Tampereen ammattikorkeakoulu

Pilvipalvelut ja tietoturva

Elväs Santeri

OPINNÄYTETYÖ
Kesäkuu 2022

Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

ELVÄS, SANTERI:
Pilvipalvelut ja tietoturva

Opinnäytetyö 75 sivua, joista liitteitä 29 sivua
Kesäkuu 2022

Opinnäytetyössä tutkittiin pilvipalveluita ja niiden tietoturvaa sekä miksi viedä tietoa pilveen. Tämän lisäksi käytiin läpi yleisimmät pilvipalveluntarjoajat. Työn tavoitteena oli tehdä lukijalle selväksi mitä ovat pilvipalvelut, kuinka ne toimivat ja mitä tulee pohtia pilvipalvelua valitessaan.

Opinnäytetyössä perehdytään pilvipalvelun määritelmään, joka sisältää pääluokat ja pilvityypit, tiedon pilveen viennin hyviin ja huonoihin puoliin sekä millainen rooli on pilven sijainnilla. Tämän lisäksi opinnäytetyössä perehdytään pilvipalveluiden tietoturvaan, pilvipalveluiden tietoturvan arviointikriteeristöön sekä muutamaan suurimpaan pilvipalveluntarjoajaan.

Opinnäytetyön aineistonkeruumenetelmänä käytettiin internettiartikkeleita pilvipalveluista, palveluntarjoajien dokumentaatiota sekä asiantuntijahaastattelua. Haastattelussa haastateltiin TUNI:n tietoturvapäällikköä. Aineisto analysoitiin aineistolähtöisellä sisällönanalyysillä.

Opinnäytetyön tuloksena on kokoelma tietoa, jonka myötä lukija saa yleisymmärryksen pilvipalveluista, niiden tietoturvasta sekä mihinkä asioihin kannattaa kiinnittää huomiota pilvipalvelua valitessaan. Tulokset osoittivat, että pilvipalveluiden käyttö voi usein olla kannattavaa. Palveluiden skaalautuvuus mahdollistaa käytön minkä tahansa kokoisille käyttäjille ja suurien tietoturvaresurssien vuoksi tietoturva on usein parempi.

Opinnäytetyön pohjalta voitaisiin tehdä jatkotutkimusta pilvipalveluiden tarkemmista osa-alueista kuten esimerkiksi järjestelmäkehityksen vaikutuksesta tietoturvaan.

Asiasanat: pilvipalvelu, tietoturva, skaalautuvuus

ABSTRACT

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

ELVÄS, SANTERI:
Cloud Computing and Cyber Security

Bachelor's thesis 75 pages, appendices 29 pages
June 2022

This thesis gathers information on cloud computing, cloud computing cyber security and reasons why data should be moved to the cloud. Additionally, it also examines the most common cloud computing providers. The goal of the thesis was to make it clear to the reader what cloud computing is, how it works and what should be considered when choosing one.

The study aimed to shed light on the definition of cloud computing, including service models and deployment models, why data should be moved to the cloud and what role does the location of the cloud have. Discussion was also provided on the cyber security of cloud computing, criteria to assess the information security of cloud services (PiTuKri) and three of the biggest cloud service providers.

A review of internet articles about cloud services, service providers documentation and an interview with TUNI information security manager were used as a method for collecting the material used in the thesis. The material was analysed with data driven content analysis

The result of the thesis is a collection of information which should give the reader a basic understanding of cloud computing, cloud computing cyber security and what to pay attention to when selecting a cloud service provider. The results show that cloud computing can often be worthwhile. The scaling possibilities of cloud computing enable customers of any size to use them, and the huge cyber security resources often means better security for your data.

Based on this thesis, a further study into the more specific fields of cloud computing cybersecurity could be made. For example, how does system development affect cybersecurity.

Key words: cloud computing, cyber security, scaling

SISÄLLYSLUETTELO

ERITYISSANASTO

EDPB	Euroopan tietosuojaneuvosto (European Data Protection Board) on eurooppalainen riippumaton elin, jonka tavoitteena on varmistaa yleisten tietosuoja-asetuksien johdonmukainen soveltaminen.
GDPR	EU:n yleinen tietosuoja-asetus (General Data Protection Regulation)
MFA	Moinivaiheinen tunnistus (Multi Factor Authentication) on sähköinen todennusmenetelmä, jossa käyttäjä saa pääsyn verkkosivustoon tai sovellukseen vasta kahden tai useamman onnistuneen todennusmekanismin jälkeen.
NIST	National Institute of Standards and Technology (NIST) on yhdysvaltalainen virasto, jonka tehtävänä on kehittää ja edistää mittaustekniikoita, standardeja ja tekniikkaa.
NoSQL	Viittaa ei-relaatiotietokantoihin, eli tietokannan tallennustyyli poikkeaa relaatiotietokannasta.
PiTuKri	Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) on työkalu pilvipalveluiden turvallisuuden arviointiin
SCC	GDPR:n vakiosopimuslausekkeet (Standard Contractual Clauses) joiden tarkoitus on varmistaa, että tiedon siirrossa EU:sta EU:n ulkopuolelle voidaan taata asianmukainen tietoturva.
SQL	Viittaa relaatiotietokantoihin, tällöin tieto tallennetaan tietynlaisena taulukkoon.
vCPU	Virtuaalinen prosessori, jolla viitataan virtuaalikoneen prosenssointiyksikköön.
VoIP	Voice over IP, mahdollistaa puheen lähettämisen ip osotteiden avulla.

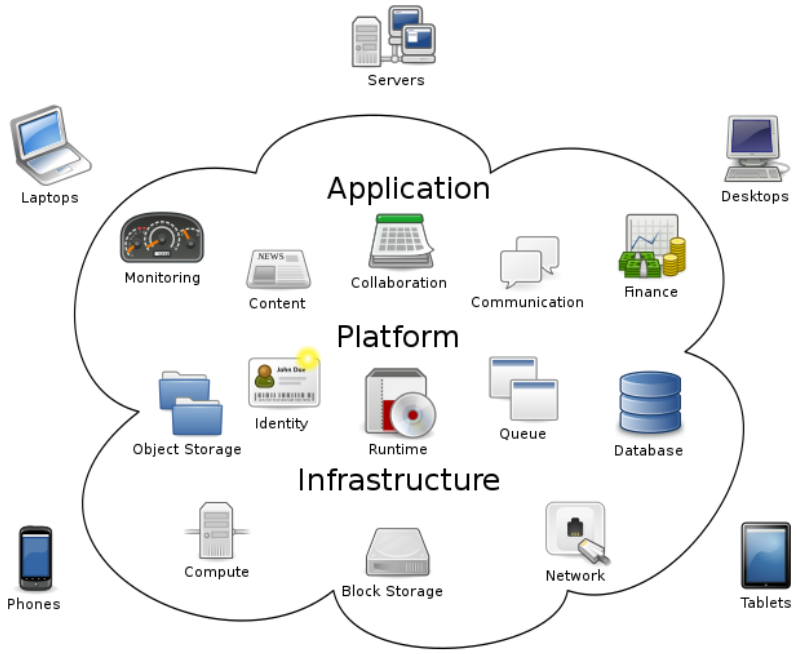
1 JOHDANTO

Pilvipalveluiden yleistyessä monet yritykset punnitsevat pilveen siirtymisen hyviä ja huonoja puolia. Oikeanlaisen ratkaisun löytämiseen on tärkeää ymmärtää kuinka pilvipalvelut toimivat ja ketkä niitä pyörittävät. Pilvipalvelut vaativat paljon luottamusta palveluntarjoajan turvallisiin käytäntöihin. Tietoturva on isossa roolissa pilvessä, kun luodaan luottamusta palveluntarjoajaan. Tässä opinnäytetyössä tarkastellaan pilvipalveluita kokonaisuutena, sekä arvioidaan niiden tietoturvallisuutta ja minkälaisia johtopäätöksiä siitä voidaan tehdä.

Opinnäytetyön tavoitteena on selittää lukijalle mitä ovat pilvipalvelut, miksi niiden käyttö saattaa olla kannattavaa, ovatko ne tietoturvallisia sekä tutustuttaa lukija muutamaan yleisimpään pilvipalveluntarjoajaan.

2 Mikä on pilvipalvelu?

Pilvipalvelu on palvelumalli, jossa tietoteknisiä resursseja toimitetaan tietoverkkojen yli. Palveluun otetaan yhteyttä internetin välityksellä. Palvelun tarjoaja voi kytkeä toiminnallisuuksia päälle tai pois sekä yhdistää niitä toisiin palveluihin kätevästi käyttäjäkokemusta haittaamatta tarpeen mukaan. Pilvipalveluita voidaan havainnollistaa kuvion 1 mukaisesti.

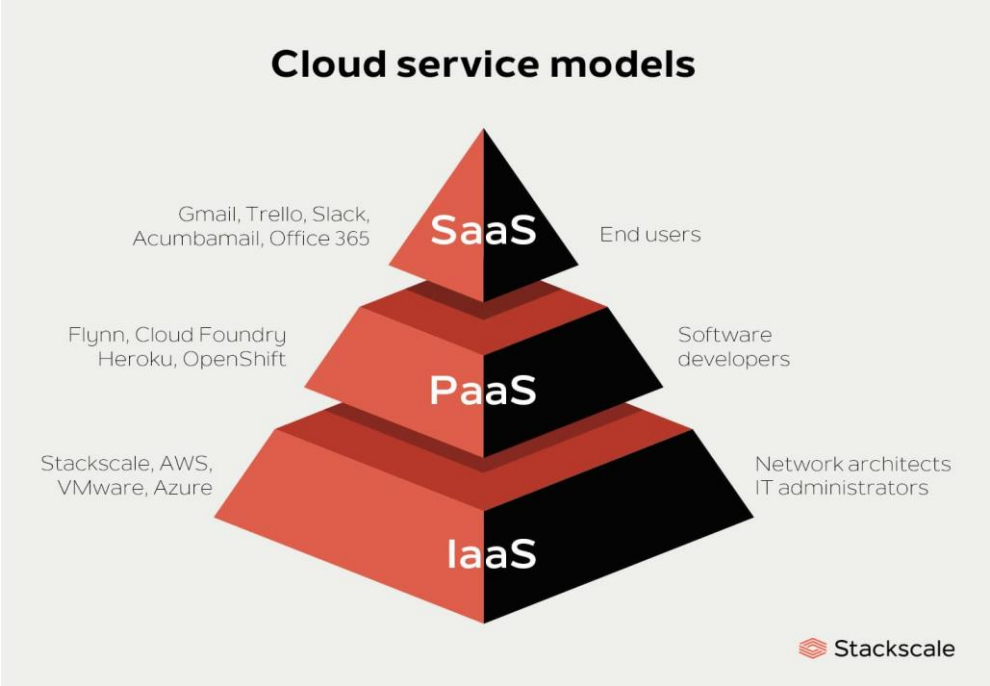


KUVIO 1. Esimerkkikuva erilaisista pilvipalveluista. (Johnston 2009)

National Institute of Standards and Technology (NIST) on määritellyt pilvipalvelu käsitteelle viisi ominaispiirrettä: itsepalvelu tarpeen vaatiessa, laaja verkkoon pääsy, resurssien yhdistäminen, nopea joustavuus ja palveluiden mittaaminen. Tämän lisäksi on kolme palveluluokkaa ja neljä pilvityyppiä. Pilvipalvelut tyypillisesti jaetaan kolmeen eri pääluokkaan sekä neljään eri pilvityyppiin.

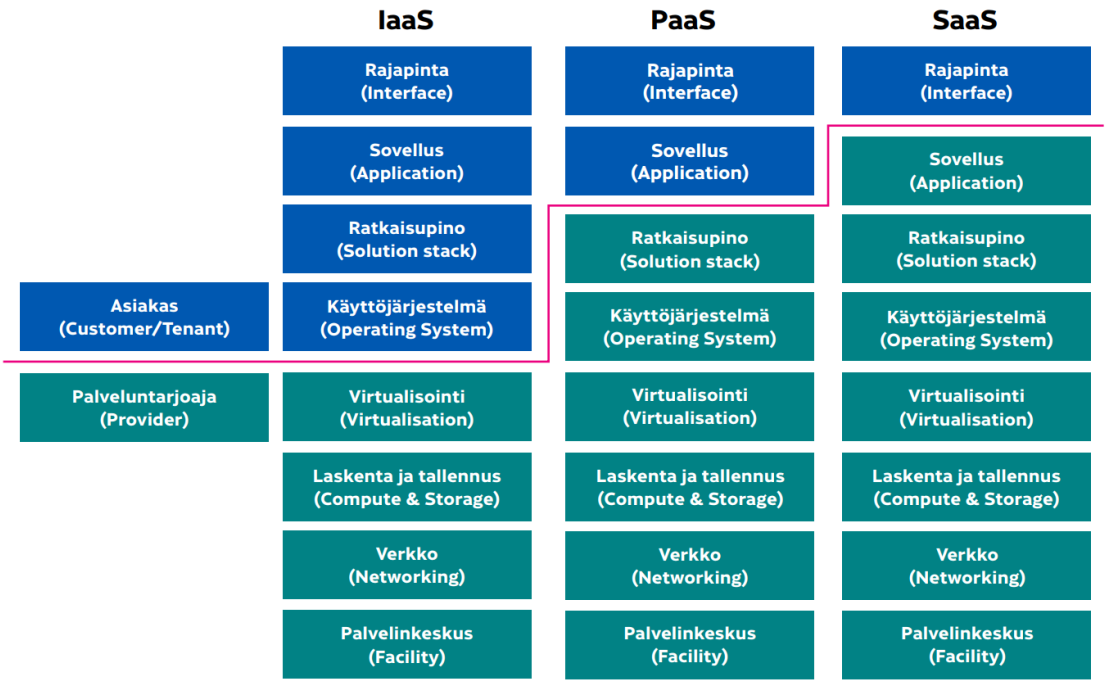
2.1 Eri pilvipalveluluokat

Pilvipalveluiden kolme pääluokkaa ovat NIST:n mukaan SaaS, PaaS ja IaaS. Nämä mallit ovat toinen toisistaan kauempana käyttäjästä, joten niitä usein kuvataan kerroksittain hahmottamaan mallien välistä loogisuutta (kuvio 2).



KUVIO 2. Pilvipalveluluokat. (Stackscale 2021)

Pilvipalveluiden turvallisuuteen, ylläpitoon ja huoltamiseen liittyvät vastuut jakautuvat kaikissa palvelumalleissa palveluntarjoajan ja asiakkaan välillä (kuvio 3). Vastuiden jakautuminen riippuu siitä, mikä palvelumalli on kyseessä. Mitä enemmän asiakas ulkoistaa palveluja, sitä vähemmän vastuuta sillä on palveluiden toiminnassa. Vastuiden jakautuminen voi kuitenkin vaihdella palveluntarjoajasta riippuen paikoittain suurestikin.



KUVIO 3. Pilvipalvelumallien tyypillinen vastuunjako (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 10)

2.1.1 SaaS

SaaS-palvelussa palveluntarjoaja vuokraa pilvessä sijaitsevan ohjelmiston asiakkaalleen. Tyypillisesti palveluntarjoajalle maksetaan kuukausi-/vuositilauksella tai kertamaksulla oikeudesta käyttää valmista sovellusta verkkoselaimen taikka tietokone-/puhelinsovelluksen kautta. Palveluntarjoaja on vastuussa ohjelmiston kehityksestä, ylläpidosta sekä ohjelmiston päivittämisestä. (Mell & Grance 2011, 2) Tämän takia SaaS palvelut ovat käyttäjän näkökulmasta helppokäyttöisiä. SaaS onkin myös yleisin pilvipalvelumalli. Käytämme SaaS-palveluita päivittäin kuten esimerkiksi sähköposti, netflix tai spotify.

SaaS-palveluiden hyviä puolia:

- Palveluntarjoaja hoitaa sovelluksen päivittämisen ja ylläpidon, joka säästää organisaatiolta resursseja (Stackscale 2021.)
- Pieni taloudellinen riski (Comptia n.d.)
- Helposti skaalautuva (IBM 2020.)
- Toimii missä vain, milloin vain. (IBM 2020.)

SaaS-Palveluiden haasteita:

- Kustomoinnin ja ominaisuuksien rajoitukset (Stackscale 2021.)
- Datan turvallisuus ja säilytys (Stackscale 2021.)
- Integraatio muiden palveluntarjoajien kanssa (Stackscale 2021.)

2.1.2 PaaS

PaaS-palvelussa asiakkaalle tarjotaan käyttövalmis sovellusalusta, jossa asiakas voi testata, suunnitella ja kehittää kustomoituja sovelluksia. Palveluntarjoajan vastuulla on infrastruktuurin hallinta mukaan lukien serverit, käyttöjärjestelmä sekä tietoverkko. Asiakkaalla on kuitenkin mahdollisuus vaikuttaa infrastruktuurin mahdollisiin applikaatioihin sekä asetuksiin. (Mell & Grance 2011, 2–3) Tavallinen käyttäjä käyttää PaaS palveluita harvemmin, esimerkkejä PaaS palvelusta ovat mm: Google App Engine, Microsoft Azure ja IBM Cloud Fountry.

PaaS-palveluiden hyviä puolia:

- Yksinkertainen ja kustannustehokas tapa luoda ja kehittää sovelluksia (Watts, Raza 2019.)
- Helposti skaalautuvia sovelluksia vähemmällä määrällä koodia (Watts, Raza 2019.)
- Nopeampi kehittää.

PaaS-palveluiden haasteita

- Mahdolliset rajoitukset operaatioissa, kun alusta ei mahdollisesti anna suorittaa kaikkia toimintoja (Stackscale 2021.)
- Palvelujen integrointi ja yhteensopivuus. (Stackscale 2021.)

2.1.3 IaaS

IaaS-palvelussa palveluntarjoaja tarjoaa asiakkaalle kokonaisen infrastruktuurin palveluna. Tyypillisesti tämä tapahtuu verkkopohjaisen liittymän kautta. Liittymän

kautta asiakas perustaa itse tarvitsemansa palvelimet ja hallinnoi alustaa. Palveluntarjoajan vastuulla on ainoastaan alusta, jota käytetään kaiken luomiseen. (Mell & Grance 2011, 3) IaaS-malli vaatiikin siis kaikista eniten osaamista palvelun ostajalta. Esimerkkejä IaaS-palveluista ovat: VMware ja Amazon AWS

IaaS-palveluiden hyviä puolia:

- Resursseja voidaan ostaa tarpeen mukaan ilman suuria laitteisto hankintoja. (Stackscale 2021.)
- Yritys pitää hallinnan infrastruktuuristaan. (Watts, Raza 2019.)
- Helposti skaalautuva alusta tarjoaa halutun määrän servereitä ja virtuaalikoneita asiakkaan tahdon mukaan. (Stackscale 2021.)
- Toimintavarmuus. (IBM 2020.)

IaaS-palveluiden haasteita

- Palveluntarjoaja vastaa yksin päivityksistä ja ylläpidosta (Taylor n.d.)
- Mahdollinen riippuvuus palveluntarjoajaan (Stackscale 2021.)
- Tietoturva. (Watts, Raza 2019.)

2.1.4 Muita palvelumalleja

Vaikka tyypillisesti kaikki pilvipalvelumallit saadaan jaoteltua kolmen pääluokan alle, on kuitenkin useita tarkempia termejä palveluille helpottamaan niiden tunnistamista. Vaihtoehtoisesti on myös laajempi termi: **Anything as a Service (XaaS)**, jolla viitataan minkä tahansa asian myymisenä palveluna.

Storage as a Service (SaaS) on pilvipalvelumalli, jossa vuokrataan tallennustilaa. Tyypillisesti isompi yritys vuokraa tilaa pienemmälle yritykselle omasta tallennustilastaan. Tallennustila palveluna on usein hyvä vaihtoehto pienille yrityksille, joilla ei ole varaa implementoida omaa tallennustila infrastruktuuriaan. (Bluepi 2015.)

Communications as a service (CaaS) on pilvipalvelumalli, jossa viestintäpalvelut ulkoistetaan. Tämä voi olla esimerkiksi voice over IP (VoIP), viestittelypalvelu tai video konferenssi applikaatio. (Bluepi 2015.)

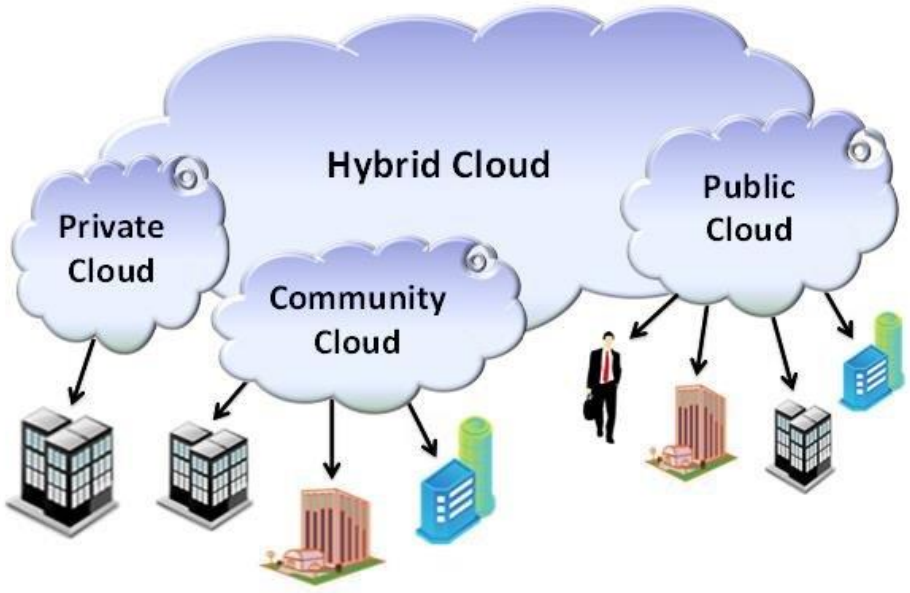
Network as a Service (NaaS) on pilvipalvelumalli, jossa vuokrataan verkkopalvelut. Tällöin palveluntarjoaja luo asiakkaalle internetinfrastruktuurin, johon sisältyy laitteet ja mahdolliset sovellukset kuten esimerkiksi palomuuri tai antivirus. (Bluepi 2015.)

Monitoring as a Service (MaaS) on pilvipalvelumalli, jossa palveluntarjoaja vuokraa monitorointia palveluille. Tyypillisin MaaS palvelu on internetin välityksellä toimiva monitorointi, joka jatkuvasti monitoroi sovellusten, systeemien sekä verkkojen tilannetta. (Bluepi 2015.)

Database as a service (DBaaS) on pilvipalvelumalli, jossa palveluntarjoaja perustaa ja ylläpitää tietokannan asiakkaalle sen antaman datan pohjalta. Tietokannan mahdollisia tyyppejä on monia esimerkiksi SQL ja NoSQL (MongoDB n.d.)

2.2 Pilvityypit

Pilvipalveluita toteutettaessa on mahdollista valita erilaisia pilvityyppejä parhaiten tukemaan pilvipalvelun tarpeita. NIST listaa neljä pääpilvityyppiä: julkinen, yksityinen, yhteisö sekä hybridi (kuvio 4).



KUVIO 4. Neljä pääpilviluokkaa. (Mell & Grance 2011)

Yritysten pilvitoteutukset koostuvat yhdestä tai useammasta pilvestä. Yrityksellä saattaa olla esimerkiksi kaksi yksityistä pilveä sekä julkinen pilvi hybridi pilven sisällä.

2.2.1 Public

Julkisen pilvityypin ratkaisuissa pilven infrastruktuuri on tarkoitettu avoimeen käyttöön. Sitä voidaan operoida ja ylläpitää yrityksen, koulun tai valtion johdosta tai niiden yhdistelmällä. Itse palvelimet ovat kuitenkin palveluntarjoajan tiloissa. (Mell & Grance 2011, 3) Julkinen pilvityyppi onkin kaikista yleisin pilvityyppi (What are public, private, and hybrid clouds? n.d.)

Julkisen pilvityypin hyviä puolia:

- hyvin luotettava toimintavarmuus. (What are public, private, and hybrid clouds? n.d.)
- Palveluntarjoaja pitää huolta, että palvelu toimii.
- helposti skaalautuva. (What are public, private, and hybrid clouds? n.d.)

Julkisen tyypin haasteita:

- Tietoturva ja kenellä on pääsy sinun dataasi. (Sam solutions n.d.)
- Kustomoinnin mahdollinen puute. (Sam solutions n.d.)

2.2.2 Private

Yksityisen pilvityypin toteutuksessa infrastruktuuri on varattu käytettäväksi vain yhdelle organisaatiolle. Organisaatiolla voi olla useampi kuluttaja ja sitä voidaan hallinnoida sekä operoida organisaation tai kolmannen osapuolen toimesta. (Mell & Grance 2011, 3)

Yksityisen pilvityypin hyviä puolia:

- Tietoturva ja selkeä tieto siitä kenellä on pääsy käsiksi dataan. (Sam solutions n.d.)

- Parempi kustomoitavuus yrityksen tarpeisiin. (What are public, private, and hybrid clouds? n.d.)
- Paremmin skaalautuva. (What are public, private, and hybrid clouds? n.d.)

Yksityisen pilvityypin haasteita:

- Kalliimpi. (Fpcomplete 2020.)
- Jos yritys ylläpitää itse infrastruktuuria, se vaatii IT-alan osaajia. (Krasteva n.d.)

2.2.3 Trusted/community

Yhteisön pilvityypin toteutuksessa infrastruktuuri toimitetaan joukolle yrityksiä/käyttäjiä, joilla on yhteinen tavoite (esim. tietoturva vaatimukset, menettelytapa tai ymmärrys käyttöehdoista). Infrastruktuurin voi omistaa, operoida sekä hallita yksi tai useampi yritys koko joukosta. (Mell & Grance 2011, 3)

Yhteisön pilvityypin hyviä puolia:

- Yhteistyö muiden dataa käyttävien tahojen kanssa (Samsolutions n.d.)
- Resursseja voidaan jakaa muiden kanssa, joka alentaa kustannuksia. (Samsolutions n.d.)

Yhteisön pilvityypin haasteita:

- Yritysten löytäminen liittymään infrastruktuurin voi olla haastavaa (Samsolutions n.d.)
- Mahdollinen kaistanleveyden tai tallennustilan loppuminen muiden organisaatioiden toimesta. (Samsolutions n.d.)

2.2.4 Hybrid

Hybridi pilvityypin toteutuksessa infrastruktuuri on kahden eri pilvityypin infrastruktuurin yhdistelmä (yksityinen, julkinen tai yhteisö) jotka pysyvät omina infrastruktuureinaan mutta ovat yhdistetty standardoidulla tekniikalla, joka sallii datan

sekä applikaatioiden siirtämisen infrastruktuureiden välillä. (Mell & Grance 2011, 3)

Hybridi pilvityypin hyviä puolia:

- Paras joustavuus ja skaalautuminen. (Samsolutions n.d.)
- Ylläpidon helppouden ja tietoturvan tasapaino. (Fpcomplete 2020.)

Hybridi pilvityypin haasteita:

- Kokonaisuuden hahmottaminen voi olla vaikeaa pilvien jakamisen vuoksi. (Flowers 2021.)

2.3 Missä pilvi sijaitsee?

Pilvipalveluihin tallennetun datan säilyttämiseen käytettävät serverit voivat sijaita palveluntarjoajasta riippuen yhdessä tai useammassa paikassa. Yleisesti pienemmät yritykset säilyttävät datansa lähellä omaa toimipistettään esim. konesalissa tai palvelinkeskuksessa, tai ne saattavat ulkoistaa palvelun vuokraten resursseja palveluntarjoajalta. On myös mahdollista, että pilvipalveluntarjoaja vuokraa resursseja suuremmalta palveluntarjoajalta. (Pilvipalveluiden turvallisuus, 9)

Suuremmilla yrityksillä on omat konesalinsa tai palvelinkeskuksensa. Ne voivat sijaita eri maissa tai mantereilla. Tämän vuoksi käyttäjän voi olla mahdotonta tietää missä hänen datansa sijaitsee. Jos datan sijainnilla on merkitystä käyttötarkoituksen kannalta, tulee se selvittää palveluntarjoajan kanssa. (Pilvipalveluiden turvallisuus, 9) Esimerkiksi Microsoft noudattaa Euroopan tietosuojaneuvoston (EDPB) suosittelemia kuutta askelta varmistaakseen, että dataa suojataan, tallennetaan ja käsitellään EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisesti. (Compliance with EU transfer requirements…, 1-34.) EDPB:n suosittelemat kuusi askelta ovat:

1. Kartoitus henkilökohtaisen datan siirtämisestä EU:n ulkopuolisiin maihin.

2. Varmista että siirtoon käytetty työkalu on tarkoitukseen kelpaava, esimerkiksi Standard Contractual Clauses (SCC).

3. Arvioi onko GDPR artiklassa 46 mainittu datansiirtotyökalu (esimerkiksi SCC) riittävän tehokas työkalu ottaen huomioon datan siirron olosuhteet.

4. Identifioi ja adoptio toimenpiteet, jotka ovat tarvittavia tuodakseen tietoturvan tason EU:n standardien mukaisiksi.

5. Tee toimenpiteiden integrointiin tarvittavat menetelmät.

6. Arvioi uudelleen turvallisuuden taso yksityisen datan siirrossa EU:n ulkopuolisiin maihin, kun se on tarpeellista ja monitoroi sitä

Datan siirron ja säilytyksen turvallisuuden arviointi on tärkeää, sillä palvelinkeskuksia sijoitetaan usein moniin eri maantieteellisiin sijainteihin ja käyttäjien tietoja kopioidaan useihin keskuksiin, jotta palveluiden toimintaa voidaan paremmin varmistaa. (Pilvipalveluiden turvallisuus, 9) Tämä taas johtaa siihen, että yritysten on pakko toimia huomioiden datan tallennuksen paikallinen lainsäädäntö sekä datan alkuperän paikallinen lainsäädäntö.

2.4 Miksi viedä tietoa pilveen

Pilvipalvelut ovat joustava tapa tuottaa palveluja, joissa täytyy päästä käsiksi dataan ajasta tai paikasta riippumatta helposti. Koska palvelut toimivat internetin välityksellä, on palveluihin helpompaa päästä käsiksi kuin on-premises palveluihin. Palveluihin voi myös ottaa yhteyden liikkeestä mobiililaitteella tai muulla vastaavalla. Pilvipalvelut mahdollistavat myös usean käyttäjän samanaikaisen toiminnan. Jos pilvipalvelut ovat geologisesti hajautettuja, helpottuu palveluiden käyttö vikatilanteissa. (Malmivaara 2022)

Pilvipalvelut ovat hyvin skaalautuvia. Asiakas voi tarpeen mukaan saada lisää resursseja palveluntarjoajalta, tai vaihtoehtoisesti vähentää niitä tarpeen vähentyessä. Tämä tarkoittaa, että asiakkaan ei tarvitse sijoittaa suuria rahasummia laitteiston hankintaan. Pilvipalveluiden asiantuntijoita löytyy paljon. Tämän vuoksi on helppoa löytää alan ammattilaisia auttamaan palveluiden käyttöönoton tai ylläpidon kanssa. (Malmivaara 2022)

Jos useat eri toimijat käyttävät samantyyppisiä pilvipalveluita ja perusrunko on samanlainen, voidaan tehdä yhteisiä palveluja tai toimintoja, jotka toimivat kaikille. Tämä voi tarkoittaa esimerkiksi yhteistä valvontaa, yhteistä portaalista tehtävää käyttöönottoa tai käyttövaltuushallintojen jakamista. Tällöin rungon päälle tehtävien palvelujen kustannuksia voidaan jakaa useamman tahon kesken. (Malmivaara 2022)

Suurilla pilvipalveluidentarjoajilla on palveluissaan käytössä hyvin suuret resurssit. Palveluntarjoajat pystyvät käyttämään automatisoituja työkaluja analysoimaan dataa, antaen paljon paremman kokonaiskuvan tallennetusta datasta. Tätä informaatiota voidaan käyttää hyödyksi esimerkiksi yritysten tavoitteiden saavuttamisessa. Datan automaattinen analysointi auttaa myös tietoturvaa. Mahdolliseen tietoturvan analysointiin on paljon enemmän resursseja pilvipalvelussa kuin on-premises toteutuksessa. (Salesforce n.d.)

Pilvipalvelut luovat koko ajan automaattisia varmuuskopioita datasta, jolloin palvelun vikasietokyky on huomattavasti parempi. Kun data on tallennettuna pilveen, on data turvassa, vaikka käyttäjän fyysinen laite häviäisi tai hajoaisi. (Salesforce n.d.)

2.5 Pilvipalveluiden ongelmia

Yksi selkeimmistä ongelmista pilvipalveluissa on internetyhteyden pakollisuus. Jos internettiin ei ole yhteyttä, ei pilvipalveluihin päästä käsiksi. Tällöin myös hidas internetyhteys voi heikentää palvelujen käyttäjäkokemusta. Pilvipalveluiden internettiin sidonnaisuus tuo myös mukanaan huomattavasti isomman uhkakartan. Tämän vuoksi ei voida ottaa huomioon pelkästään on-premises tyyppisten

palveluiden uhkia, vaan tulee myös internetin uhka ottaa huomioon. (Malmivaara 2022)

Pilvipalveluissa virheiden teko voi luoda huomattavasti suurempia vahinkoja. Jos esimerkiksi jätät palvelussa portit auki kaikille, tyypillisesti on-premises palveluissa ei-toivottujen käyttäjien määrä pysyisi sadoissa taikka tuhansissa, kun pilvipalveluissa voidaan pahimmillaan puhua koko maailmasta. (Malmivaara 2022

Vaikka Malmivaaran mukaan pilvipalveluiden asiantuntijoita ja osaamista on paljon, vaativat pilvipalvelut kuitenkin täysin erilaista osaamista kuin on-premises tyyppiset palvelut. Tällöin yritys voi joutua hankkimaan uutta osaamista.

Pilvipalveluiden yhtenä hyvänä puolena voidaan pitää datan jakamista eri datakeskuksiin. Tässäkin on kuitenkin oma ongelmansa, sillä käyttäjällä ei käytännössä ole vaikutusvaltaa siihen, missä datan geologinen sijainti on. Käyttäjällä ei myöskään ole vaikutusvaltaa siihen, keillä kolmannen osapuolen tekijöillä on pääsy käsiksi dataan. (Malmivaara 2022)

Myös pilvipalvelut ovat haavoittuvia palvelukatkoksille. Pilvipalvelut saattavat kokea katkoksia syystä tai toisesta, jolloin palveluiden toiminta saattaa katketa. Nämä mahdolliset katkokset ovat täysin asiakkaan kontrollin ulkopuolella.

Vaikka tietoturvaresurssit saattavat olla huomattavasti suuremmat pilvipalveluissa kuin on-premises ratkaisuissa, joutuu asiakas kuitenkin jakamaan salatun tietonsa toisen toimijan kanssa. Tällöin jos palveluntarjoaja joutuu tietomurron uhriksi, voidaan myös asiakkaan tiedot varastaa. (Sharma 2022)

Pilvipalveluntarjoaja omistaa infrastruktuurin, jossa asiakkaan palvelut ovat. Tällöin asiakkaalla on vähän vaikutusvaltaa palvelun suhteen. Tämä voi johtaa ongelmiin asiakkaalle. (Morefield 2019)

2.6 Mitä muuta tulee huomioida

Pilvipalveluidenkäyttöä harkittaessa käyttäjän kannattaa huomioida palveluntarjoajan avoimuus palvelunsa suhteen. Suuret palveluntarjoajat ovat usein hyvin avoimia ja tarjoavat paljon tietoa palvelustansa internetissä. Palvelusta kannattaa myös maksaa. Jos et maksa palvelusta, hankkii palveluntarjoaja rahansa toisin keinoin. Eurooppalaisena kuluttajana kannattaa sinun myös suosia eurooppalaisia palveluja amerikkalaisten palvelujen sijaan lainsäädännönkin puolesta. Euroopassa dataasi suojellaan tarkemmin, sillä Euroopan tietosuojalaki on tiukempi kuin Amerikassa. (Malmivaara 2022)

Kriisitilanteessa on tärkeää, että palveluiden toiminta on mietitty tarkkaan läpi. Dataan tulee olla pääsyä varten mietittynä varayhteys, jota voidaan tällaisessa tilanteessa käyttää. On tärkeää myös pystyä toteuttamaan pääsynhallinta esimerkiksi paikallisella tunnuksella. (Malmivaara 2022)

Pilvipalveluissa on paljon aavistamattomia kuluja. Palveluntarjoajat haluavat rahaa kaikista eri ominaisuuksista, joita palvelussa käytät ja näitä voi olla vaikea hahmottaa etukäteen. (Evolve n.d.)

3 Pilvipalveluiden tietoturvasta

Pilvipalveluiden turvallisuuteen liittyy monta tavalliselle käyttäjälle näkymätöntä tekijää. Nämä käyttäjälle näkymättömät tekijät ovat kuitenkin suuria huolenaiheita yrityksille sekä palveluntarjoajille. Pilvipalvelua valitessa onkin siis tarpeellista tutustua palveluntarjoajiin sekä heidän tietoturvallisuuteensa. Pilvipalvelun teknisen turvallisuuden kannalta olennaisia asioita ovat käytettävät teknologiat, toimintamallit, periaatteet, käyttäjänhallinta ja ohjelmiston päivityskäytännöt. (Pilvipalveluiden turvallisuus, 12.)

Pilvipalvelun turvallisuutta arvioidessa on syytä kiinnittää huomiota palvelun toteutukseen sekä palveluntarjoajan toimintaan. Suurimmat pilvipalveluiden tarjoajat ovat nykyään usein hyvin läpinäkyviä toiminansa kanssa. Asiakkaiden kannattaa tutustua mahdollisiin sertifiointeihin taikka kolmannen osapuolen teettämiin auditointeihin, sekä palveluntarjoajan julkaisemiin tietoturvaan liittyviin dokumentteihin. Kaikkea tietoa toiminnastaan palvelut eivät kuitenkaan voi paljastaa, jotta ne säilyttäisivät kilpailukykynsä sekä tietoturvallisuutensa. (Pilvipalveluiden turvallisuus, 12.)

Suomessa salassa pidettävä tieto on luokiteltu yleisesti viiteen eri turvallisuusluokkaan kuvion 5 mukaisesti. Nämä viisi luokkaa ovat: TL1 erittäin salainen, TL2 salainen, TL3 luottamuksellinen, TL4 käyttö rajoitettu sekä salassa pidettävä. TL1 on kaikista salaisinta tietoa, ja siihen pääsee käsiksi yleensä vain muutama henkilö (Roslund 2017). TL4 on väljin turvallisuusluokituksista TL1-TL4. Tämän lisäksi on myös tietoa, joka on nimetty vain salassa pidettäväksi.

KUVIO 5. Suomen turvaluokitukset asiakirjoille. (Roslund 2017)

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) on salassa pidettävän tiedon turvallisuuden parantamiseksi kehitetty työkalu. PiTuKrissa on monta eri osa-aluetta auttamaan tiedon turvallisuuden arvoinnissa. Näihin kuuluu muun muassa: Identiteetin ja pääsynhallinta, henkilöstöturvallisuus, esiehdot, turvallisuusjohtaminen, fyysinen turvallisuus, salaus ja tietojärjestelmäturvallisuus. PiTuKrissa käytettävät turvaluokitukset eroavat edellä kuvatusta yleisesti Suomessa käytetystä turvaluokituksesta hieman. PiTuKri jakaa turvallisuusluokat useampaan lohkoon kuvion 6. mukaisesti. PiTuKrin mukaan myös esimerkiksi julkista tietoa tulee suojella sen eheyden vuoksi.

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.

KUVIO 6. PiTuKrissa käsiteltävät turvallisuusluokat (Pilvipalveluiden turvallisuuden arviointikriteeristö 2020, 8)

3.1 Käyttäjänhallinta eli autentikointi

Pilvipalvelun turvalliselle toiminnalle yksi tärkeimmistä vaatimuksista on luotettava käyttäjänhallinta. Tämä sisältää palveluun rekisteröinnin, rekisteröidyn käyttäjän tunnistamisen sekä käyttöoikeuksien hallinnoinnin. (Pilvipalveluiden turvallisuus, 12.) Toimivan käyttäjänhallinnan edellytys on käyttäjien tunnistus ja sen varmentaminen. Tämän vuoksi palveluntarjoajan tulee tehdä töitä sen eteen, että autentikointi toimii halutusti. On erityisen tärkeää, että autentikointi toimii suunnitellusti hallintayhteyksiä käytettäessä, sillä hallintayhteyksillä päästään käsiksi palveluiden kriittiseen informaatioon.

Jos käyttäjänhallinta on tehty huolellisesti, voidaan tätä dataa hyödyntää myös muualla. Kun organisaatiolla on yksi paikka, jossa säilytetään ihmisten kirjautumistietoja, voidaan näillä jakaa oikeuksia useampiin eri sovelluksiin, vähentäen tarvetta muistaa useita salasanoja. Mahdollisuus hallita kaikkia käyttöoikeuksia kerralla parantaa näkyvyyttä ja hallintaa (Käyttäjätietojen ja käytön hallinta n.d).

PiTuKri listaa identiteetin ja pääsynhallintaan liittyen 3 vaatimusta: käyttöoikeushallinta (IP-01), käyttäjätunnistus (IP-02) ja hallintayhteydet (IP-03). Käyttöoikeushallinnan tavoitteena on pitää huolta, että käyttöoikeuksien jakamisessa on noudatettu vähimpien oikeuksien periaatetta. Tällöin käyttäjätunnukset luovutetaan vain niille, jotka tarvitsevat niitä tehtäviensä suorittamiseen. Tulee myös pitää huolta, että käyttäjätunnuksille on annettu oikeudet vain välttämättömiin verkkoihin, laitteisiin ja sovelluksiin. (ks. liite 1. IP-01 käyttöoikeushallinta) Käyttäjäntunnistus keskittyy tietojen ja palveluiden rajaamiseen vain siihen valtuutettuihin käyttäjiin. Tähän liittyy muun muassa käyttäjien tunnuksien henkilökohtaisuus sekä oikeanlainen todennus kirjautuessa. (ks. liite 2. IP-02 käyttäjäntunnistus) Hallintayhteyksien hallinnalla halutaan varmistaa, että hallintayhteydet on suojattu riittävän vahvasti, jotta niiden kautta valtuuttamaton taho ei pääse käsiksi palveluun. (ks. liite 3. IP-03 hallintayhteydet)

3.1.1 Henkilöstöturvallisuus

Henkilökunnalla ja sen työtavoilla on suuri vaikutus palvelun tietoturvallisuuteen. Tämän vuoksi on tärkeää tietää, minkälainen palveluntarjoajan henkilöstöpolitiikka on ja millaisia käytäntöjä se noudattaa. Palvelun turvallisuutta arvioidessa henkilöstön turvaluokitukset ovat tärkeitä pitää mielessä. (Pilvipalveluiden turvallisuus, 13.)

Henkilöstöllä, joilla on suora pääsy palvelun toiminnallisuuteen sekä asiakkaiden tietoihin tulee olla hyvä tietoturva. Kriittisten toimintojen kanssa työskenteleville henkilöille tulisi suorittaa turvallisuusselvityksiä ja pitää huolta, että he hyödyntävät käytännön toiminnoissa alan hyväksyttyjä standardeja. (Pilvipalveluiden tur-

vallisuus, 13.) Jotta hyvä tietoturvan taso voidaan säilyttää, tulee henkilöstöä kouluttaa alan uusiin tietoturvakäytäntöihin jatkuvasti. Työsuhteen päättyessä työnantajan tulee myös päivittää tai hävittää työntekijän käyttö- ja pääsyoikeudet.

PiTuKrilla on henkilöstöturvallisuuteen liittyen 5 vaatimusta: Työsuhteen elinkaaren huomioiminen (HT-01), henkilöstön luotettavuuden arviointi (HT-02), salassapito- ja vaitiolosopimukset (HT-03), turvallisuustietoisuus (HT-04), tiedonsaantitarpeet ja tehtävien erottelu (HT-05). Työsuhteen elinkaaren huomioimisen tavoitteena on pienentää henkilöstöön liittyviä riskejä työsuhteen aikana. (ks. liite 4 HT-01 Työsuhteen elinkaaren huomioiminen) Henkilöstön luotettavuuden arvioinnissa tulee tarkistaa palkattavan työntekijän tausta ennen työsuhteen alkua. (ks. liite 4 HT-02 henkilöstön luotettavuuden arviointi). Salassapito- ja vaitiolosopimukset kohdassa käsitellään mitä tietoa pidetään salassa, kuinka se tehdään sekä mitä käy, jos sopimuksen ehtoja rikotaan. (ks. liite 5. HT-03 Salassapito- ja vaitiolosopimukset) Turvallisuustietoisuus käsittelee henkilökunnan tietoturvallista osaamista, sekä pyrkii varmistamaan että henkilöstö pystyy toimimaan turvallisesti myös käytännössä (ks. liite 5 HT-04 Turvallisuustietoisuus).

3.1.2 Käyttäjät

Kyberturvallisuuskeskuksen mukaan ”yksittäinen käyttäjä voi jopa olla tietoturvallisuuden heikoin lenkki”. Tämä johtaa siihen, että käyttöympäristöstä on pidettävä hyvää huolta. Käyttöympäristöllä viitataan käyttäjän käyttämiin päätelaitteisiin sekä mahdollisiin järjestelmiin, jotka toimivat pilvipalvelun kanssa. (Pilvipalveluiden turvallisuus, 13.)

Käyttäjiä tulee ohjeistaa ja kouluttaa kuinka toimia turvallisesti oman päätelaitteensa sekä internetin käytön suhteen. Täten käyttäjät pystyvät käyttämään pilvipalveluita turvallisesti. On myös tärkeää tehdä selkeät rajaukset siitä, mitä tietoa palveluun saa tallentaa, mihin tarkoitukseen ja mistä sitä saa käyttää. (Pilvipalveluiden turvallisuus, 13.) Käyttäjien päätelaitehallintaan on tarjolla sovelluksia, joilla käyttäjien aiheuttamaa riskiä pyritään minimoimaan. Yksi esimerkki tällaisesta on Microsoft Intune.

Myös käyttäjienhallinnassa voidaan seurata PiTuKrin kriteerejä IP-01 (käyttöoikeushallinta) ja IP-02 (käyttäjätunnistus). Käyttöoikeushallinnasta on tärkeää pitää huolta, jotta tavalliset käyttäjät eivät pääse käsiksi tietoihin, joihin heillä ei ole oikeutta. (ks. liite 1. IP-01 käyttöoikeushallinta). Käyttäjätunnistuksessa on tärkeää, ettei käyttäjän tunnuksille pääse haluamattomia henkilöitä. (ks. liite 2. IP-02 käyttäjätunnistus.)

3.1.3 Kaksivaiheinen tunnistus (2FA)

Two-Factor Authentication (2FA) on hyödyllinen työkalu lisäämään palvelun tietoturvaa. Kaksivaiheinen tunnistus lisää yhden kerroksen suojausta normaalien kirjautumistietojen päälle. Kun käyttäjä kirjautuessaan syöttää kirjautumistietonsa sisään applikaatioon, tulee hänen tämän jälkeen syöttää vielä toinen tunniste järjestelmään. Tähän tarkoitukseen on muutama yleinen käytäntö, kuten:

1. Tunnuslaite on pieni avaimenperän kaltainen laite, joka luo uuden vahvistuskoodin tietyn ajan välein. Tämä koodi syötetään kirjautumisen yhteydessä vahvistuksena. Laitteiden pieni koko tekee niistä helppoja hukata ja monen laitteen tekeminen on kallista. Niiden tietoturva ei myöskään ole hyvä. (Twilio n.d.)

KUVA 1. Kaksivaiheisessa tunnistuksessa käytettävä tunnuslaite (Ronald 2010)

2. Teksti- ja puheviestit. Vahvistuskoodi lähetetään joko tekstiviestinä käyttäjän aiemmin antamaan puhelinnumeroon, tai käyttäjälle soitetaan ja robotti kertoo koodin ääneen. Koodi on niin sanottu ”one-time passcode” (OTP) jolloin se toimii vain kerran. (Twilio n.d.)

3. Sovellus tunniste. Ladattava sovellus luo ajallisen kerran toimivan koodin eli time-based one-time passcode:n (TOTP). Koodi tyypillisesti toimii alle minuutin, jolloin sitä on lähes mahdotonta arvata. Turvallisuutta lisää myös se, että koodit generoidaan ja näytetään samassa laitteessa, jolloin niitä on hyvin vaikeaa varastaa. Tämä onkin TOTP-tunnisteiden suurimpia etuja. (Twilio n.d.)

4. Push-ilmoitus. Kun halutaan toimia ilman tunnistetta, voidaan vaihtoehtoisesti käyttää push-ilmoitusta, joka lähetetään kirjautujan laitteeseen. Tällä käyttäjä voi joko hyväksyä tai hylätä kirjautumisen. Tämä poistaa mahdolliset kalastelu tai ”man-in-the-middle”-hyökkäykset. Tämän käytännön suurin ongelma on internetyhteyden pakollisuus. (Twilio n.d.)

Biometrinen tunnistus käyttää kirjautujaa tunnistautumiseen. Tällaisina tunnistautumiseen voidaan käyttää muun muassa: Sormenjälkiä, verkkokalvoa sekä kasvojen tunnistusta. (Twilio n.d.) Yleinen esimerkki biometrisestä tunnistautumisesta on älypuhelimien sormenjäljellä tunnistautuminen.

3.2 Luottamus

Pilvipalveluiden yleistyessä joudumme luottamaan pilvipalveluiden tarjoajiin paljon arkisessa internetin käytössämme. Kaikki tieto, jota luovutamme palveluun kuten kirjautumistiedot, pankkikorttien tunnusluvut sekä pin-koodit ja niin edelleen ovat mahdollisten hyökkäysten uhan alla. Jotta ihmisillä olisi halu käyttää pilvipalveluita, tulee palveluntarjoajan tietoturvallisiin käytäntöihin olla luottamus.

Helppo tapa luoda luottamusta palveluun, on olla läpinäkyvä käytännöissään. Tämän vuoksi suuret palveluntarjoajat usein tarjoavat paljon informaatiota palveluistaan internetissä. Usein palveluntarjoajat ovat teettäneet tietoturva selvityksiä

palveluistansa, jonka vuoksi asiakkaan kannattaa selvittää, onko tietoturvaselvityksiä tehty.

PiTuKri käsittelee Esiehtoja sekä turvallisuusjohtamista. Esiehdot käsittelevät järjestelmäkuvausta (EE-01) sekä lainsäädäntöjohdannaisia riskejä (EE-02). Järjestelmäkuvauksen tarkoitus on tuottaa riittävän yksinkertainen kuvaus kokonaisuudesta, jotta sen avulla voidaan arvioida palvelun yleistä soveltuvuutta sekä riskejä asiakkaan käyttötapauksessa. (ks. liite 7. EE-01 järjestelmäkuvaus) Läinsäädäntöjohdannaiset riskit toimivat myös apuna arvioidessa pilvipalvelun soveltuvuutta asiakkaan käyttötarkoitukseen. Tällöin käydään läpi mahdolliset muiden maiden lainsäädäntöjen tuomat velvollisuudet. (ks. liite 8 EE-02 lainsäädäntöjohdannaiset riskit). Turvallisuusjohtaminen sisältää turvallisuusperiaatteet (TJ-01), turvallisuuden vastuut (TJ-02), turvallisuusriskien ja -häiriöiden hallinnan (TJ-03 ja TJ-04), jatkuvuuden hallinnan (TJ-05), tietojen ja muiden suojattavien kohteiden luokittelun ja merkinnän (TJ-06), vaatimustenmukaisuuden ja tietosuojan (TJ-07) sekä palveluntarjoajien ja toimittajien turvallisuuden (TJ-08). Turvallisuusperiaatteilla varmistetaan, että organisaatio sitoutuu turvallisuuden noudattamiseen ja että turvallisuus tukee organisaation toimintaa. (ks. liite 9 TJ-01 turvallisuusperiaatteet) Turvallisuuden vastuut tulee määrittää, että turvallisuuden osa-alueilla on vastuuhenkilöt, joiden tietämys on riittävän asianmukaista. (ks. liite 9 TJ-02 turvallisuuden vastuut) Turvallisuusriskien hallinnan tavoitteena on tunnistaa ja hallita toimintaan kohdistuvat riskit riittävän nopeasti, ettei palvelun toiminta häiriinny. (ks. liite 10 TJ-03) Turvallisuushäiriöiden hallinnan tavoite on varmistaa, että organisaatio pystyy toimimaan mahdollisimman tehokkaasti ongelma tilanteissa, sekä minimoimaan mahdolliset vahingot. (ks. liite 11 TJ-04 turvallisuushäiriöiden hallinta) Jatkuvuudenhallinnan tavoitteena on varmistaa palvelun jatkuvuus esimerkiksi ennaltaehkäisevien ja korjaavien toimenpiteiden avulla. (ks. liite 12 TJ-05 jatkuvuudenhallinta) Tietojen ja muiden suojattavien kohteiden luokittelulla ja merkinnällä halutaan mahdollistaa luokittelun mukaisten turvatoimien toteutus. (ks. liite 13 TJ-06 Tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä) Vaatimustenmukaisuus ja tietosuoja käsittelee palveluun soveltuvien lakien määräykset sekä näiden noudattamista. (ks. liite 14 TJ-07 vaatimustenmukaisuus ja tietosuoja) Palveluntarjoajien ja toimittajien turvallisuus käsittelee suojattavia kohteita, joihin on pääsy pilvipalveluntarjoajan omilla

palveluntarjoajilla tai toimittajilla. Tällöin tulee varmistaa suojattavien kohteiden turvallisuus. (ks. liite 15 TJ-08 palveluntarjoajien ja toimittajien turvallisuus)

3.3 Fyysinen turva

Pilvipalvelun fyysisellä turvalla on myös merkitystä. Hyvin suojattu ja valvottu ympäristö estää tahallista ja tahatonta ilkivaltaa. Kulunvalvonnalla voidaan varmistaa, että vain tietyt henkilöt voivat liikkua alueella, jolla minimoidaan vahinkoja. (Pilvipalveluiden turvallisuus, 13.)

Pilvipalveluiden kahdentamisella voidaan paremmin taata palveluiden toimivuus poikkeustilanteissa. Esimerkiksi luonnonkatastrofin seurauksena serverit saattavat vahingoittua, jolloin palvelua voidaan tarjota toisesta sijainnista. (Pilvipalveluiden turvallisuus, 13.)

PiTuKri listaa fyysisen turvallisuuden yhteydessä 5 kriteeriä: monitasoinen suojaaminen ja riskienhallinta (FT-01), rakenteet ja turvallisuusjärjestelmät (FT-02), luvattoman pääsyn estäminen (FT-03), palveluntuottajat ja vierailijat (FT-04) sekä varautuminen ja jatkuvuudenhallinta (FT-05). Monitasoinen suojaaminen ja riskienhallinta keskittyy toinen toisiaan täydentäviin suojatoimiin. Tällöin tilat pyritään rakentamaan vyöhykkeinä, jolloin paremman suojauksen vaatimat tilat ovat sisimpänä. (ks. liite 16 FT-01 monitasoinen suojaaminen ja riskienhallinta) Rakenteet ja turvallisuusjärjestelmät pyrkivät suojaamaan fyysistä aluetta, joten tulee tarkistaa, että suojaukseen käytetään riittävän kestävää materiaalia, ja että turvallisuutta valvovat järjestelmät ovat riittävän tiukat. (ks. liite 17 FT-02 rakenteet ja turvallisuusjärjestelmät) Luvattoman pääsyn estämisen tavoitteena on pitää huolta, että vain tietyt henkilöt pääsevät salattuun tietoon fyysisesti käsiksi. (ks. liite 18 FT-03 luvattoman pääsyn estäminen) Palveluntuottajat ja vierailijat on tärkeää pystyä tunnistamaan, sekä pitää huolta että vain valtuutetuilla henkilöillä on pääsy järjestelmiin. (ks. liite 19 FT-04 palveluntuottajat ja vierailijat) Varautuminen ja jatkuvuudenhallinta keskittyy pilvipalvelun fyysisten laitteiden toiminnan jatkuvuuteen luonnon ja ihmisten aiheuttamien uhkien tapahtuessa. (ks. liite 20 FT-05 varautuminen ja jatkuvuudenhallinta)

3.4 Salaus

Pilvipalveluissa käytetään salausta. Salauksella data muokataan muotoon, jossa sitä ei pysty lukemaan ilman sen purkamista salausavaimella, jonka tietää vain datan salaaja. Salaukset ovat yleensä standardoituja. Malmivaaran mukaan yksi yleisimmistä standardeista on aes 256-salaus, joka tulee sanoista Advanced Encryption Standard ja numero 256 viittaa salausavaimen olevan 256 bittiä pitkä. Salausavaimen ollessa näin pitkä, on sen murtaminen Brute-force-hyökkäyksellä käytännössä mahdotonta.

Helppo tapa luoda tiedollesi lisäturvaa pilvipalvelussa on salata tietosi omalla laitteellasi. Tähän tarkoitukseen löytyy useita eri sovelluksia kuten esimerkiksi Boxcryptor. Ohjelma salaa valitun datan ja tallentaa salausavaimen laitteellesi, jonka jälkeen se voidaan viedä pilveen. Tällöin jos pilvipalvelun dataan pääse käsiksi ulkopuolinen taho, eivät he pysty lukemaan dataasi ilman avainta sinun laitteestasi. (Malmivaara 2022)

Kaikkea dataa ei kuitenkaan kannata salata itse. Kaikki data, jonka käyttäjä salaa omalla laitteellaan, on täysin lukematonta pilvipalveluntarjoajalle. Tämän tarkoittaa, että palveluntarjoajan on mahdotonta tehdä versionhallintaan tarvittavia tilannevedoksia. Versionhallinta on tärkeää siten, että se mahdollistaa vikatilan sattuessa datan vanhemman version hakemisen toiminnan varmistamiseksi. (Malmivaara 2022)

PiTuKri asettaa salaukselle 3 kriteeriä: salauskäytännöt ja avainhallinta (SA-01), salaus fyysisesti suojatun alueen ulkopuolella (SA-02) sekä salaus fyysisesti suojatun alueen sisäpuolella (SA-03). Salauskäytännöiden ja avaintenhallinnan rooli on varmistaa, että käytettävät salausmenetelmät luovat riittävän hyvän suojauksen tiedolle. (ks. liite 21 SA-01 salauskäytännöt ja avainhallinta) Salaus fyysisesti suojatun alueen ulkopuolella keskittyy tiedon pitämiseen salaisena fyysisen alueen ulkopuolella käyttäen hyväksyttyjä salausmenetelmiä ja tunnistusta. (ks. liite 22 SA-02 salaus fyysisesti suojatun alueen ulkopuolella) Kun taas salaus fyysisesti suojatun alueen sisäpuolella keskittyy tiedon suojaamiseen alueen sisällä fyysisin keinoin sekä salauksen avulla. (ks. liite 22 SA-03 salaus fyysisesti suojatun alueen sisäpuolella)

3.5 Puolustuksen automatisointi

Pilvipalvelut pystyvät myös puolustautumaan automatisoidusti. Pilvipalvelut pystyvät luomaan tilannekuvia palveluistansa, joiden avulla voidaan analysoida kaikkia pilvipalveluntarjoajan palveluja saadakseen tietoa, jota ne voivat hyödyntää palveluidensa suojaamisessa. Suuret palveluntarjoajat omaavat hyvin suuret resurssit, jonka vuoksi automaatio on viety niin pitkälle, että uhat voidaan huomata melkein reaaliajassa. Jos ulkopuolinen taho käyttää jo tunnettuja tekniikoita, voi pilvi hälyttää toiminnasta heti ja reagoida toimintaan, jos siihen on annettu lupa. Esimerkkejä mahdollisesta toiminnasta on käskeä vaihtamaan tunnusta, pakottaa kaksivaiheisen tunnistautumisen uudelleen tekemisen tai todeta että kone, josta yhteys on muodostettu, on uhka verkolle, kytkien koneen irti verkosta ja estäen liikenteen verkosta ennen kuin help-deskin yms. työntekijä käy varmistamassa koneen turvallisuuden. (Malmivaara 2022)

Automaattisessa puolustuksessa voidaan myös käyttää apuna muiden toimijoiden keräämää dataa. Pilvipalveluiden verkostoitumisella pilvipalvelut puolustavat toisiaan. Esimerkiksi Ukrainaan levinnyt Viper haittaohjelma tunnistettiin Malmivaaran mukaan kuudessa tunnissa Microsoftin toimesta, jonka jälkeen tunnisteet hyökkäyksen torjumiseksi jaettiin internettiin. Tällöin sen voisivat torjua kaikki dataan käsiksi päässeet. Tämän lisäksi voidaan myös skannata palveluita löytyneiden haavoittuvuuksien huomaamiseksi. Tällä voidaan helposti löytää, mistä palvelimista heikkous löytyy, jolloin ongelman korjaaminen on helppoa. Tällainen automaation mahdollisuus isoilla pilvipalveluidentarjoajilla onkin iso syy sille, miksi Malmivaara sanookin, että turvallisuuden suhteen laittaisi hän omat tietonsa pilveen konesalin sijasta. (Malmivaara 2022)

Jotkut pilvipalvelut seuraavat käyttäjiään ja luovat heille uhkaprofiilin. Jos käyttäjä käyttäytyy epätavallisesti, voi järjestelmä nostaa käyttäjän uhka tasoa. Epäilyttävästi käyttäytymistä voi olla esimerkiksi mustasta verkosta yhteyden muodostaminen tai vpn:ää käyttäen paikan useasti vaihtaminen pienen ajan sisällä. Kun käyttäjän uhkataso nousee, voi järjestelmä esimerkiksi pyytää monivaiheista tunnistautumista (multi-factor authentication) useammin tai reagoida käyttäjän tekemiin asioihin herkemmin. (Malmivaara 2022)

PiTuKrissa puhutaan järjestelmäturvallisuuden automaattisista kriteereistä kuten: jäljiteltävyys ja havainnointikyky (JT-01) sekä haittaohjelmasuojaus (JT-04). Jäljitettävyys ja havainnointikyky käsittelee sitä, kuinka järjestelmässä luvaton toiminta huomataan ja kuinka siihen suhtaudutaan. (ks. liite 23 JT-01 jäljitettävyys ja havainnointikyky) Haittaohjelmasuojaus käsittelee pilvipalvelussa ja sen ympäristössä oleviin menetelmiin ennaltaehkäistä, tunnistaa ja estää haittaohjelmia. (ks. liite 24 JT-04 Haittaohjelmasuojaus)

3.5.1 Defender

Defender on pilvipalveluissa toimiva työkalu, jolla voidaan tarkkailla tietoturvan tasoa ja hallita uhkia. Yksi esimerkki tällaisestä on Microsoft Defender. Tämä on Microsoftin tarjoama työkalu, jolla on kolme tärkeää tavoitetta: jatkuvasti arvioida tietoturvan tilaa, pitää palvelu turvallisena sekä puolustaa palvelua aktiivisesti. (What is Microsoft Defender for Cloud? 2022)

Defender käyttöliittymässä (ks. liite 25 Microsoft Defender yleiskatsaus sivu) nähdään kuusi ominaisuutta (Microsoft Defender for Cloud's overview page 2022):

- **Turvallisuuden taso:** Defender arvioi jatkuvasti käyttäjän resursseja, tilauksia sekä organisaatiota tietoturvaongelmien varalta. Sen jälkeen tulokset listataan yhteen pistearvoon, joka kertoo kokonaistilanteen. Mitä korkeammat pisteet, sitä pienempi on riskitaso.
- **Työtaakkojen suojaukset:** Defenderiin on integroitu edistynyt ja älykäs suojaus kaikille työtaakoille. Jokaista varten on eri suunnitelma. Tämä kohta käyttöliittymää näyttää yhdistettyjen resurssien kattavuuden.
- **Säännösten noudattaminen:** Defender antaa näkemyksen vaatimustenmukaisuudesta perustuen arviointeihin käyttäjän Azure ympäristöstä. Defender analysoi riskitekijöitä ympäristössä ja kartoittaa ne vaatimustenmukaisuuden kontrollereihin.
- **Palomuurien hallinta:** Kohta näyttää yhteenvedon keskittimistä ja verkoista Azure firewall managerissa.
- **Inventaario:** Ominaisuusinventaario tarjoaa yhden paikan käyttäjän turvallisuuden ryhdin katseluun. Inventaario listaa kaikki resurssit, ja ovatko ne turvallisia vai ei.

- **Tietojen suojaaminen:** Kohta näyttää kaikki resurssityypit, jotka defender on skannannut ja joiden on havaittu sisältävän arkaluontoista tietoa sekä joille löytyy suosituksia ja hälytyksiä.

3.6 Konfigurointi/käyttöönotto ja ylläpito

Pilvipalveluiden kanssa on erityisen tärkeää, että konfigurointi tehdään huolellisesti. Jos palvelua ei konfiguroida oikein, voi syntyä monenlaisia ongelmia. Tästä esimerkkinä palveluiden pohjustaminen väärälle mantereelle. Tällöin käyttäjän kaikki palvelut rakentuvat toiselle mantereelle, ja kaikki data talletetaan sinne, jolloin siihen kohdistuu eri lainsäädäntö. Konfigurointi vaihe on tärkeää tehdä hyvin. (Malmivaara 2022)

Pilvipalveluiden yhteydessä on myös hyvin tärkeää, että palvelua ylläpidetään säännöllisesti. Palveluihin usein tulee jatkuvasti lisää ominaisuuksia, palveluun tuleva uusi asetus voi vaikuttaa muihin jo ennalta oleviin asetuksiin. Tämän vuoksi on erityisen tärkeää olla koko ajan tietoinen siitä, mitä muutoksia palveluun tulee ja mitä se palvelun kannalta tarkoittaa. (Malmivaara 2022)

PiTuKri asettaa järjestelmäturvallisuuden käyttöönottoon ja ylläpidolle 3 kriteeriä: suojattavien kohteiden siirtäminen ja poistaminen (JT-05), järjestelmäkovennus (JT-02) sekä tiedon erottelu (JT-03). Suojattavien kohteiden siirtäminen keskittyy tiedon pitämisen turvassa, kun se siirretään fyysisesti suojattujen tilojen ulkopuolelle. (ks. liite 24 JT-05 suojattavien kohteiden siirtäminen ja poistaminen) Järjestelmäkovennus tarkoittaa järjestelmän asennusta siten, että se sisältää vain sen toiminnan kannalta välttämättömät toiminnallisuudet. (liite. 26 JT-02 järjestelmäkovennus) Tiedon erottelun tarkoitus on pitää huolta, että asiakkaiden salattu tieto säilytetään luotettavasti erillään muusta tiedosta, jolla varmistetaan, että vain asiakkaalla on pääsy tietoon. (ks. liite 27 JT-03 tiedon erottelu)

4 Yleisimmät palveluntarjoajat

Pilvipalveluiden kolme yleisintä palveluntarjoajaa ovat AWS, Azure ja GCP. Amazon Web Services (AWS) on Amazonin tarjoama pilvipalvelualusta. Vuonna 2006 julkaistu AWS on vanhin kolmesta palvelusta. Microsoft Azure on Microsoftin kehittämä pilvipalvelualusta, joka julkaistiin vuonna 2010. Google Cloud Platform (GCP) on kolmikon uusin tulokas, joka on julkaistu kaikille saatavaksi vuonna 2011. Google kuitenkin ilmoitti GCP:stä jo vuonna 2008. Muita pilvipalveluntarjoajia ovat esimerkiksi IBM, Alibaba Cloud ja Oracle

4.1 Palvelut

Kaikki kolme palveluntarjoajaa tarjoavat suuren valikoiman erilaisia palveluita. Muutamia yleisiä palveluja ovat erilaiset laskentateholliset palvelut kuten virtuaalikoneet, kehitysalustat, konteinerit sekä serverittömät funktiot. Näiden palveluiden tarkoitus on antaa asiakkaalle laskentatehoa käyttöönsä tarpeen vaatiessa.

Palvelu	AWS	Azure	GCP
Laskentateho	Amazon EC2	Virtuaalikoneet	Google compute engine
PaaS	AWS Elastic Beanstalk	App service	Google app engine
konteinerit	Amazon Elastic container ja Kubernetes services (ECS ja EKS)	Azure Kuberneter service (AKS)	Google Kubernetes Engine
serverittömät funktiot	AWS Lambda	Azure Functions	Google Cloud Functions

Taulukko 1. Laskentateho palveluita vertailuna AWS, Azure ja GCP

Pilvipalveluihin tallennetaan paljon dataa. Data voi vaihdella paljon, mutta yleisimmin käytettävät palvelut ovat tallennustila sekä tietokantojen hallinnointi. Tallennusmuotoja on paljon, jonka vuoksi myös palveluja on paljon. Eri palveluntarjoajilla on erilainen kokoelma tallennustilaan sekä tietokantoihin liittyviä palveluita. AWS on jakanut tallennustila palvelunsa objekti, tiedosto ja datalohkot neljään palveluun (Cloud Storage on AWS n.d.):

- **Amazon Simple Storage Service (S3):** Amazonin objektitallennus palvelu.
- **Amazon Elastic File System (EFS):** Simppeli, serveritön tiedostojen datakäsittely ilman tarvetta hallinnoida tallennustilaa
- **Amazon FSx:** Täysin hallinnoitu ja kustannustehokas tiedostotallennus palvelu, joka tarjoaa open-source mahdollisuuksia.
- **Amazon Elastic Block Store (EBS):** Helppokäyttöinen tehokas lohkotallennus palvelu.

Microsoft Azure puolestaan on jakanut tallennustila palvelunsa viiteen palveluun (Introduction to Azure Storage 2022):

- **Azure Blobs:** Suuresti skaalautuva tallennustila teksti ja binääri datalle.
- **Azure Files:** Hallinnoitu tiedostonjako pilvi ja on-premises palveluille
- **Azure Queues:** Viestientallennuspalvelu luotettavaan viestittelyyn applikaatioiden komponenttien välillä
- **Azure Tables:** NoSQL tietokanta palvelu.
- **Azure Disks:** Lohkotason tallennustila azure virtuaalikoneille.

GCP on jakanut tallennustilansa objekti, tiedosto ja lohko osiot neljään palveluun (Google Cloud online storage products n.d.):

- **Cloud storage:** Objektitallennus yrityksille. Voit tallentaa minkä tyyppistä tahansa dataa ja hakea sitä niin usein, kun haluat.
- **Persistent disk:** Google Cloud tuotteiden kanssa täysin integroitu lohkotallennus palvelu.
- **Local SSD:** Lyhtyaikainen paikallisesti kiinnitetty lohkotallennustila virtuaalikoneille sekä konteinereille
- **Filestore:** Täysin hallinnoitu palvelu migraatiolle ja tallennustilalle.

Tietokannat ovat järjestettyjä kokoelmia dataa, tyypillisesti massiivisia koossaan. Ne on suunniteltu tallentamaan dataa muotoon, jossa sitä on nopea käsitellä. ”Structured Query Language” (SQL) on standardoitu koodikieli, jota käytetään re-

laatiotietokantojen hallintaan. Relaatiotietokanta tallentaa datapisteitä, jotka liittyvät toisiinsa. Relaatiotietokannoissa data esitetään taulukossa, jossa jokainen taulukon rivi on tietue, jolla on uniikki ID ja taulukon sarakkeet sisältävät datan attribuutteja. ”Not only SQL” (NoSQL) viittaa ei-relaatiotietokantoihin. Tämä tarkoittaa, että data on tallennettu taulukkoon eri formaatissa kuin relaatiotietokannoissa. NoSQL tietokannoissa voidaan kuitenkin tehdä kyselyjä käyttämällä idiomaattisten kielten sovellusliittymiä, deklaratiivisia rakenteellisia kyselykieliä ja kyselykohtaisia esimerkkikieliä, jonka vuoksi niitä kutsutaan ”ei vain SQL” tietokannoiksi. (Oracle n.d.) Pilvipalvelut tarjoavat usein palveluita tietokantojen ylläpitoon.

Tietokanta	AWS	Azure	GCP
Relaatio (SQL)	Amazon RDS	Azure SQL Database	Google Cloud SQL
Ei relaatio (NoSQL)	Amazon DynamoDB ja Simple DB	Azure Cosmos DB ja Table Storage	Google Datastore

Taulukko 2. Yksinkertaiset tietokanta palvelut AWS, Azure ja GCP

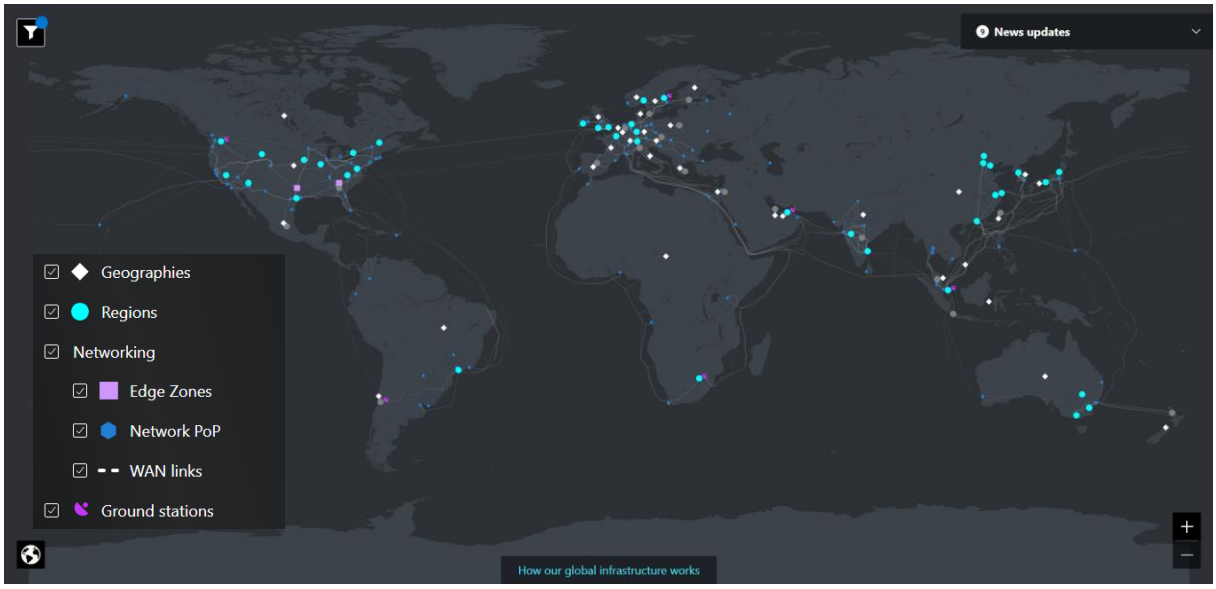
4.2 Saatavuus vyöhykkeet

Kaikilla palveluilla on palveluita ympäri maailman. Palvelut jaetaan tyypillisesti saatavuus- (Availability Zone, AZ) tai maantieteellisiin vyöhykkeisiin (Region). Maantieteelliset vyöhykkeet kuvaavat datakeskuksien rykelmää tietyllä maantieteellisellä alueella, kun taas saatavuus vyöhykkeet kuvaavat fyysisesti erillisiä datakeskuksia maantieteellisen vyöhykkeen sisällä. (Regions and availability zones 2022)

AWS:llä on 84 saatavuusvyöhykettä jaettuna 26 maantieteelliseen vyöhykkeeseen (kuvio 7). Tämä sisältää 245 maata ja territoriota. (AWS Global Infrastructure n.d.)

KUVIO 7. AWS maantieteelliset vyöhykkeet (AWS Global Infrastructure n.d.)

Microsoft Azurella on 60 maantieteellistä vyöhykettä (kuvio 8), joissa kaikissa on vähintään 3 saatavuusvyöhykettä. Tähän sisältyy yli 200 maata.



KUVIO 8. Microsoft Azuren saatavuus maailmanlaajuisesti

GCP:llä on 32 maantieteellistä vyöhykettä, jotka sisältävät yhteensä 97 saatavvus vyöhykettä (kuvio 9). Tähän sisältyy yli 200 maata ja territoriota (Cloud locations n.d.)

KUVIO 9. GCP nykyiset ja tulevat maantieteelliset vyöhykkeet (Cloud locations n.d.)

4.3 Tietoturva

Kaikki kolme palveluntarjoajaa tarjoavat palveluittensa tietoturvasta dokumentointia. AWS ja Azure listaavat palvelunsa huomattavasti selkeämmin kuin Google.

AWS listaa 26 palvelua, jotka ovat jaettu kuuteen kategoriaan: Identiteetti- ja pääsynhallinta, havaitseminen, Verkko- ja sovellussuojaus, datan suojelu, tapausreaktio ja vaatimustenmukaisuus. Näihin sisältyy esimerkiksi ”Amazon GuardDuty” joka automatisoi puolustusta, ”AWS shield” joka suojaa palveluita DDoS-hyökkäyksiltä ja ”AWS Identity and Access Management (IAM)” jolla suoritetaan indentiteetin- ja pääsynhallintaa AWS:n sisällä. (Security, Identity, and Compliance on AWS n.d.)

Azure listaa 35 palvelua jaettuna kuuteen kategoriaan: yleinen Azuren turvallisuus, tallennustilan turvallisuus, tietokantojen turvallisuus, indentiteetti- ja pääsynhallinta, varmuuskopiointi ja onnettomuuksista toipuminen sekä verkkotyöskentely. Näihin sisältyy esimerkiksi ”Microsoft Defender” joka automatisoi puolustusta, ”Azure DDoS protection” joka suojaa palveluita DDoS-hyökkäyksiltä ja

”Azure storage Service Encryption” joka automaattisesti salaa datan, joka tallennetaan Azureen. (Security services and technologies available on Azure 2022)

GCP:n dokumentaatio tietoturvapalveluista on kaikista suppein. GCP tarjoaa sivuillansa tietoturva ratkaisuista neljä eri kategoriaa: riski ja vaatimustenmukaisuus koodina (RCaC), tietoturva-analytiikka ja operaatiot, turvallisuus- ja joustavuuskehitys sekä verkkosovellus ja API-suojaus (WAAP). Näissä artikkeleissa käsitellään Googlen palveluita kuten ”Cloud Armor” jolla automatisoidaan puolustusta sekä suojellaan palvelua DDoS-hyökkäyksiä vastaan sekä ”Apigee” jolla suunnitellaan, analysoidaan sekä suojellaan ohjelmointirajapintoja (API). (Protect your organizations with Google Cloud security solutions n.d.)

Vaikka palveluiden dokumentaatio eroaa paljon, suojaavat ne silti paljon samoja asioita. Tämän vuoksi on vaikeaa hahmottaa, kenellä on paras tietoturva. Voidaan kuitenkin nähdä, että kaikki kolme palveluntarjoajaa kiinnittävät paljon huomiota palveluidensa turvallisuuteen.

4.4 Hinta

Pilvipalveluiden hinta on sidonnaista käytettyyn palveluun sekä mahdollisen tarvittavan laskentatehon tarpeeseen. Kaikilla kolmella palveluntarjoajalla on netissä laskuri, jolla hinnan voi laskea. Tämän lisäksi palveluntarjoajat saattavat tarjota alennuksia esimerkiksi pitkäaikaisen palvelun oston yhteydessä.

Palveluistansa kannattaa kuitenkin aina maksaa. Palveluntarjoajat pyörittävät yrityksiä ja yritysten tavoite on aina tehdä rahaa. Tämän vuoksi, jos palveluistansa ei maksa, voi palveluntarjoaja esimerkiksi myydä käyttäjän tietoja eteenpäin tehdäkseen palvelunsa tuottoisaksi.

5 POHDINTA

Opinnäytetyön tavoitteena oli kerätä tietoa siitä, mitä pilvipalvelut ovat, kuinka niiden tietoturva toimii ja miksi pilvipalveluita kannattaisi käyttää. Työssä kerrottiin lukijalle pilvipalveluiden käsitteestä, yleisimmistä toteutusmalleista, pilvipalveluiden hyödyistä ja haitoista sekä pilvipalveluiden tietoturvasta yleisellä tasolla. Työssä kerrottiin myös hahmottamisen helpottamisen vuoksi kolmesta suurimmasta pilvipalveluntarjoajasta ja heidän toiminnoistaan yleisesti.

Työssä käsiteltiin todella laajaa aihepiiriä hyvin yleisellä tasolla, jonka vuoksi työ antaa hyvän peruskuvan aiheesta kiinnostuneelle, jonka avulla voidaan tehdä omaa jatkotutkimusta alan tarkemmista käytännöistä. Työn lähteinä käsiteltiin pääasiassa pilvipalveluasiantuntija firmojen sivuja, jonka vuoksi tietoa kerättiin useilta eri sivustoilta tiedon puolueettomuuden varmistamiseksi. Työssä käytettiin myös TUNI:n asiantuntija haastattelua.

Tietoa hankkiessa tarjontaa riitti. Palveluntarjoajilla on hyvin suuret dokumentaatiot omasta toiminnastaan, mutta oikean tiedon löytäminen on vaikeaa tiedon hankalan muodon vuoksi. Useat palveluita myyvien yritysten nettisivut tarjoavat hyvin ytimekkäitä myyntipuheita palveluista. Tämä saattaa olla koska yritykset haluavat myydä omia palvelujansa suuren pilvipalveluntarjoajan palveluiden päälle. Tämän lisäksi useat blogityyppiset nettisivut tarjoavat mielipidekirjoituksia pilvipalveluiden asiantuntijoilta mahdollisesti saadakseen lisää tietoliikennettä sivuillensa.

Työn pohjalta voin todeta, että pilvipalveluissa on selkeästi hyviä puolia. Ne ovat joustava tapa tuottaa helposti skaalautuvia palveluita helposti paikasta riippumatta, jossa tiedonkäsittelyn automatisaatiota voidaan helposti käyttää hyödyksi. Niissä on kuitenkin myös omat ongelmansa internet yhteyden pakollisuuden, virheiden vahingollisuuden yms. kanssa. Tämän vuoksi ei voida selkeästi osoittaa kannattaisiko pilvipalveluita käyttää, vaan se on aina tapauskohtainen päätös asiakkaan toimesta. Esimerkiksi lainsäädäntö ei aina salli pilvipalveluiden käyttöä tietynlaisen datan kanssa. Tietoturvan osalta pilvipalvelut ovat kuitenkin yleensä riittävän tietoturvallisia, jos tietoruvaresursseja on palveluntarjoajalla riittävästi.

Tällöin voidaan automatisoida paljon eri palveluita, jolloin tietomurtojen tunnistuksesta tulee huomattavasti nopeampaa ja tehokkaampaa. Tämän vuoksi kannattaakin suosia suurempia palveluntarjoajia pienempien sijasta. Tulee kuitenkin pitää mielessä, että vaikka tietoturvan taso saattaa nousta, nousee myös uhkien määrä huomattavasti tiedon siirryttyä internettiin. Tällöin virheiden vaikutus korostuu huomattavasti. Kun toimitaan pilvipalveluiden tietoturvan parissa, on kuitenkin aina kyseessä jaettu vastuumalli. Tällöin palvelusta riippuen asiakas on myös itse vastuussa omasta turvallisuudestaan.

Lähtökohtaisesti kaikkien käyttäjien tulisi käyttää vähintään kaksivaiheista tunnistautumista palveluissa, mutta lisäturvaa omalle datallesi saat helposti, jos salaat sen omalla laitteellasi ennen sen vientiä pilveen. Näin ollen, jos datasi varastetaan, ei sitä voida lukea ilman erillistä salausavaintasi.

Työn aihe valittiin omasta mielenkiinnosta pilvipalveluihin ja tietoturvaan. Työn aihe oli itselleni pääasiassa uutta, ja varsinkin tietoturva osio oli haastava tiivistää informaation määrän ja tyypin vuoksi. Informaatiota on valtava määrä, ja siitä on vaikea eristää ”pääpointteja” jonka vuoksi oli hankalaa hahmottaa mihinkö tulisi keskittyä. Työn tavoitteet kuitenkin tulivat pääosin täyteen, jolloin työtä voidaan pitää onnistuneena. Työstä voitaisiin tehdä jatkotutkimus esimerkiksi järjestelmäkehityksen vaikutuksesta tietoturvaan.

LÄHTEET

AWS Global Infrastructure n.d. AWS. Verkkosivu. Viitattu 21.5.2022 https://aws.amazon.com/about-aws/global-infrastructure/

Bluepi. 2015. Different types of cloud computing service models. Verkkosivu. Viitattu 25.4.2022 https://www.bluepiit.com/blog/different-types-of-cloud-computing-service-models/

Cloud locations. n.d. Google. Verkkosivu. Viitattu 21.5.2022. https://cloud.google.com/about/locations#regions

Cloud Storage on AWS. n.d. AWS. Verkkosivu. Viitattu 21.5.2022 https://aws.amazon.com/products/storage/

Compliance with EU transfer requirements for personal data in the Microsoft cloud. 2021. Microsoft Pdf-dokumentti. Viitattu 18.4.2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRql1?culture=en-us&country=US

CompTIA. n.d. What is SaaS? Verkkosivu. Viitattu 6.4.2022 https://www.comptia.org/content/articles/what-is-saas

Evolve. n.d. What are the disadvantages of cloud computing. Verkkosivu. Viitattu 23.5.2022 https://evolve.ie/q-and-a/what-are-the-disadvantages-of-cloud-computing/

Flowers, R. 2021. Business Advantages and Disadvantages of Hybrid cloud. Connectria-blogi. 2021. Viitattu 18.4.2022.https://www.connectria.com/blog/business-advantages-and-disadvantages-of-hybrid-cloud/

FPComplete. 2020. Cloud Deployment Models: Advantages and Disadvantages. Verkkosivu. Viitattu 17.4.2022. https://www.fpcomplete.com/blog/cloud-deployment-models-advantages-and-disadvantages/

Global infrastructure. n.d. Microsoft Azure. Verkkosivu. Viitattu 31.5.2022 https://infrastructuremap.microsoft.com/explore

Google Cloud online storage products. n.d. Google. Verkkosivu. Viitattu 21.05.2022 https://cloud.google.com/products/storage

IBM. 2021. IaaS vs. PaaS vs. SaaS. Verkkosivu. Viitattu 6.4.2021. https://www.ibm.com/cloud/learn/iaas-paas-saas

IBM. 2022. Top 5 advantages of Software as a Service (SaaS). Verkkosivu. Viitattu 6.4.2022. https://www.ibm.com/cloud/blog/top-5-advantages-of-software-as-a-service

Introduction to Azure Storage. 2022. Microsoft. Verkkosivu. Viitattu 21.5.2022 https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction

Johnston, S. 2009. Cloud computing. Kuva. Viitattu 8.3.2022 https://fi.wikipedia.org/wiki/Pilvipalvelu#/media/Tiedosto:Cloud_computing.svg

Krasteva, V. n.d. Private vs Public cloud: Pros and Cons. Verkkosivu. Viitattu 17.4.2022. https://composity.com/post/private-vs-public-cloud-pros-and-cons

Käyttäjätietojen ja käytön hallinta. n.d. Microsoft. Verkkosivu. Viitattu 24.4.2022. https://www.microsoft.com/fi-fi/security/business/identity-access-management

Malmivaara, J. Tietoturvapäällikkö. Haastattelu 9.5.2022. Haastattelija Elväs, S. Teams-haastattelu

Mell & Grance. 2011. Cloud computing deployment models. Verkkosivu. Viitattu 25.4.2022 https://www.researchgate.net/figure/Cloud-Computing-Deployment-Models-Mell-and-Grance-2011_fig2_275036700

Mell, P & Grance, T. 2011. The NIST definition of cloud computing. Pdf-dokumentti. Viitattu 9.3.2022. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft Defender for Cloud's overview page. 2022. Microsoft. Verkkosivu. Viitattu 13.5.2022. https://docs.microsoft.com/en-us/azure/defender-for-cloud/overview-page

MongoDB. N.d. Database as a Service (DBaaS) Explained. Verkkosivu. Viitattu 28.5.2022 https://www.mongodb.com/database-as-a-service

Morefield. 2019. Pros and Cons of Cloud Computing. Blogi. Viitattu 23.5.2022 https://www.morefield.com/blog/pros-and-cons-of-cloud-computing/

Oracle. n.d. What Is a Database?. Verkkosivu. Viitattu 22.5.2022 https://www.oracle.com/database/what-is-database/

Pilvipalveluiden turvallisuuden arviointikriteeristö. 2020. Kyberturvallisuuskeskus. Pdf-dokumentti. Viitattu 18.4.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Pilvipalveluiden turvallisuus. n.d. Pdf-dokumentti. Viitattu 8.4.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Protect your organizations with Google Cloud security solutions. n.d. Google. Verkkosivu. Viitattu 24.5.2022 https://cloud.google.com/solutions/security

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. 2020. Pdf-dokumentti. Viitattu 18.4.2022. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Regions and availability zones. 2022. Microsoft. Verkkosivu. Viitattu 21.5.2022 https://docs.microsoft.com/en-us/azure/availability-zones/az-overview

Ronald, B. 2010. Security token. Kuva. Viitattu 25.4.2022 https://en.wikipedia.org/wiki/Security_token#/media/File:CryptoCard_two_factor.jpg

Roslund, R. 2017. Top secret – Suomessa on hyvin tarkkaan rajattu joukko ihmisiä, jotka saavat nähtäväkseen Helsingin Sanomille vuodetun kaltaista huippusalaista tietoa. Yle Uutiset 18.12.2017. Viitattu 20.5.2022. https://yle.fi/uutiset/3-9983438

Salesforce. N.d. 12 Benefits of Cloud Computing. Verkkosivu. Viitattu 19.5.2022 https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/

Security, Identity, and Compliance on AWS. n.d. AWS. Verkkosivu. Viitattu 24.5. https://aws.amazon.com/products/security/

Security services and technologies available on Azure. 2022. Microsoft. Verkkosivu. Viitattu 24.5.2022. https://docs.microsoft.com/en-us/azure/security/fundamentals/services-technologies

Sharma, H. 2022. Advantages and Disadvantages of Cloud Computing. Verkkosivu. Viitattu 23.5.2022. https://intellipaat.com/blog/tutorial/amazon-web-services-aws-tutorial/advantages-and-disadvantages-of-cloud-computing/

Stackscale. 2021. Main cloud service models: IaaS, PaaS and SaaS. Verkkosivu. Viitattu 9.3.2022. https://www.stackscale.com/blog/cloud-service-models/

Taylor, K. n.d. Advantages and Disadvantages of IaaS. Verkkosivu. Viitattu 18.4.2022. https://www.hitechnectar.com/blogs/advantages-disadvantages-of-iaas-explained/

Twilio. n.d. What is two-factor authentication (2fa)?. Verkkosivu. Viitattu 25.4.2022 https://authy.com/what-is-2fa/

Watts, S. & Raza, M. 2019. SaaS vs PaaS vs IaaS: What's the difference& how to choose. Bmc-blogi. 15.6.2019. Viitattu 8.4.2022. https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

What are public, private, and hybrid clouds?. n.d. Microsoft Azure. Verkkosivu. Viitattu 17.4.2022. https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/#overview

What is Microsoft Defender for Cloud?. 2022. Microsoft. Verkkosivu. Viitattu 13.5.2022 https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

LIITTEET

Liite 1. IP-01 Käyttöoikeushallinta

IP-01	Käyttöoikeushallinta
Vaatimus	1) Käyttöoikeuksien hallinnointi toteuttaa vähimpien oikeuksien periaatetta: a) Käyttäjätilien luontiin, hyväksymiseen ja ylläpitoon on ennalta määritelty prosessi. b) Tietojenkäsittely-ympäristön käyttäjille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat tehtävien suorittamiseksi välttämättömiä. c) Järjestelmän käyttäjistä ylläpidetään listaa. Jokaisesta myönnetystä käyttöoikeudesta jää merkintä. d) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. e) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. f) Käyttö- ja pääsyoikeudet pidetään ajan tasalla. Tarpeettomat käyttäjätilit ja oikeudet poistetaan, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta tai kun käyttäjätiliä ei ole käytetty ennalta määritettyyn aikaan). g) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. h) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti, vähintään puolivuosittain.
Soveltuvuus	Verkkolaitteet, palvelimet, tietojärjestelmät sekä työasemat ja muut päätelaitteet.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Käyttöoikeuksien hallinnointi toteuttaa vähimpien oikeuksien periaatetta: Käyttäjätunnukset on myönnetty ja luovutettu vain niille, joilla on niihin oikeus ja tehtävään/rooliin liittyvä tarve. Käyttöoikeudet on rajattu vain välttämättömiin toiminnallisuuksiin, sovelluksiin, laitteisiin ja verkkoihin.
Lisätietoja	Käyttöoikeuksien hallinnan keskeinen tavoite on pystyä varmistumaan siitä, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattavaan tietoon. Käyttöoikeuksien taustalla on suositeltavaa olla jokin sopimus tai muu dokumentoitu peruste, joka voidaan todentaa (esim. työsuhde, sopimus toteutettavasta työstä ympäristössä). Kaikkien käyttäjätunnusten osalta on huolehdittava tunnusten elinkaaresta siten, että vain tarpeelliset tunnukset ovat voimassa ja aktiivisia ja tarpeettomat käyttäjätunnukset poistetaan välittömästi. Käyttöoikeudet tulee rajata vain toiminnallisen tarpeen edellyttämään osajoukkoon. Tarpeettoman laajat oikeudet mahdollistavat ko. käyttäjälle, prosessille tai edellä mainitut haltuun saavalle hyökkääjälle tarpeettoman laajat toimintamahdolliset. Käyttöoikeuksien rajaamisella vähimpien oikeuksien periaatteen mukaiseksi voidaan pienentää sekä tahallisten että tahattomien tekojen, kuin myös esimerkiksi haittaohjelmista aiheutuvia riskejä. Erityisesti tulee huomioida, että ylläpito-oikeuksia käytetään vain ylläpitotoimiin. Ylläpitotunnuksella varustettua käyttäjätiliä ei tule käyttää esimerkiksi web-selailuun tai sähköpostin käyttöön. Pääsyoikeuksien ajantasaisuudesta varmistuminen edellyttää yleensä sitä, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esimerkiksi kuuden kuukauden välein. Tehtävänkuvan muutoksissa ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen ja poistamiseen on oltava selkeä, sovittu menettely. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan pidettyä ajantasaisina. Tämä voi edelleen tarkoittaa sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen. Vaatimuksen soveltamisessa tulee huomioida vastuujako pilvipalveluntarjoajan ja asiakkaan välillä. Tyypillisesti pilvipalveluntarjoaja on vastuussa pilvipalvelun tuottamiseen liittyvän järjestelmäkokonaisuuden käyttöoikeushallinnasta, asiakkaan vastuun koskiessa palveluntarjoajan palvelukokonaisuuden (IaaS, PaaS tai SaaS) päälle rakentuvan osuuden käyttöoikeushallintaa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaankin huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 2. IP-02 Käyttäjätunnistus

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 yksilöinnin 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 varmistuminen 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 varmistuminen. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 3. IP-03 Hallintayhteydet

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. hallinta-yhteyden kautta pystytään vaarantamaan pilvipalvelussa käsiteltävät tiedot. Useimmat hallinta-yhteystavat mahdollistavat pääsyn tietoon joko suoraan (esimerkiksi tietokantaylläpito pääsee yleensä tarvittaessa tietokannan sisältöön) tai epäsuoraan (esimerkiksi verkkolaiteylläpito pystyy yleensä muuttamaan tietojärjestelmää suojaavia palomuurisääntöjä). 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 hallinta-liikenteen turvallisuuskriittisestä luonteesta johtuen mahdollista heikommin suojatuista ympäristöistä tai päätelaitteista käsin. Turvallisuusluokiteltua tietoa sisältävän pilvipalvelualustan hallinnointi tulee-kin 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 (Käyttöoikeus-hallinta), 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 turvallisuus-alueen 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 hyppykone-käytäntöä, jossa kaikki hallintatoimet toteutetaan ja kirjataan (lokitetaan) hyppykoneen kautta. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaa-vat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 4. HT-01 Työsuhteen elinkaaren huomioiminen ja HT-02 henkilöstön luotettavuuden arviointi

HT-01	Työsuhteen elinkaaren huomioiminen
Vaatimus	1) Organisaatiolla on käytössä turvallisuuden huomioon ottava menettely työsuhteen elinkaaren eri vaiheissa. Erityisesti huomioidaan toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Henkilöstöön liittyvien riskien pienentäminen työsuhteen elinkaaren aikana.
Lisätietoja	Turvallisuustekijät huomioon ottava menettely edellyttää tyypillisesti menettelyohjeita, jotka on koulutettu ja saatavilla tarvittavilla henkilöstöryhmillä. Menettelyohjeet voidaan jakaa esimerkiksi työsuhteen elinkaaren mukaisiin kokonaisuuksiin. Ohjekokonaisuuksia voivat olla esimerkiksi rekrytointiohjeet, perehdyttämisohjeet, työsuhteen aikaisten muutosten ohjeet, työsuhteen päättymisen ohjeet ja ohjeet yksityiskohtaisempiin toimiin kuten esimerkiksi ohjeet käyttö- ja pääsyoikeuksien muutoksiin. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

HT-02	Henkilöstön luotettavuuden arviointi
Vaatimus	1) Pilvipalvelun asiakkaiden tietoja tai yhteistä IT-infrastruktuuria käyttämään pääsevien sisäisten ja ulkoisten työntekijöiden taustat tarkistetaan paikallisen lainsäädännön mahdollistamien menettelyjen mukaisesti ennen työsuhteen alkua. Lainsäädännön sallimissa rajoissa tarkistukseen sisällyttävä vähintään: a) Henkilöllisyyden todentaminen. b) Työhistorian todentaminen. c) Koulutustaustan todentaminen. 2) Turvallisuusluokiteltujen aineistojen käsittelyyn liittyvien henkilöiden luotettavuus selvitetään ja sitä seurataan asianmukaisen tason turvallisuusselvitysmenettelyin.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 2: TL IV & KV-R, TL III (kasauma) (keskeiset turvallisuusvastaavat, tekniset ylläpitäjät tai vastaavat henkilöt, joilla on pääsy suureen määrään TL IV -tietoa tai mahdollisuus vaikuttaa näiden tietojen suojaamiseen.)
Suojaustavoite	Henkilöstön luotettavuuteen liittyvien riskien pienentäminen.
Lisätietoja	2) Mikäli on olemassa suora tai epäsuora pääsy asiakkaiden suojattaviin tietoihin. Esimerkiksi virtualisointialustan (hypervisor) ylläpidolla on usein käytännössä pääsy myös virtuaalikoneissa käsiteltäviin asiakkaiden tietoihin. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 5. HT-03 Salassapito- ja vaitiolosopimukset ja HT-04 Turvallisuustietoisuus

HT-03	Salassapito- ja vaitiolositoumukset
Vaatimus	1) Salassapito- tai vaitiolositoumusmenettely on käytössä. Salassapitosopimukset on allekirjoitettava ennen sopimussuhteen alkamista tai ennen kuin pilvipalvelun asiakkaiden tietoja koskeva käyttöoikeus myönnetään.
Soveltuvuus	Pilvipalvelun tarjoajan sisäisten työntekijöiden, ulkoisten palveluntarjoajien ja toimittajien henkilöstö.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Henkilöstön luotettavuuteen liittyvien riskien pienentäminen erityisesti tietoisuuden lisäämisellä.
Lisätietoja	Salassapitosopimuksessa (tai vast.) tulee kuvata vähintään seuraavat asiat: • Mitä tietoja on käsiteltävä salassa pidettävinä • Salassapitosopimuksen ehdot • Mihin toimiin on ryhdyttävä, kun sopimus päättyy (eli esimerkiksi tietovälineet on tuhottava tai palautettava) • Kuka omistaa tiedot • Mitkä säännöt ja säädökset koskevat salassa pidettävien tietojen käyttöä ja luovuttamista muille osapuolille, jos tarpeen • Seuraamukset salassapitosopimuksen ehtojen rikkomisesta. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

HT-04	Turvallisuustietoisuus
Vaatimus	1) Keskeiset turvallisuuteen liittyvät periaatteet ja toimintatavat on kuvattuna. 2) Turvalliset toimintatavat on henkilöstölle jalkautettuna siten, että henkilöstön riittävästä turvatietoisuudesta pystytään varmistumaan. 3) Turvallisuuteen liittyvien kuvausten/ohjeistusten ajantasaisuus sekä jalkauturninen käytäntöön varmistetaan säännöllisesti, vähintään vuosittain. 4) Turvallisuuteen liittyvät ohjeet kattavat henkilötietoihin ja salassa pidettävään tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta. 5) Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti.
Soveltuvuus	Pilvipalvelun tarjoajan sisäisten työntekijöiden, ulkoisten palveluntarjoajien ja toimittajien henkilöstö.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuuteen liittyvillä periaatteilla (vrt. TJ-01) ja kuvauksilla/ohjeistuksilla sekä niiden jalkauttamisella tavoitellaan sitä, että turvalliset toimintatavat on suunniteltu ja että henkilöstö pystyy käytännössäkin toimimaan turvallisesti, huomioiden myös erikoistilanteet. Vrt. KT-01 (Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi).
Lisätietoja	Turvallisuusvastuiden määrittely on oleellista, jotta vastuuhenkilöt voivat toteuttaa heidän vastuullaan olevat turvallisuustehtävät. Mikäli muuta ei ole kuvattu, ovat turvallisuusvastuut organisaation johdolla. Vrt. TJ-02 (Turvallisuuden vastuut). Vaatimuksen täyttämisessä voidaan hyödyntää esimerkiksi seuraavaa menettelyä: 1) Henkilöstölle annetaan ohjeet ja koulutusta salassa pidettävien tietojen asianmukaisesta käsittelystä. 2) Salassa pidettävien tietojen käsittelyä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneet henkilöt dokumentoidaan. 3) Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti. 4) Tietoturvaa koskevat kohderyhmittäin räätälöidyt turvallisuuskoulutukset ja turvallisuustietoisuuden kehittämisohjelmat ovat tarjolla ja pakollisia kaikille pilvipalvelun tarjoajan sisäisille ja ulkoisille työntekijöille. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 6. HT-05 Tiedonsaantitarpeet ja tehtävien erottelu

HT-05	Tiedonsaantitarpeet ja tehtävien erottelu
Vaatimus	1) Salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä ylläpidetään luetteloa. Tällaisiksi työtehtäviksi tulkitaan kuuluvaksi myös sellaiset kehitys- ja ylläpitotehtävät, joissa on suora tai epäsuora mahdollisuus päästä salassa pidettävään tietoon, tai muuten oleellisesti vaikuttaa salassa pidettävän tiedon suojauksiin. 2) Pääsy salassa pidettävään tietoon voidaan myöntää vasta, kun henkilön työtehtävistä johtuva tiedonsaantitarve on selvitetty. 3) Luetteloa turvallisuusluokiteltujen tietojen käsittelyoikeuksista ylläpidetään luokittain. 4) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi. 5) Turvallisuusluokan III kasaumalle lisäksi: Kriittiset tehtävät ja vastuualueet on eriytetty eri henkilöille, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Erityishuomiota kiinnitettävä siihen, että yksittäinen henkilö ei pysty poistamaan toimiensa jälkiä tai merkittävästi estämään poikkeavien toimien havaitsemista.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 3-4: TL IV & KV-R, TL III (kasauma) 5: TL III (kasauma)
Suojaustavoite	Suojaustavoitteena on mahdollistaa salassa pidettävän tiedon päätyminen vain valtuutetuille henkilöille tiedonsaantitarpeen (need-to-know) mukaisesti, ja siten pienentää salassa pidettävään tietoon kohdistuvia riskejä.
Lisätietoja	Tiedonsaantitarpeen määrittämistä helpottaa se, että organisaatio on kuvannut periaatteet, jolla organisaation henkilöt pääsevät salassa pidettäviin tietoihin, sekä prosessin tai menettelytapaohjeet, joilla työtehtäväperusteisesti pääsy myönnetään ja hallinnoidaan muutostilanteissa. Käsittelyoikeusmäärittelyissä sekä työtehtävä- ja roolimäärittelyissä tulisi ottaa huomioon, ettei synny vaarallisia työ- tai rooliyhdistelmiä. Useimmissa järjestelmissä riittävä tehtävien erottelu on toteutettavissa järjestelmän ylläpitoroolien (ja henkilöiden) ja lokien valvontaan osallistuvien roolien (ja henkilöiden) erottelulla toisistaan. Usein käytettynä valvontamekanismina on myös se, että kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän ("two man rule"). Vaatimuksen arvioinnissa tulee huomioida myös vastuujako pilvipalveluntarjoajan ja asiakkaan välillä. Pilvipalveluntarjoaja ei tyypillisesti pysty vaikuttamaan esimerkiksi asiakkaan vastuulla olevan järjestelmäosuuden kehittäjien tai ylläpitäjien tiedonsaantitarpeen varmistamiseen. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaankin huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 7. EE-01 Järjestelmäkuvaus

EE-01	Järjestelmäkuvaus
Vaatimus	1) Pilvipalvelusta on järjestelmäkuvaus. Pilvipalveluntarjoajan kuvauksen perusteella on pystyttävä arvioimaan kyseisen pilvipalvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Järjestelmäkuvauksesta tulee käydä ilmi vähintään: a) Pilvipalvelun palvelu- ja toteutusmallit, sekä näihin liittyvät palvelutasosopimukset (Service Level Agreements, SLAs). b) Pilvipalvelun tarjoamisen elinkaaren (kehittäminen, käyttö, käytöstä poisto) periaatteet, menettelyt ja turvatoimet, valvontatoimet mukaan lukien. c) Pilvipalvelun kehittämisessä, ylläpidossa/hallinnassa ja käytössä käytettävän infrastruktuurin, verkon ja järjestelmäkomponenttien kuvaus. d) Muutostenhallinnan periaatteet ja käytännöt, erityisesti turvallisuuteen vaikuttavien muutosten käsittelyprosessit. e) Käsittelyprosessit merkittäville normaalikäytöstä poikkeaville tapahtumille, esimerkiksi toimintatavat merkittävissä järjestelmävikaantumisissa. f) Pilvipalvelun tarjoamiseen ja käyttöön liittyvät roolit ja vastuunjako asiakkaan ja pilvipalveluntarjoajan välillä. Kuvauksesta on käytävä selvästi esille ne toimet, jotka kuuluvat asiakkaan vastuulle pilvipalvelun turvallisuuden varmistamisessa. Pilvipalveluntarjoajan vastuisiin tulee sisältyä yhteistyövelvollisuus erityisesti poikkeamatilanteiden selvittelyssä. g) Alihankkijoille siirretyt tai ulkoistetut toiminnot.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Kuvauksen tavoitteena on mahdollistaa palvelun yleisen soveltuvuuden ja riskien arviointi suhteessa asiakkaan käyttötapaukseen.
Lisätietoja	Infrastruktuurin, verkon ja järjestelmäkomponenttien kuvauksen tulee olla riittävän yksityiskohtainen, jotta kuvauksen pohjalta pystytään arvioimaan palvelun yleistä soveltuvuutta ja riskejä suhteessa asiakkaan käyttötapaukseen. Vrt. KT-01 (Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi). Infrastruktuurin kuvauksessa voidaan tietyin rajauksin hyödyntää myös ohjelmistokoodia, jonka pohjalta kyseinen infrastruktuuri rakennetaan. Palvelumalleja ovat esimerkiksi infrastruktuuri palveluna (Infrastructure as a Service, IaaS), ohjelmistoalusta palveluna (Platform as a Service, PaaS) ja ohjelmisto palveluna (Software as a Service, SaaS). Toteutusmalleja ovat esimerkiksi yksityinen pilvi (private cloud), yhdistelmäpilvi (hybrid cloud) ja julkinen pilvi (public cloud). Osa pilvipalveluntarjoajista tarjoaa asiakkailleen mahdollisuuden ottaa käyttöönsä uusia toiminnallisuuksia, jotka ovat esikatselu- tai testausvaiheessa. Mikäli tällaisia toiminnallisuuksia halutaan ottaa käyttöön salassa pidettävän tiedon käsittelyyn, suositellaan riskienarvioinnissa huomioitavaksi muun muassa käyttöönottoon liittyvät vastuut. Uusien toiminnallisuuksien toteutuksessa voi vielä olla turvallisuuspuutteita, joista mahdollisesti aiheutuvien vahinkojen korvaaminen on sopimuksissa usein osoitettu asiakkaalle.

Liite 8. EE-02 Lainsäädäntöjohdannaiset riskit

EE-02	Lainsäädäntöjohdannaiset riskit
Vaatimus	1) Pilvipalveluun liittyvät lainsäädäntöjohdannaiset riskit ja velvoitteet on kuvattuna. Palveluntarjoajan tuottamien kuvausten perusteella on pystyttävä arvioimaan kyseisen pilvipalvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Kuvausten tulee kattaa palvelun käytön ja palvelussa käsiteltävien tietojen koko elinkaaren. Kuvauksista on käytävä ilmi vähintään: a) Palvelussa käsiteltävän tiedon fyysinen sijainti koko tiedon elinkaaren ajalta, kattaen myös mahdolliset alihankinta-/ulkoistusketjut. b) Palvelun eri toimintojen (esimerkiksi ylläpito-/hallintaratkaisut, varmistukset) ja komponenttien fyysinen sijainti koko tiedon elinkaaren ajalta. c) Mahdolliset muut palvelun tuottamiseen osallistuvat tahot, esimerkiksi mahdolliset alihankinta-/ulkoistusketjut. d) Palvelun käyttöön ja palvelussa käsiteltäviin tietoihin sovellettava lainsäädäntö ja oikeuspaikka. e) Toimijat, joilla voi sovellettavasta lainsäädännöstä johtuen olla pääsy palvelussa käsiteltäviin tietoihin. 2) Lainsäädäntöjohdannaiset riskit eivät rajoita kyseisen pilvipalvelun soveltuvuutta kyseiseen käyttötapaukseen. 3) Pilvipalvelun asiakkaan tiedot sijaitsevat koko elinkaarensa ajan vain sopimuksessa kuvatuissa fyysisissä sijainneissa. Poikkeuksena tilanne, jossa pilvipalvelun asiakas on kirjallisesti etukäteen hyväksynyt tietojen siirron tai käsittelyn muissa fyysisissä sijainneissa. 4) Pilvipalveluntarjoajan sopimusehdot eivät rajoita kyseisen pilvipalvelun soveltuvuutta kyseiseen käyttötapaukseen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Kuvauksen tavoitteena on mahdollistaa palvelun yleisen soveltuvuuden ja riskien arviointi suhteessa loppuasiakkaan käyttötapaukseen.
Lisätietoja	Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa pilvipalveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy pilvipalvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin että muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia. 1a) ja 3) Tilanteissa, joissa palvelu on toteutettu siten, että tiedon fyysinen sijainti voi vaihdella, tulee kuvata kaikki mahdolliset fyysiset sijainnit, minne tiedot voivat elinkaarensa aikana palvelussa kulkeutua. 4) Viranomaisen voi olla haastavaa pystyä täyttämään esimerkiksi tiedonhallintalain (906/2019) 13 § velvoitetta varmistua tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta koko niiden elinkaaren ajan, mikäli sopimusehtojen muuttaminen on mahdollista yksipuolisesti. Henkilötietojen käsittely voi toisaalta tietosuojasääntelyn näkökulmasta estyä, mikäli pilvipalveluntarjoaja ei pysty tarjoamaan tietosuojasääntelyn mukaista sopimusta, jonka muuttaminen ei ole mahdollista yksipuolisesti, toisin sanoen ilman pilvipalvelun asiakkaan suostumusta. Vrt. TJ-07 (Vaatimustenmukaisuus ja tietosuoja). Arvioinnissa tulee huomioida EU:n yleisen tietosuoja-asetuksen 28 artiklan 4. kohdan sekä rikosasioiden tietosuojalain 17 §:n 2 momentin vaatimukset niin sanottuja alikäsittelijöitä käytettäessä. Palveluntarjoajan (rekisterinpitäjän) tulee tehdä henkilötietojen käsittelijän kanssa kirjallinen sopimus. Pilvipalveluiden sopimuksiin ja käyttöehtoihin saattaa liittyä myös erilaisia pilvipalvelutoimittajakohtaisia tapoja määritellä palvelun (tai sen osan) fyysisiä sijaintimaita. Henkilötietojen siirtäminen EU-/ETA-alueen ulkopuolelle tulee aina tehdä EU:n yleisessä tietosuoja-asetuksessa (V luku) tai rikosasioiden tietosuojalaissa (7 luku) säädettyjen edellytysten mukaisesti. Arvioinnissa suositellaan noudatettavan taulukossa 2 kuvattuja jatkoarvioinnin yleisperiaatteita.

Liite 9. TJ-01 Turvallisuus periaatteet ja TJ-02 Turvallisuuden vastuut

TJ-01	Turvallisuusperiaatteet
Vaatimus	1) Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan. 2) Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. 3) Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan johdolle ja niiden toteutumista seurataan säännöllisesti.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuusperiaatteilla tavoitellaan sitä, että johto sitoutuu organisaation turvallisuustyöhön ja että turvallisuustyö tukee organisaation toimintaa.
Lisätietoja	Turvallisuusperiaatteet viestitään henkilöstölle ja tarvittaville sidosryhmille. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana organisaation ohjeistokokonaisuutta. Vaatimuksen täyttymisen osoittamisessa voidaan hyödyntää voimassa olevaa ISO27001-sertifiointia, edellyttäen, että sertifiointi (ml. soveltamissuunnitelma) kattaa pilvipalvelun kehittämisessä ja tuottamisessa käytettävät prosessit.

TJ-02	Turvallisuuden vastuut
Vaatimus	1) Pilvipalvelun turvallisuuden hoitamisen tehtävät ja vastuut on määritelty ja dokumentoitu. 2) Pilvipalvelun tarjoamiseen ja käyttöön liittyvä vastuunjako asiakkaan ja palveluntarjoajan välillä on kuvattu. Vrt. EE-01. 3) Pilvipalvelun tietoturvallisuudesta vastaava henkilö on nimetty.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa.
Lisätietoja	Turvallisuusvastuiden määrittely on oleellista, jotta vastuuhenkilöt voivat toteuttaa heidän vastuullaan olevat turvallisuustehtävät. Mikäli muuta ei ole kuvattu, ovat kaikki turvallisuus-vastuut organisaation johdolla. Pilvipalvelupolitiikan tai vastaavan kuvauksen määrittelyn tavoitteena on tuoda selkeästi esille, mitkä turvallisuusasioista ovat asiakkaan vastuulla ja mitkä palveluntarjoajan.

Liite 10. TJ-03 Turvallisuusriskien hallinta

TJ-03	Turvallisuusriskien hallinta
Vaatimus	1) Organisaatiolla on käytössä riskienhallintaprosessi. Riskienhallinnan on oltava säännöllinen ja jatkuva, dokumentoitu prosessi. Riskienhallintapäätökset vastuutahoineen dokumentoidaan. 2) Riskien analysoinnissa on käytettävä järjestelmällistä ja ymmärrettävää menetelmää. 3) Riskienhallinnan on katettava vähintään turvallisuusjohtamisen, tila- ja tietoturvallisuuden osa-alueet. 4) Tunnistetut riskit otetaan huomioon tarvittavien sidosryhmien osalta. Pilvipalveluntarjoajan tulee varmistaa, että asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. Vrt. TJ-08. 5) Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation turvallisuus-tavoitteiden asettamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa, turvatoimien suunnittelussa, muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä. 6) Turvatoimet on mitoitettu ottaen huomioon muun muassa tiedon luokitteluperuste, määrä, muoto ja sijoitustilat suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan. 7) Organisaatio dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Riskienhallinnan tavoitteena on tunnistaa ja hallita toimintaedellytyksiä mahdollisesti vaarantavia tekijöitä ja pitää toimintaan kohdistuvat riskit sellaisissa rajoissa, etteivät toiminta ja tavoitteet ole uhattuna.
Lisätietoja	**Lainsäädännön tai viranomaisvaatimusten huomioiminen turvallisuustason suunnittelussa** Organisaation tulee tunnistaa, mitä lainsäädännön tai viranomaisen vaatimuksia omaan toimintaan liittyy. Näiden vaatimusten täyttäminen, esimerkiksi viranomaisen hyväksynnän saamiseksi, voi edellyttää organisaation sisäisiä turvallisuusvaatimuksia tiukempien suojausten toteuttamista. Vrt. TJ-07 (Vaatimustenmukaisuus ja tietosuoja). **Riskienhallinnan kohdentaminen salassa pidettävien tietojen näkökulmasta** Riskienhallintatoimet tulee kohdentaa siihen ympäristöön, jossa salassa pidettäviä tietoja on tarkoitus käsitellä. Riskienhallintatoimenpiteet voivat olla hallinnollisia (esim. henkilöstön koulutus, ohjeet) tai teknisiä (esim. ympäristön tekniset suojaukset). **Monitasoisen suojaamisen huomiointi riskienhallinnassa** Riskienhallinnan toimenpiteiden suunnittelun tavoitteena on vähentää toimintaan kohdis-tuvia riskejä. Näiden suunnittelussa hyvä periaate on turvallisuusjärjestelyjen monitasoisuus (defence in depth). Tämä tarkoittaa sitä, että mikäli yksittäinen turvallisuusjärjestely pettää, on jäljellä silti muita suojaustoimenpiteitä. Yksittäisiin riskeihin nähden riittävän suojauksen voi toteuttaa yksittäisillä luotettavilla turvatoimilla tai useampia turvatoimia yhdistelemällä. **Riskien hallinnan ja analysoinnin menetelmiä** Riskienhallintaan ja analysointiin on olemassa useita eri menetelmiä, joilla kullakin on omat vahvuutensa ja heikkoutensa. Useissa järjestelmällisissä menetelmissä toiminta perustuu uhkien ja haavoittuvuuksien tunnistamiseen, todennäköisyyksien ja vaikuttavuuden arviointiin, tarvittavien riskejä pienentävien toimenpiteiden määritykseen, jäännösriskien arviointiin sekä korjaavien toimien seurantaan.

Liite 11. TJ-04 Turvallisuushäiriöiden hallinta

TJ-04	Turvallisuushäiriöiden hallinta
Vaatimus	1) Organisaatiolla on menettelytavat turvallisuushäiriöiden asianmukaiseen käsittelyyn. 2) Organisaatiolla on käytössään selkeät prosessit turvallisuushäiriöiden ilmoittamisesta. Organisaatiolla on määritettynä henkilöt/tahot, joille turvallisuushäiriöistä tai niiden epäilyistä tulee ilmoittaa. 3) Turvallisuushäiriöiden määrää ja tyyppejä seurataan. Toteutuneiden häiriöiden uusiutuminen on pyrittävä estämään korjaussuunnitelmissa. 4) Asiakastiedon käsittelyyn liittyvät turvallisuushäiriöt tai niiden epäilyt ilmoitetaan kyseiselle asiakkaalle.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuushäiriöiden hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa tilanteissa, minimoiden vahingot ja palauttaen tilanteen normaaliksi. Ilmoitusvelvollisuus asiakkaalle tukee asiakkaan riskienarviointia ja muun muassa vahinkojen minimointia.
Lisätietoja	Vaatimuksen täyttämisessä voi hyödyntää esimerkiksi seuraavaa toimintamallia: Turvallisuushäiriöiden hallinta on 1) suunniteltu, 2) ohjeistettu ja koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, 4) harjoiteltu, ja erityisesti 5) viestintäkäytännöt ja vastuut on sovittu. Erityisesti turvallisuusluokiteltujen tietojen käsittelyyn liittyvistä häiriöistä, tietomurroista tai sellaisten yrityksistä suositellaan ilmoittamaan Kyberturvallisuuskeskukselle. Tunnistetusta rikollisesta toiminnasta suositellaan ilmoittamaan myös poliisille. Lisäksi tulee ottaa huomioon EU:n yleisen tietosuoja-asetuksen 33 artiklassa säädetty lyhyt määräaika, sekä rikosasioiden tietosuojalain 33 §:ssä säädetty palveluntarjoajan ilmoittamisvelvollisuus.

Liite 12. TJ-05 Jatkuvuudenhallinta

TJ-05	Jatkuvuudenhallinta
Vaatimus	1) Jatkuvuudenhallinnan prosessit ja menettelyt on suunniteltu, toteutettu, testattu ja kuvattu siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin. Järjestelyissä huomioidaan erityisesti, että a) toipuminen ja jatkuvuuden varmistaminen toimintavaatimuksiin nähden riittävässä ajassa on huomioitu suunnittelussa, b) toiminnan jatkuvuussuunnitelmiin on sisällytettävä ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset tietojen käsittelyyn ja säilyttämiseen, c) poikkeamista tehdyt havainnot tuodaan osaksi riskienarviointia, ja toipumis- ja jatkuvuussuunnitelmia päivitetään tehtyjen havaintojen ja saatujen tulosten perusteella, ja d) jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa, jotta estetään luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai saatavuuden menettäminen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Jatkuvuudenhallinnan tavoitteena on varmistaa palvelun jatkuvuus siten, että pystytään vastaamaan siihen kohdistuneisiin saatavuus-, eheys- ja luottamuksellisuusvaatimuksiin.
Lisätietoja	Vaatimuksen täyttämisessä voi hyödyntää esimerkiksi seuraavaa toimintamallia: Liiketoimintaan kohdistuvien vaikutusten analyysi sekä liiketoiminnan jatkuvuutta ja varautumista koskevat suunnitelmat todennetaan, päivitetään ja testataan säännöllisin väliajoin (vähintään kerran vuodessa) tai aina organisaatiota tai ympäristöä koskevien olennaisten muutosten jälkeen. Testit koskevat myös asiakkaita ja oleellisia kolmansia osapuolia (kuten keskeisiä toimittajia), joihin näillä asioilla on vaikutusta. Testit dokumentoidaan ja tulokset otetaan huomioon tulevissa liiketoiminnan jatkuvuutta koskevissa turvatoimissa. Konesalipalvelut (kuten vesihuolto, sähkö, lämpötilan ja kosteuden säätö, tietoliikenne ja Internet-yhteys) varmistetaan ja niitä seurataan ja ylläpidetään sekä testataan säännöllisin väliajoin niiden jatkuvan tehokkuuden varmistamiseksi. Palvelut on suunniteltu sisältämään automaattisia vikasietoisia mekanismeja ja esimerkiksi kahdennuksia. Huoltotyöt tehdään toimittajien suosittelemien huoltovälien ja -tavoitteiden mukaisesti, ja niitä tekee vain valtuutettu henkilöstö. Huoltopöytäkirjoja ja niissä mahdollisesti olevia merkintöjä epäillyistä tai havaituista puutteista säilytetään ennalta sovitun ajan. Vrt. FT-05 (Varautuminen ja jatkuvuudenhallinta) ja KT-03 (Varmistus- ja palautusprosessit). Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi se, että pilvipalvelualustan päälle toteutetun asiakasjärjestelmän saatavuus on usein suoraan riippuvainen pilvipalvelualustan toimivuudesta.

Liite 13. TJ-06 Tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä

TJ-06	Tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä
Vaatimus	1) Pilvipalvelun tuottamisen ja asiakastiedon käsittelyn kannalta olennaisten suojattavien kohteiden (tiedot, laitteistot, ohjelmistot, toimitilat) luokitteluun ja merkitsemiseen on käytössä yhdenmukainen menetelmä. 2) Tietosisällöltään salassa pidettävät suojattavat kohteet (tietoaineistot, laitteistot ja järjestelmät) on luokiteltu lakisääteisten vaatimusten perusteella. 3) Pilvipalvelun tuottamiseen ja asiakastiedon käsittelyyn liittyvät laitteistot ja ohjelmistot on tunnistettu. 4) Laitteistot ja ohjelmistot on luokiteltu niiden kriittisyyden mukaisesti. 5) Kullekin laitteistolle ja ohjelmistolle on nimetty omistaja/vastuutaho. 6) Laitteistoista ja ohjelmistoista pidetään ajantasaista kirjanpitoa siten, että muutokset hyväksyttyyn kokoonpanoon pystytään havaitsemaan vertaamalla toteutusta kirjanpitoon. (Vrt. MH-01: Muutostenhallinta.)
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Luokittelun tavoitteena on tunnistaa ja mitoittaa turvatoimet suojattavien kohteiden suojaustarpeen perusteella. Merkitsemisen tavoitteena on mahdollistaa luokittelun mukaisten turvatoimien käytännön toteutus.
Lisätietoja	Luokituksen voi ilmaista eri tavoin riippuen tietoaineistosta, käsittely-ympäristöstä ja käyttäjistä. Luokittelemalla tietojenkäsittely-ympäristöt tietoaineiston mukaisesti, pystytään selkeämmin osoittamaan ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät turvatoimet. Vaatimuskohdan 5 täyttämiseen voidaan hyödyntää myös menettelyä, jossa pilvipalveluntarjoaja luokittelee kaiken asiakkaan palveluun tuottaman tietoaineiston sisäisen luokittelunsa mukaiseksi siten, että kyseisen luokittelun omaavien suojattavien kohteiden (tietoaineistot, laitteistot ja järjestelmät) käsittelyn suojaukset täyttävät salassa pidettävän tai/ja turvallisuusluokitellun salassa pidettävän tiedon suojausvaatimukset koko tiedon elinkaaren ajalta. Laitteisto- ja ohjelmistokirjanpidon ylläpitämiseen suositellaan automatisoituja menettelyjä. Kirjanpidon ajantasaisuus voidaan vaihtoehtoisesti varmistaa esimerkiksi kuukausittain tehtävillä manuaalisilla tarkastuksilla. Kirjanpidon muutoshistoria (tehdyt muutokset) tulee olla jälkikäteen selvitettävissä. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että a) asiakas on tunnistanut pilvipalveluun sijoitettavat suojattavat kohteet (asiakkaan tietoaineistot, järjestelmät ja mahdollisesti myös laitteistot), ja luokitellut ne lakisääteisten vaatimusten perusteella, b) asiakas on varmistanut, että kyseisten suojattavien kohteiden sijoittamiselle kyseiseen pilvipalveluun ei ole esteitä (vrt. EE-02), c) asiakas on varmistanut, että pilvipalveluntarjoaja on tietoinen kyseisten suojattavien kohteiden luokittelusta, ja että myös d) asiakkaalla on asiakkaan vastuulle kuuluvasta kokonaisuudesta ajantasainen kirjanpito siten, että muutokset hyväksyttyyn kokoonpanoon pystytään havaitsemaan vertaamalla toteutusta kirjanpitoon. (Vrt. MH-01: Muutostenhallinta.)

Liite 14. TJ-07 Vaatimustenmukaisuus ja tietosuoja

TJ-07	Vaatimustenmukaisuus ja tietosuoja
Vaatimus	1) Pilvipalveluun sovellettavien lakien ja säädösten määräykset sekä menettelyt näiden noudattamiseksi on tunnistettu ja dokumentoitu, sekä säännöllisesti päivitetty. 2) Riippumattomat kolmannet osapuolet arvioivat vähintään vuosittain pilvipalveluun liittyvän toiminnan, prosessit ja tietotekniikkajärjestelmät soveltuvin osin, erillisessä arviointisuunnitelmassa määritellyn kuvauksen mukaisesti. Arvioinnin tulee pyrkiä tunnistamaan mahdolliset tapaukset, joissa lakeja tai säädöksiä ei noudateta. Arviointisuunnitelma kattaa palvelun turvallisuuden siten, että kaikki keskeiset turvallisuuteen vaikuttavat kokonaisuudet arvioidaan korkeintaan kolmen vuoden välein. Havaitut poikkeamat dokumentoidaan, priorisoidaan ja korjataan niiden kriittisyyden mukaisesti. 3) Pilvipalvelun toimintaan kohdistetaan vähintään vuosittain sisäinen tarkastus, jonka tavoitteena on selvittää kuinka palvelu kokonaisuutena vastaa turvakäytäntöjensä ja sopimus- sekä lainsäädännöllisten vastuiden täyttämiseen. 4) Ylin johto vastaa siitä, että havaitut poikkeamat priorisoidaan ja korvaavat suojaukset tai korjaukset toteutetaan riittävän nopeasti.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Lainsäädännöllisten ja sopimusvelvoitteiden täyttäminen.
Lisätietoja	Pilvipalveluntarjoajan tulee huolehtia esimerkiksi henkilötietojen käsittelyn turvallisuudesta asiaa koskevan sääntelyn mukaisesti, ks. esim. tietosuojalaki (1050/2018), laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018, rikosasioiden tietosuojalaki), sekä yleisen tietosuoja-asetuksen (GDPR, (EU) 2016/679) 32 artikla. Henkilötietojen luokittelu ja luokittelun mukainen käsittely voi olla tarpeen, mikäli erilaisten henkilötietojen suojaustarpeet (oikeudelliset vaatimukset, arvo, arkaluonteisuus) eroavat tai/ja mikäli niitä käsitellään eroavasti suojattuna pilvipalveluntarjoajan eri toiminnoissa tai järjestelmissä. Vrt. vaatimuskortti EE-02. Henkilötietojen käsittelyä valvovana viranomaisena Suomessa toimii Tietosuojavaltuutettu (TSV). Henkilötietojen tietoturvaloukkauksista tulee ilmoittaa sekä TSV:lle, että tarvittaessa myös käyttäjille GDPR 33 ja 34 artiklojen mukaan. Henkilötietoloukkausten ilmoittamisessa tulee huomioida myös muu lainsäädäntö. Esimerkiksi asetuksessa (EU) 611/2013 säädetään teleyritysten velvollisuudesta ilmoittaa henkilötietojen tietoturvaloukkauksista Liikenne- ja viestintävirastolle ja tarvittaessa myös käyttäjille. Vrt. TJ-04 (Turvallisuushäiriöiden hallinta). Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että asiakas ei voi ulkoistaa omaa vastuutaan vaatimustenmukaisuuden toteuttamisesta, mukaan lukien sen varmistamista, että ulkoistuskumppani (tässä erityisesti pilvipalvelun-tarjoaja) täyttää käsitellyille tiedoille asetetut vaatimukset.

Liite 15. TJ-08 Palveluntarjoajien ja toimittajien turvallisuus

TJ-08	Palveluntarjoajien ja toimittajien turvallisuus
Vaatimus	1) Asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. Varmistettava erityisesti, että a) ennen palveluntarjoajan/toimittajan henkilöstön pääsyä suojattaviin kohteisiin, henkilöstö on läpikäynyt vastaavat suojaustoimenpiteet (sopimukset, salassapito-sitoumukset, turvaselvitykset, koulutukset), kuin pilvipalveluntarjoajankin henkilöstö, b) palveluntarjoajat/toimittajat on kirjallisesti ohjeistettu ja sopimuksin velvoitettu noudattamaan vähintään vastaavantasoisia suojauksia, kuin organisaatiokin, c) sopimusvelvoitteiden noudattamisen varmistamiseen ja valvontaan on käytössä luotettavat menettelyt, d) turvallisuusluokitellun tiedon käsittelyyn suoraan tai epäsuoraan osallistuvat palveluntarjoajat ja toimittajat ovat voimassa olevan viranomaishyväksynnän, tai vastaavan menettelyn piirissä. Menettely kattaa soveltuvin osin sekä hallinnollisen (turvallisuusjohtamisen), fyysisen että teknisen tietoturvallisuuden kokonaisuudet.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan siltä osin, kun siihen liittyy ulkoisia palveluntarjoajia tai/ja toimittajia.
Tietotyypit	1a-1c: Salassa pidettävä, henkilötiedot 1d: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojattavien kohteiden turvallisuus varmistetaan myös tilanteissa, joissa niihin on suora tai epäsuora pääsy pilvipalveluntarjoajan omilla palveluntarjoajilla tai/ja toimittajilla. Vrt. MH-02 (Järjestelmäkehitys).
Lisätietoja	Ulkoistus- ja toimitusketjujen turvallisuus vaikuttaa usein suoraan myös pilvipalvelussa käsiteltävien tietojen suojauksiin. Mikäli pilvipalveluntarjoajan palvelun turvallisuus nojaa joiltain osin ulkoistuksiin tai toimitusketjuihin, myös näiden turvallisuus on huomioitava pilvipalvelun kokonaisturvallisuuden suunnittelussa ja ylläpidossa. Tulee myös huomioida EU:n yleisen tietosuoja-asetuksen 28 artiklan 4. kohdan sekä rikosasioiden tietosuojalain 17 §:n 2 momentin vaatimukset henkilötietojen käsittelystä niin sanottuja alikäsittelijöitä käytettäessä. Palveluntarjoajan (rekisterinpitäjän) tulee tehdä henkilötietojen käsittelijän kanssa kirjallinen sopimus. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä palveluntarjoajia.

Liite 16. FT-01 Monitasoinen suojaaminen ja riskienhallinta

FT-01	Monitasoinen suojaaminen ja riskienhallinta
Vaatimus	1) Fyysiset turvatoimet on toteutettu monitasoisen suojaamisen periaatetta noudattaen. 2) Suojattavat tilat rakennuksessa on luokiteltu turvallisuusalueiksi (hallinnollinen alue, turva-alue) ja niillä on selkeästi määritellyt ja näkyvät rajat. 3) Korkeintaan turvallisuusluokan IV salassa pidettävää tietoa sisältävät tietovarannot ja tietojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle. 4) Turvallisuusluokan III kasauman muodostaneet tietovarannot ja tietojen pääsynrajauksiin ja -valvontaan käytettävät tietojärjestelmät on sijoitettava turva-alueelle. 5) Hallinnollisilla alueilla on selkeästi määritetyt näkyvät rajat ja joihin vain organisaation valtuuttamilla henkilöillä on pääsy ilman saattajaa. 6) Turva-alueilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle. 7) Turvatoimet on mitoitettu riittävälle tasolle siten, että ne vastaavat riskienarvioinnissa todettuja riskejä.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojaustavoitteena on luvattoman pääsyn estäminen pilvipalveluntarjoajan konesaliin, salassa pidettäviin tietoihin sekä varkauksien, vahinkojen, menetysten, taloudellisten tappioiden ja häiriöiden ennalta estäminen sekä vaikutusten minimointi.
Lisätietoja	Monitasoisella suojaamisella tarkoitetaan sitä, että toteutetaan joukko toisiaan täydentäviä turvatoimia. Mikäli mahdollista, tilat muodostavat keskenään sisäkkäisiä vyöhykkeitä, joissa korkeamman suojaustarpeen tilat ovat sisimpänä. Turvatoimet suunnitellaan kokonaisuutena, jossa otetaan huomioon salassa pidettävän tiedon suojaustaso, määrä, rakennusten ympäristö ja rakenne. Pilvipalveluntarjoajalla tulee olla käytössään riskienhallintaprosessi (vrt. TJ-03). Arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältävien tilojen tai rakennusten riskejä arvioidaan säännöllisesti (väh. 1 krt / vuosi) pilvipalveluntarjoajan toimesta. Riskeillä on nimetyt omistajat, arvioinnista vastaavat vastuuhenkilöt ja määritellyistä hallintatoimista vastaavat henkilöt. Riskienarviointi dokumentoidaan. Vaatimusten täyttämisessä voidaan hyödyntää seuraavaa menettelyä: Rakennus suunnitellaan niin, että sen ulkoseinät ja kuori muodostavat ensimmäisen turvallisuustason. Kulku rakennuksen sisään valvotaan ja hallitaan esimerkiksi kulunvalvontajärjestelmällä ja lukituksilla. Korkeamman suojaustarpeen tietoa käsitellään rakennuksen sisemmissä osissa siten, että tunkeutuminen tiloihin on vaikeaa ja hidasta. Turvallisuustekniset ratkaisut täydentävät rakenteellisia ratkaisuja. Suunnittelussa otetaan huomioon ikkunat, ovet ja muut aukot.

Liite 17. FT-02 Rakenteet ja turvallisuusjärjestelmät

FT-02	Rakenteet ja turvallisuusjärjestelmät
Vaatimus	1) Arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältävien tilojen tai rakennusten ulkorajat suojataan fyysisesti kestävällä tavalla sekä nykyaikaisilla ja asianmukaisilla turvatoimilla.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojaustavoitteena on luvattoman pääsyn estäminen pilvipalveluntarjoajan konesaliin, salassa pidettäviin tietoihin sekä varkauksien, vahinkojen, menetysten, taloudellisten tappioiden ja häiriöiden ennalta estäminen sekä vaikutusten minimointi.
Lisätietoja	Aluetta rajaavan aidan tai ulkokuoren seinä-, katto-, lattia-, ikkuna-, ovi- tai talotekniikan aukkojen rakenteilta ei vaadita erityisiä ominaisuuksia. Käyttötarkoitusten mukaiset rakenteet soveltuvat. Turvallisuustekniikan tulee tukea tilan ja rakennuksen kokonaisturvallisuutta. Mahdollisia turvatoimia voisivat olla esimerkiksi sijoittuminen riittävälle etäisyydelle ulkopuolisista toimijoista, aidat, vartiointi tai tekniset valvontajärjestelmät (mm. kulunvalvonta-, rikosilmoitin-, kameravalvontajärjestelmät). Järjestelmät tulee huoltaa säännöllisesti valmistajan suositusten mukaan ja varmistua niiden käyttökunnosta. Turvallisuusjärjestelmiä ja -laitteita tulee testata (väh. 1 krt / kk) ja pitää käyttökuntoisina säännöllisesti. Testaukset tulee dokumentoida. **Vaatimusten täyttämisessä (TL IV) voidaan hyödyntää seuraavaa tai vastaavaa menettelyä:** • Rakennuksen seinät ovat rakenteeltaan: teräsbetoni (50mm), lämmöneriste mineraalivilla (80mm), teräsbetoni (60mm). Tietoja säilyttävän konesalin seinärakenteet ovat rakenteeltaan: palolevy (12mm), kipsilevy + villa + kipsilevy (70mm). • Rakennus on kokonaisuudessaan kulunvalvonta- ja rikosilmoitinjärjestelmällä suojattu. Konesaliin johtavilla reiteillä on myös kameravalvonta. Järjestelmiä hallitaan ja valvotaan ulkoisen vartiointiliikkeen toimesta, jonka kanssa organisaatiolla on turvallisuussopimus. Järjestelmien huoltaminen, ylläpito, testaaminen ja dokumentointi ovat vastuutettu organisaation turvallisuudesta vastaavalle henkilölle. Järjestelmien toimivuus testataan kerran kuukaudessa. **Vaatimusten täyttämisessä (TL III kasautumisvaikutus) voidaan hyödyntää seuraavaa tai vastaavaa menettelyä:** **Konesalin tai rakennuksen seinät, lattia ja katto:** • Rakenteiden on oltava lujuudeltaan ja rakennustavaltaan sellaisia, että tilaan tunkeutuminen ei ole mahdollista ilman työkaluilla tapahtuvaa rakenteiden rikkomista. • Rakenteet tai niiden osat eivät saa olla ulkopuolelta rikkomatta irrotettavissa. Luokan 3 murronsuojaseinä täyttää edellä olevat vaatimukset. Väliseinärakenteen tulee ulottua lattiasta kattoon. • Kevyet rakenteet on vahvistettava. • Seinärakenteet voivat olla esimerkiksi: - 1x12mm kipsilevy + 1,5mm teräslevy + 12mm vaneri + runko + 12mm vaneri + 1,5mm teräslevy + 1x12mm kipsilevy. - Teräsbetoni; ≥ 80 mm. - Poltettu tiili; ≥ 85 mm+2x1,5mm teräslevy sisäpuolella tai 1,5mm teräslevy ulkopuolella ja 1,5mm teräslevy sisäpuolella. - Harkko; ≥ 70 mm+2x1,5 mm teräslevy sisäpuolella, vaihtoehtoisesti 1,5mm teräslevy ulkopuolella ja 1,5mm teräslevy sisäpuolella. Teräslevyjen päällä kipsilevy. • Lattiarakenteet voivat olla esimerkiksi: - Ontelolaatta, yli 320 mm. - Betoni ≥ 80 mm. - Muut lattiarakenteet; teräslevyvahvistus ≥3 mm. • Kattorakenteet voivat olla esimerkiksi: - Ontelolaatta. - Betoni ≥80 mm. - Muut kattorakenteet; teräslevyvahvistus ≥3 mm. Lasirakenteissa, kuten lasi- ja siirtolasiseinissä on oltava standardin SFS-EN 356 P6B mukainen suojalasitus tai ne on suojattava riittävän vahvuisella rullakalterilla tai teräsristikolla.

FT-02	Rakenteet ja turvallisuusjärjestelmät
Lisätietoja	**Ikkunat ja aukot** Ikkunoiden lasiruudut on kiinnitettävä ja ikkunat suljettava siten, ettei niitä voi ulkopuolelta rikkomatta irrottaa tai avata. Ikkunoiden ja kattoikkunoiden oltava standardin SFS-EN 356 P6B mukaista suojalasitusta tai ne on suojattava kiinteällä/lukitulla rullakalterilla, teräsristikolla tai -verkolla tai aukkojen suojauslevyllä. Muut aukot, kuten savunpoisto- ja ilmanottoaukot, on suojattava kiinteällä tai lukitulla teräsristikolla. Suojausvaatimus ei koske ikkunaa tai aukkoa, joka on vähintään 4 m:n korkeudella maan pinnasta tai muusta seisomatasosta. Suojattaessa ikkunoita ja lasisiirtoseiniä muulla kuin murronsuojalasilla on käytettävän suojarakenteen aukkokoko valittava suojattavien laitteiden koon mukaan siten, ettei esineiden kuljettaminen suojarakenteen läpi ole mahdollista sitä rikkomatta. **Ovet, saranat ja karmit:** Oven rakenteen on oltava lujuudeltaan seinärakennetta vastaava. Ovirakenteen on oltava seuraavanlainen: • Karmi on kiilattava rakenteisiin lukkojen ja saranoiden kohdalta. • Karmiin saranapuolelle on kiinnitettävä saranoiden kohdalle murtosuojatapit. • Käyntiväli lukkosivulla ei saa olla suurempi kuin 5 mm. • Huultamattoman oven käyttölukko on suojattava rakoraudalla. • Oven lasi on kiinnitettävä siten, ettei sitä voi ulkopuolelta rikkomatta irrottaa. Ovien lasit on oltava P6B murronsuojalasia tai ne on suojattava rullakalterilla, teräsristikolla tai -verkolla. Ovi, joka on testattu standardin SFS-EN 1627 mukaan luokkaan 3 täyttää edellä olevat vaatimukset. **Lukitus:** • Kiinteästi oveen asennettavalla käyttölukolla vastalevyineen, joka on standardin SFS 7020 mukaan luokiteltu joko luokkaan 1 tai 2. • Kiinteästi oveen asennettavalla varmuuslukolla vastalevyineen, joka on standardin SFS 7020 mukaan luokiteltu luokkaan 3 tai 4. **Turvallisuusjärjestelmät:** Turvallisuusjärjestelmien laitetila tulee sijoittaa turvallisuusaluetta vastaavalle alueelle. Laitetilan kulkuoikeudet määritellään työperusteisen tarpeen mukaisesti. Turvallisuusjärjestelmät tulee olla säännöllisen huollon, päivitysten ja testauksen piirissä, jolla varmistetaan järjestelmien toimintakunto ja tietoturvallisuus. Turvallisuusjärjestelmien etäyhteydet ja kenttälaitteiden asennus tulee toteuttaa riskienarvioinnin pohjalta riittävän tietoturvallisesti siten, että turvallisuusjärjestelmiin on vain valtuutetuista päätelaitteista/verkoista mahdollista päästä käsiksi ja että liikenneyhteys ja turvallisuusjärjestelmän rajapinnat on suojattu siten, että ulkopuolisilla ei ole pääsyä välitettyihin tietoihin. Korotettua rakenteellista murtoturvallisuutta ei kuitenkaan edellytetä, mikäli tilat ovat jatkuvasti miehitetty turvallisuushenkilöstön toimesta. Lisäksi turvallisuushenkilöstöllä on oltava riittävä valvontakyky, jotta poliisi tai turvallisuushenkilöstö saa indikaation tunkeutumisesta siinä määrin ajoissa, ettei tunkeutuja ehdi saada haltuunsa suojattavaa tietoa. Valvontakyky voidaan toteuttaa tarkastuskierrosten sekä turvajärjestelmien reaaliaikaisen valvonnan tai niiden yhdistelmien avulla. **Rikosilmoitinjärjestelmä ja hälytyksensiirto:** Suojattavan tilan ovet, aukot, ikkunat ovat valvottava rikosilmoitinjärjestelmän avulla. Rikosilmoitinjärjestelmän keskuslaitteet ja ilmaisimet tulee olla hyväksytty vähintään Finanssialan (FA):n luokkaan 3. Ilmoituksensiirto tulee toteuttaa valvottuna tai kahdennettuna yhteytenä. Ilmoituksensiirtolaitteen avulla tulee siirtää vartioimisliikkeelle tai muuhun turvallisuusvalvomoon vähintään seuraavat tiedot: murto, päälle/pois, sabotaasi, vika. Järjestelmää tulee operoida henkilökohtaisen koodin avulla (vähintään 4-merkkinen). Radioteitse toimivina ilmaisimina hyväksytään vain henkilökohtaiset hätäpainikkeet. Tilat tulee olla valvottuina, kun tiloissa ei oleskella. **Kulunvalvontajärjestelmä:** Turva-alueen rajalla on käytettävä sähköistä kulunvalvontaa sisään ja ulos mentäessä. Sisään mentäessä käytettävä kaksoistunnistusta (esimerkiksi pääsykoodi ja sähköinen tunniste). Kulunvalvontatunnisteiden tulee käyttää nykyaikaista ja salattua lukutekniikkaa tai organisaation tulee järjestää tunnisteidenhallinta organisaation turvallisuusohjeiden mukaisesti (TL III + TL IV). **Kameravalvontajärjestelmä:** Turvallisuusalueita, kulkureittejä ja sitä ympäröivää aluetta valvotaan tallentavalla kameravalvonnalla. Kameravalvonta ja tallenteiden säilytysaika toteutettava organisaation riskienarvioinnin perusteella.

Liite 18. FT-03 Luvattoman pääsyn estäminen

FT-03	Luvattoman pääsyn estäminen
Vaatimus	1) Kulkua arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältäviin tiloihin tai rakennuksiin suojataan ja valvotaan sähköisen kulunvalvonta-järjestelmän avulla ja/tai mekaanisilla/sähkömekaanisilla avaimilla luvattoman pääsyn estämiseksi. 2) Kulkuoikeuksien hallinta on järjestetty siten, että luvaton pääsy salassa pidettävään tietoon on estetty. Pääsy salassa pidettäviä tietoja sisältäviin tiloihin sallitaan ainoastaan työtehtävistä johtuvan tiedonsaantitarpeen perusteella.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelussa käsiteltävään salassa pidettävään tietoon, sitä käsitteleviin laitteistoihin, tai edellä mainittujen turvallisuudesta huolehtiviin järjestelmiin on pääsy vain valtuutetuilla henkilöillä.
Lisätietoja	Vaatimusten täyttämisessä voidaan hyödyntää seuraavaa menettelyä: a) Organisaatiossa on käytössä kuvalliset henkilökortit tai vastaavat näkyvät tunnisteet, ja ne ovat esillä tiloissa kuljettaessa. b) Myönnetyistä kulkuoikeuksista ja käytetyistä mekaanisista avaimista on laadittu dokumentti tai loki, joita ylläpitää organisaation nimetty vastuuhenkilö. Kulkuoikeuksien ja mekaanisten avainten myöntämis-, katoamis- ja poistamisprosessi on kuvattu kirjallisesti. Kulkuoikeuksia ja avaimia tarkastellaan säännöllisesti ja tarpeen mukaan (väh. 6kk välein tai työntekijän työsuhteen alkaessa, loppuessa tai henkilön vaihtaessa työtehtävää). c) Avainten hallintaan nimetyllä vastuuhenkilöllä on hallussaan lukostokaavio ja avainkortti. d) Kulunvalvontajärjestelmässä on käytössä kahteen tekijään perustuva tunnistautuminen (esimerkiksi tunniste + PIN-koodi). Kulkuoikeudet ja mekaaniset avaimet on yksilöity käyttäjäkohtaisesti. Mikäli käytössä on yhteiskäyttötunnuksia, on toteutettu korvaava menettely henkilön luotettavaan yksilöintiin. e) Mekaaniset avaimet ovat kopiosuojattua sarjaa. Konesalin mekaaniset avaimet ovat eri sarjassa kuin rakennuksen muut avaimet. Vara-avaimien tai kulkutunnisteen säilytys (esim. hätätilanteita varten) on järjestetty sinetöitynä lukitussa paikassa. Kuittaus avaimen tai kulkutunnisteen noudosta pystytään todentamaan jälkikäteen. f) Avaimia on säilytettävä turvallisesti, eikä niitä saa merkitä siten, että ne voi yhdistää kohteeseen. Ulkoseinään upotetuissa avainsäilöissä voidaan säilyttää vain erillisiä huoltotilojen avaimia tai reittiavainta kiinteistöön.

Liite 19. FT-04 Palveluntuottajat ja vierailijat

FT-04	Palveluntuottajat ja vierailijat
Vaatimus	1) Vierailijat tunnistetaan, varustetaan vierailijakortilla ja kirjataan. Organisaatiolla on dokumentoitu vierailijapolitiikka. Vierailijoiden suhteen sovelletaan aina isäntäperiaatetta. 2) Siivous-, huolto- ja muu palveluntuottajien henkilöstö tunnistetaan, varustetaan vierailija-korteilla ja kirjataan. Säännölliset palveluntuottajat varustetaan kuvallisella henkilökortilla. 3) Alueella itsenäisesti liikkuvat tai suojattaviin kohteisiin käsiksi pääsevät palveluntuottajat on turvallisuusselvitetty. Henkilöt, joita ei pystytä tai ei ole vielä turvallisuusselvitetty liikkuvat saatettuna. Vrt. HT-02. 4) Huoltoihin, päivityksiin ja ylläpitoon liittyvät käytännöt on kirjallisesti kuvattu ja dokumentoitu.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelussa olevaan salassa pidettävään tietoon, sitä käsitteleviin laitteistoihin, tai edellä mainittujen turvallisuudesta huolehtiviin järjestelmiin on pääsy vain valtuutetuilla, luotettavaksi arvioiduilla henkilöillä.
Lisätietoja	Käytäntöjen ja ohjeiden tulisi ottaa huomioon vähintään seuraavat: a) Tietojen eheyden turvaaminen koko elinkaaren ajan, b) salassa pidettävien tietojen turvallinen poistaminen ennen ulkopuolisten tekemää korjausta tai huoltoa, c) salassa pidettävän tiedon säilytystilan tai sitä rajaavan tilan murtohälytysjärjestelmän, kulunvalvontajärjestelmään ja muihin valvontajärjestelmiin liittyvien laitetilojen ja niiden laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat vain niiden henkilöiden toimesta, joilla on erityinen lupa ja turvallisuusselvitys alueelle, tai organisaatioon kuuluvan henkilökunnan valvonnassa, d) vastaavien palveluntuottajien kanssa on tehty sopimukset (esim. polttoaine varavoimakoneita varten), e) organisaatiolla on voimassaolevat turvallisuussopimukset vartiointiliikkeen (turvallisuuspalvelut) ja kiinteistöpalveluita (ilma, vesi, sähkö, polttoaine, siivous) tuottavan yrityksen kanssa, f) hälytysten vasteaika on sellainen, että kiinnijäämisriski on merkittävä, g) organisaatiolla on henkilöstölle kirjallisesti kuvattu huoltotoimenpiteiden aikaiset ja muiden katkosten ennakoivat toimenpiteet, h) turvallisuusjärjestelmien asennus- ja huoltotoimenpiteet suoritetaan nimetyn yrityksen toimesta, minkä henkilöt ovat turvallisuusselvitetty, i) siivous suoritetaan kerran kuukaudessa tai tarvittaessa. Siivoojat ovat turvallisuusselvitetty. Siivoojat on varustettu kuvallisella henkilökortilla.

Liite 20. FT-05 Varautuminen ja jatkuvuudenhallinta

FT-05	Varautuminen ja jatkuvuudenhallinta
Vaatimus	1) Salassa pidettäviä tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältäviä tiloja tai rakennuksia suojataan tulipalolta, vesivahingolta, räjähdyksiltä, levottomuuksilta ja muilta luonnon ja ihmisten aiheuttamilta uhilta rakenteellisilla, teknisillä ja organisatorisilla turvatoimilla. 2) Keskeisen infrastuktuurin suojauksessa toteutetaan ainakin seuraavat turvatoimet: a) Rakenteelliset turvatoimet: Rakenteellinen palosuojaus (seinä-, lattia-, katto- ja ovi/ikkuna-rakenteiden palonkestävyys sekä läpivientien tiivistäminen paloluokkaa vastaavilla tuotteilla). b) Tekniset turvatoimet: i. Tila tai rakennus on kytketty automaattiseen paloilmoitinjärjestelmään, jonka hälytys välittyy hätäkeskukseen. ii. Suojattava tila on varustettu muusta kiinteistöstä erillisellä ilmanvaihtojärjestelmällä ja automaattisilla palonrajoittimilla (esim. automaattiset savupellit). iii. Tilaan on asennettu suojattavasta tiedosta riippuen riittävät olosuhde-, lämpötila- ja kosteusanturit (verkkovirran- tai paineenvaihtelut, kuumuus/kylmyys, vesivuodot). iv. Käytössä on automaattiset sammutusjärjestelmät, jotka havaitsevat esim. tulipalon aikaisessa vaiheessa ja aloittavat alkusammutuksen. v. Sähkön häiriötön saanti on varmistettu sähkönsyötön turvaavilla laitteilla (UPS, varavoima). vi. Tietoliikenteen varmistukset, ja jäähdytysjärjestelmän kahdennus. c) Organisatoriset turvatoimet: i. Pelastussuunnitelman laatiminen. ii. Nimetty vastuuhenkilö tai taho, kenelle tieto hälytyksistä välittyy. iii. Säännölliset pelastusharjoitukset ja paloturvallisuustarkastukset paloturvallisuus-määräysten noudattamisen toteamiseksi. iv. Jatkuvuussuunnittelu.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelun konesalien (ja vastaavien) toiminnan jatkuvuus on suojattu yleisiä riskejä vastaan. Soveltuviin jatkuvuutta tukeviin turvatoimiin sisältyy tyypillisesti seuraavat:
Lisätietoja	**Soveltuviin jatkuvuutta tukeviin turvatoimiin sisältyy tyypillisesti seuraavat:** **Rakenteellinen suojaus:** - Palo-osastointi, palon tai vuodon mahdolliseksi rajaamiseksi - Palonkestävien materiaalien käyttö, esim. 60 tai 90 min - Palokatkotuotteet, joilla estetään savu- ja palokaasujen kulkeutuminen muihin tiloihin **Tekninen suojaus:** - Laitteiden säännöllisen toimivuuden testaaminen ja dokumentointi - Prosessien toimivuus ja tiedon välittyminen oikeille tahoille tai henkilöille - Varakaapeloinnit ja yhteydet, järjestelmien kahdennukset, varmuuskopioiden sykli ja laajuus - Jatkuvuussuunnittelun häiriöt a) toimitilojen b) järjestelmien c) henkilöstön täysimääräisessä saatavuudessa **Organisatorinen suojaus:** - Pelastussuunnitelmalla ja jatkuvuudenhallinnalla on tarkoitus kuvata toimenpiteet, joilla ennalta ehkäistään, minimoidaan, rajoitetaan ja palaudutaan toimintahäiriöistä, onnettomuuksista, vahingoista ja poikkeuksellisista tapahtumista. - Suunnitelmien päivittäminen tulisi olla vähintään vuosittaista Kriittiset palvelimet ja laitteet tulee tunnistaa ja varmentaa toimintavaatimusten mukaisesti. Vrt. TJ-05 (Jatkuvuudenhallinta) ja KT-03 (Varmistus- ja palautusprosessit). Mikäli järjestelmän toimintavaatimukset ovat korkeat, on järjestelmien saatavuus varmennettava murtoa, ilkivaltaa, paloa, lämpöä, kaasuja, pölyä, tärinää, vettä ja sähkönkäytön katkoksia vastaan. Kriittisiä palvelin- ja laitetiloja ohjaavan LVI-automaationhallinnan etäkäyttö on estetty. Kriittisten palvelin- ja laitetilojen olosuhdesensoreja suojataan ja valvotaan. Pilvipalvelutoteutuksen keskeinen infrastruktuuri tulisi olla vähintään kahdessa erillisessä paikassa.

Liite 21. SA-01 Salauskäytännöt ja avainhallinta

SA-01	Salauskäytännöt ja avainhallinta
Vaatimus	1) Salauskäytäntöjen ja salausavainten hallinnan prosessit on suunniteltu, toteutettu ja kuvattu. 2) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. Prosessit edellyttävät vähintään a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, ja f) valtuuttamattomien avaintenvaihtojen estämisen. 3) Viranomaisen turvallisuusluokitellun tiedon suojaamisessa käytetään viranomaisen hyväksymiä salauskäytäntöjä, -vahvuuksia ja -tuotteita.
Soveltuvuus	Asiakastiedon suojaaminen suoraan tai epäsuoraan tilanteissa, joissa salaus on suojauksen toteuttava menetelmä.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 3: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Salausmenetelmien käyttö tuottaa riittävän luotettavan suojauksen.
Lisätietoja	Erityisesti liikennöitäessä julkisen tai muun heikommin suojatun verkon kautta, salausratkaisut ovat usein ainoita suojauksia salassa pidettävän tiedon luottamuksellisuuden, ja tyypillisesti myös eheyden suojaamisessa. Koska salausratkaisujen mahdollisia puutteita on usein äärimmäisen haastavaa korvata muilla suojauksilla, salausratkaisun valintaan ja turvalliseen käyttötapaan tulee kiinnittää erityistä huomiota. Tulee myös huomioida, että erityisesti pilvipalveluissa salauksen roolina on usein myös eri asiakkaiden tietojen erottelu (vrt. JT-03) yhteiskäyttöisessä infrastruktuurissa sekä esimerkiksi tiedon tuhoamisen (vrt. SI-02) luotettavuuden tukeminen. Erityisesti turvallisuusluokitellun tiedon suojaamisessa korostuu tarve käyttää salausratkaisuja, joiden riittävästä turvallisuudesta on luotettavaa näyttöä. Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salausratkaisun oikeellisesta toiminnasta varmistumisen lisäksi tulee huomioida muun muassa salausratkaisun käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa merkittävästi tilanteeseen, jossa salausta käytetään liikennöintiin hallitun ja suojatun fyysisen alueen sisällä (esimerkiksi kahden turva-alueen välinen liikennöinti hallinnollisen alueen kautta). Muihin salausratkaisun arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi ko. käyttötapauksen vaatimukset tiedon salassapitoajalle ja eheydelle. Erilaisiin tietoaineistoihin kohdistuu erilaisia riskejä. Esimerkiksi viranomaisten turvallisuusluokitellut tiedot ovat yleensä miellettävissä valtion turvallisuuden (yleisen edun) näkökulmasta suojattaviksi. Turvallisuusluokiteltuihin tietoihin voidaan toisaalta usein olettaa kohdistuvan eriävien tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Riskien eroavaisuus tulee huomioida myös salausratkaisujen valinnassa. Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avainhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään. Salausratkaisun salausavainten hallinnointiprosessien tuleekin olla suunniteltuja, toteutettuja ja kuvattuja/ohjeistettuja. Erityisesti salausratkaisujen osalta tulee riskienarvioinnissa huomioida myös toimitusketjujen turvallisuus. Vaikka salausratkaisu olisi riittävän turvallinen esimerkiksi salausratkaisun valmistajalta lähtiessään, toimitusketjun suojaamispuutteet voivat mahdollistaa salausratkaisun peukaloinnin, ja siten johtaa turvattoman salausratkaisun käyttöönottoon tietojärjestelmän tai palvelun osana. Vrt. SA-02 (Salaus fyysisesti suojatun turvallisuusalueen ulkopuolella) ja SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella). Lisätietoja on saatavissa Kyberturvallisuuskeskuksesta. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 22. SA-02 salaus fyysisesti suojatun alueen ulkopuolella ja SA-03 salaus fyysisesti suojatun alueen sisäpuolella

SA-02	Salaus fyysisesti suojatun alueen ulkopuolella
Vaatimus	1) Siirrettäessä asiakkaan salassa pidettävää tietoa hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (esimerkiksi palveluntarjoajan konesali, vrt. FT-01) ulkopuolella, tai matalamman turvallisuustason verkon kautta, salassa pidettävä tieto siirretään käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. 2) Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. 3) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. SA-01).
Soveltuvuus	Salausratkaisut konesalien välillä, salausratkaisut muiden matalammin suojattujen verkkojen kautta liikennöitäessä.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 3: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakastiedon luottamuksellisuus tai eheys ei vaarannu tilanteissa, joissa sitä siirretään epäluotettavien verkkojen kautta.
Lisätietoja	Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut (dark fiber) tulkitaan julkisiksi verkoiksi. Radiorajapinnan käyttö langattomissa verkkoyhteyksissä (esim. WLAN, 4G) tulkitaan poistumiseksi fyysisesti suojatun turvallisuusalueen ulkopuolelle. Toisin sanoen radiorajapinnan käyttö rinnastetaan julkisen verkon kautta liikennöinniksi, mikä tulee huomioida erityisesti liikenteen salauksessa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

SA-03	Salaus fyysisesti suojatun alueen sisäpuolella
Vaatimus	1) Kun asiakkaan salassa pidettävää tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (vrt. FT-01) ja kyseisen turvallisuustason verkon sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää, mikäli tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin. Vrt. JT-03. 2) Asiakkaiden salassa pidettävät tiedot tallennetaan pilvipalveluun salatussa muodossa, mikäli käytetään yhteiskäyttöistä laitteistoa. Vrt. JT-03. 3) Salausavaimistot ovat asiakaskohtaisesti eroteltuja. 4) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. SA-01).
Soveltuvuus	Asiakastiedon käsittely-ympäristöt pilvipalvelukokonaisuudessa, mukaan lukien esimerkiksi levyjärjestelmä- ja varmistusratkaisut.
Tietotyypit	1-3: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 4: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Eri asiakkaiden tietojen erottelusuojauksen tukeminen salausteknisin menetelmin tilanteissa, joissa eri asiakkaiden tietoja käsitellään yhteiskäyttöisillä laitteistoilla. Monitasoisen suojauksen toteuttaminen, tukien koko elinkaaren mittaista suojaamista.
Lisätietoja	2: Ei koske laskutukseen tai muuhun asiakassuhteen hallinnointiin liittyvää metatietoa. Yleisesti huomioitava, että lähtökohtaisesti pilvipalveluntarjoajalla on aina pääsy palvelussa käsiteltävään tietoon, mikäli tieto on elinkaarensa aikana palvelussa selväkielisessä muodossaan (esimerkiksi asiakkaalle näytettävä kuvana). Esimerkiksi yleiset omien avainten käyttöön (BYOK, Bring Your Own Keys) tai pilvipalveluntarjoajan fyysiseen konesaliin sijoitettaviin laitteistopohjaisiin turvamoduuleihin (HSM, Hardware Security Module) pohjautuvat ratkaisumallit rajaavat, mutta eivät tyypillisesti estä pilvipalveluntarjoajan pääsymahdollisuuksia palvelussa käsiteltävään tietoon. Salausta voidaan käyttää kuitenkin täydentävänä suojauksena tukemaan esimerkiksi eri asiakkaiden tietojen erottelua, suojattavien kohteiden tuhoamisprosessia tai tehtävien erottelua. Vrt. JT-03 (Tiedon erottelu). Erityisesti pilvipalvelujen skaalautuvuuden ja asiakaskohtaisen erottelun yhdistämiseen salaus on usein suositeltava toteutustapa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että useissa pilvipalveluratkaisuissa asiakastiedon salaamiskäytännöt ovat osin asiakkaan vastuulla ja konfiguroitavissa.

Liite 23. JT-01 jäljiteltävyys ja havainnointikyky

JT-01	Jäljitettävyys ja havainnointikyky
Vaatimus	1) Luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen on toteutettu. Erityisesti: a) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. b) Keskeiset tallenteet säilytetään vähintään 6 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. c) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta) vähimpien oikeuksien periaatteen mukaisesti. d) Lokitietojen välitys lokilähteiden ja lokikeräimen välillä on toteutettu suojatusti. Välityksen osapuolet tunnistetaan. Lokitiedot välitetään käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. Vaihtoehtoisesti lokitiedot voidaan siirtää erillisen hallintaverkon kautta. e) Kellot on synkronoitu sovitun ajanlähteen kanssa. f) Turvallisuusluokan III kasaumalle lisäksi: Keskeiset tallenteet säilytetään vähintään 24 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. g) Turvallisuusluokan III kasaumalle lisäksi: Keskeiset lokitiedot ohjataan lokilähteistä erilliselle lokikeräimelle (tai erillisille lokikeräimille). 2) Pilvipalveluntarjoaja toimittaa asiakkaan pyynnöstä, pilvipalveluntarjoajan vastuualueeseen kuuluvien järjestelmäkomponenttien osalta, asiakkaaseen vaikuttavat lokitiedot muodossa, josta asiakas voi tutkia häneen vaikuttavia tapauksia. 3) Pilvipalveluntarjoaja tarjoaa mahdollisuuden (teknisen rajapinnan) reaaliaikaiseen tiedonvaihtoon asiakkaan kanssa asiakkaan tietojen turvallisuuteen liittyvien tapahtumien välittämiseen (lokitiedot, tapahtumatiedot, tietoturvahavainnot). 4) Luotettavat menetelmät turvallisuuspoikkeamien havaitsemiseksi on toteutettu. Erityisesti: a) On olemassa menettely, jolla kerätyistä tallenteista (vrt. KT-04) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan). b) Verkkoliikenteen normaali tila (liikennemäärät, protokollat ja yhteydet) on tiedossa. c) On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan. d) On olemassa menettely, jolla pilvipalveluun kuuluvista palvelimista ja muista kohteista (hosts) voidaan havainnoida poikkeamia. e) Turvallisuusluokan III kasaumalle lisäksi: On olemassa menettely, jolla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä pyritään havaitsemaan. 5) On olemassa menettely havaituista poikkeamista toipumiseen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1a-e, 2-3, 4a-d, 5: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 1f-g, 4e: TL III (kasauma)
Suojaustavoite	Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitseminen ja selvittäminen, ml. tietomurtojen tutkinta ja korjaavien toimien suunnittelun tukena toimiminen.

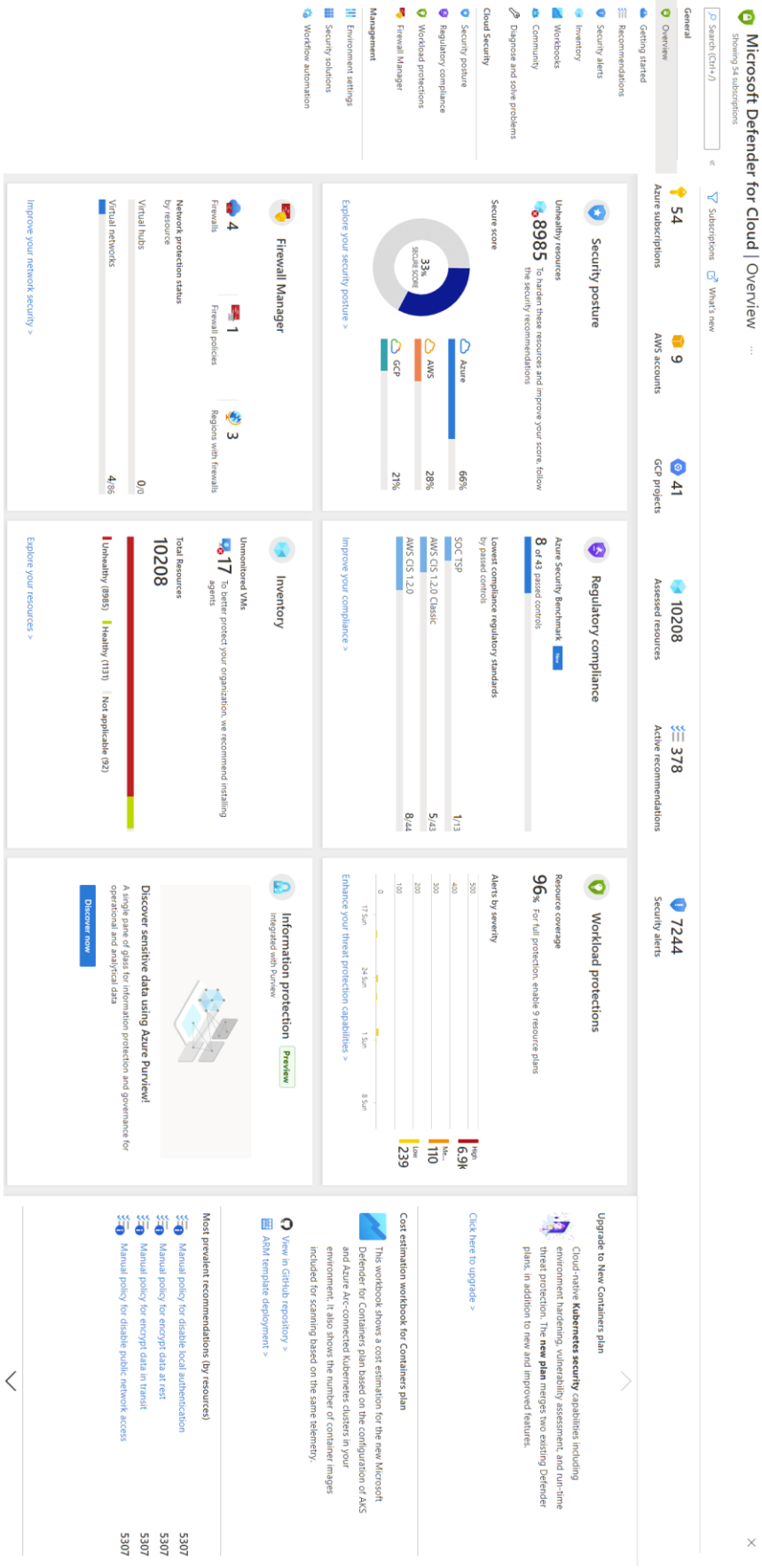
JT-01	Jäljitettävyys ja havainnointikyky
Lisätietoja	Jäljitettävyydellä tarkoitetaan järjestelmäympäristön tapahtumien kirjaamista siten, että poikkeamatilanteessa voidaan selvittää mitä toimia ympäristössä on tehty, kenen toimesta ja mitä vaikutuksia toimilla on ollut. Keskeisiä tallenteita ovat tyypillisesti keskeisten verkkolaitteiden ja palvelinten lokitiedot. Myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein. Kattavuusvaatimuksen voi useimmin toteuttaa siten, että varmistaa, että ainakin työasemien, palvelinten, verkkolaitteiden (erityisesti palomuurien, myös työasemien sovellusmuurien) ja vastaavien lokitus on päällä. Verkkolaitteiden lokeista tulisi myös pystyä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. Tapahtumalokeja olisi syytä kerätä järjestelmän toiminnasta, käyttäjäaktiviteeteista, turvaan liittyvistä tapahtumista ja poikkeuksista. Suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot vahvasti suojatulle lokipalvelimelle/-palvelimille, jonka/joiden tiedot varmuuskopioidaan säännöllisesti. Sekä ylläpitäjien oikeusturvan, kuin myös tietomurtoepäilyjen tutkinnan tukemiseksi, suositellaan tehtävien erottelua toteutettavaksi siten, että lokitietojen ylläpito on eriytetty muusta ylläpitohenkilöstöstä. Lokitietojen tallennus- ja seurantaohjelmiston toimivuutta tulee myös seurata. Lokitietojen säilytysajoissa tulee huomioida kyseessä olevan käyttötapauksen tarpeet. Esimerkiksi viranomaistoiminnassa rikosoikeudelliset vanhentumisajat voivat johtaa tyypillisesti vähintään viiden vuoden säilytysaikatarpeisiin. Väärinkäyttöyrityksen havaitseminen edellyttää useimmissa ympäristöissä käytännössä automatisoitujen havainnointi- ja hälytystyökalujen käyttöä. Lokitietojen manuaalinen tarkastelu on yleensä riittävä vain ympäristöissä, joissa lokimassat ovat hyvin pieniä ja lokien tarkasteluun on osoittaa riittävät henkilöresurssit. Tietojenkäsittely-ympäristön palauttaminen takaisin suojattuun tilaan kohtuullisessa ajassa edellyttää yleensä suunniteltuja, kuvattuja, koulutettuja sekä harjoiteltuja prosesseja sekä teknisiä menetelmiä. Verkkoliikennöinnin osalta tarkkailuun ja havaitun hyökkäyksen vaikutusten rajoittamiseen on useita soveltuvia toteutusmahdollisuuksia keskeisten verkkosolmujen tasolla tapahtuvasta tarkastelusta aina työasema- ja palvelinkohtaisiin sensoreihin sekä näiden yhdistelmiin. Riippumatta käytetyistä verkkolaitteista ja toimittajista, verkkotason havainnointikyvyn käytännön toteutus edellyttää tyypillisesti verkkoliikenteen normaalin tilan tuntemista. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 24. JT-04 Haittaohjelmasuojaus ja JT-05 Suojattavien kohteiden siirtäminen ja poistaminen

JT-04	Haittaohjelmasuojaus
Vaatimus	1) Pilvipalvelussa, mukaan lukien sen hallinnointiin käytettävissä järjestelmäympäristöissä, toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.
Soveltuvuus	Pilvipalveluun tuottamiseen liittyvät järjestelmät, mukaan lukien sen hallinnointiin käytettävät järjestelmäympäristöt.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakastiedon eheys, luottamuksellisuus tai saatavuus on riittävällä tasolla suojattu yleisiä haittaohjelmariskejä vastaan.
Lisätietoja	Haittaohjelmariskejä vastaan voidaan suojautua esimerkiksi järjestelmien kovennusmenettelyillä (vrt. JT-02), käyttöoikeuksien rajauksilla (vrt. IP-01), järjestelmien pitämisellä turvallisuuspäivitysten tasolla (vrt. KT-04), poikkeamien havainnointikyvyllä (vrt. JT-01), henkilöstön turvatietoisuudesta varmistumalla (vrt. HT-04) ja myös haittaohjelmantorjuntaohjelmistojen käytöllä. Riskejä voidaan pienentää myös riskialttiiden ympäristöjen eriyttämisellä tuotantoympäristöistä sekä muun muassa siirreltävien medioiden (esimerkiksi USB-muistien) käytön rajauksilla. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. Esimerkiksi mikäli asiakkaan vastuulle kuuluva asiakasjärjestelmä mahdollistaa tiedostojen lataamisen asiakasjärjestelmään, haittaohjelmasuojaukselle yleensä riskienhallinnalliset perusteet.

JT-05	Suojattavien kohteiden siirtäminen ja poistaminen
Vaatimus	1) Laitteita, ohjelmistoja, siirtomedioita tai vastaavia saa siirtää fyysisesti suojattujen toimitilojen ulkopuolelle vain erilliseen valtuutukseen pohjautuen. 2) Fyysisesti suojatun toimitilan ulkopuolella tapahtuva siirto ja käsittely tapahtuu siirrettävän suojattavan kohteen (luokituksen) mukaisesti. 3) Siirrettäessä asiakkaan salassa pidettävää tietoa fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolella, tieto on salatussa muodossa (vrt. SA-02) tai suojattava kohde on pilvipalveluntarjoajan henkilöstön jatkuvan valvonnan alaisuudessa. 4) Viranomaisen turvallisuusluokitellun tiedon suojaamisessa käytetään viranomaisen hyväksymiä salauskäytäntöjä, -vahvuuksia ja -tuotteita (vrt. SA-01).
Soveltuvuus	Asiakastietoa sisältävät laitteistot.
Tietotyypit	1-3: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 4: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojattavaa asiakastietoa ei vaarannu tilanteissa, joissa sitä siirretään fyysisesti suojattujen turvallisuusalueiden (esimerkiksi konesalit) ulkopuolella.
Lisätietoja	Erityisesti huomioitavaa: • Tietojen turvallinen poistaminen sekä tietovälineen tuhoaminen, vrt. SI-02 (Tietoaineistojen tuhoaminen) • Siirrettävien tietovälineiden salaus • Tietojen siirtäminen uudelle tietovälineelle, kun tietoväline korvataan Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että mikäli asiakkaan vastuulle kuuluva osuus siirtää salassa pidettävää tai/ja turvallisuusluokiteltua tietoa esimerkiksi asiakkaan päätelaitteille/päätelaitteilta, tulee tiedon/tietoliikenteen olla riittävän luotettavasti salatussa muodossa.

Liite 25. Microsoft Defender yleiskatsaus sivu



Liite 26. JT-02 järjestelmäkovennus

JT-02	Järjestelmäkovennus
Vaatimus	1) Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. 2) Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.
Soveltuvuus	Pilvipalvelun tuottamiseen liittyvät laitteistot ja ohjelmistot. Käsiteltäessä viranomaisen turvallisuusluokiteltua tietoa, kattaa myös hallintaan käytettävät päätelaitteet taustajärjestelmineen (esim. hakemistopalvelut).
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pienentää ohjelmistovirheiden ja virhekonfiguraatioiden riskiä poistamalla tarpeettomat toiminallisuudet käytöstä.
Lisätietoja	Turvallisen ohjelmistokoodin tekeminen on osoittautunut haastavaksi. Mitä enemmän ympäristössä on ohjelmistokoodia, sitä enemmän on mahdollisuuksia ohjelmistovirheille, toisin sanoen haavoittuvuuksille. Mitä enemmän ohjelmistokoodin turvallisuuteen nojaavia palveluja on tarjolla, sitä todennäköisempää on, että palveluissa on myös haavoittuvuuksia. Riskejä voidaan pienentää haavoittuvuuspinta-alaa pienentämällä, toisin sanoen tarjoamalla vain välttämättömiä palveluja alttiiksi hyökkäyksille. Järjestelmät ovat yleensä tulvillaan ominaisuuksia. Ominaisuudet ovat yleensä oletusarvoisesti päällä ja helppo ottaa käyttöön. Ominaisuudet ovat toisaalta usein myös tarpeettoman turvattomilla asetuksilla. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, nämä ovat myös pahantahtoisen toimijan käytettävissä. Jos välttämättömien palvelujen tarpeettoman turvattomia asetuksia ei muuteta, ovat nämä myös pahantahtoisen toimijan käytettävissä. Järjestelmissä on oletusarvoisesti usein käytössä esimerkiksi ennalta määriteltyjä ylläpitosalasanoja, valmiiksi asennettuja tarpeettomia ohjelmistoja ja tarpeettomia käyttäjätilejä. Koventamisella tarkoitetaan yleisesti järjestelmän asetusten muuttamista siten, että järjestelmän haavoittuvuuspinta-alaa saadaan pienennettyä. Järjestelmissä on yleisesti otettava käyttöön vain käyttövaatimusten kannalta olennaiset toiminnot, laitteet ja palvelut. Vastaavasti esimerkiksi automaattisille prosesseille on annettava vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä, jotta rajoitetaan onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja. Koventamiseen ja kovennetun asennuksen ylläpitämiseen voidaan usein hyödyntää myös konfiguraationhallintatyökaluja. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 27. JT-03 Tiedon erottelu

JT-03	Tiedon erottelu
Vaatimus	1) Asiakkaiden salassa pidettävät tiedot säilytetään luotettavasti toisistaan eroteltuna yhteiskäyttöisissä virtuaalisissa ja fyysisissä järjestelmissä.
Soveltuvuus	Salassa pidettävän asiakastiedon käsittelyyn liittyvät verkkolaitteet, virtualisointialustat, tallennusjärjestelmät, muistit, siirtomediat ja vastaavat.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakkaiden salassa pidettävään tietoon on pääsy vain kyseisellä asiakkaalla.
Lisätietoja	Erottelu on toteutettava riittävän luotettavasti, joko loogisen tai/ja fyysisen erottelun menetelmillä. Eräs yleinen käytössä oleva erottelumenetelmä esimerkiksi yhteiskäyttöisten verkkolaitteiden ja tallennusjärjestelmien osalta on salaus. Asiakaskohtaisilla avaimistoilla toteutettavaa tietoliikenteen salausta (data-in-transit) ja salausta tallennettaessa (data-at-rest) voidaan hyödyntää myös muiden turvatavoitteiden, esimerkiksi laitteistojen turvallisen hävittämisen, tukevana suojauksena. Vrt. SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella) ja KT-03 (Varmistus- ja palautusprosessit). Jos samaa laitteistoa käytetään useiden asiakkaiden tiedon käsittelyyn samanaikaisesti, tulee varmistua siitä, että tietojen fyysinen ja looginen erottelu on riittävän turvallinen. Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä fyysisiä laitteita. Esimerkiksi turvallisuusluokitellut tiedot voidaan säilyttää fyysisesti erillisellä virtualisointialustalla, jossa esimerkiksi mahdollisiin prosessorihaavoittuvuuksiin liittyvät rajapinnat on rajattu vain turvallisuusluokiteltujen tietojen valtuutettujen käyttäjien saavutettaviksi. Jos samaa laitteistoa käytetään useiden eri asiakkaiden tietojen käsittelyyn, mutta ei samanaikaisesti, tulee varmistua myös siitä, että edellisen asiakkaan tiedot on poistettu riittävän turvallisesti laitteistosta (ml. kaikki osat, BIOS, erilaisten muiden laitteiden välimuistit). Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä fyysisiä laitteita. Vrt. SI-02 (Tietoaineistojen tuhoaminen). Turvallisuusluokitellun salassa pidettävän tiedon omistajat voivat varata itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulee varmistua siitä, että verkon/järjestelmän toteutustapa mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä. Erityisesti palvelumalleilla IaaS ja PaaS, turvallisuusluokitellun tiedon erottaminen tulee varmistaa fyysisesti erillisillä verkoilla tai salatuilla virtuaalisilla tai ohjelmistopohjaisilla paikallisverkoilla. Vrt. SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella).