Lassi Tukiainen

ORGANISAATION PILVIPALVELUIDEN HALLINTA TIETOTURVAN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Tukiainen, Lassi
Organisaation pilvipalveluiden hallinta tietoturvan näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2020, 58 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Pilvipalveluiden rooli organisaatioiden työvälineinä kasvaa jatkuvasti. Pilvipalveluita hyödyntäessä organisaation tulee panostaa entistä enemmän tietoturvaan. Paras tapa varmistua työntekijöiden tietoturvallisesta työskentelystä, on määritellä ja jalkauttaa tehokkaat tietoturvakäytänteet. Tietoturvakäytänteillä, tietoturvakoulutuksilla ja erilaisilla tietoturvakampanjoilla mahdollistetaan organisaatioiden työntekijöiden paras mahdollinen tietoturvatietoisuus. Tässä pro gradu -tutkielmassa tutkitaan organisaation keinoja tietoturvalliseen pilvipalveluiden hallintaan, ja työntekijöiden tietoturvallisen työskentelyn varmistamiseen. Tutkielmassa pyritään vastaamaan kahteen tutkimuskysymykseen, jotka ovat *"Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?"* sekä *"Mitä riskejä pilvipalveluissa ja organisaation pilvipalveluiden hallinnassa on tietoturvan näkökulmasta?"*. Tutkielma sisältää kirjallisuuskatsauksen sekä empiirisen osuuden, joka toteutettiin laadullisena tapaustutkimuksena. Oleellisimpia tietoturvariskejä organisaatioille ovat eteenkin asiakkaita palvelevissa organisaatioissa arkaluonteisen tiedon vuotaminen niille, joilla ei siihen pääsyä tulisi olla. Pilvipalveluiden, joissa organisaation tietoja käsitellään, tietoturvasta ja työntekijöiden tietoturvallisesta työskentelystä voidaan varmistua asianmukaisilla tietoturvakäytänteillä, jotka sisältävät työntekijöille suunnattuja ohjeistuksia sekä vaatimuksia laitteiden ja pilvipalveluiden käytöstä. Järjestelmien ja pilvipalveluiden kokonaisturvallisuutta tarkastellessa on syytä huomioida aina ihmisen tuoma riski. Ihmisriskiä, sisältäen käyttäjän tahalliset tai tahattomat toimet, voidaan minimoida tietoturvakäytänteillä, kouluttamisella sekä tietoturvakäytänteiden noudattamisen seurannalla.

Asiasanat: Pilvilaskenta, Pilvipalvelu, Tietoturva, Tietoturvakäytänteet, Tietoturvatietoisuus, Riskienhallinta

ABSTRACT

Tukiainen, Lassi
Organizations Cloud Service Management from the Information Security perspective
Jyväskylä: University of Jyväskylä, 2020, 58 pp.
Information Systems, Master's Thesis)
Supervisor: Siponen, Mikko

The role of Cloud based services as working tools for organizations is rapidly growing. When using Cloud Services, organizations face many kinds of Information Security requirements. The best way to ensure secure working and awareness of employees is to define and implement effective Information Security Policies. The purpose of this Master's Thesis is to propose tools for organizations to manage their Cloud environment, as well as ensure the Information Security Awareness of their employees. This thesis aims to find answers to two research questions, which are: "*What an organization needs to consider when managing cloud environment from the information security perspective?"* and *"Which are the risks in the cloud services and organizations cloud environment management from the information security perspective?"*. This thesis contains a literature review and a case study. Leakage of information can be considered as the most significant risk for organizations. The information security of the cloud services processing sensitive information should be covered by effective information security policies, as well as the employees using the cloud services. When obtaining the overall security of the system or cloud service, the risk brought by human should always be considered. Human risk, including the intentional and unintentional acts, can be minimized with information security policies, information security training and monitoring the employee's adherence of information security policies.

Keywords: Cloud computing, Cloud Services, Information Security, Information Security Policies, Information Security Awareness, Risk Management

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

1.1 Tutkimuksen tausta

Pilvipalvelut ovat olleet kuluttajien keskuudessa trendi jo pitkään ja myös yritykset siirtyvät nopeaa tahtia niin käyttämään omia työkalujaan pilvipalveluina kuin myös tarjoamaan omia palveluitaan pilvipalvelun muodossa. Tämä luo yrityksille tarpeen ymmärtää syvemmin pilvipalvelumalleja ja pilviympäristön teknistä toteutusta, sekä miten eri palveluita tulisi hallita niiden mahdollisesti hajautuessa eri palveluntarjoajille. Tarvitaan myös tehokasta riskienhallintaa ja tietoturvanäkökulman huomioimista. Eri pilvipalvelumalleilla tietoturvariskit ovat hyvin erityyppisiä. Pilvipalvelun toteutusmallissa tulee huomioida esimerkiksi tiedon sensitiivisyyteen ja pilviarkkitehtuuriin liittyviä asioita. (Zhang, Wuwong, Li & Zhang, 2010.)

Pilvipalveluista puhuttaessa tulee ensin määritellä pilvilaskenta. Mellin ja Gracen (2011) mukaan pilvilaskenta mahdollistaa eri henkilöille pääsyn jaettuihin resursseihin. Sen tunnuspiirteitä ovat käyttäjän itsepalvelumainen käyttö, laaja yhteys verkon välityksellä, resurssien yhdistäminen, nopea skaalautuvuus sekä mitattava palvelu. (Mell & Grace, 2011.) Pilvilaskenta voidaan lisäksi jakaa toteutustavan mukaan neljään eri kategoriaan (ks. luku 2.2), jotka ovat julkinen pilvi, yksityinen pilvi, hybridipilvi sekä yhteisön pilvi. (Savu, 2011.) Pilvipalvelut taas ovat pilvilaskentaa hyödyntäviä, verkon yli käytettäviä palveluita. Pilvipalvelut sisältävät tyypillisesti rajapintoja ja liittymiä eri järjestelmiin ja palveluihin. (Zheng, Wu, Zhang, Lyu & Wang, 2012.) Pilvipalvelut voidaan jakaa palvelumallien mukaan kolmeen malliin: infrastruktuuri palveluna, alusta palveluna sekä sovellus palveluna.

Tietoturva on tiedon oikeellisuuden, saatavuuden ja luottamuksellisuuden varmistamista. (Von Solms & Van Niekerk, 2013.) Tiedon turvaaminen on tärkeää eteenkin pilvipalveluissa, kun tiedon fyysisestä sijainnista ei aina ole palvelun käyttäjällä tarkkaa tietoa. Erityisesti organisaatioissa tietoturva tarkoittaa tyypillisesti sen varmistamista, että organisaation kriittiseen tietoon ei päästä luvatta käsiksi ja se on oikeellista. Erityisen tärkeää organisaation kannalta tiedon

oikeellisuuden varmistamista voidaan nähdä finanssi- tai henkilötietoja käsittelevissä palveluissa. (Tchernykh, Schwiegelsohn, Talbi & Babenko, 2019.) Bulgurcun, Cavusoglun ja Benbasatin (2010) mukaan paras tapa varmistua tietoturvan noudattamisesta henkilöstön toimesta on luoda organisaatiolle tietoturvakäytänteet. Toinen oleellinen asia organisaatioiden tietoturvakäytänteiden lisäksi on yksittäisen työntekijän tietoturvatietoisuuden ylläpitäminen (ks. luku 3.2). (Bulgurcu ym., 2010.) Organisaatiotasolla tietoturvan ja tietoturvauhkien minimoimiseksi tärkeää on myös harjoittaa tehokasta riskienhallintaa. Riskienhallinnan avulla organisaatio voi tarkastella tietoturvariskejä sekä niiden vaikuttavuutta ja todennäköisyyttä, jolloin tietoturvakäytänteet ja muut organisaation prosessit voidaan määritellä riskien minimoimisen näkökulmasta. Markowski & Mannan, 2008.)

Tutkielman kirjallisuuskatsauksen ja empiirisen tutkimuksen perusteella voidaan todeta, että organisaation pilvipalveluiden hallinnassa on syytä huomioida tietoturva ja tietoturvariskit. Tehokkaaseen riskienhallintaan hyvänä keinona voidaan pitää organisaation työntekijöiden tietoturvatietoisuuden ylläpitämistä sekä tietoturvakäytänteiden määrittämistä. Toisaalta tärkeää on myös strateginen riskienhallinta ja organisaation johdon suunnitelmallisuus. Pilviympäristön hallintaan ja arkkitehtuuriin on syytä hyödyntää tietoturvalliseksi todennettuja malleja, jotta yleisimmät riskit saadaan katettua. Empiirisen tutkimuksen oleellisimpina tuloksina voidaan nähdä sitä, että organisaatiot ovat lähtökohtaisesti määritelleet tietoturvakäytänteet ja niiden jalkauttamista ja työntekijöiden tietoturvatietoisuutta ylläpidetään lähinnä tietoturvakoulutusten ja erilaisten ohjeistusten kautta. Suurten organisaatioiden pilvipalvelut koetaan empiirisen tutkimuksen perusteella tietoturvallisiksi, ja työntekijät kokevat tietoturvan erittäin tärkeäksi, jopa itsestäänselvyydeksi.

Tutkielmassa käytettyjen lähdetutkimusten osalta päätettiin rajata hakutulokset pääosin artikkeleihin, jotka on kirjoitettu viimeisen kymmenen vuoden aikana (2010-2020). Pilvipalveluihin liittyvää tutkimustietoa löytyy pitkältä ajalta, erityisen paljon pilvipalveluita ja tietoturvaa on tutkittu viimeisen kymmenen vuoden aikana.

1.2 Tutkimusongelma

Tämän tutkielman tutkimuskysymykset ovat *"Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?"* sekä *"Mitä riskejä pilvipalveluissa ja organisaation pilvipalveluiden hallinnassa on tietoturvan näkökulmasta?"*. Tutkimuksessa tarkastellaan pilvipalveluja ja organisaation pilvipalveluiden hallintaa ja selvitetään, kuinka tietoturva tulee näissä huomioida. Tutkimuksen keskeiset käsitteet ovat *pilvilaskenta, pilvipalvelut, pilvipalveluiden hallintamallit, tietoturva,* sekä *riskienhallinta.*

Tutkimusmenetelmäksi tässä tutkimuksessa valittiin laadullinen tapaustutkimus. Laadullisessa tapaustutkimuksessa keskitytään ymmärtämään tutkimuksen kohdetta ja tutkimusongelmaa syvemmin määrälliseen tutkimukseen

verrattuna, jossa keskitytään suureen otokseen ja tilastoihin. Tutkimuskohteena on yleensä yksi tai useampi tapaus, jossa keskitytään tiettyyn ympäristöön. (Baskarada, 2014.) Tämän tutkielman tapauksena tutkitaan pilvipalveluita ja niiden hallintaa organisaatioissa tietoturvan näkökulmasta. Laadullinen tapaustutkimus toteutetaan haastattelemalla tietoturvaan ja pilviympäristöihin erikoistuneita IT-alan ammattilaisia. Tutkielman empiirinen aineisto kerätään näistä haastatteluista.

Tutkimuksessa on rajattu pilvipalveluiden ja pilvipalveluiden hallintamallien riskit niihin, jotka voidaan nähdä liittyvän tietoturvaan. Kirjallisuuden osalta tutkimuksessa on rajattu lähdekirjallisuus pääosin niihin artikkeleihin, jotka on julkaistu viimeisen kymmenen vuoden aikana (2010-2020). Tutkimuksen tulosten osalta tavoitteena on löytää tietoturvariskejä, joita yritykset voivat hyödyntää pilviympäristöihin siirtyessä ja pilvipalveluiden hallintamallia käyttöönottaessa.

1.3 Tutkielman rakenne

Tutkielman kirjallisuuskatsauksen rakenne on seuraava: luvussa kaksi määritellään pilvilaskenta ja pilvipalvelut, sekä käsitellään pilvipalveluiden palvelu- ja hallintamalleja. Seuraavaksi luvussa kolme määritellään tietoturva sekä riskienhallinta ja käydään läpi tietoturvaa organisaation ja käyttäjän näkökulmasta, sekä tietojärjestelmien tietoturvaa ja riskejä. Luvussa neljä käsitellään pilvipalveluiden yleistä hallintaa palveluntarjoajan ja käyttäjäorganisaatioiden näkökulmista, sekä kuinka tietoturva tulisi huomioida pilvipalveluissa. Luku viisi on yhteenveto kirjallisuuskatsauksesta. Tutkielman empiirinen tutkimus alkaa luvussa kuusi, jossa esitellään tutkimusmenetelmä ja tutkimuksen eteneminen. Luvussa seitsemän esitellään tutkittava tapaus ja tutkimuksen aineisto. Tämän jälkeen luvussa kahdeksan esitellään tutkimuksen tulokset ja pohdinta. Luku yhdeksän on yhteenveto tutkimuksesta.

2 PILVILASKENTA JA PILVIPALVELUT

Pilvipalveluita käsitellessä tulee oleellisena seikkana määritellä pilvilaskenta sekä pilvilaskennan käyttöönottomallit sekä pilvipalvelumallit. Tämän luvun ensimmäisessä alaluvussa määritellään käsitteenä pilvilaskenta ja esitellään sen tunnuspiirteitä. Toisessa alaluvussa käsitellään pilvipalveluiden eri käyttöönottomalleja ja niiden teknistä toteutusta. Kolmannessa alaluvussa käsitellään pilvipalveluiden hallintaa ja hallintamalleja organisaatioiden näkökulmasta.

2.1 Pilvilaskenta

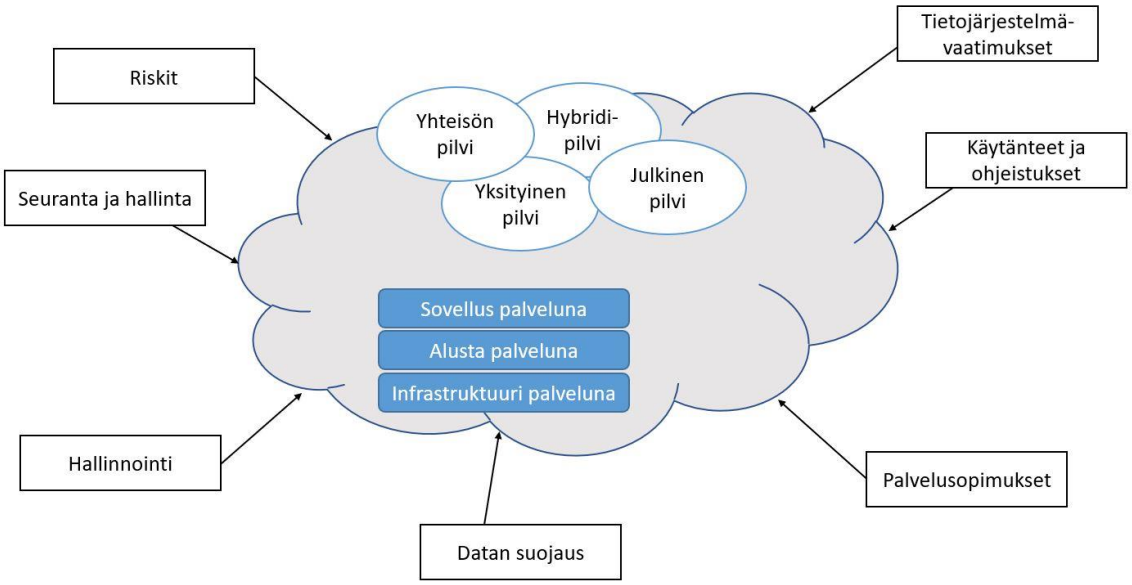
Mellin ja Grancen (2011) mukaan pilvilaskenta voidaan määritellä mallina, joka mahdollistaa verkon kautta pääsyn jaettuihin resursseihin, jotka eivät vaadi suurta vaivannäköä niiden hallinnan tai palveluntarjoajan kanssa kommunikoinnin suhteen. Nämä resurssit voivat olla esimerkiksi verkkoyhteyksiä, palvelimia, sovelluksia tai palveluja. Mell ja Grance (2011) listaavat myös viisi pilvilaskennan tunnuspiirrettä, jotka ovat:

1. *Käyttäjän itsepalvelumainen käyttö*
2. *Laaja yhteys verkon välityksellä*
3. *Resurssien yhdistäminen*
4. *Nopea skaalautuvuus*
5. *Mitattava palvelu*

Käyttäjän itsepalvelumaisella käytöllä tarkoitetaan sitä, että pilvipalvelun käyttäjä pystyy hyödyntämään pilvilaskentaa itsenäisesti, ilman palveluntarjoajan kanssa kommunikointia. Laajalla yhteydellä verkon välityksellä taas tarkoitetaan sitä, että pilvilaskentaa pystytään hyödyntämään verkkoyhteyden välityksellä eri alustoilla ja päätelaitteilla, esimerkiksi mobiililaitteilla tai tietokoneella. Resurssien yhdistäminen tarkoittaa palveluntarjoajan mahdollisuutta palvella jaetuilla resurssivarastoilla useita asiakkaita. Nopealla skaalautuvuudella tarkoitetaan sitä, että pilvilaskentaa hyödyntäen resurssit skaalautuvat automaattisesti ja dynaamisesti asiakkaille eri tarpeiden mukaan, jolloin resurssien määrää voidaan nopeasti kasvattaa tai vähentää. Pilvilaskentaa hyödyntävät palvelut ja järjestelmät ovat myös mitattavia, eli niistä saadaan nopeasti selville palveluun liittyviä oleellisia asioita, esimerkiksi aktiiviset käyttäjät. (Mell & Grance, 2011.)

Pilviympäristössä palvelut voidaan tarjota kolmena eri mallina: infrastruktuuri palveluna, alusta palveluna tai sovellus palveluna (ks. luku 2.3) ja ne voidaan olla toteutettu julkisena pilvenä, yksityisenä pilvenä, niiden yhdistelmänä, hybridipilvenä tai yhteisön pilvenä (ks. luku 2.2). Kuviossa 1 on kuvattu pilven eri toteutusvaihtoehtoja sekä niiden kannalta oleellisia vaatimuksia tai toimenpiteitä. Pilviympäristöä kohtaa poikkeuksetta tietojärjestelmävaatimuksia sekä riskejä, sekä vaatimuksia datan suojauksesta. Se vaatii organisaatiolta käytänteiden

ja ohjeistusten luomista työntekijöilleen, sekä tehokasta hallinnointia ja seurantaa. Pilvipalvelut sisältävät myös aina palvelusopimuksia esimerkiksi pilvipalvelun tarjoajan ja pilvipalvelun käyttäjän välillä. (Ramgovind, Eloff & Smith, 2010.)



KUVIO 1 Pilvilaskennan tunnuspiirteet ja vaatimukset (mukaelma Ramgovindin, Eloffin ja Smithin (2010) kuviosta)

2.2 Pilvilaskennan käyttöönottomallit

Pilvilaskenta voidaan jakaa käyttöönottomallin mukaan neljään kategoriaan, jotka ovat julkinen pilvi (public cloud), yksityinen pilvi (private cloud), yhteisön pilvi (community cloud), sekä hybridipilvi (hybrid cloud). (Savu, 2011.)

2.2.1 Julkinen pilvi

Julkinen pilvi tarkoittaa suurta, jaettua pilviympäristöä, joka on tyypillisesti useiden organisaatioiden käytettävissä. Julkisen pilven luoja ja omistaja on pilvipalveluita muille organisaatioille ja yrityksille tarjoava organisaatio. Julkisen pilven käyttäjäorganisaatioiden data sijaitsee tällöin pilvipalveluntarjoajan tiloissa. Pilvipalveluita ostavalle ja hyödyntävälle yritykselle julkisen pilven hyötyjä on todella joustava skaalautuvuus, pilvipalveluiden hyödyntäminen verkon yli ja omien palvelimien tarpeettomuus näiden palveluiden osalta. Toisaalta yrityksen voi olla haastavaa saada tietää, missä heidän omistamansa data sijaitsee. (Savu, 2011 ja Mell & Grance, 2011.)

Julkisen pilven palvelut ovat tyypillisesti jaetun hallinnan pilviympäristössä, joka on saatavilla useille eri käyttäjille tai organisaatioille. Jaetun hallinnan ja ympäristön johdosta tarvitaan salattuja yhteyksiä ja rajattuja resursseja tietyille organisaatioille. Julkisen pilven jaettu pilviympäristö tarjotaan sen piiriin kuuluville organisaatioille käytännössä *"pay-per-use"* -palveluna, joka tarkoittaa sitä,

että pilviresursseja hyödyntävä organisaatio maksaa suuresta resurssivarannosta vain niistä resursseista, jota hyödyntää. Tästä resurssivarannosta resursseja hyödyntävät samanaikaisesti useat eri organisaatiot. Jaetussa pilviympäristössä suurimman turvallisuushuolen tuokin useiden organisaatioiden saman resurssivarannon käyttäminen. (Moghaddam, Rohani, Ahmadi, Khodadadi & Madadipouya, 2015.)

Julkisen pilven tunnuspiirteitä, hyötyjä ja haasteita organisaation näkökulmasta on kuvattu taulukossa 1.

TAULUKKO 1 Julkisen pilven tunnuspiirteet sekä niiden hyödyt ja haasteet organisaation näkökulmasta (Moghaddam ym., 2015 ja Bokhari, Shallal & Tamandani, 2016)

Julkisen pilven tunnuspiirre	**Hyödyt**	**Haasteet**
Jaetut resurssivarannot	Joustava skaalautuvuus	Tietoturva
Data ja palvelut palveluntarjoajan palvelinympäristössä	Dataan liittyvä riski palveluntarjoajalla	Heikko näkyvyys datan fyysiseen sijaintiin
Kustannukset käytön mukaan	Kustannustehokkuus	

2.2.2 Yksityinen pilvi

Yksityisellä pilvellä tarkoitetaan yksittäisen organisaation tarpeisiin, joko pilveä käyttävän organisaation tai kolmannen osapuolen, luomaa pilviympäristöä. Pilviympäristön palvelimet voivat sijaita joko organisaation tiloissa, tai organisaation tilojen ulkopuolella. Pilvipalveluita käyttävälle organisaatiolle yksityisen pilven etuja ovat sen turvallisuus ja palvelinlaitteiden omistaminen, jolloin tiedetään tarkalleen, missä organisaation data sijaitsee. Toisaalta yksityisessä pilvessä ei saada kustannusetuja resurssien yhdistämisestä. (Savu, 2011 ja Mell & Grance, 2011.)

Yksityinen pilvi siis mahdollistaa julkisen pilven jaetusta pilviympäristöstä ja resurssivarannosta poiketen pilviympäristön, jossa palvelut ja resurssit sijaitsevat tietyn organisaation käytössä olevassa palvelinympäristössä. Tämä luo paremmat lähtökohdat esimerkiksi tiedon turvallisuuden ja pääsyn rajoittamiseen. Yksityisessä pilvessä ympäristön päivitykset ja ylläpito, mukaan lukien turvallisuus, on yksinkertaisempaa ja helpommin hallittavaa. Toisaalta resurssien suunnittelu näyttelee suurempaa roolia yksityisessä pilvessä, sillä pilviympäristö ei ole niin skaalautuva kuin julkisessa pilvessä, ja yksityisen pilven omistama organisaatio maksaa koko resurssivarannosta. Resurssien käyttöä on silloin myös tärkeää pyrkiä pitämään mahdollisimman lähellä resurssivarannon kapasiteetin rajaa, jotta pilviympäristön hyödyntäminen on mahdollisimman tehokasta. (Moghaddam ym., 2015.)

Yksityisen pilven tunnuspiirteitä, hyötyjä ja haasteita organisaation näkökulmasta on kuvattu taulukossa 2.

TAULUKKO 2 Yksityisen tunnuspiirteet sekä niiden hyödyt ja haasteet organisaation näkökulmasta (Moghaddam ym., 2015 ja Bokhari ym., 2016.)

Yksityisen pilven tunnuspiirre	**Hyödyt**	**Haasteet**
Organisaation oma palvelinympäristö	Tarkka tieto siitä, missä data sijaitsee fyysisesti	Kustannustehokkuus
Organisaation oma resurssivaranto	Tiedon turvallisuus, ympäristön hallinta	Resurssien kapasiteetin arviointi ja käyttö

2.2.3 Yhteisön pilvi

Yhteisön pilvi on tietylle yhteisölle jaettu pilviympäristö. Pilviympäristö palvelee tyypillisesti tiettyä tavoitetta tai yhteisöä, ja sen piiriin voi kuulua useita organisaatioita, jotka jakavat tavoitteen. Yhteisön pilveä voi hallita yhteisön organisaatio tai kolmas osapuoli. (Savu, 2011 ja Mell & Grance, 2011.) Yhteisön pilvi valitaan pilvilaskennan käyttöönottomalliksi erityisesti silloin, kun organisaatiot tarvitsevat dynaamiseen yhteistyöhön ympäristön, jossa jakaa sekä tietoa, dataa, että toiminnallisuuksia. Yhteisön pilveä hallinnoidaan tyypillisesti osana julkista pilveä, tai kolmannen osapuolen datakeskuksessa. (Moghaddam ym., 2015.)

Yhteisön pilven tunnuspiirteitä, hyötyjä ja haasteita organisaation näkökulmasta on kuvattu taulukossa 3.

TAULUKKO 3 Yhteisön pilven tunnuspiirteet sekä niiden hyödyt ja haasteet organisaation näkökulmasta (Marinos & Briscoe, 2009 ja Bokhari ym., 2016.)

Yhteisön pilven tunnuspiirre	**Hyödyt**	**Haasteet**
Jaettu pilviympäristö	Kustannustehokkuus, resurssien optimointi	Tietoturva
Datakeskuksen eksponentiaalinen kasvu		Hallittavuus, hiilijalanjälki

2.2.4 Hybridipilvi

Hybridipilvi on yhdistelmä vähintään kahdesta eri pilvestä. Hybridipilvessä eri pilviympäristöt (julkinen, yksityinen tai yhteisön pilvi) ovat itsenäisiä yksiköitä, mutta ovat yhteydessä toisiinsa mahdollistaen esimerkiksi sovellusten välisen datansiirron. Pilviympäristöjen välinen datansiirto mahdollistaa esimerkiksi resurssitasapainon säilyttämisen ja resurssien automaattisen siirron tarvittaessa ympäristöstä toiseen. Pilvipalveluja hyödyntävälle organisaatiolle hybridipilven hyötyjä ovat sen joustavuus ja saumattomuus sekä sen monipuolisuus yhdistäen niin yksityisen kuin julkisen pilven hyötyjä. (Savu, 2011 ja Mell & Grance, 2011.)

Hybridipilvessä eri pilviympäristöissä voi olla ylläpidollisesti eri tietoturvan ja tasoja jaetuille resursseille eri tietoa hyödyntävien organisaatioiden välillä.

Tästä syystä on tärkeää, että hybridipilvessä lisätään toimintoja julkisen ja yksityisen pilviympäristön yläpuolelle hallinnoimaan resurssivarantoa. Hybridipilven suurimpana hyötynä on tehokkuuden optimointi hyödyntäen resursseja niin julkisesta kuin yksityisestä pilvestä, jolloin palvelun resurssien skaalautuvuus nousee maksimitasolle. (Moghaddam ym., 2015.)

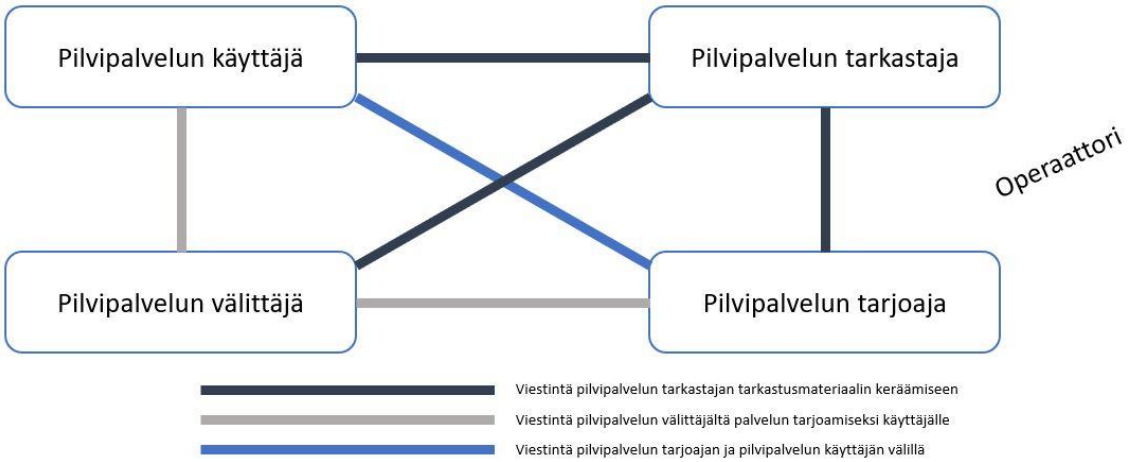
Hybridipilven tunnuspiirteitä, hyötyjä ja haasteita organisaation näkökulmasta on kuvattu taulukossa 4.

TAULUKKO 4 Hybridipilven tunnuspiirteet sekä niiden hyödyt ja haasteet organisaation näkökulmasta (Moghaddam ym., 2015 ja Bokhari ym., 2016.)

Hybridipilven tunnuspiirre	**Hyödyt**	**Haasteet**
Hyödynnetään niin organisaation omia kuin palvelun-tarjoajien resursseja	Resurssien optimointi	Datan liikkuvuus
Ylläpito jaettu eri organisaatioille	Tehokkaampi ylläpito	Tietoturva
Datakeskuksen eksponentiaalinen kasvu		Hallittavuus, hiilijalanjälki

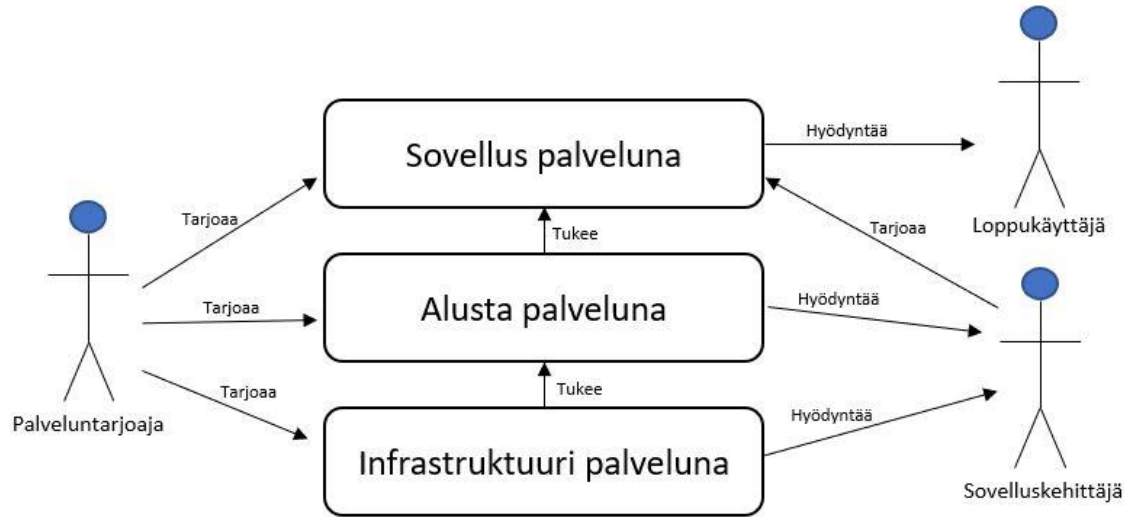
2.3 Pilvilaskentaa hyödyntävät pilvipalvelut

Pilvipalvelut ovat pilvilaskentaa hyödyntäviä, pilviteknologioita käyttäen luotuja palveluita. Pilvipalvelu voi olla esimerkiksi hotellinvarausjärjestelmä, joka sisältää useita sovelluksia ja sovellusrajapintoja. (Zheng ym., 2012.) Oleelliset toimijat pilvipalveluita tarkastellessa ovat pilvipalvelun käyttäjä, pilvipalvelun tarjoaja, pilvipalvelun tarkastaja, pilvipalvelun välittäjä sekä operaattori, jonka yhteyksiä pitkin pilvipalvelua hyödynnetään. Pilvipalvelun käyttäjä on käytännössä henkilö tai organisaatio, joka maksaa pilvipalvelusta ja hyödyntää sitä omassa tekemisessään. Pilvipalvelun tarjoaja on henkilö tai organisaatio, joka vastaa siitä, että pilvipalvelu on käytettävissä pilvipalvelun käyttäjille. Pilvipalvelun tarkastaja on osapuoli, joka tekee itsenäisen tarkastelun pilvipalveluun ja sen tietojärjestelmiin ja turvallisuuteen. Pilvipalvelun tarkastaja siis tarkastaa, onko pilvipalvelun tarjoaja käyttöönottanut pilviympäristön riittävän laadukkaalla ja tietoturvallisella tasolla, jotta sen käytöstä ei koidu haittaa pilvipalvelun käyttäjille. Pilvipalvelun välittäjä taas on taho, joka ei tuota tai ole teknisesti vastuussa pilvipalvelusta, mutta hallinnoi pilvipalvelun käyttöä ja sopimuksia pilvipalvelun tarjoajan ja pilvipalvelun käyttäjien välissä. Operaattorin roolina on tarjota mahdollisuus palvelun tarjoamiseen ja käyttöön (Bohn, Messina, Liu, Tong & Mao, 2011.) Pilvipalveluiden toimijoiden väliset suhteet ja viestintä on kuvattu kuviossa 2. (Hogan, Liu, Sokol & Tong, 2011.)



KUVIO 2 Pilviympäristön toimijat ja toimijoiden väliset suhteet (mukaelma Hoganin, Liun, Sokolin ja Tongin (2011) kuviosta.)

Teknisen toteutuksen näkökulmasta pilvipalvelussa voidaan tarkastella Infrastruktuurin palveluna, alustan palveluna sekä sovelluksen palveluna tarjoamista ja hyödyntämistä palveluntarjoajan, kehittäjän ja loppukäyttäjän näkökulmasta. Infrastruktuuri palveluna tarjotaan palveluntarjoajalta kehittäjälle, joka tarjoaa (alustan ja) sovelluksen loppukäyttäjälle, jota loppukäyttäjä hyödyntää. Alusta palveluna tarjotaan palveluntarjoajalta, ja sitä tukee (myös palveluntarjoajan tarjoama) infrastruktuuri palveluna. Sovelluskehittäjä hyödyntää alustaa, ja tarjoaa sovelluksen loppukäyttäjän käyttöön. Sovellus palveluna taas tarjotaan suoraan palveluntarjoajalta loppukäyttäjän käyttöön. Tämä prosessi on kuvattu kuviossa 3. (Marinos & Briscoe, 2009.)



KUVIO 3 Pilvipalveluiden sovelluskehityksen ja käytön roolit palvelumallien näkökulmasta. (mukaelma Marinosin ja Briscoen (2009) kuviosta)

Seuraavaksi käsitellään pilvipalveluita ja niiden palvelumalleja, jotka ovat sovellus palveluna (software as a service), alusta palveluna (platform as a service), sekä infrastruktuuri palveluna (infrastructure as a service). (Mell & Grance, 2011.)

2.3.1 Sovellus palveluna

Sovellus palveluna on palvelu, jossa sovellustoimittaja tarjoaa asiakkaan käyttöön pilviympäristössä sijaitsevan sovelluksen. Sovelluksia voidaan tyypillisesti käyttää useilla eri laitteilla webin tai sovelluskäyttöliittymän välityksellä. Sovellus palveluna mahdollistaa käyttäjien/käyttäjäorganisaatioiden sovelluksen käytön ilman vaatimuksia esimerkiksi sovellukseen liittyvän pilviympäristön, verkon tai tallennustilan huolehtimisesta, sillä sovellustoimittaja tarjoaa sovelluksen ja siihen liittyvän ympäristön valmiina palveluna. Sovellus palveluna on siis käytännössä sovellus, jota vuokrataan palveluntarjoajalta. Sovelluksen palveluna keskeisenä hyötynä pilvipalveluja hyödyntävän yrityksen kannalta on tyypillisesti se, että sen käytön kustannukset ovat vähäisempiä, kuin esimerkiksi kokonaan uuden järjestelmän luonti. Palvelu on myös joustava eikä vaadi suuria investointeja sovelluskehitykseen tai omien palvelinlaitteiden hankintaan. Sovellus palveluna on myös käytännössä rajattomasti skaalautuva palvelu, joten se tukee myös yrityksen resurssitarpeiden muutosta ja kasvua. Esimerkiksi Microsoftin 365 -sovellukset ovat sovelluksia, jotka tarjotaan asiakkaille palveluna. (Savu, 2011 ja Mell & Grance, 2011.)

Sovellus palveluna on pilvipalveluiden palvelumalleista niitä hyödyntävän organisaation näkökulmasta monessa suhteessa vaivattomin vaihtoehto, sillä sovellus palveluna pitää tyypillisesti sisällään myös infrastruktuurin, eli palvelinympäristön, ja alustan, jolla sovellus pyörii. Organisaatio saa siis valmiina pakettina käyttöönsä niin sovelluksen, jota organisaatio hyödyntää liiketoiminnassaan, kuin vaadittavat palvelinkapasiteetit ja infrastruktuurin. Sovellus palveluna -palvelumalli sisältää kuitenkin myös haasteita sitä hyödyntävälle organisaatiolle. (Tsai, Bai & Huang, 2014.)

2.3.2 Alusta palveluna

Alusta palveluna on palvelu, jossa alustatoimittaja tarjoaa asiakkaalle infrastruktuurin ja alustan, jolla asiakas voi kehittää omia sovelluksiaan. Alusta palveluna -palvelussa asiakas ei hallinnoi pilviympäristö ja -infrastruktuuria, mutta hallitsee sovellusta ja sen testausta sekä kehitystä. Alusta palveluna -palvelun keskeisenä hyötynä on sen joustavuus ja ostettu alusta, jolla sovelluskehittäjät pystyvät kehittämään ja testaamaan joustavasti sovelluksia. Kun alusta on ostettu, myös sovelluskehityksen kustannukset ovat pienempiä. Esimerkiksi Microsoft Azure on alusta, joka tarjotaan organisaatioille palveluna. (Savu, 2011. & Mell & Grance, 2011.)

2.3.3 Infrastruktuuri palveluna

Infrastruktuuri palveluna on palvelu, jossa infrastruktuurin toimittaja tarjoaa asiakkaalle kyvykkyydet prosessointiin, tallennukseen ja verkkoinfrastruktuuriin, ja tarjoaa asiakkaalle pilvilaskentaresurssit, joka mahdollistaa asiakkaalla ympäristön, jossa kehittää sovelluksia ja palveluita. Asiakas on tässä palvelumallissa

vastuussa käyttöjärjestelmistä ja sovelluksista, mutta infrastruktuurista ja esimerkiksi verkkokomponenteista vastaa infrastruktuurin toimittaja. Infrastruktuuri palveluna -palvelun keskeisimpänä hyötynä on sen joustavuus, se tukee niin julkista-, yksityistä- kuin hybridipilveä. Infrastruktuuria palveluna hyödyntävä asiakas siirtää myös pilvi-infrastruktuuriin liittyvän riskin itseltään pilvipalvelun tarjoajalle. Infrastruktuuri palveluna vähentää myös yrityksen oman palvelinympäristön tarvetta. (Savu, 2011. & Mell & Grance, 2011.)

3 TIETOTURVA JA PILVIPALVELUIDEN TURVALLISUUS

Pilvipalveluihin ja niiden käyttöön liittyy aina oleellisena asiana tietoturva. Tämän luvun ensimmäisessä alaluvussa määritellään käsitteenä tietoturva sekä esitellään sen kolmea osa-aluetta, tiedon luottamuksellisuutta, oikeellisuutta ja saatavuutta. Toisessa alaluvussa käsitellään tietoturvaa käyttäjän toimien näkökulmasta. Kolmannessa alaluvussa määritellään pilvipalveluiden turvallisuus.

3.1 Tietoturva

Tietoturva määritellään kansainvälisen ISO/IE 27002 -standardin mukaisesti tiedon luottamuksellisuuden, oikeellisuuden ja saatavuuden turvaamiseksi sekä varmistamiseksi. Turvattava tieto voi olla monessa eri muodossa, esimerkiksi paperilla, paikallisina tiedostoina tai jaetulla palvelimella. Tietoturva on siis tiedon ja sen kriittisten osien, esimerkiksi järjestelmien ja tiedonsiirron, turvaamista. Tietoa voidaan turvata esimerkiksi tietoturvahyökkäyksiä vastaan, mutta oleellisena osana on myös henkilöitävän tiedon suojaus yrityksissä dataa käsitellessä. Henkilötiedon kanssa on erittäin tärkeää rajata tietoon pääsy vain työn kannalta oleellisille henkilöille, jotta voidaan maksimoida henkilötietojen käsittelyn tietoturvallisuus. (Von Solms & Van Niekerk, 2013.)

Organisaatioissa tietoturvan tarkoituksena on suojata tietoa esimerkiksi luvattomalta pääsyltä, käytöltä tai muokkaamiselta. Pilviympäristössä on tällöin tärkeää varmistua siitä, että luvaton pääsy johtaa tahallisesti tai vahingossa tiedon luottamuksellisuuden, oikeellisuuden tai saatavuuden rikkomiseen. (Tchernykh ym., 2019.)

Seuraavaksi käsitellään tarkemmin tietoturvan osa-alueita, eli tiedon luottamuksellisuutta, oikeellisuutta ja saatavuutta sekä niiden varmistamista.

3.1.1 Tiedon luottamuksellisuus

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tiettyyn tietoon ei pääse käsiksi kukaan muu kuin ne henkilöt tai käyttäjät, joilla tietoon kuuluu olla pääsy. Tietoa tulee siis suojata luvattomalta pääsyltä, jotta sen luottamuksellisuus säilyy. Nykyään tiedon luottamuksellisuuden varmistaminen on haasteellista niin organisaatioille kuin käyttäjillekin. Tämä johtuu siitä, että eri pilvipalveluita käytettäessä palvelulle luovutettavat tiedot siirtyvät usein myös muiden organisaatioiden, kolmansien osapuolien, käytettäväksi. Tällöin, vaikka käytettävän palvelun tarjoaja sitoutuisi tiedon luottamuksellisuuden varmistamiseen estämällä luvattoman pääsyn, voi olla haastavaa varmistaa myös kolmansien osapuolten tiedonkäsittely tiedon luottamuksellisuuden säilyttämiseksi. Kolmansien osapuolten

kautta tieto voi myös levitä yhä pidemmälle. (Chowdhury, Pishva & Nishantha, 2010.)

3.1.2 Tiedon oikeellisuus

Tiedon oikeellisuudella tarkoitetaan sen yhdenmukaisuuden ja tarkkuuden varmistamista. Tiedon oikeellisuuteen liittyen on myös tärkeää varmistua siitä, että vain tietoon oikeutetut henkilöt pääsevät siihen käsiksi, jotta tietoa ei päästä muokkaamaan luvatonta pääsyä hyödyntäen. (Tchernykh ym., 2019.)

3.1.3 Tiedon saatavuus

Tiedon saatavuudella tarkoitetaan sitä, että esimerkiksi pilvipalvelu, jonka kautta oikeutetulla käyttäjällä on pääsy tietoon, on käyttäjän saatavilla ilman suunnittelemattomia, esimerkiksi palvelun huoltokatkoista johtuvia keskeytyksiä. Tämä vaatii palveluntarjoajalta panostamista niin palvelun tekniseen katkottomuuten, kuin myös eri huoltotöiden ja järjestelmäpäivitysten ajoittamisen suhteen. (Tchernykh ym., 2019.)

3.2 Tietoturva käyttäjän ja organisaation näkökulmasta

Bulgurcun ym. (2010) mukaan tietoturvaan liittyy käyttäjän näkökulmasta vahvasti käyttäjän asenne ja halu noudattaa organisaation tietoturvakäytänteitä. Käyttäjän, tai organisaation tapauksessa työntekijän, asenne tietoturvaan ja tietoturvakäytänteisiin on riippuvainen monesta asiasta. Oleellisimpina työntekijän asenteisiin vaikuttavina tekijöinä Bulgurcu ym. (2010) listaavat niin tietoturvakäytänteisiin myöntymisen kuin niiden kieltämisen hyödyt ja ”kustannukset” käyttäjän näkökulmasta. On siis oleellista, miten käyttäjä kokee tietoturvakäytänteiden noudattamisen kokonaisvaikutukset ja -seuraukset käyttäjään itseensä. Käyttäjä voi kokea tietoturvakäytänteiden noudattamisen itseään hyödyttävänä esimerkiksi turvallisuuden lisääntymisen ja palkintojen kautta, toisaalta noudattamisen ”kustannuksina” voidaan nähdä esimerkiksi työtehtävien suorittamisen vaikeutuminen. Oleellinen asia, joka vaikuttaa käyttäjän asenteisiin tietoturvakäytänteitä kohtaan, on myös käyttäjän tietoturvatietoisuus (Information security awareness), josta lisää seuraavaksi. (Bulgurcu ym., 2010.)

3.2.1 Tietoturvatietoisuus yksilön näkökulmasta

Tietoturvan käsittelyyn liittyy lähes aina verkkoyhteyksiä ja päätelaitteita. Verkon välityksellä tietoturvaiskut ovat mahdollisia, ja ne tapahtuvat tyypillisesti hyökkäyksen kohteen päätelaitteeseen. Mahdollisia tietoturvahyökkäyksiä on toteutustavaltaan todella erilaisia, yksinkertaisimmillaan sähköpostilla

automaattisesti suurelle joukolle lähetettävät kalasteluviestit. Tietoturvahyökkäykset voivat olla siis luonteeltaan yksinkertaisia sähköpostiviestillä toteutettuja, tai teknisesti vaativampia päätelaitteen käyttäjälle näkymättömiä viruksia. (Huang, Rau & Salvendy, 2010.)

Näitä hyökkäyksiä varten yritysten on panostettava tietoturvaan entistä enemmän eri toimilla, jotka vaativat järjestelmien ja sovellusten teknistä konfigurointia ja suojaamista, henkilökunnan ja käyttäjien kouluttamista, sekä riskien tiedostamista ja hallintaa. Yhä keskeisempänä aiheena tietoturvaan liittyvässä tutkimuksessa onkin nostettu nimenomaan käyttäjän rooli. Työntekijöiden tietoturvatietoisuus on elintärkeää tehokkaan tietoturvajohtamisen näkökulmasta. Tietoturvatietoisuus määritellään Bulgurcun ym. (2010) mukaan seuraavasti :

> ...työntekijän yleinen tietämys tietoturvasta ja hänen tietonsa tietoturvakäytänteistä hänen organisaatiossaan. Yleinen tietämys tietoturvasta ja tietoturvakäytänteiden tiedostaminen ovat tietoturvatietoisuuden oleellisimmat näkökulmat.

Tietoturvatietoisuus koostuu siis käytännössä **yleisestä tietoturvan tietämyksestä**, sekä **tietoturvakäytänteiden tiedostamisesta**. Näistä yleinen tietoturvan tietämys koostuu työntekijän perustiedoista ja ymmärryksestä tietoturvaa ja tietoturvauhkia kohtaan. Tietoturvakäytänteiden tiedostaminen taas koostuu työntekijän tiedosta ja ymmärryksestä sitä kohtaan, mitä organisaatio, jossa hän työskentelee, vaatii työntekijältänsä tietoturvan osalta. Käytännössä siis työntekijän tulee tuntea organisaation tietoturvakäytänteet ja mitä häneltä vaaditaan niiden vaatimusten täyttämiseksi. Keskeisinä eroina tietoturvan yleisen tietämyksen ja tietoturvakäytänteiden tiedostamisen välillä ovat käyttäjän ymmärrykseen ja yleiseen tietämykseen liittyvät asiat, jotka rinnastuvat tietoturvan yleiseen tietämykseen, ja käyttäjän tiedostamat, organisaation määrittämät vaatimukset, jotka rinnastuvat tietoturvakäytänteiden tiedostamiseen. (Bulgurcu ym., 2010.)

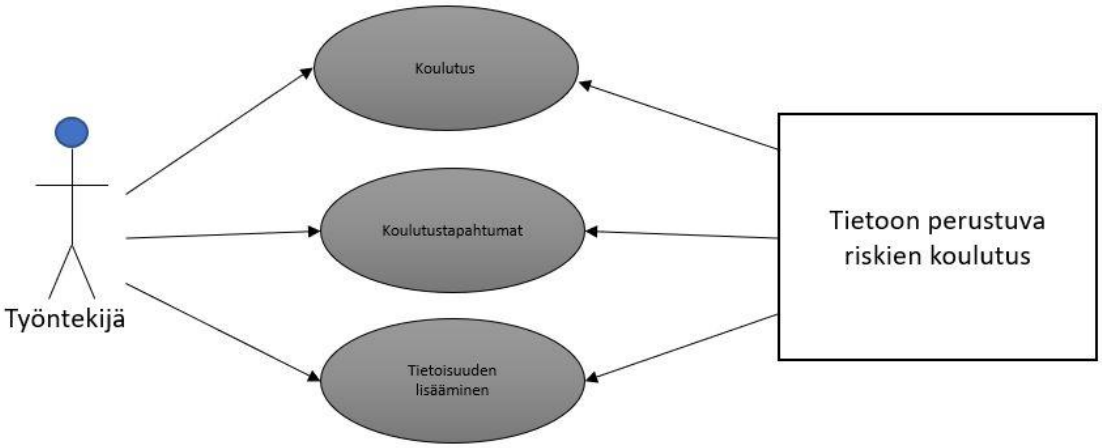
Tietoturvatietoisuuden oleellisia näkökulmia **tietoturvan yleinen tietämys** sekä **tietoturvakäytänteiden tiedostaminen** esitellään tarkemmin taulukossa 5.

TAULUKKO 5 Tietoturvatietoisuuden näkökulmat ja niiden tunnuspiirteet (Bulgurcu ym., 2010.)

Tietoturvan yleisen tietämyksen tunnuspiirteet	**Tietoturvakäytänteiden tiedostamisen tunnuspiirteet**
Tieto siitä, mitä tietoturva on ja mitä se pitää sisällään	Organisaation tietoturvakäytänteiden tuntemus
Tietoturvauhkien tunnistaminen	Tieto siitä, että organisaatio vaatii salasanan vaihtamista säännöllisesti.
Ymmärrys siitä, että salasana tulee vaihtaa säännöllisesti	

Alhawarin, Karadhehin, Taletin ja Mansourin (2012) mukaan työntekijän kouluttautuminen tietoturvariskeihin tulee tapahtua tietoon perustuen. Tällöin riskien koulutus koostuu itse koulutuksesta, jota työntekijä tekee itsenäisesti, koulutustapahtumista sekä yleisestä tietoisuuden lisäämisestä (ks. kuvio 4). Kaikki tietoon

perustuvan riskien koulutuksen kategoriat tulee säilyttää tehokkaassa työntekijän kouluttamisessa tietoturvatietoisuuden lisäämiseksi. (Alhawari ym., 2012.)



KUVIO 4 Tietoon perustuvan riskien koulutuksen prosessi (mukaelma Alhawarin ym. (2012) kuviosta.)

3.2.2 Organisaation tietoturvakäytänteet

Organisaatioiden toimintaympäristö muuttuu enenevissä määrin suuntaan, jossa tiedolla on suuri arvo ja toisaalta riskit tietoon liittyen kasvavat. Tämä vaatii organisaatioilta toimia arvokkaan tiedon suojaamiseksi. Ratkaisuksi tähän on suositeltu organisaatiokohtaisten tietoturvakäytänteiden luomista. Myös esimerkiksi tietoturvastandardi *ISO27001* kuvaa tietoturvakäytänteet pakolliseksi organisaation tietoturvanhallinnan näkökulmasta. Tietoturvakäytänteellä tarkoitetaan pääsääntöisesti dokumenttia tai dokumentteja, jotka määrittävät, miten ihmisten pitäisi toimia tai organisaation tietoturvatavoitteiden saavuttamiseksi. Organisaation tietoturvakäytänteitä voi olla eri tyyppejä. Tietoturvakäytänteen tyyppi voi olla esimerkiksi tekninen tai johtava käytänne. Tietoturvakäytänteet myös tyypillisesti sisältävät tai ainakin määrittävät organisaation käyttövaltuuksien hallintaan liittyviä käytänteitä. (Paananen, Lapke & Siponen, 2019.)

Organisaation kannalta on erittäin tärkeää, että tietoturvakäytänteet on luotu huolellisesti. Toisaalta on myös tärkeää varmistua siitä, että työntekijät noudattavat tietoturvakäytänteitä parhaalla mahdollisella tavalla. Tietoturvakäytänteiden noudattamisesta varmistumiseen organisaatiolla voi olla monia vaihtoehtoja. Tyypillinen tapa on kuitenkin määritellä kontrolleja, jotka antavat viitekehyksen esimerkiksi prosessien suunnittelulle. Kun prosessit suoritetaan näitä kontrolleja noudattaen, lähtökohtaisesti myös tietoturvakäytänteitä noudatetaan. (Wall, Palvia & Lowry, 2013.)

Floweday ja Tuyikeze (2016) nostavat artikkelissaan esille nykyään oleellisena seikkana sen, että tietoturva ja tietoturvakäytänteet nähdään usein vastakkain informaatioteknologian päätarkoituksen organisaatiolle. Tyypillisesti

organisaatiot hankkivat ja hyödyntävät informaatioteknologiaa tehostaakseen liiketoimintaansa ja eri prosesseja. Tietoturvakäytänteiden huomioiminen saattaa heikentää prosessien maksimaalista tehokkuutta, mutta se on kuitenkin tärkeää, sillä nykyään organisaatioiden liiketoiminta tai muut prosessit voivat olla täysin riippuvaisia informaatioteknologiasta. Tällöin on myös organisaatiolle elintärkeää, että prosessit ovat tietoturvallisia ja tietoturvakäytänteitä noudatetaan. (Flowerday & Tuyikeze, 2016.)

Organisaatioiden on siis tärkeää huolehtia siitä, että tietoturvakäytänteet ovat olemassa ja niitä noudatetaan. Tyypillisesti organisaatioissa pidetäänkin hyvin huolta järjestelmien teknisestä tietoturvasta ja turvallisuuden mittaamisesta. Tärkeänä osana kriittistä tietoa käsittelevien järjestelmien kokonaisturvallisuutta tarkastellessa on kuitenkin huomioida ihmiskäyttäjän tuoma ihmisriski. Tämä käyttäjän aiheuttama riski on kaikista tehokkainta minimoida nimenomaan tehokkailla tietoturvakäytänteillä. (Al-Omari, El-Gayar & Deokar, 2012.)

3.3 Tietojärjestelmien tietoturva ja riskienhallinta

Pilvipalveluihin ja tietojärjestelmien tietoturvaan liittyy aina tietoturvariskejä. Tässä alaluvussa käsitellään tietojärjestelmien tietoturvaa riskilähtöisesti, sekä määritellään käsitteenä riskienhallinta ja esitellään riskienhallinnan eri näkökulmia organisaation tietoturvariskien minimoimiseen.

3.3.1 Tietojärjestelmien tietoturva ja riskit

Tietojärjestelmien tietoturva on nykyään avainasemassa organisaation liiketoiminnan kannalta. Tietovuodoilla ja organisaation haavoittuvuudella voi olla merkittäviä vaikutuksia niin organisaation kun sen palvelun käyttäjien näkökulmasta. Vaikutukset voivat olla suoria, esimerkiksi identiteettivarkauksia, tai epäsuoria, jotka vaikuttavat esimerkiksi organisaation työntekijöiden hyvinvointiin. Tietojärjestelmien tietoturvan asianmukainen varmistaminen on siis erittäin tärkeää organisaatioille. Tietojärjestelmien tietoturvan varmistamiseen on kehitetty erilaisia työskentelymalleja, esimerkiksi tarkistuslista -metodi ja looginen metodi. Näitä metodeja organisaatiot voivat hyödyntää luodakseen tietoturvallisen ja riskejä minimoivan tietojärjestelmäympäristön. (Siponen, 2005.)

Nykyään organisaatioita myös painostetaan ottamaan käyttöön tietojärjestelmien tietoturvaan liittyviä käytänteitä ja metodeja sekä noudattamaan niihin liittyviä parhaita käytänteitä, jotta arvokkaaseen tietoon liittyviä riskejä voidaan minimoida. Yleisesti seurattavia parhaita tietojärjestelmien tietoturvakäytänteitä sisältävät esimerkiksi ISO/IEC27001, NIST-SP800 ja PCI-DSS -standardit. Tietojärjestelmiin kohdistuvat tietoturvariskit lisääntyvät jatkuvasti, joka on johtanut organisaatioiden tarpeeseen käyttöönottaa käytänteitä ja standardeja nopealla tahdilla. (Niemimaa & Niemimaa, 2017.)

3.3.2 Riskienhallinta

Riskienhallinnalla pyritään arvioimaan ja minimoimaan riskejä ja niiden vaikutuksia. Riskejä tarkastellaan riskienhallinnassa tyypillisesti kahdesta eri näkökulmasta, jotka ovat riskien todennäköisyys ja vaikutukset. Riskienhallinnassa myös tyypillisesti määritetään riskikohtaisia toimenpiteitä, jotka minimoivat riskien toteutumista. (Tang & Musa, 2011.)

Riskienhallintaan on olemassa eri metodeja. Riskienhallinnan metodeja ovat esimerkiksi **tuloslähtöinen näkökulma**, jossa keskitytään lopputulokseen ennemmin kuin prosessiin, jolla se saavutetaan, sekä **liiketoimintalähtöinen näkökulma**. Tyypillisempi näistä on tuloslähtöinen näkökulma, joka tarjoaa esimerkiksi tietoturvajohtajalle kuusivaiheisen prosessin riskienhallintaan. Liiketoimintalähtöisessä näkökulmassa painotusta viedään taas pois teknologiasta kohti organisaation oleellisimpia liiketoiminnan prosesseja. (Siponen, 2005, heinäkuu.)

Riskienhallinnan rooli voidaan nähdä riskejä ennakoivan tekniikan lisäksi myös organisaation viestinnän välineenä. Tämä mahdollistaa riskienhallinnan tehokkaana työkaluna johdon päätöksenteon tueksi. Riskienhallinnalla voidaan yhdistää johdon ja tietoturvasta vastaavan henkilöstön näkemykset organisaation tietojärjestelmien asianmukaisesta tietoturvasta. Organisaation tietojärjestelmien turvallisuuden johtaminen nojautuu tyypillisesti alan parhaisiin käytänteisiin ja tietoturvastandardeihin. Ongelmana tässä voi olla se, että riskienhallinnassa käytettävät kontrollit, jotka pienentävät riskejä, ovat yleisiä eikä organisaation tarpeiden mukaan riittävällä tasolla räätälöityjä. Tyypillisesti eri standardeissa (esimerkiksi ISO/IEC27002) määritellyt kontrollit ja käytänteet ovat kuitenkin sovellettavia suurimmalle osalle organisaatioista. (Siponen, 2005, heinäkuu ja Niemimaa & Niemimaa, 2017.)

Riskienhallinnan perinteisimmän määritelmän mukaan riskille voidaan laskea riskikerroin sen suurimpien tekijöiden, eli todennäköisyyden ja vaikutuksen mukaan. Riskin todennäköisyyttä ja vaikutusta arvioimalla voidaan tunnistaa organisaation kannalta oleellisimmat riskit, joita huomioida riskienhallinnan prosessissa. Riskienhallinnan prosessin lopputuotoksena riskianalyysi antaa formaalin raportin esimerkiksi siitä, mitä haavoittuvuuksia organisaatiolla voi olla tietoturvan näkökulmasta. Tämän jälkeen riskejä voidaan alkaa käymään tarkemmin läpi ja riskikohtaisesti luoda kontrollit, joita noudattamalla ja joiden mukaan organisaation prosessit määrittämällä voidaan minimoida riskin toteutumisen todennäköisyys. Kuviossa 4 kuvattuna riskien riskikertoimien tekijät ja riskikertoimen muodostuminen. Mitä ylempänä riski on y-akselilla ja pidemmällä x-akselilla, sitä oleellisempi riski on organisaation kannalta. Näihin riskeihin organisaatioiden tulee keskittyä. On toisaalta myös tärkeää, että alemman todennäköisyyden ja vaikutuksen riskejä minimoidaan, jotta ne eivät nouse vaikuttavuudeltaan tai todennäköisyydeltään ylemmäs. Markowski ja Mannan (2008) tarjoavatkin riskitaulukolle kolme eri vaihtoehtoa, joissa vaihtelee epätodennäköisten ja vaikuttavuudeltaan vähäisten riskien etäisyys kuvion 4 (standardimalli) mukaisen riskijaottelun nollakohdasta. Tällöin organisaatiot voivat itse määritellä

kuinka arvioida erityyppiset riskit. (Baskerville, 1993 ja Markowski & Mannan, 2008.)

Kuviossa 5 esitellyt **todennäköisyyden, vaikuttavuuden ja riskien kategoriat** ovat seuraavat:

Todennäköisyyden kategoriat:

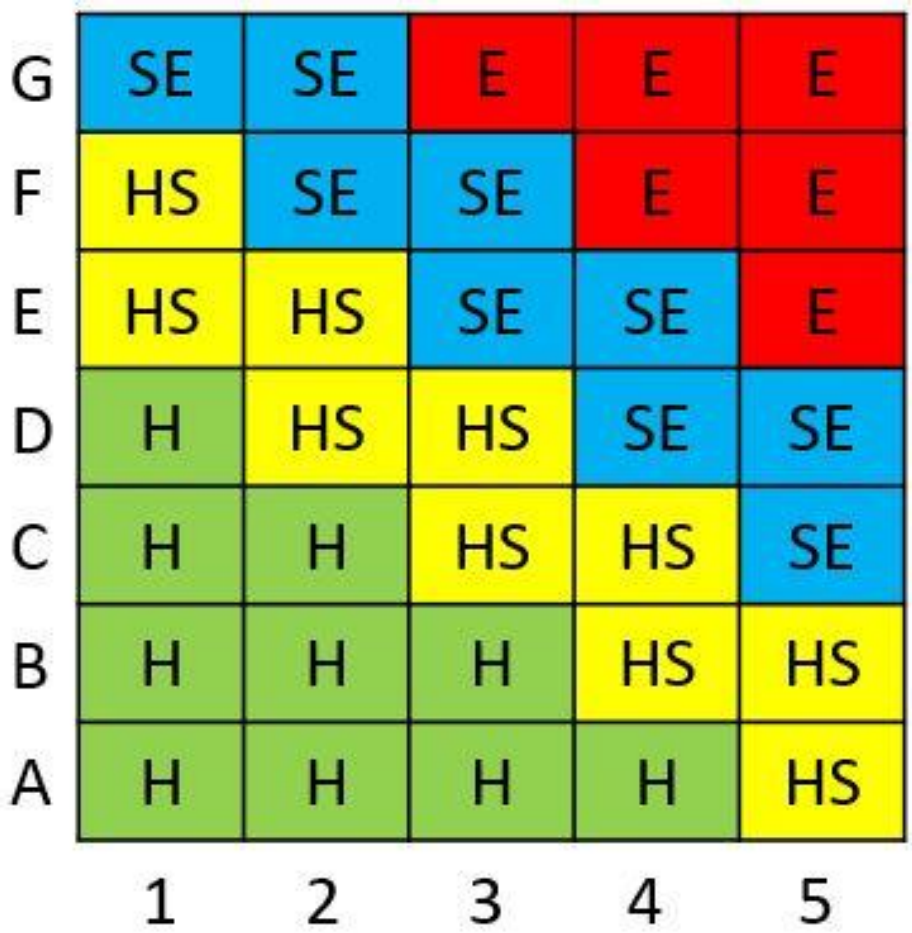
A: ei mahdollinen,
B: epätodennäköinen,
C: erittäin pieni todennäköisyys,
D: pieni todennäköisyys,
E: keskimääräinen todennäköisyys,
F: suuri todennäköisyys,
G: erittäin suuri todennäköisyys.

Vaikuttavuuden kategoriat:

1: ei vaikutusta,
2: vähäinen vaikutus,
3: keskimääräiset vaikutukset,
4: suuri vaikutus,
5: katastrofaalinen vaikutus.

Riskien kategoriat:

H: hyväksyttävä,
HS: hyväksyttävä-siedettävä,
SE: siedettävä-ei hyväksyttävä,
E: ei hyväksyttävä.



KUVIO 5 Riskienhallinnan riskianalyysi. (Mukaelma Markowskin ja Mannan'n (2008) kuviosta.)

4 PILVIPALVELUIDEN HALLINTA JA TIETOTURVA

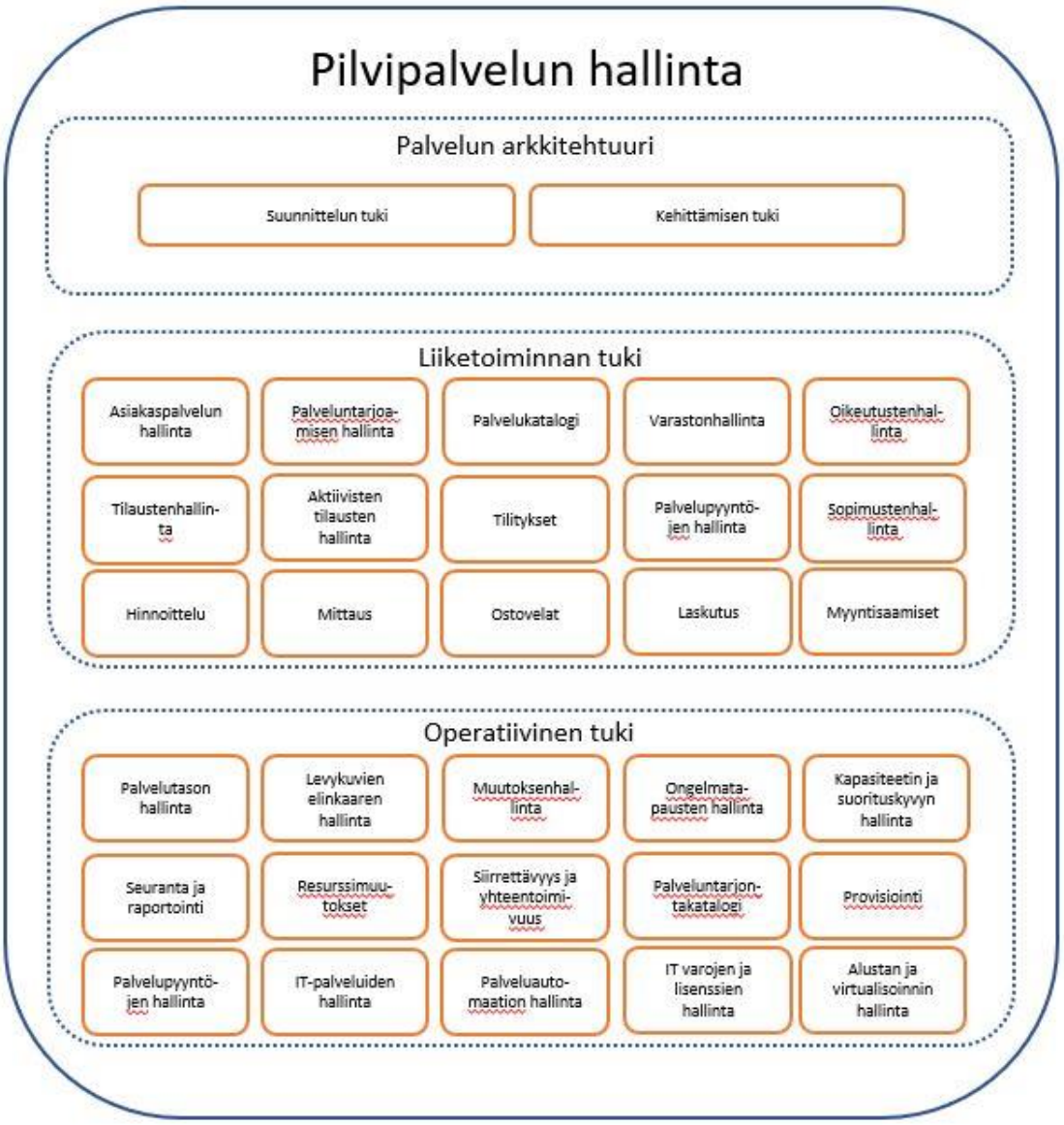
Organisaatiot ovat siirtymässä nopealla tahdilla pilviympäristöihin ja pilvipalveluiden hyödyntäjiksi. Pilvipalveluiden käyttöön liittyy paljon vaatimuksia ja organisaatiolla täytyy olla selvä suunnitelma siitä, miten niitä hallinnoidaan. Tässä luvussa käsitellään pilvipalveluiden hallintaa organisaatioissa, sekä miten tietoturvanäkökulmat tulisi ottaa huomioon pilvipalveluiden hallintaa suunnitellessa. Lopuksi käsitellään pilvipalveluiden riskejä palvelumallikohtaisesti.

4.1 Pilvipalveluiden hallinta – Palveluntarjoajan ja käyttäjäorganisaation vastuut

Amanatullahin ym. (2013) mukaan pilvipalveluiden hallintamallilla tarkoitetaan viitekehystä, jonka avulla pyritään ymmärtämään pilvipalveluihin liittyvät prosessit ja toimijat sekä heidän suhteensa. Pilvipalveluiden hallintamalleja hyödynnetään yleensä eteenkin pilviympäristöjen käyttöönotoissa. Pilvipalvelun hallintamalli sisältää useita komponentteja, yleensä ainakin palvelun kuluttajat, toimittaja(t), kehittäjät, sekä arkkitehtuurin ja kuvauksen hallinnasta. Pilvipalveluita hyödyntäessä tai tarjotessa niiden hallinta on Amanatullahin ym. (2013) mukaan välttämätöntä. Pilvipalveluiden hallinta sisältää käytänteiden, prosessien ja vaatimusten tarkkaa määrittämistä ja niiden sisällyttämistä pilvilaskentaympäristöihin. Tehokkaimmin pilvipalveluiden hallinta tapahtuu, kun siihen sisällytetään niin tekninen kuin liiketoimintalähtöinen näkökulma sekä organisaation prosessit em. liittyen. Näiden tehokas hallinta mahdollistaa luotettavan ja laadukkaan palvelun sekä varman suorituskyvyn. Laadulla ja standardien mukaisesti hallinnoitu palvelu takaa myös tietoturvan sitä hyödyntäville osapuolille. Pilvipalveluiden hallinta vaatii organisaatiolta prosesseja, käytänteiden noudattamista sekä teknologian hyödyntämistä. Käytänteet määrittävät esimerkiksi, miten palvelua tulisi käyttää ja kuka tai ketkä ovat valtuutettuja tiettyjen prosessinen suorittamiseen ja toimeenpanoon. (Amanatullah ym., 2013.)

4.1.1 Palveluntarjoajan näkökulma

Yksittäisen pilvipalvelun hallinta voidaan jakaa Amanatullahin ym. (2013) mukaan kolmeen kategoriaan, jotka ovat palvelun arkkitehtuuri, liiketoiminnan tuki sekä operatiivinen tuki (ks. kuvio 5). Pilvipalveluiden hallinta sisältää prosesseja ja aktiviteetteja, jotka pilvipalvelumallista ja sen vastuujaosta riippuen ovat joko pilvipalveluntarjoajan tai käyttäjäorganisaation vastuulla. (Amanatullah ym., 2013.)



KUVIO 6 Pilvipalvelun hallinta ja siihen liittyvät prosessit kategorioittain (mukaelma Amanatullahin ym. (2013) kuviosta.)

Pilvipalvelun arkkitehtuuri sisältää kaksi komponenttia, arkkitehtuurin suunnittelun ja arkkitehtuurin kehityksen tai suorittamisen. Pilvipalvelun arkkitehtuuri tukee pilvipalvelua hyödyntävän organisaation IT-projekteja sekä liiketoiminnan prosesseja. Laadukas arkkitehtuuri mahdollistaa pitkälläkin aikavälillä integraatiot eri järjestelmiin, palveluihin ja sovelluksiin. Tämä tukee organisaation liiketoimintatarpeita ja tulevaisuuden muutoksia. (Amanatullah, ym., 2013.)

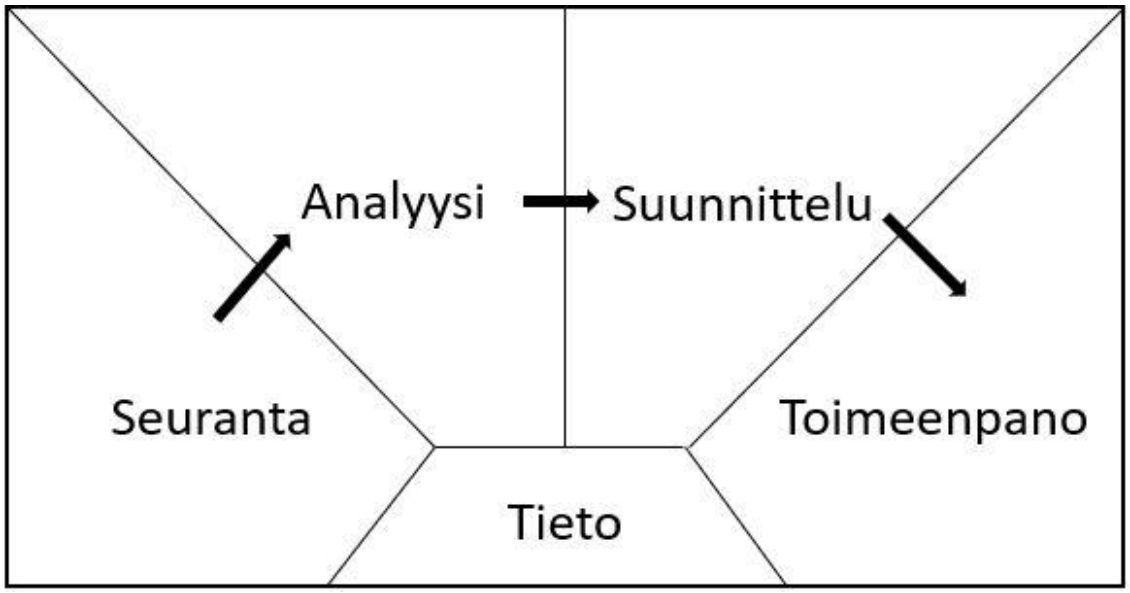
Liiketoiminnan tuki tarkoittaa pilvipalvelun kanssakäymistä eri liiketoiminnan palveluiden ja palvelunkäyttäjien kesken. Liiketoiminnan tukitoimintoihin kuuluu esimerkiksi käyttäjäorganisaation talouteen liittyvät laskutus- ja ostovelkatuki, sekä hinnoittelu- ja varastonhallintapalvelut. (Amanatullah, ym., 2013.)

Operatiivinen tuki sisältää pilvipalveluntarjoajan ja pilvipalvelun ostajaorganisaation välisen palvelutason seurannan sekä siihen liittyvän hallinnan. Palvelutason tukeen kuuluu esimerkiksi pilvipalvelun tekninen tuki ja palvelun suorituskyvyn seuraaminen ja varmistaminen. Operatiivinen tuki tapahtuu tyypillisesti pilvipalveluntarjoajan puolesta, ja kohdistuu palvelun käyttäjiin; joko ostajaorganisaatioon tai pilvipalvelua hyödyntävän organisaation kuluttaja-asiakkaisiin. (Amanatullah, ym., 2013.)

4.1.2 Käyttäjäorganisaation näkökulma

Tässä alaluvussa käsitellään pilviympäristön hallintaa pilvipalveluita hyödyntävän organisaation näkökulmasta. Organisaatioilla on tyypillisesti käytössä monia eri pilvipalveluita eri palveluntarjoajilta. Nämä eri palvelut muodostavat organisaation pilviympäristön ja asettavat organisaatiolle vaatimuksia pilviympäristön hallintaan liittyen.

Yksi esimerkki **Pilviympäristön ja sen järjestelmien hallintaan** kehitetyistä hallintamalleista on MAPE-K -luuppi (ks. kuvio 7), joka tulee sanoista seuranta (engl. monitoring), analyysi (engl. analysis), suunnittelu (engl. planning) ja toimeenpano (engl. execution). Näiden prosessien lisäksi K tulee sanasta tieto (engl. knowledge), joka ohjaa luupissa kaikkia prosesseja. Tätä palvelunhallinnan luuppia seuraamalla organisaation pilviympäristö pysyy tehokkaassa hallinnassa. (Innocent, 2012.) MAPE-K -luupin mukainen pilviympäristön hallinta perustuu jatkuvaan tietoon perustuvaan seurantaan. Seurannasta saatua dataa analysoidaan, jonka jälkeen analyysista johdetun tiedon perusteella tehdään esimerkiksi palvelun implementoinnin suunnitelma. Tämän jälkeen palvelu toimeenpannaan tai implementoidaan. Kaikissa prosesseissa hyödynnetään aktiivisesti saatavilla olevaa tietoa. (Rutten, Marchand & Simon, 2017.)



KUVIO 7 MAPE-K -luuppi (mukaelma Ruttenin ym. (2017) kuviosta.)

Moni-pilviympäristöllä pyritään automatisoimaan palveluidenhallintaa ja tarjoamaan kaikki palvelun samaa reittiä pitkin. Tällä pyritään saavuttamaan neljä tavoitetta, jotka ovat:

1. *Palvelun riittävä abstraktion taso*
2. *Automaattinen skaalautuvuus*
3. *Älykäs skaalautuvuus*
4. *Palveluntoimittajaan lukittautumisen välttäminen*

Moni-pilviympäristön ominaisuudet tuovat myös erilaisia riskejä ja tietoturvahaasteita, kuin perinteiset pilviympäristöt. Näitä riskejä on kuvattu tarkemmin taulukossa 7. (Innocent, 2012.)

4.2 Pilvipalveluiden hallinta ja tietoturva

Pilvipalveluiden käyttöönoton yhteydessä on tärkeää huomioida palvelinympäristön, pilvi-infrastruktuurin sekä itse pilvipalvelun tietoturva. Pilvilaskennan ja pilvipalveluiden tietoturvasta käytetään nimitystä pilviturvallisuus (cloud security).

Pilvipalveluiden eri palvelumalleihin liittyy niitä hyödyntävän organisaation näkökulmasta erilaisia riskejä. Yksi organisaation pilviympäristön kannalta oleellinen huomioitava asia on tiedon tai **datan turvallisuus**. Datan turvallisuutta tulee suojata erityisen tarkasti pilviympäristössä, sillä haavoittuvuudet esimerkiksi palveluntarjoajan pilvilaskentaresursseissa vaikuttavat normaalisti myös liiketoiminnan asiakkaiden toimintaan. On siksi oleellista varmistaa asianmukainen pilvipalvelun hallinnointi sekä datan turvallinen käsittely. Datan turvallisuus voidaan määritellä Padillan, Miltonin ja Johnsonin (2015) mukaan seuraavasti:

> …varmistaa pilvilaskennan palvelimien provisioinnin parhaiden käytänteiden noudattaminen internet-selaimen turvallisuudessa, käyttäen vahvaa salausproseduuria ja harkiten tunnistautumisvaltuuksia.

Turvallisuusvaatimusten täyttäminen on oleellista useille asiakkaille, esimerkiksi organisaatioiden päätöksentekijöille, sillä pilvipalvelut tukevat asiakasorganisaatioissa tavoitteiden saavuttamista. Datan turvallisuudesta huolenpitäminen on oleellista pilvipalveluntarjoajan näkökulmasta myös asiakashankinnan ja asiakassuhteiden ylläpitämisessä. Datan turvallisuus on usein avainasemassa, kun organisaatio päättää esimerkiksi palveluiden jatkosta nykyisen palveluntarjoajan kanssa tai uusien palveluiden ostamisesta. Koska pilvipalveluiden suhteen on asiakkaalle usein epävarmaa se, missä heidän datansa fyysisesti sijaitsee, on palveluntarjoajan tärkeää pitää huolta datan turvallisuudesta. Tämä luo palveluntarjoajalle esimerkiksi vaatimuksen palvelinympäristön laadukkaasta hallinnoimisesta. Palveluntarjoajan on myös huolehdittava esimerkiksi datan

varmuuskopioinneista sekä datan palautustoimenpiteistä. On palveluntarjoajien palvelinympäristön hallinnoimisesta kiinni, miten pilvipalvelussa käytettävä data säilytetään ja suojataan. Jos palvelinympäristössä tapahtuu vahinkoa, on olemassa aina riski datan lopullisesta häviämisestä. (Padilla, Milton & Johnson, 2015.)

Seuraavaksi käsitellään pilviturvallisuutta pilvipalveluiden suunnittelun, käyttöönoton ja vaatimusten näkökulmasta.

4.2.1 Suunnittelu

Pilvipalvelun käyttöönottoa suunnitellessa on eri huomioitavia näkökulmia. Tyypillisesti suunnitteluvaiheessa suositellaan tietoturvan näkökulmasta proaktiivista lähestymistapaa, joka vahvistaa organisaation kykyä seurata ja reagoida erilaisiin pilvipalveluihin ja niiden tietoturvaan liittyviin riskeihin. Organisaation koosta ja resursseista riippuen pilviturvallisuudessa suositellaan noudattamaan vähintään minimissään toimivan pilviturvallisuuden periaatetta, jolloin perusasiat tulisi olla turvattuna. Pilvipalvelun käyttöönoton suunnitteluvaiheessa organisaation tulee muodostaa tietoturvakäytänteet, standardit sekä määrittää prosessit ja roolit tietoturvallisuuden eri osa-alueille. Tärkeänä nähdään usein myös olemassaolevien kompetenssien ja kyvykkyyksien huomioimista. (Almorsy, Grundy & Ibrahim, 2011.)

4.2.2 Käyttöönotto

Pilvipalvelun käyttöönotossa organisaation tulee panostaa tietoturvan ja pilviturvallisuuden näkökulmasta moniin asioihin, sisältäen luonnollisesti tiedon luottamuksellisuuden, oikeellisuuden ja saatavuuden. Muita asioita, joihin tulee keskittyä, on mm. prosessien läpinäkyvyys ja oikeiden mittarien asettaminen. Tärkeää on myös huolehtia siitä, että data on mahdollisimman reaaliaikaista.

Pilvipalvelun käyttöönoton vaiheet ovat tyypillisesti taktinen vaihe, perustamisvaihe ja strateginen vaihe. Näissä vaiheissa on eri toimenpiteitä, jotka tulee huomioida ja varmistaa tietoturvan näkökulmasta. Jos pilvipalvelua otetaan organisaation käyttöön, tulee myös huomioida käyttäjien näkökulma. Tähän liittyy esimerkiksi käyttäjien käyttöliittymän huomiointi sekä se, millä laitteilla palvelua käytetään. On myös tärkeää ohjeistaa käyttäjät hyvin palvelun käyttöön. Pilviturvallisuuden näkökulmasta on myös tärkeää integroida organisaation tietoturvan hallinta kattamaan koko palvelunhallinnan ja -kehityksen mukaan lukien kaikki prosessit, mitä järjestelmän käyttö sisältää. Käyttöönoton jälkeen jatkokehityksen mahdollistaa usein tehokas palautekysely ja aktiivinen palautekeskustelu pilvipalvelun kehittäjien ja käyttäjien välillä. On myös tärkeää, että palaute kuuluu riittävän korkealle organisaation hierarkiassa. Palautteen kerääminen ja siihen reagointi on avainasemassa koko pilvipalvelun suunnittelu-, käyttöönotto- ja seurantavaiheessa. (Rebollo, Mellado, Fernández-Medina & Mouratidis, 2015.)

4.2.3 Vaatimukset

Pilvipalvelut ja niiden käyttöönotto sisältävät tietoturvavaatimuksia, jotka organisaation suositellaan täyttävän. Näihin vaatimuksiin kuuluu keskeisenä tekijänä tietoturvakäytänteiden dokumentointi, vaadittavat sovellusrajapinnat sekä integroitu pilvipalvelunseuranta. On myös tärkeää pitää järjestelmien turvallisuus johdonmukaisena, esimerkiksi toimialan vallitsevien standardien mukaan. Tärkeää on tämän lisäksi turvata esimerkiksi jaettujen laitteiden suojaus ja tietoturvallisuus. Viimeiseksi suositellaan myös käyttäjän virheiden minimointi esimerkiksi digitaalisilla jäljillä, jota käyttäjä jättää käyttäessään pilvipalvelua. Tällöin, esimerkiksi vahingon sattuessa käyttäjän jälkiä voidaan seurata ja selvittää kuka muutoksia on tehnyt. Käyttäjän virheitä voidaan minimoida myös mahdollisimman automaattisilla datankäsittelyprosesseilla sekä tehokkaalla järjestelmien tapahtumanhallinnalla ja säännöllisellä skannaamisella, jonka tarkoituksena on selvittää onko palvelussa päällä esimerkiksi virhetiloja tai muita ongelmia. (Almorsy ym., 2011.)

ISO 7498-2 -standardin mukaan pilvipalveluita käyttöönottaessa tietoturva tulisi ottaa huomioon useassa teemassa. Tietoturva tulee ottaa huomion, jotta pilvipalvelusta saadaan tehokas, mutta myös turvallinen ratkaisu sitä hyödyntävän organisaation tarpeisiin. Pilvipalveluiden suunnitteluun ja käyttöönottoon liittyy siis paljon vaatimuksia tietoturvan näkökulmasta. Vaatimuksia ovat ainakin tunnistautuminen ja todentaminen, valtuuttaminen, tiedon luotettavuus, tiedon oikeellisuus, hyväksyntä ja tiedon saatavuus. Nämä vaatimukset on kuvattu tarkemmin taulukossa 6. (Ramgovind ym., 2010.)

TAULUKKO 6 Pilvipalveluiden hallinnan vaatimukset organisaatiolle tietoturvan näkökulmasta. (Ramgovind ym., 2010 ja Rebollo ym., 2015)

Vaatimus	**Vaatimuksen kuvaus**
Tunnistautuminen ja todentaminen	Ennen mahdollisuutta hyödyntää ja käyttää pilvipalvelua, sen yksittäisten käyttäjien tulee tunnistautua palveluun ja todentaa oikeus palvelun käyttöön. Myös käyttäjän oikeudet palveluun tulee myöntää vasten oikeaa tarvetta ja turvallista prosessia noudattaen. Tällä pyritään varmistamaan myös pilvipalvelun käyttäjien suojaaminen ja se, että järjestelmään ei pääse luvattomasti käsiksi.
Valtuuttaminen	Valtuuttaminen on yksi tärkeimmistä tietoturvavaatimuksista pilvipalveluihin liittyen. Valtuuttamisella pyritään varmistamaan järjestelmän ja sen tiedon oikeellisuuden ylläpito. Valtuuttamisen vaatimuksella pyritään myös ohjaamaan eri käyttöoikeuksien myöntäminen niin, että riskit käyttöoikeuksien väärinkäytöstä minimoidaan.
Tiedon luotettavuus	Tiedon luotettavuudella pyritään varmistamaan organisaation datankäsittelyn hallinta eri tietokannoissa ja järjestelmissä. Erityisen tärkeää tiedon luotettavuudesta huolehtiminen on julkisen pilven

	palveluissa, jossa tietoon pääsyn rajoittamisella on tärkeä rooli. Tiedon luotettavuuden vaatimuksella suojataan myös palvelun käyttäjien data eri tietoturvaprotokollia hyödyntäen.
Tiedon oikeellisuus	Tiedon oikeellisuudelta vaaditaan erityisesti asianmukaisen huolellisuuden noudattamista datankäsittelyssä. Tarkemmat vaatimukset tiedon oikeellisuudesta määrittää vaatimus datan jakamattomuuden, johdonmukaisuuden, eristyneisyyden ja kestävyyden varmistaminen. Nämä asiat tulisi olla kunnossa riippumatta pilvipalvelun toteutus- tai palvelumallista.
Hyväksyntä	Hyväksyntää pilvipalveluissa perinteisillä turvallisuusprotokollilla, esimerkiksi digitaalisilla allekirjoituksilla, aikaleimoilla ja automaattisilla vahvistusviesteillä.
Tiedon saatavuus	Tiedon saatavuus on myös pilvipalveluiden näkökulmasta yksi oleellisimmista tietoturvavaatimuksista. Se vaikuttaa merkittävästi päätökseen siitä, hyödyntääkö organisaatio yksityistä-, julkista- vai hybridipilveä. Tiedon saatavuudessa tärkeintä on se, että palvelu tai data on aina saatavilla niille, joilla siihen on oikeus, mutta ei kenellekään muulle.
Palvelun tarkastettavuus	Pilvipalvelu tulee voida tarkastaa sisäisen tai ulkoisen tarkastajan toimesta. Tarkastaminen vaatii esimerkiksi prosessien tarkkaa määrittämistä ja dokumentointia.

5 YHTEENVETO KIRJALLISUUSKATSAUKSESTA

Tämän tutkielman tutkimuskysymykset ovat *"Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?"* sekä *"Mitä riskejä pilvipalveluissa ja organisaation pilvipalveluiden hallinnassa on tietoturvan näkökulmasta?"*. Tutkimus toteutetaan laadullisena tapaustutkimuksena ja tutkimuksen kirjallisuuskatsauksessa käytettyjen lähdetutkimusten osalta päätettiin rajata hakutulokset pääosin artikkeleihin, jotka on kirjoitettu viimeisen kymmenen vuoden aikana (2010-2020). Koska pilvipalvelut ovat alkaneet yleistymään vahvasti organisaatioiden ja yritysten käytössä, tämän tutkielman tarkoituksena oli löytää pilvipalveluille hallintamalleja ja -tapoja, jotka auttavat organisaatioita tietoturvahaasteissa.

Kirjallisuuskatsauksessa pilvilaskenta määriteltiin Mellin ja Gracen (2011) mukaan mallina, joka mahdollistaa verkon kautta pääsyn jaettuihin resursseihin, jotka eivät vaadi suurta vaivannäköä niiden hallinnan tai palveluntarjoajan kanssa kommunikoinnin suhteen. Nämä resurssit voivat olla esimerkiksi verkkoyhteyksiä, palvelimia, sovelluksia tai palveluja. Viisi pilvilaskennan tunnuspiirrettä määriteltiin käyttäjän itsepalvelumaiseksi käytöksi, laajaksi yhteydeksi verkon välityksellä, resurssien yhdistämiseksi, nopeaksi skaalautuvuudeksi ja mitattavaksi palveluksi. (Mell & Grance, 2011.) Pilvilaskennan käyttöönottomallit jaoteltiin julkiseen pilveen, yksityiseen pilveen, yhteisön pilveen ja hybridipilveen. Pilviympäristön palvelumallit edelleen jaoteltiin kolmeen osaan: infrastruktuuri palveluna, alusta palveluna sekä sovellus palveluna. (Savu, 2011.) Pilvipalvelut määriteltiin pilvilaskentaa hyödyntävinä, pilviteknologioita käyttäen luotuina palveluina, kuten esimerkiksi hotellinvarausjärjestelmä. (Zheng ym., 2012.)

Luvussa 3 käsiteltiin tietoturvaa organisaation ja käyttäjän näkökulmista sekä määriteltiin tietoturva kansainvälisen ISO/IE 27002 -standardin mukaisesti "tiedon luottamuksellisuuden, oikeellisuuden ja saatavuuden turvaamiseksi sekä varmistamiseksi". Organisaatioissa tietoturvan huomioiminen on erityisen tärkeää, jotta organisaation tietoon ei pääse luvatta käsiksi. (Tchernykh ym., 2019.) Tietoturva ja tietoturva-asioiden huomioiminen organisaatiossa jaettiin kahteen ja käsiteltiin sitä niin käyttäjän tietoturvatietoisuuden, kuin organisaatioiden tietoturvakäytänteidenkin näkökulmasta. Bulgurcun ym. (2010) mukaan tietoturvaan liittyykin käyttäjän näkökulmasta vahvasti käyttäjän asenne ja halu noudattaa organisaation tietoturvakäytänteitä. (Bulgurcu ym., 2010.) Tietoturvan lisäksi luvussa 3 määriteltiin ja käsiteltiin riskienhallintaa. Riskienhallinnalla pyritään arvioimaan ja minimoimaan riskejä ja niiden vaikutuksia. Riskejä tarkastellaan riskienhallinnassa tyypillisesti kahdesta eri näkökulmasta, jotka ovat riskien todennäköisyys ja vaikutukset. Riskienhallinnassa myös tyypillisesti määritetään riskikohtaisia toimenpiteitä, jotka minimoivat riskien toteutumista. (Tang & Musa, 2011.) Luvussa kolme esiteltiin myös riskienhallinnan kannalta perinteinen riskikertoimen muodostamisen taulukko, jota hyödyntämällä

organisaatiot voivat seurata ja huomioida riskejään. (ks. kuvio 3 riskienhallinnan riskianalyysi (mukaelma Markowskin ja Mannan'n (2008) kuviosta.)

Luvussa neljä käsiteltiin pilvipalveluiden hallintaa ja esiteltiin pilvipalveluiden hallintamalli MAPE-K -luuppi (kuvio 5). Pilvipalveluiden hallintamalli määriteltiin viitekehyksenä, jonka avulla pyritään ymmärtämään pilvipalveluihin liittyvät prosessit ja toimijat sekä heidän suhteensa. (Amanatullah ym., 2013.) Lisäksi luvussa neljä käsiteltiin pilvipalveluiden tietoturvaa ja vastattiin tutkimuskysymykseen *"Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?"*. Ramgovindin ym. (2010) ja Rebollon ym. (2015) mukaan pilvipalveluiden hallinnassa on tärkeää huomioida tietoturvan kannalta tunnistautuminen ja todentaminen, valtuuttaminen, tiedon luotettavuus sekä oikeellisuus ja saatavuus, hyväksyntä sekä palvelun tarkastettavuus (ks. taulukko 5).

Seuraavaksi taulukossa 7 on kuvattu pilvipalveluiden ominaisuuksia, niiden tietoturvariskejä sekä organisaatioiden toimenpiteitä kyseisten riskien hallitsemiseen.

TAULUKKO 7 Kirjallisuuskatsauksen perusteella saadut tulokset pilvipalveluiden ominaisuuksista ja riskeistä organisaation näkökulmasta.

Pilvipalvelun toteutus tai palvelumalli	**Palvelun ominaispiirre**	**Riski**	**Organisaation toimenpide riskin hallitsemiseen**
Infra-struktuuri palveluna	Infrastruktuuri, esim. palvelinympäristö, palveluntarjoajan tarjoama, muuten vastuu sovelluksesta käyttäjäorganisaatiolla ja sovelluskehttäjillä.	Sovelluskehitys on käyttäjä-organisaation vastuulla.	Tietoturva-käytänteiden ja työntekijöiden tietoturvatietoisuuden ylläpitäminen ja koulutus.
Sovellus palveluna	Palvelu tyypillisesti täysin palveluntarjoaja-organisaation hallinnoima.	Palvelussa data ja palvelut palveluntarjoajan palvelinsalissa, jolloin dataan liittyvä riski on palveluntarjoajalla. Toisaalta organisaatio omistaa datansa, ja datan fyysiseen sijaintiin voi olla heikko näkyvyys.	Palveluntarjoajan tarjoamaan palvelinympäristöön tutustuminen, palvelun tarkastukset ja esimerkiksi fyysisen hajauttamisen vaatiminen.
Alusta palveluna	Pilviympäristö (alusta ja infrastruktuuri) palveluntarjoajan hallinnoima, mutta sovellus tyypillisesti käyttäjäorganisaatiolle räätälöity.	Sovelluskehitys on käyttäjäorganisaation vastuulla.	Tietoturvakäytänteiden ja työntekijöiden tietoturvatietoisuuden ylläpitäminen ja koulutus.
Julkinen pilvi	Eri organisaatioiden kesken jaetut resurssivarannot.	Datan fyysiseen sijaintiin voi olla heikko näkyvyys.	Palveluntarjoajan tarjoamaan palvelinympäristöön tutustuminen, palvelun tarkastukset ja

			esimerkiksi fyysisen hajauttamisen vaatiminen.
Yksityinen pilvi	Organisaation oma resurssivaranto ja palvelinympäristö.	Tiedon turvallisuuden sekä palvelinympäristön hallinta käyttäjäorganisaation vastuulla.	Palvelinympäristön teknisen tietoturvan ja prosessien tietoturvakäytänteiden ylläpito.
Hybridipilvi	Palvelun ylläpito jaettu eri organisaatioille.	Tiedon saatavuuden varmistaminen, päivityskatkokset.	Tehokas viestintä ja esimerkiksi päivityskalenterin ylläpito.
Yhteisön pilvi	Jaettu pilviympäristö.	Tietoturva	Tehokas viestintä ja esimerkiksi päivityskalenterin ylläpito.
Moni-pilviympäristö	Yhdistelee eri pilviympäristöjä ja skaalaa tietoa niiden välillä automaattisesti ja älykkäästi	Tiedon oikeellisuuden varmistaminen	Tiedon oikeellisuuden tarkastuspistetet useammassa prosessin vaiheessa
Moni-pilviympäristö	Useita eri palvelinympäristöjä, jolloin palvelinten ja datakeskusten määrä saattaa kasvaa eksponentiaalisesti	Hiilijalanjäljen kasvaminen	Pilviympäristöjen seuranta ja palvelinten sijainnin tiedon ylläpito

Tutkielman laadullinen tapaustutkimus toteutettiin haastattelemalla tietoturvaan ja pilviympäristöihin erikoistuneita IT-alan ammattilaisia. Tutkielman empiirinen aineisto on kerätty näistä haastatteluista.

6 TUTKIMUSMENETELMÄ

Tässä luvussa kuvataan tutkimuksen tutkimusmenetelmä sekä tiedonkeruu- ja analysointimenetelmät. Tutkimuksen tarkoituksena on haastattelujen perusteella vastata tutkimuskysymyksiin *"Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?"* sekä *"Mitä riskejä pilvipalveluissa ja organisaation pilvipalveluiden hallinnassa on tietoturvan näkökulmasta?"*. Tutkimuksen empiiristä osiota edeltävät luvut 2-5, joissa pyrittiin vastaamaan tutkimuskysymyksiin käytettävissä olevan kirjallisuuden avulla. Luvusta seitsemän alkaen esitellään kirjallisuuskatsauksessa määriteltyjen teemojen pohjalta toteutettu tapaustutkimus. Tämä tutkimus toteutettiin laadullisena tapaustutkimuksessa, jonka empiirisen osuuden tieto kerättiin puolistrukturoitujen haastattelujen menetelmällä.

6.1 Tutkimusmenetelmä

Tutkimusmenetelmäksi tässä tutkimuksessa valittiin laadullinen tapaustutkimus. Baskaradan (2014) mukaan laadullisessa tapaustutkimuksessa keskitytään ymmärtämään tutkimuksen kohdetta ja tutkimusongelmaa syvemmin määrälliseen tutkimukseen verrattuna, jossa keskitytään suureen otokseen ja tilastoihin. Tutkimuskohteena on yleensä yksi tai useampi tapaus, jossa keskitytään tiettyyn ympäristöön. Tapaustutkimus sisältää myös syvällisen analyysin tapauksista, henkilöistä tai organisaatioista. Tällöin tapaustutkimus tarjoaa keinon tutkimusongelman analyyttiseen ratkaisuun. Tässä tapaustutkimuksessa pyrittiin toteuttamaan kaikki tapaustutkimuksen kuusi vaihetta, jotka ovat Baskaradan (2014) mukaan seuraavat:

- Suunnittelu
- Muotoilu
- Valmistelu
- Tiedonkeruu
- Analysointi
- Jakaminen

Laadullinen tapaustutkimus on valittu juuri siitä syystä, että siinä keskitytään tämän tutkimuksen osalta useampaan tapaukseen, ja pyritään saavuttamaan syvempi ymmärrys tapauksista. Tapauksia pyritään tässä tutkimuksessa määrittelemään, analysoimaan ja ratkaisemaan. Toisaalta laadullinen tapaustutkimus mahdollistaa myös haastateltavien äänen ja mielipiteiden havaitsemisen. Koska haastateltavina oli tutkimuksen kannalta relevanteilla taustoilla työskenteleviä

ammattilaisia, koettiin haastateltavien äänen kuuluminen tärkeäksi asiaksi, joka tuo laatua ja sisältöä tutkimuksen tuloksiin. (Eriksson & Koistinen, 2005.)

Haastattelumetodiksi päädyttiin valitsemaan puolistrukturoitu haastattelumetodi. Puolistrukturoitu haastattelumetodi koettiin sopivaksi, sillä siinä Hirsjärven ja Hurmeen (2008) mukaan haastattelun kysymykset ovat kaikille haastateltaville samalla tavalla muotoiltuja, joka helpottaa haastattelujen tulosten vertailua. Toisaalta puolistrukturoidussa haastattelussa jää haastattelijalle vapaus esimerkiksi muuttaa kysymysten järjestystä, jos kokee sen otolliseksi haastattelun tulosten kannalta. Puolistrukturoitu haastattelu mahdollistaa myös haastateltavien vastaamisen omin sanoin, eikä sido esimerkiksi vastausvaihtoehtoihin. Tämä koettiin tärkeäksi, jotta alan asiantuntijat voivat asiantuntemuksellaan myös ohjata haastattelua siihen suuntaan, joka palvelee heidän ydinosaamistaan parhaiten. (Hirsjärvi & Hurme, 2008.)

6.2 Tutkimuksen tavoite sekä tiedonkeruumenetelmä

Tämän tutkimuksen tavoitteena on vastata kahteen tutkimuskysymykseen, jotka ovat *"Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?"* sekä *"Mitä riskejä pilvipalveluissa ja organisaation pilvipalveluiden hallinnassa on tietoturvan näkökulmasta?"*. Näihin kysymyksiin pyritään löytämään vastauksia ja haastamaan tutkimuksen kirjallisuuskatsauksen tuloksia haastattelemalla IT- ja konsultointialojen ammattilaisia liitteen 1 mukaisella kysymysrungolla.

Tieto kerätään tässä tutkimuksessa puolistrukturoitujen haastattelujen metodilla. Tiedonkeruu suoritettiin puolistrukturoituja haastatteluja hyödyntäen toukokuussa 2020. Haastateltaviksi tutkimukseen valittiin 10 IT:n ja liikkeenjohdon konsultoinnin ammattilaista eri organisaatioista.

Tutkimus jaettiin teemoihin, jotka ovat organisaation tietoturva sekä tietoturvakäytänteet, työntekijöiden tietoturvatietoisuus sekä pilvipalveluiden tietoturva.

6.3 Tutkimuksen rajaukset

Tämän tutkimuksen kirjallisuuskatsauksena rajattiin tietoturvakäytänteiden, tietoturvatietoisuuden ja pilvipalveluiden tietoturva organisaation näkökulmaan. Kirjallisuuskatsaus antaa viitekehyksen tapaustutkimukselle joka toteutetaan kirjallisuuskatsauksessa määriteltyjen teemojen mukaisesti puolistrukturoituina haastatteluina. Tässä tutkielmassa kirjallisuuskatsaus muodostaa viitehtyksen tapaustutkimukselle, ja kirjallisuuskatsaus on muodostettu lähdekirjallisuuden perusteella, joka on julkaistu pääosin viimeisen kymmenen vuoden aikana (2010-2020). Empiirisen tutkimuksen tulokset on kerätty puolistrukturoiduista

haastatteluista. Haastatteluihin osallistui 10 IT :n ja konsultoinnin ammattilaista, joilla on kokemusta organisaatioissaan 1-7 vuotta.

7 TAPAUSTUTKIMUS

7.1 Haastateltavien tausta

Tähän tutkimukseen valittiin haasteltaviksi 10 asiantuntijaa IT- ja konsultointialan organisaatioista. Muita rajoituksia haastateltaville ei käytetty. Haastateltavien työtehtävät vaihtelivat, mutta voidaan todeta kaikkien haastateltavien työskennelleen pilviratkaisujen parissa. Seuraavaksi taulukossa 8 on kuvattu tarkemmin haastateltavien taustatiedot.

TAULUKKO 8 Tutkimuksen haastateltavien tausta

Haastateltava	Kokemus organisaatiossa	Työtehtävät
H1	n. 3 vuotta	Projektijohtaminen
H2	n. 1 vuosi	Pilvipalveluiden konsultointi
H3	n. 1 vuosi	Kyberturvallisuuden konsultointi
H4	n. 2 vuotta	Kyber-riskienhallinta ja konsultointi
H5	n. 4,5 vuotta	Kyberturvallisuuden konsultointi
H6	n. 4 vuotta	Riskienhallinnan konsultointi
H7	n. 4 vuotta	Tietoturvan konsultointi
H8	n. 3 vuotta	Riskienhallinnan konsultointi
H9	n. 4 vuotta	Hallinnollisen ja teknisen tietoturvan konsultointi
H10	n. 7 vuotta	Liikkeenjohdon konsultointi, riskienhallinta

7.2 Organisaation tietoturvariskit

Haastateltavilta tiedusteltiin heidän organisaatioidensa tietoturvariskejä, sekä miten organisaatiossa käsitellään tietoturvaan liittyviä riskejä. Haastateltavien vastaukset organisaatioidensa tietoturvariskeistä on koottu taulukkoon 9.

TAULUKKO 9 Haastateltavien näkemykset organisaatioiden oleellisimmista tietoturvariskeistä

Haastateltava	Organisaation tietoturvariskit
H1	Asiakastietojen vuotaminen, arkaluontoisen tiedon vuotaminen
H2	Ihmisten tahalliset tai tahattomat toimet
H3	Asiakastietojen vuotaminen, liikesalaisuuksien vuotaminen
H4	Asiakastietojen vuotaminen
H5	Mahdollisuus tietoturvan huonosta konfiguroinnista
H6	Asiakastietojen vuotaminen

H7	Asiakasdatan, hinnoittelumallien tai digitaalisen pääoman vuotaminen
H8	Asiakastietojen vuotaminen
H9	Tietovuodot, arkaluontoisen, luottamuksellisen asiakastiedon vuotaminen
H10	Asiakkaan julkaisemattoman finanssidatan vuotaminen

Organisaation tietoturvariskien käsittelyyn oli useita näkökulmia. Tyypillisesti organisaatioissa käsiteltiin tietoturvariskejä eri riskienhallintamenetelmillä. H1 kertoi myös seuraavaa :

> Organisaatiotasolla on omat riskienhallintamenetelmänsä. Tietoturvaosasto tarkkailee organisaation tietoliikennettä ja projekteissa usein mukana erillinen tietoturvavastaava.

Haasteltavien organisaatioilla oli tyypillisesti jonkinlainen sisäinen riskienhallintaorganisaatio, joka tarkastelee organisaation sisäisiä riskejä. Sisäinen riskienhallinta ei kuitenkaan kuulunut tai vaikuttanut merkittävästi haastateltavien työtä, joten selkeää vastausta organisaatioiden sisäisten riskien hallinnasta oli haastavaa löytää. Useasti esiin noussut teema työntekijöiden helposta tietoturvaraportoinnista oli erilaisten kalasteluviestien raportointi. Esimerkiksi haastateltavan 4 organisaatiossa oli nimitetty “Security Officer”, jolle tietoturvauhat ja muut havainnot tulee ilmoittaa. Lisäksi haastateltavan 4 organisaation sähköpostisovellukseen oli lisätty liitännäinen jolla epäilyttävän sähköpostin voi suoraan raportoida Security Officerille.

Jokapäiväisessä työssä tietoturvariskien hallintaa toteutettiin koulutusten kautta. Haastateltavan 2 organisaatiossa tietoturvariskejä käsiteltiin kahdella tapaa, jakamalla tietoturvariskit käyttäjän tahattomien ja tahallisten toimien mukaan:

> Tahattomia luonnollisesti koulutuksen kautta. Tuodaan käyttäjien tietoisuuteen uhkia ja riskejä mitä kohdataan ja miten yksittäinen ihminen voi siihen toimintaan tai riskiin reagoida. Tahalliseen selvät rajoitukset, kenelläkään ei ole pääsyä kaikkeen, vaan sitä rajataan sen mukaan mitä työtehtävä vaatii. Jos työtehtävä ei pääsyä tai oikeuksia edellytä niin sitä ei anneta... ....pitää käydä anomassa korkeammalta lupa siihen että tällainen oikeus tarvitaan... …Minimoidaan “blast radious” -aluetta, eli sitä aluetta mikä käyttäjävirheessä kärsii.

7.3 Organisaation tietoturvakäytänteet

Haastateltavilta kysyttiin minkälaisia tietoturvakäytänteitä heidän organisaatiollaan on ja miten varmistutaan, että tietoturvakäytänteet ovat työntekijöiden tiedossa ja niitä noudatetaan. Organisaatiokohtaiset tietoturvakäytänteet on kuvattu taulukossa 10.

TAULUKKO 10 Haastateltavien organisaatioiden tietoturvakäytänteet

Haastateltava	Kuvaus organisaation tietoturvakäytänteistä
H1	Tarkat salasanavaatimukset, VPN-yhteyden käyttö, vakioidut työskentelyvälineet, kalasteluviestien raportointityökalu.
H2	Oikeuksien ja pääsyn hakeminen ylemmältä taholta, laitteiden käyttöön liittyvät ohjeistukset
H3	Salatut ja organisaation omistamat laitteet
H4	Keskitetty laitehallinta, erilaiset ohjeistukset laitteiden käyttöön
H5	Sallitut/kielletyt pilvipalvelut
H6	Laitteiden käyttö sekä niihin liittyvä ohjeistus esimerkiksi salasanoista
H7	Sähköpostikäytänteet, salasanakäytänteet, työvälineiden käytön vaatimukset ja ohjeistukset
H8	Salasanavaatimukset, organisaation omistamien laitteiden käytön vaatimukset
H9	Alan arvostetun sertifikaatin mukaiset tietoturvakäytänteet
H10	Microsoftin parhaiden käytänteiden mukaiset salasanavaatimukset, salassa pidettävissä asioissa salassapitovelvollisuus

Haastateltavilla oli tyypillisesti organisaation tarjoamia henkilöstölle pakollisia tietoturvakoulutuksia, joilla varmistutaan siitä, että henkilöstö on tietoinen organisaation tietoturvakäytänteistä. Tietoturvakäytänteiden noudattamisen varmistaminen oli kaikilla haastateltavilla työntekijöiden koulutuksen sekä aktiivisen tiedottamisen varassa, esimerkiksi organisaation intrasivujen tai sähköpostin kautta. Haastateltavan 4 mukaan yleisesti ottaen organisaatioissa ei jalkauteta tietoturvakäytänteitä riittävällä tasolla, vaan tietoturvakäytänteet jäävät määrittelyn ja vuosittaisen pakollisen koulutuksen tasolle.

Käytännössä kaikilla haastateltavilla vastauksiksi nousivat tietoturvakoulutukset, tiedottaminen sekä esimerkiksi kalasteluviestikampanjat. Esiin nousi myös se, että organisaatio on tarkkaan määritellyt ja ohjeistanut työntekijöiden organisaation omistamien laitteiden käytön. Laitteet olivat haastateltavilla tyypillisesti myös organisaation keskitetyssä laitehallinnassa, jolloin organisaatio omistaa ja hallitsee työntekijöidensä työvälineinä käyttämiä puhelimia ja tietokoneita. Tiivistetysti voidaan todeta, että organisaatioissa luotettiin siis tietoturvakäytänteiden jalkauttamisessa ennaltaehkäisyyn erilaisten tietoturvakoulutusten, ohjeistuksien ja laitehallinnan avulla.

7.4 Työntekijän tietoturvatietoisuus

Haastateltavilta kysyttiin miten heidän organisaatioissaan pidetään huolta työntekijöiden tietoturvatietoisuudesta. Tiedusteltiin myös, kuinka tärkeänä tietoturva koetaan ja miten organisaation tietoturvakäytänteet huomioidaan työssä. Lähes kaikkien haastateltavien organisaatioissa työntekijöiden tietoturvatietoisuudesta pidettiin huolta säännöllisillä, henkilöstölle pakollisilla tietoturvakoulutuksilla. Toinen asia, joka nousi usealla haastateltavalla esille, oli säännöllinen muistuttelu kalasteluviesteistä sekä niiden raportoinnin työkalu.

Tietoturva koettiin haastateltavilla erittäin tärkeäksi. H1 kertoi, että :

> tietoturvan huomioiminen on erittäin tärkeää, varsinkin kun työskentelen asiakasrajapinnassa...

Tietoturva koettiin tärkeäksi siis erityisesti asiakasrajapinnassa työksennellessä. Syyksi haastateltavilla nousi eteenkin asiakastyö, ja luottamuksellisen sekä arkaluonteisen tiedon parissa työskentely. Tietoturvan epähuomioiminen koettiin myös mainehaittana, jonka johdosta tietoturvan huomioiminen nähtiin itsestäänselvyytenä. Esimerkiksi haastateltavan 5 mukaan hän kokee tietoturvan "Erittäin tärkeänä, vaikuttaisi jo omaan maineeseen työntekijänä, jos ei huomioisi.". Tietoturvan huomioiminen yleisesti koettiin siis itsestäänselvyytenä ja edellytyksenä asiakastöiden parissa työskennellessä.

Taulukkoon 11 on kuvattu haastateltavien vastaukset organisaatiokohtaisista tavoista, joilla varmistutaan henkilöstön tietoturvatietoisuudesta.

TAULUKKO 11 Tavat, joilla haastateltavien organisaatiot huolehtivat työntekijöiden tietoturvatietoisuudesta

Haasteltava	**Tavat joilla organisaatio huolehtii työntekijöiden tietoturvatietoisuudesta**
H1	Säännöllinen ja pakollinen tietoturvakoulutus, tietoturvaan liittyvät ohjeistukset, havainnollistavat tietojenkalasteluviestit.
H2	Henkilöstön koulutus ja ohjeistus. Teknologian ja auditoinnin avulla toteutettu valvonta.
H3	Henkilöstölle pakolliset tietoturvakoulutukset, intrasivujen kautta viestintä
H4	Käytänteet koulutetaan heti alkuun, erilaiset sähköpostikalasteluharjoitukset
H5	Vuosittaiset koulutukset
H6	Jokaiselle työntekijälle pakolliset tietoturvakoulutukset säännöllisin väliajoin
H7	Tietoturvakoulutukset sekä säännöllinen tiedottaminen intrasivuilla ja sähköpostilla
H8	Henkilöstön tietoturvakoulutukset, säännöllinen muistuttelu sähköpostilla
H9	Tietojenkalastelukampanjat, epäilyttävien sähköpostien raportointityökalu
H10	Työntekijöille pakolliset tietoturvakoulutukset sekä ajankohtaisista asioista tiedottaminen sähköpostilla ja intrasivuilla

7.5 Pilvipalveluiden tietoturva

Haasteltavilta tiedusteltiin ensin sitä, minkälaisia pilviratkaisuja he hyödyntävät työssään. Pilviratkaisujen suhteen selvitettiin, miten niihin tunnistaudutaan,

millä tasolla niiden tietoturva koetaan sekä kuinka tärkeäksi käyttämien pilvipalveluiden tietoturva koetaan.

Haasteltavilla oli käytössä erityyppisiä pilviratkaisuja. Yhteisenä nimittäjänä jokainen haastateltava hyödynsi työssään Microsoftin Office365 –pilviratkaisuja. Osalla haastateltavista oli käytössään myös muita kolmansien osapuolten pilviratkaisuja. Koettiin myös, että pilviratkaisujen käyttö on siirtymässä yhä enemmän Microsoftin kollaboraatiotyökaluihin. Esimerkiksi haastateltava 9 totesi seuraavaa:

> Työhön liittyvät pilviratkaisut on rakentunut miltei 100 % Microsoftin O365-pilvipalvelun ympärille. Siihenhän siis sisältyy Teamsit ja Sharepoint ja OneDrive. Varsinkin nyt kun sähköpostiliikenne on siirtymässä Teamsin puolelle ja tiedostot pysyvät siellä, eikä jatkuvasti lähetellä tiedostoja verkon yli. Käyttö jatkuvaa ja runsasta.

Haastateltavien vastauksissa ei kuitenkaan ollut työssä käytettävien pilviratkaisujen suhteen oleellisia eroja, kaikki haastateltavat hyödynsivät Microsoftin pilviratkaisuja, sekä jotain kolmansien osapuolten pilviratkaisuja.

Haasteltavien työssä käytettämien pilviratkaisujen tunnistautumiskeinot on kuvattu seuraavaksi taulukossa 12.

TAULUKKO 12 Haastateltavien työssä käyttämien pilvipalveluiden tunnistautumistavat

Haastateltava	**Pilvipalveluun tunnistautuminen**
H1	Kaksivaiheinen tunnistautuminen : puhelimeen lähetettävä koodi sekä salasana.
H2	Palveluntarjoajan identiteetinhallinann kautta, joskus myös oman organisaation identiteetinhallinnan kautta
H3	Kaksivaiheinen tunnistautuminen : Käyttäjätunnus ja salasana, sekä authenticator-sovellus tai token
H4	Monivaiheinen tunnistautuminen, laitteet laitehallinnan piirissä
H5	Kaksivaiheinen tunnistautuminen, joihinkin palveluihin puhelimella käy myös kasvontunnistus.
H6	Monivaiheinen tunnistautuminen : käyttäjätunnus + salasana sekä authenticator sovelluksen vahvistuskoodi
H7	Monivaiheinen tunnistautuminen
H8	Kaksivaiheinen tunnistautuminen, joissain palveluissa pelkkä käyttäjätunnus + salasana
H9	Monivaiheinen tunnistautuminen, työpöytäsovelluksissa pelkkä käyttäjätunnus + salasana : federointi tapahtuu työaseman kirjautumisen kautta
H10	Monivaiheinen tunnistautuminen : käyttäjätunnus + salasana sekä autentikaatiosovellus

Viimeiseksi haastateltavilta tiedusteltiin kuinka tärkeäksi he kokevat käyttämiensä pilvipalveluiden tietoturvan. Vastaukset on koostettu taulukkoon 13.

TAULUKKO 13 Haastateltavien vastaukset siitä, kuinka tärkeäksi he kokevat käyttämiensä pilvipalveluiden tietoturvan

Haastateltava	**Kuinka tärkeäksi pilvipalveluiden tietoturva koetaan**
H1	Tietoturva täytyy olla korkealla tasolla, koska järjestelmät sisältävät tietoa asiakkaista, prosesseista sekä kehitysprojekteista.
H2	Äärimmäisen tärkeäksi
H3	Hyvin tärkeäksi
H4	Ei käyttäisi palveluita, joissa ei olisi varmuutta tietoturvasta
H5	Todella tärkeäksi, erityisesti tiedon saatavuus on erittäin tärkeää
H6	Erityisesti asiakastiedon parissa työskennellessä erittäin tärkeää liiketoiminnalisestikin
H7	Erittäin tärkeäksi
H8	Itsestäänselväksi, asiakastöiden parissa välttämätöntä, ja erityisesti henkilökohtaisessa työssä tiedon saatavuus tärkeää
H9	Todella tärkeäksi ja luottamusta herättäväksi, koska käsitellään asiakastietoja
H10	Asiakastietojen käsittelyn kannalta elintärkeää ja välttämätöntä

8 TUTKIMUKSEN TULOKSET JA POHDINTA

Tässä luvussa käydään läpi empiirisen tutkimuksen tulokset luvussa 8.1 sekä tulosten pohdinta luvussa 8.2. Tutkimuksen tuloksissa esitellään teemoittain oleellisimmat löydökset tutkimuksesta ja tulosten pohdinnassa verrataan empiirisen tutkimuksen löydyksiä olemassa olevaan kirjallisuuteen.

8.1 Tutkimuksen tulokset

Tässä alaluvussa käydään läpi empiirisen tutkimuksen tulokset aihealueittain. Luvussa 8.1.1 käydään läpi oleelliset tulokset tietoturvan, tietoturvakäytänteiden ja tietoturvatietoisuuden osalta, ja luvussa 8.1.2 pilvipalveluiden tietoturvan osalta.

8.1.1 Tietoturva, tietoturvakäytänteet ja tietoturvatietoisuus

Organisaatioiden tietoturvariskien osalta vastaukset olivat yksipuolisia. Käytännössä kaikkien haastateltavien vastauksissa esiin nousi organisaation kannalta suurimpana riskinä asiakastietojen tai muun arkaluonteisen tiedon vuotaminen. Haasteltava 2 nosti myös esille ihmiset ja heidän tahalliset tai tahattomat toimet. Kaikki haastateltavat toimivat asiakatyössä, jolloin suurimpana riskinä he kokivat niin taloudellisesti kuin organisaation maineen kannalta asiakkaan arkaluonteisen tai julkaisemattoman finanssitiedon vuotamisen.

Haastateltavien organisaatioiden riskien käsittelyyn oli erilaisia lähestymistapoja. Siinä missä osa keskittyi vastauksissaan jo tietoturvakäytänteisiin ja niiden kouluttamiseen sekä noudattamisen valvontaan, suurin osa haastateltavista ei ollut tietoinen tarkasta tavasta jolla heidän organisaatioissaan riskejä käsitellään. Haastateltavista suurimman osan vastauksissa nousi esille sisäinen riskienhallintaorganisaatio, joka toimii kuitenkin erillään asiakastöitä tekevästä riskienhallintayksiköstä. Esille nousi myös nimitetty tietoturvasta vastaava “Security Officer”, jolle esimerkiksi epäilyttävistä sähköposteista tulee ilmoittaa.

Haastateltavien organisaatioiden tietoturvakäytänteet olivat hyvin saman tyyppisiä. Salasanavaatimukset, sekä organisaatioiden omistamien laitteiden käytön ohjeistukset nousivat usealla haastateltavalla esille. Organisaatiot olivat siis määritelleet mitä työvälineitä työntekijät saavat käyttää, ja ohjeistaneet niiden käyttöä tietoturvallisella tavalla. Ylipäänsä tietoturvakäytänteet nähtiin nimenomaan ohjeistuksena, jota organisaatio on työntekijöilleen ohjeistanut. Myös sertifiointi nousi esille, haastateltava 9 kertoi organisaationsa tietoturvakäytänteiden olevan alan arvostetun sertifikaatin mukaisia, ja täyttäneen sen.

Tietoturvakäytänteiden tietoisuudessa ja noudattamisessa haasteltavien organisaatioissa luotettiin pääosin jokaiselle organisaation työntekijälle pakolliseen tietoturvakoulutukseen. Koulutukset suoritetaan haastateltavien

organisaatioissa aloittaessa työsuhteen, mutta myös säännöllisiä, esimerkiksi vuosittaisia, koulutuksia järjestetään. Koulutusten lisäksi haastateltavat nostivat esiin yleiset ohjeistukset ja aktiivisen tiedottamisen organisaation intrasivuilla sekä sähköpostilistoilla. Myös tietoturvakampanjat nousivat esille. Haastateltavan 4 organisaatiossa oli toteutettu organisaation työntekijöilleen sähköpostilla lähettämä kalasteluviestiharjoitus. Haastateltava 5 nosti myös esille yleisesti ottaen organisaatioiden heikot kyvkkyydet tietoturvakäytänteiden jalkautukseen. Tietoturvakäytänteet on tyypillisesti määritelty, ja vuosittaiset koulutukset järjestetään, mutta sen lisäksi tietoturvakäytänteitä ei jalkauteta työntekijöille päivittäiseen työhön.

Tietoturvan tärkeyden kokeminen oli haastateltavilla yksiselitteistä. Kaikki haastateltavat kokivat tietoturvan työssään tärkeäksi tai erittäin tärkeäksi ja jopa itsestäänselvyydeksi. Syynä tietoturvan tärkeydelle nostettiin erityisesti se, että haastateltavat työskentelevät arkaluonteisen asiakastiedon parissa. Tällöin riskinä on organisaation maineen vahingoittuminen, jos asikastietoa vuotaisi.

8.1.2 Pilvipalveluiden tietoturva

Jokaisella haastateltavalla oli työssään käytössä jollain tasolla Microsoftin pilviratkaisut. Monella haastateltavalla oli myös muita kolmansien osapuolten ratkaisuja käytössään. Microsoftin pilviratkaisujen käyttö nähtiin myös yleistyvän ja työnteon siirtyvän yhä enemmän esimerkiksi sähköpostista ketteriin kollaboraatiotyökaluihin, kuten Microsoft Teamsiin. Haastateltavien käytössä oleviin pilvipalveluihin tunnistauduttiin poikkeuksetta kaksivaiheisesti, ensimmäisen vaiheen ollessa käyttäjätunnus ja salasana (joko palveluun tai työasemalle, josta federoituu esim. Työpöytäsovelluksiin) sekä autentikaatiosovelluksen vahvistuskoodi.

Haastateltavat kokivat käyttämiensä pilvipalveluiden tietoturvan hyvälle tasolle. Luottamusta haastateltavilta löytyi eteenkin isojen organisaatioiden pilvipalveluihin, jolloin haasteet ovat korkeintaan organisaation omassa, paikallisessa konfiguraatiossa. Tietoturva koettiin myös äärimmäisen tärkeäksi pilvipalveluissa. Vaatimukset työssä hyödynnettävien palveluiden tietoturvasta tulivat asiakastöistä. Tietoturva koettiin siis välttämättömänä, luottamusta herättävänä ja jopa itsestäänselvänä vaatimuksena asiakastyölle.

8.2 Tulosten pohdinta

Tässä tutkimuksessa tavoitteena oli selvittää organisaation kannalta oleellisia tietoturvariskejä, sekä miten niitä tulisi huomioida pilvipalveluiden hallinnassa. Tavoitteena oli vastata tutkimuskysymyksiin *”Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?”* sekä *”Mitä riskejä pilvipalveluissa ja organisaation pilvipalveluiden hallinnassa on tietoturvan näkökulmasta?”*. Kirjallisuuskatsauksen pohjalta löydettiin merkittäviä löydöksiä siihen,

miten organisaatioiden tulee huomioida pilvipalveluiden tietoturva esimerkiksi työntekijöiden ohjeistusten ja tietoturvakäytänteiden kautta. Kirjallisuuskatsaus osoitti myös pilviturvallisuuden kannalta oleellisia vaatimuksia esimerkiksi työntekijöiden tunnistautumiseen. Empiirinen tutkimus toteutettiin haastattelemalla IT:n ja liikkeenjohdon konsultoinnin ammattilaisia. Haastatteluissa pyrittiin selvittämään työntekijän näkökulmasta vastauksia kysymyksiin organisaation tietoturvasta, tietoturvakäytänteistä sekä niiden noudattamisen varmistamisesta, sekä haastateltavien käyttämiä pilvipalveluita ja niiden tietoturvaa sekä tunnistautumistapoja. Tässä luvussa verrataan kirjallisuuskatsauksen ja empiirisen tutkimuksen löydöksiä sekä pyritään vastaamaan tutkimuksen tutkimuskysymyksiin.

Oleellisimpina yhtäläisyyksinä kirjallisuuskatsauksen löydösten ja empiirisen tutkimuksen tulosten välillä voidaan todeta ainakin organisaation tietoturvariskit. Haastatteluista nousi esille oleellisen tiedon vuotaminen, jota myös kirjallisuus tukee. (Siponen, 2005.) Toisena asiana voidaan todeta tietoturvakäytänteet tehokkaana tapana varmistaa pilvipalveluiden tietoturva (Niemimaa & Niemimaa, 2017.) Myös empiirisen tutkimuksen haastattelut tukivat tätä, sillä haastateltavien organisaatioissa tietoturvakäytänteet olivat määritelty ja ne liittyivät juuri pilvipalveluiden käyttöön eri laitteilla. Kolmantena yhtäläisyytenä voidaan nostaa Al-Omarin ym. (2012) toteamus siitä, että tietoa käsittelevien järjestelmien kokonaisturvallisuutta tarkastellessa on syytä huomioida ihmiskäyttäjän tuoma ihmisriski, joka on tehokkainta minimoida tietoturvakäytänteillä. Myös haastatteluissa esiin nousi suurena tietoturvariskinä ihmisen tahalliset ja tahattomat toimet, joita haastateltavan 2 organisaatiossa käsiteltiin tietoturvakäytänteillä. Kirjallisuuskatsauksen löydökset ja niitä tukevat empiirisen tutkimuksen tulokset on esitelty taulukossa 14.

TAULUKKO 14 Kirjallisuuskatsauksen löydökset sekä niitä tukevat empiirisen tutkimuksen tulokset

Kirjallisuuskatsauksen löydös	**Empiirisen tutkimuksen kirjallisuuskatsauksen löydöstä tukeva tulos**
Tietovuodoilla ja organisaation haavoittuvuudella voi olla merkittäviä vaikutuksia niin organisaation kun sen palvelun käyttäjien näkökulmasta. Tietojärjestelmien tietoturvan asianmukainen varmistaminen on siis erittäin tärkeää organisaatioille. (Siponen, 2005.)	Oleellisimpia riskejä organisaatiolle ovat tietovuodot
Nykyään organisaatioita myös painostetaan ottamaan käyttöön tietojärjestelmien tietoturvaan liittyviä käytänteitä ja metodeja sekä noudattamaan niihin liittyviä parhaita käytänteitä, jotta arvokkaaseen tietoon liittyviä riskejä voidaan minimoida. Yleisesti seurattavia parhaita tietojärjestelmien tietoturvakäytänteitä sisältävät esimerkiksi ISO/IEC27001, NIST-SP800 ja	Tietoturvakäytänteiden jalkauttaminen perustuu koulutuksiin ja aktiiviseen tiedotukseen. Tietoturvakäytänteet organisaatiossa on pohjattu alan arvostettuun sertifikaattiin. Tietoturvakäytänteet liittyvät pääasiassa sallittujen palveluiden ja laitteiden käyttöön

PCI-DSS -standardit. Tietojärjestelmiin kohdistuvat tietoturvariskit lisääntyvät jatkuvasti, joka on johtanut organisaatioiden tarpeeseen käyttöönottaa käytänteitä ja standardeja nopealla tahdilla. (Niemimaa & Niemimaa, 2017.)	
Tärkeänä osana kriittistä tietoa käsittelevien järjestelmien kokonaisturvallisuutta tarkastellessa on kuitenkin huomioida ihmiskäyttäjän tuoma ihmisriski. Tämä käyttäjän aiheuttama riski on kaikista tehokkainta minimoida nimenomaan tehokkailla tietoturvakäytänteillä. (Al-Omari, El-Gayar & Deokar, 2012.)	Ihmiset suurin riski – tahattomat tai tahalliset toimet
Tietoturvakäytänteiden huomioiminen saattaa heikentää prosessien maksimaalista tehokkuutta, mutta se on kuitenkin tärkeää, sillä nykyään organisaatioiden liiketoiminta tai muut prosessit voivat olla täysin riippuvaisia informaatioteknologiasta. Tällöin on myös organisaatiolle elintärkeää, että prosessit ovat tietoturvallisia ja tietoturvakäytänteitä noudatetaan. (Flowerday & Tuyikeze, 2016.)	Tiedon saatavuus on erittäin tärkeää - että työhön vaadittava tieto on saatavilla eri laitteilla eri sijainneista
Pilvipalvelua käyttäessä käyttäjien tulee tunnistautua palveluun, ja todentaa oikeus palvelun käyttöön. Käyttäjän oikeuden palveluun tulee myöntää vasten oikeaa tarvetta. (Ramgovind ym., 2010 ja Rebollo ym., 2015)	Oikeudet myönnetään työtehtävien mukaisesti

Empiirisen tutkimuksen tulokset tarjosivat myös tuloksia, jotka eivät täysin tue kirjallisuuskatsauksen löydöksiä. Kirjallisuuden perusteella esimerkiksi oleellisimpana asiana tietoturvakäytänteitä muodostaessa on huomioida niiden noudattaminen, ei pelkästään tietoturvakäytänteiden määrittely. (Wall ym., 2013.) Haastateltavan 5 mukaan kuitenkin on tyypillistä organisaatioissa, että tietoturvakäytänteet määritellään, mutta ei jalkauteta tai valvota niiden noudattamista. Tämä ei toki todennäköisesti ole organisaatioiden tiedostama asia tai tahtotila. Kirjallisuuden perusteella myös organisaation sisäisen riskienhallinnan tulisi olla systemaattista, ja johdonmukaista. (Baskerville, 1993 ja Markowski & Mannan, 2008.) Tähän ei kuitenkaan haastateltavilta löytynyt tarkkaa tietoa, joten tätä löydöstä ei pystytty empiirisen tutkimuksen perusteella vahvistamaan. Taulukossa 15 on esitelty kirjallisuuskatsauksen löydöksiä ja empiirisen tutkimuksen tuloksia, jotka eivät tue kirjallisuuskatsauksen löydöksiä.

TAULUKKO 15 Kirjallisuuskatsauksen löydökset sekä empiirisen tutkimuksen tulokset, jotka eivät tue löydöksiä

Kirjallisuuskatsauksen löydös	**Empiirisen tutkimuksen tulos, joka ei tue kirjallisuuskatsauksen löydöstä**

Organisaation sisäisen riskienhallinnan tulisi olla systemaattista ja johdonmukaista sekä jalkautettua organisaation työntekijöille. (Baskerville, 1993 ja Markowski & Mannan, 2008.)	Riskejä käsitellään sisäisessä riskienhallinnassa, ei tarkkaa tietoa miten sisäisiä riskejä hallitaan
Organisaation kannalta on erittäin tärkeää, että tietoturvakäytänteet on luotu huolellisesti. Toisaalta on myös tärkeää varmistua siitä, että työntekijät noudattavat tietoturvakäytänteitä parhaalla mahdollisella tavalla. Tietoturvakäytänteiden noudattamisesta varmistumiseen organisaatiolla voi olla monia vaihtoehtoja. Tyypillinen tapa on kuitenkin määritellä kontrolleja, jotka antavat viitekehyksen esimerkiksi prosessien suunnittelulle. Kun prosessit suoritetaan näitä kontrolleja noudattaen, lähtökohtaisesti myös tietoturvakäytänteitä noudatetaan. (Wall, Palvia & Lowry, 2013.)	Tietoturvakäytänteiden jalkauttamista/toteutumista ei merkittävästi valvota
Tietoturvatietoisuus – organisaation tietoturvakäytänteiden tunnistaminen, ymmärrys tietoturvakäytänteistä - tieto siitä, mitä tietoturva on	Tietoturva koetaan tärkeäksi, itsestään selväksi

9 YHTEENVETO

Tässä tutkimuksessa tavoitteena oli selvittää organisaation kannalta oleellisia tietoturvariskejä, sekä miten niitä tulisi huomioida pilvipalveluiden hallinnassa. Tavoitteena oli vastata tutkimuskysymyksiin *"Mitä organisaation tulee ottaa huomioon pilvipalveluiden hallinnassa tietoturvan näkökulmasta?"* sekä *"Mitä riskejä pilvipalveluissa ja organisaation pilvipalveluiden hallinnassa on tietoturvan näkökulmasta?"*. Tutkimus koostui kirjallisuuskatsauksesta (luvut 2-5) sekä empiirisestä tutkimuksesta (luvut 6-8).

Tutkimuksen kirjallisuuskatsauksessa määriteltiin aluksi pilvilaskenta, pilvilaskennan käyttöönottomallit ja pilvipalveluiden palvelumallit. Pilvilaskenta määriteltiin Mellin ja Gracen (2011) mukaan asiana, joka mahdollistaa eri henkilöille pääsyn jaettuihin resursseihin. Sen tunnuspiirteiksi listattiin käyttäjän itsepalvelumainen käyttö, laaja yhteys verkon välityksellä, resurssien yhdistäminen, nopea skaalautuvuus sekä mitattava palvelu. (Mell & Grace, 2011.) Tämän jälkeen pilvilaskennan käyttöönottomalleiksi määriteltiin julkinen pilvi, yksityinen pilvi, hybridipilvi sekä yhteisön pilvi (Savu, 2011). Pilvipalveluiden palvelumalleiksi määriteltiin infrastruktuuri palveluna, alusta palveluna sekä sovellus palveluna (Zheng ym., 2012).

Seuraavaksi määriteltiin tietoturva tiedon oikeellisuuden, saatavuuden ja luottamuksellisuuden varmistamisena (Von Solms & Van Niekerk, 2013). Tiedon turvaaminen esitettiin tärkeänä eteenkin pilvipalveluissa. Organisaatioille tämä tarkoittaa sen varmistamista, että organisaatiolle kriittiseen tietoon ei pääse käsiksi ilman oikeutettua pääsyä tietoon. (Tchernykh ym, 2019.) Organisaatioiden parhaaksi keinoksi varmistua henkilöstön tietoturvallisesta työskentelystä esitettiin tietoturvakäytänteiden määrittely, sekä organisaation henkilöstön tietoturvatietoisuuden ylläpitäminen. (Bulgurcu ym., 2010.) Tietoturvakäytänteiden ja tietoturvan osalta myös empiirinen tapaustutkimus tuotti tuloksia, jotka viittaavat siihen, että organisaatiot huolehtivat tietoturvakäytänteidensä noudattamisesta panostamalla työntekijöidensä tietoturvatietoisuuteen.

Tutkimusmenetelmäksi tutkimukselle valittiin laadullinen tapaustutkimus, joka mahdollistaa tapauksen tai tapausten syvällisen analysoinnin haastattelujen muodossa. Haastattelumetodiksi valikoitui puolistrukturoitu haastattelu, joka jättää tilaa haastateltaville käyttää omaa ääntään ja tietämystään aiheesta. Toisaalta puolistrukturoitu haastattelumetodi myös mahdollistaa haastattelun joustavuuden esimerkiksi kysymysten järjestyksen osalta. Tapaustutkimukseen valittiin haastateltaviksi 10 alan asiantuntijaa IT:n ja liikkeenjohdon konsultoinnin organisaatioista. Haastateltavilla oli kokemusta organisaatioissaan 1-7 vuotta, ja heistä kaikki työskentelivät jollain tasolla erilaisten pilviratkaisujen parissa. Haastateltaville ei tässä tapaustutkimuksessa käytetty muita rajauksia. Kirjallisuuskatsaus loi viitekehyksen tapaustutkimukselle, ja kirjallisuuskatsauksessa hyödynnettiin rajauksena pääosin viimeisen kymmenen vuoden (2010-2020) aikana julkaistuja artikkeleita ja kirjoja sekä muuta lähdemateriaalia.

Laadullisen tapaustutkimuksen kysymykset löytyvät tutkimuksen lopusta, liitteestä 1. Tapaustutkimuksen tulokset ovat tiivistettynä seuraavat:

- Organisaatioiden kannalta oleellisimmat tietoturvariskit liittyvät tietovuotoihin
- Organisaatioiden tietoturvakäytänteet liittyvät lähinnä palveluiden ja laitteiden käyttöön ja niiden ohjeistuksiin
- Tietoturvakäytänteiden noudattamisesta varmistutaan organisaatioissa työntekijöille pakollisilla tietoturvakoulutuksilla ja tietoturvakampanjoilla
- Tietoturva koetaan erittäin tärkeäksi, ja asiakastöissä itsestään selväksi sekä luottamusta herättäväksi
- Suurin osa organisaatioista on siirtynyt hyödyntämään Microsoftin pilviratkaisuja
- Kaksivaiheinen tunnistautuminen on yleisin pilvipalveluun tunnistautumisen muoto
- Suurten organisaatioiden pilvipalveluiden tietoturvaan luotetaan

Tapaustutkimuksen tuloksista löydettiin sekä tuloksia, jotka tukevat kirjallisuuskatsauksen löydöksiä, että tuloksia, jotka eivät tue kirjallisuuskatsauksen löydöksiä. Oleellisimpina yhtäläisyyksinä kirjallisuuskatsauksen löydösten ja empiirisen tutkimuksen tulosten välillä todettiin organisaation tietoturvariskit, organisaatioiden kannalta oleellisimpia riskejä sekä kirjallisuuden, että empiirisen tutkimuksen perusteella olivat arkaluonteisen tiedon tietovuodot. Toisena yhtäläisyytenä nostettiin tietoturvakäytänteet, ja niiden hyödyntäminen pilvipalveluiden tietoturvaan käyttäjiä ohjeistamalla. Haastateltavien organisaatioissa tietoturvakäytänteillä pyrittiin nimenomaan ohjeistamaan eri pilvipalveluiden käyttäjiä tietoturvalliseen työskentelyyn. Yhtäläisyytenä nostettiin myös pilvipalveluiden kokonaisturvallisuutta tarkastellessa ihmisen rooli. Ihminen ja ihmisriski nähtiin niin kirjallisuudessa kuin myös empiirisen tutkimuksen tuloksissa oleellisena tietoturvariskinä organisaatioille. Tähän tehokkain ja tapaustutkimuksen perusteella organisaatioissa hyödynnetty tapa minimoida riskiä oli tietoturvakäytänteet, sekä niiden noudattamisen valvonta. Yhtäläisyydet kirjallisuuden löydöksistä ja empiirisen tutkimuksen tuloksista on esitelty tarkemmin taulukossa 14.

Empiirisen tutkimuksen tulokset tarjosivat myös tuloksia, jotka eivät täysin tue kirjallisuuskatsauksen löydöksiä. Kirjallisuudessa nostettiin oleellisena asiana tietoturvakäytänteiden tehokas jalkauttaminen, joka ei kaikkien haastateltavien mukaan yleisesti ottaen organisaatioissa toteudu. Kirjallisuudessa nostettiin sisäisen riskienhallinnan tärkeys esiin, ja se, että se on systemaattisesti ja johdonmukaisesti toteutettu ja jalkautettu. Empiirinen tutkimus ei tarjonnut tukea tälle löydökselle, vaan haastateltavat eivät pystyneet tarkkaan määritellä, miten heidän organisaatioissaan erilaisia tietoturvariskejä käsitellään. Haastateltavat pystyivät pääasiassa nimeämään sisäisen riskienhallintayksikön, joka toimii

erillään muusta riskienhallinnasta. Empiirisen tutkimuksen tulokset, jotka eivät täysin tue kirjallisuuden löydöksiä, on esitelty tarkemmin taulukossa 15.

LÄHTEET

Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, *32*(1), 50-65.

Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011, July). Collaboration-based cloud computing security management framework. In *2011 IEEE 4th International Conference on Cloud Computing* (pp. 364-371). IEEE.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012, January). Security policy compliance: User acceptance perspective. In *2012 45th Hawaii International Conference on System Sciences* (pp. 3317-3326). IEEE.

Amanatullah, Y., Lim, C., Ipung, H. P., & Juliandri, A. (2013, June). Toward cloud computing reference architecture: Cloud service management perspective. In *International Conference on ICT for Smart Society* (pp. 1-4). IEEE.

Baskarada, S. (2014). Qualitative case study guidelines. Baškarada, S.(2014). Qualitative case studies guidelines. The Qualitative Report, 19(40), 1-25.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*, *25*(4), 375-414.

Bohn, R. B., Messina, J., Liu, F., Tong, J., & Mao, J. (2011, July). NIST cloud computing reference architecture. In 2011 IEEE World Congress on Services (pp. 594-596). IEEE.

Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2016, March). Cloud computing service models: A comparative study. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 890-895). IEEE.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Chowdhury, Z. J., Pishva, D., & Nishantha, G. G. D. (2010, February). AES and Confidentiality from the Inside Out. In *2010 The 12th International Conference on Advanced Communication Technology (ICACT)* (Vol. 2, pp. 1587-1591). IEEE.

Eriksson, P., & Koistinen, K. (2005). *Monenlainen tapaustutkimus*. Helsinki: Kuluttajatutkimuskeskus.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. computers & security, 61, 169-183.

Hirsjärvi, S. & Hurme, H. (2008). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011). Nist cloud computing standards roadmap. *NIST Special Publication*, *35*, 6-11.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of risk and insurance*, *78*(4), 795-822.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232.

Innocent, A. (2012). Cloud infrastructure service management-a review. *arXiv preprint arXiv:1206.6016*.

Marinos, A., & Briscoe, G. (2009, December). Community cloud computing. In *IEEE International Conference on Cloud Computing* (pp. 472-484). Springer, Berlin, Heidelberg.

Markowski, A. S., & Mannan, M. S. (2008). Fuzzy risk matrix. *Journal of hazardous materials*, *159*(1), 152-157.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Moghaddam, F. F., Rohani, M. B., Ahmadi, M., Khodadadi, T., & Madadipouya, K. (2015, August). Cloud computing: Vision, architecture and Characteristics. In *2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC)* (pp. 1-6). IEEE.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1-20.

Paananen, H., Lapke, M., & Siponen, M. (2019). State of the Art in Information Security Policy Development. *Computers & Security*, 101608.

Padilla, R. S., Milton, S. K., & Johnson, L. W. (2015). Components of service value in business-to-business Cloud Computing. *Journal of Cloud Computing*, *4*(1), 15.

Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In *2010 Information Security for South Africa* (pp. 1-7). IEEE.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44-57.

Rutten, E., Marchand, N., & Simon, D. (2017). Feedback control as MAPE-K loop in autonomic computing. In *Software Engineering for Self-Adaptive Systems III. Assurances* (pp. 349-373). Springer, Cham.

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330.

Savu, L. (2011, May). Cloud computing: Deployment models, delivery models, risks and research challenges. In *2011 International Conference on Computer and Management (CAMAN)* (pp. 1-4). IEEE.

Siponen, M. T. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and organization*, *15*(4), 339-375.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems*, *14*(3), 303-315.

Tang, O., & Musa, S. N. (2011). Identifying risk issues and research advancements in supply chain risk management. *International journal of production economics*, *133*(1), 25-34

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581.

Tsai, W., Bai, X., & Huang, Y. (2014). Software-as-a-service (SaaS): perspectives and challenges. *Science China Information Sciences*, *57*(5), 1-15.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security*, *9*(4), 52-79.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010, June). Information security risk management framework for the cloud computing environments. In *2010 10th IEEE international conference on computer and information technology* (pp. 1328-1334). IEEE.

Zheng, Z., Wu, X., Zhang, Y., Lyu, M. R., & Wang, J. (2012). QoS ranking prediction for cloud services. IEEE transactions on parallel and distributed systems, 24(6), 1213-1222.

LIITE 1 HAASTATTELUISSA KÄYTETTY KYSYMYSRUNKO

Haastateltavan taustatiedot

1. Ammattinimike tai työtehtävät
2. Kokemus
    a. Nykyisissä työtehtävissä
    b. organisaatiossa

Tietoturva, tietoturvakäytänteet ja tietoturvatietoisuus

1. Organisaation näkökulma
    1.1. Mitkä ovat oleellisimpia riskejä tietoturvan kannalta organisaatiollesi?
    1.2. Minkälaisia tietoturvakäytänteitä organisaatiossasi on?
    1.3. Miten varmistutaan, että käytänteet ovat työntekijöiden tiedossa ja niitä noudatetaan?
    1.4. Miten organisaatiossasi käsitellään tietoturvaan liittyviä riskejä?
    1.5. Mitä organisaation asettamia tietoturvavaatimuksia sinun tulee huomioida työssäsi?
2. Työntekijän näkökulma
    2.1. Miten organisaatiossasi pidetään huolta työntekijän tietoturvatietoisuudesta?
    2.2. Järjestetäänkö organisaatiossasi tietoturvakoulutuksia?
    2.3. Kuinka tärkeänä koet tietoturvan huomioimisen nykyisessä työssäsi?
    2.4. Miten huomioit organisaatiosi tietoturvakäytänteet työssäsi?

Pilvipalvelut ja tietoturva

1. Minkälaisia pilviratkaisuja hyödynnät työssäsi?
    1.1. Miten käyttämiisi pilvipalveluihin tunnistaudutaan?
    1.2. Millä tasolla koet käyttämiesi pilvipalveluiden tietoturvan?
    1.3. Kuinka tärkeäksi koet käyttämiesi palveluiden tietoturvan?
2. Ovatko käyttämäsi pilvipalvelut hankittu palveluntarjoajan kautta, vai organisaatiosi kehittämiä?
    2.1. Onko käyttäjätuki palveluntarjoajan kautta hankituissa palveluissa palveluntarjoajalla, vai organisaatiollasi?