Tampereen ammattikorkeakoulu

Pilvipalvelut ja niiden tietoturva

Elisa Eskelinen

OPINNÄYTETYÖ
Marraskuu 2022

Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

ESKELINEN, ELISA:
Pilvipalvelut ja niiden tietoturva

Opinnäytetyö 26 sivua, joista liitteitä 2 sivua
Marraskuu 2022

Opinnäytetyössä selvitettiin, mitä pilvipalvelut ovat, miten ne toimivat ja miten tietoturva tulee ottaa huomioon pilvipalveluita tarkasteltaessa. Työssä esitellään pilvipalveluiden yleisimmät palvelu- ja toteutusmallit sekä perehdytään niiden tietoturvaan. Työssä tarkastellaan pilvipalveluiden käyttämisen hyötyjä sekä palveluiden käyttöön liittyviä riskejä ja ongelmia.

Työssä koottiin pilvipalveluiden rakenne selkeäksi kokonaisuudeksi, jotta lukija ymmärtää mitä pilvipalvelut ovat ja mitä ominaisuuksia ne sisältävät. Työ toteutettiin kirjallisuuskatsauksena hyödyntämällä internetartikkeleita ja dokumentaatioita.

Pilvipalveluiden tietoturva on monipuolinen ja monimutkainen asia. Tällä hetkellä ei ole helposti saatavilla suomenkielistä tietopakettia pilvipalveluista. Tämän opinnäytetyön avulla myös ICT-alan ulkopuolella työskentelevät ihmiset saavat selkeän käsityksen pilvipalveluista ja niihin liittyvistä riskeistä. Pilvipalveluiden syvällisempään tutkimiseen voisi käyttää apuna tätä opinnäytetyötä.

Asiasanat: pilvipalvelu, tietoturva

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications and Networks

ESKELINEN, ELISA:
Cloud services and security

Bachelor's thesis 26 pages, appendices 2 pages
November 2022

This thesis explains what cloud services are, how they work and how their security should be considered when viewing at cloud services. The thesis introduces the most common service and deployment models of cloud services and examines their security. The thesis examines the benefits of using cloud services as well as the risks and problems related to the use of services.

The purpose of this thesis was to compile the structure of cloud services into a clear entity. The reader gets a basic understanding what cloud services are and what features they contain. This study was carried out as a literature review using internet articles and documentation.

The cloud security is a versatile and complex matter. Currently there is no easily available information package in Finnish about cloud services. With the help of this thesis, people working outside of the ICT industry will get a clear understanding of cloud services and the risks associated with them. This thesis could be used as a help for a more in-depth study of cloud services.

Key words: cloud service, cloud security

SISÄLLYS

1 JOHDANTO 6
2 PILVIPALVELUT 7
2.1 Mitä tarkoittaa pilvipalvelu? 7
2.2 Missä pilveen tallennettu data on? 8
3 PILVIPALVELUMALLIT 10
3.1 SaaS (Software as a Service) 11
3.2 PaaS (Platform as a Service) 11
3.3 IaaS (Infrastructure as a Service) 12
4 PILVIPALVELUJEN TOTEUTUSMALLIT JA NIIDEN TURVALLISUUS 13
4.1 Yksityinen pilvi 13
4.2 Julkinen pilvi 14
4.3 Hybridipilvi 14
4.4 Yhteisöpilvi 15
5 PILVIPALVELUIDEN TIETOTURVA 16
5.1 Käyttäjähallinnan luotettavuus 17
5.2 Henkilöstöturvallisuus ja käyttäjät 18
5.3 Maantieteellinen sijainti ja fyysinen turva 19
6 MUITA PILVIPALVELUIDEN OMINAISUUKSIA 21
6.1 Pilvipalveluiden hyviä ominaisuuksia 21
6.2 Pilvipalveluiden huonoja ominaisuuksia 21
7 KUINKA KÄYTTÄJÄ VOI PARANTAA TIETOTURVAA 22
8 POHDINTA 23
LÄHTEET 24
LIITTEET 25
Liite 1. IP-02 Käyttäjätunnistus 25
Liite 2. IP-03 Hallintayhteydet 26

ERITYISSANASTO

FaaS	Functions as a Service eli funktioiden ajoalusta palveluna, palvelimeton tietojenkäsittely. Pilvipalvelumalli, jossa palveluntarjoaja vastaa resurssien allokoinnista.
IaaS	Infrastructure as a Service eli infrastruktuuri palveluna. Asiakas saa palveluntuottajalta tietokoneiden laskentatehoa, tallennustilaa ja verkkoyhteyksiä.
MFA	Multi-Factor Authentication eli monivaiheinen todennus. Käyttäjän identiteetti varmistetaan useampaa eri tunnistustapaa käyttämällä.
NIST	National Institute of Standards and Technology eli Yhdysvaltain standardisointi- ja teknologiainstituutti. Virasto kehittää mittaustekniikoita, standardeja ja tekniikkaa.
PaaS	Platform as a Service eli sovellusalusta palveluna. Asiakas saa palveluntuottajalta käyttöönsä valmiin apuohjelmien ja sovelluskehitysympäristön kokonaisuuden.
PiTuKri	Pilvipalveluiden turvallisuuden arviointikriteeristö, tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin.
SaaS	Software as a Service eli ohjelmisto palveluna. Palveluntarjoaja ylläpitää ohjelmistoa. Esimerkiksi M365-palvelut ja Gmail.

1 JOHDANTO

Pilvipalvelut ovat nykyaikaa. Ne ovat ainakin jossain määrin käytössä lähes jokaisessa tietotekniikkaa käyttävässä yrityksessä ja organisaatiossa. Koronapandemian takia jouduttiin muodostamaan nopealla aikataululla uusia työtapoja, mikä joudutti digitalisaation kehitystä. Digitalisaatio työelämässä tarkoittaa toimintatapojen tai prosessien muuttamista teknologiaa (big data, mobiiliteknologia, pilvipalvelut, robotiikka, IoT) hyödyntämällä. Yhä useammat organisaatiot ja yritykset harkitsevat lähes kokonaan pilvipalveluihin siirtymistä. Uusiin toimintatapoihin ja teknologioihin täytyy investoida. Erityisesti työntekijöiden osaamiseen tulisi kiinnittää huomiota nopean muutoksen vuoksi.

Tämä opinnäytetyö esittelee pilvipalvelut ja käsittelee niiden tietoturvaa yleisellä tasolla. Opinnäytetyössä käydään läpi pilvipalvelut yleisesti; selitetään pilvipalvelumallit ja pilvipalvelutyypit.

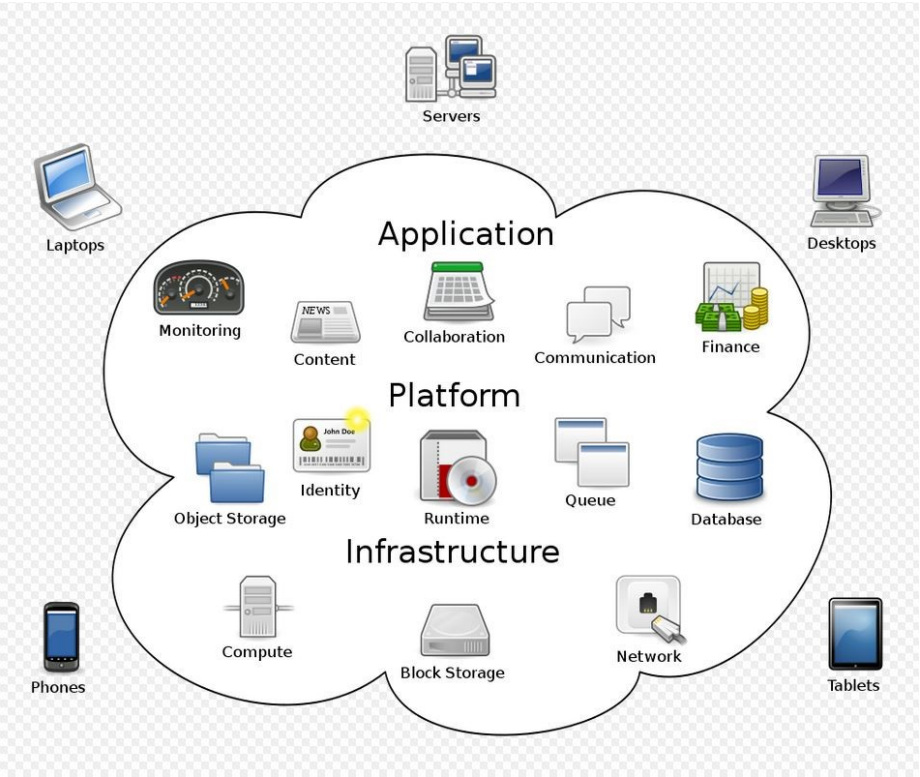
Usein pilvipalveluiden tietoturvasta ollaan huolissaan sekä uutisoinnin että pilven abstraktiuden vuoksi. Uutisiin nousee aika ajoin pilviympäristössä tapahtuneista tietoturvauhkista ja identiteettivarkauksista, jotka voivat aiheuttaa huolta niin käyttäjille kuin organisaation tietoturvasta vastaaville. Tämän opinnäytetyön tarkoituksena on selvittää, mitä asioita tulee ottaa huomioon pilvipalveluita tarkasteltaessa.

2 PILVIPALVELUT

Ennen pilvipalveluiden ja niiden tietoturvan syvempää tarkastelua on hyvä tietää, mitä pilvipalvelu oikeastaan tarkoittaa. Lisäksi pilvipalveluiden hahmottamisessa auttaa tieto siitä, missä ne sijaitsevat ja missä tieto säilytetään.

2.1 Mitä tarkoittaa pilvipalvelu?

Pilvipalvelu tarkoittaa palveluiden toteuttamista internetin välityksellä. Pilvipalvelu on kokonaisuus, jossa palvelut sijaitsevat fyysisten palvelinten sijaan skaalautuvalla pilvipalvelimella (Liimatta 2021). Pilvipalveluiden tuottamisessa käytetään jaettujen, skaalautuvien ja joustavien resurssien mallia. Se on osin toteutettu itsepalveluperiaatteella toimivaksi. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.) Palvelut tarjotaan niin, etteivät käyttäjät voi nähdä tai hallita teknistä prosessia. ”Pilvi” (eng. cloud) tulee internetin kuvaamisesta kaavioissa ja kuvaa monimutkaista infrastruktuuria (kuva 1). Tästä käsitteestä ei kuitenkaan pysty päättelemään toteutustapaa.



KUVA 1. Havainnollistava kuva pilvipalveluista (Johnston, 2009).

The National Institute of Standards and Technologyn (NIST) mukaan pilvi koostuu viidestä olennaisesta ominaisuudesta, kolmesta palvelumallista ja neljästä toteutusmallista.

Viisi olennaista ominaisuutta:

- Itsepalvelu tarpeen vaatiessa
- Laaja verkkoon pääsy
- Resurssien yhdistäminen
- Nopea joustavuus
- Palvelun mittaaminen

Kolme palvelumallia:

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Interface as a Service)

Neljä toteutusmallia:

- Yksityinen pilvi
- Julkinen pilvi
- Hybridipilvi
- Yhteisöpilvi

(Mell & Grance 2011.)

2.2 Missä pilveen tallennettu data on?

Pilvipalvelu voi olla vaikeasti ymmärrettäviä käyttäjälle, koska käyttäjä ei voi nähdä tai kokea sitä konkreettisesti. Se on hyvin abstrakti asia, jota on vaikea hahmottaa.

Palveluntarjoajasta riippuen, pilvipalveluun tallennetut tiedot voivat sijaita yhdessä tai useammassa eri paikassa, yhdessä tai useassa eri maassa. Pienemmät toimijat säilyttävät yleensä datan paikallisesti omassa tai ulkoiselta palvelun-

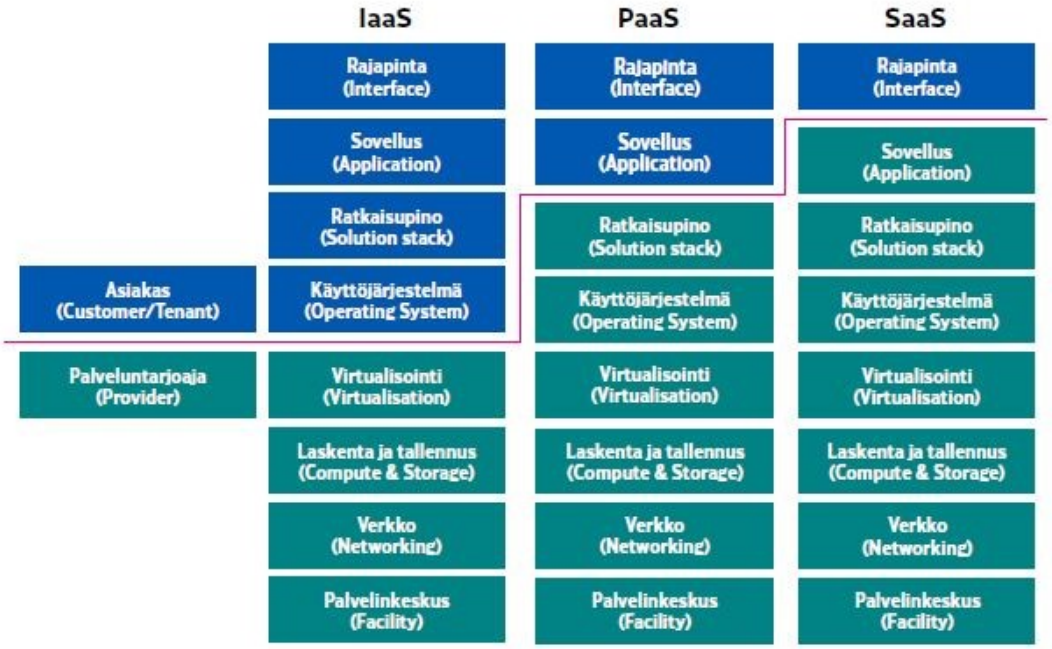
tarjoajalta vuokratussa konesalissa tai palvelinkeskuksessa. Pienemmät palveluntarjoajat saattavat vuokrata resursseja suuremmilta palveluntarjoajilta ja ylläpitää näiden pilvipalveluissa koko palveluaan tai osaa siitä. (Pilvipalveluiden tietoturva organisaatioille N.d.)

Kun puhutaan suuremmista pilvipalveluiden tuottajista, voi heidän konesalinsa tai palvelinkeskuksensa sijaita eri maissa ja eri mantereilla. Käyttäjän on tällöin mahdotonta tietää, missä hänen tietonsa liikkuu tai on tallennettuna. Osa suuremmista palveluntarjoajista pyrkii keskittämään toimintansa maantieteellisesti, esimerkiksi niin, että eurooppalaisen käyttäjän data säilytetään Euroopassa sijaitsevissa palvelinkeskuksissa. Tällöinkin osa käyttäjän tiedoista voi tallentua oman kotialueensa ulkopuolelle, esimerkiksi käyttäjän käyttäessä palvelua eri maanosassa kuin kotialueensa sijaitsee. (Pilvipalveluiden tietoturva organisaatioille N.d.)

3 PILVIPALVELUMALLIT

Pilvipalvelumallien luokitukset kertovat, millä tavalla pilvipalvelu on toteutettu. Palvelumallit kuvaavat perinteisesti vastuunjakoa asiakkaan ja tuottajan välillä sekä palveluiden pääasiallista kohdeyleisöä. Nykyään pilvipalveluiden nopean kehityksen vuoksi palvelumallit ovat muovaantuneet ja perinteiset mallien rajat ovat rikkoontuneet. (Liimatta 2021.) Pilvipalvelumallit jakaantuvat perinteisesti kolmeen pääluokkaan, joiden lisäksi on myös muita palvelumalleja, esimerkiksi FaaS (Serverless computing tai Function-as-a-service).

Turvallisuuteen ja ylläpitoon liittyvässä vastuunjaossa puhutaan niin sanotusta jaetusta vastuusta, jossa on määritelty vastuu asiakkaan ja tuottajan välillä (Nuojua 2021). Pilvipalvelumalleissa vastuun jakautuminen riippuu palvelumallista ja palvelutoteutuksen yksityiskohdista (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020). Tyypillistä vastuunjakoa tuottajan ja asiakkaan välillä on havainnollistanut Kyberturvallisuuskeskus ja Traficom (kuva 2).



KUVA 2. Tyypillinen vastuunjakomalli (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020).

Pilvipalvelutarjoaja vastaa alustan turvallisuudesta; datakeskusteknologian tarjoajien valitsemisesta ja tarkastamisesta, palvelinkeskusten fyysisen turvallisuuden

varmistamisesta, palvelinkeskusten välillä siirrettävien tietojen salauksesta ja palveluntarjoajan natiivisovellusten turvallisuuden varmistamisesta. (Nuojua 2021.)

3.1 SaaS (Software as a Service)

SaaS-mallissa asiakas saa palveluntuottajalta verkon yli käytettäviä ohjelmistoja käyttöönsä (Pilvipalveluiden tietoturva organisaatioille N.d.). Palveluntarjoaja tuottaa palvelut kokonaan (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020). Palveluntarjoajan vastuulla on siis ohjelmiston kehittäminen, ylläpito ja päivittäminen. Tämä on yleisin käytössä oleva pilvipalvelumalli. Tyypillisiä tällaisia palveluita ovat verkkoselaimella käytettävät toimisto-ohjelmistot ja tallennussovellukset (Pilvipalveluiden tietoturva organisaatioille N.d).

Palvelumallin ominaisuudet:

- Yksinkertaisinta ottaa käyttöön (Pilvipalveluiden tietoturva organisaatioille N.d.)
- Säästää aikaa ja rahaa (IaaS, PaaS and SaaS cloud service models 2022)
- Jatkuva päivittyminen ja käyttäjäkokemuksen suunnittelu (IaaS, PaaS and SaaS cloud service models 2022)
- Asiakkaalla ei ole niin paljon vaikutusvaltaa palvelun toteutukseen (Pilvipalveluiden tietoturva organisaatioille N.d.)
- Tietoturvariskit (IaaS, PaaS and SaaS cloud service models 2022)

3.2 PaaS (Platform as a Service)

PaaS:ssa asiakas saa palveluntuottajalta valmiin apuohjelmien ja sovelluskehitysympäristön kokonaisuuden käyttöönsä. Asiakas voi toteuttaa sen päälle omat ohjelmistonsa ja tietoturvaratkaisunsa. Asiakas ei kuitenkaan voi vaikuttaa tietojärjestelmien käyttöjärjestelmiin. (Pilvipalveluiden tietoturva organisaatioille N.d.) Jos käyttöjärjestelmässä tai laitteistoissa on ongelma, asiakas ei voi hallita sen vaikutusta ohjelman suorituskykyyn (IaaS, PaaS and SaaS cloud service models 2022).

Palvelumallin ominaisuudet:

- Kustannustehokas sovellusten kehitys, testaus ja käyttöönotto
- Nopea innovaatio
- Tietoturvariskit
- Integraatio- ja yhteensopivuusongelmat
- Toiminnalliset rajoitukset

(IaaS, PaaS and SaaS cloud service models 2022.)

3.3 IaaS (Infrastructure as a Service)

IaaS:ssa asiakas saa palveluntuottajalta tietokoneiden laskentatehoa, tallennustilaa ja verkkoyhteyksiä. Asiakas voi valita tai toteuttaa ohjelmistot ja loogiset yhteydet itse. Tämä palvelumalli antaa eniten vapauksia ja vastuuta asiakkaalle. (Pilvipalveluiden tietoturva organisaatioille N.d.) Asiakkaan vastuulla on esimerkiksi pääsynhallinta, salaus ja verkkoliikenteen suojaus. Asiakkaan ei tarvitse tehdä merkittäviä pääomasijoituksia laitteistoihin. (IaaS, PaaS and SaaS cloud service models 2022.).

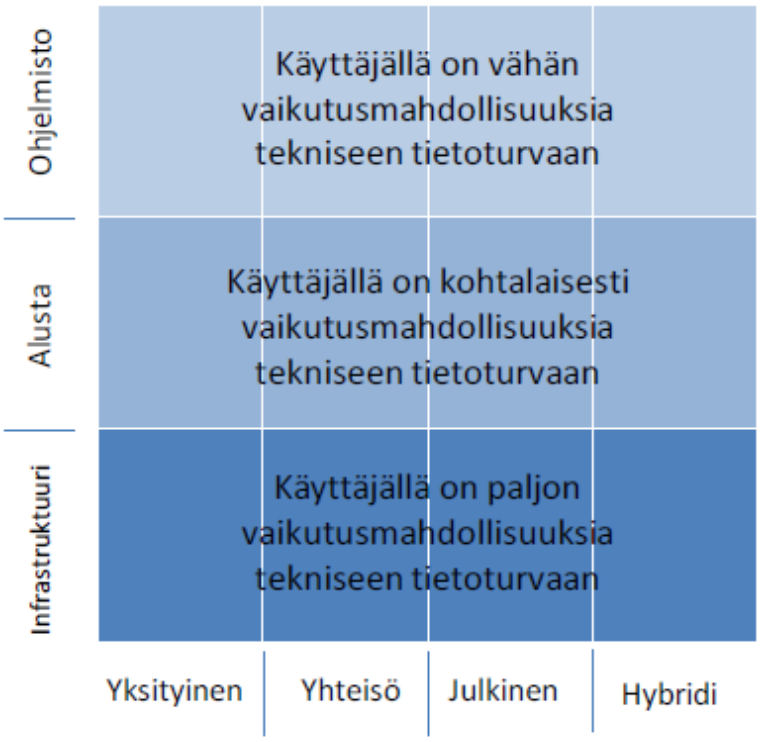
Palvelumallin ominaisuudet:

- Infrastruktuurin hallinta asiakkaalla
- Resurssien osto tarpeen mukaan ilman suuria laitteistohankintoja
- Automaatio ja skaalautuvuus
- Hallinnan ja ympäristöjen yhteen toimivuuden ongelma

(IaaS, PaaS and SaaS cloud service models 2022.)

4 PILVIPALVELUJEN TOTEUTUSMALLIT JA NIIDEN TURVALLISUUS

Pilvipalveluiden yleisimmät toteutusmallit jaetaan yksityiseen pilveen, julkiseen pilveen ja hybridipilveen. Nämä yleisimmät mallit toimivat yleensä pohjana muille toteutusmalleille, kuten yhteisöpilvien (eng. community cloud) pohjana. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.) Eri lähteistä riippuen näitä kuvaillaan joko toteutusmalleiksi tai hankintamalleiksi. Tässä opinnäytetyössä käytetään termiä toteutusmalli. Kuvassa 3 on esitetty yleisimmät palvelu- ja toteutusmallit. Palvelumallit vasemmalla ja toteutusmallit alhaalla.



KUVA 3. Pilvipalveluiden toteutusmallit (Pilvipalveluiden tietoturva organisaatioille N.d.)

4.1 Yksityinen pilvi

Yksityinen pilvipalvelu (eng. private cloud) on nimensä mukaisesti tarkoitettu yhdelle organisaatiolle ja sijaitsee yksityisessä verkossa. Tällaisen toteutusmallin voi organisaatio tehdä itse tai ulkoistaa kumppanille. Yksityisen pilvipalvelun voi toteuttaa virtuaalisena, jolloin ympäristö eriytetään loogisesti jaetusta fyysisestä

infrastruktuurista ja se voidaan yhdistää organisaation yksityiseen verkkoon. (Liimatta 2021.)

Yksityisen pilven vahvuus on pilvipalveluinfrastruktuurin ja siinä käsiteltävien tietojen fyysisen ja loogisen tason luotettava erottelu muista tietojenkäsittely-ympäristöistä, käyttäjäorganisaatioista ja ulkoisista toimijoista. Tällä toteutusmallilla pystytään toteuttamaan korkeamman turvatason palveluja kuin muilla malleilla. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.)

4.2 Julkinen pilvi

Julkinen pilvipalvelu (eng. public cloud) on toteutusmalli, jossa pilvipalvelut ovat julkisesti tarjolla kenelle tahansa (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020). Tässä toteutusmallissa palveluiden omistaja ja hallinnoija on lähes poikkeuksetta pilvipalveluiden tuottaja. Julkisten pilvipalveluiden tarjoamia vaihtoehtoja on paljon erilaisiin tarpeisiin. Esimerkiksi Microsoft Azure ja Google Cloud Platform ovat tällaisia pilvipalveluympäristöjä. (Liimatta 2021.)

Julkiseen pilven infrastruktuuriin ja dataan kohdistuu suurempi hyökkäysriski kuin yksityiseen pilveen. Riski on suurempi muun muassa muiden käyttäjien tai ulkoisten toimijoiden vuoksi. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.)

4.3 Hybridipilvi

Hybridipilvi eli yhdistelmäpilvi (eng. hybrid cloud) on toteutusmalli, jossa käytetään yksityistä ja julkista pilveä. Tässä toteutusmallissa yksityinen ja julkinen pilvi säilytetään erillisinä. Hybridipilvessä on tärkeää selvittää käyttötarkoitus, koska hybridipilviratkaisut ovat teknologia- ja pilvipalvelutoimittajakohtaisia sen rajallisen standardoinnin vuoksi. (Liimatta 2021.)

Hybridipilven turvataso riippuu siitä, onko datan mahdollista siirtyä julkisen pilven puolelle sekä siitä, kuinka turvallisuus on järjestetty pilvitoteutusten rajapinnoissa (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020).

4.4 Yhteisöpilvi

Yhteisöpilvi (eng. community cloud) on toteutusmalli, joka on tarkoitettu joukolle käyttäjiä tai organisaatioita, joilla on samat tarpeet. Samoja tarpeita voivat olla esimerkiksi turvallisuusvaatimukset, käyttöehdot ja yrityksen missio. Sen voi omistaa yksi tai useampi yhteisön organisaatio, kolmas osapuoli tai jonkinlainen yhdistelmä niistä. Se voi sijaita omissa toimitiloissa tai sen ulkopuolella. (Mell & Grance 2011.)

Yhteisöpilven turvataso on parempi kuin julkisessa pilvessä, mutta huonompi kuin yksityisessä pilvessä (Community Cloud. N.d.). Turvataso riippuu siitä, kuinka yhteisöpilvi on toteutettu.

5 PILVIPALVELUIDEN TIETOTURVA

Pilvipalveluiden tietoturva perustuu luottamukseen asiakkaan ja palvelun tarjoajan välillä. Pilvipalvelutarjoajan tavoite on saada organisaatiot ja yksityiset ihmiset luottamaan siihen, että tarjottua palvelua on turvallista käyttää. Pilvipalveluiden toteutus vaatii aivan erilaista lähestymistä tietoturvaan, kuin perinteisen ympäristön suojaaminen, koska pilvipalveluiden arkkitehtuuri on täysin erilainen. Pilvipalveluissa tietoturvan vastuu on jaettu asiakkaan ja pilvipalveluntuottajan välille. (Wallenius 2022.)

Palveluntarjoajia on erilaisia ja niihin kohdistuu erilaiset riskit. Palveluntarjoajat voidaan jakaa luokkiin; organisaatio itse, kansallinen viranomainen/julkinen toimija, kansallinen yksityinen toimija, monikansallinen viranomainen/julkinen toimija (esim. EU-maiden viranomaisyhteisö), ei-kansallinen yksityinen toimija (EU- tai ETA-alue) tai muiden maiden ei-kansallinen yksityinen toimija. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.)

Kyberturvallisuuskeskus ja Traficom ovat luoneet Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri), jolla voidaan selvittää pilvipalveluiden turvallisuutta. PiTuKri on kehitetty edistämään viranomaisten pilvipalveluissa sijaitsevan salassa pidettävän datan turvallisuutta. Se on tehty Suomen kansallisten tarpeiden näkökulmasta. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.)

Erilaisiin tietotyyppeihin kohdistuu erilaiset riskit. Esimerkiksi turvallisuusluokitellut tiedot ovat valtion turvallisuuden, yleisen edun mukaan suojattava. Näihin tietoihin voidaan olettaa kohdistuvan enemmän mielenkiintoa kuin turvallisuusluokittelemattomiin tietoihin. PiTuKrissa tietotyypit on jaoteltu suojaustarpeen mukaisiin luokkiin (taulukko 1). (Pilvipalveluiden turvallisuuden arviointikriteeristö, 2020.)

Taulukko 1. Tietotyypit (Pitukri s.8)

Tietotyyppi	Kuvaus
Julkinen	Julkinen tieto. Suojaamistarpeet tyypillisesti eheyden ja saatavuuden näkökulmista.
Salassa pidettävä	Viranomaisen kansallinen salassa pidettävä tieto, jota ei ole turvallisuusluokiteltu. Useimmat viranomaisten salassa pidettävät tiedot sisältävät henkilötietoja, ja ovat siten myös henkilötietoihin liittyvän erityislainsäädännön piirissä, vrt. tietotyyppi "Henkilötieto".
Henkilötieto	Henkilötietojen suojaamiseen liittyvän erityislainsäädännön (ml. tietosuojalaki[16], laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä[17], sekä EU:n yleinen tietosuoja-asetus[18]) alaiset tiedot.
Varautumisen näkökulmasta suojattavat tiedot	Tietoon kohdistuu tarve olla käytettävissä myös poikkeavissa olosuhteissa (varautuminen). Poikkeavilla olosuhteilla tarkoitetaan tässä tilannetta, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle.
TL IV	Viranomaisen kansalliset turvallisuusluokitellut IV-luokan salassa pidettävät tiedot. Suojaamistarve yleensä valtion turvallisuuden (yleisen edun) näkökulmasta. Suojaamisessa huomioitava myös lainsäädäntöjohdannaiset riskit[19].
Kansainvälinen RESTRICTED (KV-R)	RESTRICTED ja muut vastaavan tason kansainväliset turvallisuusluokitellut erityissuojattavat tieto-aineistot. Esimerkiksi vieraiden valtioiden ja kansainvälisten järjestöjen kanssa tehtyjen kahden- ja monenvälisten sopimusten[20] piiriin kuuluvat RESTRICTED-tason tiedot. Suojaamistarve yleensä yhden tai useamman valtion turvallisuuden (yleisen edun) näkökulmasta. Suojaamisessa huomioitava lainsäädäntöjohdannaiset riskit sekä kyseiseen tietoon kohdistuvat tiedon originaattorin tai/ja omistajan asettamat erityisvaatimukset[21].
Suuri määrä salassa pidettävää tai/ja henkilötietoa (TL IV tai TL III -kasauma)	Tilanteet, joissa kasautumisvaikutuksen arvioidaan[22] muodostavan turvallisuusluokitellun IV- tai III-tason tietovarannon. Esimerkiksi osa Suomen kriittisen infrastuktuurin ylläpitoon osallistuvien yritysten liikesalaisuuksista voi olla yksittäisinä tietoina salassa pidettäviä[23], mutta usean yrityksen muodostaman huoltovarmuuskriittisen kokonaisuuden kattavana kasaumana myös turvallisuusluokiteltuja[24] III-luokan salassa pidettäviä tietoja.
Suuri määrä TL IV -tietoa (TL III -kasauma)	Tilanteet, joissa kasautumisvaikutuksen arvioidaan muodostavan turvallisuusluokan III tietovarannon. Esimerkiksi valtionhallinnolle suunnattu yhteisöpilvi, johon kasautuu merkittävä määrä useiden viranomaisten turvallisuusluokan IV tietoa myös siten, että tietoja yhdistelemällä on muodostettavissa turvallisuusluokan III tietovaranto.
TL III ja II	Viranomaisen kansalliset turvallisuusluokan III tai/ja II tiedot. Suojaamistarve yleensä valtion turvallisuuden (yleisen edun) näkökulmasta. Suojaamisessa huomioitava myös lainsäädäntöjohdannaiset riskit.

5.1 Käyttäjähallinnan luotettavuus

Yksi tärkeimmistä pilvipalveluiden turvallisuuteen vaikuttavista tekijöistä on käyttäjähallinnan luotettavuus. Se pitää sisällään palveluun rekisteröinnin, rekisteröidyn käyttäjän tunnistamisen ja käyttöoikeuksien hallinnoinnin. Tämän tehtävänä on jakaa palvelun ja tiedon käyttöoikeudet niille, joille se kuuluu ja estää se muilta. (Pilvipalveluiden tietoturva organisaatioille N.d.) PiTuKri:ssa on jaoteltu käyttäjähallinta kolmeen eri osioon; käyttöoikeushallinta, käyttäjätunnistus ja hallintayhteydet.

Käyttöoikeushallinnan tavoite on varmistaa, että ainoastaan oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja suojattavaan tietoon. Käyttäjätunnukset myönnetään ja luovutetaan vain niille, joilla on niihin oikeus ja tarve ja ne

on rajattu vain välttämättömiin toiminnallisuuksiin, sovelluksiin, laitteisiin ja verkkoihin. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.)

Käyttäjätunnistuksen tavoite on rajata vain valtuutettujen käyttäjien pääsy tietoihin ja palveluihin. Tämä voidaan järjestää luotettavasti huolehtimalla, että todennusmenetelmä on suojattu välimieshyökkäyksiltä, tarpeetonta tietoa ei paljasteta sisäänkirjautuessa, todennuskredentiaalit ovat salatussa muodossa ja ne lähetetään verkon yli, todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä ja brute force -hyökkäyksiä vastaan. (Liite 1.)

Viimeisen PiTuKri:ssa käyttäjähallintaan liittyvän osion tavoite on, että hallintayhteydet on suojattu riittävästi, jotta niitä hyödyntämällä asiakastietoihin tai pilvipalveluun ei pääse valtuuttamattomana. Hallintayhteyksiä arvioitaessa olisi otettava huomioon erityisesti, miten hallintayhteyden kautta vaarannetaan pilvipalvelussa käytettävät tiedot. (Liite 2.)

5.2 Henkilöstöturvallisuus ja käyttäjät

Pilvipalveluita tarkasteltaessa on tärkeää tutkia, millainen henkilöstöpolitiikka palveluntarjoajalla on. On tärkeää selvittää, millaiset turvallisuusselvitykset henkilöille tehdään ja seurataanko käytännön työssä alan standardeja. Myös palveluntarjoajan käyttämillä alihankintaketjuilla ja niiden työntekijöillä tulisi olla sama turvallisuustaso. (Pilvipalveluiden tietoturva organisaatioille N.d.)

PiTukRi:ssa on määritelty henkilöstöturvallisuus viiteen eri osa-alueeseen:

1. Työsuhteen elinkaaren huomioimiseen
2. Henkilöstön luotettavuuden arviointiin
3. Salassapito- ja vaitiolositoumuksiin
4. Turvallisuustietoisuuteen sekä tiedonsaantitarpeisiin
5. Tehtävien erotteluun

Organisaation tulisi pienentää henkilöstöön ja sen luotettavuuteen liittyvät riskit koko työsuhteen aikana. Luotettavuuden parantamiseksi tulisi erityisesti lisätä tie-

toisuutta ja varmistaa asianmukaisilla ohjeistuksilla, että henkilöstö pystyy toimimaan käytännössäkin turvallisesti. Lisäksi on varmistettava, että salassa pidettävä tieto päätyy vain valtuutetuille henkilöille tiedonsaantitarpeen mukaisesti ja näin vähennetään tietoon liittyviä riskejä. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.)

Käyttäjät voivat olla suuri tietoturvariski. Siksi käyttäjät on ohjeistettava käyttämään pilvipalveluita turvallisesti. Käyttäjien on turvattava turvallisuus sekä oman päätelaitteen että internetpalvelun käytön suhteen. Organisaation on varmistettava, että pilvipalveluiden käyttäjät saavat riittävän ohjeistuksen pilvipalvelun käyttöön liittyviin rajauksiin. Käyttäjien tulee siis tietää, mitä tietoa palveluun saa tallentaa, mihin sitä tietoa saa käyttää ja missä käyttöympäristössä tai millä laitteella palvelua saa käyttää. (Pilvipalveluiden tietoturva organisaatioille N.d.)

Yksi tietoturvariski on käyttäjän päässä tapahtuva riittämätön salasanakäytäntö. Tavallisin puute on salasanan lyhyys. Toinen merkittävä salasanaan liittyvä tietoturvaongelma on saman salasanan käyttäminen monessa eri palvelussa. Eri salasanan käyttö eri palveluissa turvaa sen, ettei kaikkien palveluiden tiedot päädy vääriin käsiin, jos yksi palvelu vaarantuu. (Pilvipalveluiden suojaaminen 2019.)

5.3 Maantieteellinen sijainti ja fyysinen turva

Tietoturvaan vaikuttaa palveluntuottajien maantieteellinen sijainti; datan käsittely ja säilytys sekä ylläpito- ja hallintotoimet voivat sijaita eri sijainneissa. Sijainteihin voi liittyä riskejä esimerkiksi lainsäädännön vuoksi. Kyberturvallisuuskeskus ja Traficom määrittelee turvallisuuden näkökulmasta sijainnit Suomeen, tietosuojasääntelyn mahdollistamat alueisiin (usein esimerkiksi EU- tai ETA-alueet) ja muihin maihin. Lisäksi mailla ja organisaatioilla voi olla erilaisia sopimuksia, jotka vaikuttavat sijaintiin liittyviin riskeihin. (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020.)

Pilvipalvelun fyysinen turvallisuus on varmistettava kulunvalvonnalla niin, että vain asianomaiset henkilöt saavat pääsyn alueelle, jolloin palvelu suojataan ilki-

vallalta ja muilta vahingoilta. Sähkönjakelun keskeytyksiin ja verkkoliikenteen katkeamisiin on varauduttava varavoimalla ja kahdella eri tietoliikenneyhteydellä. Palvelut voidaan kahdentaa, jolloin palvelua voidaan edelleen tarjota, jos koko palvelinkeskuksen toiminta keskeytyy. (Pilvipalveluiden tietoturva organisaatioille N.d.)

PiTuKri:ssa on jaoteltu fyysinen turvallisuus viiteen osa-alueeseen:

1. Monitasoiseen suojaamiseen ja riskienhallintaan
2. Rakenteisiin ja turvallisuusjärjestelmiin
3. Luvattoman pääsyn estämiseen
4. Palveluntuottajiin ja vierailijoihin
5. Varautumiseen ja jatkuvuudenhallintaan

6 MUITA PILVIPALVELUIDEN OMINAISUUKSIA

Kaikkiin pilvipalveluihin liittyy toteutus- ja palvelumalleista riippumatta sekä hyötyjä että ongelmia. Pilvipalveluihin siirtyessä tai sitä miettiessä tulisi tarkastella niitä mahdollisimman laajasti. Seuraavissa kappaleissa käydään läpi pilvipalveluiden hyviä ja huonoja ominaisuuksia.

6.1 Pilvipalveluiden hyviä ominaisuuksia

Pilvipalvelun hyviä puolia on monia. Se on hyvinkin luotettava ja varma tietojen säilytyspaikka. Jos fyysinen varmuuskopio, esimerkiksi tietokone, hajoaa tai se varastetaan, hukkuvat paikallisesti tallennetut datat sen mukana. Jos data on tallennettu pilvipalveluun, säilyy data fyysisen varmuuskopion menetyksestä huolimatta. Dataan pääsee myös käsiksi missä vain, milloin vain.

Pilvipalvelut ovat kustannustehokas ratkaisu. Erillisiä laitteita datan säilömiseen ei tarvitse hankkia. Työntekijöitä tai fyysistä tilaa ei tarvitse lisätä tietojen varmuuskopiointiin ja säilytykseen.

6.2 Pilvipalveluiden huonoja ominaisuuksia

Vaikka pilvipalvelut ovat käteviä ja helppoja datansäilytyspaikkoja, liittyy niihin ongelmiakin. Suurin haitta on se, ettei pilvipalveluita voi käyttää ilman internetyhteyttä. On paikkoja, joissa ei internetiin pääse ja tällöin pilvipalveluissa sijaitseviin tietoihin ei pääse.

Pilvipalveluratkaisuihin muuttaminen organisaatiossa voi olla vaikeaa ja monimutkaista. Lisäksi yksittäiselle työntekijälle voi olla vaikeaa hahmottaa, mitä tallennuspaikkaa on käytettävä; milloin tiedot tallentuvat pilveen, milloin paikallisesti.

7 KUINKA KÄYTTÄJÄ VOI PARANTAA TIETOTURVAA

Nykyhetken etätyöskentelyn lisääntyminen organisaatioissa vaatii pääsyn tiedostoihin organisaation ja yritysten sisäverkon ulkopuolelta. Tietoturvan täytyisi olla yksi tärkeimmistä asioista organisaatioiden siirtyessä pilveen. Pilvipalveluissa tietoturvauhkat kasvavat oman sisäverkon ulkopuolelle ja näin ollen niihin tulisi kiinnittää erityistä huomiota.

Pilvipalveluiden tietoturvaan liittyy myös olennaisesti käyttäjän päässä tapahtuva tietoturvan parantaminen. Yrityksen tulisi varmistaa ja vaatia käyttäjien tietoturvatietoisuus. Käyttäjän omilla pienillä parannuksilla voi huomattavasti parantaa tietoturvaa.

Ensimmäinen vaihe tietoturvan parantamiseen on salasanan vahvuus. Nykyään salasanan pituus on tärkeämpi, kuin monimutkaisuus. Kuitenkin olisi hyvä, jos salasanassa olisi mahdollisimman monta eri merkkiä. Salasanaa tulisi myös vaihtaa mahdollisimman usein, eikä samaa salasanaa tulisi käyttää eri sovelluksissa.

Salasanan lisäksi tulisi aina olla käytössä kaksivaiheinen/monivaiheinen todennus (MFA, Multifactor Authenticator), joka on yleisimmin liitetty puhelinnumeroon, eli tekstiviesti- tai puheluvahvistus. Toinen yleinen tapa käyttää kaksivaiheista todennusta on eri mobiilisovellukset, kuten Microsoft Authenticator yms. MFA parantaa tietoturvaa huomattavasti perinteisen salasanan rinnalla.

Ulkopuolelta tapahtuvien hyökkäysten lisäksi tulisi varmistaa, ettei ulkopuolisilla ole fyysisesti pääsyä käyttäjän laitteille. Kaikilla saman tietokoneen käyttäjillä tulisi olla omat profiilit ja profiilien salasanojen tulisi olla tarpeeksi vahvat, eikä niitä saisi luovuttaa kenellekään toiselle. Kasvojen- tai sormenjälkitunnistuksen käyttöä tulisi käyttää varauksella, jotta ulkopuolinen ihminen ei voi käyttää sitä hyödyksi.

8 POHDINTA

Opinnäytetyön tavoitteena oli selvittää, mitä pilvipalvelut ovat, miten ne toimivat ja miten tietoturva tulee ottaa huomioon pilvipalveluita tarkasteltaessa. Työssä käytiin läpi pilvipalveluiden yleisimmät palvelu- ja toteutusmallit sekä niiden tietoturvaa yleisellä tasolla. Opinnäytetyön aihe tuli Tampereen ammattikorkeakoululta.

Opinnäytetyön aihe oli hyvin laaja ja aiheen rajaaminen haastavaa. Siksi opinnäytetyössä käytiin läpi vain yleisimmät toteutusmallit. Tietoa löytyi kattavasti, mutta tiedon luotettavuutta tuli harkita ja vertailla. Pilvipalveluita tarjoavilla yrityksillä on paljon tietoa internetsivuillaan, mutta niiden käyttöä lähteenä halusin vältellä. Ne keskittyivät suurilta osin johonkin tiettyyn palveluun, jota ne tarjoavat ja tietenkin mainostivat palveluaan. Lisäksi tietoa oli saatavilla erilaisista blogeista ja niissä piti tarkastella kirjoittajan näkökulmaa aiheeseen. Kuitenkin aika vähän suomenkielistä ja selkeästi selitettyä, voittoa tavoittelematonta tietoa oli saatavilla.

Pilvipalvelut ovat joustava ja hyvä tapa toteuttaa skaalautuvia palveluita paikasta riippumatta. Ne ovat joustava mahdollisuus yrityksille etätyön lisäännyttyä. Työntekijöiden on mahdollista tehdä töitä lähes mistä vaan. Omien kokemuksien mukaan pilvipalveluihin suhtaudutaan varauksella, mikä saattaa johtua siitä, ettei pilvipalveluiden rakennetta ymmärretä täysin. Pilvipalveluiden kokonaisuutta on hankalaa ymmärtää, jos asiaan ei ole perehtynyt. Lisäksi uutisointi tietoturvavuodoista lisää ihmisten jännitteitä pilvipalveluita kohtaan.

Mielenkiinto aihetta kohtaan kasvoi työtä tehdessä, kun alkoi tarkkailemaan ihmisten asenteita tarkemmin. Pilvipalveluihin siirryttäessä yksittäisten käyttäjien/työntekijöiden tietoisuutta palveluita kohtaan pitäisi kasvattaa. Organisaatioissa saattaa olla epäselvää, millainen data voidaan tallettaa pilvipalveluihin.

LÄHTEET

Community Cloud. N.d. JavaTPoint. Verkkosivu. Viitattu 12.6.2022. https://www.javatpoint.com/community-cloud

IaaS, PaaS and SaaS cloud service models. 2022. Stackscale. Verkkosivu. Viitattu 7.6.2022. https://www.stackscale.com/blog/cloud-service-models/

Liimatta, A. 2021. Pilvipalvelut: tiedä tärkeimmät termit. Tietoevry. Verkkosivu. Viitattu 15.6.2022. https://www.tietoevry.com/fi/blogi/2021/05/pilvipalvelut-tieda-tarkeimmat-termit/

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Viitattu 8.6.2022. https://csrc.nist.gov/publications/detail/sp/800-145/final

Wallenius, N. 2022. Miten pilvipalvelun tietoturva eroaa perinteisestä tietoturvasta. Niklas Wallenius. Verkkosivu. Viitattu 12.6.2022. https://niklaswallenius.fi/pilvipalvelun-tietoturva-erilainen/

Nuojua, P. 2021. Mitä sinun tulee ymmärtää jaetun vastuun mallista pilvipalveluiden tietoturvassa? F-Secure. Verkkosivu. Viitattu 15.6.2022. https://blog.f-secure.com/fi/mita-sinun-tulee-ymmartaa-jaetun-vastuun-mallista-pilvipalveluiden-tietoturvassa/

Pilvipalveluiden suojaaminen. 2019. Bittiguru. Verkkosivu. Viitattu 12.6.2022. https://www.bittiguru.fi/artikkelit/tietoturva/pilvipalveluiden-suojaaminen/

Pilvipalveluiden tietoturva organisaatioille. N.d. Kyberturvallisuuskeskus. PDF-tiedosto. Viitattu 7.6.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Pilvipalveluiden turvallisuuden arviointikriteeristö. 2020. Kyberturvallisuuskeskus. PDF-tiedosto. Viitattu 7.6.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

LIITTEET

Liite 1. IP-02 Käyttäjätunnistus

(Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)

IP-02	Käyttäjätunnistus
Vaatimus	1) Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ja asiakkaan ylläpitäjät sekä palvelun käyttäjät tunnistetaan ja todennetaan luotettavasti ennen pääsyä suojattavaan tietoon: a) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet. b) Kaikki käyttäjät tunnistetaan ja todennetaan. c) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti. d) Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin. e) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksiloinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille. f) Käyttäjien todennus tehdään vahvasti, vähintään kahteen tekijään nojautuen (esimerkiksi salasana + token). Yhteys on salattu käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. i. Poikkeuksena tilanne, jossa todennus tehdään fyysisesti suojatun turvallisuusalueen (Vrt. FT-01) sisällä vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, 1. käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, 2. käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. 2) Tilanteissa, joissa yhteys kulkee fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle (esimerkiksi pilvipalveluntarjoajan konesalin ja ylläpidon/asiakkaan päätelaitteen välillä), tieto/tietoliikenne on suojattu viranomaisen hyväksymällä salausratkaisulla. 3) Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ja asiakkaan ylläpitäjien päätelaitteet ja järjestelmät tunnistetaan riittävän luotettavasti ennen pääsyä suojattavaan tietoon.
Soveltuvuus	Verkkolaitteet, palvelimet, tietojärjestelmät sekä työasemat ja muut päätelaitteet.
Tietotyypit	1: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 2-3: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Tietoihin ja palveluihin pääsyn rajaaminen vain valtuutettuihin käyttäjiin.
Lisätietoja	Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen siitä, että 1) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), 2) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, 3) todennuksessa käytettävät tunnistamistiedot (todennuskredentiaalit) ovat aina salatussa muodossa, jos ne lähetetään verkon yli, 4) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, ja 5) todennusmenetelmä on suojattu brute force -hyökkäyksiä vastaan. Tilanteissa, joissa pilvipalveluun tunnistautumisessa hyödynnetään federoitua identiteetinhallintaa, tai/ja identiteetin- ja pääsynhallintajärjestelmiä (organisaation omia tai esimerkiksi pilvipalveluntarjoajan tuottamia), tulee arvioinnissa kiinnittää erityistä huomiota tunnistuspalvelun (Identity Provider, IdP) sekä attribuuttien välitysketjun luotettavuuteen. Salassa pidettävän tiedon käsittelyyn soveltuvat vain sellaiset tunnistuspalvelut, jotka tarjoavat vahvaan ensitunnistamiseen perustuvaa identiteettiä ja joiden attribuuttien välitysketju pystytään toteuttamaan riittävän turvallisesti tunnistukseen nojaavaan palveluun (Relying Party, RP tai Service Provider, SP) asti. Koska salassa pidettävän tiedon suojaus on yleensä suoraan riippuvainen tunnistuspalvelun luotettavuudesta, tunnistuspalvelun turvallisuudesta varmisturinen kuuluu lähes poikkeuksetta osaksi pilvipalvelun turvallisuuden arviointia. Esimerkiksi attribuuttien välityksen salausteknistä suojausta on tyypillisesti perusteltua arvioida samansuuntaisesti kuin kyseessä olevan tietotyypin suojaamiseen sovellettavan salausratkaisun avainten välitystä (vrt. SA-01, SA-02 ja SA-03). Identiteetinhallintamalleista organisaatiokeskeinen (organization-centric identity management) soveltuu yleensä esimerkiksi käyttäjäkeskeistä (user-centric) paremmin salassa pidettävän tiedon suojaamistarpeisiin, joissa on huomioitava myös käyttäjän sidonta tiettyyn organisaatioon sekä turvallisuustoteutuksen luotettavuudesta varmisturinen. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 2. IP-03 Hallintayhteydet

(Pilvipalveluiden turvallisuuden arviointikriteeristö 2020)

IP-03	Hallintayhteydet
Vaatimus	1) Hallintapääsy tapahtuu pilvipalveluympäristössä rajattujen, hallittujen ja valvottujen pisteiden (esimerkiksi hyppykoneet, hallintaportaalit ja vast.) kautta. Hallintapääsyn mahdollistavat pisteet eriytetään toisistaan vähintään siten, että pilvipalveluntarjoajan ja eri asiakkaiden hallintapisteet, sekä niiden kautta saavutettavat palvelut, ovat toisistaan luotettavasti eroteltuna (vrt. JT-03). 2) Hallintapääsy edellyttää vahvaa, vähintään kahteen todennustekijään (esimerkiksi salasana + token) pohjautuvaa käyttäjätunnistusta. 3) Hallintaliikenne on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. 4) Hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (vrt. FT-01) ulkopuolelle viedyt asiakastietoa sisältävät päätelaitteet ja muut tietovälineet (kiintolevyt, USB-muistit ja vastaavat) säilytetään salattuina käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja, tai tietovälineitä ei jätetä valvomatta. Vrt. SA-01 ja FT-01. 5) Viranomaisen turvallisuusluokitellun tiedon hallinta on mahdollista vain kyseisen turvallisuusluokan mukaisilta päätelaitteilta ja ympäristöistä sekä fyysisiltä alueilta (vrt. FT-01). 6) Viranomaisen turvallisuusluokitellun tiedon hallintaan on pääsy vain viranomaisen hyväksymällä menettelyllä salatulla hallintayhteydellä. 7) Turvallisuusluokiteltua tietoa sisältävien päätelaitteiden ja muiden tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) salaus on viranomaisen hyväksymä.
Soveltuvuus	Pilvipalveluympäristön etähallintaan käytettävät järjestelmät, ml. esimerkiksi verkkolaitteet, palvelimet, sekä työasemat ja muut päätelaitteet. Kattaa sekä pilvipalvelualustan, että sen päälle tuotetun asiakasjärjestelmän.
Tietotyypit	1-4: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 5-7: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Hallintayhteydet on suojattu riittävällä tasolla, jotta niitä hyödyntämällä ei ole asiakastietoon tai pilvipalveluun valtuuttamatonta pääsyä.
Lisätietoja	Pilvipalveluympäristöissä etähallinta on yleensä tyypillisin hallintamenettely sekä itse pilvipalvelualustan, että asiakkaan järjestelmien osalta. Etähallinnaksi tulkitaan esimerkiksi pilvipalveluntarjoajan ylläpitotoimet, jotka tapahtuvat fyysisesti suojatun konesaliympäristön ulkopuolelta käsin. Etähallinnaksi tulkitaan myös pilvipalvelun asiakkaan, omalle vastuulleen kuuluvaan järjestelmäosaan kohdistuvat ylläpitotoimet. Hallintayhteyksien suojausten arvioinnissa tulisi huomioida erityisesti se, miltä osin ko. hallintayhteyden kautta pystytään vaarantamaan pilvipalvelussa käsiteltävät tiedot. Useimmat hallintayhteystavat mahdollistavat pääsyn tietoon joko suoraan (esimerkiksi tietokantaylläpito pääsee yleensä tarvittaessa tietokannan sisältöön) tai epäsuoraan (esimerkiksi verkkolaiteylläpito pystyy yleensä muuttamaan tietojärjestelmää suojaavia palomuurisäantöjä). Hallintayhteyksiin tulkitaan kuuluvaksi lähtökohtaisesti kaikki yhteystavat, joilla on mahdollista vaikuttaa salassa pidettävien tietojen suojauksiin. Hallintayhteyksiin kuuluvat tyypillisesti myös pilvipalvelun asiakkaalle tarjottavat web-konsolit/-portaalit ja vastaavat etähallintayhteydet. Erityisesti tilanteissa, joissa hallintayhteys mahdollistaa suoran tai epäsuoran pääsyn salassa pidettävään tietoon, tulee hallintayhteys ja siihen käytettävät päätelaitteet rajata lähtökohtaisesti samalle suojaus-/turvatasolle, kuin mitä ko. tietojenkäsittely-ympäristökin. Turvallisuusluokitellun tiedon käsittelyyn käytetyn ympäristön hallinta ei lähtökohtaisesti ole hallintaliikenteen turvallisuuskriittisesta luonteesta johtuen mahdollista heikommin suojatuista ympäristöistä tai päätelaitteista käsin. Turvallisuusluokiteltua tietoa sisältävän pilvipalvelualustan hallinnointi tuleekin rajata kyseisen turvallisuusluokan vaatimukset täyttäviin päätelaitteisiin. Huomioitava, että myös päätelaitteiden hallinnointiratkaisujen ja muiden niihin kytkeytyvien taustajärjestelmien tulee täyttää kyseisen turvallisuusluokan vaatimukset, kuten myös fyysiset tilat/alueet, joista hallintaa suoritaan. Päätelaitteiden ja niihin kytkeytyvien taustajärjestelmien (esimerkiksi hakemisto- ja hallintapalvelut) suojaamisessa tulee huomioida erityisesti TT-01 (Tietoliikenneverkon rakenne), IP-01 (Käyttöoikeushallinta), IP-02 (Käyttäjätunnistus), IP-03 (Hallintayhteydet), JT-01 (Jäljitettävyys ja havainnointikyky), JT-02 (Järjestelmäkovennus), JT-04 (Haittaohjelmasuojaus), JT-05 (Suojattavien kohteiden siirtäminen ja poistaminen), SA-01 (Salauskäytännöt ja avainhallinta), SA-02 (Salaus fyysisesti suojatun turvallisuusalueen ulkopuolella), KT-04 (Haavoittuvuuksien hallinta) ja MH-01 (Muutostenhallinta) ja SI-02 (Tieto-aineistojen tuhoaminen). Päätelaitteiden ja niihin kytkeytyvien taustajärjestelmien suojaamisessa ja suojaamisen arvioinnissa voidaan hyödyntää myös Katakri 2015 -viitekehystä. Kasautumisvaikutuksen seurauksena turvallisuusluokan III tietovarantojen hallintaratkaisuissa tulee lisäksi erityisesti huomioida, että hallintaan käytettävät päätelaitteet ovat luotettavasti eroteltuja Internet-kytkentäisistä verkoista. Riittävän jäljitettävyyden toteuttamisessa voidaan hyödyntää esimerkiksi niin sanottua hyppykonekäytäntöä, jossa kaikki hallintatoimet toteutetaan ja kirjataan (lokitetaan) hyppykoneen kautta. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.