Haaga-Helia
ammattikorkeakoulu Oy

Microsoft Intune mobiililaitehallinnan mahdollisuudet yrityksen datan suojaamiseksi

Aleksi Berghem

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2019

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t) Aleksi Berghem	
Koulutusohjelma Tietojenkäsittelyn koulutusohjelma	
Raportin/Opinnäytetyön nimi Microsoft Intune mobiililaitehallinnan mahdollisuudet yrityksen datan suojaamiseksi	**Sivu- ja liitesivumäärä** 52+0

Tämän työn tavoitteena on tutkia millä tavoin yrityksen dataa voidaan suojata mobiililaitteilla tietoturvallisesti Microsoft Intune järjestelmän mobiililaitehallinnan avulla sekä sen ominaisuuksilla ja kuinka sillä voidaan ehkäistä yleisimpiä tietoturvaongelmia mobiililaitteissa. Datan sisältö voi olla esimerkiksi arkaluontoisia sähköposteja tai tiedostoja.

Teoriapohjana työssä käydään läpi pilvipalveluita sekä mobiililaitteiden tietoturvauhkia ja niiden ehkäisyä. Osana teoriaa on myös kuvaus järjestelmästä sekä sen ominaisuuksista. Näitä käytettiin pohjana toiminnallisen osuuden rakentamiselle työhön, johon sisältyy määritykset sekä testaus. Määritykset järjestelmään tehtiin teorian pohjalta. Testausta varten tehtiin määritysten pohjalta käyttötapauksia, joissa pidettiin silmällä yritysten tarpeet mobiililaitteiden käytössä. Tarpeisiin sisältyy yritysten resurssien erottaminen henkilökohtaisista resursseista, joka on tietoturvan kannalta tärkeä osa-alue. Toiminnallinen osuus tuo tutkimukseen selkeämmin hahmotettavan kokonaisuuden, joka sisältää järjestelmän ominaisuuksien toimivuuden käytännössä teoriassa havaittuihin yleisimpiin tietoturvaongelmiin mobiililaitteilla.

Työssä onnistuttiin luomaan testiympäristö, jonka avulla teoriassa esiteltyjen tietoturvaongelmien ehkäisyä pystyttiin havainnollistamaan järjestelmän avulla. Työn kokonaisuus sisälsi teorian, järjestelmän kuvauksen, määritykset, käyttötapaukset ja testauksen. Tämä luotu kokonaisuus yhdessä vastasi esitettyyn tutkimuskysymykseen. Testiympäristössä tuotettu suojauksen taso oli kuitenkin osittain puutteellinen teorian perusteella. Havaittuja puutteita on käsitelty ja perusteltu osana pohdintaa sekä osittain työn aikana.

Asiasanat
Pilvipalvelu, Tietoturvauhka, Microsoft Intune, Mobiililaitehallinta

Sisällys

Sanasto

SaaS (Software as a Service) Ohjelmisto pilvipalveluna tarjoaa ylläpidetyn ohjelmiston käyttäjälle.

PaaS (Platform as a Service) Alusta pilvipalveluna tarjoaa asiakkaalle virtuaalisen palve linympäristön.

IaaS (Infrastructure as a Service) Infrastruktuuri pilvipalveluna tarjoaa asiakkaalle virtuaa lisen konesalin tai -saleja internetin kautta, joita palveluntarjoaja ylläpitää.

IDS (Intrusion Detection System) on ohjelmoitu tunnistamaan palvelunestohyökkäykset ja se asennetaan tietoverkkoon.

iSCSI (Internet Small Computer Systems Interface) on datan siirtoon verkkojen yli käytetty standardi.

FC (Fibre Channel) avulla voidaan liittää massamuistilaitteita palvelimiin. Tekniikka on verkkoteknologiaa, jonka avulla päästään suuriin datan siirto nopeuksiin.

Microsoft Azure Microsoftin ylläpitämä pilvipalvelukokonaisuus, joka tarjoaa palveluita yrityksille ja yksityisille käyttäjille.

Etäyhteys Tällä tarkoitetaan verkon yli otettavaa yhteyttä toiseen verkossa laitteeseen. Näin pystytään seuraamaan esimerkiksi toisen työaseman näyttöä sekä hallinnoimaan sitä.

Haittaohjelma Tietokoneohjelma, jolla ulkopuolinen taho aiheuttaa tarkoituksellisesti ei-toivottuja tapahtumia vastakkaiselle osapuolelle tietokoneissa tai tietojärjestelmissä.

Kalastelu Sähköpostiviestien välityksellä tapahtuvaa tunnusten kaappaamista. Näissä yleensä huijataan käyttäjää painamaan linkkiä ja syöttämään esimerkiksi sähköposti tunnuksensa.

Palvelunestohyökkäys Verkkohyökkäys, jolla pyritään estämään käyttäjien pääsy hyökättävälle verkkosivulle.

Käytänne Käytössä oleva menettely tai tapa.

Sovellusten suojaus käytänteet Menettely tapoja, joiden avulla varmistetaan, että tiedot pysyvät suojassa hallinnoidussa sovelluksessa.

Laitteiden sopivuus käytänteet Sääntöjä ja asetuksia, joiden ehdot käyttäjien ja laitteiden on täytettävä, jotta ne voidaan rekisteröidä järjestelmään.

Ehdollinen pääsy Microsoft Azuressa käytetty työkalu, jonka avulla voidaan hallinnoida pääsyä suojattuihin resursseihin. Jos käyttäjä haluaa päästä käsiksi resurssiin, hänen pitää suorittaa vaadittu toimenpide, jonka järjestelmänvalvoja on määritellyt järjestelmään.

System Center Configuration Manager Microsoftin kehittämä järjestelmä, jonka avulla voidaan hallita laitteita sekä sovelluksia.

Monivaiheinen tunnistautuminen Kirjautumisen yhteydessä tunnusten syöttämisen lisäksi vaaditaan, että käyttäjä vahvistaa kirjautumisen mobiililaitteellaan.

Liikkuvuuspakettistrategia (Enterprise Mobility + Security) Microsoftin yrityksille tarjoama palvelukokonaisuus, joka pitää sisällään tietoturvallisia ratkaisuja työskentelyyn liikkeessä.

Azure Active Directory Premium P2 lisenssi Lisenssi tarjoaa käyttäjänhallintaan liittyviä ominaisuuksia Microsoft Azure pilvipalvelussa.

Intune lisenssi Tarjoaa käyttäjälle pääsyn Microsoft Intune järjestelmän ominaisuuksiin.

Office 365 E5 lisenssi Sisältää tavallisimmat Microsoft Office toimistotyökalut pilvessä sekä paikallisesti käytettävinä sovelluksina.

Microsoft Authenticator Microsoftin oma monivaiheiseen tunnistautumiseen käytettävä mobiilisovellus.

Tietojen salaus Menetelmä, joita käytetään tiedostojen tai laitteiden suojaamiseen. Tiedot suojataan monimutkaisella avaimella, joka on käytännössä merkkijono. Tietoihin pääsee käsiksi vain tällä avaimella.

URL-osoite Tiedoston tai verkkosivun sijainti internetissä esimerkiksi Googlen sijainti on www.google.fi.

Azure Information Protection Microsoftin tarjoama pilvipalvelu Azuressa, jonka avulla voidaan eritellä dokumentteja ja sähköposteja etikettien avulla.

Microsoft Exchange Microsoftin tuottama palvelu, jossa sähköpostit ja kalenterit pyörivät hallinnoidulla palvelimella.

Microsoft Sharepoint Microsoftin tuottama palvelu, jonka avulla voidaan luoda sivustoja sekä tallentaa tiedostoja esimerkiksi pilveen tai paikalliselle palvelimelle.

Järjestelmänvalvoja Henkilö, jolla on oikeudet hallinnoida järjestelmän palveluita, käyttäjätilejä sekä laitteita.

Mobiililaitteiden uhkien torjuntatyökalut Nämä ovat työkaluja, jonka avulla mobiililaitteissa ehkäistään haittaohjelmia kyseisessä laitteessa.

Synkronointi Tietotekniikassa yleisesti käytetty termi, joka voi liittyä datan tai prosessien synkronointiin. Prosessien synkronointi tarkoittaa, että ne etenevät samanaikaisesti. Datan synkronointi tarkoittaa, että tietojen kopioimista laitteesta tai ohjelmasta toiseen.

1 Johdanto

Tämän työn tavoitteena on tutkia millä tavoin yrityksen dataa voidaan suojata mobiililaitteilla tietoturvallisesti Microsoft Intune -järjestelmän mobiililaitehallinnan avulla sekä sen ominaisuuksilla ja kuinka sillä voidaan ehkäistä yleisimpiä tietoturvaongelmia mobiililaitteissa. Datan sisältö voi olla esimerkiksi arkaluontoisia sähköposteja tai tiedostoja.

Tietoturvan ja tietosuojan lisääntynyt tarve on yleinen huolenaihe niin yrityksille kuin yksittäisille käyttäjille ja ihmisiä kiinnostaa yhä enemmän mihin yritykset tietoja käyttävät. Henkilötietoja käsittelevien yritysten on erityisen tärkeää nykypäivänä suojata laitteensa ja järjestelmänsä tavoilla, jotka ennaltaehkäisevät tietojen pääsyn vääriin käsiin. Tietosuojarikkeet ja niistä koituvat rangaistukset sekä vaikutukset voivat olla mittavia ja haitata yrityksen toimintaa huomattavasti. Etätyöskentely on yhä yleisempää, joka on lisännyt kontrollin tarvetta laitteille, jotka sisältävät ja pääsevät käsiksi yrityksen resursseihin. Työtä varten valitsin ohjelmistojätti Microsoftin pilvialustalla toimivan laitteiden ja sovellusten hallintajärjestelmän, pilvipalveluiden yleistyneen käytön vuoksi. Pilvipalveluiden saatavuus ja ominaisuudet ovat kehittyneet valtavasti, joka houkuttelee uusia yrityksiä ottamaan palveluita käyttöön omaan ympäristöön.

Tarkoituksena työssä on käydä teoriaosuudessa läpi pilvipalveluita, keskeisiä mobiililaitteissa esiintyviä tietoturvauhkia sekä keinoja millä niitä voidaan ennaltaehkäistä. Teoriaan sisältyy myös kuvaus järjestelmästä sekä sen ominaisuuksista ja vaatimuksista. Työn aikana tehdään testiympäristö, johon tehdään määritykset teorian pohjalta tehtyjen havaintojen perusteella. Tehdyt määritykset käydään läpi työssä ja niitä perustellaan teoriaan vedoten. Määritysten pohjalta luodaan yksinkertaisia käyttötapauksia, joiden avulla järjestelmän ominaisuuksia testataan käytännössä. Testauksessa käytetään Android-pohjaista mobiililaitetta ja sovelluksina käytetään Microsoftin tarjoamia perinteisiä toimistotyökaluja.

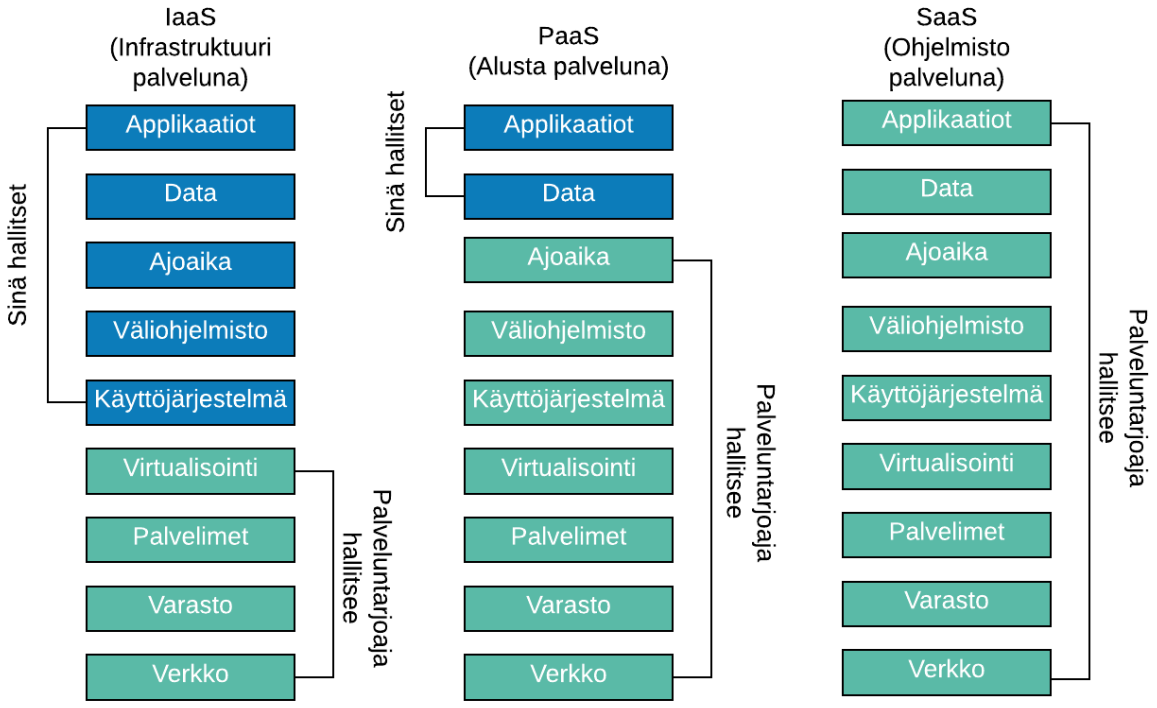
Testaus tuo toiminnallisen osuuden työhön vahvistamaan tutkimustyötä ja havainnollistamaan järjestelmän ominaisuuksia. Tarkoituksena on tutkia, kuinka järjestelmä pystyy tarjoamaan ominaisuuksillaan ratkaisuja havaittuihin yleisiin tietoturvaongelmiin mobiililaitteilla sekä huomioidaan nekin ongelmat, joihin järjestelmä ei tarjoa ratkaisua.

2 Pilvipalvelut

Pilvipalvelut ovat yksinomaan internetin kautta saatavia palveluita, jonka perustana on pilvilaskenta. Pilvipalveluiden laskutus perustuu niiden käyttötarpeeseen, jotka tekevät niistä edullisia vaihtoehtoja perinteisiin ratkaisuihin verrattuna. Pilvessä tapahtuvien palveluiden käyttäminen tuo myös joustavuutta hankintoihin, sillä tilaa tai mitä tahansa palvelua, jota olet käyttämässä voi aina hankkia lisää muutamalla klikkauksella. Niiden hyödyntäminen auttaa myös ohjaamaan resurssit palveluiden kehittämiseen, kun infrastruktuurin ylläpito vaatii vähemmän organisaatiolta itseltään. Laaja määrä erilaisia palveluita tuo nopeutta yrityksen toimintaan, kun yrityksen IT-infrastruktuuri rakennetaan pilveen. (Amazon Web Services 2019.)

2.1 Pilvipalveluiden mallit

Pilvipalvelut luokitellaan päätyyppeihin toteutustavan perusteella. Päätyyppejä on muutamia ja niiden toteutustapa kertoo, minkälaisia ominaisuuksia pilvipalvelu sisältää. Asiakas voi valita tarpeidensa mukaan, mitä palvelutyyppiä tarvitsee. (Heino 2010, 38-42; Microsoft Azure 2019.)



Kuva 1. Pilvipalveluiden mallit (Ensi-Maria 1.8.2017.)

Kuvassa 1 on havainnollistettu mitä eri pilvipalveluiden mallit pitävät sisällään ja mitä asiakas saa kustakin palvelusta. Pilvipalvelu mallit vasemmalta oikealle: infrastruktuuri pilvi-

palveluna (IaaS), alusta pilvipalveluna (PaaS) ja ohjelmisto pilvipalveluna (SaaS). Jokaiseen palveluun on erikseen merkitty sinisellä värillä, mitä asiakas itse hallitsee. Turkoosilla on merkitty osa-alueet, joita palveluntarjoaja ylläpitää ja hallitsee. SaaS-tyyppinen ratkaisu ei esimerkiksi vaadi asiakkaalta ylläpitoa ja hallintaa. (Ensi-Maria 1.8.2017.)

2.1.1 Ohjelmisto palveluna (SaaS)

Ohjelmisto palveluna on pilvipalvelu, jossa käyttäjät hyödyntävät pilveen rakennettuja sovelluksia internetin yli. Yleisimpiä esimerkkejä näistä ovat sähköposti, kalenterit ja toimistotyökalut. Microsoft Office 365 on pilvessä toimiva ohjelmisto palveluna. Käyttäjä maksaa sovelluksista, joita käyttää palveluntarjoajalle eikä muusta. Pilvessä olevat sovellukset yleensä vuokrataan ja niitä käytetään useimmiten selaimen kautta. Kaikki niihin liittyvä infrastruktuuri ja data sijaitsee palveluntarjoajan palvelinkeskuksessa. Palveluntarjoajan tehtävänä on ylläpitää palvelun saatavuutta ja turvallisuutta koskien applikaatiota ja käyttäjän dataa. Microsoft Outlook on esimerkki ohjelmisto palveluna tyyppisestä sovelluksesta, kun sitä käytetään selaimen kautta. (Microsoft Azure 2019.)

2.1.2 Alusta palveluna (PaaS)

Alusta palveluna on pilvipalvelu, jossa palveluntarjoaja tarjoaa täysin virtuaalisen palvelinympäristön ja asiakkaat saavat siitä osuutensa tarpeidensa mukaan. Näin ollen asiakas käyttää palvelun tarjoamaa kapasiteettia ja työkaluja ohjelmointirajapinnalla, jonka avulla voidaan teettää sovelluksia, joita asiakas hyödyntää itse. Asiakkaalle tarjotaan käyttöliittymä, joka sisältää siinä olevan hallintakonsolin palvelun käyttämiseen. Tämän tyyppinen pilvipalvelu kuitenkin vaatii asiakkaalta panosta ympäristön rakentamista varten omaan käyttöönsä. Loppukäyttäjä hyödyntää asiakkaan luomaa palvelua selaimen kautta. Tunnetuilla palveluntarjoajilla on hyviä olemassa olevia alusta palveluna ratkaisuja. Niitä tarjoavat esimerkiksi Google, Microsoft ja Salesforce. (Heino 2010, 38-39.)

2.1.3 Infrastruktuuri palveluna (IaaS)

Infrastruktuuri palveluna on pilvipalvelu, jossa palveluntarjoaja tarjoaa virtuaalisen konesalin tai -saleja internetissä. Palveluntarjoaja myös ylläpitää niitä. Asiakkaalle annetaan käyttöön konesalista tarvittava osuus ja hinnoittelu tapahtuu sen perusteella. Asiakas käyttää oman lohkonsa, asentamalla siihen valitsemansa käyttöjärjestelmän ja sovellukset. Palvelua voi hyödyntää esimerkiksi toissijaiseen objektipohjaiseen tallennustilaan, iSCSI- tai FC tyyppistä pääasiallista blokkitallennustilaa varmuuskopiointimahdollisuuksineen. Virtuaalikoneet ovat myös yleisessä käytössä olevia infrastruktuuri palveluna tyyppisiä ratkaisuja. Tämäkin palvelu vaatii asiakkaalta osaamista palvelun käyttöönotossa sekä ylläpidossa.

Asiakkaan käyttöliittymä sisältää komentorivityökaluja ja palvelun sisällä olevan hallintakonsolin. Amazon Web Services on tunnettu palveluntarjoaja, joka tarjoaa infrastruktuureja palveluina pilvessä. (Heino 2010, 39.)

2.2 Pilvipalveluiden turvallisuus

Pilvipalvelut ovat tietoliikenneyhteyksien takana olevia kolmannen osapuolen omistamia ja ylläpitämiä palveluita, jotka sijaitsevat todennäköisesti kokonaan toisessa maanosassa ja asiakas käyttää yleensä lohkoa virtuaalisesta palvelimesta. Ajatus tästä saattaa herättää asiakkaassa huolta koskien tietoturvaa. Pilvipalveluissa tekninen osa suojataan useilla tietoliikenne- ja palvelintekniikan metodeilla. Palveluntarjoajan ylläpitämä infrastruktuuri suojataan haitalliselta liikenteeltä palomuurin avulla. Palomuurin tarkoitus valvoa liikennettä organisaation suuntaan ja se päästää läpi vain sallitun liikenteen. Palveluntarjoaja suojaa yleensä oman infrastruktuurin palomuurin lisäksi tunkeutumisen havaitsemisjärjestelmällä eli Intrusion Detection System (IDS). Tämänkaltainen järjestelmä on yleensä laite tai ohjelmisto asennettuna palvelimeen. (Heino 2010, 68.)

Data, joka ohjautuu pilvipalveluun, salataan kryptauksen avulla. Tämä tarkoittaa, että vaikka tunkeutuja pääsisi pilvipalveluun sisään siellä oleva tieto ei ole luettavassa muodossa. Kryptaus vaatii ohjelmiston ja salausavaimia varten jonkinlaisen metodin tallentaa ne turvallisesti. Kryptaus on asiakkaan vastuulla, sillä suojausta varten tarvittavan avaimen tulisi olla tiedossa vain tiedon omistavalla taholla. (Heino 2010, 68.)

Mahdollisia uhkia, jotka on syytä ottaa huomioon pilvipalveluita käytettäessä:

- Vika koskien tietoliikenneyhteyksiä, voi estää pääsyn asiakkaalta pilvipalveluun. Tällöin pääsy sovelluksiin tai dataan estyy, joka on palvelun sisällä.
- Palveluntarjoajan osalta inhimillisen virheen sattuessa, tietyn asiakkaan tai asiakkaiden data voi korruptoitua esimerkiksi laiterikon takia. Tähän voi myös liittyä palveluntarjoajaan laitteistoon kohdistunut vahinko, jossa laitteisto tuhoutuu esimerkiksi tulipalossa. (Heino 2010, 70.)

Pilvipalveluihin liittyvä tietosuoja koskien yritystä tai yksilöä on vaikeampi osa-alue verrattuna tietoturvaan. Tietoturvaan liittyvät asiat koskevat laitteistoa, jota palveluntarjoaja ylläpitää ja käytännössä niistä saadaan hyvinkin turvallisia eri menetelmin. Tietosuojan ongelmat liittyvät suoranaisesti lainsäädäntöön. (Heino 2010, 72.)

Yritysten kannattaa hyödyntää pilvipalveluiden turvallisuuden arvioinnissa Liikenne- ja viestintävirasto Traficomin luomaa pilvipalveluiden turvallisuuden arviointikriteeristöä. Jul-

kaisusta löytyy tietoa, jonka avulla voidaan arvioida henkilöstön, tietoliikenteen, tietojärjestelmien, tietoaineistojen, fyysistä sekä käytön turvallisuutta pilvipalveluissa. Sen laadinnassa on huomioitu uusiutuva lainsäädäntö sekä sitä kehitetään ja ylläpidetään kyberturvallisuuskeskuksen toimesta. Julkaisussa kuvatut turvallisuusvaatimukset ovat luotu siten, että tavallisimmat riskit voidaan pitää siedettävällä tasolla, kun kyseessä on salassa pidettäviä tietoja pilvipalveluissa. (Kyberturvallisuuskeskus 2019.)

3 Mobiililaitteiden tietoturvauhat ja niiden ehkäiseminen

Tässä kappaleessa käydään läpi tavallisimpia skenaarioita, joissa mobiililaite voi muuttua tietoturvauhaksi yritykselle tai tavalliselle käyttäjälle. Tarkoituksena on havaita yleisempiä uhkia näihin liittyen, käyttämällä erilaisia lähteitä koskien aihetta. Havaintojen pohjalta kerätään eri lähteitä käyttäen toimenpiteitä, joilla voidaan ennaltaehkäistä haavoittuvuuksia.

Yleisimmät tietoturvauhat liittyen mobiililaitteiden tietoturvariskeihin, joita kappaleessa käydään läpi ovat: tietovuoto, käyttäjän manipulointi, julkiset Wi-Fi yhteydet, laitteen vanhentunut ohjelmisto, heikot salasanat sekä fyysiset murrot laitteisiin. Yleisten uhkien lisäksi käydään läpi ennaltaehkäisy menetelmiä, joita ovat: pääsykoodien käyttäminen, etätyhjennyksen mahdollistaminen, salauksen käyttäminen, mobiililaitteiden uhkien torjuntatyökalut sekä yrityksen omien linjausten tekemisen vaikutus ennaltaehkäisyssä.

3.1 Tietovuoto ja käyttäjän manipulointi

Tietovuodot ovat erityisesti yrityksille haasteellisia ongelmia, koska niiden vaikutukset voivat olla mittavia liittyen yrityksen toimintaan, varsinkin jos kyseinen yritys käsittelee henkilötietoja. Usein ongelmana on käyttäjän toiminta, jossa käyttäjä sallii sovelluksen käyttää ja siirtää tiettyjä tietoja puhelimesta. Tietovuoto voi tapahtua käyttäjän virheen takia esimerkiksi, kun käyttäjä siirtää yrityksen tietoja julkiseen pilveen, liittää luottamuksellista tietoa väärään paikkaan tai edelleen lähettää jonkin sähköpostin väärälle vastaanottajalle. (Raphael 22.7.2019.)

Käyttäjän manipuloinnissa noin 90% tapauksista alkaa sähköpostiviestistä. Tällaiset sähköpostiviestit sisältävät yleensä linkin, jonka valitsemiseen käyttäjä houkutellaan eri tavoin. Linkki on yleensä vaarallinen tai sen tarkoituksena on hankkia luottamuksellista tietoa. Ongelma koskee myös pöytäkoneita, mutta käyttäjät tekevät virheen todennäköisemmin mobiililaitetta käytettäessä. Tämän takana voi olla ruudun pienempi koko, vähemmän yksityiskohtia viestissä tai ilmoituspalkissa mahdollistettu linkkien painaminen suoraan. Sähköpostien lisäksi kalasteluyrityksiä voi tulla myös sosiaalisen median applikaatioiden kautta kuten WhatsApp:in kautta. (Raphael 22.7.2019.)

3.2 Julkiset Wi-Fi yhteydet ja mobiililaitteiden uhkien torjuntatyökalut

Mobiililaite on yhtä turvallinen kuin verkko, jota kautta se siirtää dataa. Nykyaikana julkiset verkot ovat hyvin yleisiä ja näissä piilee yleensä haavoittuvuuksia. Julkisen verkon käyttäminen oman mobiilidatan sijaan voi olla riski. Julkisessa verkossa muut voivat nähdä tie-

tosi. Kun laite on yhdistetty julkiseen langattomaan verkkoon se lähettää tietoja verkkosivujen tai mobiilisovellusten kautta. Näitä tietoja hakkerit pystyvät hyödyntämään ja mahdollisesti vahingoittamaan niitä. (Raphael 22.7.2019; Mazyar 31.11.2019.)

Mobiililaitteiden uhkien torjuntatyökalut tuovat suojaa uhkille, mutta eivät kuitenkaan yksinään estä käyttäjän omia virheitä aiheuttamasta uhkia laitteelle. Tyypillisesti nämä työkalut ovat luotu suojaamaan laitteita haittaohjelmilta, kalastelulta sekä palvelunestohyökkäyksiltä. Tämä auttaa esimerkiksi suojaamaan käyttäjän tietoja julkisissa langattomissa verkoissa suojaamalla yhteyden. (Gray 11.7.2018.)

3.3 Heikot salasanat ja pääsykoodien käyttäminen

Heikot salasanat ovat hyvin yleisiä, käyttäjät harvoin itse käyttävät oikeanlaista tapaa suojatakseen tilejänsä. On yleistä, että yritysmaailmassa käyttäjät käyttävät henkilökohtaisia sekä yrityksen omistamia tilejä puhelimellaan. Tämä on ongelmallista, jos käyttäjä käyttää paljon samoja salasanoja eri tileillä. Verizonin 2017 vuonna tuottaman raportin mukaan heikot salasanat olivat syynä 80% tietomurroista yrityksissä. (Raphael 22.7.2019.)

Pääsykoodit ovat tavallisimpia keinoja suojata mobiililaitteita väärinkäytöltä. Niiden tulisi kuitenkin olla tarpeeksi vahvoja, jotta pääsy laitteeseen ei ole liian helppoa. Neljä numeroinen pääsykoodi ei vaadi tarpeeksi montaa yritystä, että laitteeseen ei päästäisi käsiksi lyhyessä ajassa. Mitä enemmän numeroita koodissa käytetään, sitä enemmän on luonnollisesti olemassa vaihtoehtoja oikealle pääsykoodille. (Deloitte 2014.)

Hyvä salasana koostuu numeroiden lisäksi myös kirjaimista. Kun salasanasta tehdään vahvempi, sen murtaminen vaatii enemmän yrityksiä. Vahva salasana voi olla 16 merkkiä pitkä ja sisältää numeroiden lisäksi erikoismerkkejä ja kirjaimia. Näin jokaisen merkin kohdalla on useampi vaihtoehto mikä siihen voi sopia, jos pääsykoodia yritetään murtaa. Useimmissa mobiililaitteissa on valmiiksi suojaus, joka lukitsee puhelimen, kun epäonnistuneita avaamisyrityksiä on tehty tarpeeksi. Lukituksen pituus kasvaa joka kerta eksponentiaalisesti. (Deloitte 2014.)

3.4 Fyysiset murrot laitteisiin ja etätyhjennys

Hävinnyt tai varastettu laite on aina suuri tietoturvauhka yritykselle, varsinkin jos laitetta ei ole suojattu tarpeeksi vahvalla suojauksella tai laitteen tietoja ei ole suojattu. Laitteita voidaan suojata esimerkiksi käyttämällä vahvaa PIN-koodia, salaamalla laitteen tiedot ja käyttämällä lukitusnäytön suojausta. Vahva PIN-koodi on monimutkaisempi kuin 0000, 1234 tai oma syntymäaika. (Raphael 22.7.2019.)

Etäyhteyden avulla tehty laitteen tyhjennys on hyvä keino tuhota laitteen tiedot, kun se häviää tai varastetaan. Etäyhteydellä tehty tyhjennys vaatii laitteen olevan yhdistettynä joko puhelimen omaan tai langattomaan verkkoon. Jos puhelimesta on poistettu SIM-kortti tai se ei ole yhteydessä verkkoon etänä tyhjentäminen ei onnistu. Etätyhjentäminen vaatii verkkoyhteyden, jotta se voidaan suorittaa. (Deloitte 2014.)

3.5 Salauksen käyttäminen ja vanhentunut ohjelmisto

Täysi datan salaaminen suojaa mobiililaitteen kaikki sen sisällä olevat tiedot. Täyden salaamisen idea on, että laitteen tiedot salataan laitteisto tasolla ja suojausta ei voida purkaa ilman avainta. Laitteiston tason suojaus on sitä, että itse fyysinen komponentti on salattu, eikä pelkästään yksittäinen sovellus sen sisällä. Tämä tarkoittaa siis sitä, että vaikka laitteen osat siirretään toiseen laitteeseen, niitä ei voida hyödyntää ilman tarvittavaa avainta. Mobiililaitteissa yleensä on tarjolla erillinen osa laitteesta, joka on suojattu datan säilytystä varten. Laitteet, joiden data on suojattu salauksella, eivät vaadi erillistä ilmoitusta laitteen katoamisesta. (Securitymetrics 2019.)

Mobiililaitteissa, kuten kaikissa muissakin laitteissa, vanhentunut ohjelmisto tuo aina uusia haavoittuvuuksia esille laitteessa. Mobiililaitteiden osalta ei ole olemassa varmuutta säännöllisistä järjestelmäpäivityksistä. Ongelma koskee etenkin Android-pohjaisia laitteita. Suurin osa valmistajista ovat tehottomia tuomaan säännöllisiä päivityksiä laitteilleen. Osa ongelmasta koskee kuitenkin käyttäjiä, laitteet tulisi pitää ajan tasalla, kun päivityksiä tulee laitteisiin tai sovelluksiin. (Raphael 22.7.2019.)

3.6 Yrityksen omat linjaukset tehostamaan suojauksen tasoa

Yrityksen asettamat linjaukset liittyen tietoturvaan ovat suuressa merkityksessä tietoturvan vahvistamisessa omassa ympäristössä. Sen lisäksi tietoturvaan tulisi huomioida käytettävät laitteet, niiden päivittäminen ja käytänteiden toimivuuden takaaminen laitteissa. (Montgomery 11.9.2019.)

Ensimmäinen askel tietoturvalliseen ympäristöön on havaita heikot kohdat yrityksen tietoturvassa ja asettaa tietyt standardit, joita yrityksen tulee noudattaa liittyen mobiililaitteiden käyttöön. Alkuun on hyvä huomioida mitä laitteita on jo käytössä sekä kuka pääsee käsiksi mihinkin tietoihin ja laitteisiin. Sen jälkeen luodaan rajat normaalille käyttäytymiselle, mikä tulee laitteiden käyttöön esimerkiksi mitä sovelluksia saa käyttää. Kun rajat on luotu, niitä voidaan noudattaa normien omaisesti yrityksen sisällä ja ne ovat kaikille selkeitä toimintamalleja. (Montgomery 11.9.2019.)

Toinen askel koostuu käytännöistä, jotka luodaan uhkia varten. Laitteet tulisi rekisteröidä järjestelmään, josta niitä voidaan hallita ja järjestelmä tarjoaa tärkeää dataa, koskien esimerkiksi laitteen järjestelmäpäivityksen tilaa. Luodaan monivaiheisen tunnistautumisen sääntö sisäänkirjautumisiin, rajoitetaan laitteiden pääsyä langattomiin verkkoihin ja estetään käyttäjiä lataamasta ei tunnettuja sovelluksia laitteisiinsa. Kun näitä asioita voidaan rajoittaa järjestelmää hyödyntämällä, voidaan myös ennaltaehkäistä jatkossa uusia haavoittuvuuksia, kun laitteiden käyttöä seurataan aktiivisesti järjestelmän avulla. Tilanteissa, joissa havaitaan uusia ongelmia, voidaan reagoida nopeasti ja pystytään estämään niiden tapahtumista myös jatkossa. (Montgomery 11.9.2019.)

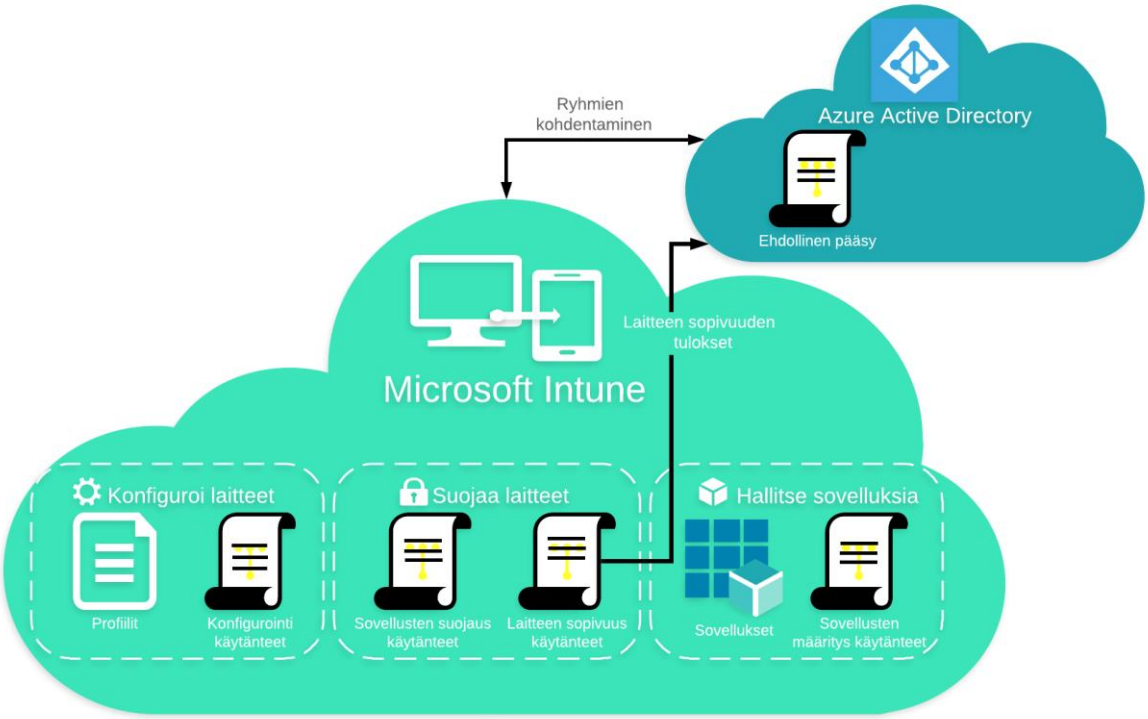
Kolmas askel sisältää jonkin mobiililaitteille soveltuvan uhkien torjuntatyökalun valitsemisen käytettäväksi laitteilla. Näin voidaan varmistaa nopea vasteaika korjaaville toimille uhan kohdatessa, joka mahdollisesti auttaa minimoimaan siitä koituvat haitat. Kun hyökkäyksiin voidaan vastata, voidaan myös taata nopea palautuminen niistä. Tämä voi pitää sisällään työntekijän ja asiakkaan tietojen lukitseminen, jotka ovat joutuneet hyökkäyksen kohteeksi. Sen lisäksi täytyy pystyä erittelemään haavoittuneet tai kadonneet laitteet. (Montgomery 11.9.2019.)

4 Microsoft Intune

Tässä luvussa käydään läpi Microsoft Intune järjestelmää ja sen ominaisuuksia sekä olennaisena osana sivutaan hieman Azure Active Directoryn roolia osana järjestelmäkokonaisuutta. Sen lisäksi luku sisältää vaatimukset Microsoft Intune järjestelmälle sekä siihen tehtävät määritykset testausta varten.

Azure Active Directory on yrityksille suunnattu järjestelmä, jonka avulla käyttäjiä voidaan yksilöidä eli se tarjoaa työkaluja käyttäjänhallintaan pilvessä. Se tarjoaa kertakirjautumismahdollisuuden useaan eri palveluun sekä sisältää monivaiheisen tunnistautumisen ominaisuuden. Monivaiheinen tunnistautuminen ennaltaehkäisee hyökkäyksiä kohdistuen yrityksien tileille tehokkaasti. Azure Active Directory sisältää ehdollisen pääsyn määritykset, jotka ovat iso osa järjestelmien käytön suojaamista. (Microsoft Azure 2019.)

Microsoft Intune on Microsoft Azure pilvialustalle rakennettu järjestelmä, joka keskittyy mobiililaitteiden ja applikaatioiden hallintaan. Järjestelmän tarkoitus on turvata työnteon tehokkuus ja datan suojaaminen. Järjestelmä on integroitu Microsoft 365 ja Azure Active Directory:n palveluiden kanssa. Tällä yhdistelmällä kontrolloidaan, kenellä on pääsy järjestelmään ja sen sisältöön. Sen lisäksi järjestelmä on yhdistetty Azure Information Protection palvelun kanssa, jolla taataan datan suojaus. Microsoft Intune järjestelmän avulla mahdollistetaan laitteidenhallinta kokonaan pilvestä tai sitä voidaan käyttää yhdessä System Center Configuration Managerin kanssa. (Microsoft Docs 2019.)



Kuva 2. Microsoft Intune:n hallinta.

Kuva 2 havainnollistaa, mitkä ovat järjestelmän pääasiallisia toimintoja ja järjestelmänvalvojan työkaluja rekisteröityjen laitteiden määritysten hallitsemiseksi. Järjestelmä sisältää laitteiden konfiguroinnin, suojauksen sekä sovellusten hallinnan. Ehdollisen pääsyn määritykset tulevat järjestelmään Azure Active Directoryn kautta. Laitteiden konfigurointi sisältää profiilit ja konfigurointi käytänteet. Laitteiden suojaus taas sovellusten suojauksen sekä sopivuus käytänteet. Sovellusten hallinta sisältää sallitut sovellukset sekä niiden määritys käytänteet. Kaikkia näitä neljää voi järjestelmänvalvoja hallita Microsoft Intune:n kautta, vaikka ehdollisen pääsyn määritykset sijaitsevat käytännössä Azuren Active Directoryssa.

Microsoft Intune:n hallinta ja sen sisältö on havainnollistettu isommassa vaaleansinisessä pilvessä. Siihen sisältyy laitteiden konfiguroinnit, suojaus sekä sovellusten hallinta. Laitteiden konfigurointiin liittyy erilaiset laiteprofiilit sekä konfigurointi käytänteet. Laitteiden suojaukseen sisältyy sovellusten suojaus ja laitteen sopivuus käytänteet. Sovellusten hallintaan sisältyy sallitut sovellukset ja niiden määritys käytänteet. Azure Active Directory on kuvattu ylempänä sinisessä pilvessä. Järjestelmät kommunikoivat keskenään. Azure Active Directoryn kautta Microsoft Intune saa esimerkiksi ehdollisen pääsyn määritykset. Ehdollista pääsyä voidaan kuitenkin hallita myös Intune:n kautta, josta määritykset synkronoituvat Azure Active Directoryyn. (Microsoft Docs 2019.)

4.1 Laitehallinnan ominaisuudet

Intunea käyttämällä yritys voi hallita organisaation omistuksessa olevia laitteita asettamalla niille erilaisia määrityksiä koskien asetuksia, ominaisuuksia sekä turvallisuutta. Tätä lähestymistapaa käytettäessä laitteet sekä niiden käyttäjät rekisteröidään järjestelmään. Laitteiden rekisteröidyttyä ne saavat säännöt ja asetukset, jotka ovat määriteltynä Intune järjestelmään. Esimerkiksi voit määritellä salasana vaatimuksia laitteeseen, luoda VPN-yhteyden sekä määrittää työkalun uhkien torjuntaa varten. Salasana vaatimus voi olla esimerkiksi PIN-koodin määrittäminen lukitusnäyttöön. (Microsoft Docs 2019.)

Henkilökohtaisille laitteille voidaan määritellä erilaisia käytänteitä tarpeiden mukaan. Käyttäjät eivät välttämättä halua organisaation järjestelmänvalvojien hallitsevan täysin omia laitteitaan. Tähän lähestymistapaan on antaa käyttäjille valintoja, jotka palvelevat käyttäjää ja yrityksen tietoturvaa samalla. Voidaan vaatia, että organisaation kaikkia resursseja varten laite rekisteröidään mutta on myös mahdollista, että käyttäjälle annetaan valinta käyttää esimerkiksi vain työsähköpostia. Applikaatiokohtaiset määritykset antavat tähän ratkaisun. Näissä ratkaisuissa laitteille yleensä määritetään monivaiheinen tunnistautuminen, jolla parannetaan huomattavasti tietoturvaa. (Microsoft Docs 2019.)

Seuraavaan luetteloon on koostettu, miten järjestelmänvalvojat voivat hyötyä Intune:n hallinnasta, kun laite on rekisteröity järjestelmään:

- Laitteista ja käyttäjistä pystytään näkemään raportteja, jotka sisältävät tietoa niistä ja niiden tilasta.
- Laitteista saadaan reaaliaikainen varastonäkymä, josta nähdään mitkä laitteet ovat yhteydessä organisaation resursseihin.
- Laitteet voidaan määritellä vastaamaan organisaation turvallisuusstandardeja.
- Voidaan jakaa laitteille sertifikaatteja, jotta niillä pystytään helposti yhdistämään organisaation verkkoon.
- Laitteen tiedot pystytään tyhjentämään etänä, jos laite katoaa, varastetaan tai sitä ei enää käytetä. (Microsoft Docs 2019.)

4.2 Applikaatiohallinnan ominaisuudet mobiililaitteissa

Applikaatiohallinnan osalta Intune on kehitetty suojaamaan organisaation dataa applikaatio tasolla, joihin sisältyy mukautetut sovellukset ja Microsoft kaupan sovellukset. Applikaatiohallintaa voidaan soveltaa organisaation omistamiin sekä henkilökohtaisiin laitteisiin. (Microsoft Docs 2019.)

Kun applikaatioita hallinnoidaan Intune:n kautta, järjestelmänvalvojat voivat:

- Lisätä ja määrittää sovelluksia käyttäjäryhmille ja laitteille, sisällyttäen vain tietyt käyttäjä- ja laiteryhmät.
- Määrittää applikaatiot käynnistymään etukäteen määritetyt asetukset aktivoituna ja päivittää jo olemassa olevia sovelluksia laitteissa.
- Nähdä raportteja käytetyistä sovelluksista ja niiden käyttöasteesta.
- Tehdä valikoivan tyhjennyksen poistaen vain organisaation datan sovelluksista. (Microsoft Docs 2019.)

Yksi tapa, millä Intune tarjoaa turvallisuutta mobiiliapplikaatioihin, on applikaatioiden suojauskäytänteillä. Applikaatioiden suojauskäytänteet käyttävät Azure Active Directorya eristämään organisaation datan henkilökohtaisesta datasta. Dataan, johon päästään käsiksi organisaation tunnuksilla, saadaan lisäsuojausta tällä tavoin. Suojauskäytänteillä voidaan rajata käyttäjän toimia esimerkiksi tietojen kopioinnissa, liittämisessä, tallennuksessa ja katselumahdollisuuksia pystytään myös rajaamaan. (Microsoft Docs 2019.)

4.3 Yleisimpiä tapoja hyödyntää järjestelmän ominaisuuksia

Ennen käyttöönottoa, organisaation tulisi arvioida mitä hyötyjä järjestelmältä pyritään saamaan. On tärkeää ottaa huomioon eri sidosryhmien tarpeet ennen uuden järjestelmän tuomista omaan ympäristöönsä, korvaamalla esimerkiksi jo olemassa olevan järjestelmän. Organisaation tulisi ottaa myös huomioon dynaamisesti muuttuvan yritysympäristön. Tässä kappaleessa käsitellään yleisempiä käyttötapoja järjestelmälle.

4.3.1 Sähköpostin ja datan suojaaminen mobiililaitteissa

Useimmat yritysten liikkuvuuspakettistrategiat alkavat suunnittelemalla suojattua pääsyä sähköposteihin työntekijöille mobiililaitteiden avulla, jotka ovat yhteydessä verkkoon. Monilla yrityksillä on käytössä omissa tiloissaan tieto- ja sovelluspalvelimia, joita ylläpidetään yrityksen omassa verkossa. Intunea ja Microsoft Enterprise Mobility ja Security palvelua hyödyntäen voidaan luoda ympäristö, jossa ehdot määrittävät, ettei yksikään mobiiliapplikaatio pääse yhdistymään sähköpostiin ennen kuin laite on rekisteröitynyt järjestelmään. Määrityksien ja asetusten kautta rekisteröidyillä laitteilla voidaan hallita sitä, miten se käyttää yrityksen dataa ja oikeuksia voidaan eritellä ryhmien avulla. Voidaan esimerkiksi määrittää, että tietyllä ryhmällä ei ole oikeutta kopioida työsähköpostin tietoja laitteen muihin kuin hallittuihin sovelluksiin. (Microsoft Docs 2019.)

4.3.2 Vaihtoehto henkilökohtaisten ja yrityksen omistamien laitteiden välillä

On yhä tavallisempaa, että työntekijät käyttävät omia mobiililaitteitaan yrityksen tarjoaman sijasta. Se tarjoaa myös yrityksille pienemmät kustannukset sekä tuo mobiililaitteilla työskentelyä varten erilaisia mahdollisuuksia työntekijöille. Ongelmana on ollut, että työntekijät harvoin suostuvat antamaan omaa laitettaan rekisteröitäväksi järjestelmään ja näin ollen yrityksen hallintaan. Tähän Intune antaa vaihtoehdon, jossa henkilökohtaista laitetta ei rekisteröidä järjestelmään, mutta sillä voidaan kuitenkin hallita sovelluksia, jotka sisältävät yrityksen dataa. (Microsoft Docs 2019.)

Yrityksen omistamille mobiililaitteille Intune tarjoaa omat mahdollisuutensa. Niille voidaan määritellä omat turvallisuusasetukset. Intune mahdollistaa myös sen, että esimerkiksi uudella iPhone:lla työntekijä käy läpi yrityksen oman asennusprosessin, jonka jälkeen hän voi Intune portaali sovelluksen avulla päästä käsiksi valikoituihin sovelluksiin. (Microsoft Docs 2019.)

4.4 Vaatimukset

Tässä osiossa käydään läpi Microsoft Intune:n käyttöönottoon liittyvät vaatimukset, jotka sisältävät tarvittavat Microsoft tilaukset, käyttöjärjestelmät ja tuetut selaimet järjestelmää varten. Intune tukee vain laitteita, joissa on jokin seuraavista käyttöjärjestelmistä.

Microsoft:

- Surface Hub
- Windows 10 Home, S, Pro, Education ja Enterprise versiot
- Windows 10 Enterprise 2019 LTSC
- Windows 10 Mobile
- Windows 10 IoT Enterprise x86, x64
- Windows 10 IoT Mobile Enterprise
- Windows Holographic for Business
- Windows 10 Teams Surface Hub
- Windows Phone 8.1, Windows 8.1 RT, PC:t joissa Windows 8.1 ylläpito tila. (Microsoft Docs 2019.)

Google:

- Android 5.0 ja myöhemmät, sisältää Samsung KNOX Standard 2.4 ja ylöspäin.
- Android enterprise. (Microsoft Docs 2019.)

Apple:

- Apple iOS ja iPadOS 11.0 ja myöhemmät.
- Mac OS X 10.12 ja myöhemmät. (Microsoft Docs 2019.)

Tuetut selaimet:

- Microsoft Edge viimeisin versio

- Microsoft Internet Explorer 11
- Safari viimeisin versio, vain Mac
- Chrome viimeisin versio
- Firefox viimeisin versio. (Microsoft Docs 2019.)

Järjestelmänvalvojan työkalut, joita käytetään selaimen kautta vaativat joko Azure portalin käyttöä tai Microsoft 365 admin centerin käyttöä. Nämä ovat siis portaaleja, joihin yhdistetään verkkoselaimella. Intunea varten on oma portaali, josta hallitaan ainoastaan rekisteröityjä laitteita. Klassinen Intune portaali vaatii selaimelta Silverlight tukea. Näitä selaimia ovat, jotka tukevat Intune konsolia:

- Internet Explorer 10 tai myöhemmät.
- Google Chrome (varhaisemmat versiot versiosta 42).
- Mozilla Firefox Silverlight sallittuna (varhaisemmat versiot versiosta 56). (Microsoft Docs 2019.)

Järjestelmän ominaisuuksien käyttöä varten, joita työssä hyödynnetään, tarvitaan seuraavat aktiiviset tilaukset:

- Microsoft Office 365
- Azure Active Directory
- Microsoft Intune
- Enterprise Mobility + Security. (Microsoft Docs 2019.)

Jokainen näistä tilauksista sisältää ilmaisen kokeilujakson, jota hyödynnetään tässä työssä. Normaalisti näistä lisensseistä ja tilauksista veloitetaan kiinteä kuukausimaksu.

4.5 Määritykset järjestelmään

Tässä osuudessa käydään läpi, mitä määrityksiä järjestelmään tehdään ennen laitteen rekisteröintiä järjestelmään. Osio sisältää käyttäjien ja ryhmien luonnin, laitteen rekisteröintiä edeltävät määritykset, ehdollisen pääsyn, sovellusten määritykset ja itse laitteelle asetetut säännöt. Tämän lisäksi käydään läpi Microsoft Intune:n tarjoamaa mahdollisuutta liittää mobiililaitteiden uhkien torjuntatyökalu osaksi järjestelmää. Järjestelmään tehtyjen määritysten on tarkoitus lisätä tietoturvaa, kun työntekijät käyttävät yrityksen resursseja työskennellessään mobiililaitteilla. Määritysten tekemisessä käytetään apuna 3. kappaleessa esitettyjä keinoja uhkien ehkäisemiseen.

Intune:n hallinnasta löytyvät eri kohdat ovat kursivoituna tekstissä ja kuvissa olennaiset kohdat ovat merkittynä punaisella. Jokaisessa kuvassa näkyy vasemmalla ylhäällä polku, jota kautta hallinnan vasemman laidan valikosta on navigoitu kuvassa olevaan näkymään ja tämä polku on kursivoituna tekstissä.

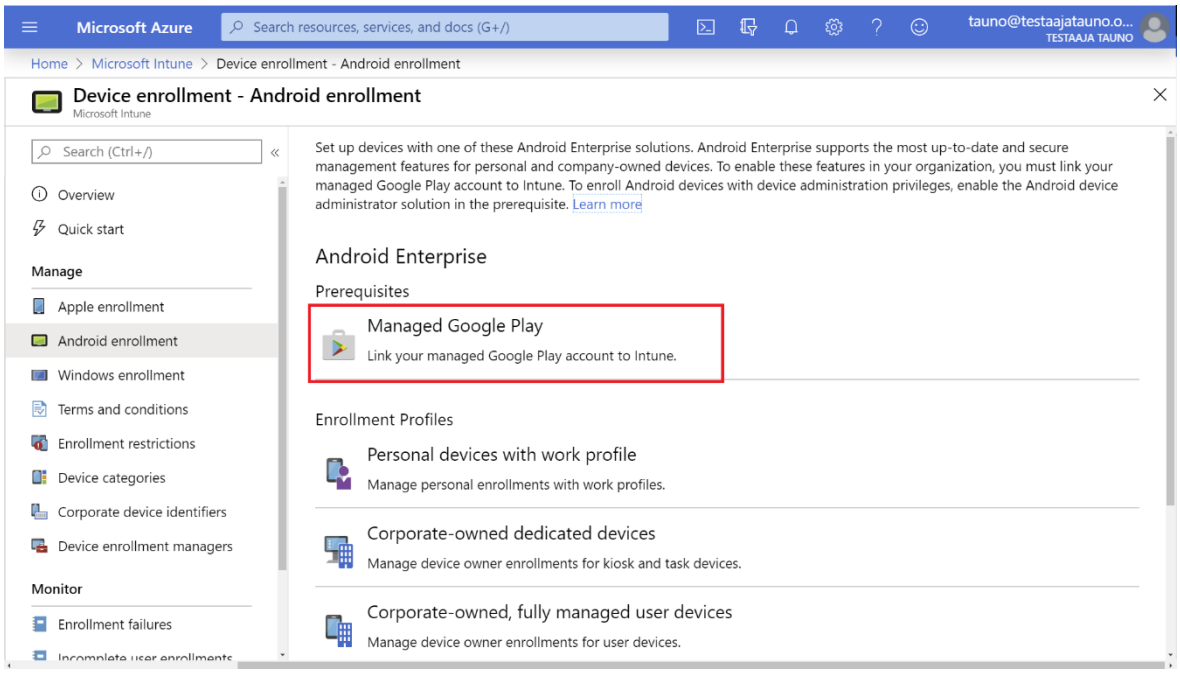
4.5.1 Käyttäjät ja ryhmät

Testaamista varten on luotu yksi järjestelmänvalvojan tili sekä yksi normaali tili, jota on tarkoitus käyttää käyttötapausten testaamisessa. Järjestelmänvalvojan tiliin on liitetty Azure Active Directory Premium P2, Enterprise Mobility + Security E5, Intune, Office 365 E5 -lisenssit määrityksiä varten. Sen lisäksi Azure Active Directoryyn on luotu testiryhmä, johon on liitetty normaali käyttäjätili. Ryhmä on tarkoitus liittää jokaiseen määritykseen, jotka konfiguroidaan Intune:n hallinnassa. Näin ryhmään määritellyt jäsenet saavat Intune:n kautta tulevat turvallisuusmääritykset laitteeseensa.

4.5.2 Laitteen rekisteröinti

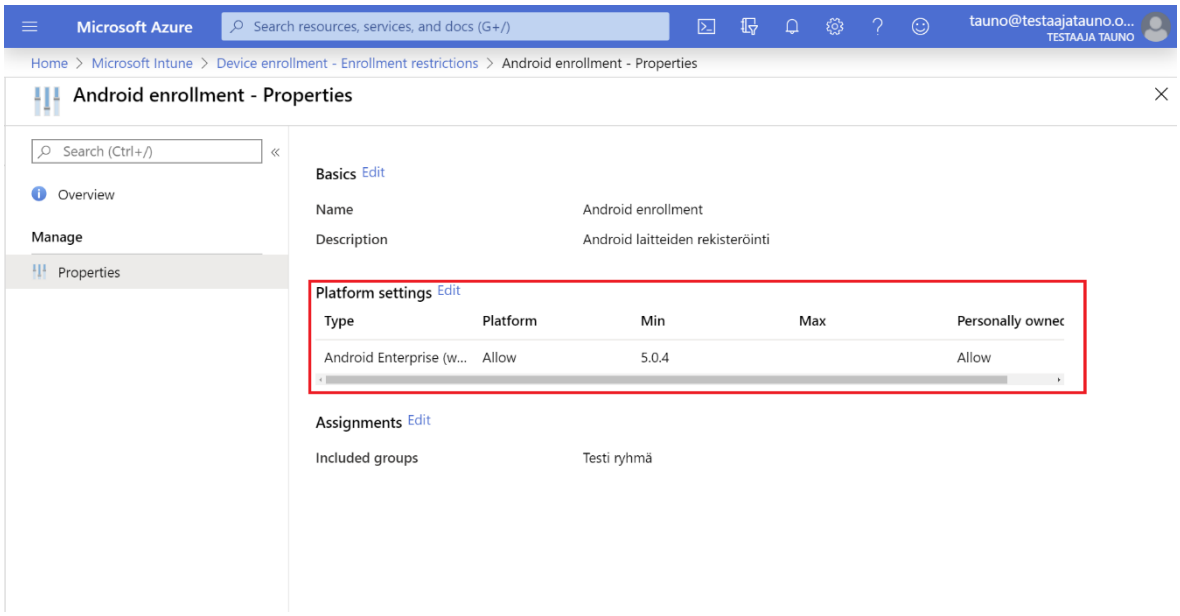
Tämä osuus käsittelee laitteen rekisteröintiä edeltävät toimenpiteet. Käyttäjän laite rekisteröidään järjestelmään käyttötapausten testauksen aikana.

Kuvassa 3 on Intune:n hallinnan laitteiden rekisteröinnin hallinta. Testattava laite on Android-pohjainen, joten Intune:n hallintaportaalista vasemmasta palkista *Manage* osion alta valitaan *Device enrollment -> Android enrollment. Android enrollment* kohdasta voidaan linkittää yrityksen Google Play -tili Intuneen, jotta Android-laitteita voidaan rekisteröidä järjestelmään ja sovelluksia voidaan hallita.



Kuva 3. Intune:n hallinta

Kuvassa 4 *Manage* osion alta valitaan *Device enrollment -> Enrollment restrictions -> Android enrollment -> Properties*. Tästä kohdasta nähdään Android-laitteille tehdyt järjestelmämääritykset rekisteröitäville laitteille. Testiympäristöä varten määritettiin Android-laitteille järjestelmän vähimmäisvaatimukseksi ohjelmistoversio 5.0.4.

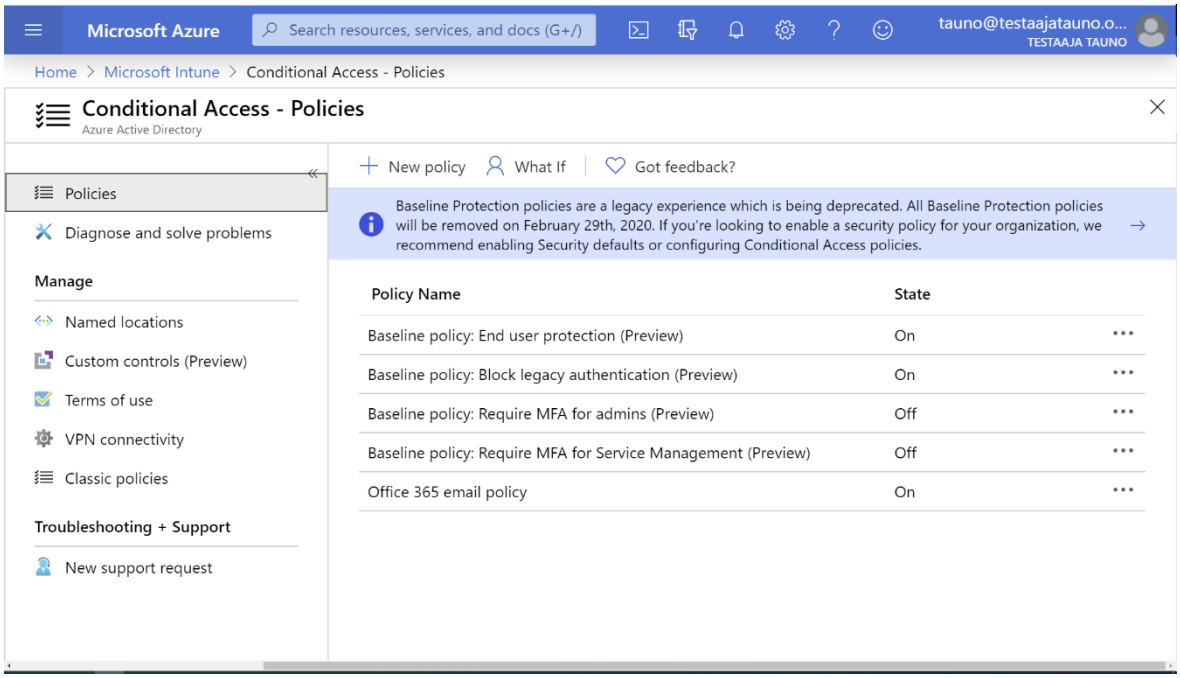


Kuva 4. Intune:n hallinta

4.5.3 Ehdollinen pääsy

Ehdolliseen pääsyyn tehdään määrityksiä koskien käsiksi pääsyä yrityksen resursseihin. Määrityksiä ja ehtoja, jonka perusteella käyttäjä pääsee käsiksi yrityksen resursseihin, voidaan määritellä sijainnin, laitteen, käyttäjän tilan ja sovelluksien mukaan.

Kuvassa 5 on ehdollisen pääsyn määritysosio Intune:n hallinnassa. Sääntöjä Intune:n portaalin kautta kohdasta *Conditional Access -> Policies -> New policy*. Microsoft Intune tarjoaa valmiiksi viisi *Baseline policy* -vaihtoehtoa, jotka voi määrittää aktiiviseksi tarpeen mukaan. Kuvassa näkyy kaikki säännöt ja ovatko ne aktiivisia. Aktiivisuus nähdään kohdan *State* alta, jossa on vaihtoehtona joko *On* tai *Off. On* tarkoittaa aktiivista ja *Off*, että sääntö ei ole aktiivinen. Tätä kautta voidaan muokata ja lisätä uusia sääntöjä.

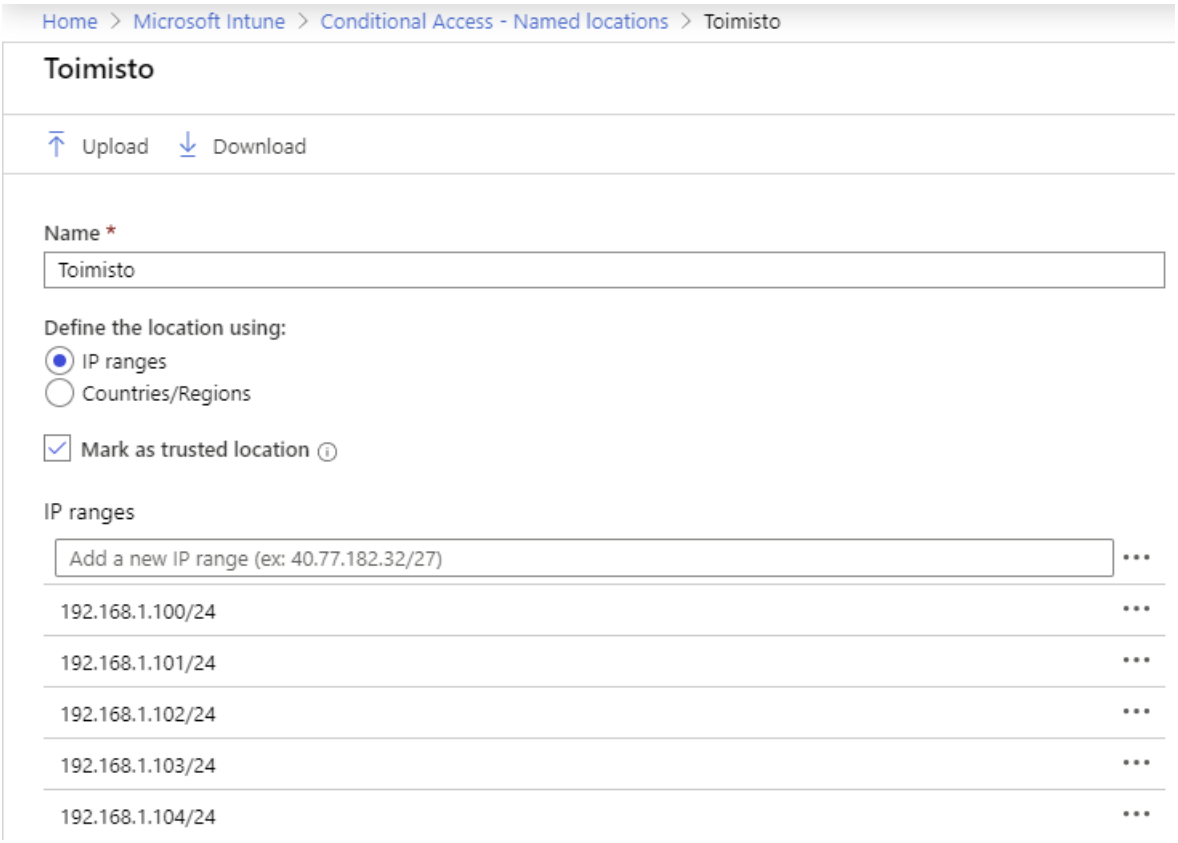


Kuva 5. Intune:n hallinta

Tämän testiympäristön käyttöä varten on määritetty testiryhmän käyttäjille pakotettu monivaiheinen tunnistautuminen, joka tapahtuu Microsoft Authenticator -sovelluksen avulla. Sen lisäksi on otettu käyttöön käytänne, joka estää kaikki kirjautumiset sovelluksiin, jotka eivät tue monivaiheista tunnistautumista.

Office sovellusten osalta määritin käytänteen, joka estää niihin kirjautumisen ei tunnetuista langattomista verkoista sekä kirjautuminen on mahdollista vain sille osoitetun sovelluksen kautta, esimerkiksi sähköpostiin voidaan kirjautua vain käyttämällä Outlookin mobiilisovellusta. Tunnetut eli sallitut verkot ovat lisätty osaksi käytännettä ja näiden kautta päästään käsiksi yrityksen resursseihin normaalisti.

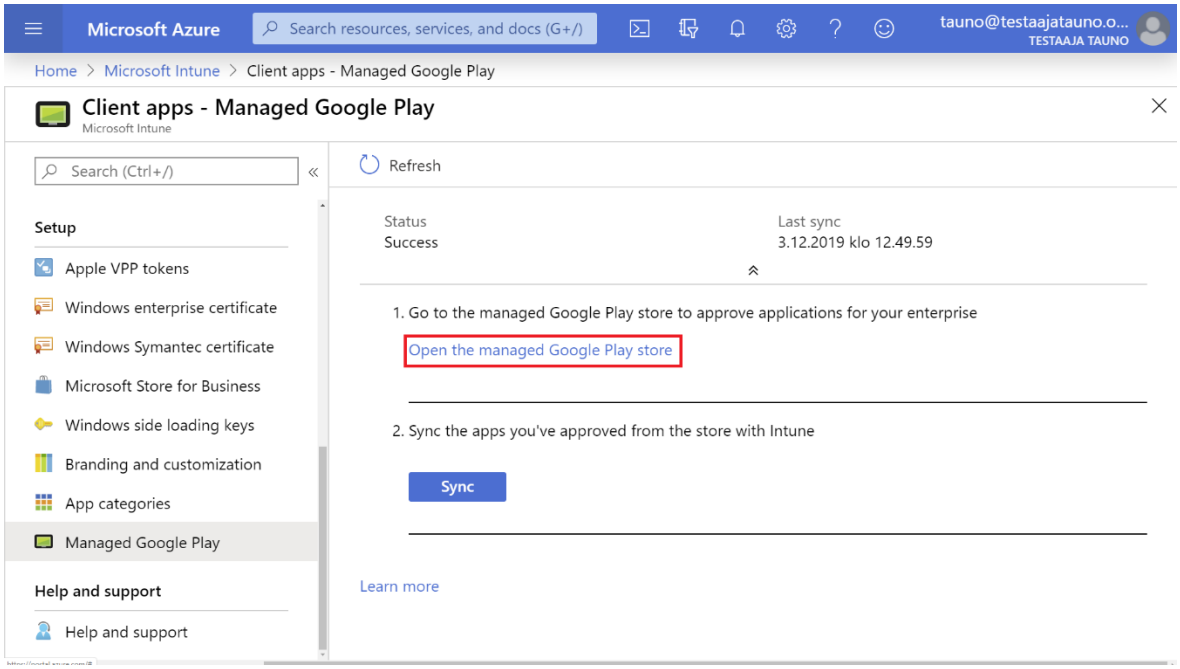
Kuvassa 6 nähdään luotu sääntö, mistä verkko-osoitteista sallitaan liikenne yrityksen resursseihin sallituilla sovelluksilla. Sallitut verkko-osoitteet ovat listattuna kohdan *IP ranges* alla. Tätä ominaisuutta hyödyntämällä voidaan estää kirjautuminen yrityksen resursseihin esimerkiksi tuntemattomista julkisista verkoista. Julkiset verkot ovat mainittuna yhtenä tietoturvauhkana kappaleessa 3.2.



Kuva 6. Intune:n hallinta

4.5.4 Sovelluksien määritykset

Kuvassa 7 on sovellusten hallintaosio Intune:n hallinnassa. Sovelluksien määrityksiä hallitaan Intune:n hallintaportaalin kautta kohdasta *Client Apps.* Android-laitteille sovelluksia voidaan lisätä kohdasta *Client Apps -> Managed Google Play*. Valitaan ”Open the managed Google Play store”, joka on merkittynä punaisella värillä kuvassa. Tämä ohjaa sinut lisäämäsi Google-tilin omaan Google Play kaupan hallintaan, josta voit lisätä sovelluksia, joita haluat hyväksyä yrityksesi Android mobiililaitteiden käyttöön.

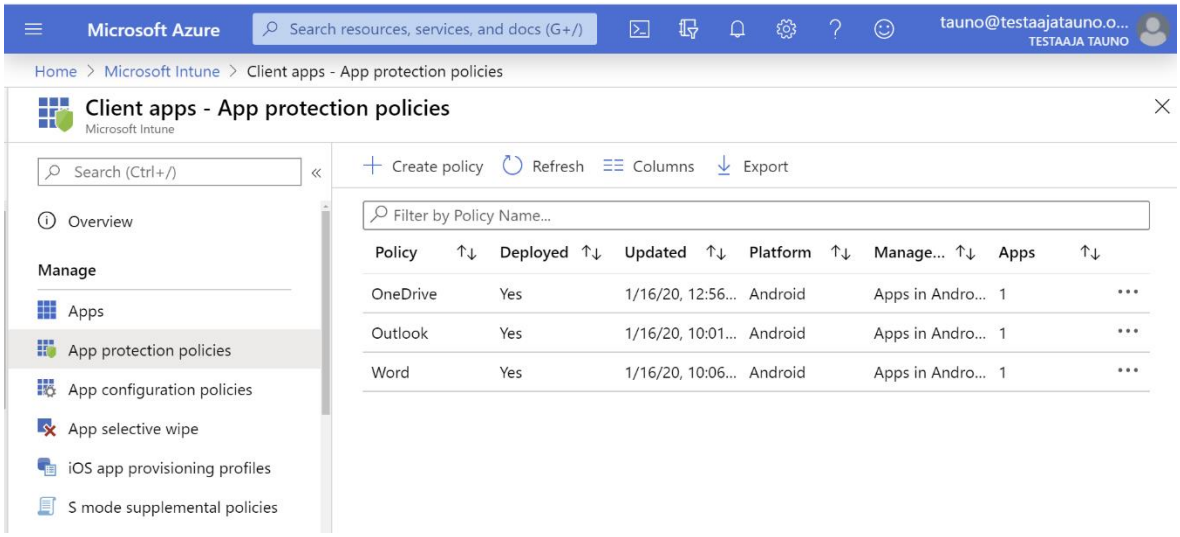


Kuva 7. Intune:n hallinta

Testiympäristöä varten hyväksytyt sovellukset, jotka otetaan käyttöön ovat: Microsoft Outlook, Microsoft Word, Microsoft OneDrive, Microsoft Authenticator sekä Intune-yritysportaali. Sovellukset lisättiin käyttöä varten kohdasta *Client apps – Apps* ja valittiin sovellus, jolle halutaan määrittää sen saatavuus esimerkiksi Outlook. Sovellus määriteltiin saatavaksi kaikille käyttäjille, joilla on rekisteröity mobiililaite.

Microsoft Authenticator määritettiin pakolliseksi sovellukseksi, jolloin se tulee yritysportaaliin kirjautumisen yhteydessä automaattisena asennuksena mobiililaitteeseen. Monivaiheisen tunnistautumisen käyttö on määritelty pakolliseksi Office 365 Exchange Online ja SharePoint sovelluksiin. Näihin sovelluksiin sisältyy esimerkiksi Microsoft OneDrive. Microsoft Authenticator on monivaiheiseen tunnistautumiseen käytettävä sovellus.

Kuvassa 8 on Intune:n hallinnan sovellusten suojaus määritysten osio. Jokaiseen sovellukseen voidaan lisätä erilaisia suojausmäärityksiä kohdasta *Client apps -> App protection policies -> Create policy* kohdasta, joka löytyy keskiosiosta vasemmalta. Testiympäristöä varten Outlook, OneDrive ja Word sovelluksille määritellään samat suojausmääritykset. Ne sisältävät datan suojaamiseen liittyvät ominaisuudet, pääsyvaatimukset sekä ehdollisen käynnistyksen. Tärkeimpinä ominaisuuksina datan suojaamiseen liittyvät ominaisuudet, jotka sisältävät tiedostojen ja niiden sisällön tallentamisen rajoittamista. Nämä rajoitukset tulevat esille tarkemmin käyttötapauksien testauksessa.



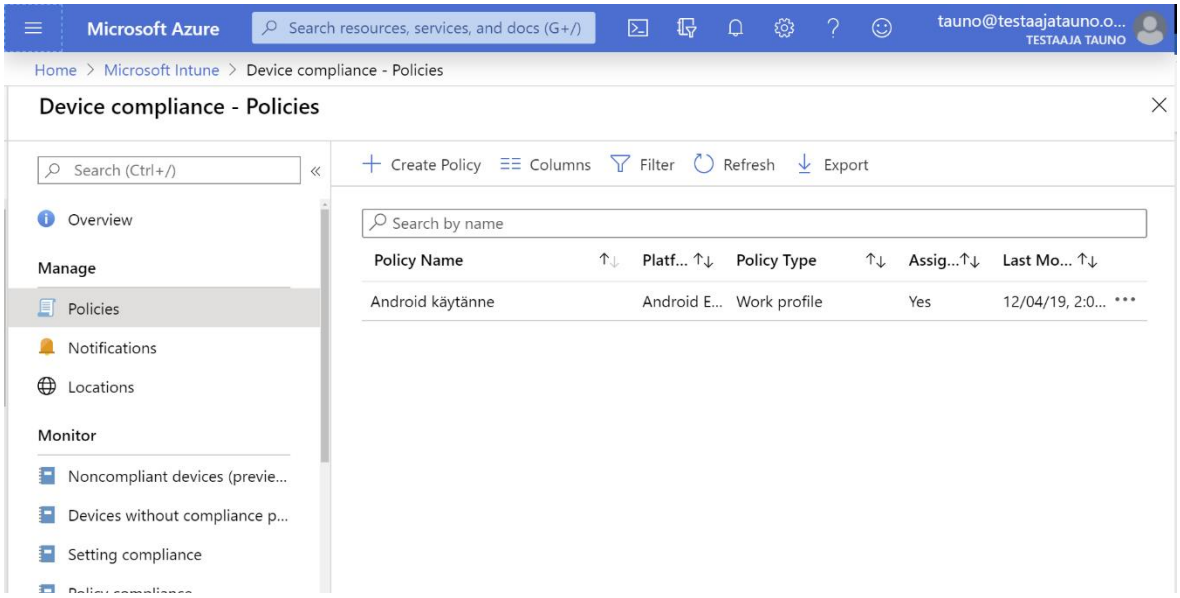
Kuva 8. Intune:n hallinta

4.5.5 Laitemääritykset

Rekisteröitäville laitteille voidaan luoda sääntöjä, joiden täytyttyä laitteet vastaavat annettuja vaatimuksia ja pääsevät käsiksi yrityksen resursseihin. Jos laite ei vastaa vaatimuksia pääsy estetään esimerkiksi sähköpostiin tai muihin yrityksen hallitsemiin sovelluksiin, jotka sisältävät yrityksen dataa.

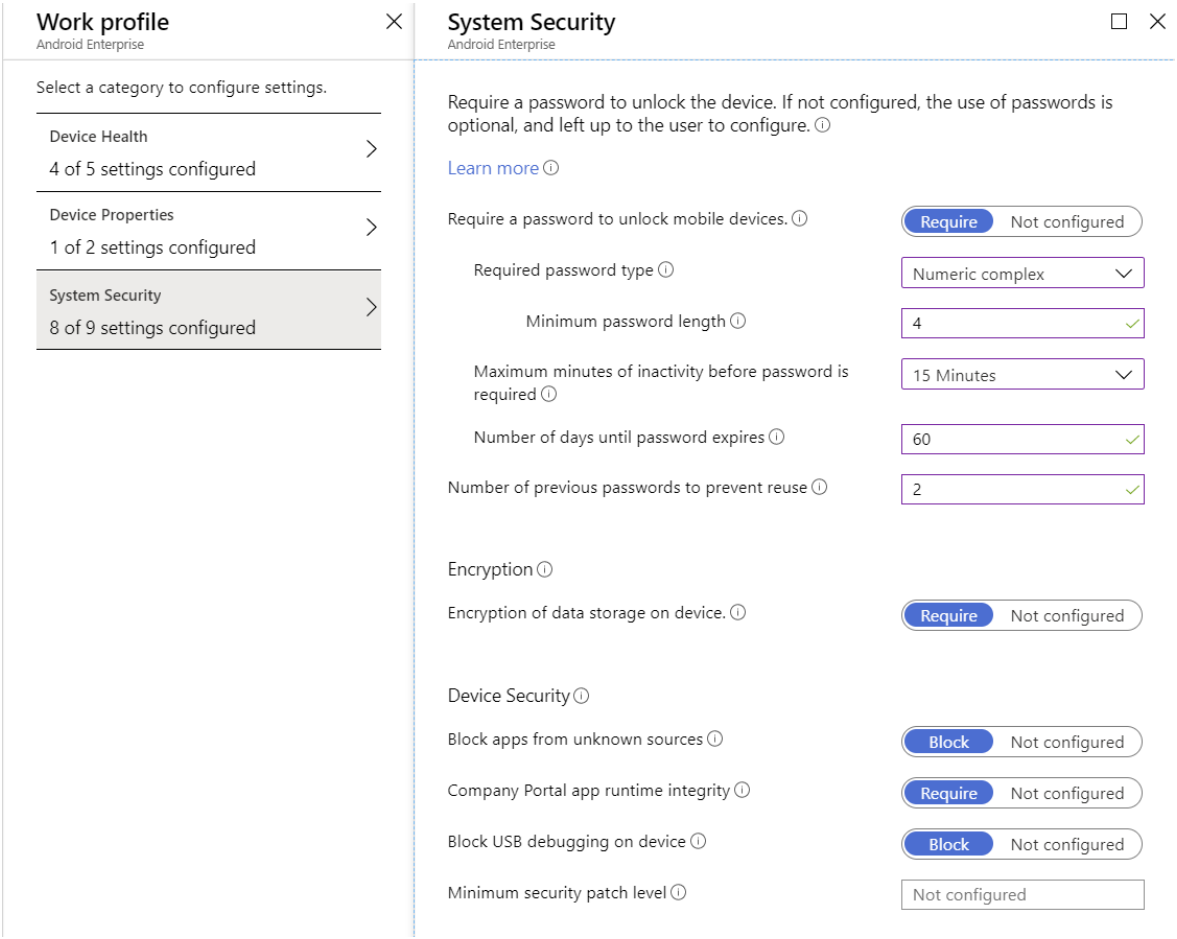
Testiympäristöön tehtiin Android-laitteille määritykset, jossa seuraavat asiat ovat vaadittuna laitteelta ennen sopivuutta: järjestelmäversio minimi Android 7.0, laitteelle on määritelty pääsykoodi sekä tietojen salaus. Järjestelmäversion minimivaatimus Android 7.0 estää rekisteröinnin ja näin ollen yrityksen resursseihin pääsyn, jos laitteen järjestelmäversio on esimerkiksi Android 6.0 tai alhaisempi. Jos vaatimukset eivät täyty, järjestelmä on määritelty lähettämään tieto sähköpostina käyttäjälle. Laite näkyy myös hallinnassa ja käyttäjän Intune-yritysportaali sovelluksessa epäsopivana järjestelmään. Tämä pitää huolen siitä, että rekisteröitävän laitteen ohjelmisto on ajan tasalla. Tämä asia on mainittuna tietoturvauhkana kappaleessa 3.5.

Kuvassa 9 on järjestelmän sopivuus käytänteet, jotka määritellään kohdasta *Device compliance -> Policies -> Create Policy.* Seuraavissa kuvissa nähdään, mitä määrityksiä käytänteelle ”Android käytänne” on luotu.



Kuva 9. Intune:n hallinta

Kuvassa 10 näkyy laitteelle tehdyt järjestelmän turvallisuusmääritykset. *System Security* kohdan alta voidaan nähdä, että laitteelle on määritelty pääsykoodi. Laitteen avaamiseen vaaditaan monimutkainen nelinumeroinen koodi. Monimutkainen tarkoittaa, että pääsykoodi ei voi olla numerojono (1234) tai neljä samaa numeroa. Suositeltavaa on myös, että ei käytä omaa syntymäpäiväänsä pääsykoodina, koska se on yleensä helposti saatavilla olevaa tietoa käyttäjästä. *Encryption* kohdan alla näkyy, että laitteelta vaaditaan suojaus. *Device Security* kohdasta on määritelty, että laitteelta estetään sovellusten asentaminen tuntemattomista lähteistä. Laitteen määrityksiin on hyödynnetty kappaleissa 3.3, 3.5 ja 3.6 esitettyjä keinoja sekä uhkia.



Kuva 10. Intune:n hallinta

4.5.6 Mobiililaitteiden uhkien torjuntatyökalut

Microsoft Intune järjestelmään on mahdollista integroida kolmannen osapuolen tarjoama mobiililaitteiden uhkien torjuntatyökalu, jonka avulla voidaan saada informaatiota laitteen yhteensopivuus käytänteistä sekä laitteen ehdollisen pääsyn säännöistä. Tätä tietoa voidaan käyttää suojaamaan yrityksen resursseja esimerkiksi Exchange palvelussa ja Sharepointissa, kun sopimattoman laitteen pääsy voidaan estää. (Microsoft Docs 2019.)

Intune luo yhteyden järjestelmän ja valitun mobiililaitteiden uhkien torjuntatyökalun palveluntarjoajan kanssa. Uhkien torjuntatyökalut skannaavat ja analysoivat mobiililaitteiden uhkia ja jakavat niitä järjestelmään. Intune taas voi käyttää näitä tietoja raporttien tekemiseen tai erilaisten suojaustoimien suorittamiseen. Esimerkkinä yhdistetty mobiililaitteiden uhkien torjuntatyökalu raportoi palveluntarjoajalle mobiililaitteen olevan yhdistynyt verkkoon, joka on haavoittuva hyökkäyksille. Tämä informaatio kategorisoidaan riskitasolle joko matalaksi, keskitasoksi tai korkeaksi uhaksi. Riskitasoa vertaillaan määrityksiin, jotka järjestelmänvalvoja on määrittänyt Intune:n hallintaan. Tähän vertailuun perustuen pääsy joihinkin yrityksen resursseihin voidaan estää tältä mobiililaitteelta. Resurssit, joita rajoitetaan, ovat järjestelmänvalvojan määrittämiä järjestelmään. (Microsoft Docs 2019.)

Kun mobiililaitteen torjuntatyökalu on asennettu laitteeseen Intune voi kerätä dataa laitteen sovelluksista ja jakaa sitä torjuntatyökalun palveluntarjoajalle. Dataa voidaan kerätä henkilökohtaisista ja yrityksen omistuksessa olevista laitteista, jotka ovat rekisteröitynä järjestelmään. Intune voi kerätä seuraavia tietoja sovelluksista: tunnuksen, version, lyhennetyn version, nimen, paketoidun koon, varsinaisen tiedostokoon sekä onko sovellus vahvistettu vai ei. (Microsoft Docs 2019.)

Lista palveluntarjoajista, joiden mobiililaitteiden uhkien torjuntatyökalut voidaan liittää Intuneen:

- Better Mobile
- Check Point
- Lookout
- Pradeo
- Sophos Mobile
- Symantec
- Wandera
- Zimperium. (Microsoft Docs 2019.)

Mobiililaitteen uhkien torjuntatyökalun lisääminen on jätetty pois testaamisesta, koska palvelu vaatii kolmannen osapuolen sovelluksen integroimista lisäksi järjestelmää. Uhkien

torjuntatyökalut mobiililaitteilla ovat olennainen osa tietoturvaa yrityksen resurssien suojaamisessa mobiililaitteilla. Tästä enemmän kappaleessa 3.6.

5 Käyttötapaukset

Tässä kappaleessa luodaan käyttötapauksia testausta varten. Käyttötapaukset luodaan 3. kappaleen perusteella, jossa esiteltiin yleisempiä tietoturva uhkia mobiililaitteilla. Käyttötapauksissa käydään läpi itse käyttötapaus, yleiskatsaus, toimijat, esiehdot ja toimintaskenaario. Sen lisäksi luodaan kaavio, joka havainnollistaa käyttötapausta visuaalisesti.

Käyttötapauksen kaavio on yksinkertainen, eikä se näytä käyttötapauksen yksityiskohtia. Se on yhteenveto yhteyksistä käyttötapausten, toimijoiden ja järjestelmien välillä. Käyttötapauskaavio ei sisällä järjestystä milloin mikäkin vaihe toteutuu, jotta haluttuun lopputulokseen päästään. Käyttötapauskaaviossa on eri merkintätapoja, joiden tarkoitus on havainnollistaa esimerkiksi järjestelmän toimivuutta. Merkintätavat sisältävät toimijan, käyttötapauksen, linkityksen sekä käsiteltävän järjestelmän. (Visual Paradigm 2019.)

Toimijalla tarkoitetaan tekijää, joka käyttää järjestelmää. Toimija käynnistää käyttötapauksen. Toimija sijoitetaan järjestelmän ulkopuolelle tekijäksi. Käyttötapaus on järjestelmän sisällä oleva järjestelmän toiminto, johon toimijat linkitetään. Linkitys asetetaan toimijan ja käyttötapauksen välille. Järjestelmä on käyttötapauksessa yleensä kuin iso laatikko, jonka sisälle rakennetaan käyttötapauksia. Järjestelmän ulkopuolelle lisätään toimijat ja linkitykset tehdään käyttötapauksiin, jotka ovat soikeita kuvioita kaaviossa. (Visual Paradigm 2019.)

Linkityksissä tavallinen viiva tarkoittaa suoraa kytköstä toimijasta käyttötapaukseen. Katkoviivalla merkityt linkitykset voivat sisältää kahta eri merkitystä: jatkuu tai sisältyy. Jatkuminen tarkoittaa, että käyttötapaukseen palataan. Sisältyy tarkoittaa, että käyttötapaukset liittyvät toisiinsa. Nuolella ja viivalla yhdistetyt käyttötapaukset tarkoittavat, että nuolella osoitettu käyttötapaus on toisen käyttötapauksen vanhempi. Nämä käyttötapaukset erotellaan nimeämällä ne lapsi- ja vanhempiobjekteiksi. Linkityksiä on hyödynnetty kuvissa 10 ja 11. (Visual Paradigm 2019.)

5.1 Mobiililaitteen rekisteröinti työkäyttöön

Käyttötapaus: Mobiililaitteen rekisteröinti työkäyttöön.

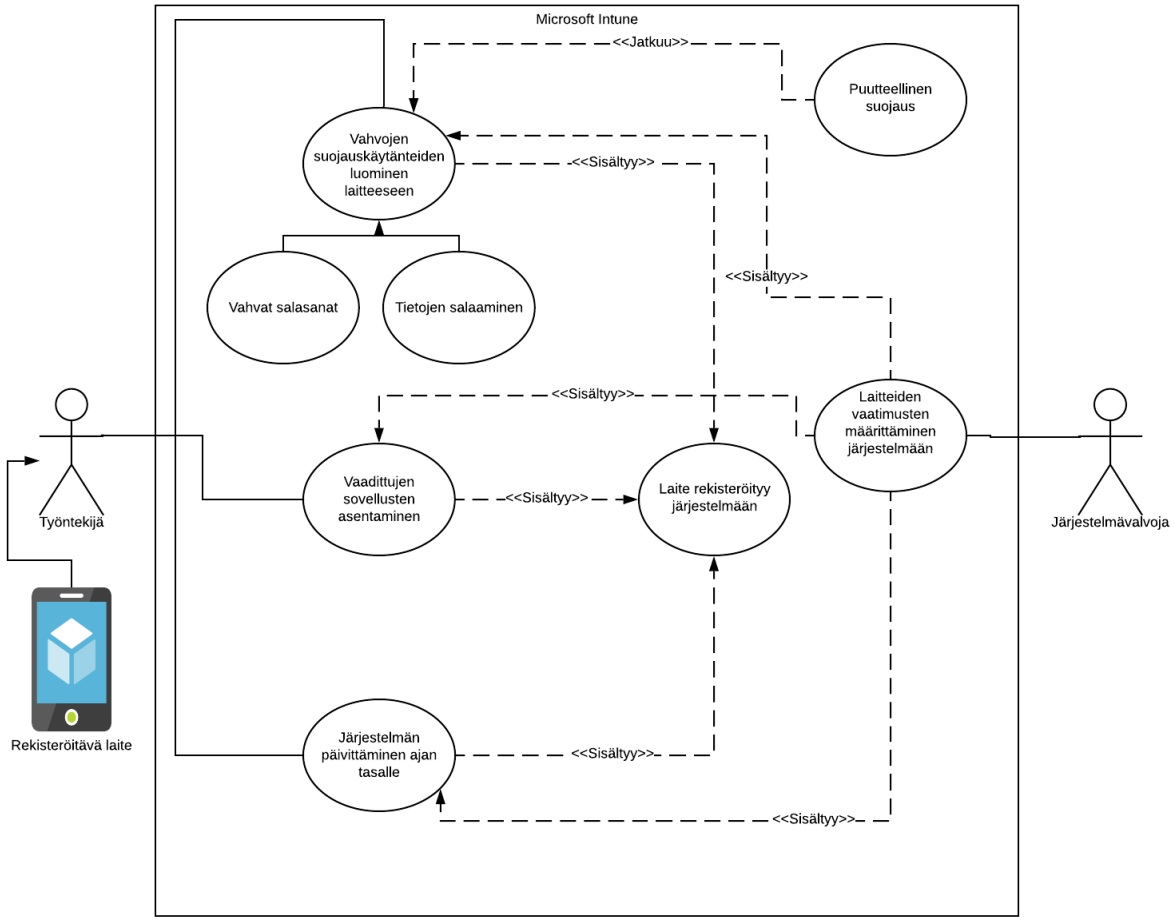
Yleiskatsaus: Työntekijä asentaa omaan henkilökohtaiseen puhelimeensa rekisteröintiä ja työskentelyä varten tarvittavat sovellukset. Tämä sisältää Intune-yritysportaalin asentamisen laitteen rekisteröimistä varten ja työhön tarvittavien sovellusten asentamisen laitteeseen. Asennettavat työsovellukset eritellään ennen testausta. Järjestelmä luo laitteeseen työprofiilin, jonka avulla erotellaan esimerkiksi töihin liittyvät sovellukset käyttäjän henkilökohtaisista sovelluksista.

Toimijat: Työntekijä.

Esiehdot: Käyttäjä on lisännyt mobiililaitteeseen Google-tilin sovellusten asentamista varten.

Toiminta skenaario:

1. Käyttötapaus alkaa, kun käyttäjä rekisteröi oman laitteensa järjestelmään asentamalla Google Play kaupasta Intune-yritysportaalin ja käynnistämällä sen. Sovelluksen käynnistyttyä käyttäjä lisää työtilinsä siihen.
2. Käyttäjä etenee ohjeiden mukaisesti ja tekee tarvittavat muutokset puhelimeen, joita portaali käskee tekemään tarvittaessa. Määritysten jälkeen laite merkitään järjestelmään sopivaksi.
3. Käyttäjä asentaa työskentelyyn tarvittavat sovellukset ja ottaa käyttöön Microsoft Authenticator sovelluksen.



Kuva 11. Mobiililaitteen rekisteröinti työkäyttöön.

Kuva 11 on käyttötapauskaavio, joka on luotu mobiililaitteen rekisteröinnille työkäyttöön, kun hallintajärjestelmänä käytetään Microsoft Intune:a. Vasemmalla nähdään pääasiallinen toimija, joka suorittaa eri käyttötapauksia laitteen rekisteröinnin suorittamiseksi järjestelmään. Toimijan alla on lapsiobjekti, joka tässä tapauksessa on rekisteröitävä laite. Oikealla puolella toimijana on järjestelmänvalvoja, joka määrittää vaatimukset laitteen rekisteröintiä varten. Vaatimuksien määritykset määrittävät työntekijän käyttötapaukset, jotka ovat järjestelmän päivittäminen ajan tasalle, vahvojen suojauskäytänteiden luominen laitteeseen sekä vaadittujen sovellusten asentaminen. Työntekijän käyttötapaus vahvojen suojauskäytänteiden luominen sisältää kaksi lapsiobjektia. Vahvojen suojauskäytänteiden luominen laitteeseen sisältää vahvat salasanat ja tietojen salaamisen. Kun kaikki käyttötapaukset ovat suoritettu onnistuneesti, laite rekisteröityy järjestelmään. Vahvan suojauskäytänteiden luomisen käyttötapauksessa on havainnollistettu puutteellinen suojaus, joka tarkoittaa, että käyttötapaus jatkuu niin kauan kuin se on suoritettu vaatimusten mukaisesti.

5.2 Mobiililaitteella työskentely

Käyttötapaus: Mobiililaitteella työskentely.

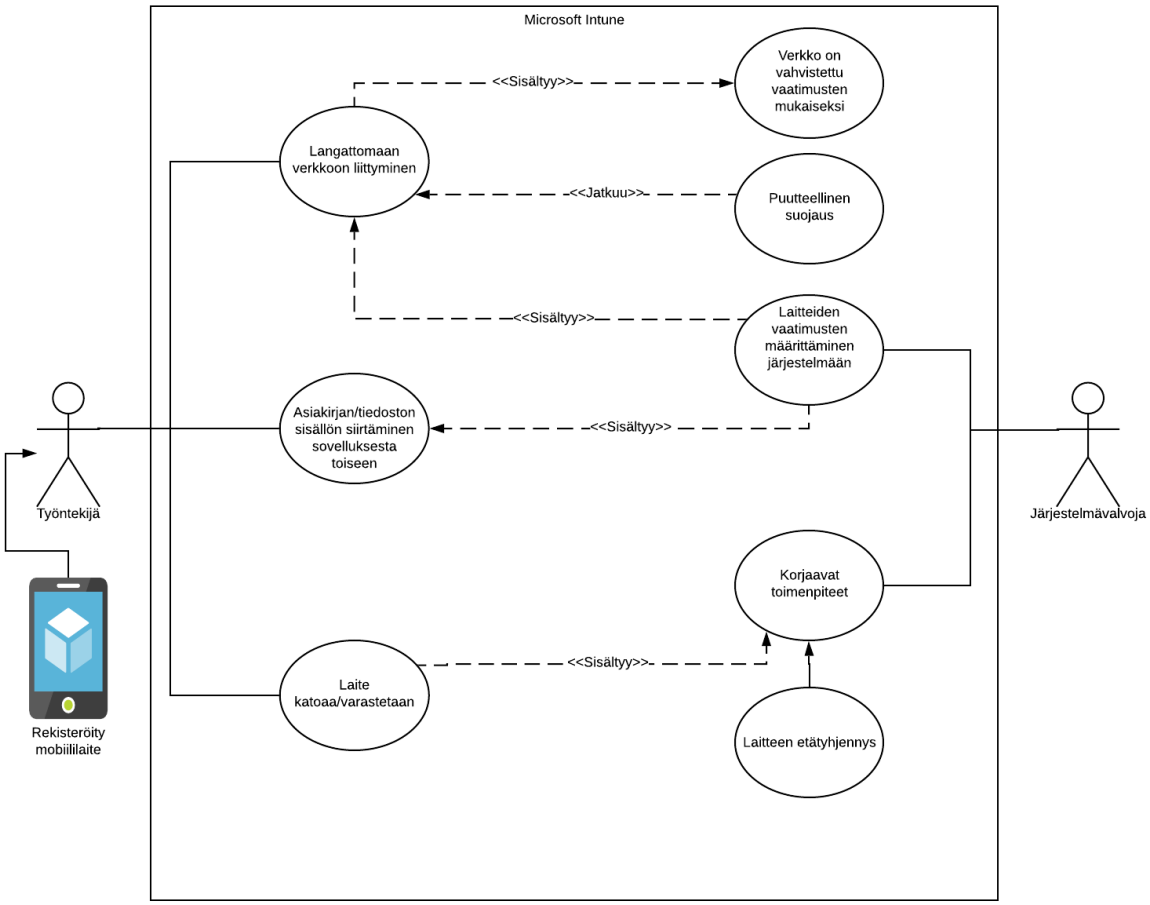
Yleiskatsaus: Työntekijä käyttää rekisteröityä mobiililaitettaan työskentelyyn.

Toimijat: Työntekijä ja järjestelmänvalvoja.

Esiehdot: Työntekijän laite on rekisteröity järjestelmään onnistuneesti ja työntekoon tarvittavat sovellukset on asennettu sekä konfiguroinnit on tehty. Sovellusten asennukset ja konfiguroinnit käydään läpi edellisessä käyttötapauksessa.

Toiminta skenaario:

1. Käyttötapaus alkaa, kun työntekijä avaa sähköpostin, hoitaa erilaisia työtehtäviä siirtämällä ja tallentamalla asiakirjoja sekä niiden tietoja eri sijainteihin mobiililaitteessa ja pilvessä.
2. Käyttäjä kadottaa mobiililaitteensa. Toimintaohjeiden mukaisesti, käyttäjä tekee ilmoituksen välittömästi IT-osastolle, josta järjestelmäasiantuntija suorittaa etätyhjennyksen kadonneelle laitteelle.



Kuva 12. Mobiililaitteella työskentely.

Kuva 12 on käyttötapauskaavio mobiililaitteella työskentelyyn. Vasemmalla toimijana on työntekijä ja oikealla järjestelmänvalvoja. Käyttötapaus hyvin samanlainen kuin edellinen, kuitenkin ilman käyttötapausten yhteistä päämäärää. Työntekijä suorittaa erilaisia työtehtäviä, kuten siirtää ja tallentaa asiakirjoja sovelluksesta toiseen puhelimella. Mahdolliseksi käyttötapaukseksi on liitetty laitteen katoaminen tai varastaminen. Tämä lisää järjestelmänvalvojan rooliin määritysten lisäksi laitteen tyhjentämisen etäyhteyden avulla. Korjaavat toimenpiteet käyttötapaus on liitetty tähän ja sen lapsiobjektina toimii laitteen etätyhjennys. Järjestelmänvalvojan tekemien määritysten avulla voidaan kontrolloida mihin verkkoon mobiililaitteella voidaan liittyä ja tuntemattomaan verkkoon yhdistäminen voidaan estää.

6 Testaus

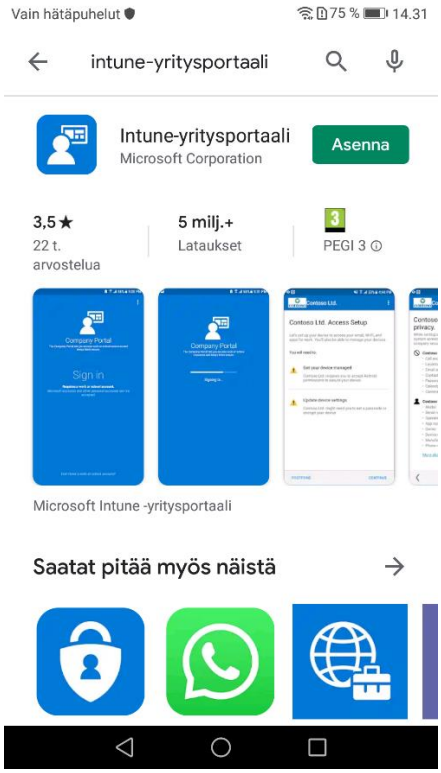
Tässä osuudessa käydään läpi kaikki 5. kappaleessa esitetyt käyttötapaukset. Testaamisessa käytetään yhtä Android-pohjaista mobiililaitetta sekä perinteisiä Microsoft Office 365 tarjoamia toimistotyökaluja. Alla on listattuna puhelimen malli ja käyttöjärjestelmä sekä hyödynnettävät sovellukset, jotka saadaan käyttöön Microsoft Office 365 tilauksella.

- Laitteen malli: Honor 7 Lite
- Käyttöjärjestelmä: Android 7.0 Marshmallow, Huawei Emotion UI
- Laitteeseen asennettavat ohjelmat: Microsoft Intune yritysportaali, Microsoft Authenticator, Microsoft Outlook, Microsoft OneDrive sekä Microsoft Word.

Testauksessa hyödynnetään käyttötapauksia, jotka ovat suunniteltu yrityskäyttöä silmällä pitäen. Tämä tulee esille henkilökohtaisten ja yrityksen resurssien erottamisella toisistaan. Käyttötapaukset ovat taas tehty määritysten perusteella, joihin on käytetty pohjana kappaleen 3 teoriaa, jossa on eritelty tavallisimpia tietoturvauhkia mobiililaitteilla ja kuinka niitä voidaan ehkäistä. Testauksessa on tarkoitus todentaa käytännössä, mitä tietyillä järjestelmän ominaisuuksilla voidaan tehdä, jotta dataa pystytään suojaamaan mobiililaitteissa. Kummassakin käyttötapauksessa on käyty vaiheittain, mitä niiden aikana tehdään ja testaus etenee sen mukaan.

6.1 Mobiililaitteen rekisteröinti työkäyttöön

Kuvassa 13 käyttäjä on avannut mobiililaitteellaan Google Play kaupan, jossa kirjoittaa hakukenttään ylhäällä ”intune-yritysportaali” ja etenee asentamaan sovelluksen valitsemalla vihreätä ”Asenna” -painiketta. Tämä on ensimmäinen vaihe, kun laitetta rekisteröidään osaksi Microsoft Intune järjestelmää.

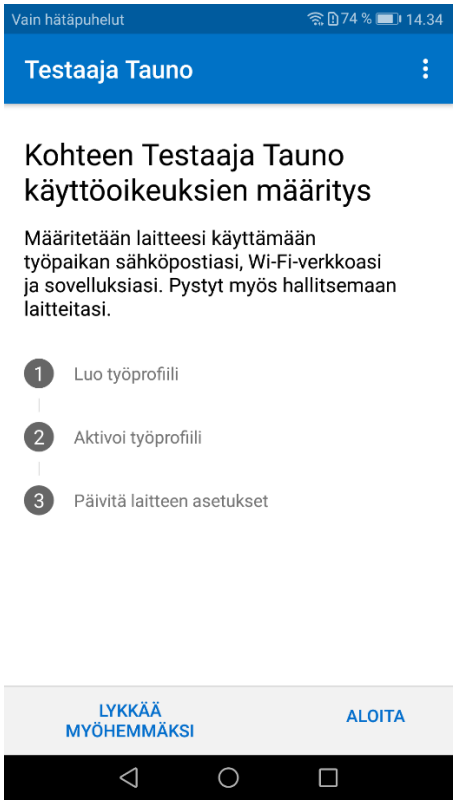


Kuva 13. Google Play kauppa.

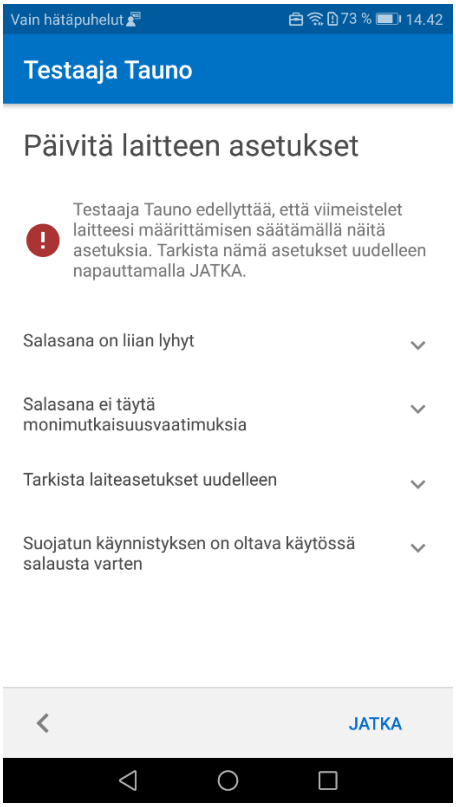
Kuva 14. Intune-yritysportaali.

Kuvassa 14 käyttäjä käynnistää Intune-yritysportaalin mobiililaitteellaan asennuksen valmistuttua, josta aukeaa kirjautumisruutu. Käyttäjä valitsee ”Kirjaudu sisään” ja etenee syöttämään työtilinsä ja salasanan. Intune-yritysportaali on laitteen rekisteröimiseen käytetty sovellus.

Kuvassa 15 käyttäjä on kirjautunut sisään portaaliin ja aloittaa käyttöoikeuksien määrittelemisen luomalla ja aktivoimalla työprofiilin (kohta 2) sekä päivittää laitteen asetukset vaatimusten mukaiseksi. Portaali ohjaa käyttäjää jokaisessa kohdassa eteenpäin ja pyytää tekemään tarvittavia muutoksia tarpeen mukaan.



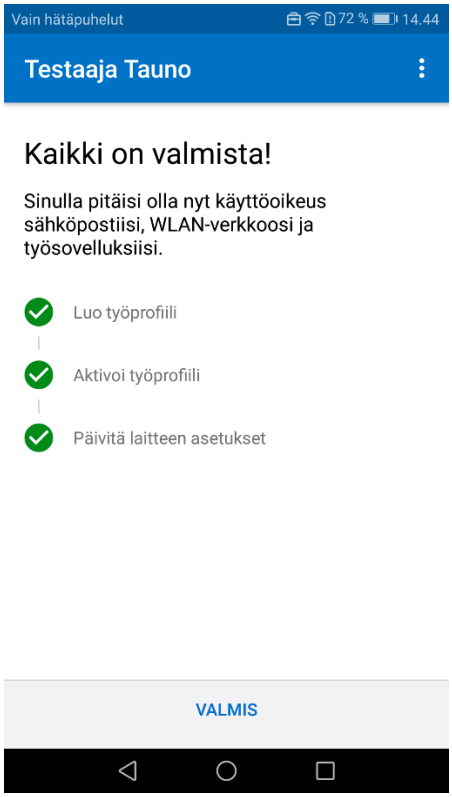
Kuva 15. Intune-yritysportaali.



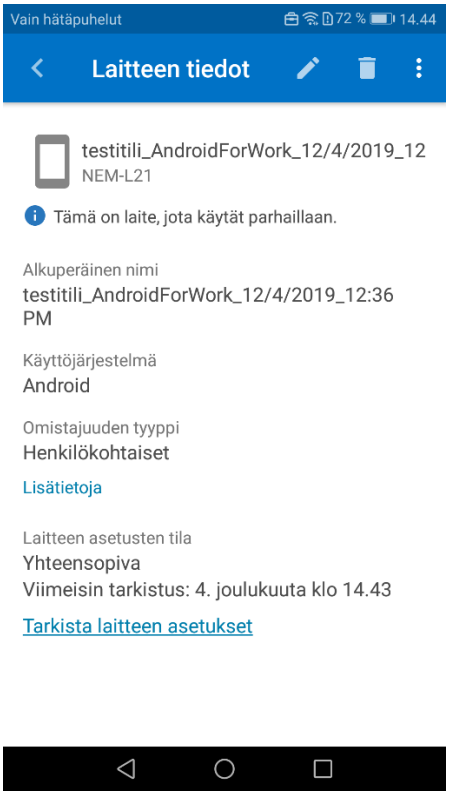
Kuva 16. Intune-yritysportaali.

Kuvan 16 kohdassa asetuksia voidaan muuttaa painamalla jokaista oikealla olevaa nuolta alaspäin ja valitsemalla ”ratkaise”. Näin rekisteröitävä laite voidaan pakottamaan käyttämään vaadittuja suojauskeinoja, jotka tässä tapauksessa ovat lukitusnäytön suojaus salasanalla sekä laitteen salausta. Salasanan vähimmäisvaatimukset ovat 16 merkkiä, numeroita, kirjaimia ja erikoismerkki. Kun käyttäjä on ratkaissut jokaisen vaaditun kohdan, rekisteröiminen voi jatkua. Nämä keinot ovat listattuna tietoturvauhkien ennaltaehkäisyyn mobiililaitteissa kappaleissa 3.3 - 3.5.

Kuvan 17 kohdassa käyttäjä on suorittanut vaatimusten mukaiset muutokset laitteen suojaukseen eli luonut vaatimusten mukaisen salasanan sekä aktivoinut laitteen suojauksen. Tämän jälkeen rekisteröinti on valmis ja mobiililaite tulee myös näkyviin Microsoft Intune:n hallintaan.



Kuva 17. Intune-yritysportaali.



Kuva 18. Intune-yritysportaali.

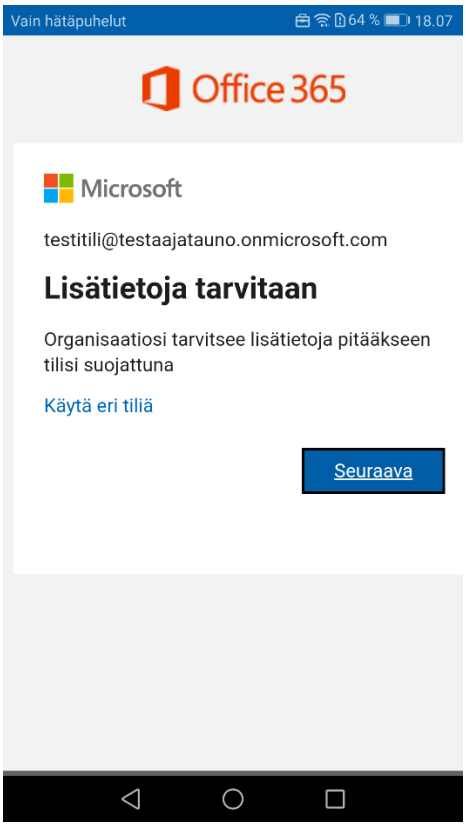
Kuvassa 18 asennuksen jälkeen sovellus näyttää käyttäjälle laitteen tiedot, josta voidaan myös varmistaa, että laite on yhteensopiva. Tämän jälkeen käyttäjä voi aloittaa tarvittavien sovelluksien asentamisen Google Play kaupan kautta, jotta laitteella pystytään käyttämään yrityksen resursseja työskentelyssä. Asennukset suoritetaan työprofiilin Google Play kaupan avulla, joka on erillinen sovellus laitteessa. Sovellus tulee työprofiilin yhteydessä laitteeseen. Tässä tapauksessa Intune-yritysportaalin yhteydessä määritelty työprofiili asensi käyttäjälle myös Microsoft Authenticator sovelluksen automaattisesti, joka oli määriteltynä kappaleessa 4.5.4. Muut työhön tarvittavat sovellukset käyttäjä asentaa itse manuaalisesti Google Play kaupan kautta. Tässä tapauksessa nämä sovellukset ovat listattuna tämän kappaleen alussa. Asennusten jälkeen käyttäjä kirjautuu työtilillään sovelluksiin.

Kun yritys hallitsee mitä sovelluksia käyttäjä voi asentaa, pystytään minimoimaan haitallisten ohjelmien asentumista laitteeseen. Vaikka tässä tapauksessa kyse on käyttäjän omasta laitteesta, jossa on erillinen työprofiili. Näin ollen yritys pystyy hallitsemaan vain

työprofiilin sisältöä ja sen sovelluksia eikä sen ulkopuolista toimintaa. Jos kyseessä olisi organisaation oma laite hallinta ja tietoturva voidaan maksimoida. Kun laite on kokonaan yrityksen hallinnassa, voidaan myös päättää itse minkä valmistajan laitteita ja malleja otetaan yrityksen käyttöön. Näistä suojakeinoista on kerrottu tarkemmin kappaleessa 3.6.

Kuva 19 kuvaa tilannetta, jossa Microsoft Outlook:ia varten on tehty erillinen määritys, joka vaatii käyttäjää käyttämään PIN-koodia kirjautumisen yhteydessä. PIN-koodin määrityksen jälkeen käyttäjä voi kirjautua lisäämälleen työtililleen normaalisti. PIN-koodi auttaa suojaamaan työsovelluksia, jos esimerkiksi puhelin sattuu olemaan avattuna ja ulkopuolinen pääsee siihen käsiksi.

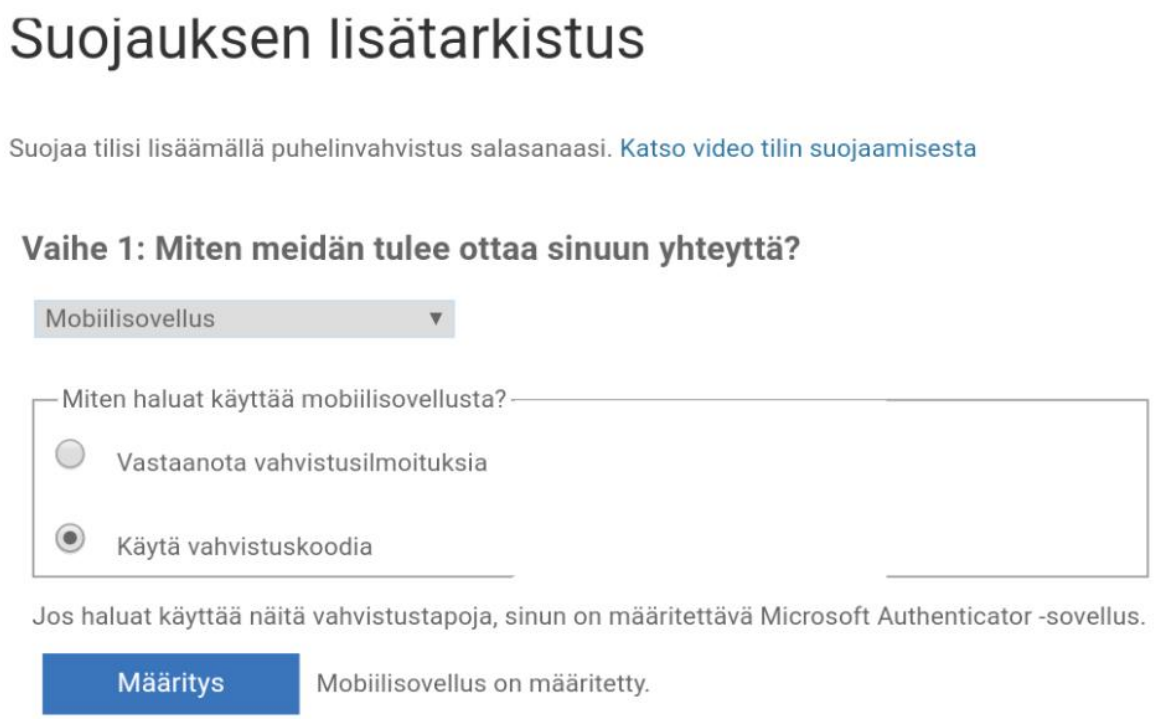
Kuva 19. Outlookin määritys.



Kuva 20. OneDriven määritys

Kuvassa 20 käyttäjä on avannut Microsoft OneDrive sovelluksen ja liittänyt työtilinsä siihen. Kuvasta voidaan havaita, että organisaatio vaatii sovellusta varten lisämäärityksiä. Tässä tapauksessa lisämääritys on monivaiheisen tunnistautumisen lisääminen työtilille, joka tulee pakotetun käytänteen myötä. Näin voidaan varmistaa, että pelkillä käyttäjätunnuksilla ei voida kirjautua työtilille. Tällä keinolla ehkäistään sähköpostiviesteillä tapahtuvan kalastelun toimivuutta. Monivaiheinen tunnistautuminen lisää huomattavasti tietoturvaa, kun kirjaudutaan omalle työtilille eri laitteilla. Aiheesta kerrotaan tarkemmin kappaleessa 4.1.

Kuvassa 21 käyttäjä on valinnut edellisestä näkymästä ”Seuraava”, josta sovellus ohjaa käyttäjää asentamaan monivaiheisen tunnistautumisen OneDriven määrityksen yhteydessä, jos sitä ei ole vielä asennettu kyseiseen mobiililaitteeseen. Käyttäjä valitsee ensin ”Miten meidän tulee ottaa sinuun yhteyttä?” -kohdan vetovalikosta ensin ”Mobiilisovellus” ja sen jälkeen kohdasta ”Miten haluat käyttää mobiilisovellusta?” itselleen sopivan vaihtoehdon. Sen jälkeen asennusta voidaan jatkaa valitsemalla vasemmalta alhaalta ”Määritys”.

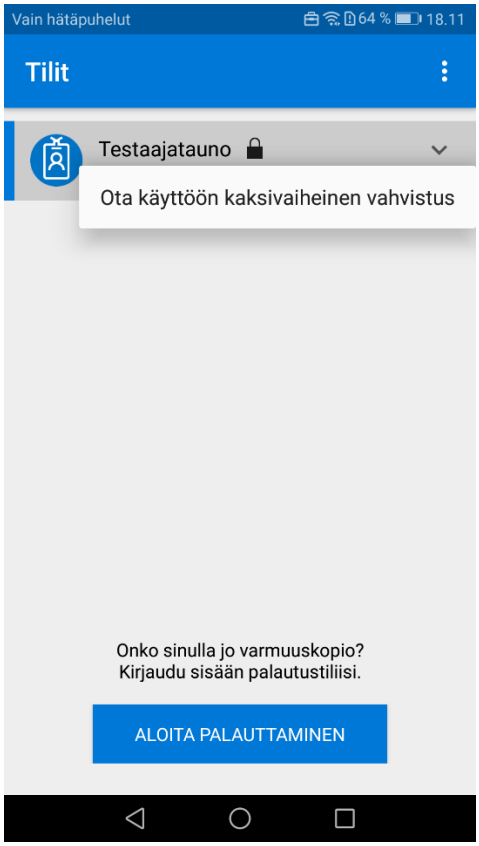


Kuva 21. OneDriven määritys

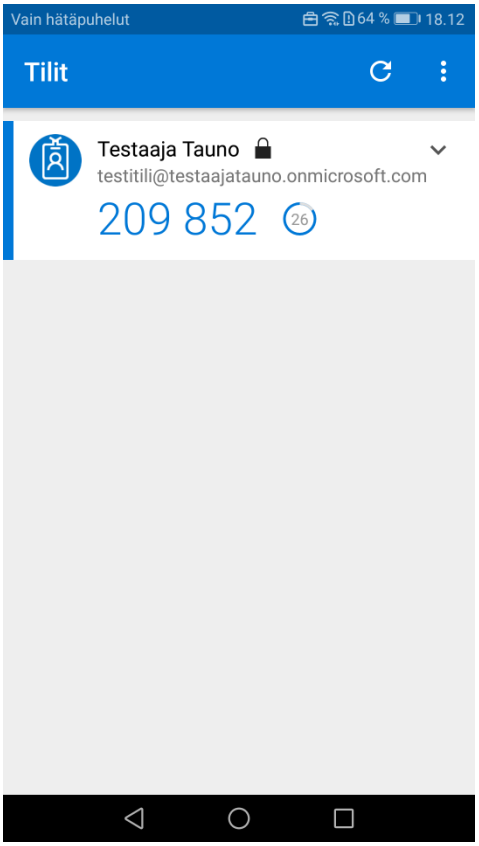
Kuva 22. Monivaiheisen tunnistautumisen määritys

Kuvassa 22 sovellus ohjeistaa käyttäjää asentamaan Microsoft Authenticator sovelluksen ja sen jälkeen lisäämään tilin sovellukseen. Tässä tapauksessa sovellus on jo asennettu, joten kohdan ”Koodi” ja ”URL-osoite” kopioidaan talteen ja ne syötetään Microsoft Authenticator sovellukseen työtilin lisäyksen yhteydessä.

Kuvassa 23 käyttäjä on avannut Microsoft Authenticator sovelluksen mobiililaitteella ja lisää oman työtilinsä siihen. Microsoft OneDrive:ä ei olla suljettu, koska määritys jatkuu tämän vaiheen jälkeen. Kun tili on lisätty, voidaan sen kohdalta valita nuolesta, joka osoittaa alaspäin, ”ota käyttöön kaksivaiheinen vahvistus”. Jonka jälkeen käyttäjä syöttää OneDriven määrityksen aikana saamansa koodin ja URL-osoitteen kenttiin.



Kuva 23. Authenticatorin määritys



Kuva 24. Authenticatorin määritys

Kuvan 24 näkymän jälkeen siirrytään takaisin Microsoft OneDrive sovellukseen, jonka jälkeen sovellus pyytää syöttämään Authenticatorissa näkyvän numerokoodin OneDriveen pääsyä varten.

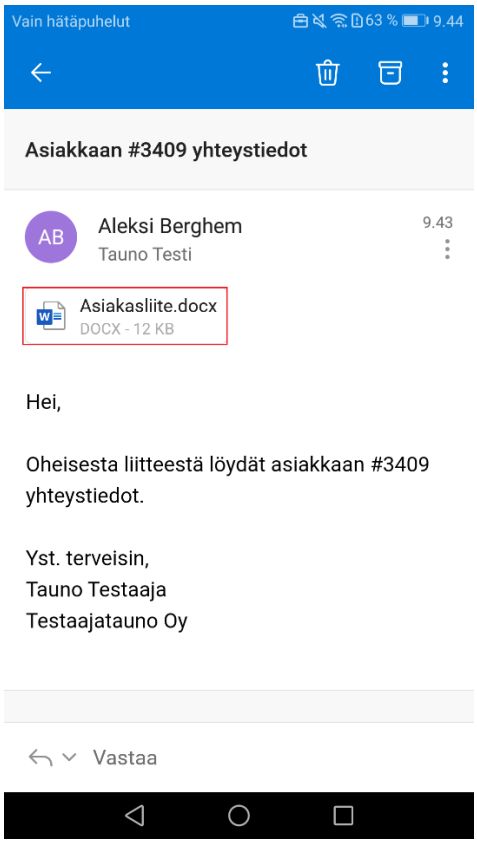
Kuvassa 25 käyttäjä on asentanut tarvittavat sovellukset työntekoa varten puhelimeensa. Laite on yrityksen käytänteiden mukainen, jotta työskentely laitteella on tietoturvan näkökulmasta turvallista. Työprofiilin sovellukset ovat merkattuna punaisella työkalupakilla, jotta henkilökohtaiset resurssit voidaan erotella yrityksen resursseista.

Kuva 25. Työprofiilin sovellukset kotinäkymässä.

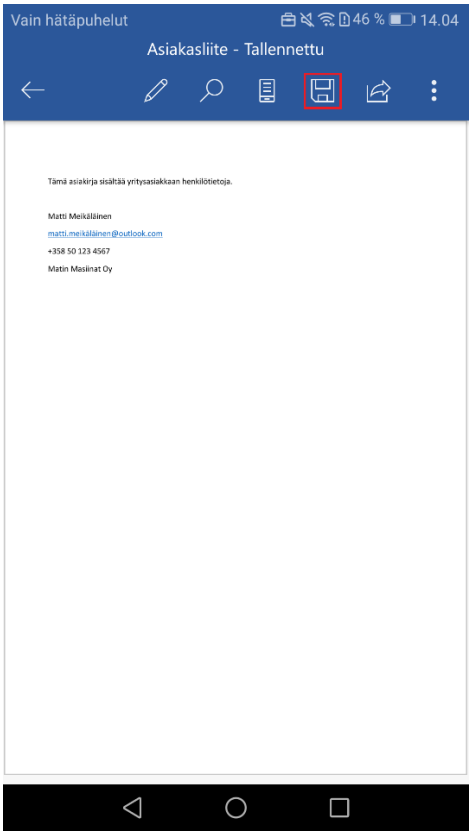
6.2 Mobiililaitteella työskentely

Tässä käyttötapauksessa kuviin on lisätty punainen neliö helpottamaan käyttäjän tekemien valintojen etenemistä jokaisessa vaiheessa.

Kuvassa 26 käyttäjä on avannut Outlook sähköpostisovelluksen puhelimellaan ja avannut saapuneet kansiosta viestin, jossa on liitteenä asiakastietoja sisältävä Word asiakirja. Painamalla viestin sisällä liitettä laite avaa sen erillisessä asiakirjojen luku- ja muokkausso-velluksessa, joka tässä tapauksessa on Microsoft Word.



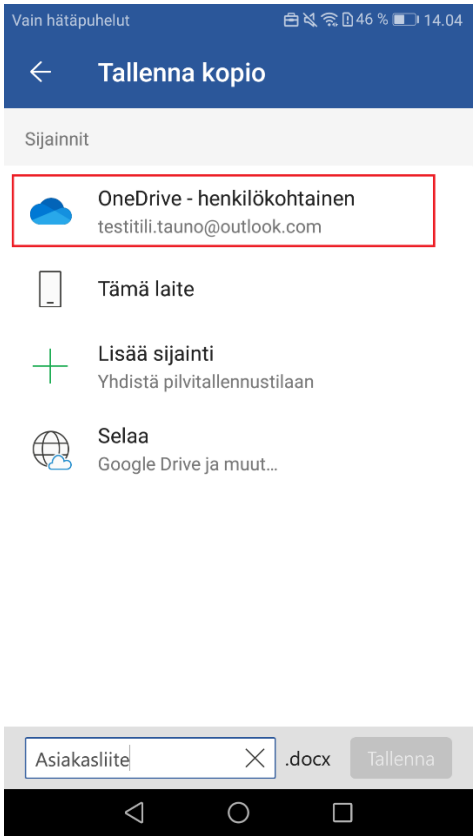
Kuva 26. Outlook sähköposti



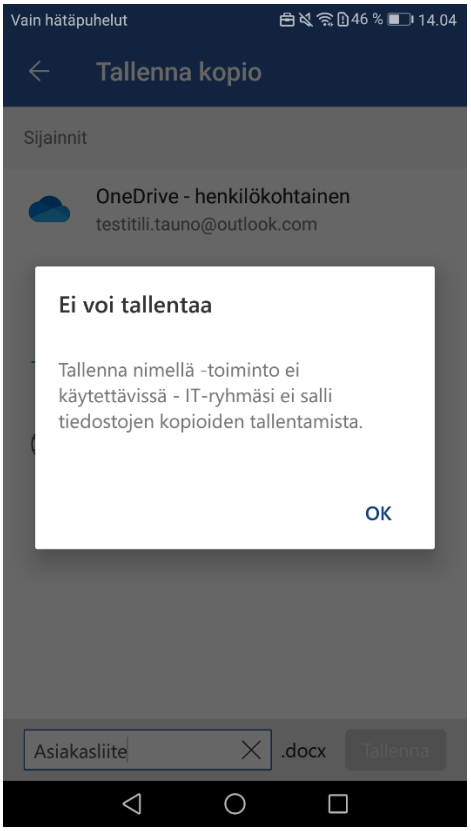
Kuva 27. Word asiakirja

Kuvassa 27 käyttäjä on avannut liitteen, jossa on asiakastietoja ja etenee tallentamaan sitä pilveen itsellensä jatkokäyttöä varten painamalla oikealta yläkulmasta levyikoni nappia, joka on kehystetty punaisella laatikolla.

Kuvan 28 levyikoni nappi tuo käyttäjän tallennus vaihtoehtoihin kopion tallentamiseksi. Käyttäjä tässä tapauksessa valitsee tallennuskohteeksi henkilökohtaisen OneDrive tilinsä.



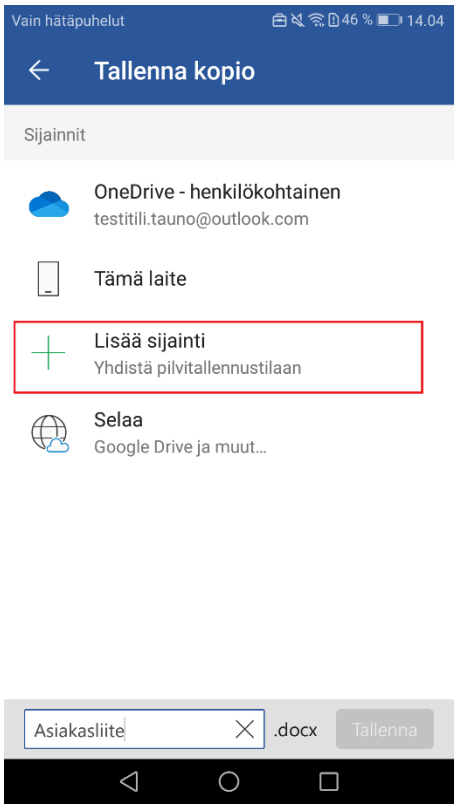
Kuva 28. OneDrive tallennus



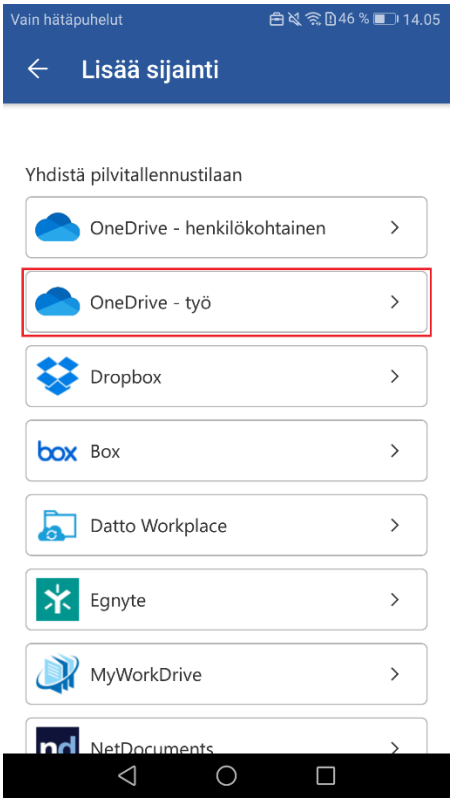
Kuva 29. OneDrive tallennus

Kuvassa 29 käyttäjän valittua henkilökohtaisen tilinsä järjestelmä antaa virheilmoituksen, joka ilmoittaa tallentumisen estymisestä. Tallennus on määritysten mukaan estetty henkilökohtaisille tileille mobiililaitteilla, jos käsitellään organisaation resursseja. Tässä tapauksessa kuvitellaan, että liitetiedosto on otettu henkilön työsähköpostista, joten tallentaminen henkilökohtaiseen tiliin estetään.

Kuvassa 30 käyttäjä voi edetä tallentamaan tiedoston työtilillensä valitsemalla ”Lisää sijainti” tai valitsemalla luettelosta työtilinsä. Tässä tapauksessa käyttäjä ei ole vielä lisännyt työtiliään OneDriveen.



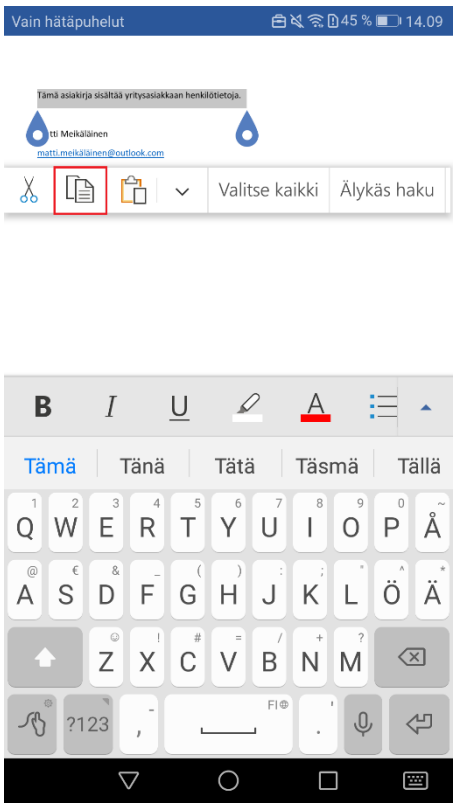
Kuva 30. OneDrive tallennus



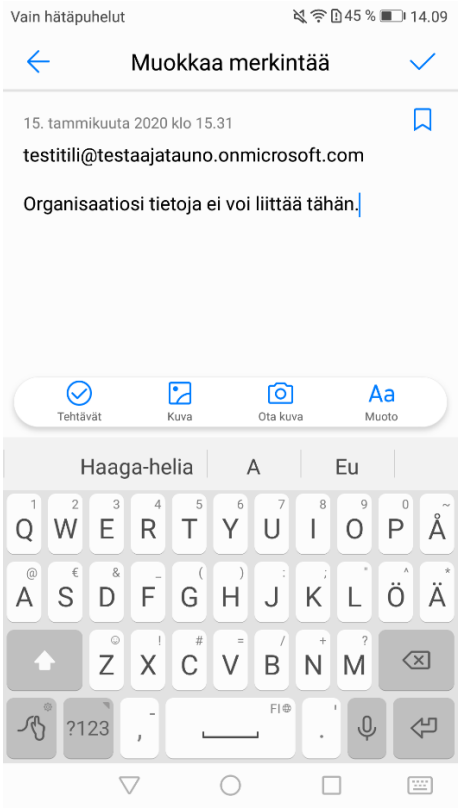
Kuva 31. OneDrive tallennus

Kuvassa 31 valittuaan ”Lisää sijainti” järjestelmä ohjaa käyttäjän valitsemaan minkä tilin hän haluaa lisätä. Kohdasta valitaan ”OneDrive – työ”, johon työntekijä voi tallentaa organisaation omistamat resurssit kuten kyseisen asiakirjan. Tässä tapauksessa järjestelmä on määritelty rajaamaan organisaation resurssien tallentamista siten, että muita vaihtoehtoja ei ole mahdollista käyttää. Valinnan jälkeen sovellus ohjaa käyttäjän kirjautumaan normaalisti työtililleen, jonka jälkeen sijainti lisätään listaan. Tämän jälkeen asiakirjan kopion tallennus onnistuu lisätylle työtilille, jos se on organisaation sisäinen tili.

Kuvassa 32 käyttäjä kopioi asiakirjan tietoja ja tarkoituksena on siirtää niitä toiseen sijaintiin.



Kuva 32. Word asiakirja

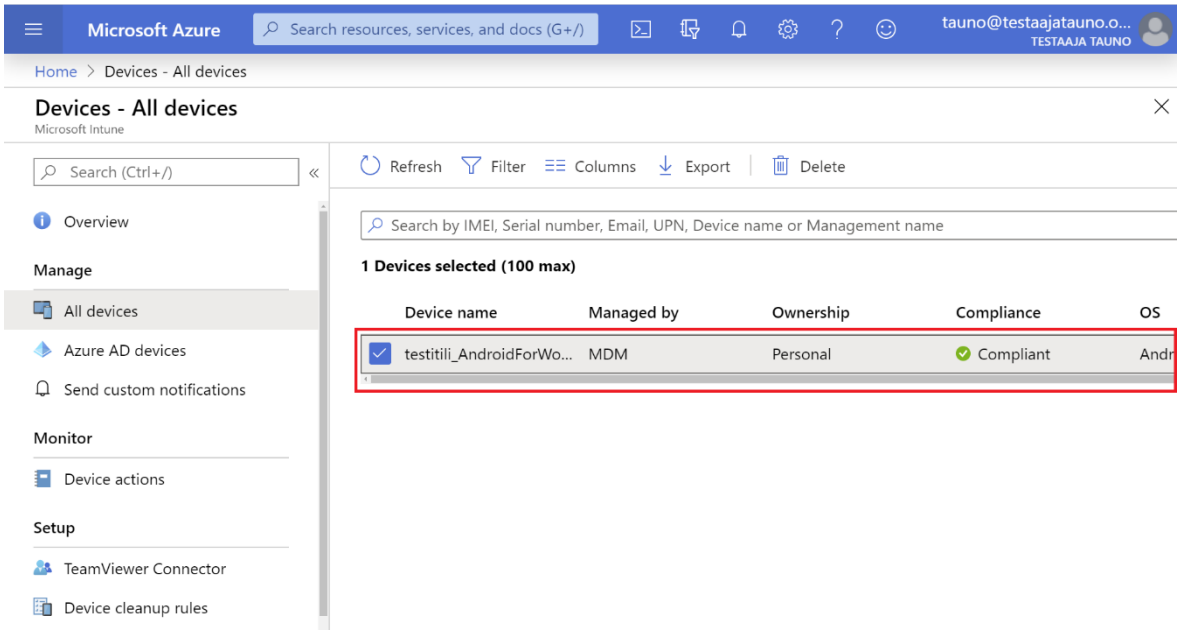


Kuva 33. Muistio

Kuvassa 33 käyttäjä on avannut mobiililaitteen oman muistion ja koittanut liittää tietoja asiakirjasta sinne. Sovelluksiin tehtyjen määritysten perusteella tietojen liittäminen organisaation ulkopuolisiin sovelluksiin on estetty eli tässä tapauksessa mobiililaitteen omaan muistioon. Liittäessä käyttäjä saa tekstikenttään ilmoituksen ”Organisaatiosi tietoja ei voi liittää tähän”. Tiedoston tai tietojen siirtäminen tiedoston sisältä on rajoitettu, jotta käyttäjien tekemiä virheitä voidaan minimoida. Tällä tavoin estetään virhetoiminta, joka on selitetty kappaleessa 3.1.

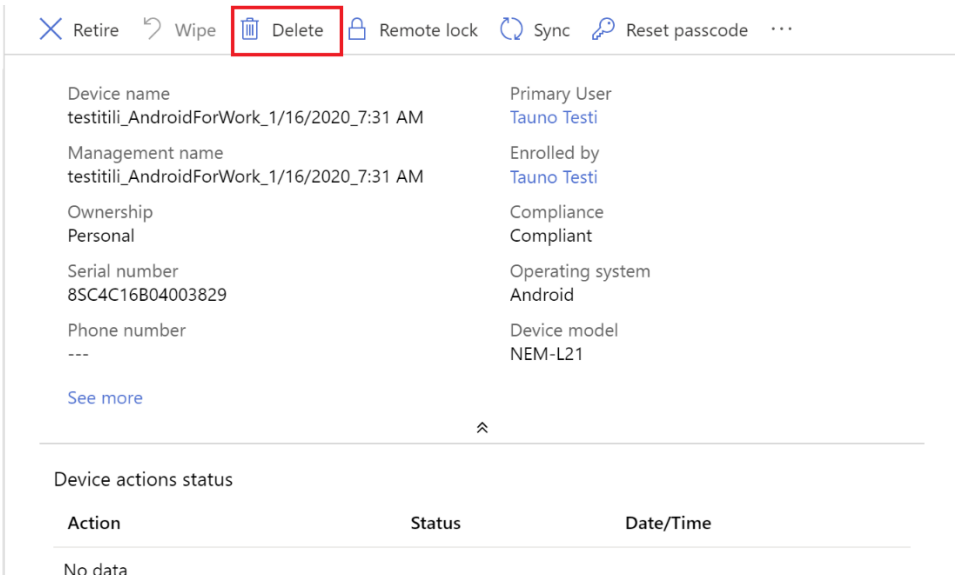
Tässä vaiheessa käyttötapausta kuvataan tilanne, jossa käyttäjä on kadottanut mobiililaitteensa. Kun käyttäjä on tehnyt ilmoituksen katoamisesta IT-osastolle, järjestelmänvalvojan suorittaa Intune:n hallinnasta seuraavat toimet yrityksen resurssien suojaamiseksi.

Kuvassa 34 järjestelmänvalvoja avaa portaalista vasemmalta valikosta etenemällä kohdista *Devices -> All devices* ja valitsee kyseisen laitteen listasta.



Kuva 34. Intune:n hallinta

Kuvassa 35 oikea laitekortti on avattuna, josta seuraavaksi valitaan ylhäältä ”Delete” -toiminto. Tällöin järjestelmä poistaa työprofiilin laitteesta ja sen sisältämät sovellukset seuraavan kerran, kun laite on yhteydessä verkkoon. Laite on koko ajan yhteydessä järjestelmään sen rekisteröinnin jälkeen, kun sillä on verkkoyhteys ja näin ollen poistotoiminnon antava käsky tulee myös sitä kautta laitteeseen välittömästi. Tällä tavoin yrityksen resurssit voidaan suojata ulkopuolisilta, vaikka laitetta ei tavoitettaisi fyysisesti. Tätä toimenpidettä kutsutaan etätyhjennykseksi. Toimenpide on selitetty tarkemmin suojauskeinona kappaleessa 3.4.



Kuva 35. Intune:n hallinta

7 Pohdinta

Työn aikana selvitettiin mitkä ovat yleisempiä tietoturvauhkia sekä niiden ehkäisykeinoja mobiililaitteissa. Työssä tutkittiin, miten tietoturvauhkia mobiililaitteissa pystytään ehkäisemään käytännössä, käyttämällä Microsoft Intune järjestelmän ominaisuuksia.

Ongelmien ehkäisyä varten olennaista oli, että järjestelmään tehdään määritykset rekisteröitäville laitteille. Määritysten avulla pystytään hallitsemaan resurssien käyttöä ja käsiksi pääsyä laitteissa. Määritykset oli tehty kappaleen 3 teoriaa hyödyntäen. Testauksen aikana pystyttiin todistamaan käyttötapausten avulla, miten käytännössä järjestelmän ominaisuuksilla voidaan ehkäistä mobiililaitteiden yleisimpiä tietoturvauhkia, joita oli käsitelty kappaleessa 3. Käyttötapaukset oli luotu yrityskäyttöä silmällä pitäen, jotta tämä yritysaspekti tulisi paremmin työssä esille. Kappaleen 5.1 käyttötapaus sisälsi tavallisen tilanteen, missä työntekijä ottaa uuden työpuhelimen käyttöönsä ja tätä varten laite rekisteröidään järjestelmään sekä sovellukset asennettiin työskentelyä varten valmiiksi. Toisessa käyttötapauksessa kappaleessa 5.2 käytiin läpi tavallista työskentely tilannetta mobiililaitteella, joka sisälsi sähköpostin käytön, asiakirjojen muokkaamisen sekä niiden tallentamisen pilvipalveluun.

Olennaista testauksessa oli havainnollistaa, kuinka yrityksen resursseja voidaan erottaa henkilökohtaisista resursseista käyttämällä esimerkiksi erillistä työtiliä. Työtili luotiin rekisteröinnin yhteydessä laitteeseen, joka sisälsi työsovellukset. Sen lisäksi määritysten avulla säädettiin, minne organisaation resursseja laitteella voidaan tallentaa tai millä niitä voidaan hallinnoida. Tässä tapauksessa organisaation resursseja hallinnoitiin juurikin asennetuilla työsovelluksilla.

Ongelmat, joihin itse järjestelmästä ei löytynyt suoraa ratkaisua, olivat kalasteluun puuttuminen. Kalastelua voidaan ehkäistä monivaiheisella tunnistautumisella, joka on osana Microsoftin käyttäjätilien hallintaa pilvessä. Testauksesta jätettiin myös pois mobiililaitteiden uhkien torjuntatyökalun käyttö, jolla olisi pystytty lisäämään tietoturvaa. Mobiililaitteiden uhkien torjuntatyökalun käyttö olisi vaatinut kolmannen osapuolen ohjelman lisäämistä järjestelmään. Tämän takia se rajattiin testauksesta pois, koska se ei ole varsinaisesti järjestelmän oma ominaisuus.

Microsoft Intune on erittäin varteenotettava hallintajärjestelmä yrityksen laitteille ja koko järjestelmä on rakennettu pilveen, jota pidetään yleisesti IT-maailmassa nykyaikaisena ratkaisuna. Järjestelmä on helppo ottaa käyttöön ja laitteiden liittäminen järjestelmään on

selkeää. Ympäristön rakentaminen tietoturvalliseksi on kuitenkin järjestelmänvalvojan vastuulla ja vaatii oman työnsä. Vastuuhun sisältyy tietoturvallisten käytänteiden tuntemusta sen perusteella järjestelmään tehtävien määritysten tekeminen ja testaaminen toimiviksi.

Haasteena työssä oli ympäristön luominen sellaiseksi, että se vastaisi yrityksen tarpeita tietoturvallisesti sekä käytettävyydeltään. Julkisten verkkojen estäminen järjestelmään rekisteröidyiltä laitteilta on mahdollista, tekemällä määrityksiä verkkoon. Käytännössä voidaan estää kaikki tuntemattomat langattomat verkot ja sallitut verkot joudutaan erikseen merkitsemään järjestelmään. Itse työssä tehtiin määritykset sallituista verkoista kappaleessa 4.5.3 mutta resurssien puutteiden vuoksi tätä ei voitu tuoda mukaan testaukseen, vaikka langattomista verkoista oli käyttötapaus tehtynä kappaleessa 5. Testausta varten havainnollistamiseen olisi tarvittu kahta eri langatonta verkkoa, joihin minulla ei ollut mahdollisuutta, koska en omistanut kahta reititintä. Testasin ainoastaan erillisillä määrityksillä ominaisuuden toimivuutta, jota en sisällyttänyt itse työn dokumentaatioon, koska se ei olisi palvellut työn sisältöä. Käytännössä testaus piti sisällään eri IP-osoitteen määrityksen ja näin ollen laite ei päässyt käytetystä verkosta käsiksi esimerkiksi yrityksen sähköpostiin, koska se ei ollut sallittujen verkkojen listalla. Tämän lisäksi haasteena oli punnita, onko esimerkiksi tarpeellista asettaa PIN-koodeja itse mobiililaitteen avaamisen lisäksi jokaisen sovelluksen avaamisen yhteyteen. PIN-koodien käyttäminen sovellusten avaamisen yhteydessä saattaa olla enemmänkin työskentelyä kuormittava tekijä, koska mobiililaitteen lukitusnäyttö on jo suojattu koodilla.

Työ on elänyt valtavasti sitä tehdessäni. Olen hahmottanut tekemisen lomassa selkeämmin työn varsinaista rajausta sekä mikä olisi olennaista työn toimivuuden kannalta. Työstä jätettiin pois kokonaan EU:n määrittelemä yleinen tietosuojasopimus sekä käyttötapauksia tehdessä päädyttiin kahteen yksinkertaiseen tapaukseen, jotta työn sisältö pysyisi kompaktina kokonaisuutena. Sisällön määrän väheneminen on helpottanut työssä tutkittavia asioita, kun se on voitu rajata tällöin ajallisesti hallittavammaksi kokonaisuudeksi. Tutkimuskysymys on muuttunut työn aikana useaan otteeseen selkeämmäksi, kun sisältöä on rajattu työtä tehdessä.

Olen oppinut valtavasti itse järjestelmästä työn aikana ja oppinut sen käyttöä myös käytännössä, kun lisäsin toiminnallisen osuuden työhön. Jouduin työn aikana toiminnallisessa osuudessa rakentamaan siinä käytettävän ympäristön alusta alkaen, käyttäen Microsoftin dokumentaatiota. Tämä sisälsi tilien luomisen, lisenssien tilaamisen ja järjestelmän määritykset. Osuuden aikana pystyin testaamaan erilaisia määrityksiä järjestelmään ja heti todentamaan niiden toimivuuden, kun olin rekisteröinyt testattavan mobiililaitteen järjestel-

mään. Alkuperäinen tavoitteeni olikin, että pystyisin tuomaan käytäntöä tutkimuksen lisäksi, jota pidän erittäin arvokkaana osaamisena tulevaan työelämään. Tämä tulee esille kykynä opetella itsenäisesti uusia tekniikoita ja soveltamaan niitä käytännössä.

Käytännön lisäksi olen oppinut tutkimuksen myötä erittäin paljon Microsoft Intune:n ominaisuuksista ja mihin se pystyy yrityskäytössä. Ydinomaisuudet pitivät sisällään laitteiden tietoturvan parantamisen sekä sovellusten hallinnoinnin ja tietoturvan. Olenkin havainnut, että mobiililaitteiden hallinta tässä järjestelmässä on vain pieni osa suurta kokonaisuutta, jolla pystytään käytännössä tuottamaan yrityksille iso osa niiden IT:n infrastruktuuria. Hallitsen työn myötä pienen kokonaisuuden yhdestä järjestelmästä ja sen mahdollisuuksista tietoturvaongelmien ehkäisyssä. Tämän kautta voin aloittaa laajentamaan osaamistani muihin Microsoftin tuottamiin järjestelmiin, jotka tarjoavat yritysten resursseille tietoturvaratkaisuja. Isompien järjestelmäkokonaisuuksien hallitseminen edesauttaa palveluiden tarjoamista yrityksille kokonaisvaltaisemmin ja mahdollistaa työskentelyn yrittäjänä tulevaisuudessa. Työn aikana olen myös oppinut keskittymään enemmän olennaiseen ja selittämään asiat selkeämmin niistä tietämättömälle. Toimiva viestintä sekä esitystavat ovat tärkeä osa yritysten toimintaa, jolla voidaan ehkäistä ajan tuhlaamista ja niistä koituvia tappioita. Yhden viestin tulisi sisältää kaikki olennaiset tiedot ja se ei vaadi perään viittä jatkokysymystä. Näin jatkoselvittelyyn ei tarvitse tuhlata aikaa ja viestintä on suoritettu oikein.

Lähteet

Amazon Web Services 2019. What is Cloud Computing? Luettavissa: https://aws.amazon.com/what-is-cloud-computing/ Luettu: 17.10.2019

Microsoft Azure 2019. What is SaaS? Luettavissa: https://azure.microsoft.com/en-in/overview/what-is-saas/ Luettu: 17.10.2019

Microsoft Azure 2019. Serverless computing. Luettavissa: https://azure.microsoft.com/en-in/overview/serverless-computing/ Luettu: 17.10.2019

Microsoft Azure 2019. What is cloud computing? Luettavissa: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ Luettu: 17.10.2019.

Ensi-Maria 1.8.2017. IaaS, PaaS, SaaS – What do they mean? CloudOnMove. Luettavissa: http://cloudonmove.com/iaas-paas-saas-what-do-they-mean/ Luettu: 18.10.2019.

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

Microsoft Docs 2019. Microsoft Intune overview. Microsoft Intune is an MDM and MAM provider for your devices. Luettavissa: https://docs.microsoft.com/en-us/intune/fundamentals/what-is-intune Luettu: 25.10.2019.

Microsoft 2019. Microsoft 365. Microsoft Enterprise Mobility + Security. Luettavissa: https://www.microsoft.com/fi-fi/microsoft-365/enterprise-mobility-security/microsoft-intune Luettu: 25.10.2019.

Microsoft Docs 2019. Common wasy to use Microsoft Intune. Luettavissa: https://docs.microsoft.com/fi-fi/intune/fundamentals/common-scenarios Luettu: 26.10.2019.

Microsoft Docs 2019. Basic setup. Luettavissa: https://docs.microsoft.com/en-us/intune/fundamentals/migration-guide-setup Luettu: 15.11.2019.

Microsoft Docs 2019. Supported operating systems and browsers in Intune. Luettavissa: https://docs.microsoft.com/en-us/intune/fundamentals/supported-devices-browsers Luettu: 15.11.2019.

Microsoft Docs 2019. Set up Intune. Luettavissa: https://docs.microsoft.com/en-us/intune/fundamentals/setup-steps Luettu: 15.11.2019.

Raphael, JR. 22.7.2019. 7 mobile security threats you should take seriously in 2019. Luettavissa: https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html Luettu: 16.11.2019.

Deloitte 2014. Mobile devices: Secure or security risk? Luettavissa: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/mobile_device_secure_security_risk.pdf Luettu: 16.11.2019.

Mazyar, H. 31.11.2019. vpnMentor. Miksi sinun TODELLA tulee lakata käyttämästä julkista Wi-Fiä. Luettavissa: https://fi.vpnmentor.com/blog/miksi-sinun-todella-tulee-lakata-kayttamasta-julkista-wi-fia/ Luettu: 16.11.2019.

Securitymetrics 2019. Mateaki, G. Securing Mobile Devices With Mobile Encryption. Luettavissa: https://www.securitymetrics.com/blog/securing-mobile-devices-mobile-encryption Luettu: 18.11.2019.

Gray, R. 11.7.2018. Mobile Threat Defense. Luettavissa: https://www.wandera.com/mobile-threat-defense/what-is-mobile-threat-defense-mtd/ Luettu: 18.11.2019.

Montgomery, M. 11.9.2019. Protect Your Enterprise by Setting Standards for Mobile Security. Luettavissa: https://www.securitymagazine.com/articles/90884-protect-your-enterprise-by-setting-standards-for-mobile-security Luettu: 18.11.2019.

Microsoft Azure 2019. Azure Active Directory. Luettavissa: https://azure.microsoft.com/en-us/services/active-directory/ Luettu: 4.12.2019.

Kyberturvallisuuskeskus 2019. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf Luettu: 9.12.2019.

Microsoft Docs 2019. Learn about Conditional Access and Intune. Luettavissa: https://docs.microsoft.com/en-us/intune/protect/conditional-access Luettu: 13.12.2019.

Visual Paradigm 2019. What is Use Case Diagram? Luettavissa: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-use-case-diagram/ Luettu: 13.12.2019.

Microsoft Docs 2019. Mobile Threat Defense integration with Intune. Luettavissa: https://docs.microsoft.com/en-us/intune/protect/mobile-threat-defense Luettu: 31.12.2019.