

Marko Pylkkänen

TIETOTURVALLINEN PILVIPALVELU SOSIAALI- JA TERVEYDENHUOLLOSSA

TIETOTURVALLINEN PILVIPALVELU SOSIAALI- JA TERVEYDENHUOLLOSSA

Marko Pylkkänen
Opinnäytetyö
Kevät 2022
Hyvinvointia edistävien digipalveluiden
asiantuntijan tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu

Tekniikan ylempi ammattikorkeakoulututkinto, hyvinvointia edistävien digipalveluiden asiantuntijan tutkinto-ohjelma

Tekijä: Marko Pylkkänen

Opinnäytetyön nimi: Tietoturallinen pilvipalvelu sosiaali- ja terveydenhuollossa

Työn ohjaaja(t): Janne Kumpuoja, Rami Kokkala, Atte Karhu

Työn valmistumislukukausi ja -vuosi: Kevät 2022

Sivumäärä: 65

Opinnäytetyö tehtiin osana 2M-IT:n ja sen asiakkaiden Pata-ohjelmistokehityshanketta, joka toteutti sosiaali- ja terveydenhuollon työvälineitä asiakasohjauksen tarpeisiin. 2M-IT on julkisten sosiaali- ja terveydenhuollon toimijoiden omistama tietotekniikkayhtiö. Työn tavoitteena oli tukea hanketta ja organisaatiota tietoturallisuuden kehittämisessä. Pata-järjestelmä toteutettiin Microsoft-pilvipalvelualustalle hyödyntäen pääosin Power Platform- ja Dynamics 365 -teknologioita.

Menetelmänä käytettiin kirjallisuuskatsausta tietoturallisuuden perusteista ja julkisten pilvipalvelujen tietoturallisuuden erityispiirteistä. Lisäksi selvitettiin Suomessa käytössä olevia tietoturallisuuden arvioinnin menetelmiä sekä sosiaali- ja terveydenhuollon tiedonkäsittelyn keskeistä lainsäädäntöä. Käytännön tutkimustapauksena esiteltiin tietoturallisuuden kannalta oleellisia Pata-järjestelmän piirteitä. Toteutetun järjestelmän tietoturallisuutta arvioitiin Kyberturvallisuuskeskuksen tarjoaman pilvipalvelujen tietoturallisuuden arviointikriteeristön (PiTuKri) mukaisesti itsearviointina. Arvioinnin tulokset, joita ei julkaista, tuotettiin erilliseen PiTuKri-arviointityökaluun.

Tietoturallisuuden itsearvioinnin suorittamisen aikaan Pata-järjestelmän kehittäminen oli vielä kesken. Kuten oli oletettavaa, arvioinnissa ilmeni useita tietoturallisuuden kehittämiskohteita, joiden havaitseminen edesauttoi järjestelmän jatkokehittämistä sekä tietoturallisuuden yleistä kehittämistä organisaatiossa.

Vastaus keskeiseen kysymykseen, soveltuuko monikansallisen yhtiön tuottama pilvipalvelualusta suomalaiseen sosiaali- ja terveydenhuollon tietojen käsittelyyn, osoitettiin teorian ja käytännön toteutuksen ja tietoturallisuuden arvioinnin avulla. Tuloksena havaittiin, että Pata-järjestelmä, joka ei ole varautumisen kannalta kriittinen, voidaan rakentaa pilvipalvelualustalle, kun pilvipalvelun tarjoajan toimintatavat ja palvelut tukevat vahvaa tietoturallisuutta ja pilvipalvelun tarjoaja noudattaa paikallista lainsäädäntöä.

Kehittämisajatuksena esitettiin, että Pata-järjestelmän ehkä voisi toteuttaa matalamman tason kehittämisvälineillä, jolloin ympäristö ei olisi yhtä altis jatkuville muutoksille kuin Power Platformin tuotteet. Lisäksi ohjelmistojen lisensointikustannukset pysyisivät tällä tavoin maltillisempina tekijänoikeuksien ollessa laajemmin omissa käsissä. Tosin matalamman tason ohjelmistoteknologian hyödyntäminen voi johtaa hitaampaan etenemiseen ja sitä kautta korkeampiin kehittämiskuluihin.

Asiasanat: Tietoturallisuus, pilvipalvelu, sosiaalihuolto, terveydenhuolto, asiakasohjaus, power platform

ABSTRACT

Oulu University of Applied Sciences

Master Programme in Technology, Degree Programme in Well-being Digital Service Expertise

Author(s): Marko Pylkkänen

Title of thesis: Secure cloud-based information management in Finnish social and healthcare

Supervisor(s): Janne Kumpuoja, Rami Kokkala, Atte Karhu

Term and year when the thesis was submitted: Spring, 2022

Number of pages: 65

The goal of this study was to improve information security in a project developing customer service application for Finnish public sector social and healthcare. At the time of this study, the Pata-project's software development on Microsoft Dynamics 365 Customer Service and other Power Platform SaaS services was still on-going.

The main problem was to evaluate information security aspects of public cloud adoption in public sector health and social care services, where personal data is highly sensitive.

Basic steps were taken in a form of literature review as foundations of information security were studied. Next, the most relevant laws and regulations in Finland and EU were introduced as well as common methods of assessing information security.. The last section of literature review contains cloud-specific aspects of information security.

A case study of practical cloud-based information security was conducted with the Pata-system. First a technology review was done focusing mainly on information security aspects. An information security self-assessment based on the Criteria for Assessing the Information Security of Cloud Services (The PiTuKri) was performed to determine the current status of Pata-system and to identify areas requiring improvement. The criteria is published by National Cyber Security Center in Finland (Kyberturvallisuuskeskus). The assessment resulted several targets for improvement, which was expected as the application development was still on-going. Thus, this study satisfied the goal of improving information security within the project.

To answer the question, is public cloud platform safe enough for social and healthcare applications in Finland, the answer is yes, it is, based on facts and experiences of the case study utilizing Microsoft's high level cloud services, which appear to have excellent processes, practices, guidelines and track record in regards of information security. Microsoft appears to respect local laws. There are no special contingency requirements for the Pata-system because it is intended for customer service centers which are not mission critical. In case of extreme conditions, the customer service can be omitted for some time.

Moving from high-level SaaS applications to more basic Azure software development could mitigate unexpected changes in production environment of the Power Platform. This could also reduce software licensing costs, but on the other hand, the development might require more efforts.

Keywords: information security, cloud services, social services, healthcare, public sector, power platform

SISÄLLYS

SISÄLLYS.....	5
SANASTO.....	7
1 JOHDANTO	10
2 TIETOTURVALLISUUDEN PERUSTEET.....	11
2.1 Digitaalinen turvallisuus.....	11
2.2 Tietoturvallisuus ja CIA-malli	13
2.3 Parkerian Hexad – tietoturvallisuuden kuusi kulmaa	15
2.4 Riski ja uhka	16
2.5 Riskien hallintaprosessi ja häiriöiden hallinta	18
2.6 Lakien ja määräysten noudattaminen.....	21
2.7 Tietoturvallisuuden arvioinnin kriteeristöt.....	23
2.8 Julkisen pilvipalvelun erityispiirteet.....	25
3 PATA-JÄRJESTELMÄ.....	30
3.1 Tenantin rakenne ja yhteiset peruspalvelut - infrastruktuuri	31
3.2 Power Platform.....	35
3.3 Dynamics 365 Customer Service ja Omnichannel	37
3.4 Tietoarkkitehtuuri.....	38
3.5 Järjestelmän toiminnot	39
3.6 SaaS-palvelujen edut ja haasteet - Power Platform	40
4 TIETOTURVALLISUUDEN ITSEARVIOINTI	43
4.1 Arvioinnin eteneminen	44
4.2 Esiehdot	47
4.3 Turvallisuusjohtaminen.....	49
4.4 Henkilöstöturvallisuus.....	49
4.5 Fyysinen turvallisuus	50
4.6 Tietoliikenneturvallisuus	50
4.7 Identiteetin ja pääsyn hallinta	52
4.8 Tietojärjestelmäturvallisuus	54
4.9 Salaukskäytännöt ja avainten hallinta	56
4.10 Käyttöturvallisuus, siirrettävyys ja yhteensopivuus.....	58
4.11 Muutostenhallinta ja järjestelmäkehitys	58

5	HAVAINTOJA JA POHDINTAA	60
5.1	Johtopäätöksiä Pata-järjestelmän tietoturvallisuudesta	61
5.2	Organisaation valmiudet pilveen	63
6	LOPUKSI	64
	LÄHTEET	66
	LIITTEET	71

SANASTO

App Service (Azure)

Azuren App Service on SaaS tason palvelu, jossa voidaan helposti kehittää, viedä tuotantoon ja skaalata web-sovelluksia ja rajapintapalveluja (API, Application Programming Interface). (Microsoft, 2022u)

Azure

Microsoft Azure on julkinen pilvialusta, tarjoaa käytännössä kaikki palvelut modernin IT-infrastruktuurin toteuttamiseksi ja pilvipohjaisten sovellusten kehittämiseksi. (Microsoft, 2022f)

Azure Active Directory (AAD)

Microsoftin Azure-pilvipalveluun kuuluva identiteetinhallinta-, tunnistamis- ja käyttöoikeuspalvelu. (Microsoft, 2021d)

Azure Express Route

Asiakaskohtainen verkkoyhteys Azure-palveluihin. (Microsoft, 2021b)

Conditional Access

Microsoftin pilvipalvelujen identiteetin- ja pääsynhallinnan (Azure Active Directory) toiminto, joka sisältää kehittyneitä tietoturvallisuuden hallintakeinoja, kuten monivaiheinen tunnistautuminen. (Microsoft, 2022k)

DDoS

Distributed denial of service attack, eli hajautettu palvelunestohyökkäys pyrkii ylikuormittamaan internet-palvelun resurssit, jolloin asiakkaat eivät pääse käyttämään palvelua. (Microsoft, 2022q)

Defense in depth

Pitkään käytössä, sotavoimien lanseeraama malli, jossa kohdetta suojataan kerroksittain. Tavoitteena on hidastaa hyökkäyksen etenemistä ja tunnistaa hyökkäys ajoissa vahinkojen välttämiseksi. (Microsoft, 2022r, Gates, S. 2019)

DevOps

Microsoftin DevOps-ohjelmisto tarjoaa ketterän ohjelmistokehityksen välineet vaatimusmäärittelyyn, laadunvarmistukseen, ohjelmiston julkaisuun ja lähdekoodin hallintaan. (Microsoft, 2022a)

Digitaalinen turvallisuus

Usein kyberturvallisuuden synonyymi. Digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. (Sanastokeskus, 2018)

Dynamics 365 Customer Service

Microsoft D365 CS on asiakkuudenhallintajärjestelmä, joka on tarkoitettu asiakaskontaktien hallintaan. (Microsoft, 2022l)

Hybridipilvi / yhdistelmäpilvi

Pilvipalvelun ja konesalissa tuotettujen palvelujen yhdistelmä, jossa tietojen käsittely hajautetaan pilven ja konesalin kesken tietoturvallisuuden, varautumisen, kustannusten, kapasiteettitarpeen tai muun syyn vuoksi omassa konesalissa, ja osa palveluista toteutetaan pilvipalveluna. (Microsoft, 2022n)

Jatkuvuudenhallinta

Organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa. (Sanastokeskus, 2018)

Julkinen pilvipalvelu (engl. public cloud)

Internettiin sijoittuva pilvipalvelu. (NIST, 2011)

Jäännösriski (engl. residual risk)

Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä. (Sanastokeskus, 2018)

Kyberturvallisuus

Tavoitetilä, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kybertoimintaympäristön synonyyminä voidaan käyttää termiä digitaalinen toimintaympäristö. (Sanastokeskus, 2018)

Monivaiheinen tunnistautuminen

Monivaiheinen tunnistautuminen (engl. multi-factor authentication, MFA) tarkoittaa palveluun kirjautuvan käyttäjän tunnistamista useammalla keinolla. (manigcloud.fi)

Pilvipalvelu

Pilvipalveluilla tarkoitetaan verkon yli saavutettavaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään jaettujen, skaalautuvien ja joustavien resurssien mallia, joka on automatisoitu osin itsepalveluperiaatteella tuotettavaksi. (Kyberturvallisuuskeskus, 2019)

Power Apps

Microsoftin Power Platformiin sijoittuva low-code sovelluskehitys- ja tuotantoteknologia. (Microsoft, 2022o)

Power Platform

Microsoftin SaaS pilvipalveluympäristö, johon kuuluu mm. Power Apps, Dynamics 365, Power BI ja Dataverse-tietovaranto. Power Platform hyödyntää tiettyjä Azure-palveluita, kuten Azure Active Directoryä. (Microsoft, 2022e)

Sertifiointi

Tietoturvallisuuden arvioinnin vahvistamiseksi organisaatio tai rajattu tietojärjestelmäkokoisuus voidaan sertifioida tiettyä kriteeristöä vastaan. Esimerkiksi Kyberturvallisuuskeskuksen hyväksymät tietoturvallisuuden arviointilaitokset voivat suorittaa sertifiointin.

Tenantti (engl. tenant)

SaaS pilvipalvelujen yhteydessä tenantti on asiakkaan valitsema palvelujen sijainti, joka sisältää pilvipalveluja tuottavat palvelimet. Esimerkiksi Pata-järjestelmän tenantti sijaitsee EU:n alueella, North Europe ja West Europe alueilla. Azure PaaS palvelujen ja IaaS infrastruktuuripalvelujen, kuten virtuaalipalvelinten kohdalla tenantti voi sijaita datakeskuksissa maailmanlaajuisesti. Käytettävien datakeskusten sijainti voidaan kuitenkin erikseen määritellä. Azure AD tenantti on tietty Azure AD, joka sisältää asiakkaan käyttäjätilit ja -ryhmät. (Microsoft, 2021e)

Tietoturvallisuus

Järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus. (Sanastokeskus, 2018)

Tietosuoja

Ihmisten yksityisyyden suojeleminen ja yksilöä koskevien tietojen suojaaminen oikeudellomalta käytöltä henkilötietoja käsiteltäessä. (Sanastokeskus, 2018)

Subscription

Microsoft Azure Subscription on Microsoftin kanssa tehtävä sopimus yhden tai useamman pilvialustan tai pilvipalvelun käyttämisestä. (Microsoft, 2021q)

Riskienhallinta

Järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet. (Sanastokeskus, 2018)

Varautuminen

Toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa. (Sanastokeskus, 2018)

Yksityinen pilvi (engl. Private Cloud)

Kapasiteettipalvelu, joka ei ole tarjolla julkisesti, vaan on kohdistettu valituille toimijoille. Yksityinen pilvi voi tarjota korkeampaa tietoturvallisuutta ja tietosuojaa, kuin julkinen pilvipalvelu. (Microsoft, 2022p)

Zero Trust

Nollaluottamus, (engl. Zero Trust) eli "luottamattomuuden periaate" on kehitetty modernien ja ketterästi kehittyvien ICT-ympäristöjen suunnitteluun. Se auttaa rakentamaan tietoturvaa nykypäivän monimutkaisessa maailmassa, jossa eri ICT-järjestelmät integroituvat toisiinsa. Zero Trust -mallin perustana on nimensä mukaisesti, että luottamus on nolla kaikilla ajan hetkillä. Laitteet ja käyttäjät tunnistetaan kaikissa tilanteissa ja päätös pääsyn sallimisesta perustuu riskiarvioon. Vahvan tunnistautumisen käyttö on yksi perusasioita. (Salo, 2022)

1 JOHDANTO

Opinnäytetyö on tehty osana 2M-IT:n ja sen asiakkaiden Pata-ohjelmistokehityshanketta, joka toteuttaa työvälineitä sosiaali- ja terveydenhuollon asiakasohjauksen tarpeisiin. 2M-IT on julkisten sosiaali- ja terveydenhuollon toimijoiden omistama tietotekniikkayhtiö. Opinnäytetyön on tarkoitus tukea Pata-ohjelmistokehitystä ja 2M-IT:tä organisaationa tietoturvallisuuden kehittämisessä. Ohjelmistoa kehitetään Microsoft-pilvipalvelualustalle. Niinpä tämän työn nimeksi muodotui Tietoturallinen pilvipalvelu sosiaali- ja terveydenhuollossa.

Kyberturvallisuuskeskus määrittelee pilvipalvelun seuraavasti: *”Pilvipalveluilla tarkoitetaan verkon yli saavutettavaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään ja -ettujen, skaalautuvien ja joustavien resurssien mallia, joka on automatisoitu osin itsepalveluperiaatteella tuotettavaksi.”* (Kyberturvallisuuskeskus, 2019)

Luvussa 2 käsitellään alkuun tietoturvallisuuden perusteita ja käsitteitä yleisellä tasolla. Tämän jälkeen tutustutaan ylätasolla julkisen sosiaali- ja terveydenhuollon tiedonkäsittelyä ohjaavaan lainsäädäntöön. Seuraavaksi esitellään tietoturvallisuuden arviointimenetelmiä ja -kriteeristöjä. Luvun loppuun tarkastellaan, millaisia tietoturvallisuuden erityispiirteitä liittyy nimenomaan pilvipalveluihin.

Luvussa 3 esitellään Pata-järjestelmä painottaen tietoturvallisuuteen liittyviä seikkoja. Pata-järjestelmän toteutustavassa on pitkälti hyödynnetty korkean tason pilvipalveluita, joissa ympäristöjen hallinta on pääosin Microsoftin vastuulla. Tietoturvallisuus ei ole pelkkää teknologiaa, vaan teknologiaa hyödyntävien organisaatioiden ja ihmisten toiminta voi oleellisesti edesauttaa tai heikentää turvallisuutta, minkä hyvin tuo esiin luvussa 4 esitelty tietoturvallisuuden itsearviointiarviointi. Luku 5 on teoriaosuuteen ja kokemuksiin perustuvaa pohdintaa pilvipalveluista, Pata-järjestelmän toteutustavasta, tietoturvallisuudesta sekä organisaatiollisista valmiuksista. Keskeinen kysymys on, soveltuvatko monikansallisten yhtiöiden tuottamat pilvipalvelut suomalaiseen sosiaali- ja terveydenhuollon tietojen käsittelyyn. Pohdintaa herättävät myös kysymykset korkean tason SaaS-palvelujen hyödyistä ja haitoista.

Tavoitteena on, että tämä dokumentti voisi olla oppaana sellaiselle, joka ehkä harkitsee pilvipalvelujen toteuttamista sosiaali- ja terveydenhuollon toimialalla, tai sitten ihan muulla alalla. Tämä opinnäytetyön raporttiosa on julkinen. Työhön liittyy muita dokumentteja, jotka sisältävät 2M-IT:n liikesalaisuuksia.

2 TIETOTURVALLISUUDEN PERUSTEET

Tämä luku tietoturvan perusteista pohjautuu Andressin (2019) pohdintaan. Aluksi tietoturvan perusteita käsitellään yleisellä tasolla, ottamatta kantaa, onko kyseessä pilvipalvelu tai muun tyyppinen tietojenkäsittelyratkaisu. Pilvipalvelun erityispiirteitä, lainsäädäntöä ja tietoturvallisuuden arviointia tarkastellaan luvun loppupuolella.

Tietotekniikan ja arkaluonteisenkin tiedon käsittely erilaisilla tietovälineillä liittyy usein arkipäiväisiin toimiin. Tuskin kuluu päivääkään ilman tietokonetta, puhelinta, älytelevisiota, nettiä tai esimerkiksi pankkikorttia, jonka tietoja saattaa olla monessakin nettikaupassa. Pystyykö tavallinen ihminen tietämään, kenellä kaikilla on pääsy luottamuksellisiin tietoihin, kuten terveystiedot, palkanmaksu, verotus, internetasiointin tiedot tai maantieteellinen sijainti? Voivatko terveydenhuollon tiedot vuotaa internettiin tai onko rahat turvassa pankkitilillä. Pysyväthän asunnon omistajatiedot oikeina?

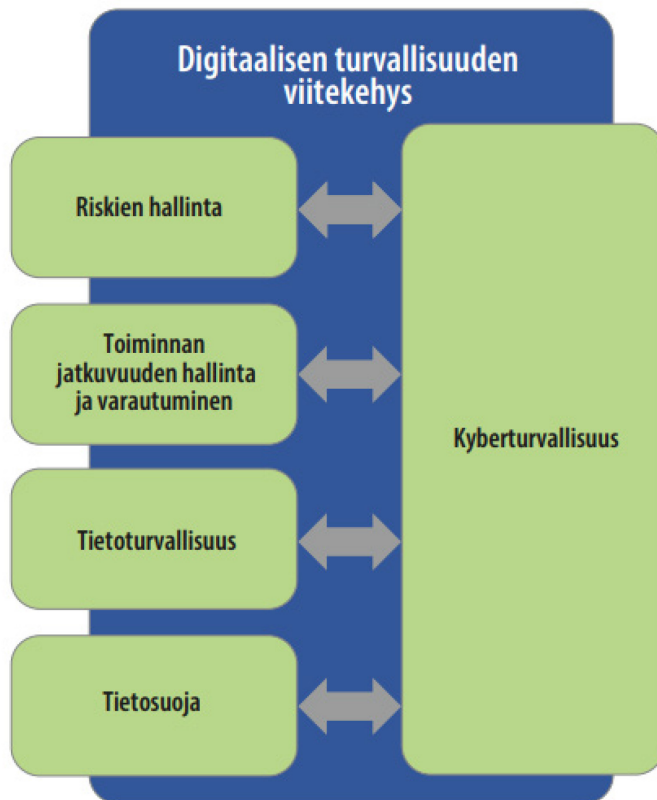
Kolme vuosikymmentä sitten, 90-luvun alussa, pankkimaailma ja suurten yritysten taloushallinto oli jo sähköistetty. Sen sijaan vain harvat kotitaloudet hoitivat raha-asioitaan digitaalisesti eli puhelinmodeemin välityksellä. Laskuja maksettiin ennemminkin pankin maksuautomaatin ääressä. Teknologia oli vielä kehittymätöntä ja sen hyödyntäjiä oli vähän, eikä näin ollen tietoturvaan liittyvää rikollisuuttakaan juuri esiintynyt. Kiihtyvällä tahdilla uudistuva teknologia ja globaali verkkoympäristö asettaa jatkuvasti uusia haasteita tietojenkäsittelyn turvallisuudelle.

Mistä sitten tietoturvallisuudessa on kyse ja kuinka riittävä turvallisuus saavutetaan? Esittelen seuraavassa tietoturvan käsitteitä sekä kansainvälisten että suomalaisten viitekehysten kautta.

2.1 Digitaalinen turvallisuus

Suomessa valtionhallinto on ottanut käyttöön käsitteen digitaalinen turvallisuus. Valtiovarainministeriö (2020) pohjustaa digitaalisen turvallisuuden tavoitetta seuraavasti: *”Kansalaisten, yritysten ja yhteisöjen tulee voida luottaa eettisesti kestäviin, avointa ja läpinäkyvää toimintaa tukeviin ja turvallisiin julkisen hallinnon palveluihin. Digitalisoitumisen nopea edistyminen, tietojen laittomaan käyttöön ja virheellisillä tiedoilla vaikuttamiseen liittyvät uhkat sekä lisääntynyt kansallinen ja kansainvälinen keskinäisriippuvuus asettavat uusia vaatimuksia koko julkisen hallinnon digitaaliselle turvallisuudelle ja sen ohjaukselle.”*

Digitaalisen turvallisuuden viitekehys (KUVIO 1) sisältää riskien hallinnan sekä toiminnan jatkuvuuden hallinnan ja varautumisen prosessit. Viitekehyksessä on tunnistettu kyberturvallisuus yhdistävänä käsitteenä, johon edellä mainittujen prosessien lisäksi liittyvät myös tietoturvallisuus ja tietosuoja.



KUVIO 1 Valtionvarainministeriön (2020) määrittelemä digitaalisen turvallisuuden viitekehys.

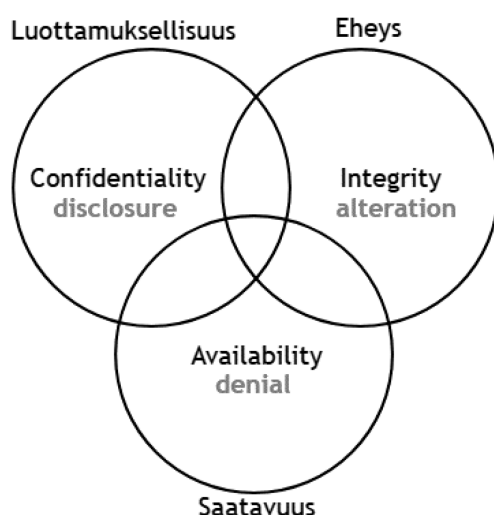
Valtiovarainministeriö tarkastelee viitekehysten kautta erityisesti valtiohallinnon tavoitteita ja vastuita. Viitekehys on merkityksellinen tämän opinnäytetyön kannalta, sillä tarkastelun kohteena on julkisen sektorin sote-palvelu. Lakien ohella mm. sosiaali- ja terveysministeriö ohjeistaa kunta- ja hyvinvointialuetasoa palvelujen toteuttamisessa ja tietojen käsittelyssä. Tietoturvallisuuden käsitteistöä on siis hyvä hahmottaa myös tämän viitekehysten kautta. Viitekehysten käsitteet on avattu tarkemmin sanastossa sivulla 7.

2.2 Tietoturvallisuus ja CIA-malli

Turvallisuus yleisenä käsitteenä tarkoittaa ihmisten, asioiden ja tavaroiden suojaamista, oli kyse sitten verkkohyökkäyksestä, luonnonkatastrofista, ilkivallasta, häviämisestä tai virheellisestä käytöstä. (Andress, 2019)

Valtiovarainministeriö käyttää dokumenteissaan Sanastokeskuksen määritelmää tietoturvallisuudesta: *”Järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus.”* (Sanastokeskus, 2018)

Andress (2019) käsittelee kirjassaan samoja käsitteitä. Hän toteaa, että on usein hyödyllistä lähestyä asiaa mallin kautta. Hän esittelee CIA-mallin (KUVIO 2), jonka kolme peruskäsitettä ovat täysin yhtenevät Sanastokeskuksen määritelmän kanssa. Sama malli voidaan esittää myös käsitteiden negaatioina, jotka ovat disclosure – paljastaminen, alteration – muuntaminen ja denial – kieltäminen/estäminen.



KUVIO 2 CIA-malli (Andress, 2019)

Yksittäistä tietoturvatapausta voidaan tarkastella vähintäänkin näiden kolmen näkökulman kautta. Kirjassaan Andress kertoo esimerkin arkaluonteista tietoa sisältävien salakirjoittamattomien varmuuskopionauhojen lähetyksestä, joka katoaa tai varastetaan. Nämä olivat ainoat jäljellä olevat kopiot tiedoista.

Saatavuuden näkökulmasta esimerkin ongelmana on, että ainoat kopiot tiedoista ovat hävinneet. Luottamuksellisuuden näkökulmasta ongelmana on, että joku toinen taho on saattanut saada salaamattomia arkaluonteisia tietoja haltuunsa. Vaikka nauhat saataisiin takaisin, on tiedon eheys

ongelma, koska ei voida varmuudella tietää, onko joku toinen taho muuttanut nauhoilla olevia sa-laamattomia tietoja. (Andress, 2019) Seuraavissa kappaleissa esitellään CIA-mallin käsitteet tar-kemmin.

CONFIDENTIALITY - LUOTTAMUKSELLISUUS

Luottamuksellisuus tarkoittaa, että tietoja voivat käsitellä ainoastaan valtuutetut tahot. Esimerkiksi terveydenhuollon tietojen käsittely on luottamuksellista. Terveystietoja saavat käsitellä terveyden-huollon ammattihenkilöt, joilla on lain tarkoittama hoitosuhde tai muu syy potilaan tietojen käsitte-lemiseen. Luottamuksellisuus voi rikkoontua helposti esimerkiksi tilanteessa, jossa vastaanoton odotustilassa hoitaja haastattelee potilasta, jolloin odotustilan toiset potilaat kuulevat arkaluontei-sen keskustelun.

INTEGRITY – EHEYYS

Tiedon eheyden turvaaminen tarkoittaa sitä, että tieto ei muutu hallitsemattomasti teknisestä syystä eikä kukaan henkilö muuta tietoa kuin tarkoituksenmukaisella tavalla. Esimerkkinä eheyden hal-linnasta mainittakoon Microsoft Teams -työtilat, joissa vain tunnistetuilla, työtilaan kutsutuilla hen-kilöillä on oikeus käsitellä ja muuttaa tietoja. Teknisen eheyden ongelmia voi syntyä esimerkiksi viallisen varmuuskopionauhan vuoksi, jolloin tietoja ei täysin saada luettua.

Tiedon eheydellä on erityinen merkitys, jos tietoa käytetään henkilön turvallisuuteen liittyvässä pro-sessissa, kuten esimerkiksi potilaan hoidon päätöksenteossa. (Andress, 2019)

AVAILABILITY – SAATAVUUS

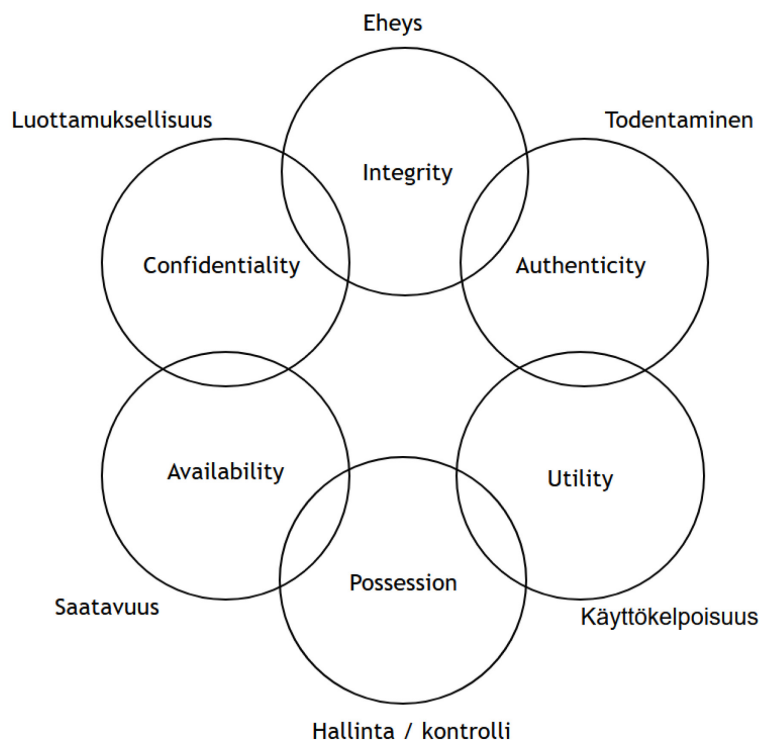
Tiedon saatavuus on kolmas keskeisistä tarkastelukulmista. Esimerkiksi potilaan leikkauksen yh-teydessä on tärkeä tietää, mitä lääkkeitä potilaalle on annettu. Jos potilastietojärjestelmään tallen-nettuja tietoja ei ole saatavilla, voi turvallisten hoitopäätösten teko vaikeutua. Kriittisissä tilanteissa tiedon saatavuuteen onkin kiinnitettävä erityistä huomiota esimerkiksi tiedon kahdentamisella. Leik-kauksen yhteydessä tietoja voidaan mahdollisesti kirjoittaa myös paperille ja käyttää ennalta tehtyjä paperitulosteita.

Toisena esimerkkinä saatavuuden ongelmasta voidaan mainita internetsivustoihin kohdistuvat ns. palvelunestohyökkäykset (engl. Distributed Denial of Service, DDoS), joissa pahantahtoiset toimijat ylikuormittavat palvelimia siten, että oikeat asiakkaat eivät pääse asioimaan. (Microsoft, 2022q)

2.3 Parkerian Hexad – tietoturvallisuuden kuusi kulmaa

Edellisessä kappaleessa kuvattu CIA-malli antaa hyvän lähtökohdan tietoturvallisuuden riskien arviointiin. Kuten Valtiovarainministeriön käyttöönottama digitaalinen turvallisuus -viitekehys kappaleessa 2.1 osoittaa, tietoturvallisuuden ongelmakenttä on laaja, eikä täyttä yksikäsitteisyyttä ole. Parkerian Hexad laajentaa CIA-mallia kolmella käsitteellä lähestyen digitaalisen turvallisuuden viitekehystä.

Messier, R. 2019 esittelee Parkerian Hexad -mallin väljästi suomennettuna seuraavasti: ”Vuonna 1988 Donn Parker lisäsi CIA-malliin kolme uutta ominaisuutta. Näitäkään ominaisuuksia ei pidetä vakiintuneina, koska keskusteluissa viitataan tarpeeseen purkaa malli edelleen yksityiskohtaisempiin ominaisuuksiin.” Parkerin määrittelemät CIA mallia tarkentavat käsitteet ovat todentaminen, käyttökelpoisuus ja hallinta (KUVIO 3).



KUVIO 3 The Parkerian Hexad (Messier, 2019)

Parkerian Hexad helpottaa tapauskohtaisten tietoturvakysymysten käsittelyä tarjoamalla käytännönläheisemmät näkökulmat kuin CIA-malli, jonka kolme teemaa ovat sellaisenaan laajempia käsitteitä. Seuraavissa kappaleissa tarkastellaan lähemmin Parkerin lisäämiä uusia käsitteitä.

POSESSION (OR CONTROL, SUOM. HALLINTA)

Tietojen säilyttäminen ja siirtäminen tulee hoitaa siten, että ulkopuoliset tahot eivät missään tilanteessa pääse niihin käsiksi. On oltava varmuus tietovälineiden tai tiedonsiirtokanavien hallinnasta siten tiedon koko elinkaaren ajalla. Esimerkiksi ulkoinen kiintolevy tulee säilyttää turvallisessa paikassa ja luotettujen tahojen hallinnassa.

AUTHENTICITY (TAI NON-REPUDIATION, SUOM. TODENNETTAVUUS, KIISTÄMÄTTÖMYYS)

Todentamisella pyritään osoittamaan, että tieto tai dokumentti on se, mitä se esittää olevansa. Esimerkiksi, sähköpostin digitaalinen allekirjoituksen avulla vastaanottaja voi varmistua lähettäjän henkilöllisyydestä. Digitaalisen allekirjoituksen luotettavuus perustuu allekirjoituksessa käytettävän avaimen turvalliseen säilyttämiseen. Todentaminen tässä tapauksessa siis merkitsee, että vastaanotetut tiedot ovat peräisin ilmoitetusta lähteestä.

UTILITY (SUOM. KÄYTTÖKELPOISUUS)

Käyttökelpoisuus tarkoittaa, että tallennetut tai vastaanotetut tiedot saadaan käyttöön luotettavasti. Esimerkiksi 90-luvulla käytössä ollut 3,5 tuuman levyke eli 'korppu', joka sisältää tärkeitä tietoja. Levykkeellä olevat tiedot eivät ehkä olekaan käyttökelpoisia, koska nykyisissä tietokoneissa ei ole korppuasemaa, joka pystyisi lukemaan bitit levyn pinnalta. Eli data on luultavasti olemassa, mutta se ei ole käyttökelpoista.

2.4 Riski ja uhka

Sana riski on mainittu tässä dokumentissa jo useita kertoja. Se onkin tietoturvallisuuden kehittämisessä keskeinen käsite, samoin kuin sen sukulaiskäsite uhka. Nämä käsitteet on helppo yhdistää arkielämän tilanteisiin, esimerkiksi kysytään mikä hanketta uhkaa tai mitkä ovat hankkeen riskitekijät. (Messier, 2019)

Tietoturvallisuuden kannalta uhka on jokin taho, toimija, laite tai muu sellainen, jolla on mahdollisuus murtaa tiedon luottamuksellisuus, eheys tai saatavuus. Murtamisessa hyödynnettävää tietojärjestelmän heikkoa piirrettä kutsutaan haavoittuvuudeksi (engl. vulnerability). Uhka ei kuitenkaan

välttämättä ole jokin ulkopuolinen pahantahoinen toimija, vaan uhkan voi muodostaa esimerkiksi huono toimintatapa tai vaikkapa vanhentuneet laitteet. (Messier, 2019) Esimerkiksi eräässä kone-salissa oli kulkuväylällä valokatkaisijan vieressä kytkin, jolla pystyi vaihtamaan konesalin palvelin-ten virransyötön ulkoverkosta akkujen varaan. Kävi niin, että eräs henkilö oli vahingossa, pois läh-tiessään kääntänyt väärästä kytkimestä. Kytkimen vahinkokäytöstä seurasi se, että akkuvirran lo-puttua palvelimet sammuiivat tai tekivät häilytyksiä valvomoon. Tämä kytkin suojattiin myöhemmin kotelolla.

Dictionary.com esittää, että riski on altistumista mahdolliseen vahingoittumiseen tai menetykseen. Riskin mahdollisuus on todennäköisyyttä, joka on mitattava käsite. Samoin vahingoittuminen tai menetys ovat mitattavia. Näin ollen riskiin liittyy lukuarvoja, eikä riskin siis tarvitse olla muodotonta, epäselvää tai häilyvää. (Messier, 2019)

TODENNÄKÖISYYS

Arkikielessä sanaa riski saatetaan käyttää virheellisesti, kun itse asiassa tarkoitetaan mahdolli-suutta tai todennäköisyyttä. Todennäköisyys voidaan määrittää, kun on tarpeeksi tietoa. Esimer-kiksi voidaan määrittää todennäköisyys, kuinka monta perjantaita osuu kuukauden 13. päivälle al-kavan vuoden aikana. Tässä esimerkissä tulos on tarkastikin määritettävissä.

Tietoturvallisuuden kohdalla todennäköisyyden määrittäminen on vaikeampaa. Mikä on hajautetun denial of service -hyökkäyksen todennäköisyys tietyn yrityksen kohdalla? Impreva Incapsula- tie-toturvayhtiön laskurilla saadaan tulos, jonka mukaan 2500 työntekijän internetkaupparyityksen to-dennäköisyys joutua DDoS-hyökkäyksen kohteeksi on 36 prosenttia. Mitä tällainen prosenttiluku tarkoittaa? Estyykö 36 % kaupanteosta DDoS-hyökkäysten vuoksi? Todennäköisyyksien laskemi-nen tietoturvallisuuden kohdalla on vaikeaa, ja vaikka laskenta onnistuisi, niin tulosten ymmärtämi-nen voi olla haastavaa.

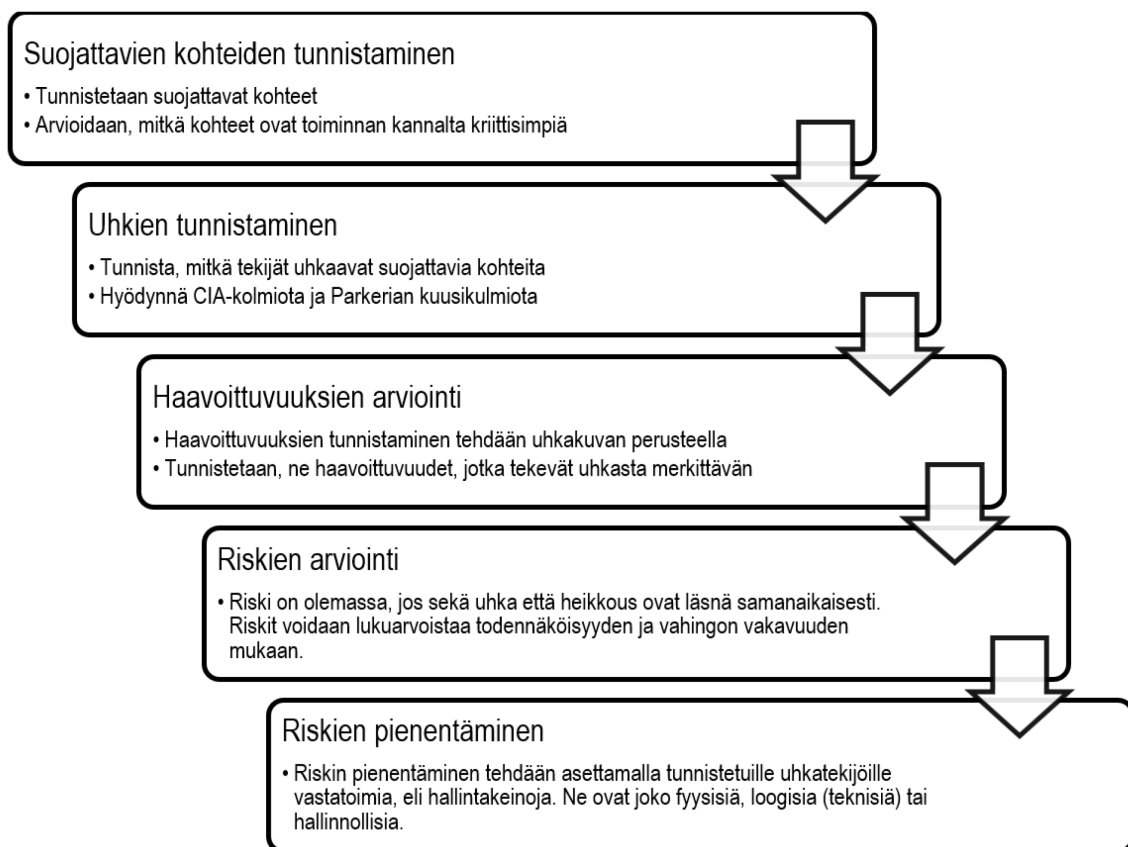
VAHINKO, MENETYS

Vahingon, haitan tai menetyksen (engl. loss) määrittäminen on helpompaa, joskin ei täysin ongel-matonta. Esimerkiksi, jos yrityksen tietoturva on pettänyt, ja liikesalaisuuksia on vuotanut, niin mikä on konkreettinen menetys, kun yrityksellä kuitenkin edelleen on hallinnassaan nämä tiedot. Mene-tyksen suuruus tai vahingon vakavuus riippuu siitä, mikä taho tiedot anasti ja mihin tarkoitukseen se niitä käyttää.

Kun sekä todennäköisyys että vahingon vakavuus on arvioitu, voidaan määrittää riski. Riski on todennäköisyyden ja vahingon tulo. Riskiä voi siis vähentää sekä todennäköisyyden, että vahingon vakavuuden kautta. *"Riski = todennäköisyys x vahingon vakavuus"* Todennäköisyys tässä riskin laskennassa tarkoittaa tietyn uhkan todennäköisyyttä. Vahingon vakavuus on arvio siitä, kuinka pahoin jokin haavoittuvuus voi aiheuttaa vahinkoa. (Messier, 2019)

2.5 Riskien hallintaprosessi ja häiriöiden hallinta

Riskien hallintaprosessi on yksi keskeinen elementti Valtiovarainministeriön Digitaalinen turvallisuus -mallissa (kappale 2.1). Riskien hallintaprosessin tavoitteena on systemaattisesti ja aktiivisesti suojata toiminnalle tärkeitä voimavaroja, tietoja ja tiedonkäsittelyjärjestelmiä ja pienentää riskejä liiketoiminnan tarpeiden mukaisesti (KUVIO 4).



KUVIO 4 Riskien hallintaprosessi. (Mukaillen Andress, 2019)

Prosessi lähtee liikkeelle suojattavien kohteiden tunnistamisesta painottaen toiminnan kannalta tärkeimpiä kohteita. Kun suojattavat kohteet on tunnistettu, tehdään selvitys, millaisia uhkatekijöitä

näihin liittyy. Tässä voidaan hyödyntää esimerkiksi edellä esiteltyjä CIA- ja Parkerian Hexad -mal-
leja. Uhkatekijöiden tunnistamisen ja muodostuneen uhkakuvan perusteella selvitetään, mitä heik-
kouksia tai haavoittuvuuksia suojattaviin kohteisiin liittyy. Selvityksessä korostetaan haavoittuvuu-
ksia, jotka tekevät uhkasta merkittävän.

Messierin (2019) mukaan riski on olemassa, jos sekä uhka että haavoittuvuus ovat läsnä saman-
aikaisesti. Riskeistä muodostetaan mitattavia suureita antamalla todennäköisyydelle ja vahingon
vakavuudelle lukuarvoja. Riskien pienentäminen kohdistetaan ensin suurimpiin riskeihin, eli niihin,
jotka ovat todennäköisimpiä ja aiheuttavat vakavimpia vahinkoja. Tietoturvallisuuden riskejä pie-
nennetään asettamalla uhkatekijöille vastatoimia eli hallintakeinoja (engl. controls). Tavoitteena on
pienentää riski hyväksyttävälle tasolle. Prosessin tuotoksena muotoutuu ns. jäännösriski (engl. re-
sidual risk), eli hallittu riskitaso, jonka organisaatio on valmis hyväksymään.

Fyysiset hallintakeinot suojaavat fyysisistä ympäristöä, johon tietojärjestelmät sijoittuvat tai jossa tie-
dot sijaitsevat. Tilojen pääsynhallinta, aidat, portit, lukot, järjestysmiehet ja valvontakamerat ovat
esimerkkejä fyysisistä hallintakeinoista.

Loogiset hallintakeinot eli tekniset hallintakeinot suojaavat järjestelmiä, tietoverkkoja ja ympäristöjä,
jotka käsittelevät, lähettävät ja säilyttävät tietoa. Esimerkkeinä mainittakoon salasanat, salaus, pää-
syn hallinta, palomuurit ja hyökkäyksen tunnistamisen järjestelmät. Loogiset hallintakeinot estävät
luvattomat tietojen käsittelytoimet.

Hallinnolliset hallintakeinot ovat sääntöjä, lakeja, politiikkoja, käytäntöjä, ohjeistuksia ja muita asi-
oita, joita voidaan kuvata tekstimuotoon. Hallinnollisilla hallintakeinoilla määrätään, kuinka käyttä-
jien tulee toimia ympäristössä.

(Andress, 2019)

HÄIRIÖN HALLITA

Vaikka riskien pienentämiseksi asetetaan erilaisia hallintakeinoja, on tarpeen varustautua tilantei-
siin, että jokin tunnistettu tai aikaisemmin tunnistamaton riski silti toteutuu. Häiriön hallinta (tai on-
gelman hallinta) on pääosin reagointia toteutuneeseen riskiin. Osana riskienhallintaprosessia on
varmaankin jo tunnistettu organisaation tärkeimmät suojattavat kohteet, joihin häiriönhallintapro-
sessin tulisi ensisijaisesti kohdistua. Hyvän suunnittelun tuloksena organisaatiolla tulisi olla suun-
nitelmat häiriötilanteiden varalle. Kriittisten kohteiden osalta häiriönhallinnan suunnitelmat tulee
säännöllisesti katselmoida, testata ja harjoitella.

Häiriönhallintaprosessin osa-alueita ylätasolla ovat

- varautuminen (engl. preparation, contingency planning)
- tunnistaminen ja analysointi (engl. detection and analysis)
- rajaaminen (engl. containment)
- puhdistaminen (engl. eradication)
- palauttaminen (engl. recovery)
- jälkitoimet (post incident activity).

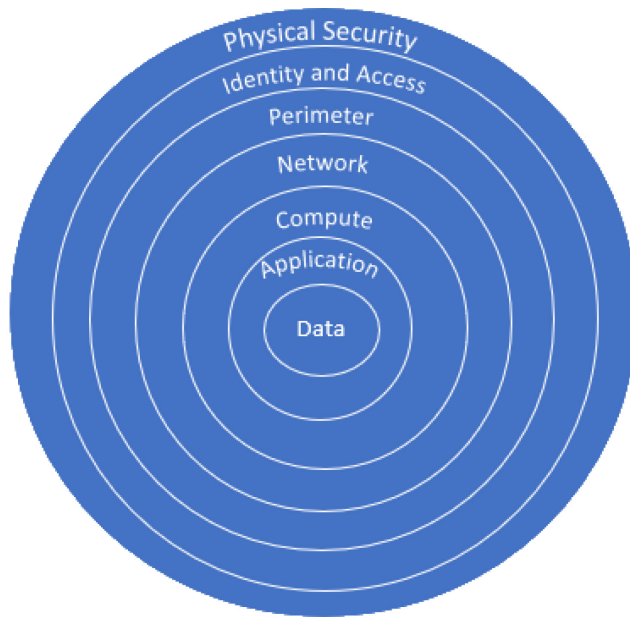
Varautuminen on toimi, joka tulee tehdä ennen häiriön tapahtumista. Se sisältää hallinnollisia toimia, häiriönhallinnan prosessien koulutusta ja harjoittelua sekä teknisiä toimia, jotka auttavat häiriön poistamisessa. Tavoitteena on, että organisaatio on valmiina toimimaan, kun häiriö tapahtuu. Muut häiriönhallinnan prosessivaiheet ovat yhtä tärkeitä kuin varautuminen, mutta ne jätetään tässä kuvaamatta, koska ne löytyvät Andressin kirjasta.

(Andress, 2019)

Valtiovarainministeriön digitaalinen turvallisuus -mallissa (kappale 2.1) edellä kuvattua häiriön hallintaa lähinnä vastaavat käsitteet ovat jatkuvuuden hallinta ja varautuminen. Mallin mukaan jatkuvuuden hallinta on *"organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa"* ja varautuminen puolestaan on *"toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa"*. (Valtiovarainministeriö, 2020)

DEFENSE IN DEPTH

Syvyysuuntainen turvallisuussuunnittelu, eli englanniksi Defense of Depth (Sanastokeskus, 2018) on pitkään käytössä ollut sotavoimien lanseeraama malli, jossa kohdetta suojataan kerroksittain. Tavoitteena on, että suojauskerrosten läpi tunkeutuminen hidastaa hyökkäyksen etenemistä ja antaa aikaa tunnistaa hyökkäys ennen vahinkojen syntymistä. Yksittäisen kerroksen pettäessä suojaus edelleen toimii. Mallia sovelletaan edelleen, esimerkiksi kyberturvallisuuden kohdalla suojattava kohde on yleensä data eli tiedot. (KUVIO 5),



KUVIO 5 Defense in depth (Speedos Blog, 2022)

Suojauksia ja valvontaa toteutetaan eri kerroksiin, joita ovat lähteestä riippuen esimerkiksi sovellus, laskentakapasiteetti, tietoliikenne, toimialue, tunnistaminen ja pääsynhallinta sekä fyysinen turvallisuus. Kuhunkin kerrokseen kuuluu turvallisuuden hallintakeinoja ja suojausmenetelmiä. Tapahtumalokit ja valvonta mahdollistavat häiriön tunnistamisen ja vastatoimien asettamisen. (Microsoft, 2022r, Gates, S. 2019)

2.6 Lakien ja määräysten noudattaminen

Vaatimustenmukaisuus jakautuu kahteen osaan, lakien ja säännösten noudattamiseen ja teollisuusstandardien vaatimustenmukaisuuteen. Tässä kappaleessa käsitellään Suomessa voimassa olevia tietoturvallisuutta ja tietojen käsittelyyn liittyviä lakeja ja säädöksiä.

Suomessa julkisia sosiaalipalveluja ja terveystalvveluja, niiden tuottamista ja tietojen käsittelyä koskevat sekä toimialariippumattomat yleislait, että toimialakohtaiset erityislait. Lakien soveltamisessa erityislailia on määräävämpi asema kuin yleislailia. Euroopan Unionin lainsäädännössä General Data Protection Regulation (GDPR) asettaa yksittäiselle henkilölle oikeuden pyytää henkilötietojensa poistoa tietojärjestelmistä. (gdpr.eu 2022). Tämän lainsäädännön edelle menee kuitenkin sosiaali- ja terveydenhuollon erityislait, jotka määrittelevät mm. tiettyjen potilastietojen osalta tietojen poistamiseen rajoituksia tai kieltoja. Perusteluina on mm. potilaan hoidon jatkuvuuden ja turvallisuuden varmistaminen.

Suomessa on voimassa erityinen tietosuojalaki (Tietosuojalaki, 5.12.2018/1050), joka tarkentaa GDPR:n säännöksiä henkilötietojen käsittelystä. Julkisia organisaatioita sitoo myös ns. tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta, 906/2019), joka ohjaa viranomaisten tiedonkäsittelyä yhdenmukaiseen ja tietoturvalliseen käsittelyyn. Sote-toimialan erityislainsäädäntönä mainitakoon laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021), joka ohjaa nimenomaan sosiaali- ja terveydenhuollon asiakastietojen ja asiakkaan itsensä tuottamien hyvinvointitietojen tietoturvallista käsittelyä ja sisältää vaatimuksia tietojärjestelmille ja niiden valmistajille sekä sosiaali- ja terveydenhuollon palvelun antajille. Yksityiskohtaiset olennaiset vaatimukset tietojärjestelmille annetaan Terveyden ja hyvinvoinnin laitoksen määräyksissä. (Terveyden ja hyvinvoinnin laitos, 2022)

Valvira on sosiaali- ja terveysalan lupa- ja valvontavirasto, joka valvoo mm. sosiaali- ja terveydenhuollon toiminnan asianmukaisuutta. Se kuvaa tehtäväänsä seuraavasti: *"Valvira valvoo sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettujen tietojärjestelmien olennaisen vaatimusten toteutumista. Tietojärjestelmällä tarkoitetaan sosiaali- tai terveydenhuollon asiakastietojen sähköistä käsittelyä varten toteutettua ohjelmistoa tai järjestelmää, jonka avulla tallennetaan ja ylläpidetään asiakas- tai potilasasiakirjoja ja niissä olevia tietoja. Tietojärjestelmän tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuoja sekä toiminnallisuutta koskevat olennaiset vaatimukset, ennen kuin sen saa ottaa käyttöön. Tietojärjestelmän valmistaja on vastuussa vaatimustenmukaisuuden osoittamisesta."* (Sosiaali- ja terveysalan lupa- ja valvontavirasto, 2022)

Edellä mainittujen lakien lisäksi on myös monia muita lakeja ja säädöksiä, jotka asettavat vaatimuksia tietojärjestelmien kehittämiselle. Näistä löytyy lisätietoa sosiaali- ja terveysministeriön julkaisusta Lainsäädäntö ohjaa asiakas- ja potilastietojen hallintaa (Sosiaali- ja terveysministeriö, 2022).

Tiedon sisältö vaikuttaa Suomessa olevan lainsäädännön mukaan siihen, miten, missä ja kuka voi käsitellä, siirtää tai säilyttää tietoa. Aina ei ole tarjolla täysin selkeitä tapauskohtaisia ohjeita, vaan on tehtävä tietoturvallisuuden arviointiin perustuvia päätöksiä. Tietoa luokitellaan sisältöön perustuvan suojausvaatimusten perusteella esimerkiksi pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) mukaan luokkiin julkinen, salassa pidettävä, henkilötieto, varautumisen näkökulmasta suojattavat tiedot ja turvallisuusluokitellut IV-luokan salassa pidettävät tiedot. PiTuKri-arviointikriteeristö esitellään seuraavassa osiossa.

2.7 Tietoturvallisuuden arvioinnin kriteeristöt

Lakien ja asetusten noudattamisen osoittamiseksi ja oman toiminnan tietoturvallisuuden varmistamiseksi organisaatiot voivat hyödyntää yleisesti käytössä olevia viitekehyksiä tai arviointikriteeristöjä. Lait eivät välttämättä vaadi tällaista käytäntöä, mutta useilla toimialoilla on liiketoiminnalle eduksi – tai jopa välttämätöntä mukautua tällaisin normeihin.

Viitekehyksiä voidaan hyödyntää tietoturvallisuuden kehittämisessä ja arvioinnissa. Arvioinnin vahvistamiseksi organisaatio tai rajattu tietojärjestelmäkokonaisuus voidaan sertifioida tiettyä kriteeristöä vastaan. Esimerkiksi Kyberturvallisuuskeskuksen hyväksymät tietoturvallisuuden arviointilaitokset ovat kirjoittamishetkellä Nixu Certification Oy, KPMG IT Sertifiointi Oy ja Inspecta Sertifiointi Oy. (Kyberturvallisuuskeskus, 2022). Erityisesti valtiohallinnon turvaluokiteltua tietoa käsittelevät järjestelmät tulee sertifioida. Lisäksi Kansallisen potilastiedon arkistoon (Kanta) liittyvät tietojärjestelmät tulee sertifioida. (Valvira, 2022) Sertifiointia ei kuitenkaan vaadita kaikkien toimijoiden tai tietojärjestelmien kohdalla, mutta kriteeristöjä voidaan silti hyödyntää hyvän tietoturvallisuuden osoittamisessa ja kehittämisessä.

ISO 27000 -SARJA

”Tietoturvallisuuden johtamisjärjestelmällä organisaatiosi suojaa tieto-omaisuuttaan. Tietoturvallisuuden johtamisjärjestelmän rakentamisessa tukena on standardisarja ISO/IEC 27000, joka tarjoaa suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin.”

ISO 27001

”Tässä tietoturvallisuuden hallintajärjestelmän päästandardissa esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Standardi sisältää myös organisaation tarpeisiin mukautettua tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset. Vaatimukset ovat yleisluonteisia ja ne soveltuvat kaikentyyppisille ja -kokoisille organisaatioille.”

ISO 27002

”Standardi on tarkoitettu käytettäväksi standardiin ISO/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toteuttamisprosessissa. Se sopii myös ohjeistukseksi yleisesti hyväksyttyjen tietoturvallisuuden hallintakeinojen toteuttamiseen.”

Standardia voidaan hyödyntää toimiala- tai organisaatiokohtaisten tietoturvallisuuden hallintaohjeiden kehittämisessä, sillä siinä otetaan huomioon toimialaa tai organisaatiota koskevat tietoturvallisuuden riskiympäristöt.”

(Suomen standardisoimisliitto, 2022)

KATAKRI

Ulkoministeriö, joka toimii kansallisena turvallisuusviranomaisena (National Security Authority, NSA) on tuottanut viranomaisia varten laaditun Katakriin – tietoturvallisuuden auditointityökalun.

”Katakri on viranomaisten auditointityökalu, jota viranomainen voi käyttää arvioidessaan kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa.

Katakria voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjä yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä.”

(Valtiovarainministeriö, 2020a)

PITUKRI – PILVIPALVELUIDEN TURVALLISUUDEN ARVIOINTIKRITEERISTÖ

PiTuKri on Kyberturvallisuuskeskuksen julkaisema erityisesti pilvipalveluiden tietoturvallisuuden arviointia varten laadittu arviointikriteeristö. Sitä vastaan ei tällä hetkellä ole mahdollista sertifioitua, mutta se perustuu pitkälti edellä kuvattuun Katakri -kriteeristöön, jota vastaan tehdään sertifiointeja. PiTuKria hyödynnetään Pata-järjestelmän itsearvioinnissa. Tarkempi kuvaus PiTuKrista ja itsearvioinnin toteuttamisesta on esitelty luvussa 4 Tietoturvallisuuden itsearviointi.

”Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. Kriteeristö on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Kriteeristö on laadittu Suomen kansallisten tarpeiden näkökulmasta. Laadinnassa on hyödynnetty erityisesti BSI:n pilviturvallisuuskriteeristöä, CSA-pilviturvallisuusyhteisön sujausmatriisia, ISO27001 – ja ISO27017 -standardeja, sekä Katakri-kriteeristöä” (Kyberturvallisuuskeskus, 2019)

2.8 Julkisen pilvipalvelun erityispiirteet

Dotsonin (2019) mukaan käsite julkinen pilvipalvelu tarkoittaa, että palvelu on yleisön saavutettavissa, eli käytännössä se sijaitsee internetissä ja on kenen tahansa hankittavissa. Pilvipalvelut ovat yleistyneet viime vuosina nopeasti. Sosiaali- ja terveydenhuolto eivät ole ihan kärkisijoilla tämän uuden teknologian omaksumisessa, sillä tietosuoja ja tietoturvaluus herättävät paljon kysymyksiä. Tosiasia on, että rikollisuus pyrkii hyödyntämään julkisessa pilvipalvelussa olevia tietoja omaan tarkoitukseensa. Helposti voi myös ajatella, että internetissä 'mikään ei ole turvassa'. Seuraavassa esitellään joitakin tietoturvaluuden kannalta merkittäviä pilvipalvelujen ominaisuuksia. Tarkastelun lähtökohtana on, että pilvipalvelualustaa hyödynnetään sekä tietojärjestelmän kehittämiseen että palvelutuotantoon. Pilvipalveluihin liitetään myös käsitteet ketteryys (engl. agility), skaalautuvuus (engl. scalability) ja elastisuus (engl. elasticity). Pilvipalvelut tuovat ohjelmistokehitykseen, testaukseen ja julkaisuun ketteryttä. Pilvipalvelun skaalautuvuus parantaa saatavuutta, kun pilvikapasiteettia voidaan tarpeen mukaan lisätä. Ketteryttä, skaalautuvuutta ja elastisuutta ei tässä tämän enempää käsitellä. (GeeksforGeeks, 2022)

ITSEPALVELU

Yleisesti käytössä olevat pilvipalvelut toimivat itsepalveluperiaatteella. Karheasti ajatellen toimintamalli on sama kuin nettikaupassa. Asiakas valitsee haluamansa tuotteet tai tilaukset ja maksaa niistä. Microsoftin pilvipalveluissa käytetäänkin käsitettä tilaus, jota esitellään tarkemmin kappaleessa 3.1 sivulla 31. Pilvipalvelun käyttöönotossa vaaditaan ymmärrettävästi paljon enemmän teknistä osaamista kuin nettiososten tekemisessä. Hyvä pilvipalvelualusta on tuotteistettu pitkälle, siten että asiakkaan käyttökokemus ja saavutettava hyöty ovat korkealla tasolla. Pilvipalvelualustan hyödyntäminen vaatii saman tyyppistä teknistä erityisosaamista kuin konesalissa tuotettavien palvelujen suunnittelu ja toteuttaminen vaativat. Vaikka pilvipalvelun tarjoajalla onkin paljon vastuuta tietoturvaluudesta, niin myös asiakkaan tulee kyetä huolehtimaan turvaluudesta omalta osaltaan.

PILVEN TOTEUTUSTAPA

Tyypillisiä pilvipalvelun toteutustapoja ovat yksityinen pilvi (private cloud), yhdistelmäpilvi (hybrid cloud) ja julkinen pilvi (public cloud). Toteutustavan valintaa ohjaa usein tietoturvaluuteen liittyvät

kysymykset. Vahvasti suojatusta konesalista toteutettu yksityinen pilvi voi tarjota esimerkiksi tietoturvaluokitellun tiedon käsittelyyn vaaditun turvatason. Julkinen pilvi on saatavuutensa, joustavuutensa ja kustannustasonsa puolesta saanut vahvan markkina-aseman. Yhdistelmäpilvi on palvelukokonaisuus, joka sisältää yksityisen ja julkisen pilven toimintoja, joihin tietojen käsittely jaotetaan esimerkiksi tiedon tietoturva vaatimusten mukaan. Muita toteutusmalleja ovat esimerkiksi eri toimijoista koostuvan yhteisön yhteisöpilvet (community/government cloud). Tässä työssä tarkastellaan lähinnä julkisia pilvipalveluja, joiden tuottajina käytännössä ovat monikansalliset yksityiset toimijat. (NIST, 2011 ja Kyberturvallisuuskeskus, 2019)

FYYSINEN SIJAINTI

Pilvipalvelun tuottaja tarjoaa palvelua konesaleistaan. Asiakas ei pääse vaikuttamaan konesalien sijaintiin eikä fyysisten palvelinten konfiguraatioon, ainakaan julkisen pilvipalvelun osalta. Pilvipalvelun tarjoaja voi tarjota palvelua tietyistä maista tai alueista. Esimerkiksi Pata-järjestelmä hyödyntää Microsoftin pilvipalveluja alueista North Europe ja West Europe. North Europe datakeskus sijaitsee Irlannissa ja West Europe datakeskus sijaitsee Hollannissa.

ZERO TRUST

Nollaluottamus, (engl. Zero Trust) on strategia tai malli, joka auttaa yrityksiä toteuttamaan turvallisia tietojenkäsittelyratkaisuja modernissa ympäristössä. Salo (2022) kuvaa sitä näin: *”Zero Trust eli ”luottamattomuuden periaate” on kehitetty modernien ja ketterästi kehittyvien ICT-ympäristöjen suunnitteluun. Se auttaa rakentamaan tietoturvaa nykypäivän monimutkaisessa maailmassa, jossa eri ICT-järjestelmät integroituvat toisiinsa. Zero Trust -mallin perustana on nimensä mukaisesti, että luottamus on nolla kaikilla ajan hetkillä. Laitteet ja käyttäjät tunnistetaan kaikissa tilanteissa ja päättös pääsyn sallimisesta perustuu riskiarvioon. Vahvan tunnistautumisen käyttö on yksi perusasioita.”*

Mallissa on kolme keskeistä periaatetta. Käyttäjän varmistaminen periaate, vähimpien oikeuksien periaate ja se, että oletetaan aina pahinta.

Käyttäjän varmistaminen tarkoittaa moneen lähteeseen perustavaa tunnistamista ja valtuuttamista. Lähteitä ovat esimerkiksi käyttäjän identiteetti ja sijainti, laitteen luotettavuus. Tulee myös selvittää onko käyttötapahtumaan liittyviä epäilyttäviä poikkeamia tai epäsäännöllisyyksiä. Vähimpien oi-

keuksien periaate on kuvattu seuraavassa kappaleessa. Se, että oletetaan pahinta, on ajattelu-malli, joka auttaa rajaamaan vahinkoja suojausten pettäessä. Vahingon laajuus voidaan rajata esi-merkiksi segmentoinnin tai muun hallintakeinon avulla. (Microsoft, 2022t)

VÄHIMPIEN OIKEUKSIEN PERIAATE

Usein organisaatiossa tarkasti rajattu joukko, jolla on valtuudet hallita koko pilviympäristöä. Pää-synhallinnassa on yleisesti käytössä vähimpien oikeuksien periaate, jonka mukaan käyttövaltuuk-sia annetaan mahdollisimman vähän (engl. least privilege) tietyn tehtävän tai roolin suoritta-miseksi.

Pilviympäristön voi olla jaettu usean hankkeen kesken ja ympäristön sisällä voi olla monia kehitys- ja tuotantoympäristöjä, jotka tulee erottaa toisistaan mm. ohjelmistojen, konfiguraation, tietojen ja käyttövaltuuksien osalta. Luvussa 3 esitellään Pata-järjestelmän pilviympäristöä ja vähimpien oi-keuksien periaatteen mukaista toteutusta.

TUNNISTAMINEN, KÄYTTÖVALTUUDET JA VALVONTA

Parkerian Hexadin (KUVIO 3 sivulla 15) käsite todentaminen on erittäin keskeistä julkisten pilvipal-velujen kohdalla, koska ympäristö - internet on lähtökohtaisesti vihamielinen. Tyypillisesti pilvipal-velujen kaikkia hallintatoimia ja kaikkea tiedon käsittelyä valvotaan. Hallintatoimia voivat suorittaa vain tunnistetut henkilöt tai ohjelmistot, joilla on toimenpiteen vaatimat käyttövaltuudet. Vastaavasti sovellusten loppukäyttäjien kirjautumiset ja tiedon käsittely yleensä kirjataan lokiin.

Microsoftin tunnistamista koskevat ominaisuudet noudattavat osaltaan edellä kuvattua Zero Trust -strategiaa. Pilvipalveluissa voi olla hyvin edistyneitä tietoturvallisuutta lisääviä valvontatoimia, ku-ten tekoälypohjainen käyttäjän kirjautumisen sijainnin seuranta. Järjestelmä voi tarvittaessa estää normaalia poikkeavan kirjautumisen. (Conditional Access, Microsoft, 2022k)

DISASTER RECOVERY

Julkisten pilvipalvelujen, ja varsinkin palvelun tarjoajan hallinnoimien PaaS ja SaaS -palvelujen ominaisuuksiin voi kuulua tietojen palauttamismahdollisuus. Palauttaminen voidaan kohdistaa ha-luttuun ajankohtaan historiassa. Palautushistorian pituus vaihtelee palvelukohtaisesti. Esimerkiksi Azure SQL Database on Microsoftin hallinnoima relaatiotietokanta, jossa on valmiina kahdentami-sen ja palauttamisen ominaisuudet. (Microsoft, 2022s)

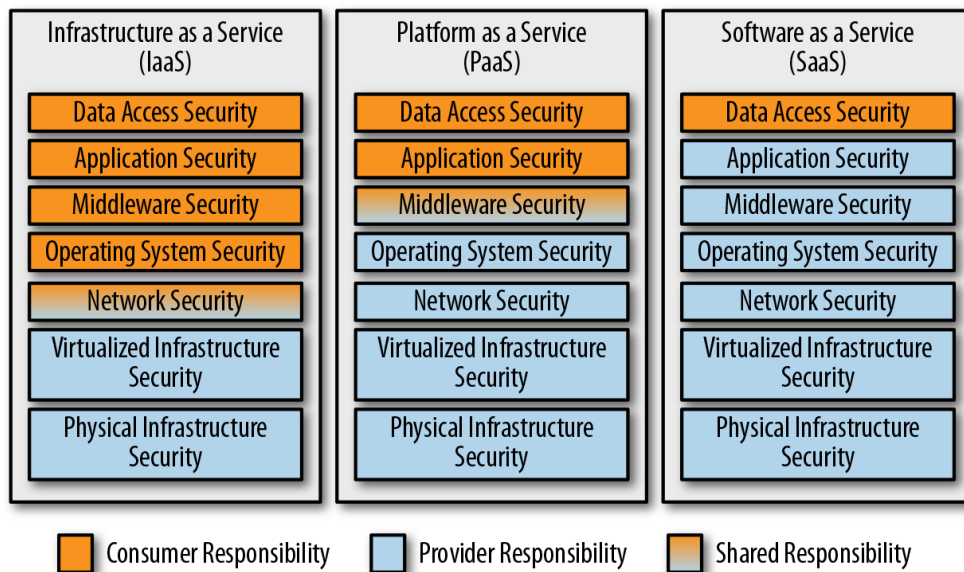
PILVEN PALVELUMALLIT

Pilvipalvelujen hahmottamiseen on vakiintunut termit IaaS, PaaS ja SaaS. Infrastructure as a Service (IaaS) tarkoittaa perusteknologian tasoita pilvipalvelua, jossa pilvipalvelualusta tarjoaa kone-salin omaiset palvelut kuten tietoliikenteen ja virtuaalipalvelimen. Platform as a Service (PaaS) tarkoittaa pilvipalvelua, jossa palveluntarjoaja vastaa laajemmin teknisestä toteutuksesta. Esimerkiksi tarjolla voi olla valmiita helposti käyttöön otettavia tietokantoja tai ohjelmiston suoritussympäristöjä. SaaS on korkean tason pilvipalvelu, jossa asiakas saa käyttöönsä kehittyneitä ohjelmistopalveluita. Tässä opinnäytetyössä, kappaleessa 3.2 sivulla 35 esitellään Microsoftin Power Platform, joka on SaaS pilvipalvelu. Tällainen luokittelu ei kuitenkaan ole tietoturvallisuuden arvioinnissa oikea lähestymistapa, koska luokittelujen rajat ovat sumentuneet ajan saatossa. Tärkeämpää on tunnistaa, mitä palvelussa on ja mitä siinä ei ole. Vaikka Power Platform sisältää pitkälti valmiita ratkaisuja, on siinä myös ohjelmiston kehittämisvälineet. On siis syytä tuntea, mitä toimintoja pilvipalvelu tarjoaa, miten sitä käytetään ja miten tietoturvallisuuden vastuut jakautuvat.

JAETUN VASTUUN MALLI PILVESSÄ

On tärkeää tunnistaa, mistä osasta tietoturvallisuutta asiakas on itse vastuussa. Tässä pilvipalvelu eroaa olennaisesti konesalipalvelusta. Varsinkin, jos ajatellaan organisaation itse hallinnoimaa konesalia, ovat palvelujen ja tietoliikenteen turvallisuus kokonaan omalla vastuulla. Organisaation oman konesaliympäristön IT-palveluja on perinteisesti voitu hallita sisäisin sopimuksien ja käytäntöiden kautta. Liiketoiminta on tottunut asettamaan IT-ympäristöä koskevia teknisiä vaatimuksia sovelluspalvelujen tuottamiseksi, luottaen, että tietoturvallisuudesta on huolehdittu.

Pilviympäristössä ei aina ole kovin selkeää, mihin pilvipalveluympäristön tarjoajan vastuu loppuu, ja mistä alkaa asiakkaan vastuu. Rajanveto asiakkaan ja pilven tarjoajan vastuiden välillä riippuu siitä, millaisia pilvipalveluja käytetään. KUVIO 6 havainnollistaa edellä kuvattuja palvelumalleja ja sitä, kuinka IaaS palvelun asiakkaalla on huomattavasti enemmän vastuuta kuin esimerkiksi SaaS-palvelun asiakkaalla.



KUVIO 6 Tietoturvallisuuden vastuunjako pilvipalveluissa (Dotson, C. 2019)

Pilvipalvelun tarjoajalla on täysi vastuu fyysisen infrastruktuurin turvallisuudesta ja virtualisoitujen ympäristöjen turvallisuudesta, sisältäen usein edistyneitä hallintakeinoja, joihin ei yritysten tietoturvaosaaminen tai -resursointi riitä. Virtuaalipalvelimien ajo IaaS-ympäristössä tuo hyvin esiin tietoturvallisuuden jaetun vastuun. Pilvipalvelun tarjoajan vastuulla on, että ulkoinen tietoliikenne ja ympäristö, jossa virtuaalipalvelin sijaitsee, on turvattu. IaaS-palvelujen asiakas on vastuussa virtuaalipalvelimeen asennetun tietoliikenteen ja ohjelmiston tietoturvallisuudesta, mukaan lukien käyttöjärjestelmän tietoturvapäivitykset.

SaaS ja PaaS -palvelumalleissa asiakkaan on pystyttävä luottamaan pilvipalvelun tarjoajaan yhä laajemmin, koska se vastaa tietoturvan teknisistä ratkaisuista valtaosin. Asian voi nähdä etuna, kun rahaa vastaan saadaan tasokas, hallittu alustapalvelu, jossa tietoturvallisuudesta huolehditaan ammattimaisesti. Pata-järjestelmän hyödyntämiä pilvipalveluita ja vastuunjakoa havainnollistaa KUVIO 10 sivulla 33.

SOPIMUKSELLINEN NÄKÖKULMA

Koska julkisten pilvipalvelujen tarjoajat ovat usein suuria monikansallisia yrityksiä, ei yksittäisellä asiakkaalla tai organisaatiolla ole mahdollisuutta asettaa IT-ympäristön vaatimuksia, vaan palvelun tarjoaja sanelee palvelun ominaisuudet ja ehdot. Asiakkaan rooliksi jää hyväksyä tai olla hyväksymättä palvelusopimukset. Tämä koskee myös monia tietoturvallisuutta koskevia ratkaisuja.

3 PATA-JÄRJESTELMÄ

Tämä opinnäytetyö on osa 2M-IT:n hanketta, jossa kehitetään tehokasta tiedonkäsittelyratkaisua monikanavaisen asiakasohjaustiimin käyttöön. Perusajatuksena on, että kansalainen voi joustavasti ottaa yhteyttä sosiaali- ja terveydenhuollon palveluihin ja että asiakasta palvelevilla sote-ammattihenkilöillä on tehokkaat välineet tiedon löytämiseen ja asiakkaan ohjaamiseen. Pata-asiakasohjauksen toimintamallissa asiakaspalvelija on keskiössä oheisen kuvion esittämällä tavalla (KUVIO 7). Asiakasohjauksen palveluita ovat esimerkiksi sosiaalipalvelujen neuvonta ja ohjaus sekä terveydenhuollon neuvonta ja hoidon tarpeen arviointi. Joustavuutta saavutetaan, kun asiakasohjauksen keskittäminen mahdollistaa pidemmät palveluajat. Joustavuus tarkoittaa myös sitä, että monipuolinen valikoima yhteydenottotapoja.



KUVIO 7 Pata-toimintamalli ylätasolla (2M-IT)

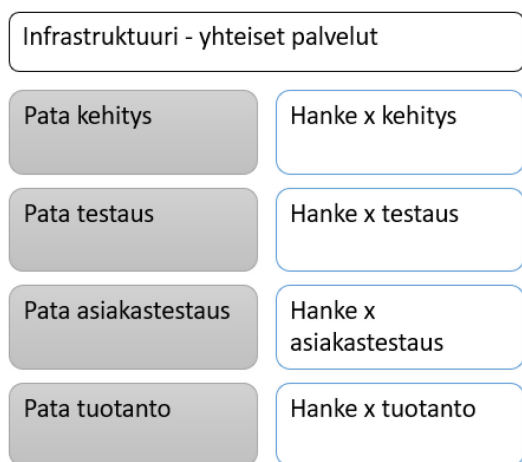
Perinteisen puhelinsoiton lisäksi asiakas voi saada apua chatbotilta ja käydä chat- tai videokeskustelua asiakaspalvelijan kanssa. Opinnäytetyön valmistuessa oli osa toiminnoista jo saavuttanut tuotantovalmiuden ketterän kehittämistyön jatkuessa edelleen. Tässä kappaleessa esitellään Pata-järjestelmä toiminnan, teknologian ja kehittämisprosessin näkökulmasta. Järjestelmän kuvaamisessa painotetaan tietoturvallisuuden kannalta merkityksellisiä näkökohtia.

3.1 Tenantin rakenne ja yhteiset peruspalvelut - infrastruktuuri

Englannin kielen sana tenant tarkoittaa yleiskielessä vuokralaista. Pilvipalvelujen yhteydessä tenant, tai suomalaisittain tenantti tarkoittaa asiakkaan valitsemaa palvelua ja sijaintia, joka sisältää pilvipalveluja tuottavat palvelimet. Esimerkiksi Pata-järjestelmän tenantti sijaitsee EU:n alueella, North Europe ja West Europe alueilla. Azure-tenantin merkittävä piirre on, että tenantissa on yksi asiakkaan käyttäjät ja käyttäjäryhmät sisältävä Azure Active Directory -identiteetinhallintapalvelu. (Microsoft, 2021e). 2M-IT on hankkinut palvelutuotantoa varten tenantin, jossa myös Pata-järjestelmää kehitetään ja tuotetaan. Tätä tenanttia kutsutaan jatkossa palvelutenantiksi.

Palvelutenantti sisältää yhteisten palvelujen tilauksen (engl. subscription) lisäksi järjestelmä- ja hankekohtaisia tilauksia (KUVIO 8). Tilaus on käsite johon (muutaman muun Azure-käsitteen ohella) kohdistetaan tenantissa käyttöönotetut palvelut, käyttöoikeudet, resurssit ja niiden kulut. Tilaus mahdollistaa käyttöoikeuksien rajaamisen. Esimerkiksi Global Administrator voi hallita koko Azure-ympäristön kaikkia tilauksia, kun taas Pata-hankkeessa toimiva Azure Contributor voi hallita yhden tilauksen resursseja, eikä voi myöntää oikeuksia toisille käyttäjille. (Microsoft, 2021q)

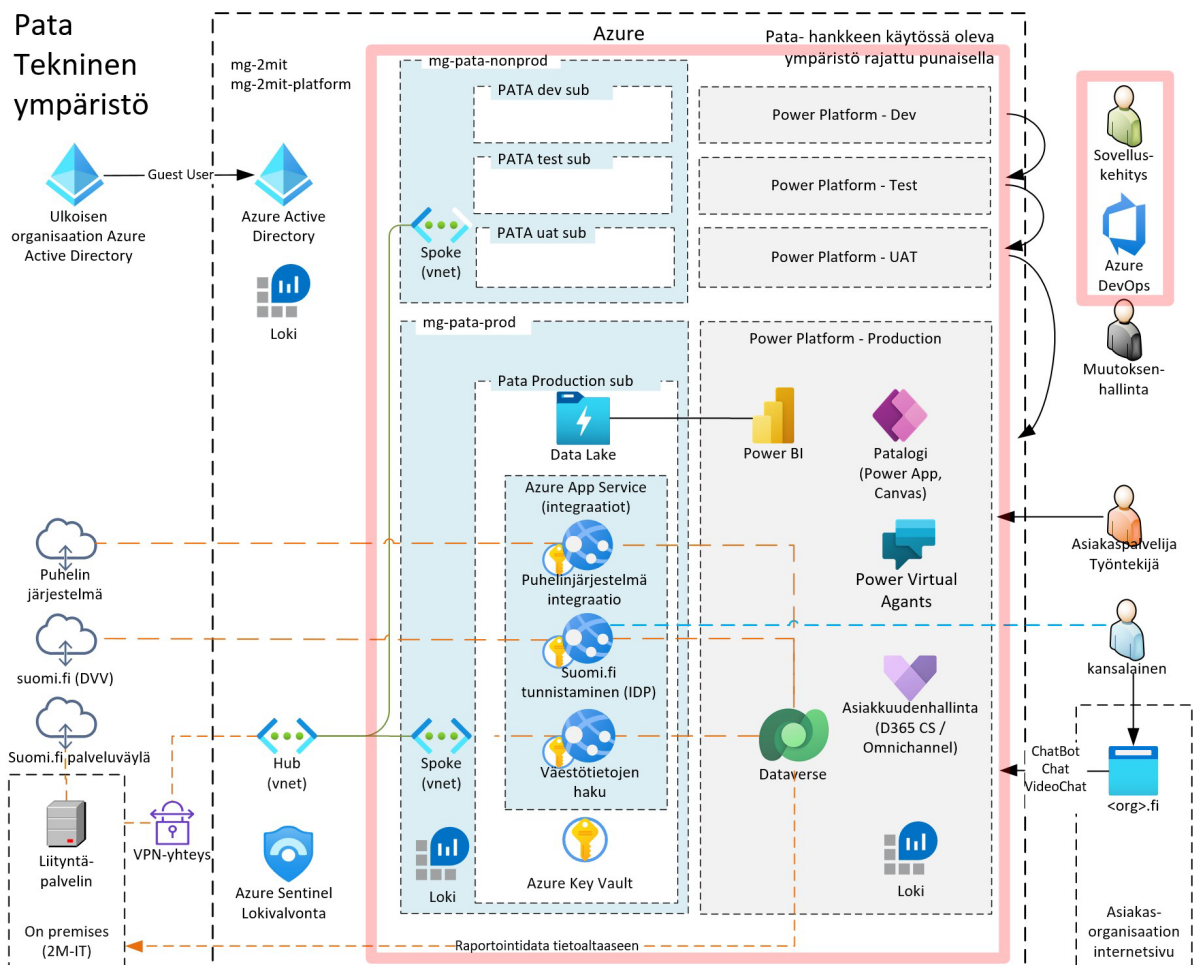
Yhteisten palvelujen tilaukseen on konfiguroitu lukuisia 'peruspalveluita', joiden voidaan ajatella vastaavan perinteisen konesalin infrastruktuuria. 2M-IT:n konfiguroimat tenantin peruspalvelut tarjoavat tietoturvallisen ympäristön eri hankkeiden käyttöön sisältäen esimerkiksi käyttäjähallinnan ja tietoliikenteen organisaatiokohtaiset käytännöt ja koventamiset.



KUVIO 8 Palvelutenantissa sijaitsevat Azure-tilaukset, mahdollistavat useiden eri hankkeiden ja käyttövaltuuksien hallinnan.

Pata-järjestelmää varten on konfiguroitu neljä eri ympäristöä. Tenantissa on myös muita asiakas-järjestelmiä tai hankkeita. 2M-IT:n organisaatiossa tietoturvallisuuden vastuu jakautuu yhteisistä palveluista vastaavan tekniikkaosaston ja ohjelmistoa kehittävän hankkeen kesken.

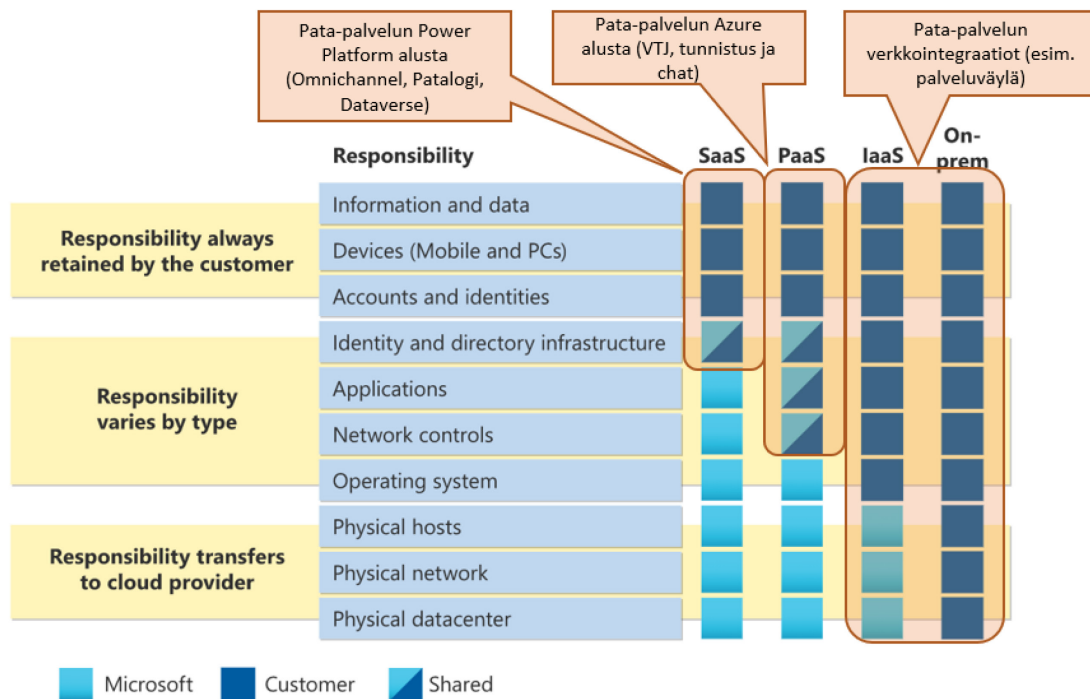
Pata-järjestelmän tekninen ympäristö (KUVIO 9) koostuu Azure ja Power Platform -ympäristöistä, joita on käytössä kehitys-, testaus, asiakastestaus- ja tuotantokäyttöä varten. Pata-kehityshankkeen hallinnassa oleva osuus on ympäröity leveällä punaisella viivalla. Tämän viivan ulkopuolella ovat yhteiset palvelut, kuten identiteettihallinta, tietoliikenne sekä ohjelmistokehityksen prosessit.



KUVIO 9 Pata-järjestelmän tekninen ympäristö

Azuren DevOps-ohjelmisto tarjoaa ketterän ohjelmistokehittämisen välineet vaatimusmäärittelyyn, laadunvarmistukseen, ohjelmiston julkaisuun ja lähdekoodin hallintaan. Ohjelmistokehityksen ja julkaisuprosessin hallinnassa käytetään DevOps-palvelua (Microsoft, 2022a). Azure-palvelujen hyödyntämistä Pata-järjestelmän toimintojen näkökulmasta havainnollistaa KUVIO 10. Power Platform, Omnichannel ja Dataverse ovat SaaS palveluja. Integraatiot ovat

pääosin Azure App Serviceä hyödyntäviä PaaS toteutuksia. Tietoliikenneyhteyksiä on toteutettu IaaS- ja konesalitekniikalla.



KUVIO 10 Pata-järjestelmä hyödyntää pääosin PaaS ja SaaS mallin pilvipalveluja (Microsoft 2022j, mukaillen)

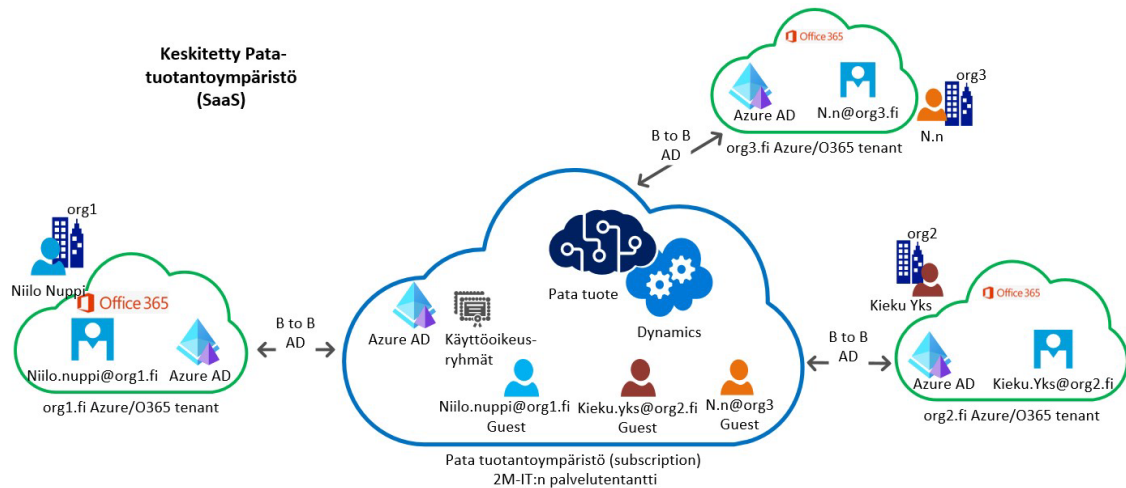
Seuraavassa esitellään muutamia palvelutenantin yhteisen alueen palveluita, jotka Pata-järjestelmä vaatii toimiakseen, ja joita 2M-IT:n organisaatiossa vain rajatulla joukolla on valtuudet hallita.

IDENTITEETINHALLINTA

Pilvipalvelussa identiteetinhallinta ja tunnistaminen ovat erittäin kriittisiä toimintoja, jopa vielä kriittisempiä kuin konesalissa tapahtuva identiteetin hallinta, koska internetissä sijaitseva palvelu on ehdottomasti suojattava ulkopuolisilta. Pilvipalvelujen piirteisiin kuuluu myös se, että kaikki tiedonkäsittely tapahtuu tunnistetusti ja että tietojen käsittely- ja valvontatapahtumat kirjataan lokiin.

Azure Active Directory (AAD) on Microsoftin identiteetinhallintapalvelu, joka perustetaan osana Azure-tenantin käyttöönottoa. Keskeisiä toimintoja ovat käyttäjätilin hallinta, tunnistaminen, valtuuksien hallinta, suojaus ja valvonta. AAD hallinnoi sekä järjestelmänvalvojien että sovelluskäyttäjien identiteettejä, tunnistamista ja käyttäjäryhmiin kuulumista. AAD kommunikoi toisen organisaation tenantissa sijaitsevan AADn kanssa, jolloin voidaan hyödyntää toisen organisaation työntekijöiden käyttäjätunnuksia. AAD hallinnoi myös ohjelmistoille asetettuja käyttöoikeusidentiteettejä

(Service Principal). Käyttöoikeuksia hallitaan AAD:n käyttäjäryhmien kautta. Identiteetinhallintaa kuvataan Pata-järjestelmän osalta tarkemmin tietoturvallisuuden arvioinnin yhteydessä kohdassa 4.7 Identiteetin ja pääsyn hallinta. (Microsoft, 2021f) Pata-tuotantoympäristö on määritelty siten, että se palvelee useita organisaatioita samanaikaisesti. (KUVIO 11). Pata-järjestelmän toteutuksessa Power Platformin Dataverse-tietovarannon ominaisuudet tukevat asiakaskohtaisen tiedon hallintaa. Tätä on selvitetty tarkemmin kohdassa Power Platform - Dataverse, sivulla 36.



KUVIO 11 Keskitetty Pata-tuotantoympäristö sijaitsee palvelutenantissa ja palvelee samanaikaisesti useita organisaatioita. Ulkopuolisen organisaation työntekijöiden tunnukset kutsutaan tuotantoympäristöön ns. vieraskäyttäjiksi (engl. Guest User)

TIETOLIIKENNE

Azure-pilvessä sekä Azuren ja 2M-IT:n konesalin välille rakennettu tietoverkkoratkaisu koostuu osittain Azuren virtuaalisista tietoliikenneresursseista ja osittain 2M-IT:n konesaliympäristön fyysisistä laitteista. Tietoliikenteen pääpiirteet on esitetty graafisesti sivulla 32, KUVIO 9 Pata-järjestelmän tekninen ympäristö. Tietoliikenteen ratkaisuja on käsitelty tarkemmin Pata-järjestelmän tietoturvallisuuden arvioinnissa kohdassa 4.6 Tietoliikenneturvallisuus.

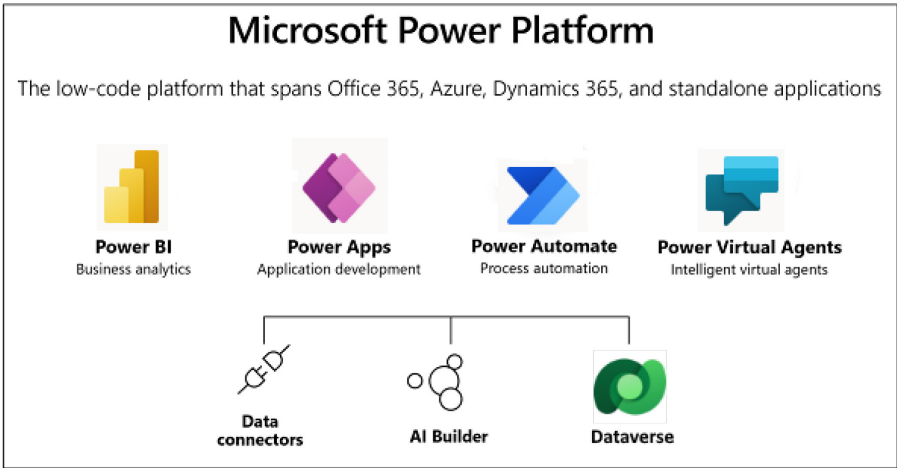
VALVONTA

2M-IT valvoo Azure-pilvipalvelua keskitetysti mm. Azuren Sentinel-palvelun avulla, johon kootaan valvonnan kannalta keskeiset tiedot. Valvontaa suoritetaan monella tasolla, esimerkiksi tietoliikenteessä, integraatioiden suorittamisessa, hallintatoimissa ja tiedon ylläpidossa. Osa valvontatiedoista ja lokeista muodostuu automaattisesti Azuren PaaS ja SaaS palvelujen tuottamana, kun taas joihinkin järjestelmäosiin pitää toteuttaa asiakaskohtaisia auditointiominaisuuksia esimerkiksi lain

tai ulkoisen integroitavan järjestelmän vaatimusten vuoksi. (Microsoft, 2022b) Valvonnan ja auditoinnin toteuttaminen on sekä sovelluskehityksen, että tenantin yhteisten palvelujen vastuulla.

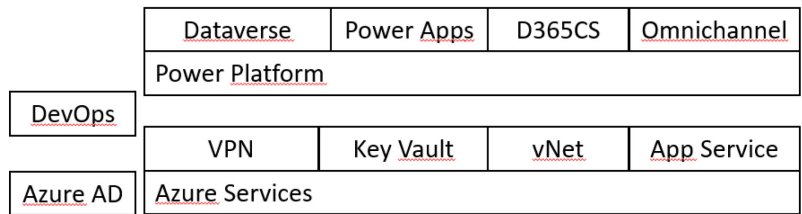
3.2 Power Platform

Pata-järjestelmässä hyödynnetään Microsoftin SaaS tason alustapalvelukokonaisuutta eli Power Platformia, jonka sisältämät Dynamics 365 Customer Service ja sen lisäosa Omnichannel olivat perusteena Power Platformin käyttöönotolle. Se sisältää välineet Dynamics 365 ja Power Apps kehittämiseen. Tämän lisäksi Power Platform sisältää mm. Microsoftin toteuttamat rajapintapalvelut ja tietoturvallisuuden hallinnan. (KUVIO 12)



KUVIO 12 Microsoft Power Platform (Microsoft 22e)

Power Platformissa voi olla useita ympäristöjä samaan tapaan kuin Azuressa voi olla useita tilauksia. Power Platform hyödyntää useita Azuren palveluita, kuten Azure AD identiteetinhallintaa. KUVIO 13 havainnollistaa Power Platformin suhdetta muihin Microsoftin pilvipalveluihin.

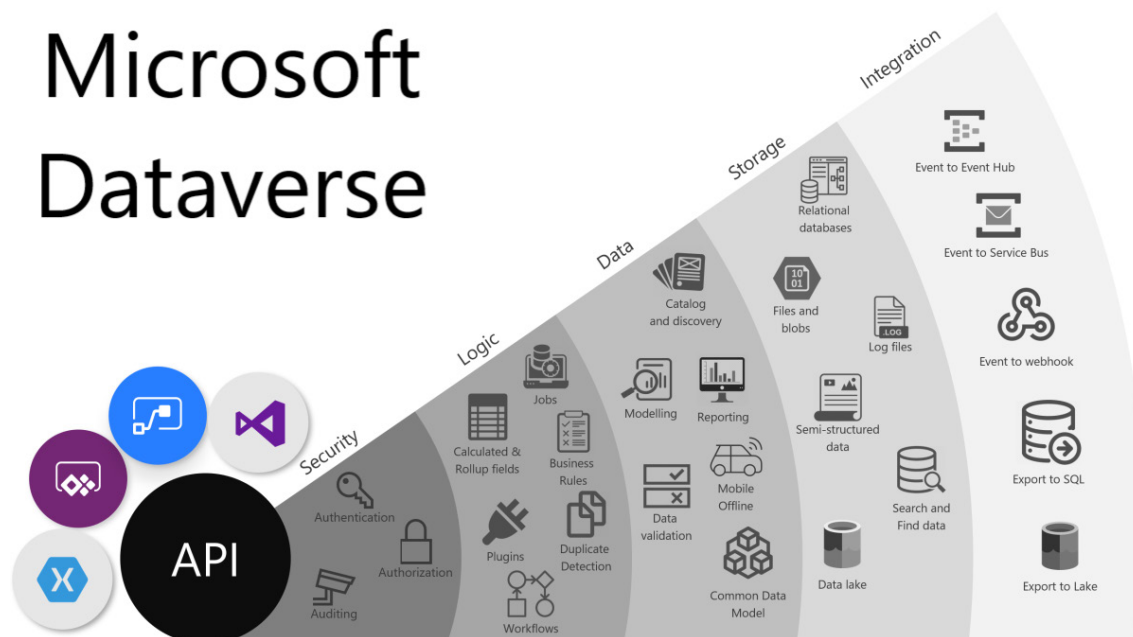


KUVIO 13 Pata-järjestelmä hyödyntää Microsoftin Azure ja Power Platform -teknologioita.

On kuitenkin hyvä tunnistaa, että Power Platform on oma kokonaisuutensa, joka kommunikoi internetin yli Azuren palvelujen kanssa. Power Platformia hyödynnettäessä ei näin ollen ole mahdollista reitittää tietoliikennettä esimerkiksi Azure-virtuaaliverkkojen kautta.

POWER PLATFORM - DATAVERSE

Power Platformin tietovaranto Dataverse on tietoturvan kannalta keskiössä. Se tarjoaa laajamittaisesti eri kyvykkyyksiä turvalliseen tietojen käsittelyyn. Dataverse hyödyntää Azure Active Directoryn tunnistautumista sekä henkilöille että palveluille, ja näihin perustuu valtuuttaminen kaikkiin Dataversen rajapintoihin ja prosesseihin. Se mahdollistaa tietojen turvallisen käsittelyn ja myös joustavan Power Apps -ohjelmistokehityksen. KUVIO 14 esittää Dataversen arkkitehtuurin.



KUVIO 14 Microsoft Dataverse arkkitehtuuri (Microsoft 2022e)

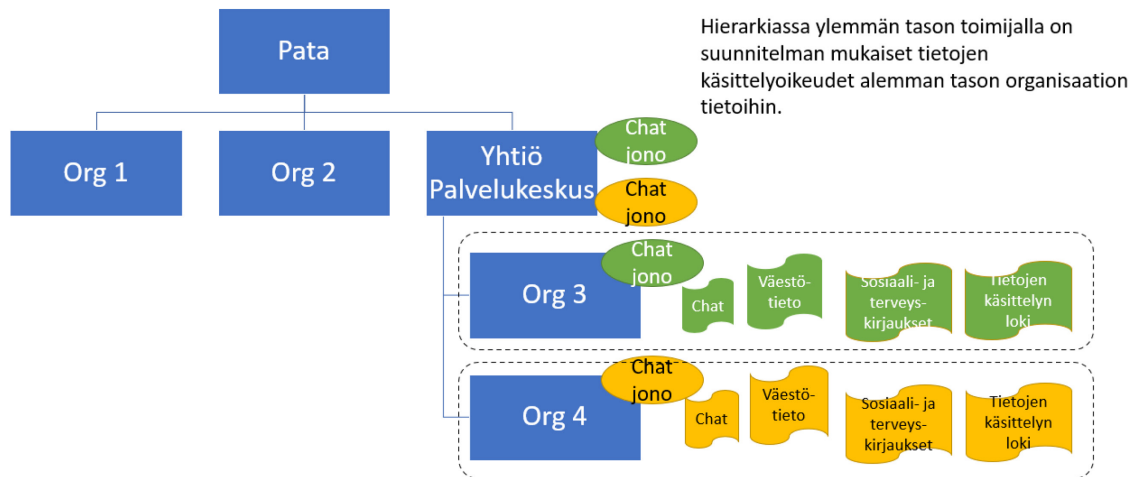
Dataversen keskeiset ominaisuudet ovat roolipohjaisuus, liiketoimintayksiköt ja hierarkkinen dataan pääsyn hallinta:

Roolipohjaisuus

Tietojen käsittelyoikeus on roolipohjainen (security role). Azure AD:n tunnistetut käyttäjät tai käyttäjäryhmät liitetään rooleihin.

Liiketoimintayksiköt

Liiketoimintayksiköt (KUVIO 15) tuovat rakenteen organisaatiokohtaisen tiedon hallintaan. Pata-palvelussa liiketoimintayksiköt ovat käytännössä rekisterinpitäjiä tai heidän valtuuttamia toimijoita.



KUVIO 15 Organisaatioiden tietoja hallitaan Dataversen Business Unit -käsitteen avulla

Hierarkkinen dataan pääsyn hallintarakenne

Tietojen käsittelyoikeutta voidaan rakenteistaa hierarkkisesti, siten että liiketoimintayksiköillä on hierarkkiset suhteet keskenään. Tämä mahdollistaa Pata-palvelun tuottamisen usealle asiakkaalle yhdestä tuotantoympäristöstä. (Rybaric, R. 2020)

3.3 Dynamics 365 Customer Service ja Omnichannel

Dynamics 365 Customer Service (D365CS) on asiakaspalvelutyöhön tarkoitettu Microsoftin asiakkuudenhallintatuote. Se hyödyntää Power Platformin sisäistä tietovarantoa Dataverseä. Näin D365CS:n käsittelemät tiedot ovat myös low-code tekniikalla tehtyjen Power Appsien käytettävissä. D365CS on tuote, jonka periaatteessa voi ottaa käyttöön sellaisenaan, mutta käytännössä aina tehdään asiakaskohtaisia muokkauksia. (Microsoft, 2022l). Omnichannel on laajennus D365CS-ohjelmaan. Se lisää kokonaisuuteen mm. chat ja videopuhelu -ominaisuudet. (Microsoft, 2022m)

Pata-järjestelmän kohdalla Dynamics 365 ja Omnichannel palveluita on mukautettu. Esimerkiksi työnkulkua, asiakkaan tunnistamista, väestötiedon käyttöä asiakkuuden hallinnassa, yhteydenoton syyn kirjaamista ja hoidon tarpeen arvioinnin prosessia on muutettu. Muutokset ovat kohdistuneet sekä käyttöliittymään, että Dataverse-tietovarantoon.

3.4 Tietoarkkitehtuuri

Asiakasohjausprosessissa syntyy tietoja yhteyden ottajasta, asiointikanavasta, palvelun tarpeesta ja suoritetusta ohjaustoimenpiteestä. Asiakasohjausta varten on rakennettu tietosisältöjä palvelupaikoista, palveluista ja palveluun pääsemisen kriteereistä. Alla olevassa taulukossa on ryhmitelty keskeisiä tietosisältöjä. (TAULUKKO 1)

TAULUKKO 1 Pata-tietosisällöt

Tietoryhmä	Lisätietoja
Väestötieto	Pata hakee väestötietoja Digi- ja väestötietoviraston (DVV) muutosrajapinta-palvelusta. Tieto siirretään suomi.fi palveluväylän kautta 2M-IT:n konesaliin, josta se edelleen, ilman välitallennusta siirretään VPN-yhden kautta Microsoft Azureen / Dataverse-tietovarantoon. Väestötietoa koostuu järjestelmään myös asiakkaan tunnistautuessa suomi.fi -palvelua vastaan chat-kanavassa.
Terveystieto	Asiakkaan / yhteydenottajan terveysongelmaan liittyvät tiedot.
Sosiaalipalvelujen tieto	Asiakkaan / yhteydenottajan terveysongelmaan liittyvät tiedot.
Chat/chatbot	Anonyymin tai tunnistetun asiakkaan kanssa käytyjä chat-keskusteluja.
Raportointi	Raportointitiedot tuotetaan Azuren ja Dataversen sisällöistä. Tietoja voidaan kopioida teknisen rajapinnan kautta rekisterinpitäjän tai muun toimijan järjestelmään.
Tuotannonohjaus	Sosiaali- ja terveydenhuollon palvelut, palvelupaikat, ratkaisupankin tiedot ja palvelujen poikkeustiedot.
Suoritetieto	Työn suorittamiseen liittyvää tietoa, johon liittyy henkilökuntaa koskevaa henkilötietoa.
Lokitieto	Eri yhteyksissä syntyvää lokitietoa. Microsoft Power Platformin tarjoamat auditointiominaisuudet eivät sellaisenaan riitä.

Lainsäädäntö asettaa sääntöjä tiedon ja lokien säilyttämiseen erityisesti sosiaali- ja terveystiedon ja väestötiedon osalta. Tästä johtuen tietojen käsittely, siirtäminen ja säilyttäminen on rajattu EU:n alueelle. Tietojen keskeinen säilytyspaikka on Microsoft Power Platformin Dataverse, joka on kuvattu kohdassa Power Platform - Dataverse, sivulla 36.

3.5 Järjestelmän toiminnot

Asiakasta palvelevalle henkilöstölle, joita ovat sairaanhoitajat ja sosiaalityöntekijät, tarjotaan tehokkaita ratkaisutiedon löytämiseen ja käsittelyyn. Oheinen KUVIO 16 esittää mustalla pohjalla Pata-tietojärjestelmän keskeiset toiminnot, jotka rakentuvat Microsoft Dynamics 365 Customer Service -käyttöliittymään eheäksi käyttökokemukseksi. Vihreällä pohjalla on prosessiin liittyviä järjestelmiä, kuten puhelinjärjestelmä sekä sosiaalihuollon asiakastietojärjestelmä (ATJ) ja terveydenhuollon potilastietojärjestelmä (PTJ).



KUVIO 16 Pata-järjestelmän toiminnot

Pata-järjestelmän komponentit voidaan ryhmitellä alustateknologiaan, sovellustoimintoihin, integraatioon ja sovelluskäyttöön liittyviksi. Sovelluskehityksen kannalta keskeisimmät alustan komponentit ovat Microsoft D365 Customer Service, Omnichannel, Power Apps, Dataverse, PowerBI sekä Azuren tarjoamat komponentit, kuten Azure App Service. (TAULUKKO 2)

Asiakkuuden hallinta, asiakaspalvelun ohjaus ja raportointi ovat Dynamics-ratkaisun keskeisiä ominaisuuksia. Tähän integroidaan väestötietojärjestelmä ja suomi.fi tunnistaminen. Asiakkaan yhteydenotossa käytetään monikanavaisen palvelun mahdollistavaa Omnichannel-laajennusosaa, joka tarjoaa chatbot, chat ja videoyhteysskanavat. Myöhemmässä vaiheessa Omnichanneliin voidaan liittää myös äänipuhelut, jolloin erillistä puhelinjärjestelmää ei tarvita. Palvelukatalogi ja ratkaisupankki tarjoavat sosiaali- ja terveydenhuollon palvelutietoja ja ohjauksessa tarvittavia ohjeita. Hoidon tarpeen arviointi (HTA) moduuli auttaa asiakaspalvelijaa tekemään nopean, yhteismitallisen hoidon tarpeen arvioinnin.

TAULUKKO 2 Pata-järjestelmän teknologiat ja komponentit

Komponentti	Tarkoitus	Lisätietoja
Microsoft Dynamics 365 Customer Service ja OmniChannel, Chat/ChatBot	alustateknologia	Power Platform
Microsoft Power Apps	alustateknologia	Power Platform
Microsoft Dataverse	alustateknologia	Power Platform tietojen käsittelypalvelu/tietovaranto.
Microsoft Azure (PaaS, IaaS)	alustateknologia	mm. integraatiot täällä
Pata – asiakkuudenhallinta (CRM)	sovellustoiminto	Hyödyntää D365 ja OmniChannel
Patalogi / PatalogiPro	sovellustoiminto	Palvelutietojen hallinta, Power Platform
HTA	sovellustoiminto	Hoidon tarpeen arviointi, Power Platform
Raportointi	sovellustoiminto	Power BI
Yhteydenottajan tunnistaminen	integraatio	DVV palvelu
Väestötietojen haku	integraatio	DVV palvelu, suomi.fi palveluväylä, liityntäpalvelin
Puhelinjärjestelmän integraatio	integraatio	
Sovelluskäyttö	työpöytä /selainkäyttö	Verkkoselain, Edge, Chrome (ei IE).
ChatBot, Chat, Videochat (yhteydenottaja)	Kansalainen ottaa yhteyttä web-selaimella	Verkkoselain
Tukipalvelut	työpöytä/selainkäyttö	Verkkoselain

3.6 SaaS-palvelujen edut ja haasteet - Power Platform

Pata-järjestelmän kannalta keskeinen Power Platform tarjoaa ohjelmistokehityksen käyttöön hyvin toteutetun ja suojatun tietokannan ja low-code ohjelmistokehitysvälineet. Dynamics 365 on myös osa Power Platformia. Pitkälle viedyt SaaS palvelut siirtävät monet tietoturvallisuuden huolenaiheet ja vastuut Microsoftille. Näin sovelluskehityksessä, Power Appsien tekemisessä ja Dynamics 365:n mukauttamisessa voidaan pääosin keskittyä toiminnallisuuksien toteuttamiseen. Kappaleessa 3.2 Power Platform kuvataan Power Platformin ominaisuuksia tarkemmin.

MUUTOSTEN HALLINNAN HAASTEET

Käytännössä Power Platformin tarjoamat palvelut ovat ohjelmia, joita Microsoftin monet tuotetiimit koodaavat ja julkaisevat tuotantoversioina. Pata-kehittämisen, n. 9 kuukauden aikana on havaittu useita kertoja, että ympäristöön on tullut yllättäviä muutoksia. Power Platformiin on toki tullut hyviä uudistuksia, mutta valitettavasti myös yllättäviä epäjohtonmukaisuuksia tai odottamattomia muutoksia toimintalogiikkaan. Näiden seurauksena asiakkaat ovat saaneet yllättäviä ja myös negatiivisia kokemuksia. Useampaan kertaan on tuotekehitystiimin täytynyt käydä korjaamassa Microsoftin tuotejulkaisun aiheuttamien muutosten seuraamuksia. Ongelman tekee kiusalliseksi se, että Microsoftin uusia julkaisuja ei pystytä testaamaan etukäteen, vaikka Pata-järjestelmässä on erilliset testausympäristöt (KUVIO 9, sivu 32), sillä versiojulkaisut kohdistuvat samanaikaisesti kaikkiin Pata-ympäristöihin (kehitys, testaus, asiakastestaus ja tuotanto).

Microsoft toki dokumentoi uusien julkaisujen ominaisuudet. (Microsoft, 2022r). Vaikuttaa kuitenkin siltä, että Power Platformia kehittävät tuotetiimit julkaisevat osia hiukan hiomattomina, jolloin Microsoft palvelujen kesken syntyy epäjohtonmukaisuuksia tai ne eivät vastaa dokumentaatiota. Koska muutostahti on kova, ei Power Platformin päälle rakennettua ohjelmistoa voi jättää kovin pitkään oman onnensa nojaan, vaan on aktiivisesti seurattava, että Microsoftin julkaisemat muutokset eivät ainakaan riko sovellusta.

Korkean tason SaaS palvelujen, kuten Power Platformin tuotteiden hyödyntäminen tuo ohjelmistokehitykseen nopeutta, mutta esimerkiksi Pata-järjestelmä lähestyy kipukynnystä, jossa alemman tason kehitysvälineillä toteuttamalla, ottamalla itse laajempi vastuu ohjelmiston toteuttamisesta, alkaa näyttämään muutoshallinnan kannalta houkuttelevalta vaihtoehdolta. On tosin huomioitava, että alemman tason alustapalveluihin perustuva ohjelmistokehitys voi olla merkittävästi hitaampaa.

OHJELMISTOKEHITYSPROSESSIN KOVENTAMINEN

Microsoft Azuren ja Power Platformin muodostama kokonaisuus on verrattain monimutkainen. Tämän rinnalla, ohjelmistokehityksen automaatiossa hyödynnettävä Microsoft DevOps (esitelty kirjassa 3.1) tuo omat haasteensa. Tietoturvallisuuden kannalta Microsoftin DevOps, jonka kautta tuodaan uusia ohjelmistoja tuotantoon, voi sisältää uhkatekijöitä. Eräs tunnistettu uhka liittyy siihen, että ulkopuolinen taho voisi tuoda haitallista lähdekoodia osaksi ohjelmistoversiota. On siis huolehdittava myös DevOps järjestelmän suojauksista siten, että automatisoitu prosessi on hallittu ja kaikki toimijat prosessissa tunnistetaan ja valtuutetaan asianmukaisesti. DevOps järjestelmän kohdalla tietoturallinen tunnistaminen ja valtuutus tehdään ohjelmistoon liitetävän identiteetin, eli

Azure Service Principalin ja siihen liittyvän hallintaprosessin avulla. Noudattamalla Zero Trust -turvallisuusstrategiaa saavutetaan korkea suojaustaso ohjelmistokehityksen ja lähdekoodin hallinnan prosesseissa (Microsoft, 2022i)

4 TIETOTURVALLISUUDEN ITSEARVIOINTI

Pata-järjestelmän tietoturvallisuuden itsearviointi suoritettiin opinnäytetyön käytännön harjoituksena. Työn tavoitteenahan oli tukea Pata-järjestelmän tietoturvallista kehittämistä. Arviointi toteutettiin PiTuKri – pilvipalveluiden tietoturvallisuuden arviointikriteeristöä vasten. Kyberturvallisuuskeskuksen (2019a) mukaan ”*Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. Kriteeristö on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Kriteeristö on laadittu Suomen kansallisten tarpeiden näkökulmasta.*”

Kriteeristö sisältää kaksi dokumenttia. Tekstiosa sisältää johdantoa pilvipalvelujen tietoturvallisuuden, käyttöohjeet, aihepiirikohtaiset vaatimukset ja esimerkkejä soveltamisesta (Kyberturvallisuuskeskus, 2019a). Arvioinnin tueksi on saatavilla Excel-arviointityökalu, joka tukee systemaattista arvioinnin suorittamista (Kyberturvallisuuskeskus, 2019b). Itsearviointi suoritettiin arviointityökalua hyödyntäen. Tuloksia ei tässä käydä systemaattisesti läpi kohta kohdalta koska ne eivät ole julkisia. Itsearvioinnin tukena käytettiin Microsoftin hiljattain teettämän Azure tietoturva-auditoinnin tuloksia (Microsoft, 2022h).

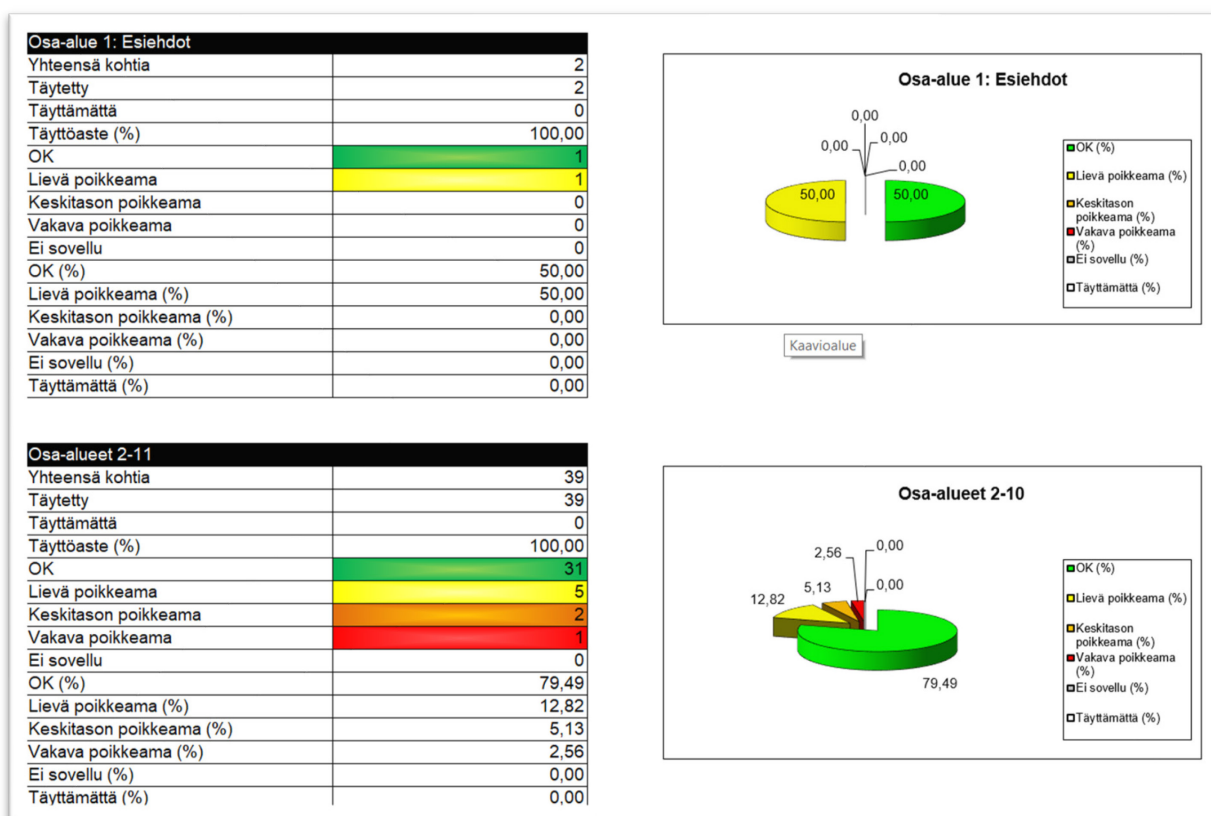
Arvioinnit tehdään Excel-työkalun välilehdille Esiehdot ja Osa-alueet 2-11. Kullakin osa-alueilla on useita kysymyksiä. Arvioinnin tulos tulee merkitä työkalun vaatimusrivin neljanteen sarakkeeseen teksteillä, joiden tulee olla täsmälleen oikein kirjoitettu. Tekstit ovat Ei sovellu, OK, Lievä poikkeama, Keskitason poikkeama ja Vakava poikkeama (KUVIO 17).

Vaatimus	Tietotyyppi	Kuvaus vaatimusten	Arviointitulos	Kommentit
Osa-alue 9: Käyttöturvallisuus				
KT-01 - Järjestelmäkuvauksen jatkuvuuden ja käytettävyyden tukemiseksi				
1) Pilvipalvelusta on kattavat järjestelmäkuvaukset sekä ohjeet palvelun turvalliseen ylläpitoon ja hallintaan. Kuvaukset ja ohjeistukset ovat sellaisella tasolla, että niiden avulla pystytään uskottavasti välttämään käytön aikaiset virheet sekä varmistumaan sopimusvelvoitteiden mukainen palautuminen häiriötilanteista.	Salassa pidettävä, henkilötiedot	esimerkki --- esimerkki dokumentaatio abc Microsoft dokumentaatio	Lievä poikkeama	VASTUU: Jaettu
2) Järjestelmäkuvaukset ja ohjeet pidetään ajan tasalla.		Lievä poikkeama esimerkki		
3) Järjestelmäkuvaukset ja ohjeet ovat henkilöstölle jalkautettuna ja saatavilla roolien mukaisesti.				
KT-02 - Suorituskyvyn hallinta				
1) Pilvipalvelun suorituskyky (kapasiteetti) mitoitetaan siten, että palvelutasosopimusten mukainen palvelutaso pystytään luotettavasti tarjoamaan. Mitoitukseen on sisällyttävä toteutuneen suorituskykytarpeen seuranta sekä tulevien suorituskykytarpeiden ennusteet.	Salassa pidettävä, henkilötiedot	Esimerkki - tietoturvallisuuskuvaus Dokumentti xxx Microsoft dokumentaatio	OK	VASTUU: Pilvipalvelun tarjoaja 2M-IT:n asiakasorganisaatiot rajattu ulos.
2) Pilvipalveluntarjoajan on mahdollistettava asiakkaalle annettujen järjestelmäresurssien (esim. tietojenkäsittely- tai tallennuskapasiteetin) käytön seuranta.				
KT-03 - Varmistus- ja palautusprosessit				
1) Varmistus- ja palautusprosessit on suunniteltu, toteutettu, testattu ja kuvattu osana jatkuvuussuunnitelmaa siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin. Ennustettavasti huomioitava:	1-2: Salassa pidettävä, henkilötiedot 3: TL IV & KV-R, TL III (kasauma)	Idk jffafalo jd lakjd fladf oaldfola sj Vakava poikkeama elka di aoldjfasdjfla djfolafl dj	Vakava poikkeama	VASTUU: 1: Jaettu 2 a-c jaettu 2 d-f: pilvipalvelun tarjoaja xxx xx rajattu ulos.

KUVIO 17 Arviointityökalun käyttö

Kun arvioinnin tulos on kirjattu merkilleen oikein, muuttuu solun väri, esimerkiksi OK teksti saa aikaan vihreän värin ja työkalu kykenee muodostamaan yhteenvedon Tilastoja -välilehdelle.

Kyberturvallisuuskeskuksen tuottama Excel-arviointityökalu tuottaa raporttisivun, jossa on yhteenvedo arvioitujen osa-alueiden tilanteesta, kuinka moni kohta on hyväksytty ja paljonko on eri tasoisia poikkeamia. KUVIO 18 on kuvitteellinen esimerkki arviointityökalun tuottamasta raportista.



KUVIO 18 Esimerkki PiTuKri arviointityökalun raportista

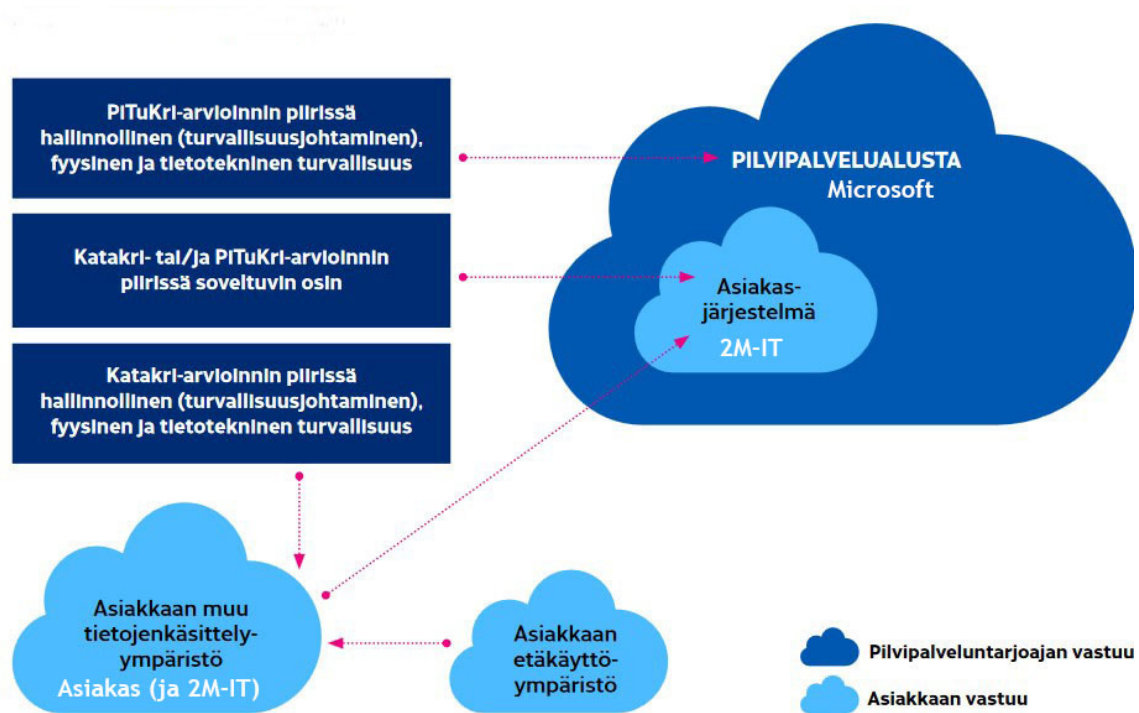
Työkalu tukee systemaattista osa-alueiden läpikäyntiä ja raportti antaa hyvän suuntiman tietoturvallisuuden kehittämiseen.

4.1 Arvioinnin eteneminen

PiTuKri ohjeistaa arviointityötä sisältäen määrittelyä ja rajausohjeita käyttötapausten, arviointimenetelmien valinnan, riskienarvioinnin ja tietotyyppien suhteen. Itsearvioinnissa sovellettavat käyttötapaudet on määritelty seuraavassa kappaleessa. Tämän jälkeen esitellään arviointikriteeristön soveltamista ohjaavat tietotyypit. Kun käyttötapaudet ja tietotyypit on selvillä, ja varmistutaan käytettävistä arviointimenetelmistä, voidaan edetä PiTuKri esiehtoihin (Kappale 4.2).

PATA-ITSEARVIOINNIN KÄYTTÖTAPAUKSET

Pata-järjestelmä sijaitsee Microsoftin tarjoamassa julkisessa pilvipalvelussa. PiTuKrin mukaan pilvipalvelun tarjoajalla on vastuu alustapalvelun tietoturvallisuudesta. Asiakkaan vastuulla on yleensä huolehtia pilvipalvelussa suoritettavan asiakasjärjestelmän turvallisuudesta sekä toimitaan liittyvien muiden tiedonkäsittely-ympäristöjen tuvallisuudesta. Pilvipalvelualustan ja asiakasjärjestelmän suhdetta havainnollistaa alla oleva KUVIO 19.

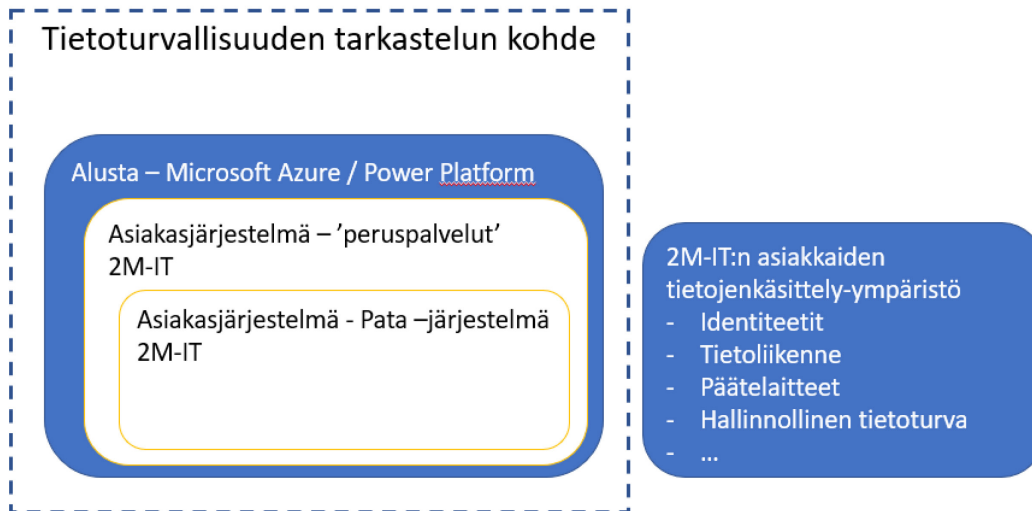


KUVIO 19 Käsittely-ympäristöjen vastuunjako (Kyberturvallisuuskeskus, 2019, muokattu)

Pata-järjestelmän kohdalla vastuu jakaantuu hienojakoisemmin, koska 2M-IT on asiakasjärjestelmän tuottaja ja 2M-IT:n asiakkailta, sosiaali- ja terveydenhuollon palveluja tuottavilla organisaatioilla, on omia tietojenkäsittely-ympäristöjä, kuten KUVIO 20 havainnollistaa:

- Microsoft on alustapalvelun tuottaja
- 2M-IT vastaa asiakasjärjestelmän tietoturvallisuudesta, kun se kehittää ja tuottaa asiakasjärjestelmää palveluna asiakkailleen. Asiakasjärjestelmä voidaan jakaa kahteen osaan, pilviympäristön peruspalveluihin eli infrastruktuuriin ja varsinaiseen asiakasjärjestelmään – Pata-järjestelmään

- 2M-IT:n asiakasorganisaatiot, sosiaali- ja terveydenhuollon palveluntuottajat vastaavat omista tietojenkäsittely-ympäristöistään. Tosin vastuu voi tässä olla jaettu, koska osa ympäristöstä kuten tietoliikenne- ja päätelaitteet saattavat olla 2M-IT:n tuottamia. Asiakasorganisaatiolla on joka tapauksessa hallinnollisia ja fyysisiä tietoturvallisuuden vastuita.



KUVIO 20 Pilvipalvelualusta, asiakasjärjestelmä ja asiakkaan muu tietojenkäsittely-ympäristö

Pata-järjestelmän tietoturvallisuuden tarkastelun kohde on ympäröity katkoviivalla. Tässä työssä keskitytään pilvipalvelualustan ja asiakasjärjestelmän tietoturvallisuuteen. Microsoftin Azure- tai Power Platform- palveluita ei kuitenkaan lähdetä kategorisesti arvioimaan, vaan keskitytään Pata-järjestelmässä hyödynnettäviin palveluihin.

PiTuKrin vaatimuksia tulee kohdentaa pilvipalvelun tyyppin mukaisesti joko asiakasympäristöön tai pilvipalvelun tarjoajan osuuteen. Kohdentamisessa hyödynnettiin PiTuKrin tekstiosan esimerkkiä sivulta 55, jossa asiakasjärjestelmä on sijoitettu pilvipalveluntarjoajan PaaS-palvelumallilla tuotettuun alustaan (Liite1).

TIETOTYYPIT JA TYÖKALUN OMINAISUUDET

Riskien hallintaprosessin (kappale 2.5) mukaan tulee tunnistaa suojattavat kohteet ja niihin liittyvät uhkat. Tiedon suojaaminen on tietoturvallisuuden keskeinen tavoite. Eli on tunnistettava, mitkä tiedot ovat erityisesti suojattavia ja mitkä vaativat vähemmän suojasta. Esimerkiksi Pata-järjestelmän sisältämät palvelupaikkojen tiedot ovat julkista tietoa, joten niiden suojaaminen ei ole ensisijaista.

Tavoitearkkitehtuurin mukaan Pata-järjestelmä voi sisältää arkaluonteista tietoa kansalaisesta, joka asioi asiakaspalvelussa. Tällaisia tietoja ovat esimerkiksi nimi, kotiosoite, henkilötunnus, henkilön terveystiedot ja henkilöön liittyvät sosiaalihuollon tiedot. Lisäksi järjestelmässä on työntekijöihin liittyvää henkilötietoa, kuten nimi ja sähköpostiosoite.

PiTuKri jaottelee tietotyypit suojaustarpeen mukaisiin luokkiin. (Kyberturvallisuuskeskus, 2019, sivu 8). Tietotyypit ovat julkinen, salassa pidettävä, henkilötieto, varautumisen näkökulmasta suojattavat tiedot ja turvaluokiteltu tieto (TL). Edellä kuvatut Pata-järjestelmän tiedot kuuluvat ryhmiin julkinen, salassa pidettävä ja henkilötieto. Turvaluokiteltua tietoa ei Pata-järjestelmässä ole. PiTuKrin vaatimuksia sovelletaan tietotyyppiin mukaisesti. Alla olevassa Excel-arviointityökalun esimerkissä arvioija on oikeanpuoleisen sarakkeen perusteella yliviivannut vaatimukset, jotka liittyvät turvaluokiteltuun (TL) tietoon, koska tämän tyyppistä tietoa ei Pata-järjestelmässä ole (KUVIO 21).

TI-05 - tiedonsaantitarpeet ja tehtävien erottelu	
1) Salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä ylläpidetään uutteloa. Tällaisiksi työtehtäviksi tulkitaan kuuluvaksi myös sellaiset kehitys- ja /tai läpikäytävät, joissa on suora tai epäsuora mahdollisuus päästä salassa pidettävään tietoon, tai muuten oleellisesti vaikuttaa salassa pidettävän tiedon suojauksiin.	1-2: Salassa pidettävä, henkilötiedot
2) Pääsy salassa pidettävään tietoon voidaan myöntää vasta, kun henkilön työtehtävistä johtuva tiedonsaantitarve on selvitetty.	3-4: TL IV & KV-R, TL III (kasauma)
3) Luetteloa turvallisuuksiluokiteltujen tietojen käsittelyoikeuksista ylläpidetään uokittain.	5: TL III (kasauma)
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) Turvallisuuksiluokan III kasaumalle lisäksi: Kriittiset tehtävät ja vastuualueet on eriytetty eri henkilöille, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Erityishuomiota kiinnitettävään, että yksittäinen henkilö ei pysty poistamaan toimimensa jälkiä tai merkittävästi estämään onnistuneiden toimien havaitsemista.	

KUVIO 21 Esimerkki PiTuKri arviointityökalusta, kuinka suojattavan tiedon tyyppi vaikuttaa kriteeristön soveltamiseen. Yliviivatut kriteerit jätetään huomiotta.

PiTuKri hyödyntää tietotyyppejä myös tiedon fyysiseen sijaintiin liittyvien riskien arvioinnissa. Fyysisen sijainnin vaatimuksia tarkastellaan kappaleessa 4.2 Esiehdot.

4.2 Esiehdot

PiTuKri muodostuu 11 osa-alueesta tai vaatimuskortista. Esiehdot antavat kuvan arvioitavan ratkaisun lähtötasosta ja samalla ohjeistavat organisaatiota, jonka vastuulla on salassa pidettävän tiedon suojaaminen. Esiehtojen täyttyessä tarkastellaan PiTuKrin etenemismallin mukaisesti jatkoarvioinnin mahdollisuuksia.

LAINSÄÄDÄNTÖJOHDANNAISET RISKIT

”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.” (Kyberturvallisuuskeskus, 2019a)

Pata-järjestelmään liittyvä tietoturvaluokitus (ei julkinen) sisältää arviointia ja linjauksia lainsäädäntöjohdannaisista riskeistä. Pata-alustapalvelut tuottaa Microsoft, jonka palvelujen tietoturvaluokitusta on hiljattain auditoitu sekä kansainvälisesti, että suomalaista kriteeristöä (Katakri/PiTuKri) vastaan.

Microsoftin järjestelmissä asiakas on aina segmentoitu. 2M-IT ja sen asiakkaat ovat julkishallinnon (segmentin) asiakkaita. Microsoft, oman vakuutuksensa mukaan, ei luovuta, eikä ole koskaan luovuttanut EU maan julkisen sektorin asiakkaan henkilötietoa yhdellekään hallitukselle. (Microsoft, 2021a)

JATKOARVIOINNIN MAHDOLLISUUDET

Microsoftin pilvipalveluja hyödynnetään EU:n alueella sijaitsevista konesaleista, North Europe ja West Europe alueista (engl. region). Pilvialustan kuvaukset löytyvät Microsoftin dokumentaatiosta (Microsoft, 2022e ja Microsoft, 2022f). Pata-järjestelmäkuvaus on esitetty tämän opinnäytetyön osassa 3. Palvelu ei ole kriittinen varautumisen kannalta samalla tavoin kuin esimerkiksi potilastietojärjestelmä, koska asiakasneuvonta ja ohjaus on poikkeusoloissa vähemmän tärkeää. Tällä perusteella palvelu voi sijaita internetissä.

PiTuKrin mukaan tietotyyppi, pilvipalvelun tyyppi ja palvelun tarjoaja vaikuttavat siihen, missä maassa palvelu voi sijaita. Liite 3 sisältää taulukon, jonka perusteella sijaintia voidaan arvioida. Taulukon tiedot on tehty arvioinnin lähtökohdaksi. Mahdollista sijaintiin perustuvaa riskiä voidaan pienentää asettamalla hallintakeinoja. Esimerkki hallintakeinosta voisi olla esimerkiksi ulkoisten suojausavainten käyttö. Koska Pata-järjestelmässä käsitellään tietotyyppiä salassa pidettävä ja henkilötieto, voidaan taulukkoa seuraamalla todeta, että pilvipalvelutyyppille ei aseteta rajoitteita. Tiedon fyysinen sijainti tulee olla EU/ETA. Palvelun tarjoajalle ei aseteta rajoitteita. Jatkoarviointiin voitiin siis edetä.

4.3 Turvallisuusjohtaminen

2M-IT:n sisäinen Pata-tietoturvaluuskuvaus sisältää kattavat kuvaukset turvallisuusjohtamisen osalta. 2M-IT:n osalta seurataan organisaation sisäisiä Palvelunhallinnan Johtamisjärjestelmän prosesseja. Oleellista turvallisuusjohtamisen osalta on, että se koskettaa kaikkia Pata-järjestelmän toimijoita, ohjelmistokehitystä, palvelutuotantoa ja sovelluksen loppukäyttäjiä (2M-IT:n asiakkaat). Eli kunkin organisaation on omalta osaltaan pidettävä huolta turvallisuusjohtamisesta. Kuvauksen osa-alueet seuraavat PiTuKri-kriteeristön rakennetta:

- turvallisuusperiaatteet
- turvallisuuden vastuut
- turvallisuusriskien hallinta
- turvallisuushäiriöiden hallinta
- jatkuvuuden hallinta
- tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä
- vaatimustenmukaisuus ja tietosuojat
- palveluntarjoajien ja toimittajien turvallisuus

4.4 Henkilöstöturvallisuus

Tietoturvapoliittika, sekä siitä johdetut periaatteet ja ohjeistukset ohjaavat 2M-IT:n toimintojen johtamista ja käytännön toimintaa. 2M-IT:llä ja järjestelmän tietoja käsittelevillä organisaatioilla tulee olla ajantasainen henkilöstön tietoturvaohjeistus, joka kuvaa käytännöt ja prosessit.

2M-IT:n ja sen asiakkaiden henkilöstön pääsy ja käyttövaltuudet sidotaan voimassa olevaan työsuhteeseen. Tätä on kuvattu tarkemmin 2M-IT:n sisäisessä Identiteetin ja pääsynhallinnan periaatteet -dokumentissa.

Salassapito- ja vaitiolosopimukset edellytetään sekä 2M-IT:n että palvelua tuottavalta alihankkijalta. Microsoftin pilvipalvelua ylläpitäviltä henkilöiltä ei ole mahdollista vaatia salassapito- ja vaitiolosopimuksia. Microsoftia sitoo 2M-IT:n ja Microsoftin välinen sopimus, ja EU:ssa voimassa oleva lainsäädäntö.

4.5 Fyysinen turvallisuus

”Suojaustavoitteena on luvattoman pääsyn estäminen palveluntarjoajan konesaliin, salassa pidettäviin tietoihin sekä varkauksien, vahinkojen, menetysten, taloudellisten tappioiden ja häiriöiden ennalta estäminen sekä vaikutusten minimointi.” (Kyberturvallisuuskeskus, 2019a)

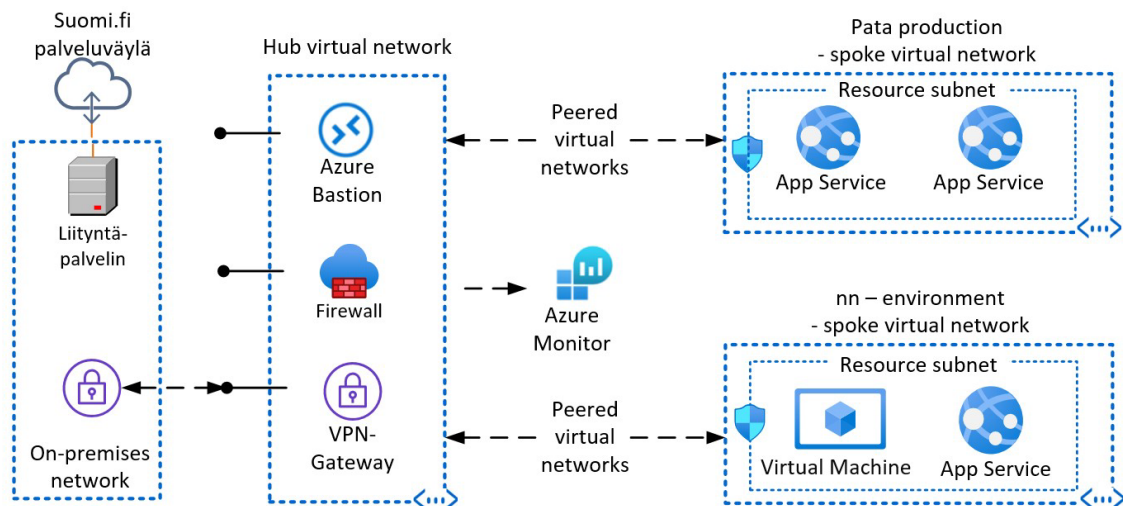
Microsoft-pilvipalvelun osalta fyysistä turvallisuutta ei ole mahdollista todentaa. 2M-IT:n ja Microsoftin välissä sopimuksissa Microsoft palveluntuottajana sitoutuu tietoturvalliseen palveluiden tuottamiseen. Microsoftin palveluihin liittyvät kuvaukset ja sopimukset antavat riittävän tiedon fyysisestä turvallisuudesta löytyvät lähteestä Azure facilities, premises, and physical security (Microsoft, 2022j).

4.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden vastuu jakautuu Microsoftin ja pilvipalvelun asiakkaan välillä palvelun tyypistä riippuen. Esimerkiksi Power Platformin osalla tietoliikenteen turvallisuus on valtaosaltaan Microsoftin vastuulla, mutta sovellusta käyttävien henkilöiden ja ulkopuolisten sovellusten (kuten Azure DevOps) tietoliikenne tulee suojata hyvien käytänteiden mukaisesti. Tietoliikennettä havainnollistaa KUVIO 9 sivulla 32. Seuraavassa käsitellään muutamia arvioinnissa nousseita keskeisiä näkökohtia.

AZURE-TIETOLIIKENNETURVALLISUUS

Sovelluskäyttäjien (verkkoselaimen) ja Azuren välinen tiedonsiirto suojataan TLS/SSL-protokollan mukaisesti. Tietoliikenne Azuressa toteutetaan Microsoftin suositusten mukaisesti Hub and Spoke verkkotopologian mukaisesti. Perusidea on toteuttaa pilveen useita aliverkkoja (spoke) eri hankkeita ja kehittämisympäristöjä varten. Keskitetty Hub-osio kokoaa pilven aliverkot yhteen ja muodostaa tarvittavat ulkoiset yhteydet, esimerkiksi yhteyden pilven ja 2M-IT:n konesalin välille. (KUVIO 22)



KUVIO 22 Tuotantoympäristö on erotettu muista ympäristöistä virtuaaliverkkojen avulla. Ulkoreunan (Hub) sisäpuolella jaettu erillisiin alueisiin. (Microsoft 2022j, mukaillen)

Azuren vNet-rakenteet linkittyvät Azure-tilauksiin, jolloin kehittäjille voidaan antaa riittävät oikeudet tiettyjen verkko-osioiden (vNet) hallintaan vähimpien oikeuksien periaatteen (least privileged) mukaisesti.

Siirrettäessä henkilötietoa tai muuta arkaluonteista tietoa esimerkiksi Potilastietojärjestelmien ja Pata-palvelun välillä, käytetään aina suojattua yhteyttä. 2M-IT:n ja Digi- ja väestötietoviraston välinen väestötietojen siirto tapahtuu suomi.fi palveluväylän kautta suojattuna.

Power Platform ja Dynamics 365 liikennöinti kontrolloidaan Microsoftin toteuttamien suojauksien kautta. Suojauksessa hyödynnetään mm. Azure AD identiteettejä, security group-määrittystä, sovellusten jakamista, liiketoimintayksikköä ja käyttäjärooleja. Power Platformin tietoliikennettä ei voi ohjata edellä kuvattuun Azuren Hub & Spoke virtuaaliverkkoon, vaan se kulkee Microsoftin määrittelmien internet liitännäspisteiden kautta. Power Platformin tietoliikennettä on mahdollisuus vahvistaa hankkimalla Azure Express Route, joka yhdistää asiakkaan tietoverkon asiakaskohtaisella yhteydellä pilvipalveluun (Microsoft, 2021b).

ORGANISAATION SISÄINEN TIETOLIIKENNETURVALLISUUS

2M-IT:n tarjoama tietoliikenne turvataan alan hyvien käytäntöjen mukaisesti segmentoinnin ja palomuurauksen ym. avulla. Tiedon siirrossa Azuren ja 2M-IT:n konesalien välillä käytetään salattua VPN yhteyttä. 2M-IT:n asiakasorganisaatiot vastaavat oman työasemaympäristönsä tietoliikenneturvallisuudesta.

Tavoitteena on, että Azure/D365 pilvipalvelussa käsiteltävien tietojen käyttö ei esty, tai niiden luotamuksellisuus tai eheys ei vaarannu yleisten verkkohyökkäysten seurauksena. Pata-järjestelmä hyödyntää suojautumisessa Microsoftin tarjoamia ratkaisuja, koska Power Platformin palvelut ja Azuressa käytössä olevat palvelut ovat kaikki Microsoftin hallinnoimia (engl. Managed Service). Paleluissa on käytössä kehittyneitä suojausominaisuuksia. (Microsoft, 2022q).

4.7 Identiteetin ja pääsyn hallinta

Pata on pilvipalvelu, jota tarjotaan palveluna useille asiakasorganisaatioille siten, että tuotantoympäristössä on usean organisaation käyttäjiä ja usean organisaation tietoa samanaikaisesti. Ulkoiset sovelluksen käyttäjät kutsutaan Pata-tuotantoympäristöön vieraina (Guest User). Tällä tavoin sovelluksen käyttäjille ei ole tarvetta luoda uusia käyttäjätunnuksia.

Järjestelmän ylläpitäjien tunnukset toteutetaan 2M-IT:n linjauksen mukaisesti ns. admin-tunnuksina, joiden käyttöä ja elinkaarta valvotaan tarkemmin, kuin sovelluksen käyttäjien tunnuksia.

KÄYTTÖOIKEUSHALLINTA

Käyttäjätunnukset myönnetään ja luovutetaan vain niille, joilla on tehtävään/rooliin liittyvä tarve ja tietojen käsittelyn peruste. Käyttöoikeudet on rajattu vain välttämättömiin toiminnallisuuksiin, sovelluksiin, laitteisiin ja verkkoihin. Tunnukset ja käyttöoikeudet hallitaan Azure AD identiteetin hallinnan ja käyttäjäryhmien avulla. (Microsoft, 2021f). Käyttäjätunnuksien suojataan ja valvotaan Azure AD:n kehittyneiden ominaisuuksien avulla. (engl. Conditional Access, Multi-factor Authentication) (Microsoft, 2022k)

KÄYTTÖOIKEUS

Sovelluskäyttäjän käyttäjätilin luonti ja käyttöoikeuksien myöntäminen tapahtuu seuraavasti

- a) Käyttäjän organisaatio perustaa pilvi-identiteetin omaan Microsoft 365 -ympäristöönsä
- b) Käyttäjän organisaatio määrittelee tarvittavat Pata-käyttöoikeudet ja tekee käyttöoikeuspyynnön 2M-IT:lle.
- c) Käyttäjä kutsutaan Pata- tuotantoympäristöön vieraskäyttäjänä (Guest User) ja hänelle lisätään käyttöoikeuden mukaisiin Azure AD-ryhmiin

- d) Käyttäjän tiliin liitetään tarvittavat ohjelmistolisenssit (esimerkiksi Dynamics 365 Customer Service)
- e) Käyttäjälle määritellään Power Platform ja Dynamics 365 roolipohjaiset käyttöoikeudet ja liitetään oikeaan liiketoimintayksikköön
- f) Käyttäjälle lähetetään tiedote/kutsu uudesta käyttöoikeudesta.

Sovelluskäyttäjän organisaation tulee ilmoittaa käyttötarpeen päättymisestä. Ilmoittamatta jättäminen heikentää tietoturvaa ja saattaa aiheuttaa tarpeettomia ohjelmistolisenssikuluja.

Ylläpitäjät tarvitsevat 2M-IT:n luoman konsulttitunnuksen 2M-IT:n prosessin mukaisesti. Erityisesti ylläpitövaltuuksia omaavia tunnuksia suojataan tiukennetulla Azure AD:n tietoturvalla, sisältäen laajan lokituksen ja riskiperustaisen ehdollisen pääsynhallinnan.

KÄYTTÄJÄTUNNISTUS

Vain valtuutetut käyttäjät pääsevät käsiksi tietoihin. Käyttäjätunnistuksen periaatteet ovat:

- g) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.
- h) Kaikki käyttäjät tunnistetaan ja todennetaan.
- i) Tunnistamisessa ja todennuksessa käytetään henkilön oman organisaation määrittämää Azure AD identiteettiä. Henkilö kutsutaan tuotantoympäristöön vierailijana (Guest User)
- j) Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin.
- k) Tunnukset ovat henkilökohtaisia
- l) Käyttäjien todennus tehdään vahvasti, vähintään kahteen tekijään nojautuen. Käytössä on Microsoftin MFA (Multi-factor Authentication).
- m) Hyödynnetään Azure Active Directoryn ehdollista pääsynhallintaa (Conditional Access), jonka käytännöt (policies) asettavat kriteereitä käyttäjän kirjautumisen hyväksymiseen. Esimerkiksi käyttäjä ei voi kirjautua toiselta mantereelta. (Microsoft, 2022k)

4.8 Tietojärjestelmäturvallisuus

Pilvipalvelussa tietojärjestelmäturvallisuuden vastuu on jaettu. Osan asioista hoitaa pilvipalvelun tuottaja ja osan palvelun asiakas. Pata-järjestelmän asiakkuudenhallinta ja monikanavainen yhteydenottoratkaisu on toteutettu Microsoft Dynamics 365 Customer Service ja Omnichannel-tekniologialla, joka sijoittuu Microsoft Power Platform -alustapalvelukokonaisuuteen (SaaS). Integraatiot on toteutettu Microsoft Azuren alustan räätälöinneillä (PaaS). Pilvipalvelun käyttöä Pata-järjestelmässä havainnollistaa KUVIO 10 sivulla 33.

JÄLJITETTÄVYYS JA HAVAINNOINTIKYKY

Pata-palvelu koostuu eri alustoista ja komponenteista. Palvelun jäljitettävyys ja havainnointikyky perustuu näiden eri komponenttien ja alustojen sisäänrakennettuihin kyvykkyyksiin, osittain konfiguroitu Pata-palvelun auditointitarpeisiin, sekä tarvittaessa laajennettu saavuttamaan halutun auditointitason.

Lokeja seurataan lokien hallintajärjestelmillä ja niihin määritettyjen sääntöpohjaisten hälytysten avulla. Lokien avulla seurataan järjestelmän ja alustapalvelun toimintaa. Sovellus tuottaa lokitietoa tiedon käytöstä, muuttamisesta ja katselemisesta kunkin tietoluokan vaatimusten mukaan. Pata-palvelua ja lokitietoja valvotaan ulkoisesti, 2M-IT:n keskitetystä valvontapalvelusta. Azure Sentinel toimii tässä yhtenä koostavana palveluna.

JÄRJESTELMÄKOVENNUS

Tietojärjestelmät toteutetaan noudattaen 2M-IT:n pilven hallintamalli-dokumenttia (ei julkinen). Sovelluskehityksessä noudatetaan tietoturvallisia sovelluskehityksen käytänteitä perustuen mm. Microsoft Secure Development Lifecycle sekä OWASP Top 10. Näiden käytänteiden lisäksi järjestelmäkovennusta edistävät seuraavat tekijät:

- Alusta hyödyntää Microsoft SaaS pohjaisia ratkaisuja, joissa tietyltä osin infrastruktuurin lisäksi myös sovellustasoiset kovennukset ovat delegoitu Microsoftin vastuulle. Näissä Microsoft noudattaa sisäisesti samaa Secure Development Lifecycle:ia, sekä muita tietoturvastandardeja kuten ISO/IEC 27001 (tämä sertifiointi on Pata-alustan osajärjestelmistä mm. Azure DevOps, Dynamics 365, Power Automate, Power BI, Power Apps, ja Power Virtual Agents palveluilla).

- Räätyäidyt palvelut toteutetaan pääosin PaaS-palveluilla, jotka ovat Microsoftin hallinnoimia (engl. Managed Service). Tällöin Microsoft vastaa infrastruktuurin ja käyttöjärjestelmän lisäksi mm. kehitys- ja tuotantoympäristön ylläpidosta esimerkiksi tekemällä alustaan tarvittavat tietoturvaapäivitykset.
- Azure-resurssit provisioidaan Cloud Adoption Framework -pohjaiseen alustaan, jossa valmiiksi käyttöön otettu tiettyjä järjestelmäkovernuksia.
- Alusta hyödyntää valmiisiin sääntöihin, tekoälyyn ja koneoppimiseen perustuvia tietoturvaehdotuksia ja hälytyksiä. Teknologioita ovat esimerkiksi Azure AD Identity Protection, Azure Defender for Cloud, Microsoft 365 Defender ja Microsoft Sentinel.
- Kaikki järjestelmän käyttö ja komponenttien toiminta kirjataan lokeihin. Tämä mahdollistaa sekä riskitilanteiden seurannan sopivilla työkaluilla (esim. Azure Sentinel), sekä historia-tietoihin perustuvan tietoturvaloukkauksien metsästy.
- Kaikki data ja liikenne on lähtökohtaisesti suojattuna ja ei suojattu liikenne estetään.
- Datakohteet varmuuskopioidaan/historioidaan
- Järjestelmän rajapinnat ja palvelut suojataan Azure AD:lla. Lähtökohtaisesti käyttäjien kontekstissa toimivat kutsut tehdään käyttäjien delegoidulla identiteetillä, jotta käyttäjän oikeuskonteksti säilyy ja audit lokeihin jää kiistattomasti tieto suorittavasta tahosta.

TIEDON EROTTELU

Pata-järjestelmä huolehtii siitä, että asiakkaiden salassa pidettävään tietoon on pääsy vain kyseisellä asiakkaalla tai valtuuden omaavalla taholla. Asiakkaiden salassa pidettävät tiedot säilytetään luotettavasti toisistaan eroteltuna yhteiskäyttöisessä Dataverse-tietovarannossa, jonka keskeiset ominaisuudet on esitelty kohdassa Power Platform - Dataverse sivulla 36.

Pata on yhteiskäyttöinen alusta, jossa monet tiedot tallentuvat tietomallimielessä samoihin tauluihin. Power Platform Dataverse tarjoaa jokaiselle taulussa olevalle tietueelle omistaja käsitteen, joka vastaa tietueen omistavaa tahoa (rekisterinpitäjää), ja johon pohjautuu Dataverse oikeusmallissa olevat oikeuskäytänteet (vain omistajatahon alaiset käyttäjät tai valtuutetut saavat nähdä ja/tai muokata kyseisiä tietueita).

Nämä oikeuskäytänteet pätevät riippumatta käyttökontekstista, oli käyttö esim. Dynamics 365 Omnichannel käyttöliittymän tai suoraan Dataverse rajapinnan kautta.

Järjestelmässä pyritään säilömään salassa pidettävää tietoa mahdollisimman vähän Dataverse tietalueen ulkopuolella, jolloin tiedot pysyvät suojattuna yllä kuvatuilla käytänteillä. Poikkeuksena ovat järjestelmäintegraatioissa esiintyvät väliaikaiset käsittelytiedot, jotka pyritään säilömään mahdollisimman lyhyen ajan tiedot, sekä audit- ja lokitiedot, joissa pyritään mahdollisuuksien mukaan hyödyntämään tietojen pseudonymisointia (esim. lokin tunnistetiedot pitää korreloida asiakasrekisterissä olevaan kansalaisen tietoihin, jotta lokeista pystyisi päättämään myös henkilöllisyys).

HAITTAOHJELMASUOJAUS

Tavoitteena on, että asiakastiedon eheys, luottamuksellisuus tai saatavuus on riittävällä tasolla suojattu yleisiä haittaohjelmariskejä vastaan.

Pata-pilvipalvelun haittaohjelmasuojauksesta vastaa lähtökohtaisesti Microsoft. Haittaohjelmien suojausta voidaan harkinnan perusteella kasvattaa hankkimalla erillinen varmistuspalvelu.

Haittaohjelmilta on suojauduttava myös henkilöstön tietoturvaosaamista kehittämällä. Järjestelmäympäristöissä tulee olla luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen. Loppuasiakkaat ovat vastuussa omien päätelaitteiden suojauksesta.

4.9 Salauskäytännöt ja avainten hallinta

SOVELLUSKÄYTTÄJÄN KÄYTTÖLIITTYMÄ

Tietoliikenne sovelluskäyttäjän verkkoselaimen ja Azuren välillä salataan TLS-protokollan mukaisesti. Microsoft käyttää tuottamissaan alustapalveluissa TLS-protokollan versiota 1.2. Vanhemmat TLS-versiot (1.0, 1.1) ja SSL-protokollat eivät ole sallittuja ja ne on estetty Azuren käytänteillä (engl. policy).

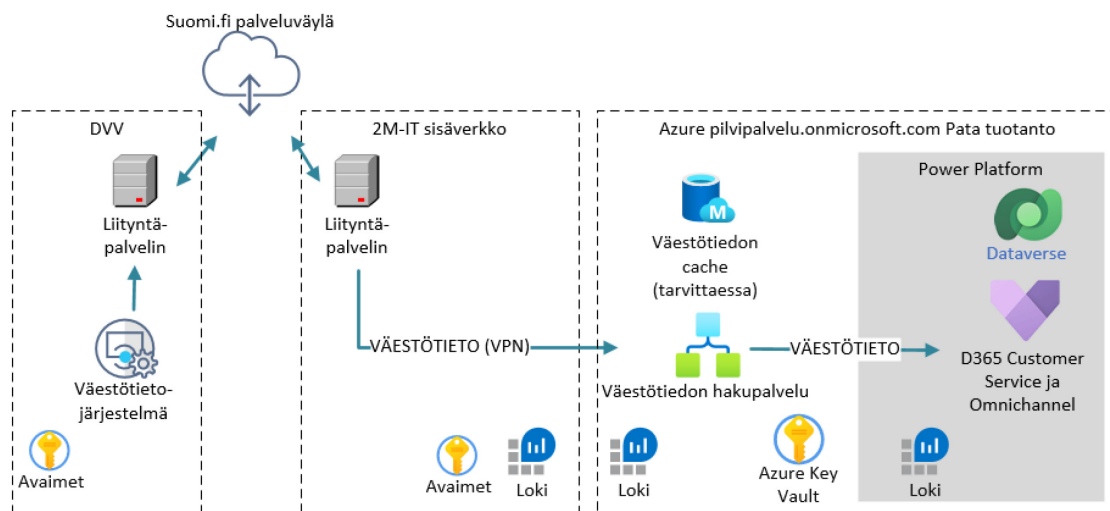
AZURE

Microsoft Azure, Power platform ja M365 palveluissa tiedot tallennetaan salattuina fyysisille kiintolevyille (Bitlocker salausteknologia). Lisäksi Power Platform alusta tarjoaa automaattisesti Microsoft SQL Server alustoille tallennetun tiedon salauksen (Transparent Data Encryption, TDE). Salausavaimien hallinnasta vastaa Microsoft. Näiden salausteknologioiden avulla tietoja suojataan

laitteiden fyysistä turvallisuuden rikkoutumista vastaan ja matalan tason pääsyä tietokannan tietoihin.

INTEGRAATIOIDEN TURVALLISUUS

Integraatioiden toteutus Azuressa noudattaa Zero Trust periaatteita, sisältäen esimerkiksi identiteetin, ja käyttövaltuuden, varmenteet, valvonnan ja salauksen. Sovelluskoodia suoritetaan esimerkiksi Microsoftin hallinnoimassa (Managed Service) Azure App Service -palvelussa, jossa Microsoft on vastuussa tietoturvapäivityksistä. Integroitavat järjestelmät tai niistä vastaavat organisaatiot asettavat vaatimuksia integraatioiden toteuttamiselle. Alla oleva KUVIO 23 esittää väestötietojärjestelmän ja Pata-järjestelmän välisen integraation toteutusta, jossa dataa siirretään suomi.fi palveluväylän kautta.



KUVIO 23 Väestötietointegraatiossa noudatetaan Digi- ja väestötietoviraston (DVV) määrittämää prosessia ja varmenteiden hallintaa. Suomi.fi palveluväylän tietoliikenteessä käytetään palveluväylän vaatimusten mukaisia prosesseja.

Azuren App Service on SaaS tason palvelu, jossa voidaan helposti kehittää, viedä tuotantoon ja skaalata web-sovelluksia ja rajapintapalveluja (API, Application Programming Interface). Tuettuja ohjelmointikieliä ovat .NET, .NET Core, Node.js, Java, Python ja PHP. Ohjelmistoja voidaan suorittaa konteissa, Windowsissa tai Linuxissa. (Microsoft, 2022u)

VARMENTEIDEN JA AVAIMIEN HALLINTA

Järjestelmän tiedon ja tietoliikenteen salaukseen käytetään komponentista riippuen joko 2M-IT:n tai Microsoftin hallinnoimia varmenteita ja avaimia. Avaimet säilytetään pääsääntöisesti Azure Key

Vaultissa. Microsoftin hallinnoimat avaimet tulevat tätä varten tehdystä palvelusta, ja niiden uusiminen on automaattista.

2M-IT:llä on dokumentoitu varmenteiden ja avainten hallintaprosessi, jonka avulla varmenteiden käyttämän avaimet tuotetaan turvallisesti ja varmenteista pidetään kirjaa ja niiden uusimisesta huolehditaan säännöllisesti, jotta järjestelmien saatavuus ei vaarannu varmenteiden vanhentumisen vuoksi.

4.10 Käyttöturvallisuus, siirrettävyys ja yhteensopivuus

Jatkuvuuden tukemiseksi vaadittava järjestelmän dokumentaatiovastuu jakautuu Microsoftin ja 2M-IT:n kesken. Microsoftin dokumentaation on kattava. 2M-IT:n osalta järjestelmästä on runsaasti dokumentaatiota.

Dataverse tarjoaa ohjelmointirajapinnat, jonka piirissä on koko Pata-järjestelmän sisältö. Tietorakenne ja rajapinnat päivittyvät automaattisen ohjelmistoversioiden päivityksen kautta.

Microsoft tarjoaa teknisen rajapinnan asiakkaan tietojen toimitukseen asiakkaalle soveltuvassa, käyttökelpoisessa ja yleisesti yhteensopivassa muodossa. Tietojen tuontiin ja vientiin sekä palvelun hallintaan käytetään turvallisia, vakiintuneita verkkoprotokollia siten, että siirrettävien tietojen luottamuksellisuudesta, eheydestä ja saatavuudesta voidaan varmistua.

4.11 Muutostenhallinta ja järjestelmäkehitys

Muutokset toteutetaan 2M-IT:n palveluhallinnan johtamisjärjestelmän muutoksenhallintaprosessin mukaisesti. Prosessilla hallitaan kaikkien 2M-IT:n palveluihin kohdistuvien muutosten ja julkaisujen elinkaarta. Tavoitteina ovat:

- Mahdollistaa muutosten ja julkaisujen tekeminen minimaalisilla palveluihin kohdistuvilla häiriöillä, sekä varmistaa ettei palveluiden ja palvelukomponenttien eheys vaarannu
- Varmistua, että kaikki muutokset ja julkaisut ovat dokumentoituja, arvioituja ja kun muutos tai julkaisu on hyväksytty, se myös suunnitellaan, aikataulutetaan, testataan, implementoidaan ja dokumentoidaan
- Varmistua, että kaikki muutokset konfiguraation rakenteeseen on dokumentoitu 2M-IT:n käyttämään konfiguraationhallintajärjestelmään.

Muutoksen hallinnassa arvioidaan muutoksen vaikutukset tuotantopalveluille asiantuntijoiden tuke-
mana. Arviointi tunnistaa myös tarvittavan hyväksyntätason, mahdollisen muutosryhmän kokoon-
panon, liiketoimintaperustelun, sekä muutoksen vaikutukset, kustannukset, hyödyt ja riskit.

JÄRJESTELMÄKEHITYS JA TESTAUS

Ohjelmiston kehittämisessä noudatetaan ketterän kehittämisen menetelmää. Kehittämisympäristö
sisältää erilliset kehitys, testaus ja asiakastestausympäristöt. Ympäristöt on rakennettu sekä Power
Platformiin, että Azureen. KUVIO 9 Pata-järjestelmän tekninen ympäristö sivulla 32 esittää kehitys-
ja tuotantoympäristöjen rakenteen ja ohjelmistokehityksen prosessin ylätasolla.

Sovellukset ja ohjelmointirajapinnat (API) suunnitellaan, kehitetään, testataan ja otetaan käyttöön
alan hyvien turvallisuuskäytäntöjen mukaisesti. Rajapintojen on kestävä yleiset hyökkäysmene-
telmät ilman, että käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu.

Tuotantoympäristö on eriytetty muista ympäristöistä (esimerkiksi kehitys-, testaus- ja laadunvar-
mistusympäristöistä).

Versionhallinnan turvallisuus on huomioitu siten, että menettelyt luotettavasti estävät valtuuttamat-
tomien versioiden siirron tuotantoympäristöön. Azure DevOps on tuotantoympäristöstä erillään.
DevOps prosessin käyttöoikeuksia säännöstellään ja valvotaan samalla tavalla kuin hallintatunnuk-
sia muutenkin.

5 HAVAINTOJA JA POHDINTAA

Pata-järjestelmä ja Microsoft pilvipalvelut muodostavat kokonaisuuden, jonka tietoturvallisuutta on jaetun vastuun vuoksi ilmeisen vaikea arvioida. Microsoftin SaaS ja PaaS palvelut ovat asiakkaalle paljolti 'musta laatikko', jonka luotetaan tekevän sitä, mitä Microsoftin dokumentaatioissa luvataan. Tämän varmentamiseksi Microsoft on aktiivinen teettämään palvelujen auditointeja sekä kansainvälisten viitekehysten että kotimaisten kriteeristöjen vaatimuksia vastaan. Sote-toimialalla pilvipalvelujen hyödyntäminen on melko uutta. Julkisen sote-sektorin ICT-osaamisen painopiste on edelleen konesalissa tuotetuissa palveluissa.

Palataan tämän dokumentin johdantokappaleessa esiteltyyn pilvipalvelun määritelmään: *"Pilvipalveluilla tarkoitetaan verkon yli saavutettavaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään jaettujen, skaalautuvien ja joustavien resurssien mallia, joka on automatisoitu osin itsepalveluperiaatteella tuotettavaksi"* (Kyberturvallisuuskeskus, 2019).

Määritelmästä voidaan poimia keskeiset sanat: verkon yli, resurssit ja itsepalvelu. Hahmotetaan seuraavaksi tätä määritelmää kappaleessa 2.2 esitellyn CIA-mallin avulla. Kun yhdistetään mallin peruskäsitteet luottamuksellisuus, eheys ja saatavuus pilvipalvelun määritelmästä poimituihin käsitteisiin, voidaan tuottaa pilvipalvelujen tietoturvallisuuden yleiset vaatimukset:

Luottamus säilyy

- kun tietoliikenne verkon yli pysyy salattuna
- kun pilvipalveluresurssit on suojattu siten, että vain valtuutetut tahot käsittelevät tietoa
- kun itsepalveluratkaisu sisältää havainnollisia luottamuksellisuuden hallintakeinoja, esimerkiksi käyttöoikeuksien määrittely on selkeää, ja asiakas saa valvontatietoa palvelun toiminnasta.

Tieto pysyy eheänä

- jos tietoliikenne ei katkeile hallitsemattomasti tai korruptoidu
- kun pilvipalvelussa käsitellään tietoa hallitusti ja laadukkaasti, palvelu on vikasietoinen ja tunnistaa virhetoimintoja
- kun itsepalvelu toimii loogisesti, siten, ettei käyttäjä ei vahingossa sekoita tiedon käsittelyä pilvessä.

Tieto ja palvelu on saatavilla

- jos tietoliikenneyhteydet ja vararatkaisut toimivat odotusten mukaan
- jos pilvipalveluresurssit noudattavat sovittua palvelutasoa, ja palautuminen on suunniteltua
- kun pilvipalvelun palvelut ovat selkeitä, niin että asiakas ymmärtää saatavuuteen vaikuttavan konfiguraation (jonka tekee itsepalveluna).

Edellä esitetty kömpelöähkö sanaleikki ei anna tietoturvallisuudesta koko kuvaa, mutta se hyvin kyllä avaa, miten tärkeitä CIA-mallin peruskäsitteet ovat myös pilvipalvelun kohdalla. Pilvipalvelun olemuksesta voidaan huomata, että hyvä tuotteistaminen on tärkeää. Selkeä rakenne, havainnollisuus, loogisuus, kyky antaa palautetta, ja helppokäyttöisyys ovat onnistumisen eväitä. Itsepalveluasiakkaan on tultava vakuutetuksi, että CIA-tavoitteet ja tietoturvallisuus toteutuvat.

5.1 Johtopäätöksiä Pata-järjestelmän tietoturvallisuudesta

Lainsäädäntöjohdannaisten riskien kohdalla on kyse siitä, toimiiko pilvipalvelun tuottaja, eli Microsoft kaikissa tilanteissa Suomen ja EU:n lainsäädännön mukaisesti. Vastavoimana tiedetään olevan esimerkiksi USA:n lainsäädäntö, joka edellyttää monikansallisia, Yhdysvalloissa toimivia yrityksiä luovuttamaan pyydettyä järjestelmän tietoja viranomaiselle. Microsoft on juuri tällainen monikansallinen yhtiö, joka toimii myös Yhdysvalloissa.

Luottamuksen saavuttaminen edellyttää, että asiakas voi riittävällä tasolla vakuuttua palvelun tarjoajan suorituskyvystä ja periaatteista. Esimerkiksi, palvelun tarjoajan tulee kunnioittaa asiakkaan tietovarantoa, eikä missään nimessä luovuta sitä ulkopuolisille. Tässä on sama logiikka kuin nettiostoksen tekemisessä. Tuskin kukaan haluaa asioida nettikaupassa, jonka tiedetään tai epäillään luovuttavan asiakkaan maksuvälinetietoja ulkopuolisille. Kun toteutetaan sote-toimialalle kansalaisten arkaluonteista henkilötietoa sisältävää tietojen käsittelyratkaisua, on tietojen vuotamisen uhka huomattavasti pelottavampi kuin yksittäisen nettiasiakkaan kohdalla.

PILVIPALVELUN SIJAINTI JA PALVELUNTARJOAJAN MAINE

Millä voidaan perustella organisaation ulkopuolisen toimijan luotettavuutta? Onko merkitystä, missä maassa yhtiö pitää pääkonttoriaan?

Kun vertaillaan isoja, monikansallisia pilvipalvelujen tarjoajia, ei ole olemassa yksikäsitteistä vastausta mikä yhtiö olisi paras valinta. Yhtiöillä on hyvin erilaisia palvelusisältöjä, varsinkin kun puhutaan SaaS-tason palveluista. Useimmilla isoilla yhtiöillä vaikuttaa olevan pääkonttori Yhdysvalloissa. Selvää on kuitenkin, että Pata-järjestelmän tietojen käsittelyn, varsinkin henkilötietojen käsittelyn tulee tapahtua EU:n alueella. Microsoft on sanonut suunnittelevansa datakeskusta Suomeen. (Microsoft, 2022g) Tämä edelleen parantaa tiedonkäsittelyn turvallisuutta, varsinkin jos tarkastellaan poikkeusoloihin varautumista. Pata-järjestelmä on kahdentamisen vuoksi konfiguroitu hyödyntämään kahta palvelualueutta, joten täysin Suomessa tapahtuvaa tiedon käsittelyä ei tultane näkemään kovin pian. Ehkä Ruotsissa sijaitseva datakeskus toimisi hyvänä parina tälle.

Isoista monikansallisista yhtiöistä, jotka tekevät merkittävää liiketoimintaa pilvipalvelujen tarjoajina, voidaan olettaa, että ne tekevät kaikkensa asiakkaiden luottamuksen saavuttamiseksi. Kappaleessa 4.2 Esiehdot käsitellään Pata-lainsäädäntöjohdannaisia riskejä. Yhdysvaltalainen Microsoft ilmaisee noudattavansa EU:n lainsäädäntöä, eikä se oman ilmoituksensa mukaan luovuta tietoja toisille hallituksille, siitä huolimatta, että esimerkiksi EU:n ja USA:n lainsäädännöt ovat keskenään ristiriidassa tiedon luovuttamisen osalta.

MICROSOFTIN TEETTÄMÄT TIETOTURVALLISUUDEN AUDITOINNIT

Microsoft arvioituttaa pilvipalvelujaan säännöllisesti. Kyse on kategorisesta tietoturva-auditoinnista, jossa käydään läpi koko tarjonta. Microsoft julkaisee asiakkailleen auditoinnin tulokset internet-sivuillaan (Microsoft, 2021c) Dokumenttien lukeminen edellyttää Microsoft-pilviasiakkuutta.

Azure-palveluja on auditoitu KPMG:n toimesta myös suomalaista Katakri-kriteeristöä vastaan vuonna 2022. (Microsoft, 2022h) Tässä ei auditoitu Power Platformia.

Edellä kuvatut seikat antavat kohtalaisen vahvan kuvan siitä, että Microsoft käsittelee tietoa turvallisesti ja paikallisten lakien mukaisesti.

PILVIALUSTAN MUUTOSTEN HALLINTA

Tietojärjestelmäturvallisuus on Pata-järjestelmän pilvialustassa, eli Power Platformissa hyvällä tasolla. Huolen aiheeksi on noussut pilvialustassa usein tapahtuvat muutokset. Tätä ongelmaa on kuvattu tarkemmin kappaleessa 3.6 sivulla 40. Power Platformiin tulee jatkuvasti paljon hyviä uudistuksia, mutta valitettavasti myös yllättäviä epäjohtonmukaisuuksia tai odottamattomia muutok-

sia toimintalogiikkaan. Koska muutostahti on kova, ei Power Platformin päälle rakennettua ohjelmistoa voi jättää kovin pitkään oman onnensa nojaan, vaan on aktiivisesti seurattava, että Microsoftin tekemät muutokset eivät ainakaan riko sovellusta.

5.2 Organisaation valmiudet pilveen

2M-IT:llä on vahva osaaminen tietotekniikan ja sovelluspalvelujen tuottamisesta asiakkailleen – sosiaali- ja terveydenhuollon julkisille organisaatioille. Kuten aikaisemmin on todettu, toimialan isot järjestelmät ovat pääosin konesaliaikakauden tuotteita, samoin kuin toiminnan tukijärjestelmät, esimerkiksi henkilöstö- ja taloushallinnan järjestelmät. Tietyt palvelut halutaan edelleen tuottaa 'kivijalasta', jotta kyetään toimimaan poikkeusoloissa.

Sote-toimiallakin pilviteknologian hyödyntämisen arkipäivää ovat Microsoft Office 365 ympäristöjen ja niihin liittyvien tukipalvelujen tarjoaminen asiakkaille. Ominaista on, että järjestelmiin liittyy käyttöönottoprojekteja, pilvi-infrastruktuurin rakentamista sisältäen asiakaskohtaisia valintoja esimerkiksi palvelutasosta. Tällaiset palvelut eivät tyypillisesti sisällä ohjelmistokehitystä.

Pilveen liittyvä ohjelmistokehitys on kuluneen kahden vuoden aikana tuonut 2M-IT:lle uusia vahvuuksia, kun on lähdetty toteuttamaan asiakkaille suunnattua pilvipalveluympäristöä ja sinne kehitettäviä ohjelmistoja. Pata-järjestelmä on, kuten aikaisemmin on kuvattu, asiakasorganisaatioiden kannalta keskitetty palvelu, jossa ne saavat SaaS palvelumallin mukaisesti ohjelmiston, lisenssit, käyttäjätuen ym. palvelut kokonaisuutena. 2M-IT:n osaaminen on kasvanut erityisesti pilviympäristöjen hallinnan osalta. Pata-hanke on omalta osaltaan tuonut yritykselle näköalaa, miten asiakkaille voidaan kehittää ja tarjota palveluja pilvialustalta. Kuluneen kahden vuoden aikana on otettu isoja edistysaskeleita mm. pilvipalvelumallien, tietoturvallisuuden, kyberturvallisuuden, ohjelmistokehityksen, ja henkilöstön osaamisen kohdalla.

6 LOPUKSI

Usein kuulee sanottavan, että isot yhtiöt, jotka keskittyvät pilvipalvelujen tuottamiseen, pystyvät tekemään sen paljon laadukkaammin ja turvallisemmin kuin organisaatio itse kykenisi omassa konesalissaan. Samaa ajatusta markkinoivat konesalipalvelujen suurtuottajat. Keskitetyt konesaliympäristöt ovatkin pilvipalvelujen rinnalla merkittävä palvelumalli. Tällöin konesalia hallinnoi toimija, jolla on siihen mahdollisuus erikoistua. Varautumisen kannalta erityisten kriittisten palvelujen ympäristöksi ei internetissä sijaitseva pilvipalvelu, eikä ulkopuolisen toimijan konesalipalvelukaan aina sovellu, vaan palvelinkapasiteetti on ehkä sijoitettava lähelle toimintaa. Esimerkiksi yliopistosairaala saattaa kansallisen turvallisuuden vuoksi haluta tuottaa tietyt tietojenkäsittelypalvelut sairaalan omasta konesalista. Tähän ongelmakenttään ovat pilvipalvelujen tarjoajat tuoneet markkinoille yhdistelmäpilaritratkaisuja, joissa ikään kuin hyödynnetään parhaat puolet sekä konesalista, että pilvestä.

Palvelujen kehittäminen, käyttöönotto ja tuottaminen pilvestä ei välttämättä, ainakaan alkuun, ole sen helpompaa kuin palvelun tuottaminen konesalissa. Pilvipalveluympäristön hyödyntäminen sosiaali- ja terveydenhuollon toimialalla edellyttää organisaatiolta erityisosaamista, esimerkiksi pilven tietoturvallisten peruspalvelujen eli ns. infrastruktuurin rakentamiseen ja ylläpitämiseen. Samoin tietoturallinen ohjelmistokehitys pilviympäristössä vaatii osaavan tiimin. Ohjelmistokehityksen painopiste tuntuu siirtyvän pilvialustojen suuntaan, jotka tarjoavat kehittäjille yhä parempia välineitä, helpompaa ohjelmistojen tuotantoon julkaisua ja joustavaa, jopa automaattista skaalautumista.

Oman konesaliympäristön voi tarkoituksella tai vahingossa 'jäädättää' siten, että ympäristöä, palvelimia, tietoverkkoa, suojauksia ja käyttöjärjestelmiä päivitetään vain minimitasolla. Moni alalla työskentelevä on saattanut törmätä esimerkiksi vanhoihin palvelimiin, joiden käyttöjärjestelmän tuki on päättynyt. Tässä tilanteessa omasta konesalista muodostuu uhkatekijä, koska tuen päättymisen jälkeen tunnistettuja haavoittuvuuksia ei ehkä voida enää poistaa.

Pilviympäristö, esimerkiksi Azuren palveluympäristö on jatkuvassa muutoksessa, kun pilvipalvelun tarjoaja uudistaa ympäristöä. Se asettaa palvelua hyödyntäville tai ohjelmistoa kehittäville asian tuntijoille jatkuvan haasteen, koska tarvitaan halua ja valmiuksia omaksua uutta teknologiaa. Tietoturvallisuuden kannalta on kuitenkin erittäin hyvä, että ympäristö pysyy ajantasaisena.

Luotettava pilvipalvelun tarjoaja varmistaa osaltaan tietoturvallisuuden, ylläpitää ympäristöä ajantasaisena, reagoi tunnistettuihin haavoittuvuuksiin nopeasti ja ohjeistaa asiakasta tietoturvallisuuden kehittämisessä. Luotettavuus tulee esille mm. tietoturvallisuuden hallintakeinojen toteutuksissa, selkeissä (itsepalvelu-) prosesseissa, auditoinneissa ja dokumentaation laadussa.

Pilvipalvelut soveltuvat sosiaali- ja terveydenhuollon ohjelmistokehityksen ja -palvelujen alustaksi, kun ne toteutetaan parhaiden käytänteiden mukaan tietoturvallisuuden ja tietosuojan vaatimukset huomioiden. Tässä opinnäytetyössä arvioitu Pata-järjestelmä nojautuu paljolti Microsoftin PaaS ja SaaS alustalle toteuttamiin tietoturvan hallintakeinoin, mikä edesauttaa turvallisen sovelluksen toteuttamista. Tietoturvallisuuden itsearviointi tuotti tietoa, jonka avulla Pata-järjestelmän tietoturvaluutta voitiin kehittää. Näin tämä opinnäytetyö osaltaan, tunnistamalla tietoturvallisuuden poikkeamia, tukee ohjelmistokehityksen tavoitteita ja järjestelmän tietoturvaluutta, mikä olikin tavoitteena.

Opinnäytetyön tekijän kannalta tietoturvallisuuden perusteiden läpikäynti ja varsinkin pilvipalveluihin liittyvien erityisominaisuuksien selvittely on nostanut osaamistasoa merkittävästi. PiTuKri-kriteeristön mukaan tehty tietoturvallisuuden itsearviointi on poistanut arviointiprosessiin liittyvät salamyhkäisyydet ja menetelmä vaikuttaa käyttökelpoiselta jatkossakin. Tietoturvallisuuden parempi ymmärtäminen on antanut arkkitehdille Pata-järjestelmän kehittämiseen ja tulevien työtehtävien haasteisiin ihan uuden näköalan. Tavoitteena tässä työssä on ollut kirjoittaa asiat auki siten, että tämä dokumentti toimisi oppaana tai lähteenä muille asiasta kiinnostuneille. Toivottavasti joku lukija koee tämän hyödylliseksi.

LÄHTEET

Andress, J. 2019. Foundations of information security: a straightforward introduction. No Starch Press. Hakupäivä 8.2.2022 <https://lccn.loc.gov/2019024099>

Ben-David J. 2021. Cloud Elasticity vs Cloud Scalability. Turbonomic Blog. Hakupäivä 5.4.2022 <https://blog.turbonomic.com/blog/on-technology/cloud-elasticity-vs-cloud-scalability>

Immonen M. 2022. Blogi: Zero Trust korvaa vanhentuneen kuorisuojausajattelun ja kankeat VPN:t. Itewiki. Hakupäivä 27.4.2022. <https://www.itewiki.fi/p/blogi-zero-trust-korvaa-vanhentuneen-kuori-suojausajattelun-ja-kankeat-vpn-t>

Dictionary.com 2022. Hakupäivä 9.3.2022 <https://www.dictionary.com/>

Dotson, C. 2019. Practical cloud security. O'Reilly Media, Inc. Hakupäivä 21.2.2022 <https://learning.oreilly.com/library/view/practical-cloud-security/9781492037507/> Vaatii käyttöoikeuden.

gdpr.eu, 2022. What is GDPR, the EU's new data protection law? Hakupäivä 23.3.2022 <https://gdpr.eu/what-is-gdpr/>

GeeksforGeeks, 2022. Scalability and Elasticity in Cloud Computing. Hakupäivä 25.4.2022. <https://www.geeksforgeeks.org/scalability-and-elasticity-in-cloud-computing/>

Kyberturvallisuuskeskus, 2019a. Pilvipalveluiden turvallisuuden arviointikriteeristö (liitetiedosto, pdf). Hakupäivä 14.3.2022. <https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri>

Kyberturvallisuuskeskus, 2019b. PiTuKri, arviointityökalu (liitetiedosto, xlsx) Hakupäivä 1.4.2022. <https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri>

Kyberturvallisuuskeskus, 2022. Hyväksytyt tietoturvallisuuden arviointilaitokset. Hakupäivä 14.3.2022. <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset>

Laki julkisen hallinnon tiedonhallinnasta, 906/2019. Hakupäivä 4.4.2022. <https://www.finlex.fi/fi/laki/alkup/2019/20190906>

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021. Hakupäivä 13.3.2022. <https://finlex.fi/fi/laki/ajantasa/2021/20210784>

Messier, R. 2019, CEH v10 Certified Ethical Hacker Study Guide. Sybex. Hakupäivä 22.2.2022 <https://learning.oreilly.com/library/view/ceh-v10-certified/9781119533191/> Vaatii käyttöoikeuden.

Microsoft, 2021a. Compliance with EU transfer requirements for personal data in the Microsoft cloud. Hakupäivä 29.3.2022. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRql1?culture=en-us&country=US>

Microsoft, 2021b. Using Azure ExpressRoute with Microsoft Power Platform. Hakupäivä 1.4.2022. <https://powerapps.microsoft.com/en-us/blog/using-azure-expressroute-with-microsoft-power-platform/>

Microsoft, 2021c. Azure – Commercial – System Security Plan (2021), FedRAMP Reports. Hakupäivä 4.4.2022 https://servicetrust.microsoft.com/ViewPage/MSComplianceGuideV3?doc-Tab=7027ead0-3d6b-11e9-b9e1-290b1eb4cdeb_FedRAMP_Reports (Huom. dokumentti ei ole julkinen, vaatii Azure Information Protection -katseluohjelman)

Microsoft, 2021d. Microsoft Azure glossary: A dictionary of cloud terminology on the Azure platform. Hakupäivä 12.4.2022. <https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology>

Microsoft, 2021e. Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings. Hakupäivä 13.4.2022. <https://docs.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings>

Microsoft, 2021f. Azure Active Directory Documentation. Hakupäivä 13.4.2022. <https://docs.microsoft.com/en-us/azure/active-directory/>

Microsoft, 2022a. Azure DevOps. Hakupäivä 1.4.2022. <https://azure.microsoft.com/en-us/services/>

Microsoft, 2022b. Microsoft Sentinel. Hakupäivä 1.4.2022 <https://azure.microsoft.com/en-us/services/microsoft-sentinel/>

Microsoft, 2022c. Dataverse. Hakupäivä 1.4.2022 [Dataverse for Business Applications ~ Ozkary - Emerging Technologies](#)

Microsoft, 2022d. Dataverse security concepts. Hakupäivä 1.4.2022 <https://docs.microsoft.com/en-us/power-platform/admin/wp-security-cds>

Microsoft, 2022e. Microsoft Power Platform -dokumentaatio. Hakupäivä 4.4.2022 <https://docs.microsoft.com/fi-fi/power-platform/>

Microsoft, 2022f. Azure documentation. Hakupäivä 4.4.2022. <https://docs.microsoft.com/en-us/azure/>

Microsoft, 2022g. Microsoft intent to build datacenter region in Finland. <https://news.microsoft.com/europe/2022/03/17/microsoft-announces-intent-to-build-a-new-datacenter-region-in-finland-accelerating-sustainable-digital-transformation-and-enabling-large-scale-carbon-free-district-heating/>

Microsoft, 2022h. Azure KPMG auditointi. (ei julkinen). Hakupäivä 4.4.2022. <https://www.microsoft.com/en-us/download/details.aspx?id=54536>

Microsoft, 2022i. Connect to Microsoft Azure, DevOps Pipelines. Hakupäivä 5.4.2022. <https://docs.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure?view=azure-devops>

Microsoft, 2022j. Azure facilities, premises and physical security. Hakupäivä 5.4.2022. <https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security>

Microsoft, 2022k. What is Conditional Access. Hakupäivä 6.4.2022. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

Microsoft, 2022l. Tutustu asiakaspalvelusovellukseen. Hakupäivä 6.4.2022 <https://docs.microsoft.com/fi-fi/dynamics365/customer-service/help-hub>

Microsoft, 2022m. Omnichannel for Customer Service esittely. Hakupäivä 6.4.2022. <https://docs.microsoft.com/fi-fi/dynamics365/customer-service/introduction-omnichannel>

Microsoft, 2022n. What is a hybrid cloud. Hakupäivä 13.4.2022. <https://azure.microsoft.com/en-us/overview/what-is-hybrid-cloud-computing/>

Microsoft, 2022o. Power Appsin kuvaus. Hakupäivä 13.4.2022. <https://docs.microsoft.com/fi-fi/power-apps/powerapps-overview>

Microsoft, 2022p. Cloud computing terms. Hakupäivä 13.4.2022. <https://azure.microsoft.com/en-gb/overview/cloud-computing-dictionary/>

Microsoft, 2022q. Azure DDoS Protection Standard overview. Hakupäivä 11.3.2022. <https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview>

Microsoft, 2022r. Defense in depth security in Azure. Hakupäivä 24.4.2022. <https://docs.microsoft.com/en-us/shows/azure-videos/defense-in-depth-security-in-azure>

Microsoft, 2022r. Dynamics 365 release schedule and early access. Hakupäivä 23.4.2022. <https://docs.microsoft.com/en-us/dynamics365/get-started/release-schedule>

Microsoft, 2022s. Restore your Azure SQL Database or failover to a secondary. Hakupäivä 27.4.2022. <https://docs.microsoft.com/en-us/azure/azure-sql/database/disaster-recovery-guidance>

Microsoft, 2022t. Suhtaudu tietoturvaan aktiivisesti Zero Trust -suojausmallilla. Hakupäivä 27.4.2022. <https://www.microsoft.com/fi-fi/security/business/zero-trust>

Microsoft, 2022u. App Service. Hakupäivä 28.4.2022. <https://azure.microsoft.com/en-us/services/app-service/#overview>

Gates, S. 2019. Modern Defense in Depth. O'Reilly Media, Inc. Hakupäivä 26.4.2022. <https://learning.oreilly.com/library/view/modern-defense-in/9781492050360/> Vaatii käyttöoikeuden.

NIST. 2011. Special Publication 800-145: The NIST Definition of Cloud Computing. National Institute of Standards and Technology. Hakupäivä 28.3.2022. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Okeyode D. 2021. Microsoft Azure Security Technologies Certification and Beyond. Packt Publishing. Hakupäivä 22.2.2022. <https://learning.oreilly.com/library/view/microsoft-azure-security/9781800562653/> Vaatii käyttöoikeuden.

Rybaric, R. 2020. Microsoft Power Platform Enterprise Architecture. Packt Publishing. Hakupäivä 22.2.2022 <https://learning.oreilly.com/library/view/microsoft-power-platform/9781800204577/> Vaatii käyttöoikeuden.

Salo, A. 2022. Mikä on Zero Trust?. Elisa blogit. Hakupäivä 27.4.2022. <https://yriyksille.elisa.fi/ideat/zero-trust-nollaluottamus-turvaa-ict-ymparistosi/>

Sanastokeskus 2018. TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018) [Kyberturvallisuuden sanasto \(TSK 52\) | Sanastokeskus](#)

Sosiaali- ja terveysalan lupa- ja valvontavirasto, 2022 Sosiaali- ja terveydenhuollon tietojärjestelmät. Hakupäivä 13.3.2022 <https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat/>

Sosiaali- ja terveysministeriö, 2022: Lainsäädäntö ohjaa asiakas- ja potilastietojen hallintaa. Hakupäivä 14.3.2022. <https://stm.fi/asiakas-potilastietojen-hallinta>

Speedos Blog, 2022. Azure Security and Monitoring. Hakupäivä 25.4.2022. <https://saeedtas-bih.blog/professional-blog/azure-fundamentals-3/>

Suomen standardisoimisliitto, 2022, ISO/IEC 27000 Tietoturvallisuuden standardisarja. Hakupäivä 14.3.2022. <https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/>

Terveyden ja hyvinvoinnin laitos, 2022. Tiedonhallinta sosiaali- ja terveysalalla – määräykset ja määrittelyt. Hakupäivä 13.3.2022 <https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt>

Tietosuojalaki, 1050/2018., Hakupäivä 4.4.2022. <https://www.finlex.fi/fi/laki/alkup/2018/20181050>

Tietosuojalaki, 5.12.2018/1050. Hakupäivä 26.2.2022 <https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>

Valtioneuvosto, 2020. Kansallinen turvallisuusauditointikriteeristö Katakri 2020 julkaistu. Hakupäivä 14.3.2022. <https://valtioneuvosto.fi/-/kansallinen-turvallisuusauditointikriteeristo-katakri-2020-julkaistu>

Valtiovarainministeriö, 2020a. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka) Hakupäivä 1.4.2022 <http://urn.fi/URN:ISBN:978-952-367-289-5>

Valtiovarainministeriö, 2020b. Julkisen hallinnon digitaalinen turvallisuus. Julkisen hallinnon ICT. Hakupäivä 22.2.2022. <http://julkaisut.valtioneuvosto.fi/handle/10024/162169>

LIITTEET

Liite 1 PiTuKri: Esimerkki vaatimusten kohdentamisesta vastuihin

Liite 2 PiTuKri: Esimerkki kriteeristön soveltamisesta salassa pidettävän tiedon suojausten vaatimustenmukaisuuden arvioinnissa

Liite 3 PiTuKri: Jatkoarvioinnin mahdollisuudet

Liite 1 PiTuKri: Esimerkki vaatimusten kohdentamisesta vastuittain

Palvelumallina PaaS

Tässä esimerkissä kuvataan PiTuKri:ssä kuvattujen vaatimusten kohdentaminen vastuittain tilanteessa, jossa asiakasjärjestelmä on sijoitettu pilvipalveluntarjoajan PaaS-palvelumallilla tuotettuun alustaan.

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (soveltuvuuden arviointi)	x
	3	-	x
	4	x (soveltuvuuden arviointi)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (soveltuvin osin)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	- (Huom: Vaihtelua palveluntarjoajittain vastuurajoista, esimerkiksi sovellusten osalta.)	x
JT-03	1	- (Ellei asiakasjärjestelmässä edelleen eri erottelutarpeisia asiakkaiden tietoja.)	x

Liite 2: Esimerkkejä kriteeristön soveltamisesta vaatimustenmukaisuuden arviointiin

Esimerkki 1: Salassa pidettävän tiedon suojausten vaatimustenmukaisuuden arviointi

Tässä kuvataan esimerkki siitä, kuinka kriteeristöä voidaan soveltaa turvallisuusluokittelemattoman salassa pidettävän tiedon suojausten vaatimustenmukaisuuden arviointiin suhteessa tiedonhallintalain (906/2019) vaatimuksiin. Esimerkissä asiakkaana on viranomais A, joka haluaa arvioida uuden, vielä suunnitteluvaiheessa olevan pilvipalveluun sijoitettavan tietojärjestelmänsä suojausten riittävyyttä turvallisuusluokittelemattoman salassa pidettävän tiedon käsittelyyn.

Viranomais A on tunnistanut tiedonhallintalain ja PiTuKrin vaatimusten välillä seuraavat A:n järjestelmäympäristöön kohdistuvat yhteydet:

- 12 §: Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen: HT-02 (Henkilöstön luotettavuuden arviointi); HT-03 (Salassapito- ja vaitiolositoumukset)
- 14 §: Tietojen siirtäminen tietoverkossa: SA-02 (Salaus fyysisesti suojatun turvallisuusalueen ulkopuolella) / Kohdat 1-2; SA-01 / Kohdat 1-2.
- 16 §: Tietojärjestelmien käyttöoikeuksien hallinta: IP-01 (Käyttöoikeushallinta)
- 17 §: Lokitietojen kerääminen: JT-01 (Jäljitettävyys ja havainnointikyky) / kohdat 1-3
- 21 §: Tietoaineistojen säilytystarpeen määrittäminen (tuhoaminen säilytysajan päätyttyä): SI-02 (Tietoaineistojen tuhoaminen)

Tiedonhallinnan järjestämiseen (4 §) soveltuu keskeisesti järjestelmäympäristöön liittyvien vastuiden määrittely vaatimuskortissa TJ-02 (Turvallisuuden vastuut), ajantasaisten ohjeiden järjestäminen vaatimuskortissa HT-04 (Turvallisuustietoisuus) sekä valvonta vaatimuskortissa TJ-07 (Vaatimustenmukaisuus ja tietosuoja). Toisaalta tietojenkäsittelyyn liittyvien riskien tunnistamiseen ja tietoturvallisuustoimenpiteiden riskienarviointipohjaiseen mitoittamiseen soveltuu suoraan vaatimuskortti TJ-03 (Turvallisuusriskien hallinta).

Viranomais A on lisäksi tunnistanut omassa riskienhallinnassaan (13 §), että esimerkiksi riittävän vikasietoisuuden ja toiminnallisen käytettävyyden saavuttamiseksi pystytään hyödyntämään vaatimuskortteja TJ-05 (Jatkuvuudenhallinta), KT-03 (Varmistus- ja palautusprosessit), MH-01 (Muutostenhallinta) ja MH-02 (Järjestelmäkehitys), kuten myös TT-02 (Yleisiä verkkohyökkäyksiä vastaan suojautuminen). Tietoturvallisuuden tilan seuranta (13 §) tukee suoraan JT-01 (Jäljitettävyys ja havainnointikyky). Toisaalta esimerkiksi elinkaaren kestävään suojaukseen liittyy oleellisesti KT-04 (Haavoittuvuuksien hallinta) ja SI-02 (Tietoaineistojen tuhoaminen). Toisaalta A on tunnistanut, että käyttöoikeushallinto edellyttää luotettavasti toimiakseen myös käyttäjätunnistusta (IP-02), ja toisaalta esimerkiksi järjestelmän haavoittuvuusvaruuden pienentämiseksi verkkotekniset rajoitukset (TT-01) ja järjestelmäkovennukset (JT-02) ovat riskiperusteisesti välttämättömiä. Koska järjestelmän turvallisuus nojaa suoraan hallintayhteyksien suojauksiin (IP-03), myös nämä A näkee kriittisiksi järjestelmältä edellytettäviksi suojauksiksi.

Viranomais A on riskienarvioinnissaan (13 §) lisäksi tunnistanut, että tietoaineistojen turvallisuuden luotettava varmistaminen (15 §) edellyttää myös fyysisen turvallisuuden (FT-01 - FT-05) huomioimista soveltuvin osin. Jotta viranomais A pystyy saamaan varmuutta turvallisuustyön jatkuvuudesta ja ylläpidosta, myös turvallisuusjohtamisen osa-alue on hyödynnettävissä soveltuvin osin.

Viranomais A on riskienhallinnassaan tehnyt tietoisin valinnan siitä, että mikäli kehitettävä tietojärjestelmä olisi myöhemmin tarpeen siirtää toiseen pilvipalvelualustaan, tämä voisi aiheuttaa merkittäviä kustannuksia ja edellyttää järjestelmän uudelleenrakennusta merkittävässä määrin. A hyväksyykin siirrettävyyteen liittyvät riskit, ja ei sovelta esimerkiksi vaatimuskorttia SI-01 (Siirrettävyys) tähän kyseiseen järjestelmään.

LIITE 3 PiTuKri: Jatkoarvioinnin mahdollisuudet

Taulukko 2. Jatkoarvioinnin mahdollisuudet.

Tietotyyppi	Pilvipalvelu- tyyppi	Fyysinen sijainti	Palvelun- tarjoaja	Lisätietoja
Julkinen	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Soveltuvien suojausten arvioinnissa painotus riittävän eheyden ja saatavuuden varmistamisessa.
Salassa pidettävä	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Mikäli ei sisällä henkilötietoja. Mikäli sisältää, vertaa riviin "Henkilötieto" alla. Tulee myös huomioida, että tiedonhallintalain (906/2019) 13 § edellyttää riskien tunnistamista ja suojausten mitoittamista riskienarvioinnin mukaisesti. Viranomaisen riskienarvioinnin tulokset voivatkin edellyttää kattavampia suojaus- tai rajoituksia, kuin mihin PiTuKri:ssä otetaan kantaa.
Henkilötieto	Ei rajoitteita	Tietosuoja-sääntelyn mahdollistamat alueet, usein esim. EU/ETA	Ei rajoitteita, ellei kyseisiin henkilö-tietoihin liittyvän riskienarvioinnin perusteella rajoituksia	Palvelukokonaisuuden tulee täyttää henkilötietojen suojaamiseen liittyvä erityislainsäädäntö. Henkilötietojen käsittely edellyttää tietojen luonteen perusteella tehtävää riskiarviointia, mistä voi seurata rajoitteita myös tietojen fyysisen sijainnin, tietojen hallinnoinnin ja palveluntarjoajan valintaan.
Varautumisen näkökulmasta suojattavat tiedot	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon kohdistuu tarve olla käytettävissä myös poikkeavissa olosuhteissa (varautuminen). Tiedon hallinnoinnin oltava mahdollista tilanteessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana).
TL IV	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana).
Suuri määrä salassa pidettävää tai/ja henkilötietoa (TL IV -kasauma)	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana).
Kansainvälinen RESTRICTED (KV-R)	Yksityinen/ yhteisö	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana). Suojaamisessa huomioitava ko. tietoon kohdistuvat tiedon originaattorin tai/ja omistajan asettamat erityisvaatimukset. Vrt. Katakri 2015.
Suuri määrä salassa pidettävää tietoa tai/ja TL IV -tietoa tai/ja henkilötietoa (TL III -kasauma)	Yksityinen/ yhteisö ³⁴	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana). Kasautumisvaikutuksessa huomioitava menetelmät, joilla rajataan pääsy vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, ja joilla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä havaitaan. Kun arviointityökaluna käytetään PiTuKria, tulisi kasautumisvaikutus tulkita siten, että TL IV -vaatimusten lisäksi suojausilta edellytetään tietovarannon fyysiselle suojaukselle turva-alueita (FT-01), erityistä luotettavuutta erottelutoteutukselle (JT-03) sekä sovelluskerroksen turvallisuudelle (MH-02 / kohta 1), tehostettua jäljitettävyyttä ja havainnointikykyä (JT-01 / Kohdat 1f-g ja 4e) sekä tehtävien luotettavaa erottelua (HT-05 / kohta 5). Vrt. Katakri 2015 (I 01 / Lisätietoja / Kasautumisvaikutus).
TL III ja TL II	Yksityinen/ yhteisö	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana). Huomioitava turvallisuusluokan III tai/II lisäsuojausvaatimukset ³⁵ , vrt. Katakri 2015.

³⁴ Yhteistopilvi (community/government cloud) tietyin rajoituksin, esimerkiksi valtionhallinnon tai muun viranomaisyhteisön käyttöön rajattu palvelu.

³⁵ Käytännön toteutusmallina yleensä pilviteknologian käyttö fyysisesti suojattujen turva-alueiden sisällä siten, että kyseinen turvallisuusluokan III/II käsittely-ympäristö on kokonaisuudessaan fyysisesti ja loogisesti luotettavasti eriytettyä muista ympäristöistä.