Azure Information Protection -palvelun käyttöönotto Fidalle

Robert Hakola

2019 Laurea

Laurea-ammattikorkeakoulu

Azure Information Protection -palvelun käyttöönotto Fidalle

Robert Hakola
Tietojenkäsittelyn tradenomi
Opinnäytetyö
Toukokuu 2019

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Robert Hakola

Azure Information Protection -palvelun käyttöönotto Fidalle

Vuosi 2019 Sivumäärä 42

Tässä toiminnallisessa opinnäytetyössä kuvattiin projekti, jossa suunniteltiin ja parannettiin Fida International Ry:n tietoturvaa EU:n yleisen tietosuoja-asetuksen eli GDPR:n myötä tulleiden vaatimusten takia. Kehittämistehtävänä otettiin AIP (Azure Information Protection) -palvelu käyttöön Fidan työympäristöön Windows 10-, MacOS- ja Android -laitteille. AIP:in tehtävänä on parantaa organisaation tietoturvaa suojaamalla halutut tiedostot ja sähköpostit.

Opinnäytetyön teoreettinen viitekehys sisältää työn tekemisen kannalta keskeisimpiä käsitteitä ja käytettyjä menetelmiä. Teoriaosuudessa huomioidaan myös AIP -konfiguraatio asetukset yleisellä tasolla, joka auttaa lukijaa hahmottamaan käyttöönottoprojektia.

Työn tietoperustana käytettiin alan kirjallisuuttaa ja sähköisiä julkaisuja. Tärkeässä osassa olivat organisaation palveluksessa olevien henkilöiden ja ulkoisten palveluntarjoajien asiantuntemus. Työssä käytettiin teknistä dokumentaatiota ja osallistuvaa havainnointia.

Työn tuloksena saatiin organisaatiolle tietoturvaa parantava suojattu sähköposti käyttöön OWA:n (Outlook Web App) avulla. Työssä onnistuttiin Windows 10 -laitteille ottamaan AIP -palvelu onnistuneesti käyttöön, mutta MacOS- ja Android -laitteille käyttöönotto ei onnistunut. Tästä huolimatta organisaatio sai käyttöönotosta tärkeää informaatiota jatkokehittämistä ajatellen.

Asiasanat: Azure, pilvipalvelu, tietoturva, suojaus

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Robert Hakola

Azure Information Protection service deployment to Fida

Year 2019 Pages 42

This thesis was an outline of a project that was made for Fida International organization, in order to plan and improve their information security. The reason for improvements was due to general data protection regulations by the EU. Azure Information Protection (AIP) service was chosen to be deployed in Fida's work environment that includes Windows 10, MacOS and Android devices. The function of AIP is to improve security on chosen files and emails.

The theoretical framework of the thesis discussed the foundation for the concepts and methods that allow the work to be done. The theoretical part took into account the configurations of the AIP settings in the basic level thus allowing the reader to understand the deployment project better.

The knowledge base was gathered using professional literature and electronical publications. Consultants and Fida staff's expertise played a vital role in the project. Technical documentation and observation were also applied.

Information security was improved for the organization by deploying a secure email via Outlook Web App (OWA). The project was successful with Windows 10 devices but MacOS and Android devices failed to work with AIP services. Fida International gained important information for the future development of their data security.

Keywords: Azure, cloud service, information security, protection

Sisällys

1 Johdanto

Tämän opinnäytetyön toimeksiantajana on Fida International ry ja kehittämistyön aiheena on Azure Infromation Protection -palvelun käyttöönotto Fidalle. Kehittämistyö valittiin yhdessä toimeksiantajan kanssa ja sen katsottiin hyödyntävän merkittävästi organisaation nykyistä tietoturvaa tiedostojen ja sähköpostin suojauksella. Valinnan taustalla oli EU:n yleisen tietosuoja-asetuksen eli GDPR:n myötä tulleet vaatimukset. Kehittämistyön haluttiin mahdollistavan CYOD:in (Choose your own device) ja tulevaisuudessa BYOD:in (Bring your own device) käyttöönotto.

Kehittämistyön tarkoituksena on esitellä Microsoftin AIP (Azure Information Protection) palvelu. Esittelyn lisäksi työssä tullaan kuvamaan järjestelmän käyttöönottoprojekti. Kehittämistyö tullaan rajamaan Windows 10, MacOS ja Android käyttöliittymiin. Opinnäytetyössä esitellään Fidan nykyistä työympäristöä yleisellä tasolla. Opinnäytetyössä ei kerrota täysin tarkkaa kuvaa Fidan tietoturvakäytänteistä ja AIP:in -konfiguraatio asetuksia, koska ne voisivat vaarantaa toimeksiantajan tietoturvaa.

Käyttöönottoprojektissa tullaan käymään läpi eri vaiheet AIP:n käyttöönotosta. Tässä työssä pyritään kuvaamaan mahdollisimman yksityiskohtaisesti, miten AIP asennetaan ja otetaan käyttöön päätelaitteilla. Käyttöönoton eri vaiheita esitetään kuvakaappauksilla ja samalla selitetään mitä kyseisessä kohdassa tehtiin ja huomioitiin.

Käyttöönottoprojekti on luonteeltaan kehittämistutkimus. Menetelmänä työssä on käytetty osallistuvaa havainnointia.

2 Opinnäytetyön lähtökohdat

Organisaatiossa halutaan pitää tietoturva-asiat ajan tasalla ja tämä käyttöönottoprojekti käynnistyi EU:n yleisen tietosuoja-asetuksen eli GDPR:n vaatimusten takia. Lähdin toteuttamaan käyttöönottoprojektia ollessani työharjoittelussa Fida International ry:ssä keväällä 2018.

2.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimii Fida International ry, joka on suomalainen vuodesta 1927 toiminut lähetys- ja kehitysyhteistyöjärjestö. Fida toimii lähes 50 maassa ja erityisenä tavoitteena on parantaa kaikista vaikeimmassa asemassa olevien lasten oikeuksia. (Fida International Ry.)

Fidalla on noin 190 työntekijää kotimaassa sekä ulkomailla kehitysyhteistyön ja humanitaarisen avun asiantuntijoina. Ulkomaan hankkeissa työskentelee noin 300 paikallista henkilöä. (Fida International Ry.)

Fidan laitteistoista, ohjelmista ja tietoturvasta vastaa hallinto-osaston ICT-tiimi. Tiimissä on tietohallintopäällikön lisäksi yksi ICT-lähitukihenkilö. Tiimin lisäksi Fidalla on IT-kumppani, joka on ICT-tiimin tukena. Organisaatiossa on noin 130 tietokonetta ja mobiililaitetta, joista ICT-tiimi vastaa.

2.2 Toimeksianto

Tämän opinnäyteyön aiheena on Fida Internatioal Ry:n tietoturvan kehittämisprojekti. Projektin tarkoituksena on ottaa käyttöön Mircrosoftin tarjoama palvelu nimeltä AIP (Azure Information Protection). AIP:n käyttöönoton tulisi kehittää Fidan tietoturvaa tiedostojen ja sähköpostin tasolla, EU:n yleisen tietosuoja-asetuksen tulleiden vaatimusten takia. Sen tulisi mahdollistaa CYOD (Choose your own device) ja tulevaisuudessa BYOD (Bring your own device) käyttöönotto organisaatiossa.

Ollessani työharjoittelussa olin mukana kehittämässä ja työskentelemässä erilaisissa tietoturvaprojekteissa. Päädyimme toimeksiantajan kanssa valitsemaan AIP:n käyttöönoton, koska siitä näimme olevan eniten hyötyä Fidan nykyisiin tarpeisiin ja se edistäisi GDPR:n mukana tulleita vaatimuksia paremmasta tietosuojasta, varsinkin sähköpostien osalta.

AIP on Microsoftin uusimpia Azure-palveluita ja siitä ei siksi löydy paljon tietoa. Toimeksiantaja halusi kuitenkin selvittää, miten AIP voitaisiin ottaa käyttöön Fidalla ja miten se toimisi eri alustoilla. Toimeksiantaja halusi selvityksen sen toiminnallisuuksista Fidan käyttöympäristössä.

2.3 Kehittämiskohteen kuvaus

Fidan käyttämä nykyinen Office 365 -ympäristö ja lisenssit (Microsoft Enterprise Mobility + Security E3 ja Office 365 ProPlus) mahdollistavat AIP:n käyttöönoton. Nykyisessä ympäristössä Fidalla on Windows 10 -tietokoneita, Android -laitteita ja MacOS -tietokoneita. Office -tiedostoja ei ole oletusarvoisesti salattu ja sähköpostissa käytetään yleistä TLS-salausta.

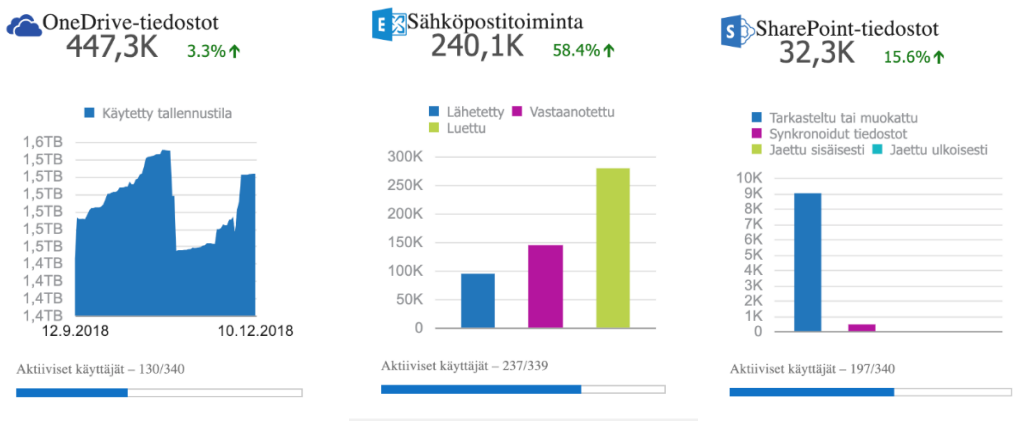
Seuraavissa kuvioissa esitellään toimeksiantajan käytössä olevilta Office 365 -käyttäjiltä saatua informaatiota OneDrive-tiedostoista, sähköpostitoiminnasta ja SharePoint-tiedostoista. Tarkkailun kohteeksi valittiin kaikista oleellisimmat käyttöönottoon liittyvistä tiedoista, jotta saataisiin kuvaa siitä, miten paljon organisaatiossa liikkuu tiedostoja ja sähköposteja 90 päivän aikajaksolla (12.9.2018-10.12.2018).

OneDrive-tiedostoja oli 130 aktiivisella käyttäjällä tarkastelujakson aikana käytössä noin 447 000. Tiedostojen tallennuksessa oli noin 3,3 % nousu. (Kuvio 1.)

Fidan käytössä olevien aktiivisten käyttäjien toimesta lähetettiin sähköpostiviestejä saman tarkastelujakson aikana noin 95 000, vastaanotettuja sähköpostiviestejä oli noin 145 000 ja

sähköpostiviestejä luettiin yhteensä noin 280 000 kertaa. Luku 240 000 koostuu lähetettyjen ja vastaanotettujen summasta. (Kuvio 1.)

Käyttäjät ovat tarkastelleet, muokanneet, synkronoineet, jakaneet sisäisesti tai ulkoisesti tiedostoja noin 32 300 kertaa saman tarkastelujakson aikana. (Kuvio 1.)



Kuvio 1: Käytettyä tallennustilaa OneDrive-tiedostoissa, SharePoint-tiedostojen käyttödataa ja sähköpostitoimintaa lähetetyistä, vastaanotetuista ja luetuista sähköpostiviesteistä.

2.4 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tämän kehittämistyön tavoitteena on Fida International ry:n tietoturvan kehittäminen EU:n yleisen tietosuoja-asetuksen eli GDPR:n myötä tulleiden vaatimusten takia. Siihen pyritään ottamalla käyttöön tiedostojen ja sähköpostien parempi salaus Microsoft AIP:in avulla. Käyttöönoton tavoitteena on myös mahdollistaa CYOD (Choose your own device) käyttöönotto Fidalla entistä tietoturvallisemmin ja mahdollistaa tulevaisuudessa BYOD (Bring your own Device) käyttöönotto. Kehittämistyön tavoitteena on parantaa tietoturvaa salaamalla tiedostot ja sähköpostit siten, että esimerkiksi johtoryhmän, hallituksen ja henkilöstöyksikön tiedostoihin ei ole pääsyä muilla, kuin niillä henkilöillä, jotka tarvitsevat niitä työskentelyyn. Tiedostoihin ja salattuihin sähköposteihin ei olisi pääsyä muilla Fidan työntekijöillä kuin ainoastaan ryhmään kuuluvilla henkilöillä. Näistä oikeuksista vastaisivat Fidan järjestelmänvalvojat. Tavoitteena on myös salata ulkopuolisille lähetetyt arkaluontoiset sähköpostiviestit AIP:n tarjoaman suojatun sähköpostin avulla.

Opinnäytetyön tutkimusongelmana on se, että voidaanko AIP ottaa käyttöön ja mitä se vaatii Fidan käytössä olevilta Windows 10 -tietokoneilta, Android -laiteilta ja MacOS -tietokoneilta. Tutkimuksen tavoitteena on myös tehdä selvitys suojatun sähköpostin toimivuudesta Fidan käyttöympäristössä ja sen ulkopuolelle lähetetyissä sähköposteissa.

2.5 Aihealueen rajaus

Kehittämistyö rajataan Windows 10 Pro -(versio 1709 ja uudemmat), MacOS -(High Sierra versio 13.3.3 ja uudemmat) ja Android -(Oreo 8.0 ja uudemmat) käyttöliittymiin. Työssä tarkastellaan vain Fidan toimistolla työskentelevien tietokoneita ja mobiililaitteita, joita on yhteensä noin 60.

Opinnäytetyössä esitellään Fidan nykyistä työympäristöä ja yleisesti Fidan tietoturvakäytänteitä. Tietoturvasyistä opinnäytetyössä ei kerrota täysin tarkkaa kuvaa Fidan käytänteistä, tietosuojasta ja AIP:n asetuksista, jotta Fidan tietoturva ei vaarantuisi. AIP:n konfiguraatio asetuksia tullaan kuvamaan yleisellä tasolla. Työssä ei myöskään käsitellä GDPR-asetusta tai tietosuojaa.

2.6 Keskeiset käsitteet

Microsoft Azure	Microsoftin tarjoama pilvipalvelu alusta (Bergius 2014).
GDPR	EU:n yleinen tietosuoja-asetus, jonka tavoitteena on mm. parantaa yksilöiden henkilötietosuojaa organisaatioiden pitämissä rekistereissä, tiedostoissa jne. (Tietosuojamalli).
Azure Information Protection (AIP)	Arkaluontoisten tietojen suojaamiseen ja jakamiseen palvelun avulla (Microsoft 2018a).
AIP label	Tiedoston tai sähköpostin suojaus tason valitseminen AIP palveluun luoduilla leimoilla (Microsoft 2018a).
Pilvi	Verkossa oleva tieto, ohjelma tai palvelu (Kangasniemi & Lintulahti, 2017).
Pilvipalvelu	Palvelimia, jotka toimivat verkossa (Murugesan & Bojanova 2016, 54).
Suojattu sähköposti	Azure Information Protectionissa tuleva lisäpalvelu, jolla voidaan lähettää turvallisesti sähköposteja organisaation sisällä ja ulkopuolelle (Microsoft 2019e).

Outlook Web App (OWA)	Selaimessa toimiva Microsoftin sähköpostipalvelu sähköpostin lukemiseen ja lähettämiseen (Microsoft Office).

3 Pilvipalvelu

Pilvipalvelut ovat yleiskielellä internetistä hankittua tietokonekapasiteettia, sovelluksia, tai muita palvelusuoritteita. Alalla toimivat ammattilaiset pitävät kuitenkin tärkeänä, miten määritellään, mikä on pilvipalvelu ja mikä ei. Ilmiö on muutakin kuin pelkkä uusi palvelu. Se on myös kokonaan uusi toimintapa. ”Cloud Computing” voidaan esitellä niin, että se on toimintamalli, jonka kautta olisi mahdollista luopua fyysisistä konesaleista. (Heino 2010, 32.)

On kyseessä sitten laskennallinen tietokonepalvelu tai verkkoresurssi, ohjelmisto tai mikä muu tahansa IT-palvelu, jonka tarjoajana käyttäjälle on pilvi, on tällöin kyseessä pilvipalvelu (Murugesan & Bojanova 2016, 54).

Pilvipalvelu on ylikuormitettu terminä, koska se sisältää kaikenkokoisia infrastruktuureja, joilla on eri tyyppiset hallintamenetelmät ja erikokoisia käyttäjämääriä. Tästä syystä useita pilvityyppejä on suunniteltu:

Public Cloud (Julkinen Pilvi): Julkinen pilvi on kaikista yleisin ja eniten tunnettu pilvimuoto ja se on kaikille avoin. Julkisia pilviä tarjotaan mallilla, jossa maksetaan käytön mukaan. Jotkut pilvipalvelut ovat myös tarjolla ilmaiseksi. (Murugesan & Bojanova 2016, 57.) Tämä infrastruktuuri on tehty suurelle yleisölle tai laajalle teollisuuskonsernille ja sen omistaa organisaatio, joka pitää yllä pilvipalveluita (Marinescu 2013, 9.)

Private Cloud (Yksityinen Pilvi): Tätä Infrastruktuuria käytetään yksinomaan organisaatioille. Organisaatio tai myös kolmas osapuoli voi hallita palvelua ja se voidaan sijoittaa joko organisaation sisäisiin tai ulkopuolisiin tiloihin (Marinescu 2013, 9.)

Virtual Private Cloud (Virtuaalinen Yksityinen pilvi): Virtuaalinen yksityinen pilvi on osa julkista pilveä, mutta se on määritelty käyttäjälle sen tarpeiden mukaan lisäämällä sinne lisä sääntöjä ja ominaisuuksia kyseisen käyttäjän tarvitsemien erityisvaatimusten turvallisuuden ja määräystenmukaisuuden täyttämiseksi organisaatiossa. Virtuaalinen yksityinen pilvi tarjoaa käyttäjälle enemmän hallintavaltaa käyttämiinsä resursseihin kuin pelkkä julkinen pilvi. (Murugesan & Bojanova 2016, 57.)

Community Cloud (Yhteisö Pilvi): Tämän infrastruktuurin jakaa useat eri organisaatiot ja se ylläpitää tiettyyn alaan erikoistuneita organisaatioita, joilla on yhteinen asia (esimerkiksi missio, tietoturvavaatimukset, toimintaperiaatteet ja lain ja ohjeiden noudattamisen näkökohdat). Palvelua voidaan hallita organisaatiokohtaisesti tai kolmannen osapuolen toimesta. Se voi sijaita niiden tiloissa tai ulkopuolella. (Marinescu 2013, 9.)

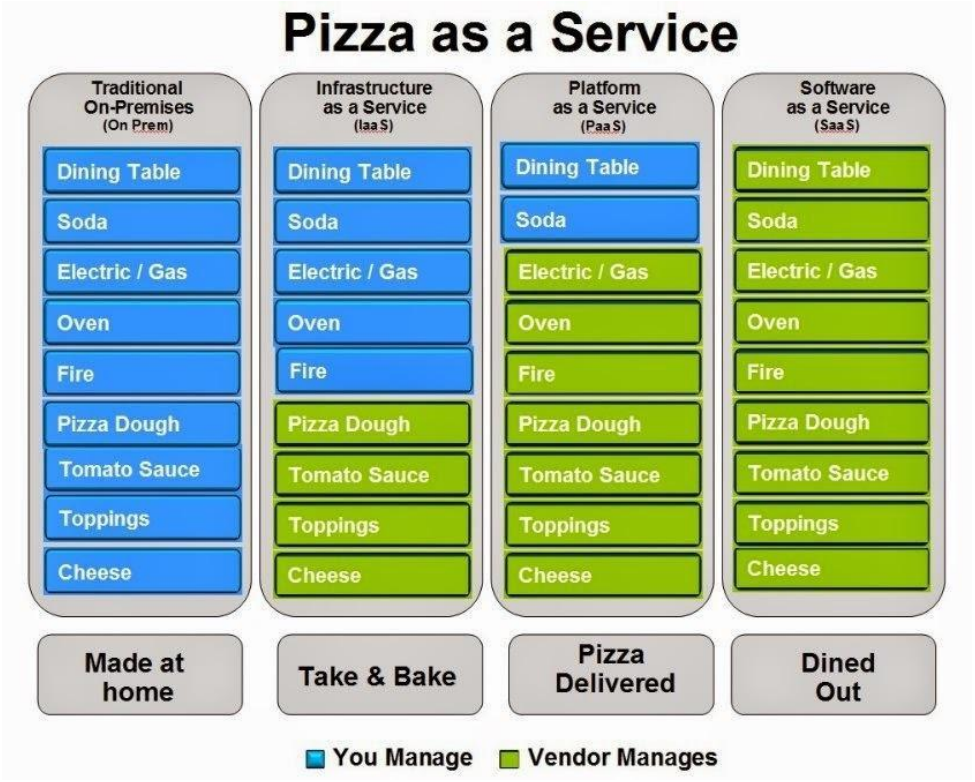
Hybrid Cloud (Hybridi pilvi): Hybridi pilvi on kahden tai useamman yllä esitetyn pilven yhdistelmä. Ne pysyvät ainutlaatuisina kokonaisuuksina itsessään, mutta ne ovat yhteydessä toisiinsa standardoidun tai patentoidun tekniikoiden kanssa, joka mahdollistaa tietojen ja sovellusten siirrettävyyden palveluiden välillä (esimerkiksi ”cloud bursting” joka jakaa tietokuormaa pilvipalveluiden kesken). (Marinescu 2013, 9.) Hybridimalli mahdollistaa valikoivan toteutuksen organisaation eri huolenaiheista liittyen turvallisuuteen, määräysten mukaisuuteen ja hallinnan menettämiseen ja samalla se mahdollistaa kustannustehokkaan julkisen pilven käyttöönoton, jossa on myös enemmän sovellus vaihtoehtoja (Murugesan & Bojanova 2016, 57-58).

3.1 Cloud Service Models (Pilvipalvelumallit)

Pilvipalvelumalleja on kolmen tyyppisiä: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) ja Software as a Service (SaaS). Jokainen pilvipalvelumalli antaa abstraktiotason, joka auttaa ja ottaa pois taakkaa palvelun käyttäjältä erityisesti silloin, kun ollaan rakentamassa ja ottamassa käyttöön järjestelmiä (Kavis 2014, 31).

Perinteisessä datakeskuksessa IT-tiimin tehtävänä on rakentaa ja hallita kaikkea. Omia ratkaisuja kehittelevien ja kaupallisia palveluja ostavien yritysten on asennettava ja hallittava monia palvelimia, sekä kehitettävä ja asennettava uusia ohjelmistoja. Niiden yritysten tulee varmistaa, että asianmukaiset tietoturvatasot laitetaan käytäntöön ja asennettava tietosuojakorjauksia jatkuvasti (esimerkiksi käyttöjärjestelmiin, laiteohjelmistoihin, sovelluksiin, tietojärjestelmiin ja tietokantoihin). Jokainen pilvipalvelumalli tarjoaa abstraktiotason ja automaation näille tehtäville. Tämä helpottaa ja nopeuttaa yrityksiä käyttämään enemmän aikaa ydintoiminnan kehittämiseen ja vähemmän aikaa infrastruktuurin hallitsemiseen (Kavis 2014, 31).

Pizza as a service -mallin (Pizza palveluna) avulla voidaan havainnollistaa pilvipalvelumalleja. ”Traditional On-Premises” (Perinteinen paikallinen) on palvelu, jossa kaikki tehdään itse ”taikinasta” lähtien. IaaS palvelussa noudetaan valmiiksi tehty ”taikina”, ”kastike”, ”päällysteet” ja ”juusto”, mutta loput hoidetaan itse. PaaS palvelussa käytännössä käyttäjälle toimitetaan kaikki kotiin, mutta edelleen hoidettavaksi jäävät esimerkin mukaan ”ruokapöytä” ja ”juoma”. SaaS palvelussa hoidetaan kaikki, vain ”syöminen ulkona” jää hoidettavaksi. (Kuvio 2.)



Kuvio 2: Pizza as a service -malli havainnollistaa yksinkertaisella menetelmällä On Prem, IaaS, PaaS ja SaaS -palveluita. (Episerver)

3.1.1 Infrastructure as a Service (IaaS)

IaaS (infrastruktuuri palveluna) -pilvi on raaka tietokoneinfrastruktuuri, kuten palvelimet, keskussuoritin, tallennustila, verkkolaitteet ja palvelinkeskustilat ja ne toimitetaan palveluna kysynnän mukaan. Näiden resurssien ostamisen sijaista käyttäjät saavat ne täysin ulkoistettuina palveluina, niin pitkän aikaa kuin niitä tarvitaan. Palvelu laskutetaan resurssien käytön mukaan. (Murugesan & Bojanova 2016, 55.)

Käyttäjä voi hyödyntää ostamiaan palveluita ottamalla käyttöön omavalintaisia ohjelmistoja, jotka voivat sisältää käyttöjärjestelmiä ja sovelluksia (Kuvio 2.) Käyttäjä ei itse hoida tai hallitse alustana toimivaa pilvi-infrastruktuuria, mutta hallitsee käytössä olevia käyttöjärjestelmiä, talletustilaa ja käyttöönotettuja sovelluksia ja mahdollisesti käyttäjällä on rajoitettu hallinta valikoiduista tietoliikennekomponenteista (esimerkiksi konekohtainen palomuuri) (Kavis 2014, 31.) Tämän tyyppistä pilveä myös kutsutaan hyötypilveksi tai infrastruktuuripilveksi (Murugesan & Bojanova 2016, 55).

3.1.2 Platform as a Service (PaaS)

PaaS (sovellusalusta palveluna) -mallissa alusta ja työkalut sovelluskehittämiselle ja väliohjelmisto järjestelmille isännöi kauppias. Kauppias tarjoaa sovelluskehittäjille yksinkertaisesti

sen, että he voivat koodata ja ottaa käyttöön sovelluksia ilman, että heidän tarvitsee olla vuorovaikutuksessa perustana olevan infrastruktuurin kanssa. (Kuvio 2.)

PaaS -mallinen alusta tarjoaa monia työkaluja ja palveluita, joita tarvitaan sovellusten rakentamiseen ja toimittamiseen. Lisäksi se tarjoaa palveluita, kuten työnkulkupalvelua sovellusten suunnitteluun, kehittämiseen, testaukseen, käyttöönottoon ja isännöintiin. (Murugesan & Bojanova 2016, 55.)

3.1.3 Software as a Service (SaaS)

SaaS (ohjelmisto palveluna) -pilviä voidaan kutsua ohjelmistopilvinä. Tässä mallissa ohjelmistoa isännöi pilvikauppias, joka toimittaa palvelun käyttäjälle yleensä internetin kautta tai omasta verkosta (Kuvio 2.)

SaaS poistaa tarpeen sovelluksien asentamiselta ja käyttämiseltä paikallisesti käyttäjän tietokoneelta. Se vapauttaa käyttäjän taakalta, joka tulee laitteiston ja sovelluksien ylläpidosta ja päivityksistä. Käyttäjä ei itse omista ohjelmiston lisenssiä ja käyttäjiä laskutetaan heidän käyttämiensä palveluiden käytön mukaan. Palvelun alkuun ei tule isoa kustannusta, vaan pikemminkin kustannukset koostuvat jatkuvasta palvelun laskutuksesta. (Murugesan & Bojanova 2016, 54-55.)

3.2 Microsoft Azure

Microsoft Azure Platform julkaistiin kaupalliseen käyttöön alkuvuodesta 2010 (Rizzo, Rais, Otegem, Bishop, Durzi, Tejada & Mann 2012, 39). Toimintaperiaatteiltaan Microsoftin tuote oli julkaisuvuonna pilvipalvelumallien mukainen (Salo 2010, 125).

Microsoftilla on useita organisaatiolle suunnattuja SaaS-pilvipalveluita ja niitä käytetään niille suunniteltuihin käyttötarkoituksiin. Esimerkkeinä Microsoftin SaaS-pilvipalveluista ovat muun muassa Office 365 (tietotyöläisen työkalut), CRM Online (asiakkuudenhallinta) ja Intune (laitehallinta). Azure poikkeaa näistä siinä, että se on enemmänkin alustapalvelu ja sen tavoitteeksi voidaankin katsoa pikemminkin, että se toimii kaikenlaisten sovellusten, palvelujen ja palvelimien alustana. ”Azure on siis yleiskäyttöinen alustapalvelu, joka tarjoaa sekä IaaS- (Infrastructure as a Service) että PaaS-tyyppistä (Platform as a Service) palvelua sovellusten alustaksi ja lisäksi vielä erilaisia lisäkomponentteja, joita voidaan hyödyntää laajentamaan Azuressa isännöitävien sovellusten toimintaa.” (Bergius 2014.)

Azure-komponentit voidaan asettaa karkeasti kolmeen eri ryhmään. Ensimmäisenä ovat varsinaiset alustapalvelut (palvelinkapasiteetti), toisena tallennuspalvelut ja kolmantena lisäpalvelut (Bergius 2014). Seuraavaksi käydään läpi varsinaisia alustapalveluita, johon kuuluu kolme eri palvelua (WebSites, Cloud Services ja Virtual Machines.)

3.3 Azuren alustapalvelut

WebSites -palvelu on tarkoitettu web-sivujen pyörittämiseen. Palvelu on hyvin yksinkertainen ja sitä pääsee käyttämään rekisteröitymällä portaaliin ja sieltä etsimällä kohdan Websites. (Keijo 2014) Palvelussa on mahdollista hyödyntää webissä yleisesti käytettyjä palvelimia esimerkiksi WordPress -palvelinta. WebSites palvelu on PaaS-tyyppinen palvelu ja sitä ajetaan Windows -alustalla, mutta siitä huolimatta palvelua voidaan hyödyntää monilla Microsoftista riippumattomilla ohjelmointikielillä, ohjelmointiympäristöillä ja lisäpalveluilla. (Bergius 2014.)

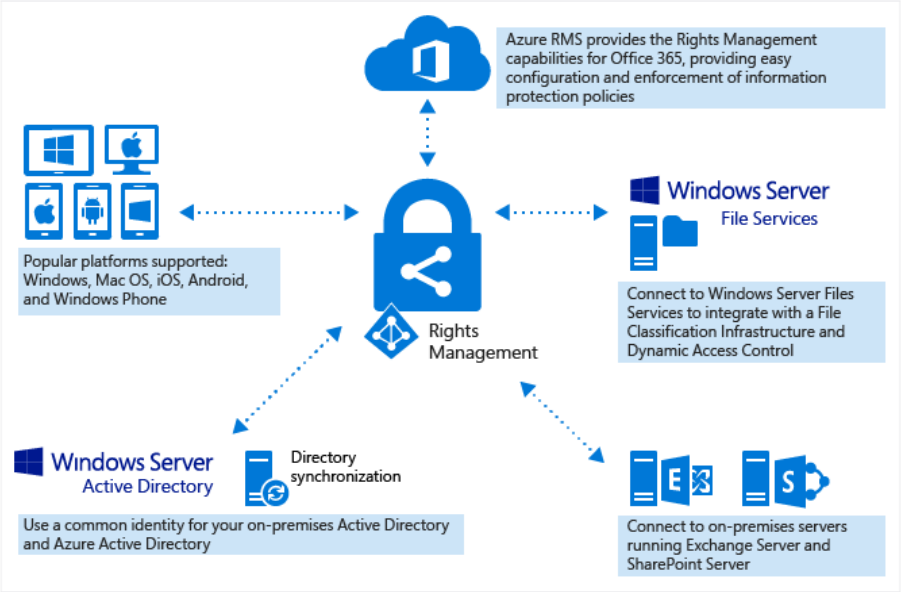
Cloud Service-palvelua voidaan hyödyntää Websovellusten alustana. ”Web Sites –palvelusta poiketen Cloud Services–palvelu on tarkoitettu sovelluksille, joissa käyttöliittymä ja sovelluksen logiikka on erotettu toisistaan.” Tässä tapauksessa kumpikin sijoitetaan omille palvelimilleen ja sitten tarpeiden mukaan palvelinryhmiä voidaan skaalata itsenäisesti. Cloud Service-palveluun perustuvissa sovelluksien toteutuksissa voidaan hyödyntää käyttämällä erityyppisiä ohjelmointikieliä, ohjelmointiympäristöjä, sekä siinä voidaan hyödyntää tietokantoja ja Azuren tarjoamia lisäpalveluja. Sovellus voidaan yhdistää organisaation sisällä muihin liiketoimintasovelluksiin. (Bergius 2014.)

Virtual Machine-palvelu mahdollistaa virtuaalikoneiden ajamisen Azuren palveluissa. Käyttäjän luodessa palvelua valitaan valmiiksi määritetyistä kapasiteettikokonaisuuksista (keskusyksiköiden ja keskusmuistien määrästä). Käyttäjä valitsee haluamansa tallennustilan määrän ja voi halutessaan valita perinteisen kovalevyn tai SSD -levyn, johon käyttäjän varsinaiset tiedot tallennetaan. ”Virtuaalikoneissa voidaan käyttää sekä Windows -palvelinkäyttöjärjestelmää, että Linuxin eri variaatioita ja lisäksi virtuaalikoneisiin on saatavilla erilaisia palvelinsovelluksia valmiina paketteina.” (Bergius 2014.)

3.4 Azure Rights Management

Azure Rights Management (Azure RMS) on suojausteknologia, jota AIP käyttää. Azure RMS on pilvipohjainen suojauspalvelu ja se käyttää salaus-, identiteetti- ja valtuutuskäytänteitä auttaakseen käyttäjää suojamaan tiedostoja ja sähköposteja, sekä se toimii useiden laitteiden kanssa (puhelimet, tabletit ja tietokoneet). Tieto voidaan suojata sekä organisaation sisällä tai sen ulkopuolella, koska suojaus pysyy tiedostossa, vaikka suojattu tiedosto lähtisi organisaation ulkopuolelle (Microsoft 2018c).

Azure RMS:ää voidaan hyödyntää Office 365 -palvelussa ja se mahdollistaa helpon konfiguraatio ja toimeenpanon AIP:n politiikoille. Sitä voidaan myös hyödyntää Windows Server tiedostopalvelussa, on-premises palvelimilla sekä Windows Serverin Active Directoryn tunnistautumisessa. Azure RMS tukee myös useita suosittuja alustoja: Windows, Mac OS, iOS, Android sekä Windows puhelimia. (Kuvio 3.)

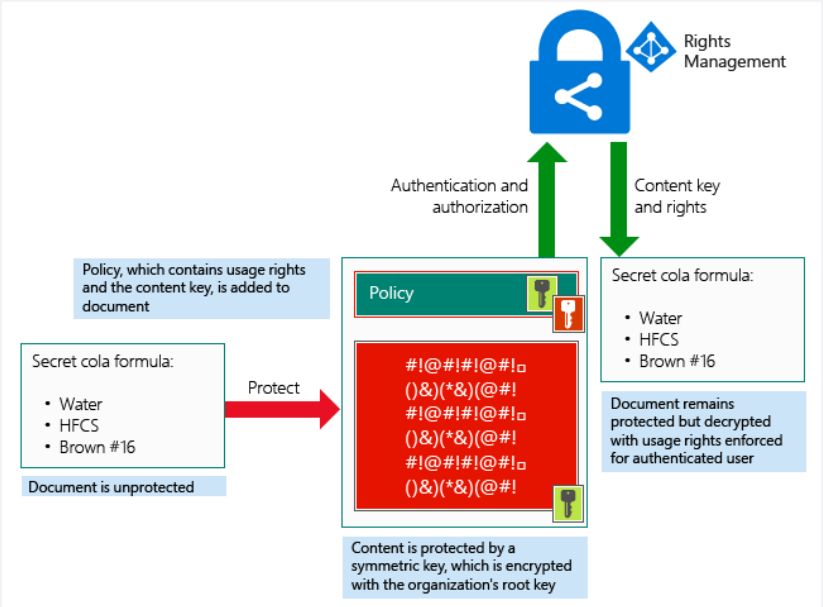


Kuvio 3: Rights Management palvelun eri hyödyt. (Microsoft)

Tärkeä huomioon otettava asia Azure RMS:n toiminnassa on se, että palvelu AIP:ssa ei näe, eikä varastoi käyttäjän tietoja osana suojausprosessia. Suojattavia tietoja ei koskaan lähetetä tai varastoida Azure-palveluun, ellei erityisesti niitä haluta tallentaa tai käytetä toista pilvipalvelua, joka varastoi tiedot Azureen. Azure RMS yksinkertaisesti tekee tiedot dokumentissa lukukelvottomiksi kaikille paitsi sallituille käyttäjille ja palveluille. (Microsoft 2019a.)

Tiedot ovat salattuja sovellustasolla ja se sisältää politiikat, jotka määrittelevät valtuudet käyttää dokumenttia. Silloin kun salattua dokumenttia käyttää oikeudet omaava käyttäjä tai se siirtyy luotetulle palvelulle dokumentin salaus puretaan ja oikeudet, jotka ollaan määritelty politiikoissa, vahvistetaan (Microsoft 2019a).

Seuraavan kuvion avulla havainnollistetaan, miten suojaus tapahtuu korkealla tasolla. Dokumentti, joka on suojattu sisältää salaisen kaavan (Secret formula) ja sitten se avataan onnistuneesti valtuutetun käyttäjän tai palvelun pyynnöstä. Dokumentti on suojattu sisältöavaimella (vihreä avain tässä kuviossa). Tämä on uniikki jokaiselle dokumentille ja se asetetaan tiedoston ylätunnisteeseen ja suojataan käyttäjän Azure Information Protection haltijan juuriavaimella (Punainen avain kuviossa). (Kuvio 4.)



Kuvio 4: Azure RMS:n suojauksen prosessit. (Microsoft)

Microsoft voi generoida ja hallita käyttäjän haltija-avainta tai käyttäjä voi itse generoida ja hallita omaa avaintaan. Suojaus prosessin aikana ei koskaan lähetetä salaista kaavaa Azurelle. (Microsoft 2019a.)

3.5 Azure Information Protection (AIP)

AIP on Microsoftin uusimpia pilvipalveluita sähköpostien ja tiedostojen suojaamiseen eri organisaatioissa (Microsoft 2018a). Seuraavaksi esitellään AIP yleisesti. Lisäksi esitellään muutamia ominaisuuksia, joista voisi olla eniten hyötyä organisaatiolle. AIP -konfiguraatio esitetään käyttöönottokappaleessa.

3.5.1 AIP yleisesti

”Henkilötiedot kannattaa suojata järjestelmätason lisäksi myös tiedostotasolla. Tietoturvan kannalta paras ratkaisu on salata data hallintapalvelulla, joka mahdollistaa tietojen hallinnan ja salauksen tallennuspaikasta ja -välineistä riippumatta.” AIP palvelun avulla voidaan hallita ja valvoa dokumenttikohtaista käyttöä luomalla valmiita käytäntöjä, jotka salaavat tiedot automaattisesti. Se mahdollistaa valmiiden painikkeiden tuomisen Office -työkaluihin, joista käyttäjä voi valita haluamansa salauksen dokumentille ja sähköpostille. (Microsoft 2017.)

AIP:n useimmat ominaisuudet tarvitsevat Premium P1 (Microsoft Enterprise Mobility + Security E3) tai P2 (Microsoft Enterprise Mobility + Security E5) lisenssin. Premium P1 ja P2 lisensseissä ei ole paljon eroja. Isoin ja hyödyllisin ero P2 lisenssissä tulee siitä, että se mahdollistaa AIP -skannerin automaattisen luokittelun, leimaamisen ja suojauksen tuettuihin paikallisiin tiedos-

toihin, AIP skannerista kerrotaan luvussa 3.5.3. Suojattua sähköpostia voidaan hyödyntää organisaation Office 365 -lisenssillä, eikä se tarvitse käyttäjältä erikseen Premium -lisenssiä. (Microsoft Azure.)

3.5.2 Tietojen seuranta ja oikeuksien kumoaminen

Azure Infromation Protection mahdollistaa myös tiedoston käytön seuraamisen, eli sen avulla voidaan seurata, ketkä ovat käyttäneet tiedostoa. Seuraamisella mahdollistetaan oikeuksien kumoaminen halutulta käyttäjältä eli kun havaitaan henkilö, jolla ei tulisi olla enää pääsyä tiedostoon, voidaan tällöin häneltä evätä jatkossa pääsy siihen. Tämä tapahtuu tiedostojen seuraamissivustosta, joka kuuluu osaksi AIP -palvelua. Sivusto toimii tällä hetkellä Windows -tietokoneilla, MacOS -tietokoneilla sekä puhelimilla ja tableteilla. (Microsoft 2018b.)

Kun käyttäjällä on oikea lisenssi organisaatiossa, voidaan palvelua käyttää ja tällöin nähdä, ketkä ovat yrittäneet tunnistautumalla aukaista suojattuja dokumentteja oli kyseessä sitten onnistunut tai epäonnistunut yritys. Jokaisesta avaamisyrityksestä jää aikaleima ja siitä voidaan havaita käyttäjän sen hetkinen sijainti. Joissakin tapauksissa sijainti ei ole aina tarkka, koska esimerkiksi käyttäjällä voi olla avatessa suojattua dokumenttia käytössä VPN (Virtual Private Network) -yhteys tai heidän tietokoneellaan voi olla IPv6-osoite ja nämä estävät tarkan sijainnin määrittämisen. (Microsoft 2018b.)

3.5.3 AIP -skanneri

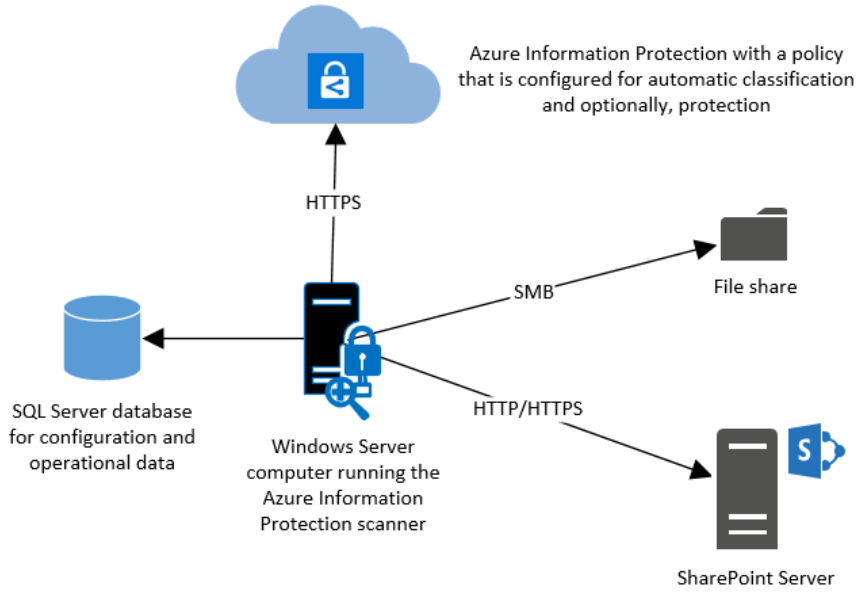
AIP tarjoama skanneri on ohjelma, joka on suunniteltu havaitsemaan, luokittelemaan ja vaihtoehtoisesti suojaamaan dokumentit, jotka ovat tallennettuna paikallisissa tiedostoissa ja Sharepoint-palvelimella (Kevin 2018).

AIP -skanneri tarvitsee toimiakseen Windows server 2016 tai Windows server 2012 R2:n. Testaukseen voidaan käyttää Windows käyttöjärjestelmää, jota AIP tukee. Tietokone voi olla fyysinen tai virtuaalikone ja se tarvitsee nopean ja luotettavan internetyhteyden toimiakseen. Skanneri vaatii ainakin 10 gigatavun vapaan tallennuskapasiteetin väliaikaisille tiedostoille ja neliydinprosessorin, jolloin se kykenee skannaaman 16 tiedostoa samanaikaisesti, jotka voivat olla kooltaan 625 MB. (Microsoft 2019b.)

Windows -palvelimen lisäksi tarvitaan Windows -käyttäjä, joka voi tunnistautua Azure AD:hen ja ladata sieltä AIP -politiikat. Tämän käyttäjän pitää olla Active Directory-käyttäjä ja sen pitää olla synkronoitu Azure AD:hen. Samalla tulisi luokitella asetus paikalliselle käyttäjälle oikeus sisäänkirjautumiseen. Tätä asetusta tarvitaan skannerin asentamiseen ja konfiguraatioon, mutta ei käyttämiseen. Se voidaan kytkeä pois päältä, kun käyttöönotto on suoritettu. Asetus palvelimen käyttäjän sisäänkirjautumiseen oikeus luokitellaan automaattisesti skannerin asennuksen yhteydessä ja tätä käyttäjää asetuksineen tarvitaan asennuksessa, konfiguraatiossa sekä skannerin käyttämisessä. (Microsoft 2019b.)

Kun käyttäjä on konfiguroinut AIP -politiikat leimoille, jotka luokittelevat tiedostot automaattisesti, voi käyttäjä aloittaa palvelun käyttämisen. Kun skanneri löytää tiedoston, se voi asettaa leiman, joka vastaa konfiguraatiossa asetettuja ehtoja. Leimoilla voidaan asettaa tiedostoihin luokitukset ja vaihtoehtoisesti asettaa haluttaessa myös suojaus. (Microsoft 2019b.)

Kuviossa 5 AIP -politiikat ovat määritelty ja skanneri toimii Windows -serveriltä. AIP -skanneri voi etsiä leimattavia ja suojattavia tiedostoja tiedoston jaosta, jotka ovat samassa verkossa ja SharePoint-serveriltä verkon yli. AIP -skanneri hakee konfiguroidut tiedot ja operatiivisen datan SQL -serverin tietokannasta.



Kuvio 5: AIP skanneri toiminnassa. (Microsoft)

4 Tutkimus- ja kehittämismenetelmät

Käyttöönottoprojekti on luonteeltaan kehittämistutkimus. Menetelmänä työssä on käytetty osallistuvaa havainnointia. Työssä käsitellään myös kerätyn tiedon validiteetit ja reliabiliteetit.

4.1 Kehittämistutkimus

Kehittämistutkimuksella tähdätään muutokseen. Kehittämistutkimus on yhdistelmä kvalitatiivista ja kvantitatiivista tutkimusta. Kehittämistutkimus voi olla pelkästään kvalitatiivista tutkimusta, jonka tavoitteena on muutoksen aikaansaaminen. (Kananen 2015, 39.)

Kehittämistutkimuksella pyritään siihen, että organisaatiossa tarvittava muutos saadaan aikaan. Perinteiseen ja laadulliseen tutkimukseen verrattuna kehittämistutkimuksella pyritään

myös ongelman poistamiseen. Perinteinen tutkimus päättyy ongelman ratkaisuun, mutta ongelman poistaminen ei kuulu siihen. Kehittämistutkimus alkaa siitä, mihin perinteinen tutkimus päättyy. (Kananen 2015, 40.)

Tutkija osallistuu kehittämistutkimukseen toimijana. Kehittämistutkimus on Kanasen mukaan kahdeksan vaiheinen. Vaiheet ovat: 1. Ongelman määrittely, 2. Ongelman tutkiminen, 3. Ongelman syiden ja seurausten analysointi, 4.Ratkaisun esittäminen, 5. Ratkaisun testaaminen, 6. Ratkaisun muokkaus testauksen pohjalta, 7. Uuden ratkaisun testaaminen/kokeilu ja 8. Johtopäätökset. (Kananen 2012, 53.)

4.2 Osallistuva havainnointi

Havainnointia voidaan pitää tärkeänä ja hyödyllisenä tutkimuksellisen kehittämistyön menetelmänä. Havainnoinnissa päästään tapahtumien luonnollisiin ympäristöihin, siksi havainnointi sopii hyvin kehittämistehtäviin. (Ojasalo, Moilanen & Ritalahti 2014, 114.)

Tutkijan läsnäolo tutkimustilanteessa tekee havainnoinnista osallistuvaa. Osallistuvassa havainnoinnissa tutkijan rooli on yleensä osallistua toimintaan. (Kananen 2012, 95.)

4.3 Kerätyn tiedon validiteetti ja reliabiliteetti

Kehittämistutkimuksen luotettavuutta ja laatua mittaavat reliabiliteetti ja validiteetti. Kehittämistutkimuksessa luotettavuuden mittaaminen on haasteellista, koska kysymyksessä ei ole oma tutkimusote, vaan kooste laadullisen ja määrällisen ongelman ratkaisusta. Siksi kehittämistutkimusta arvioidaan niiden menetelmien avulla, joita käytetään. Kun käytetään laadullista tutkimusta, käytetään sen luotettavuuden kriteeristoa. On tärkeää arvioida, onko kaikki tutkimuksen vaiheet tehty oikein. (Kananen 2012, 111.)

Mahdollisimman hyvä lopputulos on kehittämistutkimuksen tavoite. Suunnitteluvaiheessa tulee varmistaa tulosten oikeellisuus. Luotettavuutta ei voida tarkistella jälkikäteen, koska silloin toiminta olisi vain toteavaa. Kehittämistyön reliabiliteetti mitataan sillä, että muutos on seurausta käytetystä interventiosta, eikä muista tekijöistä. Validiteetilla tarkoitetaan taas sitä, että on tutkittu oikeita asioita. (Kananen 2012, 112.)

5 Toiminnallinen kehittämistyö Fidassa

Ollessani työharjoittelussa osallistuin Fidan tietoturvaa kehittäviin projekteihin. Osana näitä kartoitimme nykyistä tietoturvatasoa organisaatiossa. Tein itsenäistä tiedonhakua, jossa keräsin tietoa AIP:in toiminnallisuuksista ja siitä, miten sitä voitaisiin hyödyntää Fidan järjestelmiin. Kävimme Fidan tietohallintopäällikön kanssa palavereita käyttöönotosta ja hyödynsimme ulkopuolisia asiantuntijoita Fidan IT-kumppania ja suomalaista IT-konsultointi yritystä. Käyttöönottoprojektissa oltiin yhteydessä Microsoftin asiantuntijan kanssa.

5.1 Tietoturvakartoitus järjestelmäkortin avulla

Tietoturvakartoituksen yhteydessä käytiin läpi eri järjestelmiä ja palveluita Fidalla sovellus/järjestelmäkorttien avulla, joille annettiin pisteytys nykyisestä tilanteesta. Kohdista, joista ei saatu pisteitä, etsittiin parannuskohteita.

Fidan sovelluskortissa on eri tasoja, joiden mukaan edettiin tutkien nykyisten palvelujen/järjestelmien tietoturvaa. ”Kriittinen” -tasolta voitaisiin siirtyä ”Parannettavaa” -tasoon silloin, kun sovellus täyttää kaikki kohdat ”Käyttöoikeudet”, ”Tunnistautuminen”, ”Suojaus” ja ”Elpyminen”. Parannettavasta tasosta katsottiin edellä mainitut kaikki kohdat, että voitaisiin siirtyä seuraavalle tasolle eli ”Turvallinen”. Huomattiin, että voidaan parantaa ”Turvallinen” kohdan ”Suojaus” eli ”Järjestelmän tieto salattu (ei luettavana)” ottamalla käyttöön AIP:n Office 365 -ympäristössä. (Kuvio 6.)

JÄRJESTELMÄN TIETOTURVAKORTTI

	Käyttöoikeudet	Tunnistautuminen	Suojaus	Elpyminen
Kriittinen	Järjestelmä on hallinnassa	Tietoturvallinen salasana	Järjestelmä tuettu ja päivitetään jatkuvasti	Merkittävä data varmuuskopioidaan
Parannettavaa	Suunnitelmalliset käyttöoikeudet ja roolit	Lokitiedot käyttäjien toiminnasta	Salaus ja suojaus tietoliikenteessä, siirtotiedostoissa ja integraatioissa	Varmuuskopioinnin seuranta ja testaus palautuksissa
Turvallinen	Pääkäyttäjä vastaa käyttöoikeuksista ja tuesta	2FA tai biometrinen tunnistus	Järjestelmän tieto salattu (ei luettavana)	Varmuuskopiot säännöllisesti järjestelmän ulkopuolelle

Kortti antaa järjestelmälle tietoturvasta pisteet 0-12. Jokaisesta täytetystä vaatimuksesta saa pisteen. Seuraavalle tasolle pääsee vasta, kun edellisen tason kaikki vaatimukset on täytetty.
Järjestelmän tietoturvan tasot: kriittinen (0-3 p.), parannettavaa (4-7 p.), turvallinen (8-12 p.).

Kuvio 6: Fidan sovelluskortti, tekijä Aki Tervo

5.2 Palaverit

Ensimmäisissä palavereissa teimme päätöksen siitä, että AIP olisi palvelu, jolla kehittäisimme organisaation tietoturvaa paremmaksi tiedostojen ja sähköpostin suojauksen avulla. Sovimme käyttöönoton aloituspalaverista, jonka järjestin Fidan tiloissa ja esittelin siellä.

5.2.1 Käyttöönoton aloituspalaveri

Aloituspalaverin tarkoituksena oli käydä läpi Fidalle oleellisimmat asiat käyttöönoton kannalta yhdessä tietohallintopäällikön ja hallinto-osaston johtajan kanssa. Olin tehnyt esityksen tietohallintopäällikön pyynnöstä ja kävin siinä muun muassa läpi AIP:n eri ominaisuuksia.

Palaverissa kävimme läpi AIP -politiikat, mitkä sopisivat Fidalle ja esityksen jälkeen kävimme läpi sellaisia ominaisuuksia, jotka pitäisi testata nykyisten Windows - ja Android -laitteiden kanssa. Fidalla oltiin otettu käyttöön uusia MacOS -tietokoneita ja käyttöönoton yhtenä tavoitteena oli selvittää, miten AIP voitaisiin ottaa käyttöön niiden kanssa. Kävimme muita ominaisuuksia läpi ja selvisi että AIP:ssa voitaisiin hyödyntää salattua sähköpostia Fidan ulkopuoliseen viestintään, joten senkin toimivuus tulisi testata.

Aloituspalaverissa sain tehtäväkseni aloittaa yhteydenpidon Fidan IT-kumppanin kanssa, joka laittoi käytäntöön suunnittelemamme politiikat. Sovimme yhteydenpidosta tietohallintopäällikön kanssa ja alustavasti käyttöönoton aikataulusta.

5.2.2 Palaverit tietohallintopäällikön kanssa

Pidimme säännöllisesti 1-2 palaveria kuukaudessa tietohallintopäällikön kanssa pois lukien kesälomakausi. Palaverit kestivät keskimäärin noin kaksi tuntia. Olimme myös yhteydessä puhelimitse ja sähköpostitse.

Seuraavissa palavereissa kävimme vielä muun muassa läpi sitä, ketkä olisivat onnistuneen käyttöönoton jälkeen testiryhmä, joille ensimmäisinä asennettaisiin AIP -sovellukset. Kävimme läpi sitä, miten käyttöönoton jälkeen uudet ominaisuudet koulutettaisiin Fidan toimiston henkilökunnalle. Palavereissa kävimme tilannekatsausta käyttöönoton eri vaiheista.

5.2.3 IT-kumppanin palaverit

IT-kumppanin kanssa pidetyssä ensimmäisessä palaverissa käytiin läpi politiikkoja, mitä aloituspalaverissa olimme päättäneet. Palaverissa sovittiin yhteydenpidosta sähköpostilla ja projektin aikana olin usein käyttöönottoon liittyvistä asioista yhteydessä IT-kumppanin kanssa.

Seuraavissa palavereissa kävimme muun muassa läpi ongelmia, mitä MacOS -tietokoneissa oli käyttöönotossa ilmentynyt. Pyrimme selvittämään yhdessä, mistä nämä virheet voisivat johtua ja pidimme yhteyttä entistä enemmän käyttöönotossa ilmentyneiden ongelmien vuoksi. Loimme myös yhdessä IT-kumppanin kanssa tiketin havaituista ongelmasta ja olin tämän jälkeen yhteydessä Microsoft-asiantuntijaan.

5.2.4 Microsoft asiantuntija

MacOS -tietokoneiden kanssa oli ongelmia saada näkymään AIP -palvelussa luodut labelit IRM-yhdistysongelman takia. Microsoft asiantuntijan mukaan AIP -sovellus ei tulisi MacOS -tietokoneille sellaisenaan. Sitä tulisi käyttää Security and Compliance Centerin Sensitivity (luottamuksellisuus) -osion avulla, joka oli tällä hetkellä vasta testivaiheessa.

Microsoft asiantuntija neuvoi laittamaan nopeat päivitykset päälle MacOS Office -tuotteista, jonka piti ratkaista ongelma. Tätä ennen piti siirtää Intunesta AIP -palvelun tiedot Security and Compliance Centerin luottamuksellisuus -osioon. Tähän saimme ohjeistuksen sähköpostin kautta ja linkin sivulle, mistä löysimme tarvittavat tiedot siirron toteuttamiseen. Luvussa 6.2.4 on selostus siitä, mitä huomioita tehtiin siirron jälkeen.

5.2.5 Suomalaisen IT-konsultointi yrityksen palaveri

Suomalaista IT-konsultointi yritystä pyydettiin apuun selvittämään, voitaisiinko AIP -palvelun saada toimimaan Fidan käytössä olevilla MacOS -tietokoneilla. Palaverissa kävimme läpi ongelmat, joita käyttöönotossa oli ilmennyt. Asiantuntijapalvelu oli saanut näkyviin labelit esiasetuksilla omassa palvelussa vanhemmalla käyttöjärjestelmällä ilman erillisiä sovelluksia tai Microsoft asiantuntijan neuvomaa Sensitivity-osiota.

Tutkimme yhdessä virhettä, joka oli tullut Fidan käyttöympäristössä ja jatkoimme myös sähköpostin ja puhelimen välityksellä kommunikointia virheen tutkinnan tiimoilta. Emme kuitenkaan löytäneet selkeyttä miksi Fidan ympäristössä MacOS tietokoneilla IRM-palveluun ei saanut yhteyttä, vaikka kaikki asetukset näyttivät olevan kunnossa.

6 Kehittämistyön toteutus

Projektin vaiheet on kuvattu taulukossa 1. Ensin tehtiin kartoitus Fidan tietosuojasta, laitteistoista ja palveluista. Tämän jälkeen tehtiin suunnitelma, jossa käytiin läpi AIP:n politiikkoja ja Fidan kannalta tärkeimmät asiat käyttöönotossa. Suunnitelman jälkeen annettiin Fidan IT-kumppanille työpyyntö laittaa konfiguraatio Fidan työympäristöön sopivaksi. Asiantuntijapalvelun konfiguraation jälkeen aloitettiin Windows-, MacOS- ja Android -asennukset ja testaus. Asennusten ja testausten jälkeen laitettiin suojattu sähköposti käyttöön testiympäristöön. Testiympäristön kokeilujen jälkeen koulutettiin Fidan työntekijät suojatun sähköpostin käyttöön aamupalaverissa, johon oli valmistettu esitys. Koulutusten jälkeen aloitettiin käyttöönotto Fidan toimistossa ilmoittamalla siitä Teams-palvelussa ja jakamalla loppukäyttäjäohje. Käyttöönoton jälkeen tehtiin analyysi siitä, mitä huomioita ja kehitysehdotuksia löysin toimeksiantajalle.

Projektin aikataulutus		
Azure Infromation Protection	Muuta infoa	Varattua aikaa noin
Kartoitus	Kartoitus Fidan tietosuojasta, laitteistosta ja palveluista	**2 vk**
Suunnitelma	AIP politiikat ja Fidan kannalta tärkeimmät asiat käyttöönotosta	**2 vk**
Asiantuntijapalvelu	AIP palvelun konfiguraatio Fidan työympäristöön sopivaksi	**1 vk**
Windows asennus	Win10 AIP asennus ja testaus	**1 vk**
MacOS asennus	MacOS RMS -jako sovelluksen ja luottamuksellinen osion asennus ja testaus	**2 vk**
Android asennus	Android AIP asennus ja testaus	**1 vk**
Käyttöönotto testiympäristöön	Fidan testiympäristöön laitteisiin	**1 vk**
Käyttäjien koulutus	Fidan toimiston työntekijöiden koulutus aamupalaverissa	**1 vrk**
Käyttöönotto Fidalle	Ilmoitus Teams palvelussa ja loppukäyttäjäohje	**1 vrk**
Käyttöönoton analyysi	Huomiota mitä tehtiin käyttöönotossa	**1 vk**

Taulukko 1: Taulukossa hahmotelma siitä, miten AIP:n käyttöönotto eteni vaiheittain.

6.1 Projektin aloitus

Projektia lähdettiin toteuttamaan tekemällä selvitys nykyisestä Fidan tietosuojasta, palveluista ja laitteistosta. Tarkempi selostus tästä löytyy luvussa 5.1. Selvityksessä päädyimme siihen, että eniten tietosuojaa parantava ominaisuus olisi AIP:n käyttöönotto Fidalla. Se ei ainoastaan parantaisi uusia MacOS -tietokoneella työskentelevien tietosuojaa, vaan samalla myös huomattavasti parantaisi Windows 10 -tietokoneiden ja Android -laitteiden tietosuojaa.

Selvityksien jälkeen laadimme AIP:n palveluun konfiguraatioasetuksia ja selvitimme, mitkä politiikat tulisivat käytäntöön esiasetuksien kanssa ja mitä muutettaisiin. Valmiin selvityksen ja suunnitelman pohjalta lähetettiin työpyyntö eteenpäin Fidan ulkopuoliseen asiantuntijapalveluun.

Fidan IT-kumppani laittoi toimeen selvityksestä laaditut käytänteet. Tämän pohjalta alettiin toteuttamaan käyttöönottoa asentamalla Azure Information Protection Clientia sekä RMS-Sharing sovellusta päätelaiteille.

6.2 Azure Information Protection käyttöönotto

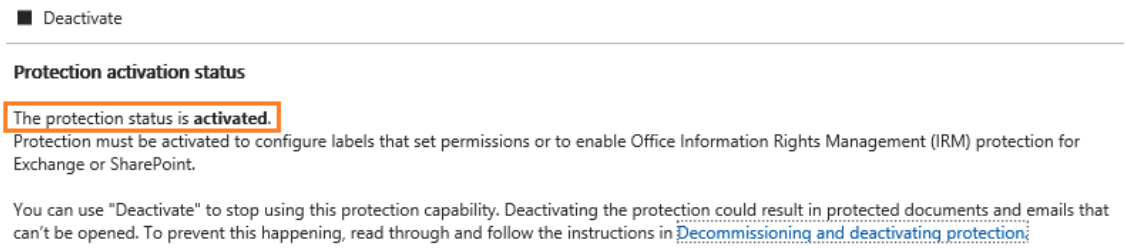
Seuraavaksi käydään läpi yleisellä tasolla AIP konfiguraatioasetuksia Microsoftin omia sivustoja hyödyntäen. Luvussa käydään vaiheittain Windows 10, MacOS, Android ja suojatun sähköpostin käyttöönotot. Luvussa pyritään kertomaan tarkemmin, miten käyttöönotto toteutettiin vaiheittain, sekä virheistä, joita MacOS- sekä Android -laitteilla huomioitiin. Kuvakaappauksia on hyödynnetty selvemmän kuvan saamiseksi käyttöönotosta.

Luvussa 6.2.4 käydään yleisesti läpi luottamuksellisia leimoja, jotka Microsoft asiantuntija oli ohjeistanut MacOS -tietokoneiden käyttöönottoon. Niillä pyrittiin saavuttamaan sama tulos kuin Windows 10 -asennuksessa, jotta AIP -palvelu olisi saatu toimimaan odotetulla tavalla.

6.2.1 AIP -konfiguraatio

Tässä luvussa käydään AIP -konfiguraatiota yleisesti tietoturvan takia. AIP tarvitsee tietyt lisenssit toimiakseen. Nämä löytyvät luvusta 3.5.1. AIP ei ole automaattisesti käytössä ja se otetaan käyttöön Azure portalin kautta järjestelmävalvojatiliä käyttäen. Valikosta etsitään ”Create a resource” ja sitten käytetään hakua ”marketplace” kohdasta ja etsitään ”Azure Information Protection”. Haun jälkeen valitaan listasta AIP ja sen jälkeen painetaan kohdasta ”Create”. Seuraavia kertoja varten kannattaa valita valinta ”Pin to dashboard”. Tämän avulla seuraavilla kerroilla voidaan navigoida AIP -asetuksiin hallintapaneelin kautta paljon nopeammin. (Microsoft 2019c.)

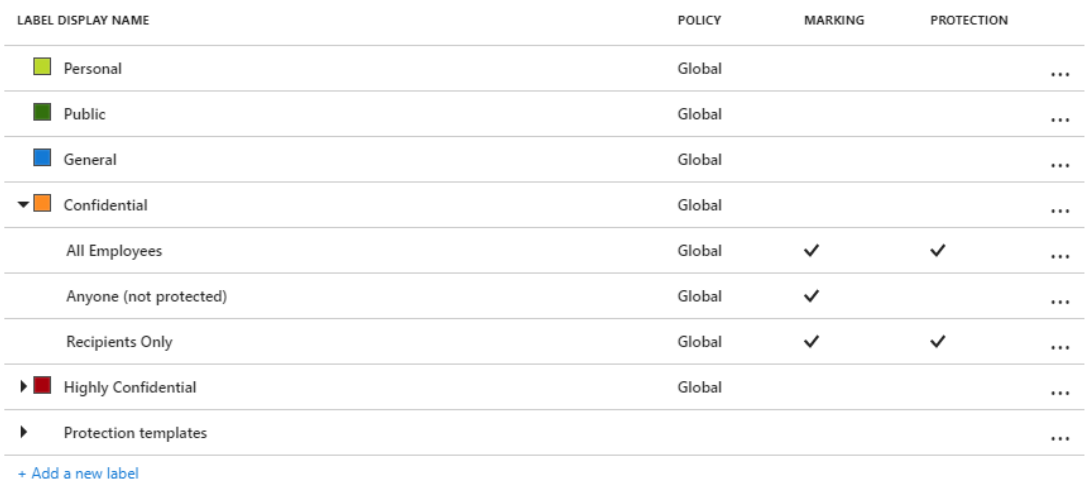
AIP -asetuksista on hyvä käydä tarkistamassa AIP -aktivoinnin onnistuminen ja että suojaus on päällä. Samasta paneelista voidaan kytkeä suojaus pois käytöstä painamalla valintaa ”Deactivate”. Paneeli myös ilmoittaa selkeästi nykyisen suojauksen tason. (Kuvio 7.)



Kuvio 7: AIP palvelun aktiivisen suojauksen näkymä. (Microsoft)

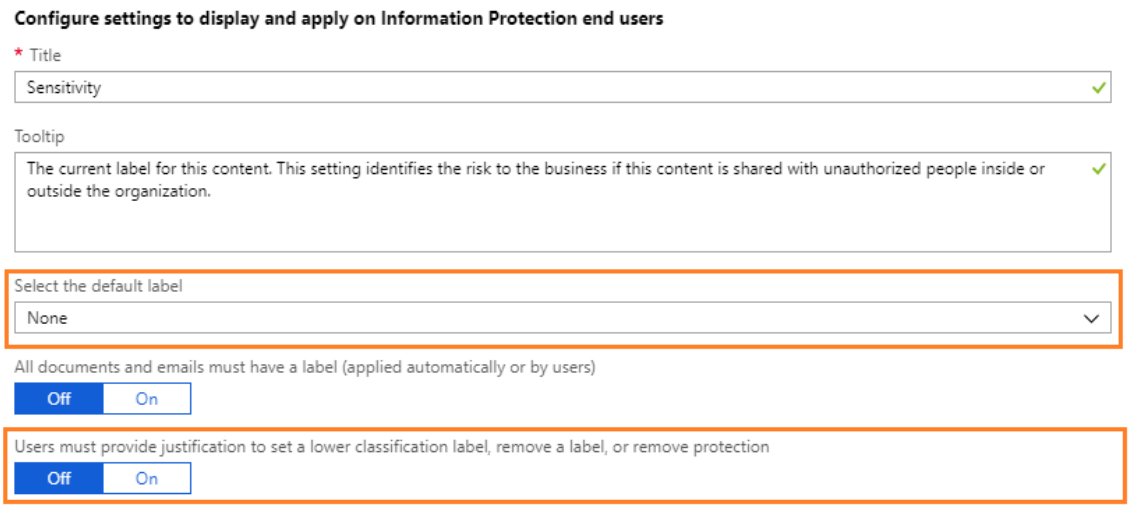
AIP -palvelu luo automaattisesti oletuspolitiikat ensimmäisellä kerralla, kun palvelu käynnistetään. Oletuspolitiikat sisältävät heti käyttöön valmiita leimoja ja asetuksia. Niitä voidaan halutessa muokata tai luoda uusia. (Microsoft 2019c.)

Kuviossa 8 on määritelty eri leimoja eri käyttötarkoituksiin (henkilökohtainen, julkinen, yleinen, luottamuksellinen ja erittäin luottamuksellinen). Luottamuksellisen kohdasta löytyy alikategoriat (kaikki työntekijät, kuka tahansa (ei suojattu) ja vastaanottaja ainoastaan). Oletus konfiguraatiossa vain osaan leimoista on määritelty merkintä ja/tai suojaus. Merkintä voi olla alaviite, yläviite tai vesileima.



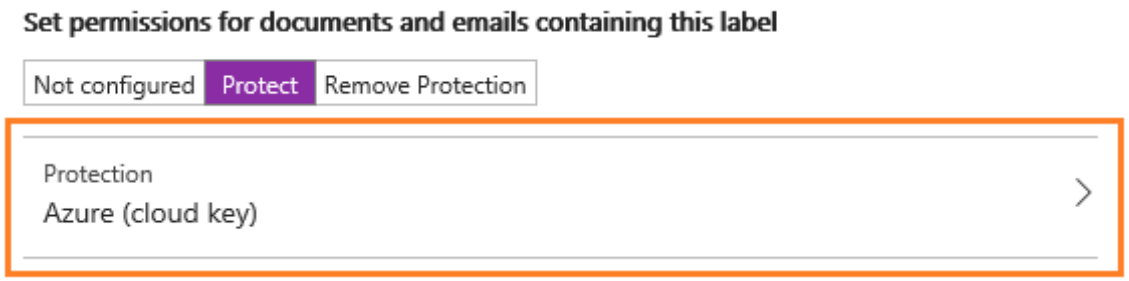
Kuvio 8: AIP listaus leimoista (Microsoft)

Kuviossa 9 on uuden leiman luominen. Uuteen leimaan voidaan valita uusi otsikko kohdasta ”Title”. Kohdasta ”Tooltip” voidaan määrittää ohjeteksti käyttäjille, joka ilmoitetaan palvelun sovelluksessa. Kohdasta ”Select the defaul label” voidaan määrittää ”General” -leima, joka tulisi automaattisesti jokaiselle, kun luodaan uusi dokumentti tai sähköposti päätelaitteella. Tämä ei ole pakollinen ja voi useassa tapauksessa olla parempi, että sitä ei valita. Käyttöliittymä on yksinkertainen ja käyttäjän on helppo valita haluttu leima, jos tiedosto tarvitsee esimerkiksi suojauksen. Tämän takia asetuskohta ”All documents and emails must have a label…” yleisimmissä tapauksissa kannattaa jättää valitsematta, koska tällöin käyttäjät eivät voi tallentaa dokumentteja ja sähköposteja ilman leimaa. Kohdassa ”User must provide justification…” voidaan esimerkiksi suojatuissa luottamuksellisissa leimoissa valita tämä vaihtoehto haluttaessa, jos halutaan oikeudet omaavalle käyttäjälle mahdollisuus muokata tiedoston suojausta.



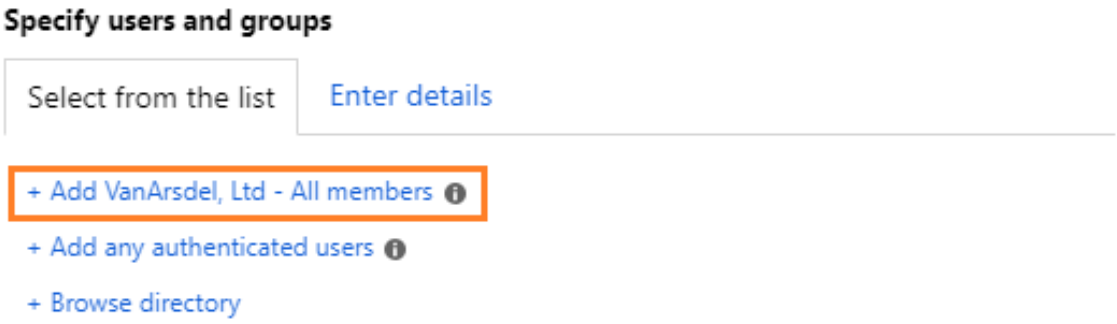
Kuvio 9: AIP -leiman asetuksia. (Microsoft)

Tästä valinnasta voidaan valita, onko dokumentilla suojausta. Vaihtoehtoina on Azure (cloud key), joka on tallennettuna Azuren pilveen. Vaihtoehtoisesti voidaan käyttää HYOK:ia (Hold your own key), jolloin salausavain ei ole Azuren pilvessä. Azure(cloud key) on varmempi vaihtoehto ja se käyttää Azure Rights Management-palvelua suojatakseen dokumentit ja sähköpostit. (Microsoft h.) Jos halutaan käyttää vain leimoja, jotta voidaan tunnistaa tietyt sähköpostit ja dokumentit leima merkintöjen avulla, voidaan valita ”Remove Protection”. Tällöin tietoja ei suojata. (Kuvio 10.)



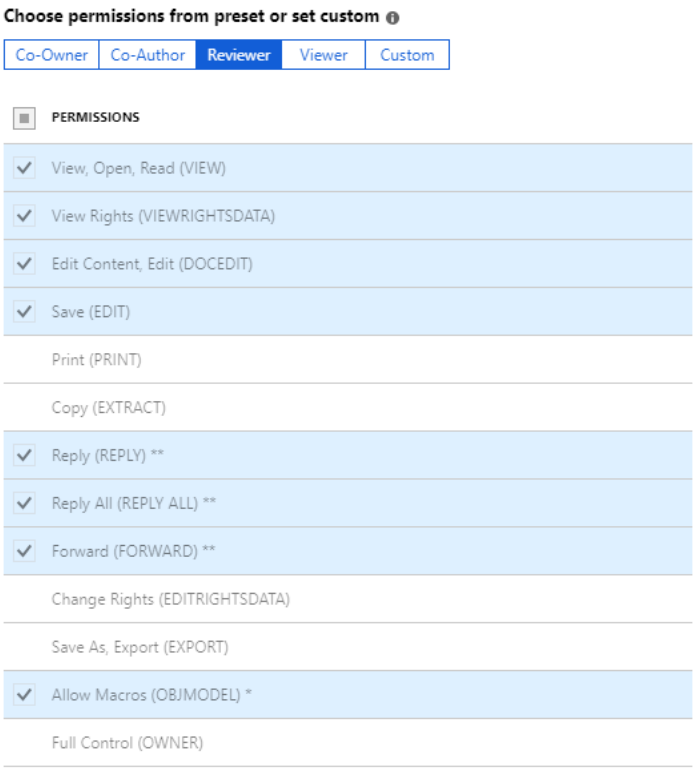
Kuvio 10: AIP -asetukset, suojaus. (Microsoft)

Tästä asetuskohdasta valitaan henkilöt ja ryhmät, joille voidaan asettaa oikeus käyttää muokattavana olevaa leimaa. Valinta voidaan tehdä koko organisaatiossa työskenteleville henkilöille, tietylle ryhmälle tai yksittäisille henkilöille. Valintoja voidaan tehdä useita ja ne voivat sisältää eri vaihtoehtoja oikeuksista (luku, muokkaus jne.). (Kuvio 11.)



Kuvio 11: AIP -asetukset, käyttäjät ja ryhmät. (Microsoft)

Henkilöiden ja ryhmien valinnan jälkeen valitaan käyttöoikeudet. Käyttöoikeudet voidaan antaa kätevästi käyttäen esiasetuksia, esimerkiksi Reviewer, jolloin käyttäjälle myönnetään kuvassa näkyvät oikeudet. Oikeuksia voidaan muokata tarvittaessa jälkikäteen. (Kuvio 12.)



Kuvio 12: Oikeuksien hallinta. (Microsoft)

Asetuksista löytyy monia muita ominaisuuksia, joilla voidaan räätälöidä asetukset oikeaksi omaan organisaatioon. Asetuksista voidaan mm. kytkeä päälle aiemmin tässä luvussa mainittu vesileima ja sitä on mahdollista muokata omaan organisaatioon sopivaksi.

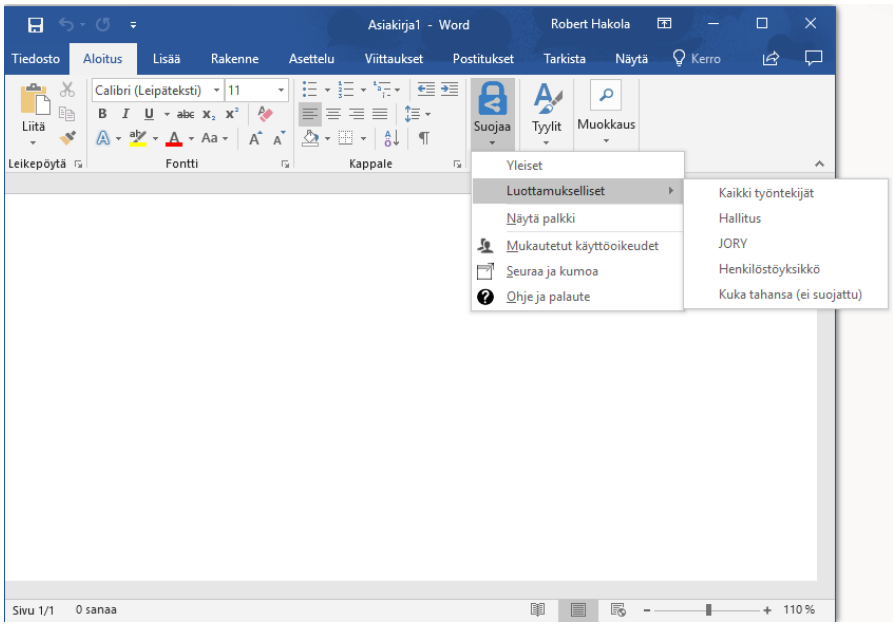
Konfiguraatiossa on mahdollista tehdä asetus, joka tunnistaa tiedostosta automaattisesti esimerkiksi luottokorttinumeron. Asetuksista löytyy monia muita esiasetuksia numero/kirjain -

yhdistelmiä mm. talousalan, terveysalan ja yksityisyyden automaattiseen suojaukseen. Suojaus tapahtuu niin, että tiedostosta, jota ollaan muokkaamassa, löytyy esimerkiksi luottokorttinumerolta näyttävä numeroyhdistelmä (4242-4242-4242-4242), jolloin AIP havaitsee ja ehdottaa käyttäjälle suositellun suojauksen dokumenttiin. Tässä tapauksessa olisi luotu esimerkiksi luottamuksellinen/luottokortti -leima, jolloin esimerkiksi Word-dokumenttia muokatessa olisi Wordin yläpalkkiin tullut ilmoitus suositellusta leimasta, joka tulisi ottaa käyttöön. Tässä on jätetty käyttäjälle mahdollisuus olla valitsematta suositeltua suojausta eli käyttäjä voi tarvittaessa painaa hylkää-nappia. Tämä on laitettu siitä syystä, että joskus AIP voi tunnistaa väärän numeroyhdistelmän luottokorttina, jolloin suositeltua leimaa ei tarvita. (Microsoft 2019d.)

6.2.2 Asennus ja testaus Windows 10:llä

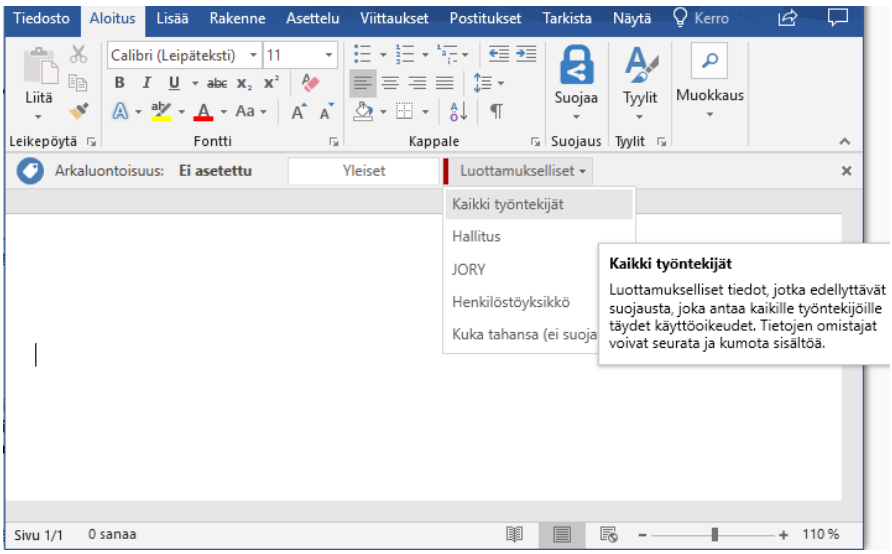
Windows 10 asennuksessa ladattiin AIP:n asiakasohjelma Portal Azurerms-verkkosivulta. Asennus suoritettiin ilman esiasetuksia, koska tarvittavat politiikat oli luotu jo aiemmin. Asennuksen jälkeen asiakasohjelmisto pyysi rekisteröitymään palveluun ja tarkistamaan, onko käyttäjällä oikeuksia ottaa käyttöön asiakasohjelmiston tarjoamaa palvelua.

AIP:n asennuksen jälkeen Wordiin ja muihin AIP:tä tukeviin sovelluksiin ilmestyy aloitus -välilehdelle ”Suojaa”-valinta, joka on AIP:n käyttöliittymä Office -sovelluksissa. Käyttöliittymässä voi suojata dokumentin valmiiksi luoduilla suojausasetuksilla, valita mukautetut käyttöoikeudet tai seurata ja kumota oikeuksia. Käyttöliittymästä voidaan kytkeä pikavalintapalkki käyttöön. Käyttöliittymästä löytyy myös ohje ja palauteosio, josta löytyy perustietoja ohjelmiston asennuksesta. (Kuvio 13.)



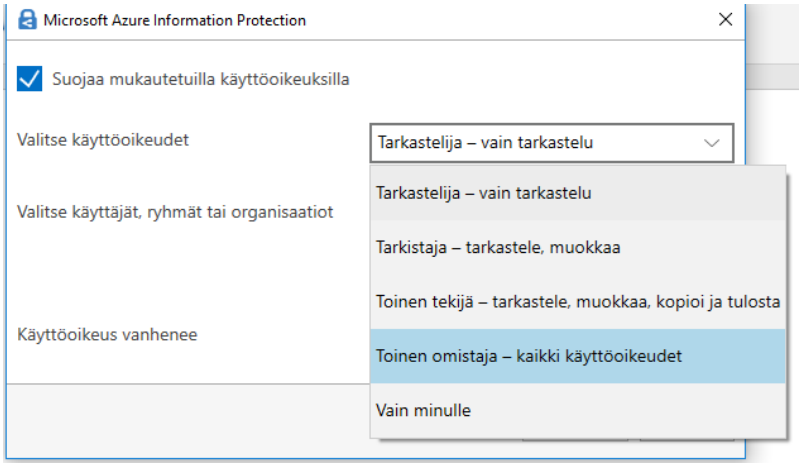
Kuvio 13: Käyttöliittymä Wordissa, ”Suojaa-painike”

AIP:n käyttäminen toimii yksinkertaisimmillaan hyödyntämällä valmiiksi luotuja labeleitä, johon on määritelty valmiiksi käyttöoikeudet. Palkki on oletuksena käytössä kaikissa sovelluksissa, jotka tukevat AIP:ia. Palkki voidaan ottaa käyttöön ja kytkeä pois käytöstä ”Suojaa”-valinnasta. (Kuvio 14.)



Kuvio 14: Käyttöliittymä Wordissa: oikeuksien jakaminen

AIP tarjoaa mahdollisuuden tehdä dokumentteja käyttäjän luomilla käyttöoikeuksilla. Käyttöliittymä on yksinkertainen ja käyttöoikeus kohdassa voidaan valita viidestä erilaisesta valinnasta. Jos käyttäjä ei valitse ”Vain minulle”-vaihtoehtoa, pitää tällöin määrittää käyttöoikeuksien lisäksi, kenelle dokumentti aukeaa. Käyttöoikeuksia voidaan määritellä tietylle käyttäjälle, ryhmälle tai organisaatiolle, jolle tiedosto on tarkoitettu. Käyttäjä voi halutessaan luoda dokumentille vanhenemisajan. (Kuvio 15.)

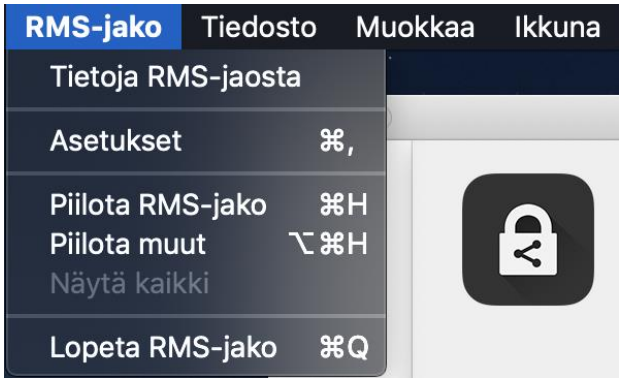


Kuvio 15: Mukautetut käyttöoikeudet

6.2.3 Asennus ja testaus MacOS:llä

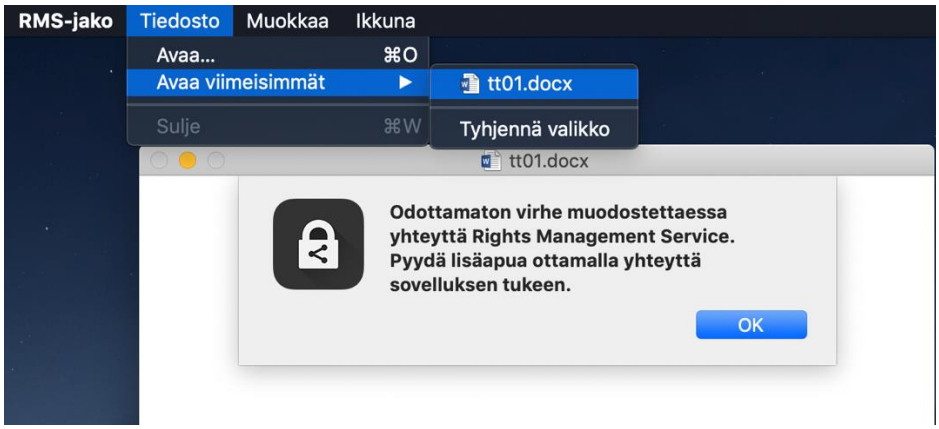
Ohjeiden mukainen asennus MacOS -laitteille tapahtui Portal Azurerms-verkkosivun kautta. Sieltä valittiin MacOS -käyttöliittymä ja linkki ohjasi Applen sovelluskauppaan, josta pääsi asentamaan RMS-jakosovelluksen. Asennuksen jälkeen RMS-jakosovellus ei kysynyt Office tunnuksia tai mitään vastaavaa, niin kuin AIP -sovellus oli tehnyt Windows 10 -tietokoneella.

RMS-jakosovelluksen käyttöliittymä on paljon suppeampi, kuin Windowsin vastaavaa AIP -sovellus. Sovelluksessa on RMS-jako-välilehti, josta pääsee näkemään tietoja RMS-jaosta ja asetuksia sovelluksesta. Kun käyttäjä klikkaa valintaa tietoja RMS-jaosta, niin ohjelma ei reagoinut mitenkään. Asetukset kohdassa oli yksi valintaruutu, joka mahdollisti tietojen lähettämisen ohjelman parantamiseksi. (Kuvio 16.)



Kuvio 16: RMS-jako-sovellus, käyttöliittymä ja kuvake.

RMS-jakosovelluksen tiedosto -välilehden takaa löytyy mahdollisuus avata tiedosto tai avata viimeisin tiedosto, mitä sovelluksella on avattu. Esimerkkidokumenttina käytetään tt01.docx:ia, joka on Windows 10 -tietokoneella AIP -sovelluksen avulla suojattu käyttäen Fidalle luotuja suojausasetuksia. Dokumentin käyttöoikeudet on annettu ”Kaikki työntekijät”-ryhmälle. Dokumenttia avatessa RMS-jakosovellus ilmoittaa seuravanlaisen virheen ”Odottamaton virhe muodostaessa yhteyttä Rights Management Service. Pyydä lisäapua ottamalla yhteyttä sovelluksen tukeen.” (Kuvio 17).



Kuvio 17: RMS-jakosovelluksen tiedosto -välilehti.

6.2.4 MacOS:n luottamuksellisuusleimojen testaus

Tämän toiminnallisuuden testaus ja käyttöönotto tehtiin Microsoft asiantuntijan ohjeistuksella, joka saatiin palaverissa. Lisätietoja palaverista löytyy luvusta 5.2.4.

Luottamuksellisuusleimojen avulla pyrittiin saamaan muun muassa Microsoft Word ja Outlook sovelluksiin näkyviin leimat, jotka olimme luoneet AIP -konfiguraatiossa ja siirtäneet ne Security & Compliance centeriin. Leimat saatiin onnistuneesti näkyviin, mutta vain yksi leimoista toimi osittain IRM tunnistus virheen, joka löytyy kuviosta 17, takia. Yksi luoduista leimoista suojatun sähköpostin lähettämiseen toimi, mutta vastaanottaja ei voinut avata lähetettyä suojattua sähköpostia MacOS -tietokoneella saman IRM-tunnistusvirheen takia. Microsoft asiantuntijan ohjeistuksesta huolimatta AIP -palvelua ei saatu toimimaan MacOS -tietokoneille.

6.2.5 Asennus ja testaus Android -laitteille

Androidille sovellus asennetaan Google Play kaupasta. Sovellus haettiin hakusanoilla Azure Information Protection.

Asennuksen jälkeen AIP -sovellus jää taustalle päälle ja dokumenttia avatessa sovelluksen pitäisi purkaa salaus. Tällä hetkellä Microsoftin mukaan ohjelmalla ei voida suojata uusia dokumentteja, mutta avaamisen pitäisi onnistua.

Testissä Windows 10 -tietokoneella lähetettiin suojattu Word-tiedosto puhelimelle. Android -puhelimen testeissä ei onnistuttu avaamaan tiedostoa AIP -sovelluksen avulla ja tämä viittasi samaan IRM-tunnistusvirheeseen, joka oli tullut MacOS -tietokoneiden käyttöönotossa (Kuvio 17).

Suojatun sähköpostin avaaminen ja vastaaminen toimi Anroidin Outlook -sovelluksella ilman AIP -sovellusta. Tällä hetkellä uusia suojattuja sähköposteja ei voitu lähettää Android -sovelluksen kautta, mutta seuraavassa luvussa esitellyn OWA:n avulla lähettäminen onnistui.

6.2.6 Suojattu sähköposti ja testaus Outlook Web App:issa (OWA)

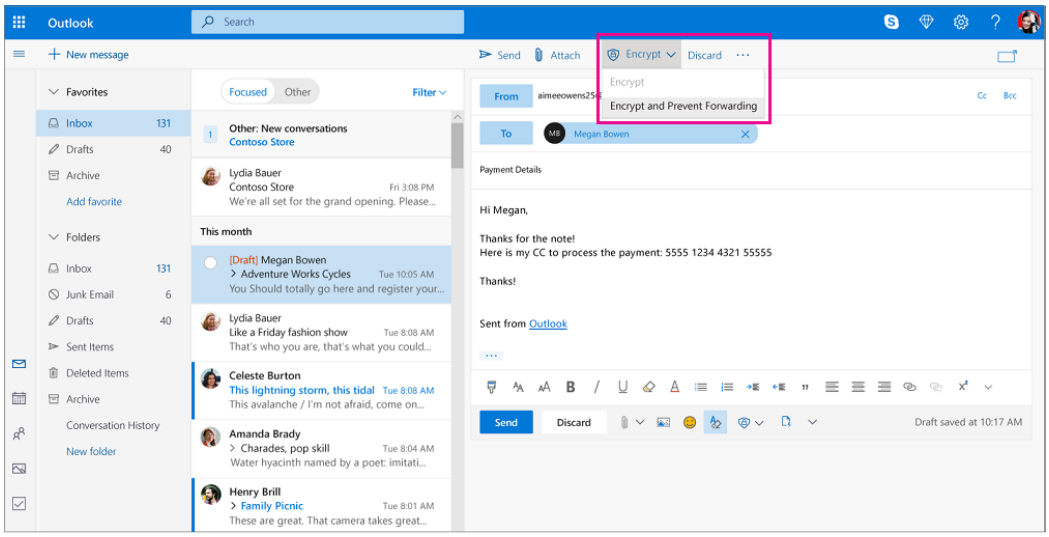
Lopulta Fidassa päädyttiin valitsemaan suojatun sähköpostin käyttämisen OWA:n avulla, koska emme olleet useista käytetyistä työtunneista ja hyödyntämistämme asiantuntijapalveluista huolimatta saaneet AIP -palvelua toimimaan MacOS -tietokoneilla tai Android -laitteilla. OWA:n avulla saimme yhden ominaisuuden lisää, joka parantaa merkittävästi organisaation tietosuojaa.

Suojattu sähköposti kuuluu osaksi Office 365 Yritys E3- ja E5-lisenssejä. Suojattu sähköposti toimii organisaatiossa kaikilla käyttäjillä, joille on luotu organisaation käyttäjätili.

Suojattu sähköposti yhdistää sähköpostin kryptauksen ja rights managementin (käyttöoikeuksien hallinta) toiminnon. Käyttöoikeuksien hallinta -toiminto tulee AIP:n avulla. Suojattu sähköposti tuli automaattisesti toimintaan osana AIP:n käyttöönottoa, koska sen tarvitsema Information rights management (IRM) oli otettu organisaatiossa käyttöön. (Microsoft 2019e.)

MacOS Outlook -sovelluksessa todettiin sama kuvion 17 mukainen IRM-virhe. Virheiden takia MacOS -tietokoneiden Outlook -sovelluksen kautta ei voitu lähettää tai avata suojattua sähköpostia. Organisaatiossa haluttiin yhdenmukainen käyttöliittymä kaikille työntekijöille suojattuun sähköpostiin ja toimivaksi havaittu käyttö organisaatiossa tapahtuu OWA:n avulla.

OWA:n käyttöliittymä on yksinkertainen ja se toimii yleisimmillä selaimilla. Sähköpostisuojauksen saa kytkettyä päälle, kun avataan uusi viesti ja valitaan kohta ”Encrypt” (Suojaa). Suojauksessa on toinen vaihtoehto ”Encrypt and Prevent Forwarding” (Älä lähetä edelleen). Älä lähetä edelleen-vaihtoehdossa on sama suojaus, kuin pelkässä suojaa-vaihtoehdossa, mutta se estää vastaanottajaa lähettämästä viestiä eteenpäin, sekä estää tulostamasta tai kopioimasta sitä. (Kuvio 18.)



Kuvio 18: OWA:n käyttöliittymä ja suojauspainike. (Microsoft)

Kuviossa 19 voidaan nähdä mallisähköpostiviesti lähetettynä ulkopuoliselle sähköpostin tarjoajalle esimerkiksi Googlen tarjoamaan Gmailiin. Sähköpostin lukeminen on helppoa ja tapahtuu painamalla ”Read the Message” (Lue viesti) ja seuraamalla ohjeita. Vaihtoehtona on kirjautua Microsoftin tunnuksilla tai käyttämällä kertakäyttöistä koodia, joka lähetetään käyttäjän sähköpostiin.

Kuvio 19: Suojatun sähköpostin lähettäminen ulkopuoliselle sähköpostin tarjoajalle. (Microsoft)

Suojatun sähköpostin käyttäminen tapahtuu vain Microsoftin palvelimella, joten viestin sisältö on aina suojattu. Suojatussa sähköpostissa lähetetyt liitetiedostot myös suojataan sähköpostia lähetettäessä. Tuetut tiedostot ovat tällä hetkellä Office -tuotteiden tiedostot esim. Word, Excel ja PowerPoint. Jos ´älä lähetä edelleen´ toimintoa on käytetty ja mukana ollut liitetiedosto on ladattu tietokoneelle ja se lähetetään uudella sähköpostiviestillä eteenpäin, ei viestin vastaanottaja voi avata tiedostoa, koska sähköpostiviesti on edelleen suojattu ´älä lähetä edelleen´ toiminnolla. (Microsoft 2019e.)

Suojatun sähköpostin käyttäminen Windows -tietokoneilla toimi OWA:ssa oletetusti ja liitetiedostot onnistuttiin avaamaan tietokoneella asennetuilla Office -sovelluksilla. MacOS ja Android käyttöjärjestelmillä pystyttiin OWA:n avulla lähettämään ja lukemaan suojattuja sähköpostiviestejä, mutta havaittiin IRM-virheeseen viittaava virhe (katso kuvio 17) avattaessa liitetiedostoja Office -sovelluksilla.

7 Kehittämiskohteen tulokset

Käyttöönotossa ei saatu AIP -toimintoja toimimaan MacOS -tietokoneilla IRM-virheen takia, joka löytyy kuviosta 17. Android laitteella ei tällä hetkellä saatu haluttuja ominaisuuksia käyttöön, mutta suojatun sähköpostin lukeminen onnistui Outlook -sovelluksella. Windows -tietokoneella AIP -käyttöönotto toimi oletetulla tavalla ja käyttöönotto oli onnistunut.

Käyttöönottoa ei toteuteta sellaisenaan, koska organisaatiossa MacOS -tietokoneita on otettu käyttöön jo useita, ja tällöin suojattujen dokumenttien avaaminen ei olisi mahdollista kaikilla käyttäjillä. Toiminnallisuuksista otettiin vain osa käyttöön eli suojattu sähköposti.

Organisaatiossa haluttiin yhdenmukainen käyttöympäristö suojatulle sähköpostille. Käyttöönottoprojektissa onnistuttiin löytämään tapa, jolla suojattua sähköpostia voitiin käyttää kaikilla laitteilla samalla tavalla eli OWA:n avulla. Tarkempi selostus löytyy luvusta 6.2.6.

7.1 Käyttöönoton laitteet

Windows -tietokoneiden käyttöönotto onnistui kaikilta osin ja päästiin haluttuihin tuloksiin. Käyttöönoton testivaiheessa onnistuttiin salaamaan useita eri tiedostoja ja ne pystyttiin avaamaan ongelmitta. Dokumentit, joita suojattiin olivat muun muassa Microsoft Word, Excel ja PowerPoint tiedostoja ja niitä salattiin konfiguraatiossa luoduilla erilaisilla suojauksilla. Testausvaiheessa lähetettiin suojattuja sähköposteja Microsoft Outlookin kautta ja niissäkin saatiin halutut testitulokset, eli vain asianmukaisilla oikeuksilla varustetut käyttäjät pystyivät avaamaan sähköposteja.

MacOS -laitteiden Office -sovelluksiin olisi pitänyt automaattisesti tulla näkyviin sovelluksien suojauspainikkeet AIP -käyttöönoton yhteydessä. Tämä selvitettiin palaverissa suomalaisen IT-konsultointi yrityksen kanssa. Tarkempi selostus tästä löytyy luvusta 5.2.5. Suojauspainikkeen kautta havaittiin samankaltainen ongelma kuin RMS-jako sovelluksen asentamisessa, eikä luotuja suojausleimoja saatu näkyviin (Kuvio 17). Käyttöönotto ei sujunut MacOS -tietokoneella useiden yritysten jälkeen. Vaikka ICT-lähitukihenkilöä konsultoitiin ja prosessia testattiin toisilla MacOS -tietokoneilla, ilmeni niilläkin samat ongelmat, mitä oltiin saatu omalla tietokoneella. Fidan IT-kumppanin, suomalaisen IT-konsultointi yrityksen ja Microsoft asiantuntijan osaamista käytettiin selvittämään, missä vika voisi olla. Avusta ja yrityksistä huolimatta lopullista ratkaisua ongelmaan ei löytynyt.

Android -laitteilla ei päästy haluttuun tulokseen testausvaiheessa. Android -laitteilla havaittiin sama ongelma kuin MacOS -laitteilla, eli tiedostoja ei voitu avata tai suojata. Androidilla onnistuttiin avaamaan testivaiheessa suojattu sähköposti Outlook -sovelluksen avulla, mutta tällä hetkellä uusien suojattujen sähköpostien lähetys ei toimi, niiden Outlook -sovelluksessa. Suojatun sähköpostin avaamiseen ei tarvittu erillistä AIP -sovellusta.

7.2 Suojattu sähköposti

Suojatun sähköpostin käyttöönotto onnistui. Suojattua sähköpostia käytettään laitteiden selaimilla OWA:n kautta.

Tiedostojen lähettäminen onnistuu suojatun sähköpostin avulla, siinä pitää vain huomioida se, että tiedoston muokkaamin tai kopioiminen ei onnistu selaimessa. MacOS -tietokoneilla tässä tulee ongelma, varsinkin jos dokumentissa on paljon tietoja, jotka tulisi saada helposti kopioitua toiseen sovellukseen. MacOS -tietokoneiden tunnistusongelmien takia tietokoneelle ladattua dokumenttia ei voida avata, mutta Windows -tietokoneella tämä onnistuu.

8 Yhteenveto ja johtopäätökset

AIP on niin uusi palvelu, että muista organisaatioista ei ollut tullut ainakaan julkiseen käyttöön käyttöönottotutkimuksia, joita olisi voinut hyödyntää tässä työssä havaittuihin ongelmiin. Käyttöönottoprojektissa käytettiin tämän takia asiantuntijapalveluita, jotka olisivat voineet mahdollisesti löytää ratkaisun kuviossa 17 havaittuun ongelmaan. Projektin aikataulu, joka on kuvattu taulukossa 1 oli suuntaa antava. Aikataulussa pysyttiin ihan hyvin, vaikka MacOS -tietokoneessa havaittu ongelma hidasti käyttöönottoprojektia.

AIP -käyttöönottoprojektissa onnistuttiin ottamaan käyttöön suojattu sähköposti, joka lisäsi tietoturvaa ja täytti EU:n yleisen tietosuoja-asetuksen eli GDPR:n myötä tulleita vaatimuksia. Testauksessa päästiin haluttuun tulokseen Windows 10 -tietokoneilla, AIP -sovelluksella ja projektissa luoduilla konfiguraatioasetuksilla. Käyttöönotossa ei testausvaiheessa päästy onnistuneeseen käyttöönottoon MacOS -tietokoneilla ja Android -puhelimilla. Näistä MacOS -tietokone olisi ollut tärkeämpi saada toimimaan, jotta AIP voidaan ottaa organisaatiossa käyttöön halutulla tavalla.

Uusien MacOS -tietokoneiden määrä on lisääntynyt huomattavasti organisaation otettua CYOD:in käyttöön. Tämä vaikutti siihen, että AIP -palvelua ei voitu ottaa Windows 10 -tietokoneille käyttöön. Tämä aiheuttaisi ongelmia, koska organisaatiossa olevilla MacOS -tietokoneilla ei voitaisi avata AIP:lla suojattuja tiedostoja.

Onnistuneen suojatun sähköpostin käyttöönotto OWA:ssa tuo jo haluttua tietoturvaa Fidan sisäiseen ja ulkoiseen viestintään. Onnistunut sähköpostin suojaus mahdollisti CYOD:in käyttöönoton ja tuo tarvittavaa tietoturvaa mahdolliseen BYOD:in käyttöönottoon.

Onnistunut Windows 10 -testaus tuo jatkoa ajatellen tärkeää informaatiota mahdolliselta uudelta käyttöönottoprojektilta. Vaikka MacOS -tietokoneilla ja Android -laitteilla ei päästy haluttuun lopputulokseen testauksessa, tuo sekin hyvää informaatiota jatkoa ajatellen.

Microsoftin julkaistaessa toimivan Office -päivityksen ja AIP -sovelluksen, jolla voidaan suojaus saada MacOS -tietokoneille, on tällöin hyötyä niistä tiedoista, joita käyttöönottoprojektissa on havaittu testausvaiheessa.

Tämä opinnäytetyö oli luonteeltaan kehittämistutkimus ja tutkija osallistui kehittämistutkimukseen toimijana. Menetelmänä käytettiin osallistuvaa havainnointia.

Tutkimusta tehtiin tekemällä taustatyötä etsimällä tietoa eri lähteistä, jotka todettiin luotettaviksi. Palaverit olivat isona osana tutkimusta ja sidosryhmät olivat sitoutuneita saattamaan projektin päätökseen. Tehty muutos voidaan osoittaa olleen seurausta käytetystä interventiosta eikä muista tekijöistä. Tämä osoittaa kehittämistyön reliabiliteetin. Tutkimuksen lopputulos osoittaa, että on tutkittu oikeita asioita eli tutkimuksen validiteetti täyttyi.

9 Jatkokehitysehdotukset

Microsoftin julkaistessa tarvittavat päivityksen ja toimivan AIP -sovelluksen voidaan organisaatiossa aloittaa mahdollinen uusi käyttöönottoprojekti, jossa voidaan hyödyntää tässä kehittämistyössä havaittuja asioita.

Uuden käyttöönottoprojektiin voidaan lisäksi ottaa käyttöön AIP:n tarjoama AIP -skanneri, josta kerrottiin luvussa 3.5.3. AIP -skanneri tuo vielä parempaa suojausta organisaatioon, ottamalla käyttöön automaattisen skannauksen. Skannaustyökalu voitaisiin ottaa vain osalle käyttäjiä, jotka käsittelevät eniten tietosuojattua materiaalia. AIP -skanneri tarvitsee toimiakseen vain paremman lisenssin niiltä käyttäjiltä, joille se halutaan käyttöön. Lisäksi se tarvitsee nopean internetyhteyden sekä Windows server 2016- tai Windows server 2012 R2:n -tietokoneen, joka voi olla virtuaalinen.

10 Oman oppimisen arviointi

Kehittämistyöt eivät aina mene suunnitellulla tavalla, mutta käyttöönottoprojekti on tuonut paljon tarvittavia taitoja tulevaisuutta ajatellen. Käyttöönottoprojekti oli mielestäni erittäin antoisa ja mielenkiintoinen, koska aihe ei ollut entuudestaan tuttu minulle. Vaikka testausvaiheessa ei päästy kaikilla laitteilla haluttuun lopputulokseen, niin käyttöönottoprojekti on antanut paljon osaamista tulevaisuuden työelämääni. Tiivis yhteydenpito työpaikan edustajan kanssa ja käyttöönottovaiheessa kommunikointi asiantuntijapalveluiden ja Microsoftin asiantuntijan kanssa toi paljon hyviä kommunikointitaitoja, joita tarvitaan työelämässä.

Tiedonhaku ja uuden oppiminen on tuonut tarvittavia työelämän taitoja, koska tietojenkäsittelyn alalla tulee jatkuvasti uutta tekniikkaa, sovelluksia ja uutta tietoa, joita tulee oppia. Kehittämistyössä onnistuneesti otetun suojatun sähköpostin kouluttaminen organisaatiossa työskenteleville työntekijöille toi tarvittavia taitoja työelämääni.

Lähteet

Painetut

Heino, P. 2010. Pilvipalvelut. Helsinki: Talentum.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä: Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2015. Kehittämistutkimuksen kirjoittamisen käytännön opas: Miten kirjoitan kehittämistutkimuksen vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kavis, M. 2014. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Hoboken: John Wiley & Sons.

Marinescu, D. C. 2013. Cloud computing: Theory and practice. USA: Morgan Kaufmann.

Murugesan, S. & Bojanova, I. 2016. Encyclopedia of Cloud Computing. United Kingdom: John Wiley & Sons.

Ojasalo, K., Moilanen T. & Ritalahti J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3., uudistettu painos. Helsinki: Sanoma Pro.

Rizzo, T., Rais, R. B., Otegem, M. V., Bishop, D. Durzi, G., Tejada, Z. & Mann, D. 2012. Programming Microsoft's Clouds: Windows Azure and Office 365. Indiana: John Wiley & Sons.

Salo, I. 2010. Cloud computing: Palvelut verkossa. Jyväskylä: Docendo.

Sähköiset lähteet

Bergius, K. 2014. MIKÄ SE AZURE OIKEIN ON? Viitattu 19.2.2019. https://www.sulava.com/mika-se-azure-oikein/

Kangasniemi, H. & Lintulahti M. 2017. Mikä on pilvipalvelu? Viitattu 7.5.2019. https://yksityisille.hub.elisa.fi/mika-on-pilvipalvelu/

Fida International Ry. Fida International ry:n esittely yhdistyksen kotisivulta. Viitattu 12.12.2018. https://www.fida.info/medialle/fida-lyhyesti/

Keijo, K. 2014. MICROSOFT AZURE WEBSITES – WEBBISOVELLUS KÄYTTÖÖN MINUUTEISSA. Viitattu 20.2.2019. https://www.sulava.com/microsoft-azure-websites-webbisovellus-kayttoon-minuuteissa/

Kevin, M. 2018. Installation, Configuration, and Usage of the AIP Scanner. Viitattu 26.3.2019. https://techcommunity.microsoft.com/t5/Azure-Information-Protection/Installation-Configuration-and-Usage-of-the-AIP -Scanner/ba-p/221792

Microsoft Azure. Azure Information Protection pricing. Viitattu 31.1.2019. https://azure.microsoft.com/en-gb/pricing/details/information-protection/

Microsoft Office. Sähköposti Outlook Web Appissa. Viitattu 7.5.2019. https://support.office.com/fi-fi/article/s%C3%A4hk%C3%B6posti-Outlook -web-appissa-ed7b1cb9-ef40-4fbd-a302-278cc7f4dcf5

Microsoft. 2017. EU:n tietosuoja-asetus askarruttaa suomalaisorganisaatioita – myös Microsoft valmistautuu uudistukseen. Viitattu 28.11.2018. https://news.microsoft.com/fi-fi/2017/03/22/eun-tietosuoja-asetus-askarruttaa-suomalaisorganisaatioita-myos-microsoft-valmistautuu-uudistukseen/

Microsoft. 2018a. What is Azure Infromation Protection. Viitattu 2.11.2018. https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Microsoft. 2018b. User Guide: Track and revoke your documents when you use Azure Information Protection. Viitattu 5.11.2018. https://docs.microsoft.com/en-us/azure/information-protection/rms-client/client-track-revoke

Microsoft. 2018c. What is Azure Rights Management? Viitattu 21.2.2019. https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms

Microsoft. 2019a. How does Azure RMS work? Under the hood. Viitattu 21.2.2019. https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work

Microsoft. 2019b. Deploying the Azure Information Protection scanner to automatically classify and protect files. Viitattu 27.2.2019. https://docs.microsoft.com/en-us/azure/information-protection/deploy-AIP -scanner

Microsoft. 2019c. Quickstart: Get started with Azure Information Protection in the Azure portal. Viitattu 18.3.2019. https://docs.microsoft.com/en-us/azure/information-protection/quickstart-viewpolicy

Microsoft. 2019d. Tutorial: Edit the Azure Information Protection policy and create a new label. Viitattu 22.3.2019. https://docs.microsoft.com/en-us/azure/information-protection/infoprotect-quick-start-tutorial

Microsoft. 2019e. Office 365 Message Encryption FAQ. Viitattu 25.3.2019. https://docs.microsoft.com/fi-fi/office365/securitycompliance/ome-faq

Tietosuojamalli. GDPR - EU:n uusi tietosuoja-asetus. Viitattu 7.5.2019. https://fakta.tietosuojamalli.fi/aihe/gdpr

Julkaisemattomat

Fidan IT-kumppani

Micorsoft asiantuntija

Suomalainen IT-konsultointi yritys

Kuviot

Taulukot