Niko Korajoki

Pilvipalvelumallien tietoturvariskejä ja niiden torjunta

Tietotekniikan kandidaatintutkielma

4. toukokuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Niko Korajoki

Yhteystiedot: korniksa@student.jyu.fi

Ohjaaja: Annemari Auvinen

Työn nimi: Pilvipalvelumallien tietoturvariskejä ja niiden torjunta

Title in English: Information security risks of cloud service models and their prevention

Työ: Kandidaatintutkielma

Sivumäärä: 22+0

Tiivistelmä: Tämän kandidaatintutkielma tarkoituksena on kartoittaa pilvipalvelumalleja ja niiden tietoturvariskejä. Tutkielman ajatuksena on käydä läpi millaisia tietoturvariskejä eri pilvipalvelumalleihin kohdistuu, ja millaisia keinoja niiden torjumiseksi on olemassa. Tutkielma on toteutettu kirjallisuuskatsauksena.

Avainsanat: pilvipalvelut, tietoturva

Abstract: The purpose of this bachelor's thesis is to map cloud service models and their information security risks. The idea of the thesis is to review what kind of information security risks are faced by different cloud service models, and what kind of means exist to combat them. The thesis was carried out as a literature review.

Keywords: cloud services, informartion security

Kuviot

Sisällys

1 Johdanto

Pilvipalveluista on tullut laajalle levinnyt teknologia. Pilvipalvelut tarjoavat skaalautuvan, kustannustehokkaan ja on-demand-laskentainfrastruktuurin, jonka avulla organisaatiot voivat siirtää sovelluksensa ja tietonsa keskitetylle alustalle. Pilvipalveluiden laajan käyttöönoton myötä tietoturvariskit ovat kuitenkin nousseet merkittäväksi huolenaiheeksi monille organisaatioille ja yksityishenkilöille.

Tietoturvaloukkauksilla ja tietovarkauksilla voi olla vakava vaikutus yrityksiin, jotka tallentavat arkaluontoisia tietojaan pilveen. Nämä riskit voivat vaihdella luvattomasta tietojen käsittelystä immateriaalioikeuksien varkauksiin tai muuhun tietoturvaloukkaukseen, joka voi vahingoittaa vakavasti organisaation mainetta ja liiketoimintaa. Lisäksi organisaatioiden on otettava huomioon tietoturvaloukkausten mahdolliset oikeudelliset ja lainsäädännölliset vaikutukset, koska ne voivat johtaa merkittäviin taloudellisiin ja oikeudellisiin seuraamuksiin.

Kun organisaatiot jatkavat tietojensa siirtämistä pilveen, on tärkeää arvioida ja hallita pilvipalveluihin liittyviä tietoturvariskejä. On olennaista ymmärtää, että pilviturvallisuus on pilvipalvelun tarjoajan ja käyttäjän yhteinen vastuu. Pilvipalveluntarjoajat varmistavat pilviinfrastruktuurin turvallisuuden, mutta käyttäjät ovat vastuussa tietojensa ja pilvessä toimivien sovellusten turvaamisesta.

Tämän tutkielman tavoitteena on tunnistaa ja käsitellä tietoturvariskejä, jotka liittyvät kolmeen pilvipalvelumalliin – IaaS, PaaS ja SaaS – sekä tarjota käyttäjille ennaltaehkäisystrategioita näiden riskien vähentämiseksi. Tutkimalla näitä riskejä ja ennaltaehkäisystrategioita, tämä tutkielma pyrkii edistämään pilviturvallisuuden ymmärtämistä.

2 Pilvipalvelut

Pilvipalvelut ja pilvipalvelumallit ovat joukko tiedonkäsittelypalveluita, kuten Infrastructure-as-a-Service(IaaS), Platform-as-a-Service(PaaS) ja Software-as-a-Service(SaaS), jotka toimitetaan internetin kautta useimmiten "pay per use", eli käytönmukaisen laskutuksen mukaan. Nämä palvelut tarjoavat käyttäjilleen monia etuja, kuten paremman skaalautuvuuden, joustavuuden ja alhaisemmat kustannukset verrattuna perinteiseen paikalliseen tietojenkäsittelyyn (Armbrust ym. 2010).

Pilvipalveluista on tullut viime vuosina yhä suositumpia, ja monet organisaatiot ovat omaksuneet pilviratkaisuja erilaisiin käyttötarkoituksiin, kuten tiedon tallentamiseen, sovelluskehitykseen ja työryhmien tai jopa organisaatioiden väliseen yhteistyöhön (Varia 2009). Pilvipalveluiden suosiota on johtanut pilvipalveluiden tarjoajien, kuten Amazon Web Services (AWS), Microsfot Azure ja Google Cloud Platform(GCP) nopea kasvu, jotka tarjoavat laajan valikoiman pilvipalveluita erilaisiin liiketoiminnan tarpeisiin (Hasan, Alamari ja A.E. 2012).

Pilvipalveluiden käyttöönotto tuo kuitenkin mukanaan myös useita erilaisia haasteita, kuten turvallisuus- ja vaatimustenmukaisuusongelmia, tietosuojaa ja palvelun toimittajan yhtäkkistä sulkemista (Rittinghouse ja Ransome 2016). Näistä haasteista huolimatta pilvipalveluiden edut ovat edelleen houkutelleet yrityksiä ja yksityisiä käyttäjiä pilven pariin.

Pilvipalveluiden etujen täysimääräiseksi ymmärtämiseksi organisaatioiden on arvioitava huolellisesti liiketoimintatarpeensa ja valittava sopiva pilvipalvelumalli ja toimittaja. Heillä on myös oltava vankka ymmärrys pilvipalveluiden hallinnasta ja hallinnosta, varmistaakseen heidän pilvipalveluiden tehokkaan ja turvallisen käytön, että hallinnan. (Mell ja Grance 2011).

Pilvipalvelut tarjoavat organisaatioille tehokkaan joukon työkaluja kustannusten vähentämiseen, sekä ketteryyden että työtehon lisäämiseen.

2.1 IaaS

IaaS eli "Infrastructure-as-a-service"on pilvipalvelumalli jonka avulla asiakkaat voivat vuokrata laskentaresursseja, kuten virtuaalikoneita, tallennustilaa ja verkottumista käyttökohtaisesti. IaaS-palveluntarjoajat tarjoavat valikoiman virtualisoituja infrastruktuuripalveluita, jotka voidaan räätälöidä vastaamaan asiakkaiden erityistarpeita (Buyya ym. 2009).

IaaS-mallissa asiakkaat vuokraavat infrastruktuuripalvelut palveluntarjoajalta, joka vastaa taustalla olevien laitteistojen ja ohjelmistojen ylläpidosta. Asiakkaat voivat mukauttaa virtuaalista infrastruktuuriaan, mukaan lukien käyttöjärjestelmänsä, väliohjelmistonsa ja sovelluksensa, ja ottaa ne käyttöön palveluntarjoajan infrastruktuurissa (Vaquero ym. 2009).

IaaS-malli tarjoaa asiakkaille useita etuja. Asiakkaat voivat välttää oman fyysisen infrastruktuurinsa hankintaan ja ylläpitoon liittyvät kustannukset, ja vuokrata sen sijaan virtuaalisen infrastruktuurin palvelut palveluntarjoajalta (Marston ym. 2011). Tämä voi olla erityisen houkuttelevaa pienille ja keskisuurille yrityksille, joilla ei välttämättä ole resursseja tai halua investoida omaan fyysiseen infrastruktuuriinsa.

Asiakkaat voivat mukauttaa virtuaalisen infrastruktuurinsa vastaamaan erityisiä tarpeitaan, ja ottaa käyttöön sovelluksiaan palveluntarjoajan infrastruktuurissa. Koska infrastruktuuri on virtualisoitu, asiakkaat voivat heposti siirtää sovelluksiaan eri palveluntarjoajien välillä, tai jopa saman palveluntarjoajan omistamien eri datakeskusten välillä (Hajinab 2013)

IaaS-malli on tehokas ratkaisu laskentaresurssien tarjoamiseen asiakkaille (Marston ym. 2011). Vuokraamalla virtuaalisen infrastruktuurin palvelut palveluntarjoajalta, asiakkaat voivat nauttia edistyneiden laskentaresurssien eduista, välttäen samalla fyysisen infrastruktuurin hankintaan ja ylläpitoon liittyviä kustannuksia. Skaalautuvuuden, joustavuuden ja kustannustehokkuuden ansiosta IaaS-malli tulee mitä luultavimmin jatkamaan suosiotaan tulevina vuosina.

2.2 PaaS

PaaS eli "Platform-as-a-service"pilvipalvelumalli tarjoaa alustan sovellusten rakentamiseen, käytöönottoon ja hallintaan. PaaS-mallissa pilvipalveluntarjoaja tarjoaa alustan, joka koos-

tuu ajonaikaisesta ympäristöstä, ohjelmointikielistä, kirjastoista sekä sovellusten kehittämiseen ja käyttöönottoon tarvittavista työkaluista. Näin kehittäjät voivat keskittyä sovellusten rakentamiseen ja käyttöönottoon, ilman että heidän tarvitsee huoolehtia infrastruktuurin hallinnasta ja ylläpidosta (Vaquero ym. 2009).

PaaS-mallin yleisimpiin käyttäjiin kuuluvat kehittäjät ja organisaatiot, jotka haluavat noepasti kehittää ja ottaa käyttöön sovelluksia ilman merkittävi infrastruktuuri-investointeja (Vaquero ym. 2009). PaaS-palveluntarjoajat tarjoavat erilaisia palveluita, mukaan lukien sovelluskehityskehiykset, tietokannat, väliohjelmistoot ja viestipalvelut, joita voidaan käyttää mobiili- ja verkkosovellusten rakentamiseen ja käyttöönottoon (Kavis 2011).

PaaS-mallin avulla kehittäjät voivat myös hyödyntää pilvi-infrastruktuurin skaalautuvuutta ja joustavuutta, jolloin he voivat helposti sakaalata sovelluksiaan ylös tai alas muuttuvan kysynnän mukaan (Armbrust ym. 2010). Tämä tekee PaaS-mallista erityisen hyödyllisen sovelluksissa, joissa on vaihteleva työkuorma, tai jotka vaativat nopeaa skaalausta.

Eduistaan huolimatta PaaS-malli sisältää myös joitain haasteita, kuten huolta toimittajan lukkiutumisesta ja taustalla olevan infrastruktuurin rajoitetusta hallinnasta (Marston ym. 2011). Lisäksi kaikki sovellukset eivät sovellu käyttöönotettavaksi PaaS-alustoille, etenkään ne joilla on erityisiä laitteistovaatimuksia tai korkean suorituskyvyn laskentatarpeita.

PaaS-malli tarjoaa kehittäjälle tehokkaan alusta jonka avulla voidaan rakentaa ja ottaa käyttöön ssovelluksia nopeasti ja helposti hyödyntäen pilvi-infrastruktuurin skaalautuvuutta ja joustavuutta.

2.3 SaaS

SaaS eli "Software-as-a-service"on muunnos pilvilaskentamallista, joka koostuu edellämainituista palvelumalleista (Armbrust ym. 2010). SaaS-malli on pilvilaskentapinon korekin kerros, joka tarjoaa loppukäyttäjille pääsyn sovelluksiin internetin kautta. SaaS-pilvipalvelumallissa ohjelmistosovelluksia isännöi ja ylläpitää kolmas osapuoli, joka on vastuussa sovellusten saatavuuden, suorituskyvyn sekä turvallisuuden varmistamisesta (Mell ja Grance 2011).

SaaS-pilvipalvelumalli tarjoaa useita etuja loppukäyttäjille, mukaan lukien kustannussääs-

töt, lyhentynyt markkinoilletuloaika, sekä pääsy edistyneisiin ominaisuuksiin(Subramanian ja Abdluz-Aziz 2017). Malli sopii erityisen hyvin pienille ja keskisuurille yrityksille, joilla ei välttämättä ole resursseja kehittää ja ylläpitää omia ohjelmistosovelluksiaan (Subramanian ja Abdluz-Aziz 2017). Ulkoistamalla sovellusten ylläpidon kolmannen osapuolen palveluntarjoajalle, yritykset voivat keskittyä ydinosaamiseensa nauttien samalla edistyneiden ohjelmistosovellusten eduista.

Koska sovelluksia isännöidään pilvessä, niiden käyttämiä resursseja voidaan helposti skaalata vastaamaan muuttuvaa kysyntää. Yrityksille tämä tarkoittaa nopeaa ja helppoa tapaa lisätä tai poistaa käyttäjiä tarpeen mukaan, ilman että heidän tarvitsee huolehtia näiden käyttäjien tukemiseen tarvittavasta infrastruktuuristaMell ja Grance 2011. Koska sovellukset toimitetaan internetin kautta, käyttäjät voivat käyttää niitä mistä tahansa, millä tuetulla laitteella tahansa, kunhan omaa nettiyhteyden. Näin yritykset voivat myös tukea etätyötä, jonka suosio on kasvanut erityisesti covid pandemian myötä (“Working conditions in the time of COVID-19: Implications for the future” 2022).

2.4 Pilvipalveluiden etuja

Pilvipalveluista on tullut suosittu vaihtoehto organisaatioille IT-infrastruktuurinsa ja -sovellustensa hallinnassa. Pilvialustojen käytön tärkeimmät edut ovat skaalautuvuus, kustannustehokkuus sekä korkeampi saatavuus ja luotettavuus.

Skaalautuvuus on yksi pilvialustojen merkittävimmistä eduista. Organisaatiot voivat skaalata resurssejaan ylös tai alas muuttuvien tarpeidensa mukaan ilman lisälaitteiston tarvetta (Jansen ja Grance 2014). Näin organisaatiot voivat reagoida nopeasti kysynnän muutoksiin, kuten kausivaihteluihin, ilman kalliita infrastruktuuri-investointeja. Lisäksi pilvialusto tarjoaa joustavan skaalauksen, mikä tarkoittaa, että resursseja voidaan varata tai poistaa automaattisesti kysynnän perusteella, mikä johtaa korkeampaan resurssien käyttöön ja alhaisempiin kustannuksiin (Gong, Xu ja Liu 2010).

Kustannustehokkuus on toinen pilvialustojen suuri etu. Organisaatiot voivat säästää laitteisto-, ylläpito- ja sähkökustannuksia, kun pilvipalveluntarjoajat hallitsevat taustalla olevaa infrastruktuuria ja tarjoavat resursseja jakoperusteisesti (Buyya ym. 2009). Lisäksi pilviympäris-

töt voivat tarjota mittakaavaetuja, koska pilvipalveluntarjoajat voivat hajauttaa infrastruktuurin ja resurssien kustannukset useille asiakkaille (Jansen ja Grance 2014).

Parempi käytettävyys ja luotettavuus ovat myös merkittäviä pilvialustojen etuja. Pilvipalveluntarjoajat on suunniteltu varmistamaan mahdollisimman pitkä käyttöaika redundanssi- ja vikasietomekanismien avulla (Wang ym. 2014. Lisäksi pilvipalveluntarjoajat tarjoavat usein maantieteellisesti hajautettuja datakeskuksia, jotka voivat parantaa käytettävyyttä vähentämällä luonnonkatastrofien tai alueellisten katkosten vaikutuksia (Grossman 2009).

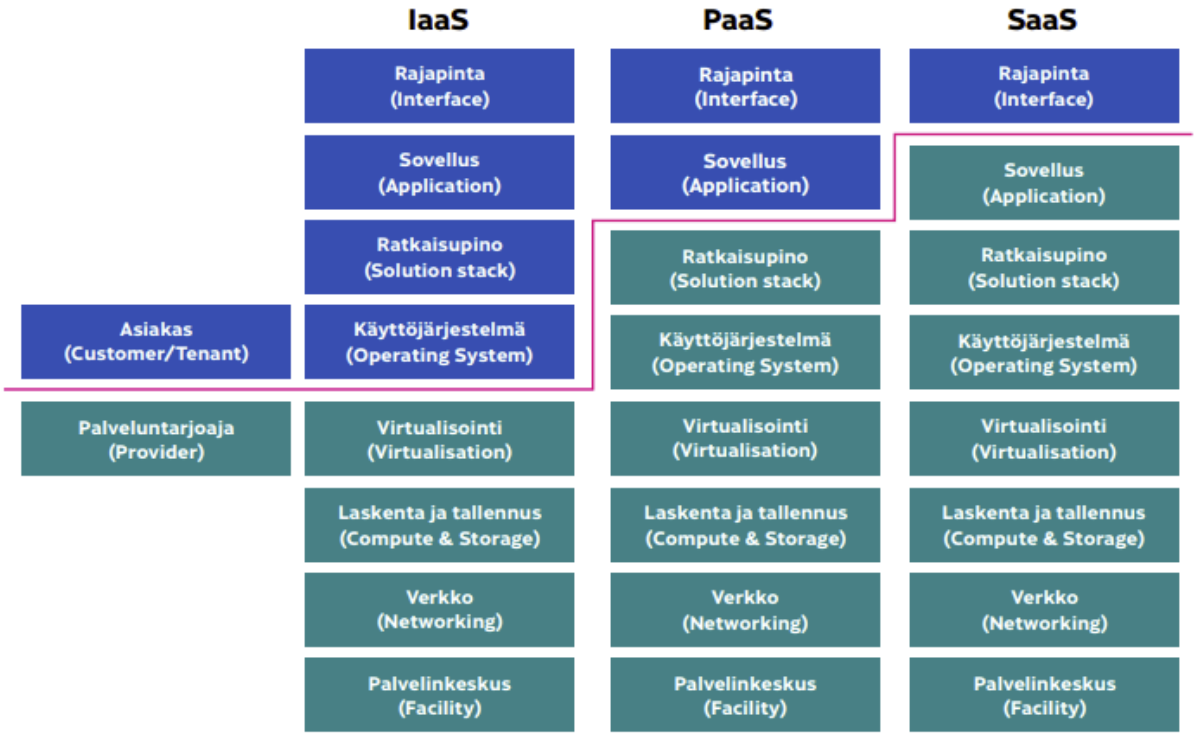
Voidaan todeta, että pilvialustat tarjoavat organisaatioille useita etuja, kuten skaalautuvuuden, kustannustehokkuuden sekä paremman käytettävyyden ja luotettavuuden. Nämä edut voivat auttaa organisaatioita vastaamaan nopeasti kysynnän muutoksiin, säästämään kustannuksia ja parantamaan IT-infrastruktuurinsa ja -sovellustensa saatavuutta ja luotettavuutta. Siksi pilvialustoista on tulossa yhä suositumpi valinta organisaatioille, jotka haluavat hallita IT-resurssejaan tehokkaasti ja tuloksellisesti.

3 Pilvipalveluiden tietoturvariskejä ja niiden torjunta

Pilvipalveluista on tullut suosittu vaihtoehto organisaatioille IT-infrastruktuurin ja -sovellusten hallintaan (Alzahrani ym. 2020). Kun organisaatiot kuitenkin luottavat edelleen pilvipalveluihin, ne kohtaavat myös lisääntyviä kyberturvallisuusriskejä (Ali, Raza ja Khan 2021). Pilvipalveluntarjoajat ovat vastuussa taustalla olevan infrastruktuurin ja palveluiden turvaamisesta, kun taas asiakkaat ovat vastuussa tietojensa ja pilvessä toimivien sovellusten turvaamisesta (Bhardwaj, Jain ja Jain 2018). Siksi on olennaista ymmärtää pilvipalveluita ympäröivä kyberturvallisuusympäristö mahdollisten uhkien vähentämiseksi.

Pilviympäristön kyberturvallisuusuhat voivat vaihdella tietomurroista, DDoS-hyökkäyksistä ja haittaohjelmatartunnoista sisäpiiriuhkiin ja toimitusketjuhyökkäuksiin (Khan ym. 2021). Nämä uhat voivat johtaa luvattomaan pääsyyn arkaluonteisiin tietoihin, immateriaalioikeuksien menettämiseen ja liiketoiminnan häiriöihin (Hashmi ym. 2019). Lisäksi pilvipalvelujen jaetun vastuun malli voi luoda mahdollisen aukon tietoturvaohjauksessa, koska asiakkaat eivät välttämättä ole tietoisia vastuistaan (Zissis ja Lekkas, n.d.).

Kuva 3. Tyypillinen vastuujakomalli.



[27] National Institute of Standards and Technology (NIST). 2011. Special Publication 800-145: The NIST Definition of Cloud Computing. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Kuvio 1. Vastuunjakomalli

3.1 IaaS-mallin uhkat ja mitigointi

IaaS-malliin liittyy paljon erilaisia riskejä, mallin luonteen vuoksi käyttäjän vastuut kasvavat muihin malleihin verrattuna.

Yksi IaaS-mallin tärkeimmistä tietoturvariskeistä on virtuaalikoneiden luvaton käyttö ja tietomurrot. Hyökkääjät voivat hyödyntäävirtuaalikoneiden, hypervisoreiden tai hallintaliitäntöjen haavoittuvuuksia päästäkseen luvattomasti pilviympäristöön(Garg, Versteeg ja Buyya 2013). Riskien mitigoimiseen suositellaan käytettäväksi vahvoja todennusmekanismeja, kuten monitekijätodennusta (MFA). Monitekijätodennus tulisi ottaa käyttöön se varmistamiseksi, että vain valtuutetut käyttäjät voivat käyttää pilviresursseja. Lisäksi virtuaalikoneisiin ja hypervisoreihin tulee asentaa säännöllisiä tietoturvakorjauksia ja -päivityksiä tunnettujen haavoittuvuuksien korjaamiseksi ja hyökkäyspinna vähentämiseksi (Garg, Versteeg ja Buyya 2013).

Myös tietojen menetys ja tietovuoto ovat merkittäviä IaaS-mallin riskejä. Tiedot voivat kadota laitteistovikojen, ohjelmistovirheiden tai tahattoman poistamisen vuoksi. Tietovuoto voi tapahtua, kun tiedot paljastuvat vahingossa tai jaetaan luvattomien käyttäjien kanssa joko virheellisen määrityksen, tai haitallisen toiminnan vuoksi. Tietojen varmuuskopiot tulee ottaa käyttöön säännöllisin testauksin ja validoinnilla, jotta tiedot voidaan palauttaa katoamisen sattuessa(Ristenpart ym. 2009). Tietojen suojaamiseksi luvattomalta käytöltä tulisi käyttää tietojen salaustekniikoita, kuten salausta levossa että siirron aikana. Pääsyn hallinta ja käyttöoikeudet tulee määrittää oikein, jotta tietojen käyttö rajoitetaan valtuutetuille käyttäjille ja estetään tietovuodot (Ristenpart ym. 2009).

Sisäpiiriuhat, mukaan lukien oikeutettujen työntekijöiden tai urakoitsijoiden haitalliset toimet muodostavat merkittävän riskin IaaS-mallissa. Sisäpiiriläiset voivat tarkoituksellisesti väärinkäyttää oikeuksiaa pästäkseen luvatta muokkaamaan tai varastamaan tietoja tai häiritäkseen palvelua(Prasad ym. 2016). Uhan mitigointiin käytetään "Vähiten etuoikeuksia-periaatetta, jossa käyttäjille myönnetään vain työtehtäviensä suorittamiseen tarvittavat luvat. Käyttäjien toimien säännöllinen seuranta ja auditointi tulisi suoorittaa epätavallisen tai epäilyttävän toiminnan havaitsemiseksi (Han, Choi ja Kim 2014).

Palvelunestohyökkäykset, eli DoS-hyökkäykset, joiden tarkoituksena on häiritä tai heiken-

tää pilvipalvelujen saatavuuttaa, ovat vakava huolenaihe IaaS-mallissa. Hyökkääjät voivat täyttää pilviympäristön liiallisilla pyynnöillä tai hyödyntää verkkoinfrastruktuurin tai hypervisorien haavoittuvuuksia aiheuttaakseen palveluhäiriöitä. Vahvojen verkon suojaustoimintojen, kuten palomuurien, tunkeutumisen havaitsemisjärjestelmien ja nopeudenrajoitusten käyttöönotto voi auttaa estämään ja havaitsemaan DoS-hyökkäyksiä.(Ristenpart ym. 2009) Virtuaalikoneiden jakaminen useille eri käytettävyysvyöhykkeille tai alueille voi myös parantaa käytettävyyttä ja lieventää DoS-hyökkäysten vaikutusta. Verkkoinfrastruktuurin ja hypervisorien haavoittuvuuksien säännöllinen seuranta ja auditoointi ovat ratkaisevia toimia DoS-hyökkäysten estämisessä (Morsy, Grundy ja Müller 2010)

3.2 PaaS-mallin uhkat ja mitigointi

PaaS-mallin sisältää edelliseen verrattuna hieman erilaisia tietoturvariskejä, mallien välillä tapahtuva vastuunjako muuttaa tietoturvariskien luonnetta.

PaaS-palveluntarjoajat yleensä tallentavat ja käsittelevät tietoja käyttäjien puolesta, mikä herättää huolta tietosuojasta ja tietosuojasta. Luvaton käyttö, tietomurrot tai tietovuoto voivat aiheuttaa merkittäviä seurauksia. Lieventämistoimenpiteisiin kuuluu vahvojen pääsynvalvonta-, salaus- ja tietojen erotteluteknikoiden käyttöönotto tietojen yksityisyyden ja suojan varmistamiseksi (Yan ym. 2015).

PaaS-alustat voivat tuoda sovelluskerrokseen haavoittuvuuksia, kuten turvattomia koodauskäytäntöjä tai riittämättömiä suojauskokoonpanoja. Lieventämistoimenpiteitä ovat turvallisten koodauskäytäntöjen noudattaminen, säännöllisten turvallisuusarviointien suorittaminen ja asianmukaisten suojauskokoonpanojen, mukaan lukien palomuurit ja tunkeutumisen havaitsemisjärjestelmät, käyttöönotto yleisiltä sovellustason hyökkäyksiltä suojautumiseksi (Ali Babar, Verner ja Nguyen 2016).

Organisaatiot voivat tulla voimakkaasti riippuvaisiksi PaaS-palveluntarjoajasta sovellusten isännöinnissä, kehitystyökaluissa ja muissa palveluissaan.(Hashmi ym. 2019) Tämä herättää huolta toimittajan lukituksesta, palvelun saatavuudesta ja toiminnan jatkuvuudesta. Lieventämistoimenpiteitä ovat PaaS-palveluntarjoajan kanssa tehtyjen palvelutasosopimusten (SLA) huolellinen arviointi, varmuuskopiointi- ja palautusstrategioiden käyttöönotto sekä valmius-

suunnitelmien laatiminen toimittajan lukkiutumiseen ja palvelun keskeytyksiin liittyvien riskien vähentämiseksi (Jung, Kim ja Kim 2019).

PaaS-alustoissa on yleensä useita käyttäjiä eri rooleilla ja oikeuksilla, mikä voi tuoda sisäpiiriuhkia. Luvaton käyttö, haitalliset toiminnot tai oikeuksien väärinkäyttö voivat aiheuttaa turvallisuusriskejä PaaS-ympäristölle.(Bhardwaj, Jain ja Jain 2018) Lieventämistoimenpiteisiin kuuluvat vahvojen todennus- ja valtuutusmekanismien käyttöönotto, roolipohjaiset pääsynhallintajärjestelmät sekä käyttäjien toimintojen seuranta ja auditointi sisäpiiriuhkien havaitsemiseksi ja estämiseksi (Li ym. 2017).

PaaS-mallin käyttäjien on tutustuttava myös lakisääteisiin vaatimuksiin, kuten tietosuojamääräyksiin, alan standardeihin sekä sopimusvelvoitteisiin. Näiden noudattamatta jättäminen voi johtaa laillisiin vastuihin ja mainehaittoihin(Sun ym. 2016). Lieventämistoimenpiteitä ovat PaaS-palveluntarjoajan laillisten sopimusten, SLA-sopimusten ja vaatimustenmukaisuusvaatimusten tarkistaminen ja ymmärtäminen sekä tarvittavien kontrollien ja toimenpiteiden toteuttaminen asiaankuuluvien säädösten ja standardien noudattamisen varmistamiseksi (Liu ym. 2016).

3.3 SaaS-mallin uhkat ja mitigointi

SaaS-palveluntarjoajat yleensä tallentavat ja käsittelevät tietoja käyttäjien puolesta, mikä herättää huolta tietosuojasta ja tietosuojasta. Luvaton käyttö, tietomurrot tai tietovuoto voivat aiheuttaa merkittäviä seurauksia(Raza ym. 2017). Lieventämistoimenpiteisiin kuuluu vahvojen pääsynvalvonta-, salaus- ja tietojen erottelutekniikoiden käyttöönotto tietojen yksityisyyden ja suojan varmistamiseksi (Hashizume, Rosado ja Fernández-Medina 2013).

SaaS-sovellukset vaativat usein todennus- ja valtuutusmekanismeja käyttäjien pääsyn hallintaan. Heikko tai riittämätön identiteetin ja käyttöoikeuksien hallinta voi johtaa luvattomaan käyttöön, tilin kaappaamiseen ja sisäpiirin uhkiin(Ali, Raza ja Khan 2021). Lieventämistoimenpiteitä ovat monitekijätodennuksen käyttöönotto, roolipohjaiset käyttöoikeuksien hallitukset ja käyttäjien käyttöoikeuksien säännölliset tarkistukset asianmukaisten käyttöoikeustasojen varmistamiseksi (Koronios, Anagnostopoulos ja Daassi 2014).

SaaS-sovellukset luottavat pilveen tallennettujen tietojen eheyteen. Tietojen peukalointi, tietojen korruptoituminen tai tietojen menettäminen voi johtaa vakaviin seurauksiin.(Hashmi ym. 2019) Lieventämistoimenpiteisiin kuuluvat tietojen varmuuskopiointi- ja palautusstrategioiden käyttöönotto, säännöllisten tietojen eheystarkastusten suorittaminen ja tietojen luvattomien muutosten seuranta tietojen eheyden ja saatavuuden varmistamiseksi (Sultan 2017).

Organisaatiot luottavat SaaS-sovellusten saatavuuteen päivittäisessä toiminnassaan. Palvelukatkot, seisokit tai suorituskykyongelmat voivat häiritä liiketoimintaprosesseja ja johtaa tuottavuuden menetyksiin(Shajan ja Rahaswamy 2021). Lieventämistoimenpiteitä ovat SaaS-palveluntarjoajan kanssa tehtyjen palvelutasosopimusten (SLA) tarkistaminen ja ymmärtäminen, redundanttien järjestelmien ja varmuuskopiointisuunnitelmien käyttöönotto sekä valmiustoimenpiteiden toteuttaminen palvelun saatavuuden ja jatkuvuuden varmistamiseksi (Sun ym. 2016).

4 Yhteenveto

Pilvipalveluista on tullut suosittu paradigma tietojenkäsittelyresurssien ja -palvelujen toimittamisessa Internetin kautta. Se aiheuttaa kuitenkin myös turvallisuusriskejä, joihin organisaatioiden on puututtava turvatakseen tietonsa ja varmistaakseen pilvipalveluidensa luottamuksellisuuden, eheyden ja saatavuuden. Akateeminen tutkimus on tunnistanut useita tietoturvariskejä kolmessa pilvipalvelumallissa: IaaS, PaaS ja SaaS, sekä suositeltuja lieventäviä toimenpiteitä.

IaaS (Infrastructure-as-a-Service): IaaS-mallissa organisaatiot vuokraavat virtualisoituja laskentaresursseja, kuten virtuaalikoneita (VM:itä), tallennustilaa ja verkkoja pilvipalveluntarjoajilta. IaaS:ään liittyviä tietoturvariskejä ovat virtualisoinnin haavoittuvuudet, kuten hypervisorhyökkäykset ja VM-pako, jotka voivat johtaa luvattomaan käyttöön ja tietomurtoihin (Almorsy, Grundy ja Müller 2016). Näiden riskien vähentämiseksi tulee ottaa käyttöön vahva todennus, säännölliset tietoturva-arvioinnit, verkon suojauksen valvonta ja korjaustiedostojen hallinta.

PaaS (Platform-as-a-Service): PaaS-mallissa pilvipalveluntarjoajat tarjoavat alustan sovellusten kehittämiseen ja käyttöönottoon ilman tarvetta hallita taustalla olevaa infrastruktuuria. PaaS:n tietoturvariskejä ovat epävarmat sovelluskehityskäytännöt, kuten turvallisten koodauskäytäntöjen puute, mikä voi johtaa haavoittuvuuksiin käytössä olevissa sovelluksissa (Hashizume, Rosado ja Fernández-Medina 2013). Lieventämistoimenpiteisiin tulisi kuulua suojatut koodauskäytännöt, säännölliset turvallisuusarvioinnit ja PaaS-alustan tarjoamien turvaominaisuuksien, kuten pääsynvalvonta ja suojatut API:t, käyttöönotto.

SaaS (Software-as-a-Service): SaaS-mallissa organisaatiot käyttävät pilvipalveluntarjoajien tarjoamia pilvipohjaisia sovelluksia. SaaS:n tietoturvariskejä ovat tietoturvaloukkaukset, luvaton pääsy arkaluontoisiin tietoihin sekä tietojen säilytyspaikasta ja viranomaisvaatimuksista johtuvat vaatimustenmukaisuusriskit(Jung, Kim ja Kim 2019). Lieventämistoimenpiteisiin tulisi kuulua vahva todennus, tietojen salaus, varmuuskopiot, SLA-sopimukset (Service Level Agreements) ja vaatimustenmukaisuustarkistukset sen varmistamiseksi, että tiedot suojataan ja säilytetään säädösten vaatimusten mukaisesti (Raza ym. 2017)).

Yllä mainittujen erityisten riskien ja lieventämistoimenpiteiden lisäksi organisaatioiden tulee myös arvioida huolellisesti pilvipalveluntarjoajien tietoturvakäytäntöjä, mukaan lukien fyysiset turvatoimenpiteet, pääsynvalvonta, tietojen salaus ja häiriötilanteisiin reagointikyky (Zhou ym. 2013). Pilvipalveluntarjoajien kanssa tehdyissä sopimuksissa tulee myös hahmotella selkeästi molempien osapuolten turvallisuusvaatimukset ja vastuut riittävän turvatoimien varmistamiseksi.

Lähteet

Ali, Wajid, Babar Raza ja Suleman Ullah Khan. 2021. “Cybersecurity Threats, Vulnerabilities, and Attacks: A Survey on Cloud Environment”. *IEEE Access* 9:26500–26517.

Ali Babar, M., J. Verner ja H. A. Nguyen. 2016. “Security in cloud computing: Opportunities and challenges”. *IEEE Cloud Computing* 3 (4): 16–25.

Almorsy, M., J. Grundy ja I. Müller. 2016. “An analysis of the cloud computing security problem”. *arXiv preprint arXiv:1609.01107.*

Alzahrani, Abdullah I, Mohammed Alsaleh, Mohammad A Alsolami ja Saad Almehmadi. 2020. “Cloud computing adoption factors in the public sector: a systematic review”. *International Journal of Advanced Computer Science and Applications* 11 (9): 85–91.

Armbrust, M, A Fox, R Griffith, A Joseph, R Katz, A Konwinski ja M Zaharia. 2010. “A view of cloud computing”. *Communications of the ACM* 53:50–58.

Bhardwaj, Monika, Vipin Jain ja Shikha Jain. 2018. “A survey on security issues in cloud computing”. *Journal of Network and Computer Applications* 89:11–25.

Buyya, R, C.S Yeo, S Venugopal, J Broberg ja I Brandic. 2009. “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility”. *Future Generation computer systems* 25:599–616.

Garg, S, S Versteeg ja R Buyya. 2013. “A framework for ranking of cloud copmuiting services”. *Future Generation Computer Systems* 29:1012–1023.

Gong, Weiming, Guanglin Xu ja Anxue Liu. 2010. “Cloud computing and its key techniques”. *Journal of Software* 21 (2): 363–376.

Grossman, Robert L. 2009. “The case for cloud computing”. *IT professional* 11 (2): 23–27.

Hajinab, S, S Najafi. 2013. “Virtualization as a core element of cloud computing technology”. *Future Generation computer systems* 9:10–18.

Han, Y, Y Choi ja D Kim. 2014. “Protecting virtual machines against insider attacks in cloud computing: Survey of current approaches.” *Journal of Network and Computer Applications* 37:82–91.

Hasan, M.R, A Alamari ja Saddujm A.E. 2012. “Cloud computing: Overview and risk analysis”. *Journal of Advanced Computer Science and Technology Research* 2:102–116.

Hashizume, K., D. G. Rosado ja E. Fernández-Medina. 2013. “An analysis of security issues for cloud computing”. *Journal of Internet Services and Applications* 4 (5): 5–13.

Hashmi, Muhammad Shoaib, Muhammad Bilal, Syed Ali, Mushtaq Ahmed ja Muhammad Sheraz Khan. 2019. “Security issues and their solutions in cloud computing: A survey”. *Journal of Ambient Intelligence and Humanized Computing* 10 (4): 1239–1254.

Jansen, Wayne A, ja Timothy Grance. 2014. “Guidelines on security and privacy in public cloud computing”. *NIST Special Publication* 800 (146): 1–84.

Jung, J., Y. Kim ja S. Kim. 2019. “A comprehensive review on security risks and countermeasures for Platform as a Service in cloud computing”. *International Journal of Distributed Sensor Networks* 15 (10): 1550147719882352.

Kavis, M. 2011. “Understanding PaaS.” *Computer* 44:92–95.

Khan, Muhammad Atif, Muhammad Qasim, Muhammad Rizwan Asghar ja Muhammad Naeem. 2021. “Security challenges and solutions in cloud computing: a systematic review”. *Concurrency and Computation: Practice and Experience* 33 (10): e6557.

Koronios, A., D. Anagnostopoulos ja M. Daassi. 2014. “Security as a service in the cloud”. *Information Systems Management* 31 (3): 249–259.

Li, X., X. Huang, K. J. Lin, L. Zhang ja Q. Hu. 2017. “Insider threats in cloud computing: Detection, analysis, and prevention”. *IEEE Transactions on Services Computing* 10 (1): 6–21.

Liu, C., J. Liu, X. Chen ja X. Liao. 2016. “Cloud service model-based risk assessment for cloud computing”. *Future Generation Computer Systems* 61:36–48.

Marston, S, Z Li, S Bandyopadhyay, J Zhang ja A Ghalasi. 2011. “Cloud computing—The business perspective.” *Decision Support Systems* 51:176–189.

Mell, P, ja T Grance. 2011. “The NIST definition of cloud computing”. *National Institute of Standards and Technology* 53:50–56.

Morsy, M.A., J Grundy ja I Müller. 2010. “An analysis of the cloud computing security problem.” *Proceedings of the 2010 ACM Symposium on Applied Computing,* 1990–1996.

Prasad, A.R., S Shah, S Garg ja R Buyya. 2016. “Securing data in the cloud: Opportunities and challenges.” *Future Generation Computer Systems* 56:701–716.

Raza, S., M. Shafiq, Z. Shafiq ja M. H. Rehman. 2017. “Cloud computing security risks and mitigation strategies: A systematic review”. *Future Computing and Informatics Journal* 2 (1): 1–16.

Ristenpart, T, E Tromer, H Shacham ja S Savage. 2009. “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds.” *Proceedings of the 16th ACM conference on Computer and Communications Security,* 199–212.

Rittinghouse, J.W., ja J.F. Ransome. 2016. *Cloud computing: implementation, management, and security.* Amazon Web Services Whitepaper.

Shajan, Anette, ja Shanta Rahaswamy. 2021. “Survey of Security Threats and Countermeasures in Cloud Computing”. *United Internation Journal for Research Technology* 02.

Subramanian, N, ja A.R Abdluz-Aziz. 2017. “The software as a service (SaaS) model of cloud computing: A survey of security challenges”. *Journal of Network and Computer Applications* 80:17–29.

Sultan, N. 2017. “A review of the state-of-the-art cloud security and privacy-preserving models in big data environments”. *Journal of Cloud Computing* 6 (1): 1–23.

Sun, M., C. Liu, Z. Wang ja X. Wang. 2016. “Secure data sharing in cloud computing: A survey”. *IEEE Transactions on Services Computing* 9 (2): 261–276.

Wang, Xiaoyu, Dan Zhang, Guihua Liang ja Ying Shi. 2014. “Research on cloud computing security problem and strategy”, 250–253.

Vaquero, L.M, L Rodero-Merino, J Caceres ja M Lindner. 2009. “A break in the clouds: towards a cloud definition”. *ACM SIGCOMM Computer Communication Review* 39:50–55.

Varia, J. 2009. “Cloud computing use cases”. *Amazon Web Services Whitepaper* 1:1–17.

“Working conditions in the time of COVID-19: Implications for the future”. 2022. Viitattu 27. helmikuuta 2023. https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef22012en.pdf.

Yan, Z., X. Liu, X. Wu ja X. Liang. 2015. “Data privacy protection for cloud computing”. *Future Generation Computer Systems* 51:36–43.

Zhou, M., R. Zhang, W. Xie ja M. Qiu. 2013. “Ensuring data security and privacy in cloud computing”. *Communications Magazine, IEEE* 51 (11): 111–116.

Zissis, Dimitrios, ja Dimitrios Lekkas. n.d. “Security issues and challenges for cloud computing”. *Journal of Advanced Research in Information Technology and Management* 5 (1): 1–11.