe rajataan yleisimpiin haavoittuvuuslähteisiin IaaS -palvelumuodossa. IaaS –palveluita käsittelevä aiempi kirjallisuus tukee valitun rajauksen relanvanttiutta, sillä sen mukaan ulkopuolisista hyökkäyksistä johtuvat haavoittuvuudet ja palvelun teknisestä toteutuksesta johtuvat haavoittuvuudet kattavat suuren osan IaaS- palvelumuodon haavoittuvuuksista kokonaisuudessaan.

Tutkimusmenetelmänä tutkielmassa käytetään käsitteellistä kirjallisuustutkimusta. Käsitteellisen kirjallisuustutkimuksen kautta työssä käydään läpi IaaS -palvelumuodon haavoittuvuuksia aiempaan kirjallisuuteen pohjautuen. Työn kirjallisuuskatsaukseen on pyritty keräämään lähdemateriaaliksi relevanteimpia tutkimusongelmaan liittyviä artikkeleita. Lähdemateriaalin relevanttius on pyritty varmistamaan käyttämällä tietojenkäsittelyn alan keskeisimpien julkaisujen artikkeleita sekä valitsemalla lähdemateriaaliksi tuoreimpia sekä eniten siteerattuja artikkeleita.

Aiemman kirjallisuuden kautta käy ilmi, että pilvipalveluiden palvelumuodoista juuri IaaS -palvelumuoto on merkittävin, sillä se muodostaa pohjan PaaS ja SaaS -palvelumuodoille sekä on organisaatioiden eniten käyttämä. Aiemman kirjallisuuden löydökset osoittavat, että IaaS -palvelumuodossa on erityisen runsaasti palvelun teknisestä toteutuksesta johtuvia haavoittuvuuksia sekä lukuisia palvelun ulkopuolisista hyökkäyksistä aiheutuvia haavoittuvuuksia. Työssä esiteltyjä teknisestä toteutuksesta johtuvia haavoittuvuuskategorioita ovat virtualisoinnista, pääsynvalvonnasta, API:sta sekä resurssienhallinnasta aiheutuvat haavoittuvuudet, joista jokaisella kategorialla on lukuisia yksittäisiä haavoittuvuusmuotoja. Palvelun ulkopuolisista hyökkäyksistä johtuvia haavoittuvuuskategorioita ovat puolestaan DDoS -hyökkäykset, injektiohyökkäykset sekä virtuaalikoneinstanssien hyväksikäyttö.

Avainsanat
IaaS, haavoittuvuus, virtualisointi, virtuaalikone, hyökkäys

Ohjaaja
Yliopistonlehtori, Ari Vesanen

Alkusanat

“A small step for me, a huge leap for information science.” - J. Kerkelä 2015

Sisällysluettelo

Lyhenteet

IaaS - Infrastructure as a service

PaaS - Platform as a service

SaaS - Software as a service

DSR - Design science research

SLA - Service level agreement

XSS - Cross-site scripting

VMM - Virtual machine monitor

XML - Extensible Markup Language

DDoS - Distributed Denial of Service

1. Johdanto

Tutkielman tarkoituksena on tutkia pilvipalveluiden “infrastructure as a service” (IaaS) -palvelumuodon keskeisiä tämänhetkisiä haavoittuvuuksia kirjallisuuslähteiden avulla. Kirjallisuuslähteisiin pohjautuen tutkielmassa tarkastellaan IaaS -palvelumuodon haavoittuvuuksia keskittyen teknisistä ratkaisuista sekä ulkoisista hyökkäyksistä aiheutuviin haavoittuvuuksiin. Työn aihe on merkittävä, sillä IaaS -palvelumuoto on laajasti käytetty ja jatkuvasti yleistyvä palvelu erityisesti organisaatioiden käytössä. Kaufman (2009) korostaa IaaS -palveluiden käytön laajuutta mainitsemalla, että palveluja käyttävät yritykset pienistä yrityksistä aina Fortune 500 -listan yrityksiin asti sekä hallitukset. IaaS -palvelumuodon yleistyminen on seurausta tämän hetken liiketoimintaympäristön aiheuttamista vaatimuksista, joita ovat esimerkiksi palvelun jatkuva saatavuus, skaalautuvuus sekä suorituskyky. Mainittuihin vaatimuksiin IaaS -palvelut vastaavat tarjoamalla asiakkaan käyttöön periaatteessa rajattoman määrän resursseja asiakkaan tarpeen mukaan, riippumatta asiakkaan sijainnista ja resurssitarpeen ajankohdasta. Armbrust et al. (2010) painottavat pilvipalveluiden tarjoamien resurssimäärän hyödyllisyyttä mainitsemalla, että asiakkaalle 1000 palvelimen käyttö tunnin ajan pilvipalvelun kautta ei maksa enempää kuin yhden palvelimen käyttö 1000 tunnin ajan. Tämän analogian mukaisesti organisaatioiden kannattaa hyödyntää pilvipalveluita käyttötapauksesta riippumatta saavuttaakseen mahdollisimman korkean IT-infrastruktuurin tehokkuuden.

IaaS -palveluiden tarjoamien mahdollisuuksien vastapainona täytyy huomioida palveluihin liittyvät ongelmat. IaaS -palveluissa ongelmia aiheuttavat erityisesti ulkoiset hyökkäykset sekä pilvipalveluiden teknisestä toteutuksesta johtuvat haavoittuvuudet. Runsaan käyttäjämäärän sekä suuren tietomäärän takia haavoittuvuuksien vaikutus pilvipalveluissa voi nousta suureksi. Tämän takia IaaS -palveluntarjoajien on huomioitava ja ehkäistävä vaikeasti hallittavia ja rahallisesti kalliita ongelmatilanteita aiheuttavia haavoittuvuuksia. Pilvipalveluiden palvelumuodoista erityisesti IaaS -palvelumuotoon liittyvät haavoittuvuudet ovat merkittäviä, sillä tätä palvelumuotoa käyttävät organisaatiot, jolloin haavoittuvuuksien aiheuttamien ongelmien vaikutus ja rahallinen arvo korostuu. Ongelmatilanteiden ehkäisy on mahdollista vain kun haavoittuvuuksien aiheuttajat on tunnistettu tehokkaasti.

1.1 Aiempi tutkimus

IaaS -palvelumuodon haavoittuvuuksista löytyy laajasti artikkeleita siihen nähden, että se on suhteellisen tuore liiketoimintaympäristössä käyttöön otettu teknologiaratkaisu. Julkaistut artikkelit käsittelevät kattavasti IaaS -palveluiden tekniseen toteutukseen sekä turvallisuuteen liittyviä ongelmia erityisesti organisaatioiden näkökulmasta. Julkaistuissa artikkeleissa käydään läpi myös yleisellä tasolla yksityisyyteen sekä lainopillisiin kysymyksiin liittyviä ongelmia. Aiempi tutkimus rakentaa perusteellisen pohjan haavoittuvuuksille yleisesti sekä erittelee keskeisiä haavoittuvuuksia yksityiskohtaisesti eri näkökulmista, painottuen kuitenkin enimmäkseen organisaatioiden näkökulmaan.

Erityisesti viime vuosina pilvipalveluiden haavoittuvuuksia ja ongelmia käsittelevien tutkimusten julkaisumäärä on ollut huimassa nousussa johtuen pilvipalveluiden yleistymisestä sekä yksityisten että yritysten käytössä. Suuri osa pilvipalveluita

koskevista tutkimuksista on keskittynyt palveluiden haavoittuvuuksien ja ongelmien kvalitatiiviseen tai kvantitatiiviseen analysoimiseen, mutta osa tutkimuksista käyttää lähestymistapana myös "Design science research" (DSR) metodeja, joiden pohjalta kyseiset tutkimukset pyrkivät tuottamaan artefakteja, joiden avulla palveluntarjoajat pystyvät ehkäisemään pilvipalveluiden haavoittuvuuksia.

1.2 Tutkimusongelma

Tutkimuskysymyksenä tutkielmassa on, mitkä ovat pilvipalveluiden IaaS -palvelumuodon tämänhetkiset keskeiset teknisistä ratkaisuista ja ulkopuolisista hyökkäyksistä aiheutuvat haavoittuvuudet. Ongelman rajaaminen pilvipalveluiden IaaS -palvelumuotoon sekä keskittyminen haavoittuvuuksiin, jotka aiheutuvat teknisistä ratkaisuista sekä ulkopuolisista hyökkäyksistä, rajaa tutkielman fokuksen vaikutukseltaan ja rahalliselta arvoltaan merkittävimpiin haavoittuvuuksiin, johtuen siitä että organisaatiot käyttävät yleisesti IaaS -palvelumuotoa. Keskittymistä palvelun teknisestä toteutuksesta ja ulkopuolisista hyökkäyksistä aiheutuviin haavoittuvuuksiin tukee se että kyseiset haavoittuvuudet lukeutuvat pilvipalvelun turvallisuuteen liittyviin seikkoihin, jotka Grobauer, Walloscheck & Stöcker (2011) esittävät merkittävimmäksi esteeksi pilvipalveluiden yleistymiselle. IaaS palvelumuodon merkittävyyttä korostaa se, että pilvipalveluiden muut palvelumuodot eli PaaS ja SaaS rakentuvat IaaS -palvelumuodon ratkaisujen päälle (Gibson, Rondeau, Eveleigh, & Tan, 2012). Tutkimusmenetelmänä tutkielmassa käytetään käsitteellistä kirjallisuustutkimusta.

1.3 IaaS -palvelumuoto

IaaS on pilvipalveluiden palvelumuoto, jossa asiakas käyttää palveluntarjoajan tarjoamaa infrastruktuuria ohjelmiston ajamiseen. IaaS -palvelumuodossa palveluntarjoaja tarjoaa siis laitteisto-, varastointi-, palvelin- ja ohjelmistoresurssit, jolloin asiakkaan ei tarvitse huolehtia infrastruktuurin toteutukseen liittyvistä asioista ajaessaan sovellusta IaaS -palvelussa. (Subashini & Kavitha, 2011)

IaaS -palvelun vahvuuksia on skaalautuvuus, sillä palveluntarjoajalla on resurssipoolissa (eng. resource pool) suuri määrä resursseja, joita asiakas voi allokoida käyttöönsä tarpeen mukaan. Skaalautuvuuden johdosta organisaatiot voivat ottaa käyttöön resursseja lyhyessä ajassa virtuaalipalvelimien kautta, kuten Subashini & Kavitha (2011) toteavat. Resurssien skaalautuvuuden johdosta IaaS -palvelu on laajalti käytetty organisaatioiden sovellusten infrastruktuurina, sillä organisaatioiden sovellusten käyttökuormitus ja siitä johtuva resurssien tarve on tyypillisesti vaihtelevaa. Subashini & Kavitha (2011) esittävät että erityisesti kasvavissa yrityksissä skaalautuvuus mahdollistaa yritykselle kasvua tukevan infrastruktuurin, jossa yrityksen ei tarvitse huolehtia resurssien saatavuudesta. Toinen vahvuus IaaS -palveluissa on resurssien virtualisointi. Virtualisointi toteutetaan IaaS -palveluissa virtuaalikoneiden avulla (eng. virtual machine), jotka ovat eristettyjä pilvipalvelun laitteistosta sekä muista virtuaalikoneista. Virtuaalikoneiden kautta asiakkaat voivat käyttää pilvipalvelun resursseja yhtäaikaisesti vaikuttamatta toisiinsa. (Chang, Chen, & Dillon, 2010) Virtualisoinnin kautta on myös toteutettu palvelun resurssien abstrahointi helposti hallinnoitavaksi organisaatioille, kuten Gibson et al. (2012) nostavat esille. Mainittujen vahvuuksien lisäksi keskeinen vahvuus IaaS -palvelumuodossa yrityksille on palvelun hinta. IaaS -palvelumuodossa palvelun hinta

määrittyy suoraan sen mukaan kuinka paljon asiakas käyttää palvelun resursseja, jolloin yritys ei joudu maksamaan kalliita ylläpitomaksuja resursseista joita se ei käytä. (“5 Important Benefits of Infrastructure as a Service”, 2014)

Kuva 1. Pilvipalveluiden palvelumuodot.

Kuvassa 1 on esitettynä pilvipalveluiden palvelutasojen rakenne kokonaisuudessaan. Kuva esittää IaaS -palvelumuodon ominaisuuden, jossa IaaS -palvelumuoto toimii ylempien kerrosten, eli SaaS ja PaaS -palvelumuotojen pohjana.

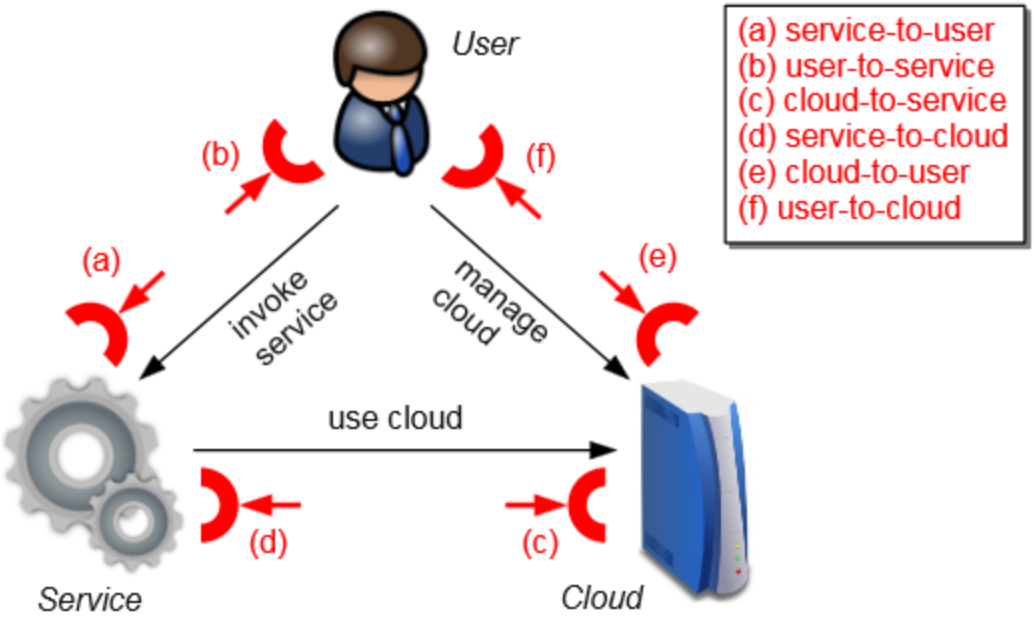
2. Ulkopuolisista hyökkäyksistä johtuvat haavoittuvuudet

Internetin aikakaudella tutuksi tulleet web-palveluiden uhkat kuten phishing, injektiohyökkäykset ja botnetit ovat uhkana myös IaaS- palveluiden ympäristössä, mutta näiden lisäksi IaaS -palveluiden virtualisointi aiheuttaa uudenlaisia haavoittuvuuksia. Virtualisoinnista aiheutuviin haavoittuvuuksiin lukeutuvat virtuaalikoneiden resurssien sijainti samalla fyysisellä laitteistolla, mikä aiheuttaa sen että pahantahtoisten käyttäjien resurssit sijaitsevat tällöin yleisten resurssien kanssa samalla laitteistolla, mistä aiheutuu sivupolku pahantahtoiselle käyttäjälle virtuaalikoneen kautta kohdedataan. (Chang et al., 2010) Virtualisointi aiheuttaa myös suoraan lisää haavoittuvuuksia palveluun, sillä virtualisoidut ympäristöt ovat alttiita samoille haavoittuvuuksille kuin normaalit ympäristöt, mutta virtualisoiduissa ympäristöissä on enemmän palvelun tulokohtia sekä palvelun sisäiset yhteydet ovat monimutkaisempia. (Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013)

Seuraavissa luvuissa käydään läpi aiemmissa tutkimuksissa löydettyjä ja esitettyjä IaaS -palvelumuodossa esiintyviä ulkopuolisista hyökkäyksistä ja palvelun teknisestä toteutuksesta johtuvia haavoittuvuuksia. Näiden haavoittuvuuskategorioiden avulla IaaS -palvelumuodon merkittävät haavoittuvuudet saadaan käsiteltyä kattavasti.

2.1 Hyökkäysrajapinnat

Pilvipalvelun toteutukseen liittyvät rajapinnat aiheuttavat haavoittuvuuksia palvelukokonaisuuteen. Ensinnä rajapinta käyttäjän ja palvelun välillä on toteutettu tavallisen asiakas-palvelin rajapinnan avulla. Tästä johtuen kaikki hyökkäystyypit, jotka ovat mahdollisia asiakas-palvelin -rajapinnan kautta, ovat mahdollisia myös pilvipalveluissa, esimerkkinä SQL -injektio, käyttöoikeuksien väärentäminen ja phishing -hyökkäykset. (Gruschka & Jensen, 2010) Toinen rajapinta on palveluinstanssin ja pilvipalvelun välinen rajapinta, joka voidaan jaotella siten, että palveluinstanssi on palvelun osa, jota voidaan käyttää toteuttamaan hyökkäys palvelua vastaan kokonaisuudessaan. Mainitun rajapinnan kautta tapahtuvista hyökkäyksistä mainittakoon esimerkkinä DDoS -hyökkäys, injektiohyökkäykset sekä vahingollisen virtuaalikoneinstanssin kautta suoritettavat hyökkäykset. (Gruschka & Jensen, 2010) Kolmantena toimijoiden välisenä rajapintakokonaisuutena Gruschka & Jensen (2010) mainitsevat asiakkaan ja palveluntarjoajan välisen rajapinnan, joka ilmenee palvelussa käyttäjälle tarjottujen resurssien kontrollirajapintana. Asiakkaan ja palvelun välinen rajapinta sisältää saman tyyppiset haavoittuvuudet kuin asiakas-palvelinrajapinta (Gruschka & Jensen, 2010).



Kuva 2. Pilvipalveluiden hyökkäysrajapinnat (Gruschka, & Jensen, 2010). Copyright © 2010, IEEE

Kuvassa 2 on koostettuna pilvipalveluiden hyökkäysrajapinnat kokonaisuudessaan. Kuvasta nähdään rajapintojen kaksisuuntainen luonne, jolloin esimerkiksi asiakas-palvelinrajapinta sisältää haavoittuvuuksia, joita pilvipalvelua vastaan hyökkäävä pahantahtoinen käyttäjä voi hyväksikäyttää molempiin suuntiin (Gruschka & Jensen, 2010).

2.2 Hyökkäystyypit

Injektiohyökkäykset

Pilvipalvelun ulkopuolisiin haavoittuvuuksiin luetaan injektiohaavoittuudet, joiden kautta hyökkääjä pyrkii manipuloimaan palvelua suorittamaan toimintoja ohjelmoijan tarkoitusten vastaisesti. Injektiohaavoittuvuuksia ovat SQL -injektio, käskyinjektio sekä “cross-site scripting” (XSS). SQL -injektio toteutetaan sisällyttämällä syötteeseen SQL -koodi, joka virheellisesti suoritetaan palvelun tietokannassa. Käskyinjektio on vastaava kuin SQL -injektio, mutta siinä syötteen sisältämä koodi suoritetaan käyttöjärjestelmän kautta. XSS puolestaan sisältää syötteessä JavaScript -koodin, joka suoritetaan kohteen selaimessa. (Grobauer et al., 2011) Injektiohaavoittuvuus ilmenee esimerkiksi tilanteessa, jossa IaaS -palvelua käyttävä ulkopuolinen käyttäjä saa käyttöönsä esimerkiksi VMM:n, eli ”virtual machine monitorin”, käyttöoikeudet injektiokäskyjen avulla. Injektiohaavoittuvuuksia ehkäisevät kontrollimekanismit, kuten isolointi-, inspektointi- ja väliintulomekanismit, eivät ole täysin toimintavarmoja olemassa olevissa pilvipalveluissa. (Subashini & Kavitha, 2011)

Injektiohyökkäysiin liittyen XML-signeeraus aiheuttaa pilvipalveluun haavoittuvuuden, joka alunperin havaittiin IaaS -palvelu Amazon EC2:en kautta. XML-signeerausta

hyväksikäyttävässä hyökkäyksessä pahantahtoinen käyttäjä hankkii haltuunsa käyttäjän lähettämän SOAP -viestin ja käyttää alkuperäisen viestin vartaloa vahingollisen viestin vartalona. Vahingolliseen viestiin hyökkääjä lisää alkuperäisen viestin vartaloon vahingollisen toiminnon kääreessä (eng. wrap), jolloin palvelu suorittaa myös viestiin lisätyt toiminnot, sillä viesti sisältää edelleen alkuperäisen viestin signeerauksen. (Gruschka, Lacono, Schwenk, & Jensen, 2009)

DDoS

IaaS -palvelun keskeisenä ominaisuutena on resurssien dynaaminen tarjoaminen asiakkaalle. Tämän ominaisuuden johdosta pilvipalvelut ovat erityisen haavoittuvaisia DDoS -hyökkäyksille, joissa hyökkääjä lähettää jatkuvasti tiettyjä pyyntöjä palveluun. Dynaamisen resurssien allokoinnin johdosta palvelu pyrkii allokoimaan lisää resursseja suorittaakseen DDoS -hyökkäyksen pyynnöt. (Gruschka et al., 2009) DDoS – hyökkäyksen vaikutus on tehokkaimmillaan, kun se kohdistetaan tiettyyn palvelun palvelimeen, joka on tulokohtana ulkopuolisille pyynnöille tietylle palvelinjoukolle, kuten Gruschka et al. (2009) mainitsevat.

Virtuaalikoneinstanssien hyväksikäyttö

IaaS-palveluissa palvelu tarjotaan asiakkaille virtuaalikoneiden kautta. Pahantahtoinen käyttäjä voi hyväksikäyttää toteutusta ujuttamalla vahingollisen virtuaalikoneinstanssin palveluun, jolloin palvelu automaattisesti alkaa ohjaamaan asiakkaita tähän virtuaalikoneinstanssiin. Tämän tyyppinen hyökkäys mahdollistaa pahantahtoiselle käyttäjälle minkä tahansa toimenpiteen suorittamisen asiakkaan datalle. (Gruschka et al., 2009)

Virtuaalikoneinstansseihin liittyen Xiao & Xiao (2013) nostavat esille, että virtuaalikoneinstanssit mahdollistavat ulkopuoliselle hyökkääjälle rajapinnan virtuaalikoneinstanssia hyödyntävään hyökkäykseen. Hyökkäyksen toteutukseen liittyy, että pahantahtoinen käyttäjä asettaa oman virtuaalikoneinstanssin samalle palveluntarjoajan palvelimelle hyökkäyksen kohteen kanssa. Tämän jälkeen hyökkääjä pystyy seuraamaan kohteen virtuaalikoneinstassin käyttömääriä, eniten haettuja sivuja sekä pahimmassa tapauksessa saamaan selville käyttäjätunnuksia ja tiedostojen sijainteja palvelimella. (Xiao, & Xiao, 2013)

Sosiaalinen manipulointi

Pilvipalvelun ulkopuolisiin haavoittuvuuksiin, sisältäen IaaS -palvelumuodon, lukeutuu sosiaalisesta manipuloinnista aiheutuva haavoittuvuus. Sosiaalisen manipuloinnin kautta, päästessään käsiksi käyttäjän pääsytietoihin, pahantahtoinen käyttäjä pystyy hallinnoimaan käyttäjän dataa. (Hashizume et al., 2013)

3 Palvelun teknisestä toteutuksesta johtuvat haavoittuvuudet

IaaS -palvelumuoto perustuu virtualisointiin, jonka avulla yhdistetään erillään olevia resursseja verkostoiksi, jotka tarjotaan käyttäjille lyhyellä viiveellä asiakkaan tarpeen mukaisesti. Tämä aiheuttaa IaaS -palvelumuodon "multitenancy" piirteen, jossa yksittäiset asiakkaat käyttävät yhteisiä resursseja samoilla palvelimilla. IaaS -palvelumuoto sisältää käyttämiensä teknologiaratkaisuiden ominaiset haavoittuvuudet, mutta lisäksi myös teknologioiden yhdistämisestä aiheutuvat uudet haavoittuvuudet. (Vaquero, Rodero-Merino, & Morán, 2011) Seuraavissa luvuissa käsitellään erityisesti pilvipalveluiden resurssien ja asiakkaiden virtuaaliympäristön integroinnista aiheituvia teknisiä haavoittuvuuksia.

3.1 Virtualisointi

IaaS -palveluiden toteutuksen abstrahoiminen virtualisoinnin avulla aiheuttaa sen, että pilvipalveluiden kontrolloiminen on täysin palveluntarjoajan varassa. Asiakkaan ei ole mahdollista hallita pilvipalvelusta tulevia yhteyksiä ja suorittaa yhteyksille esimerkiksi haavoittuvuusskannausta, koska nämä "ystävälliset" skannaukset on mahdotonta erottaa pahantahtoisen käyttäjän hyökkäystoimenpiteistä. (Grobauer et al., 2011) Virtualisointi aiheuttaa myös sen että Internetin ruuhka vaikuttaa sekä fyysisiin että virtuaalisiin verkostoihin, jolloin tilanne, jossa kaksi samalla palvelimella toimivaa virtuaalikonetta kommunikoivat, hidastuu palvelun ulkopuolelta tulevan ruuhkan vaikutuksesta, kuten Grobauer et al. (2011) mainitsevat. Virtualisointi aiheuttaa myös sen että pahantahtoinen käyttäjä käyttää resursseja samasta pilvipalvelun resurssipoolista kuin tavallinen käyttäjä, jolloin esimerkiksi pahantahtoisen käyttäjän käynnistämä vahingollinen toiminta pilvipalvelun resurssien avulla yhdistetään kaikkiin käyttäjiin, jotka vahingollisen toiminnan aikana käyttävät pilvipalvelun resursseja naamioiden näin pahantahtoisen käyttäjän, kuten Chang et al. (2010) huomauttavat.

IaaS -palvelun prosessointiresurssit tarjotaan myös asiakkaalle virtuaalikoneiden kautta, jotta resursseja pystytään allokoimaan asiakkaille tehokkaasti on-demand -tyylisesti. Prosessointiresurssien saatavuus virtuaalikoneiden kautta toteutetaan pilvipalveluissa kloonaamalla virtuaalikoneen levykuvia ja erilaistamalla niitä hieman. Levykuvien kautta pilvipalvelun asiakkaana esiintyvän ulkopuolisen hyökkääjän on mahdollista saada selville levykuvien konfigurointimalli ja tätä kautta saada pääsy muiden asiakkaiden virtuaalikoneiden levykuviin. (Grobauer et al., 2011) Toinen levykuviin liittyvä uhka aiheutuu, jos asiakas ottaa virtuaalikoneen levykuvan epäluotettavasta lähteestä Amazon EC2 tyyppisen virtuaalikoneiden levykuvien kauppapaikan kautta, esimerkiksi suoraan hyökkääjältä, jolloin virtuaalikoneen levykuva voi sisältää takaoven hyökkääjälle, kuten Grobauer et al. (2011) mainitsevat. Toisaalta virtuaalikoneiden levykuvien kauppapaikkojen myötä levykuvien leviäminen lisääntyy, jolloin alkuperäisestä levykuvasta kloonattu levykuva voi sisältää dataa, jota kloonatun levykuvan luoja ei tarkoittanut julkistaa (Grobauer et al., 2011).

3.2 Resurssienhallinta

IaaS -palvelumuodon mahdollistama resurssien nopea varaaminen asiakkaan tarpeen mukaan aiheuttaa palveluntarjoajalle vaatimuksen, että heidän täytyy taata asiakkaalle palvelun laatu, luotettavuus, saatavuus sekä suorituskyky kuten Chang et al. (2010) esittävät. Kyseiset palvelutasoon liittyvät seikat määritetään "Service level agreement" (SLA) -sopimuksessa. SLA -sopimus aiheuttaa palveluntarjoajalle vaatimuksen seurata resurssien saatavuutta reaaliaikaisesti ja hallita resurssien allokointi tehokkaasti, jotta asiakkaiden SLA -sopimuksessa määritetyt palvelutasot saavutetaan. Erityisesti, kun SLA -sopimuksessa määritettyä palvelutasoa ei pystytä saavuttamaan palveluntarjoajan puolesta, palveluntarjoajan on kyettävä hylkäämään asiakkailta tulevat uudet vaatimukset, jotta palvelu pystyy tehostamaan palvelun tilaa itsenäisesti. (Chang et al., 2010)

IaaS -palveluiden resurssienhallintaan liittyen Grobauer et al. (2011) nostavat esille, että tehokkaan resurssien allokoinnin mahdollistamiseksi resurssienhallinta on toteutettu IaaS -palveluissa yhden palveluntarjoajan rajapinnan kautta, johon yksittäiset virtuaalikoneet ovat yhteydessä. Virtuaalikoneita hallitseva rajapinta palveluissa on "Virtual Machine Monitor" (VMM) niminen ratkaisu, joka vastaa palvelussa yksittäisten virtuaalikoneiden sijoittamisesta fyysisille palvelimille ja niiden eristämisestä. VMM:n avulla toteutettu resurssienhallinta aiheuttaa kriittisen haavoittuvuuden hyökkääjän päästessä käsiksi rajapintaan, jolloin hyökkääjä voi siirtää VMM:n kautta yksittäisen virtuaalikoneen vahingolliselle palvelimelle. (Grobauer et al., 2011) (Hashizume et al., 2013)

Palvelun infrastruktuuri on toteutettu siten, että resurssit ovat jakautuneet maantieteellisesti erillään oleviin sijainteihin, minkä vuoksi avaimien tallentaminen yleisesti avainten hallinnassa standardeina käytettyihin keskitettyihin sijainteihin on mahdotonta. Tästä johtuen palvelussa joudutaan käyttämään useita avaimia yksittäisten asiakkaiden resurssien hallinnoimiseen, mikä johtaa heikkoon avainten hallintaproseduuriin. (Grobauer et al., 2011) Myös Pearson & Banameur (2010) nostavat esille palvelun jakautuneen infrastruktuurin aiheuttaman haavoittuvuuden, joka aiheutuu kun datan prosessointi- ja varastointiympäristö ei ole määritelty palvelussa, minkä seurauksena yksityisyyden varmistaminen turvakontrollien avulla vaikeutuu. Mainittu haavoittuvuus ilmenee siten, että palvelun prosessoidessa tai varastoidessa dataa eri valtioiden alueella, valtiolla voi olla lain takaama oikeus saada data haltuunsa. (Pearson & Banameur, 2010) Maantieteellisesti jakautunut prosessointi ja varastointi aiheuttavat haavoittuvuuden myös tilanteissa, joissa tietyn maan lait määrittävät, että tietyn tyyppinen arkaluontoinen data ei saa päätyä maan rajojen ulkopuolelle, kuten Kavitha & Subashini (2011) mainitsevat.

Datan katoaminen pilvipalveluissa aiheutuu siitä, kun pilvipalvelun fyysisiä resursseja eli kiintolevyjä joudutaan hävittämään elinkaarensa lopussa. Tällöin kiintolevyjen datan siirtäminen ja tämän jälkeinen kiintolevyjen puhdistus täytyy suorittaa määritettyjen käytäntöjen mukaisesti, jotta asiakkaan dataa ei jää siirtämättä ennen kiintolevyn puhdistusta ja hävittämistä tai dataa jää kiintolevylle epätäydellisen puhdistuksen johdosta. Tehokas datan siirtäminen ja puhdistus on käytännössä vaikea suorittaa pilvipalveluissa, koska resurssit on toteutettu resurssipoolin kautta, jolloin fyysisten kiintolevyjen sisältämässä datassa on paljon sisäisiä yhteyksiä. (Fernandes, Freire, Gomes, Inácio, & Soares, 2014) Toinen datan katoamisen aiheuttava tekijä aiheutuu pilvipalvelun kiintolevyresurssien palvelukatkoksesta, joka voi pahimmillaan johtaa

pysyviin datan menetyksiin, kuten kyseiseen haavoittuvuuteen liittyvät esiintyneet tapaukset ovat osoittaneet (Dahbur, Mohammad, & Tarakji, 2011). Esimerkkinä datan häviämiseen liittyvästä tapauksesta Armbrust et al. (2010) mainitsevat The Linkup nimisen yrityksen tapauksen, jossa yritys menetti 45 % asiakkaiden datasta johtuen kolmannen osapuolen tarjoamien resurssipalveluiden saatavuuden katkeamisesta. Tämä johti lopulta The Linkup:in konkurssiin.

3.3 Pääsynvalvonta

IaaS -palvelu vaatii turvallisen toimivuuden takia mekanismit autentikointiin, autorisointiin ja identiteettihallintaan. Toisaalta palvelun joustavuuden aikaansaamiseksi pääsynvalvonta mekanismit täytyy toteuttaa hienojakoisesti, kuten Takabi, Joshi & Ahn (2010) nostavat esille. Näiden mekanismien toteutuksessa esiintyy ongelmia esimerkiksi identiteettihallintaan liittyvässä pääsytietojen hallinnassa, jossa salasanan palautusmekanismit ovat toimineet nykyisissä ratkaisuissa heikosti. Autorisointikontrolleissa on esiintynyt ongelmia myös luvattomien URL-arvausten kautta. (Grobauer et al., 2011) Yksi syy puutteellisiin autorisointikontrolleihin johtuu standardien velvollisuuksien jaottelun vaikeudesta, sillä IaaS -palvelussa on vaikea määrittää, mitkä ovat ne valtuudet, jotka asiakas tarvitsee suorittaakseen tehtävänsä asiakkaiden monimuotoisuuden takia, kuten Grobauer et al. (2011) nostavat esille.

IaaS -palvelun toteutuksen johdosta palveluntarjoajilla on laajat hallinnointimahdollisuudet. Tämä johtaa siihen, että palvelutarjoajan on toteutettava turvallisuusmekanismeja palvelun sisäisten työntekijöiden pääsyyn asiakkaiden dataan. Turvallisuusmekanismiksi datan yhtenäisyyden varmistamiseksi, palveluntarjoajan on toteutettava sisäinen auditointi, jonka avulla varmistetaan, ettei palvelussa tapahdu datatransaktioita, joita ei pystytä jäljittämään. Kuitenkin tämänhetkisissä julkisissa pilvipalveluissa kattava auditointi on ratkaisua vailla oleva ongelma. (Pearson & Banameur, 2010) Artikkelissaan Abreu, Correira & Rocha (2011) nostavat esille, että IaaS -palvelussa palvelun sisäinen pahantahtoinen työntekijä voi hyökätä palvelua vastaan suhteellisen helposti, jos työntekijällä on hallussaan ylläpitäjän oikeudet VMM:ään. VMM:än avulla työntekijä voi ottaa tilannekuvan (eng. snapshot) tietyn virtuaalikoneen muistista sekä asentaa loogisia levyasemia. VMM:llä otetun muistin tilannekuvan kautta pahantahtoisella työntekijällä on pääsy palveluun tallennettuihin salasanoihin, sillä ne ovat yleensä selkotekstimuodossa. Jos data on puolestaan salatussa muodossa, työntekijä voi suorittaa hallussaan olevalle virtuaalikoneen muistin tilannekuvalle algoritmien avulla toteutetun haun, jonka tuloksena salatusta datasta eristyy avain, jolla työntekijä saa purettua datan salauksen. Kolmas tapa jota pahantahtoinen työntekijä voi käyttää hyväkseen päästäkseen käsiksi dataan, toteutetaan siten, että työntekijä luo uuden virtuaalikoneen, johon hänellä on pääsyoikeudet ja kopioi asiakkaan virtuaalikoneen sisältämän datan luomaansa virtuaalikoneeseen. (Abreu et al. 2011)

3.4 API:n aiheuttamat haavoittuvuudet

Pilvipalvelut tarjoavat erityyppisiä palvelumuotoja, jolloin palvelumuodosta toiseen vaihtaminen merkitsee yleensä palveluntarjoajasta toiseen vaihtamista. Tämä merkitsee myös sitä, että IaaS -palvelun data liikkuu kyseisten palveluntarjoajien rajapintojen yli.

Palveluntarjoajat tarjoavat erilaisia turvallisuuskäytäntöjä, jolloin palveluntarjoajan rajapinnan yli liikuttaessa esiintyy tietomurrolle haavoittuva kohta. (Takabi et al., 2010) Rajapintojen yli liikuttaessa käyttäjän on mahdotonta varmistaa datan eheyden säilyminen laskennan jälkeen. Tämä ilmenee erityisesti tilanteissa, joissa alkuperäinen palveluntarjoaja ulkoistaa asiakkaan pyynnön kolmannelle osapuolelle, jolloin kolmas osapuoli voi palauttaa vääriä tuloksia ilman että palveluntarjoaja tai asiakas havaitsevat tämän suoraan. Kolmannen osapuolen kautta menetetty datan eheys voi johtua esimerkiksi kolmannen osapuolen tarkoituksellisesta resurssien säästämisestä välittämättä datan eheyden menettämisestä, huonoista palvelukäytännöistä tai hyökkäyksen vaikutuksen alla olevasta palvelusta. (Xiao & Xiao, 2013)

Kun asiakas haluaa ulkoistaa laskentaa IaaS -palvelun avulla, mutta käyttää omia palvelimiaan datan varastoimiseen, data liikkuu asiakkaan palvelimelta palveluntarjoajan palvelimelle selkotekstimuodossa. Tämä aiheuttaa sen, että datan liikkuessa rajapinnan yli asiakkaan palvelimelta palveluntarjoajan palvelimelle data on suoraan luettavissa hyökkääjän päästessä käsiksi dataan. (Ren, Wang, & Wang, 2012) Mainitun haavoittuvuuden ehkäisemiseksi asiakas voi käyttää useita pilvipalveluntarjoajia hajauttaen datan, jolloin yksittäisen palvelun sisältämän datan vaarantuessa datan luottamuksellisuus kokonaisuudessaan ei vaarannu. Ongelmaksi nousee kuitenkin yksittäisten palveluiden API:en eroavuudet, jolloin asiakkaan on vaikea toteuttaa ja hallita integroimiaan pilvipalveluita tehokkaasti, jolloin asiakkaan on käytännössä pakko käyttää yhden palveluntarjoajan palveluita. (Chang et al., 2010)

Lu et al. (2013) paneutuvat artikkelissaan syvällisesti API:n aiheuttamiin haavoittuvuuksiin ja nostavat esille API:in liittyviä ongelmia. Yleisimpinä ongelmina tutkimuksensa perusteella Lu et al. (2013) nostavat esille palvelun pysähtymishäiriön (eng. halt failure) ja sisältöhäiriön (eng. content failure). Nämä ongelmat aiheuttavat palvelun saatavuuteen liittyvän haavoittuvuuden. Sisältöön liittyvät häiriöt ovat tarkemmin käyttäjälle tulkitsemattomia virheviestejä, palvelusta puuttuvaa sisältöä, virheellistä palvelun sisältöä ja odottamatonta sisältöä. Pysähtymishäiriöön liittyvät ongelmat ovat puolestaan tilanteita, joissa palvelu juuttuu tiettyyn tilaan, eikä käyttäjä onnistu palauttamaan palvelua alkuperäiseen tilaansa. (Lu et al., 2013)

4. Löydösten pohdinta

Luvuissa 2 ja 3 aiemman kirjallisuuden pohjalta esiteltyjen haavoittuvuuksien määrä ja monipuolisuus osoittaa sen, että IaaS -palvelumuoto ja pilvipalvelut kokonaisuudessaan eivät ole nykyisessä tilassaan suinkaan täysin luotettava palvelu. Haavoittuvuuksien lähteenä IaaS -palveluissa ovat jo ennestään webin ja muiden pilvipalveluissa käytettyjen teknologioiden ominaiset haavoittuvuudet, mutta lisäksi pilvipalveluiden virtualisoinnista ja palvelun resurssien yhteiskäyttö luontoisesta toteutuksesta johtuvat uudet haavoittuvuudet, kuten Vaquero et al. (2011) nostavat esille. IaaS -palveluiden virtualisointi ja palvelun resurssien yhteiskäyttö aiheuttavat uusia haavoittuvuuslähteitä sekä palvelun ulkopuolisiin haavoittuvuuksiin että palvelun tekniseen toteutukseen. IaaS -palveluiden ominaiset haavoittuvuudet, eli haavoittuvuudet, joiden lähteenä on nimenomaan pilvipalvelun virtualisointi, painottuvat kokonaisuudessaan palvelun sisäpuolisiin haavoittuvuuksiin. Toisin sanoen IaaS -palveluiden virtualisointi ei aiheuta lukumäärällisesti niin monia haavoittuvuuksia ulkopuolisiin haavoittuvuuksiin kuin palvelun sisäisiin haavoittuvuuksiin. Mainitun ilmiön johdosta pilvipalvelujen sisäiset sisäisten haavoittuvuuksien merkitys kasvaa verrattuna ulkopuolisiin haavoittuvuuksiin, jotka ovat olleet tyypillisesti merkittävimpiä haavoittuvuuksien lähteitä webin aikakaudella.

Seuraavissa kappaleissa pyritään analysoimaan luvussa 2 esille nostettujen IaaS -palvelumuodon merkittävimpiä ulkopuolisista hyökkäyksistä johtuvia haavoittuvuuksia sekä teknisestä toteutuksesta johtuvia sisäisiä haavoittuvuuksia. Haavoittuvuuden merkittävyys on pyritty arvioimaan ja erittelemään siten, kuinka laajasti se vaikuttaa palveluun kokonaisuudessaan.

4.1 Merkittävimmät ulkopuoliset haavoittuvuudet

Virtualisointi luo IaaS -palvelumuodon ulkoisiin haavoittuvuuksiin uudenlaisen rajapinnan verrattuna perinteisiin, asiakas-palvelin mallin web-sovelluksiin. Virtuaaliympäristö on altis perinteisen ympäristön rajapinnan haavoittuvuuksien lisäksi virtuaalisuuden aiheuttamille haavoittuvuuksille, kuten Hashizume et al. (2013) nostavat esille. Haavoittuvuudet aiheutuvat erityisesti virtuaalisuuden aiheuttamista lisääntyneistä palvelun tulokohdista sekä palvelun toteutuksen kompleksisuuden lisääntymisestä (Hashizume et al., 2013). Syvällisemmin virtualisointi tuo kompleksisuutta palveluun suoraan lisäämällä uuden rajapinnan asiakkaan ja palvelun välille. Tämä on virtuaalikoneinstanssin ja palvelun välinen rajapinta. Lisäksi palveluissa toteutetaan asiakkaan resurssienhallinta rajapinta, jonka kautta asiakas on suoraan yhteydessä palvelimeen. (Gruschka & Jensen, 2010) Luonnollisesti kasvava kompleksisuus ja lisääntyneet tulokohdat, lisäävät palvelun rajapintojen kautta aiheutuvia haavoittuvuuksia ulkopuolisille hyökkäyksille. Jokainen ylimääräinen rajapinta lisää palvelun haavoittuvuutta kokonaisuudessaan, sillä yksittäisillä rajapinnoilla täytyy olla omat turvallisuuskontrollimekanismit hyökkäysten ehkäisemiseksi. Kokonaisuudessaan ulkopuoliset haavoittuvuudet IaaS -palvelumuodossa pohjautuvatkin pitkälle virtualisoinnista aiheutuviin haavoittuvuuksiin, sillä virtuaalikoneinstanssi toteuttaa monipuolisimman rajapinnan palveluun, jolloin rajapinnassa on todennäköisesti myös eniten haavoittuvuuksia. Virtualisoinnin kompleksisuus ja sen toteutuksen kätkeminen

käyttäjiltä aiheuttaa myös sen, että asiakkaan on mahdotonta arvioida palvelun virtualisoinnin luotettavuutta.

IaaS -palveluiden toteutus mahdollistaa DDoS -hyökkäysten laajamittaisen toteuttamisen. Tämä aiheutuu erityisesti siitä, että IaaS -palvelu pyrkii allokoimaan lisää resursseja vastatakseen asiakkaalta tuleviin lisääntyviin pyyntöihin, jolloin myös DDoS -hyökkäysten tilanteessa IaaS -palvelu pyrkii vastaamaan DDoS -hyökkäyksen pyyntötulvaan lisäämällä resursseja hyökkääjän käskyjen käsittelyyn (Gruschka et al., 2009). DDoS -hyökkäyksiin liittyvän haavoittuvuuden merkitys korostuu, kun DDoS -hyökkäys suunnataan tiettyyn palvelimeen, joka toimii palvelun tulokohtana asiakkailta tuleviin yhteyksiin, kuten Gruschka et. al. (2009) nostavat esille. DDoS -hyökkäysten toteutuksen helppoudesta IaaS -palvelumuotoa vastaan ja niiden vaikuttavuudesta IaaS -palvelun toimivuuteen nousee esille kriittinen tarve ehkäistä kyseisten hyökkäysten toteutusta. DDoS -hyökkäysten ehkäisy tuo omat haasteensa IaaS –palvelun jo valmiiksi monimutkaiseen toteutukseen, sillä palvelun palvelimet saavat jatkuvasti suuren määrän pyyntöjä lukuisilta käyttäjiltä, joista suurin osa on normaaleja käyttäjiä. Tällöin pahantahtoisen käyttäjän suorittama DDOS -hyökkäys on vaikea isoloida palvelun pyyntötulvasta.

4.2 Merkittävimmät teknisestä toteutuksesta johtuvat haavoittuvuudet

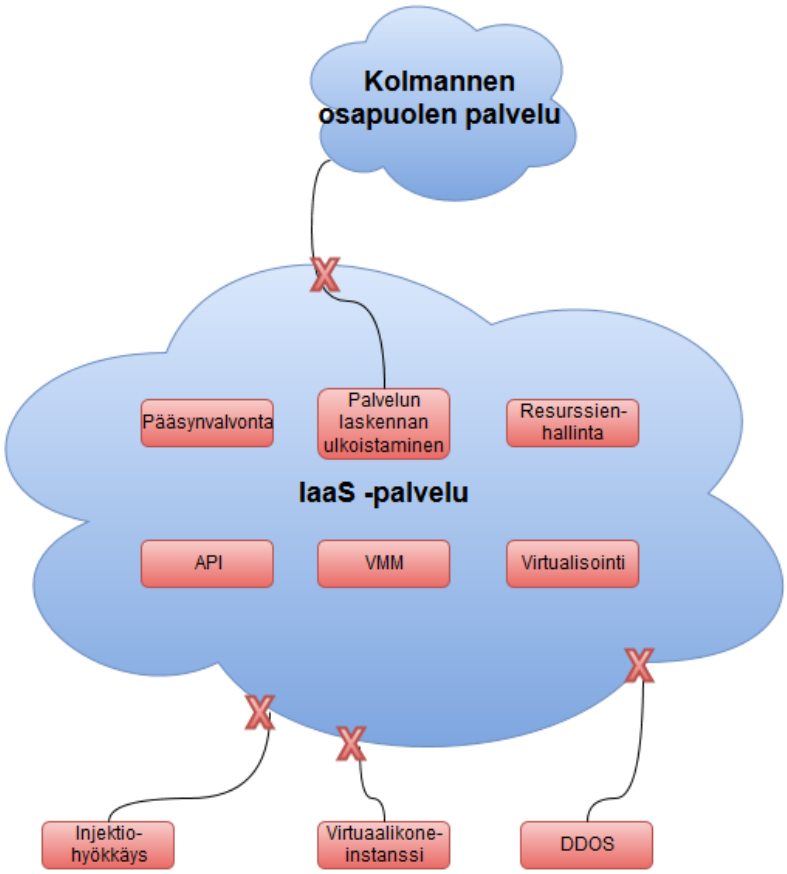
VMM on IaaS -palvelumuodon keskeinen ratkaisu resurssien ja virtuaalikoneinstanssien hallitsemiseksi, sen avulla palveluntarjoaja allokoi resurssit sekä eristää virtuaalikoneet (Grobauer et al., 2011). VMM muodostaa tällöin pilvipalvelun moduulin, jonka toiminnasta pilvipalvelun toiminta on kokonaisuudessaan suoraan riippuvainen. VMM on oltava tehokas, jotta pilvipalvelu pystyy vastaamaan yksittäisten asiakkaiden SLA:ssa määriteltyihin palveluntasoihin, kuten Chang, Chen & Dillon (2010) nostavat artikkelissaan esille. Toisaalta VMM:n on oltava Hashizumen et al. (2013) mukaan samanaikaisesti myös turvallinen, jotta hyökkääjä ei pääse sen kautta käsiksi pilvipalveluiden hallintaan. Yhteenvetona mainittujen VMM:n toiminnallisten ja turvallisuusvaatimusten pohjalta voidaan todeta, että VMM aiheuttaa kriittisen moduulin, jonka haavoittuvuuksien merkitys on suurin yksittäisistä pilvipalvelun tekniseen toteutukseen liittyvistä moduuleista pilvipalvelun kannalta kokonaisuudessaan.

VMM:llä toteutetun resurssienhallinnan takia pilvipalvelun työntekijöillä on oltava laajat käyttöoikeudet. Käyttöoikeuksien kautta pilvipalvelun data on haavoittuvainen palveluntarjoajan sisäisten työntekijöiden tekemiin tietomurtoihin, kuten Abreu et al. (2011) nostavat artikkelissaan esille. Sisäisten tietomurtojen ehkäisemiseksi palveluntarjoajan tulee toteuttaa tehokkaat auditointimenetelmät, joiden kautta työntekijöiden suorittamia toimia voidaan monitoroida. Kuitenkin tämänhetkisissä julkisissa pilvipalveluissa kattava auditointi on ratkaisua vailla oleva ongelma. (Pearson & Banameur, 2010) Palvelun sisäisten työntekijöiden valvonnan merkitys on keskeistä, sillä sisäisten tietomurtojen todennäköisyys kasvaa pilvipalveluiden datamäärien kasvaessa ja erityisesti organisaatioiden IaaS -palvelun hyödyntämisen lisääntyessä, minkä myötä palvelun varastoiman datan arvo kasvaa.

Pahantahtoinen käyttäjä voi käyttää pilvipalveluiden resursseja toteuttaakseen DDoS -hyökkäyksen johonkin ulkopuoliseen kohteeseen, jolloin hyökkääjällä on suuri määrä resursseja käytössään hyökkäyksen toteuttamiseen (Constantin, 2014). Tämän tyyppiset,

pilvipalvelun resursseja hyväksikäyttävät, DDoS -hyökkäykset ovat kriittinen haavoittuvuus pilvipalveluiden teknisessä toteutuksessa, sillä pilvipalveluiden tarjoaman resurssien määrän avulla hyökkääjällä on mahdollista toteuttaa vaikutukseltaan suuria hyökkäyksiä jopa valtioiden palveluita vastaan. Pilvipalveluiden kautta toteutetut DDoS -hyökkäykset on erittäin vaikea sulkea, koska pahantahtoiset käyttäjät käyttävät samoja resursseja lukuisten muiden käyttäjien kanssa, jolloin pahantahtoisen käyttäjän jäljittäminen on vaikeaa. (Chang et al. 2010)

Xiaon & Xiaon (2013) sekä Takabin et al. (2010) artikkeleissa esille nostamat pilvipalveluiden prosessoinnin ulkoistamisesta kolmansille osapuolille aiheutuvat haavoittuvuudet ovat merkittäviä, sillä ulkoistamisen takia alkuperäisen palveluntarjoajan on mahdotonta varmistaa rajapintojen turvallisuus ja tätä kautta datan eheyden säilyminen. Ongelma korostuu Chang et al. (2010) mainitsemasta yksittäisten palveluntarjoajien API:en eroavuudesta, mistä johtuen asiakkaan sekä palvelun tarjoajan on mahdotonta integroida ulkopuolisia palveluntarjoajia tehokkaasti käyttöönsä. Palveluntarjoajien väliset rajapinnat lisäävät luvussa 4.1 mainittuihin palvelun sisäisiin rajapintoihin uuden rajapinnan, joka osaltaan aiheuttaa analogisesti lisää haavoittuvuuksia rajapintojen lisääntyessä.



Kuva 3. Pilvipalveluiden merkittävimmät sisäiset ja ulkoiset haavoittuvuudet.

Kuvassa 3 on koottuna IaaS -palvelumuodon merkittävimpiä haavoittuvuuskategorioita. IaaS -palvelun teknisestä toteutuksesta johtuvat sisäiset haavoittuvuudet on esitetty kuvassa pilven sisässä ja palvelun ulkopuolisista hyökkäyksistä johtuvat haavoittuvuudet on esitetty puolestaan pilven ulkopuolella.

5. Johtopäätökset

Tässä luvussa koostetaan työn tuloksista yhteenveto sekä pohditaan työn tulosten sekä työn merkitystä kokonaisuudessaan. Työn merkitystä pohditaan erityisesti henkilökohtaisella tasolla, koska tämän tyyppisen työn lukijakunta jää todennäköisesti suhteellisen suppeaksi. Luvussa käydään läpi myös työn rajoituksia sekä löydösten yleistettävyyttä ja tämän kautta pohditaan näkökulmia lisätutkimukselle. Lisäksi pohditaan lähteiden luotettavuutta, ajantasaisuutta sekä lähdeartikkeleiden näkökulmien monipuolisuutta. Työn rajoitusten kautta pyritään perustelemaan lisätutkimusaiheiden tarpeellisuutta.

5.1 Työn tulosten yhteenveto ja työn merkitys

Työn tuloksina löydettiin kattavasti tutkimusongelmaan vastaavia pilvipalveluiden IaaS -palvelumuodon keskeisiä haavoittuvuuksia. Työn tulokset pohjautuvat tiukasti aiempaan kirjallisuuteen työssä käytetystä tutkimusmetelmästä, eli käsitteellisestä kirjallisuustutkimuksesta, johtuen. Luvussa 4, kirjallisuudesta löydettyjen näkökulmien pohjalta, on johdettu oman ajattelun kautta löydösten yksittäisiä näkökulmia yhdistäviä näkökulmia IaaS -palvelumuodon keskeisiin haavoittuvuuksiin liittyen. Oman pohdinnan kautta tuotetuissa näkökulmissa on pyritty sitomaan aiempien tutkimusten kautta löydettyjä haavoittuvuuksia todelliseen pilvipalveluiden ympäristöön. Esille nostetut oman ajattelun kautta johdetut näkökulmat eivät ole siis aiempien tutkimusten kautta verifioituja näkökulmia, mutta näkökulmat perustuvat hyvin pitkälle aiemman kirjallisuuden löydöksiin, jolloin ne muodostavat valideja hypoteeseja aiheeseen liittyen. Lisätutkimuksessa voitaisiin keskittyä esimerkiksi juuri näiden hypoteesien verifioimiseen.

Yhteenvetona tuloksista voidaan todeta, että tämänhetkisessä tilassaan IaaS -palvelumuodossa on runsaasti haavoittuvuuksia sekä ulkopuolisista hyökkäyksistä sekä palvelun teknisestä toteutuksesta johtuen. Nämä haavoittuvuudet ja erityisesti teknisestä toteutuksesta johtuvat haavoittuvuuden pohjautuvat pitkälti virtualisoinnista ja palvelun resurssien yhteiskäytöstä johtuviin ominaisuuksiin. Havaitut haavoittuvuudet ovat aiempien tutkimusten perusteella tämänhetkisissä johtavissakin pilvipalveluissa ratkaisua vailla olevia ongelmia.

Työn tulosten perusteella työn merkityksestä voidaan sanoa, että työ on erittäin ajantasainen, sillä tuloksissa onnistuttiin nostamaan esille monipuolisia haavoittuvuuksia IaaS -palvelumuodossa. Työn ajantasaisuutta tukee myös se, että aiheesta löytyi runsaasti aiempaa tutkimusta ja aiheeseen liittyvien tutkimusartikkeleiden julkaisujen määrän trendi on kasvava. Useissa aiemmissa tutkimuksissa on pyritty nostamaan esille yksityiskohtaisia teoreettisia näkökulmia IaaS -palvelumuodon haavoittuvuuksiin liittyen jättäen huomioimatta, miten näkökulmat liittyvät yleisesti pilvipalveluiden todelliseen ympäristöön. Näitä pilvipalveluiden todelliseen ympäristöön liittyviä näkökulmia on pyritty osaltaan nostamaan esille luvussa 4, mikä nostaa työn merkitystä tuoden esille näkökulmia, joita aiemmissa tutkimuksissa ei ole aktiivisesti huomioitu.

Henkilökohtaisella tasolla työ perehdytti kattavasti pilvipalveluiden tämän hetkiseen tilaan ja pilvipalveluiden tietoturvatarpeisiin. Työn edetessä henkilökohtainen ymmärrys

pilvipalveluista lisääntyi runsaasti sekä erityisesti näkökulmat pilvipalveluiden tietoturvapuutteisiin monipuolistuivat. Pilvipalveluiden tietoturvapuutteiden ymmärryksen lisääntyminen työn kautta on merkittävää, sillä aihe on keskeinen tämänhetkisessä ohjelmistoliiketoiminnassa. Työn pohjalta on helppo jatkaa lisätutkimukseen aiheesta esimerkiksi Pro gradun muodossa.

5.2 Työn rajoitukset ja löydösten yleistettävyys

Työn merkittävänä rajoituksena voidaan pitää tutkimusmenetelmänä käytettyä käsitteellistä kirjallisuustutkimusta, sillä tutkimusmenetelmä rajoittaa tutkimuksen uuden tiedon tuottamista, jolloin jo valmiiksi runsaasti tutkitussa aiheessa työn merkitys vähenee. Toinen rajoitus työssä on lähteiden suhteellinen vähäisyys aiheen monipuolisuuteen nähden. Erityisesti lähteitä, joissa IaaS -palvelumuodon haavoittuvuuksia olisi pohdittu empiirisestä näkökulmasta, olisi ollut tarpeen käyttää enemmän. Johtuen lähteiden yksipuolisuudesta, työn kirjallisuuskatsaus jääkin näkökulmaltaan hyvin teoriapohjaiseksi, eikä haavoittuvuuksia päästä kattavasti linkittämään todelliseen pilvipalveluiden ympäristöön.

Löydökset ovat osaltaan hyvin yleistettäviä, sillä lähdeartikkeleina on käytetty tietojenkäsittelyn alan johtavien lehtien julkaisemia artikkeleita. Lähdeartikkeleiden valikoinnista käytettiin myös siteerauksiin pohjautuvaa karsintaa, jossa mukaan pyrittiin ottamaan eniten siteerattuja artikkeleita. Siteerauksien karsinta suoritettiin Scopuksen ja Google Scholarin tarjoamien siteerauksiin perustuvan artikkelien järjestämisen avulla. Runsaimmin siteerattujen artikkelien käyttö varmistaa sen, että akateeminen yhteisö on havainnut artikkelin sisällön olevan relevanttia käyttäen siteeratun artikkelin sisältöä oman tutkimuksensa pohjana. Lähdeartikkelit koostuvat tuoreista julkaisuista, joista kaikki ovat julkaistu 2009 vuoden jälkeen, mistä johtuen löydökset ovat relevantteja nykyisissä IaaS -palveluissa.

5.3 Lisätutkimus

Lisätutkimusaiheena työssä esille nousseiden asioiden pohjalta olisi IaaS -palveluiden haavoittuvuuksien tutkiminen empiirisen näkökulman kautta. Asian tutkiminen empiirisesti olisi relevanttia myös siksi, että aiemmin julkaistuissa tutkimuksissa ei ole laajasti keskitytty empiirisiin näkökulmiin IaaS -palvelumuodon haavoittuvuuksissa. Empiirisen tutkimuksen voisi toteuttaa esimerkiksi kvantitatiivisena tutkimuksena, jolloin haavoittuvuuksien merkitykselle todellisessa pilvipalveluiden ympäristössä saataisiin konkreettisia arvoja, joiden kautta haavoittuvuuksien merkityssuhteita voitaisiin arvioida luotettavasti.

Lähdeluettelo

5 Important Benefits of Infrastructure as a Service. (2014). Viitattu 16.12.2015. Saatavilla: http://www.statetechmagazine.com/article/2014/03/5-important-benefits-infrastructure-service

Abreu, A., Correira, M., & Rocha, F. (2011). The Final Frontier: Confidentiality and Privacy in the Cloud. *Computer*. (9). 44-50.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.

Chang, E., Chen, E., & Dillon, T. (2010) Cloud Computing: Issues and Challenges. *In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, 27-33. IEEE.

Constantin, L. (2014). Attackers install DDos bots on Amazon cloud, exploit Elastisearch weakness. Viitattu 16.12.2015. Saatavilla: http://www.computerworld.com/article/2490432/cloud-security/attackers-install-ddos-bots-on-amazon-cloud--exploit-elasticsearch-weakness.html

Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011). A survey of risks, threats and vulnerabilities in cloud computing. *In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications on,* 12. ACM.

Fernandes, D., Freire, M., Gomes, J., Inácio, P., & Soares, L. (2014). Security Issues in Cloud Environments: A Survey. *International Journal of Information Security*. 13(2). 113-170.

Gibson, J., Rondeau, R., Eveleigh, D., & Tan, Q. (2012). Benefits and challenges of three cloud computing service models. *In Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on,* 198-205. IEEE.

Grobauer, B., Walloschek, T., & Stöcker, E. (2011). Understanding cloud computing vulnerabilities. *Security & privacy, IEEE*, 9(2), 50-57.

Gruschka, N., & Jensen, M. (2010). Attack surfaces: A taxonomy for attacks on cloud services. *In 2010 IEEE 3rd international conference on cloud computing on,* 276-279. IEEE.

Gruschka, N., Lacono, L., Schwenk, J., & Jensen, M. (2009). On Technical Security Issues in Cloud Computing. *In Cloud Computing, 2009. CLOUD '09. IEEE International Conference on*, 109-116. IEEE

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 1-13.

Kaufman, L.M. (2009). Data Security in the World of Cloud Computing. *Security & Privacy, IEEE*. 7(4), 61-64.

Lu, Q., Zhu, L., Bass, L., Xu, X., Li, Z., & Wada, H. (2013). Cloud API issues: an empirical study and impact. *In Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures on*, 23-32. ACM.

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on,* 693-702. IEEE.

Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. *Internet Computing, IEEE*, 16(1), 69-73.

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

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, (6), 24-31.

Vaquero, L. M., Rodero-Merino, L., & Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. *Computing*, 91(1), 93-118.

Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud computing. *Communications Surveys & Tutorials, IEEE*, 15(2), 843-859.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, 1(1), 7-18.