Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

EERO NIEMI

Mobiililaitteiden keskitetty hallinta Androidille

TIETOJENKÄSITTELYN KOULUTUSOHJELMA
2020

Tekijä
Niemi, Eero

Julkaisun laji
Opinnäytetyö, AMK

Päivämäärä
Toukokuu 2020

Sivumäärä
23

Julkaisun kieli
Suomi

Julkaisun nimi
Mobiililaitteiden keskitetty hallinta Androidille

Tutkinto-ohjelma
Tietojenkäsittely

Tiivistelmä
Mobiililaitteiden käyttö yrityksissä yleistyy jatkuvasti, ja sen myötä mobiililaitehallintaan on kiinnitettävä riittävästi huomiota. Ennen mobiililaitteiden käyttöönottoa yrityksen tulee tehdä tarkka suunnitelma siitä, miten laitteiden hallinta tullaan toteuttamaan ja mikä hallintajärjestelmä otetaan käyttöön. Suunnitelma tulee tehdä tarkkaan, jotta se mukautuu yrityksen omiin vaatimuksiin ja liiketoimintaan mahdollisimman hyvin.

Opinnäytetyössä tutkittiin Android-laitteiden keskitettyyn hallintaan tarjolla olevia ratkaisuja ja hallintajärjestelmiä. Työssä tehtiin suunnitelma siitä, miten yrityksessä voitaisiin ottaa uudet Android-laitteet käyttöön mahdollisimman nopeasti ja turvallisesti. Suunnitelmassa käytiin läpi asiat, jotka yrityksen tulee huomioida ennen laitteiden käyttöönottoa. Työssä vertailtiin kolmea eri mobiililaitteiden hallintajärjestelmää ja valittiin yritykselle lopulta Miradoren ratkaisu käyttöön.

Asiasanat
Android, mobiililaite, hallintajärjestelmä

Author Niemi, Eero	Type of Publication Bachelor's thesis	Date May 2020
	Number of pages 23	Language of publication: Finnish

Title of publication
Mobile device management for Android

Degree program
Degree programme in Business Information Technology

Abstract

The use of mobile devices in companies is constantly becoming more common and therefore sufficient attention must be paid to mobile device management. Before the initialization of mobile devices the company must make a detailed plan for how the device management will be organized and which management system will be implemented. The plan should be more carefully so that it adapts to the requirements and business strategies of the company.

The thesis examines the solution available for the centralized management of Android devices. The thesis considers a plan on how a company could initialize new Android devices as quickly and safety as possible. The plan reviews the things a company should consider before deploying equipment. This thesis compares three different mobile device management systems and finally the solution of Miradore is selected for the company.

Key words
Android, mobile device, management system

SISÄLLYS

1 JOHDANTO

Mobiililaitteiden käyttö yleistyy jatkuvasti tavallisten kuluttajien lisäksi myös yritysten jokapäiväisessä toiminnassa. Yrityksissä käytetään nykyään työasemia ja muita oheislaitteita paljon hyödyksi, mutta keskitetyn mobiililaitehallinnan avulla myös mobiililaitteet tukevat yrityksen toimintaa tehokkaasti. Yrityksen mobiililaitteisiin voidaan jakaa keskitetysti esimerkiksi asetusmääritykset, yrityksen toimintaan tarvittavat sovellukset ja erilaiset tietoturvaohjelmat/asetukset.

Android on noussut vuosi vuodelta suositumpaan asemaan mobiilikäyttöjärjestelmiä vertailtaessa ja se kilpailee suosiosta Applen iOS:n kanssa. Yrityksissä se on helppo valinta työntekijöiden käytössä olevien älypuhelimien käyttöjärjestelmäksi, mutta Android tuo mukanaan myös haasteita. Avoimen lähdekoodin ratkaisuun perustuva Android antaa nimittäin mahdollisuudet haittaohjelmien levitykselle Androidin Google Play -sovelluskaupan kautta. Androidin uusista tietoturva-aukoista uutisoidaan jatkuvasti, ja tämä on yritysmaailmassa tietysti huono asia. Yrityksen toiminnassa jokaisen osa-alueen tulisi olla sellainen, että tietoturvallinen ympäristö saadaan turvattua joka tilanteessa.

Tämän opinnäytetyön tarkoituksena on tutkia yritystasolla mobiililaitteiden keskitettyä hallintaa. Tilaajaa tällä opinnäytetyölle ei erikseen ollut, joten opinnäytetyö keskittyy keskitetyn hallinnan käsittelemiseen oman tutkimuksen kautta. Työ keskittyy mobiililaitteisiin, joissa on Android-käyttöjärjestelmä. Opinnäytetyössä tutkitaan toteutustapoja mobiililaitteiden keskitetylle hallinnalle ja käydään läpi sen mukanaan tuomia ominaisuuksia. Työn tarkoituksena on tutkia, mitä vaatimuksia keskitetty hallinta tuo mukanaan ja mihin hallinnalla pyritään. Tutkitaan myös tietoturvallisuuden näkökulmasta keskitettyä hallintaa. Tietoturva on tärkeä osa keskitetyn hallinnan suunnittelussa, koska sen unohtaminen saa parhaillaan aikaan tietovuotoja ja muita kriittisiä ongelmia yrityksen sisällä.

2 ANDROID-KÄYTTÖJÄRJESTELMÄ

Android on maailman suosituin mobiililaitteiden käyttöjärjestelmä ja se perustuu Linux-ytimeen. Android-käyttöjärjestelmä tunnetaan varmasti parhaiten älypuhelimien ja tablettien käyttöjärjestelmänä, mutta nykyään Androidia hyödynnetään myös esimerkiksi älykelloissa ja autostereoissa. Android perustuu avoimeen lähdekoodiin, joka mahdollistaa sen ilmaisen käytön ja sovellusten kehittämisen maksuttomasti. Googlen tarjoamat sovellusten kehittämistyökalut ovat avoimia kaikille, eli kuka tahansa käyttöjärjestelmän käyttäjistä voi lähteä mukaan sovelluskehitykseen halutessaan. Android-puhelimia on saatavilla lähes jokaisesta hintaluokasta halvimmista perusmalleista aina laajoilla ominaisuuksilla varustettuihin lippulaivamalleihin. Android-käyttöjärjestelmää käyttäviä laitteita on markkinoilla tarjolla monilta eri valmistajilta, kuten esimerkiksi Samsung, Sony, LG ja Huawei.

Android-käyttäjällä yksi tärkeä ja olennainen osa käyttöjärjestelmää on Google Play -sovelluskauppa. Sovelluskaupan kautta käyttäjä voi ladata vapaasti laitteeseensa esimerkiksi haluamiaan pelejä ja omiin tarpeisiinsa sopivia sovelluksia. Sovellusta ladatessaan käyttäjälle voi kuitenkin tulla erilaisia käyttölupapyyntöjä sovellukselta esimerkiksi puhelimen sijaintiin ja mikrofonin käyttöön. Näiden lupien sallimisessa tulee kuitenkin olla tarkkana, sillä tietyt sovellukset saattavat kalastella käyttäjiltä sovelluksen käytön kannalta tarpeettomia käyttölupia.

Käyttöjärjestelmän avoimuus antaa monipuoliset mahdollisuudet sen tehokkaalle ja vaivattomalle käytölle, mutta avoimuus tuo myös mukanaan tietoturvallisuuden haasteet. Hakkerit voivat helposti kehittää erilaisia haittaohjelmia sovelluskauppaan, josta käyttäjät saattavat ladata näitä laitteeseensa. Google Play -kaupan tarjontaa toki seurataan aktiivisesti, mutta monesti haittaohjelman löytyessä moni käyttäjä on jo ladannut laitteeseensa haittaohjelman.

2.1 Androidin historia

Android Inc perustettiin vuonna 2003 Palo Altossa, Kaliforniassa. Andy Rubin, Rich Miner, Chris White ja Nick Sears olivat yhtiön neljä perustajaa. Rubin kuvaili perustamisen alkuvaiheessa Android Inc:n kehittävän älykkäämpiä mobiililaitteita, joiden avulla ollaan paremmin tietoisia laitteen käyttäjän sijainnista ja käyttäjän omista mieltymyksistä. Alkuperäisen suunnitelman mukaan Android Inc:n oli tarkoitus ryhtyä kehittää edistyksellisiä digitaalikameroiden käyttöjärjestelmiä. Digitaalikameroiden markkinat olivat kuitenkin laskussa, joten yhtiö päätti keskittyä Androidin kehittämiseen nimenomaan mobiililaitteiden käyttöjärjestelmänä. (Callaham 2019.)

Androidin ensimmäinen älypuhelin julkaistiin vuonna 2008, T-Mobile G1 (Kuva 1), joka tunnetaan myös nimellä HTC Dream. Älypuhelinta ruvettiin myymään jo samana vuonna Yhdysvalloissa, ja puhelimessa oli jo tuolloin esimerkiksi 3,2 tuuman kosketusnäyttö sekä QWERTY-näppäimistö. Kyseinen laite sai myös huonoja arvosteluja, koska puhelimessa ei ollut ollenkaan 3,5mm:n kuulokeliitäntää. 3,5mm:n kuulokeliitäntä löytyy nykyään jokaisesta Android-laitteesta. (Callaham 2019.)

Kuva 1. T-Mobile G1 -älypuhelin (mobiili.fi 2018).

2.2 Androidin versiohistoria

Vuonna 2009 Android julkaisi ensimmäisen koodinimellä varustetun käyttöjärjestelmän, joka oli nimeltään Android Cupcake 1.5. Tästä alkoi perinne, jonka mukaan jokainen käyttöjärjestelmäpäivitys on nimellään viitannut makeisiin elintarvikkeisiin (Kuva 2). Android Cupcake toi kehyksen kolmansien osapuolien widgeteille, joka erotti käyttöjärjestelmän muista vastaavista. (Raphael 2020.)

Kuva 2. Android-käyttöjärjestelmäversiot Alphasta Nougatiin (Robinson 2016).

Android on julkaissut käyttöjärjestelmälleen lukuisia päivityksiä vuodesta 2009 aina tähän päivään saakka, koska sen pyrkimys on kehittää järjestelmäänsä jatkuvasti entistä käyttäjäystävällisemmäksi ja tehokkaammaksi. Uusin Android-versio on Android 10, joka toi mukanaan sen käyttäjälle jälleen lisää uusia ominaisuuksia. Android 10 -versiossa on esimerkiksi uusi ominaisuus, jonka avulla voi luoda QR-koodin omaan Wi-Fi -verkkoon. Toinen vaihtoehto on skannata QR-koodi ja laitteen Wi-Fi -asetuksista liittyä Wi-Fi -verkkoon (Cipriani 2020). Sovelluskehittäjille Androidin versioiden suuri lukumäärä asettaa selkeän haasteen, sillä sovellusten toimivuutta eri versioissa ei voida varmistaa.

2.3 Vahvuudet ja heikkoudet

Yksi Androidin vahvuuksista on sen päivitettävyys, koska laitteen käyttäjä saa suoraan aloitusnäytölleen ilmoituksena tiedon uusista päivityksistä laitteeseen asennetuille sovelluksille. Avoimeen lähdekoodiin perustuvat sovellukset ovat myös Androidin vahvuus. Google Play -sovelluskaupassa on suuri valikoima täysin ilmaisia sovelluksia, joista laitteen käyttäjä voi valita omiin tarpeisiinsa sopivimmat ja ladata ne nopeasti omaan Android-laitteeseensa. Android-käyttöjärjestelmällä varustettuja puhelimia löytyy myös monelta eri laitevalmistajalta, kuten esimerkiksi Samsung, Huawei ja Sony. Androidin pahimmalle kilpailijalle iOS:lle tämä on selkeä haaste, sillä iOS-käyttöjärjestelmällä varustetut laitteet rajoittuvat vain Appleen. Vahvuutena Androidille voidaan vielä todeta Google-palveluiden laaja valikoima, esimerkiksi pilvipalvelu Google Drive ja pilvipalvelu Gmail. (Bhasin 2019.)

Käyttöjärjestelmässä on myös merkittäviä heikkouksia, jotka ovat varmasti tulleet jokaiselle Android-käyttäjälle tutuiksi. Android-käyttöjärjestelmässä ei ole esimerkiksi Applen iTunesin kaltaista keskitettyä ohjelmistoa, josta Apple-laitteiden käyttäjä voi etsiä helposti musiikkia ja videoita. Androidin ilmaiset sovellukset tuovat mukanaan myös mainokset, jotka vähentävät olennaisesti laitteen käytön mukavuutta. Mainokset avautuvat yleensä käyttäjälle sovellusta käytettäessä laitteen ylä- tai alaosaan ja niitä ei yleensä käyttäjä voi sulkea mitenkään. Heikkoutena Androidille voidaan pitää myös internet-yhteyden suurta roolia laitteen monipuolisen käytön takaamiseksi. Iso osa Androidin sovelluksista vaatii jatkuvaa internetyhteyttä, eli käyttäjän ollessa internetyhteyksien ulkopuolella laitteen käyttö jää melko yksipuoliseksi. Aiemmin todettu käyttöjärjestelmän avoimuus voidaan nähdä sekä vahvuutena että heikkoutena. Avoimen lähdekoodin Android antaa nimittäin sovelluskehittäjille paljon mahdollisuuksia sovellusten kehitykseen, mutta myös lähdekoodin manipulointi on tämän vuoksi helppoa. Google Play -sovelluskauppaan voidaan esimerkiksi lisätä viruksen sisältävä sovellus, jonka lataamalla käyttäjän tietoturva on uhattuna. (Bhasin 2019.)

2.4 Käyttöliittymä ja ominaisuudet

Android antaa käyttäjälleen todella paljon mahdollisuuksia muokata käyttöliittymää ja omaa aloitusnäyttöä käyttäjän omien tarpeiden mukaisesti. Käyttöjärjestelmää hyödyntävässä laitteessa on jo oletuksena tiettyjä sovelluksia kuten esimerkiksi kello, selain, kamera ja galleria. Halutessaan käyttäjä voi kuitenkin ladata Google Play -sovelluskaupasta oletussovellusten tilalle vastaavia sovelluksia. Google-tilin luonti ja internet-yhteys ovat kuitenkin vaatimukset sovelluskaupan käytölle. Android-käyttäjän on myös mahdollista käyttää laitteessaan widgettejä. Ne ovat pienoisohjelmia, jotka näyttävät sovelluksen oleellisimman tiedon suoraan laitteen työpöydällä, eli widget pyörii taustalla eikä käyttäjän tarvitse edes avata kyseistä sovellusta.

Android on myös moniajoon kykenevä käyttöjärjestelmä, eli Android-laite pystyy ajamaan montaa sovellusta samanaikaisesti. Käyttäjällä voi olla esimerkiksi yksi sovellus avattuna laitteen näytölle ja samaan aikaan kolme muuta sovellusta jäävät auki taustalle. Tämä on yritysmaailmassa hyvä asia, sillä työntekijät voivat esimerkiksi käyttää monia yrityksen käytössä olevia sovelluksia samanaikaisesti Android-laitteilla, ilman sovellusten jatkuvaa uudelleenkäynnistämistä. Mikäli käynnissä olevia sovelluksia on samanaikaisesti liikaa, voi tietysti laite myös hieman tästä syystä hidastua tai ylikuumentua. Tämän vuoksi Android-laitteen käyttäjän on hyvä välillä sulkea tarpeettomat sovellukset taustalta, jotta ei suorituskyky heikkene.

Android-laitteissa on kosketusnäytöllinen käyttöliittymä, jossa on kuitenkin mahdollista käyttää myös normaalia hiirtä. Lähes aina Android-laitteita käytetään kuitenkin juuri kosketusnäyttöä hyödyntämällä. Androidissa on myös niin sanottu monikosketusominaisuus, joka mahdollistaa esimerkiksi näytölle avattujen kuvien zoomaamisen tekemällä näytöllä ”nipistysliikkeen”. Uusimmissa Android-versioissa tuetaan myös ominaisuutta, jossa laitteen käyttäjä liikuttaa sormeaan näytöllä eri kirjaimien välillä tekstin kirjoittamiseksi. Android arvaa tämän jälkeen, mitä sanaa käyttäjä tarkoittaa ja syöttää automaattisesti sanan käyttäjän viestikenttään. Tämä kirjoitustapa vaatii opettelua, mutta kokeneemmat käyttäjät osaavat kirjoittaa tämän ominaisuuden avulla jopa paremmin. (Karch 2019.)

3 MOBIILILAITTEIDEN HALLINNAN TYÖKALUT

Mobiililaitteiden hallintaan on kehitetty erilaisia työkaluja, joiden avulla pystytään tehostamaan yrityksen mobiililaitehallintaa erityisesti jollakin tietyllä osa-alueella. Nämä työkalut jaetaan mobiililaitteiden hallintaan, mobiilisovellusten hallintaan, yhtenäiseen päätepisteiden hallintaan sekä liikkuvuuden hallintaan. Edellä mainituista työkaluista yrityksen on tärkeää ottaa käyttöönsä se, joka soveltuu parhaiten yrityksen toimintastrategiaan. Mikäli yrityksessä lähdetään käyttämään väärää työkalua mobiililaitteiden hallintaan, se voi vaikuttaa yrityksen liiketoimintaan tappiollisesti. Yrityksen on siis tärkeää ymmärtää näiden työkalujen erot, jotta valinta ei ole omalle yritykselle epäedullinen.

3.1 Mobile Device Management (MDM)

Mobile Device Management on keskitetyn hallinnan työkalu, jolla tarkoitetaan mobiililaitteiden hallintaa. MDM antaa yrityksen IT-osastolle mahdollisuuden työntekijän tai yrityksen omistaman mobiililaitteen hallitsemiseen, suojaamiseen ja seuraamiseen. Tyypillistä on, että jokaisella laitteella ja työntekijällä on oma ”profiilinsa”, joka on määritetty työntekijän osaamisalueeseen soveltuvaksi. MDM-mallissa yritys voi määrittää esimerkiksi Wi-Fi -yhteyden, sekä hallita ja asentaa yrityssovelluksia etänä laitteeseen. Varastettu tai kadonnut laite voidaan myös MDM-ratkaisussa IT-osaston toimesta lukita tai tyhjentää, mikä on erittäin hyvä asia tietoturvan näkökulmasta. (Tess 2018.)

Tällä hetkellä on olemassa kaksi tapaa, jolla yritykset voivat hallita mobiililaitteitaan. Työntekijälle voidaan antaa yrityksen omistama mobiililaite, tai vaihtoehtoisesti työntekijä voi käyttää BYOD-mallia. BYOD on lyhennetty sanoista ”Bring your own device”. BYOD-ratkaisua käyttämällä yrityksen työntekijä voi käyttää omaa älypuhelintaan yrityksen työtehtävissä hyödykseen. BYOD ei ole pienissä ja keskisuurissa yrityksissä uusi asia, koska sitä on hyödynnetty yritysten liiketoiminnassa jo vuodesta 2004 alkaen. BYOD-mallin käyttö lisääntyy jatkuvasti, ja sen hyödyntäminen on kasvanut merkittävästi vuosi vuodelta. Yritysten omat laitteet ovat myös monilla käytössä, koska osa käyttäjistä ei halua yrityksen hallinnoimia MDM-ohjelmistoja omiin

laitteisiinsa. Nämä käyttäjät ovat pelänneet, että yritykset pääsisivät käsiksi arkaluontoiseen dataan, kuten esimerkiksi valokuviin ja viesteihin. (Shiong 2019.)

3.2 Mobile Application Management (MAM)

Mobile Application Management tarkoittaa mobiilisovellusten hallintaa. Tällä menetelmällä yritys hallitsee yrityssovelluksia ja niihin liittyviä tietoja, joten itse laitteita ei hallinnoida yrityksen toimesta tässä mallissa. MAM-ratkaisua käyttämällä yrityksen on mahdollista hallita yrityksen sovelluksiin pääsyä, sekä sovellusten sisältöjä ilman itse fyysisen laitteen hallintaa. MAM-ratkaisun vahvuus on myös se, että sovelluksia voidaan päivittää etänä. Uudet korjauspäivitykset saadaan jaettua mobiililaitteisiin etänä hyvin nopeasti, joka on tietysti tietoturvauhkien aikana merkittävä etu. MAM-mallista yksi esimerkki on yrityksen sähköposti, joka on MAM:n yleisin muoto. Liittämisen ja kopioinnin tapaisia ominaisuuksia voidaan tarpeen mukaan yrityksen toimesta rajoittaa. Tällä menettelyllä voidaan turvata se, etteivät työntekijät jaa yritystietoja hyväksymättömiin sovelluksiin. (Mearian 2017.)

3.3 Enterprise Mobility Management (EMM)

Enterprise Mobility Management tarkoittaa joukkoa palveluita sekä tekniikoita, joiden avulla yritystiedot turvataan työntekijöiden mobiililaitteissa. Yrityksellä voi olla EMM-mallissa erilaisia tapoja toteuttaa näiden palveluiden ja tekniikoiden käyttöönotto, mutta tyypillistä on perustaa tietyt mobiilihallintajärjestelmät ja
-palvelut suojaamaan immateriaalioikeuksia. Kunkin yrityksen tulee määrittää sellainen EMM-järjestelmä, joka soveltuu parhaiten omaan liiketoimintaan. Osa yrityksistä keskittyy esimerkiksi vain tiettyjen sovellusten suojaamiseen, kun taas toisissa yrityksissä voidaan keskittyä vain dataan ja sen suojaamiseen. EMM-mallin työkalujen avulla yritykset uskovat antavansa työntekijöilleen enemmän mahdollisuuksia mobiililaitteiden hallintaan. (Kapko 2017.)

3.4 Unified Endpoint Management (UEM)

UEM (Unified Endpoint Management) -termillä tarkoitetaan yhtenäistä päätepisteiden hallintaa. Esimerkiksi MDM- ja EMM-malleissa on paljon rajatummat keinot mobiililaitteiden hallintaan kuin UEM-mallissa. Kun laitteiden hallintaa pitää tehostaa koko ajan muuttuvassa mobiiliympäristössä, tarvitaan koko ajan edistyneempiä ominaisuuksia. UEM tuo mukanaan hallinnalle uusia tärkeitä ominaisuuksia edellä mainittujen hallintatyökalujen rinnalle. UEM kykenee esimerkiksi mobiililaitteiden hallintaan, mobiilisovellusten hallintaan, tietoturvauhkien hallintaan, sisällön hallintaan ja käyttöoikeuksien hallintaan. Tämä mobiilihallinnan työkalu siis takaa todella laajat ominaisuudet IT-osastolle laitteiden hallitsemiseksi. (Cheuvront 2018.)

IT-osastolla vähenee myös alkumäärittelyt ja työtunnit UEM:n käytön myötä. Käyttäjät ja heidän mobiililaitteensa voidaan nimittäin rekisteröidä suoraan UEM-ratkaisuun, mikä ei yleensä vaadi yrityksen IT-osastolta toimia. Itse asennusprosessi on myös yksinkertainen, sillä UEM tukee ilmoittautumisohjelmia, kuten esimerkiksi Googlen Android Zero-touch -ratkaisu ja Applen laitteiden rekisteröintiohjelma DEP. (Cheuvront 2018.)

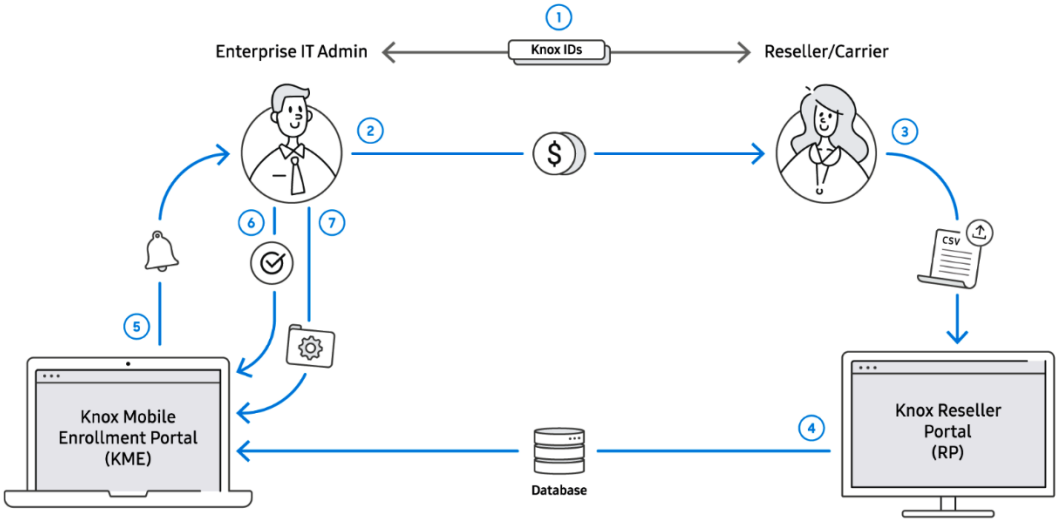
UEM-ratkaisu on helppo myös siksi, että se integroituu olemassa olevaan infrastruktuuriin, kuten esimerkiksi Microsoft Active Directory ja Lightweight Directory Access Protocol (LDAP). IT-osaston aikaa ja kustannuksia saadaan näin ollen säästettyä tuomalla AD- ja LDAP-tietueet suoraan itse UEM-ratkaisuun ilman tarvetta rakentaa tietueita alusta lähtien uudelleen. (Cheuvront 2018.)

4 AUTOMATISOITU ANDROID-LAITTEIDEN REKISTERÖINTI

Android-laitteille on olemassa kaksi ratkaisua automatisoidulle laitteiden rekisteröinnille. Nämä kaksi automatisoitua ratkaisua ovat Knox Mobile Enrollment ja Zero-touch Enrollment, joiden avulla saadaan automatisoidusti rekisteröityä uudet Android-laitteet yrityksessä mobiililaitehallintaan. Nämä laiterekisteröintimenetelmät säästävät aikaa uusien Android-laitteiden alkumäärittelyssä ja käyttöönotossa. Näiden hallintamenetelmien avulla saadaan siis täysin automatisoidusti uudet Android-laitteet yrityksen hallintaan, mikä helpottaa suurien laitemäärien käyttöönottoa huomattavasti.

4.1 Samsung Knox Mobile Enrollment

Samsungin Knox Mobile Enrollment on Samsungin mobiililaitteiden rekisteröintiin tarkoitettu käyttöönottopalvelu. Sen avulla yritys voi rekisteröidä suuren määrän uusia mobiililaitteita helposti ja nopeasti täysin automatisoidulla tavalla. Knox Mobile Enrollment -ratkaisussa laitteiden jälleenmyyjät tekevät tiivistä yhteistyötä yrityksen kanssa, jotta laitteiden asennukset saadaan yksinkertaistettua. Kun KME halutaan ottaa yrityksessä käyttöön, perustetaan yritystili KME:n palveluun ja sen jälkeen valtuutetaan Samsung-jälleenmyyjä lisäämään laitteet Knox Mobile Enrollmentin ympäristöön (Kuvio 1). Samsung-laitteiden jälleenmyyjät lataavat laitteiden sarjanumerot KME:n portaaliin ja yhdistävät tiedot palvelun käyttöönottavaan yritykseen. Tämän jälkeen yrityksen IT-osasto voi aktivoida laitteet käyttöön KME-portaalissa. Knox Mobile Enrollment -käyttöönottopalvelun avulla jo laitteen ensimmäinen käynnistys riittää siihen, että yhteys muodostetaan Samsungin KME-palvelimelle lähettämällä laitteen sarjanumero palvelimelle. Tämä vaatii toki sen, että laitteella on internet-yhteys käytettävissä. Mikäli sarjanumero tunnistetaan palvelua käyttöönottavan yrityksen laitteeksi, Samsungin mobiililaitteiden rekisteröintiprosessi alkaa välittömästi. (Samsung for Business 2019.)



Kuvio 1. Knox Mobile Enrollment -käyttööottoprosessin vaiheet (Samsung Knox 2019).

4.2 Zero-touch Enrollment

Toinen automatisoitu laitteiden rekisteröintiä helpottava palvelu on Zero-touch Enrollment. Tämänkin käyttöönottopalvelun avulla vältetään laitteiden manuaaliset määritykset, jotka veisivät IT-osastolta paljon aikaa ja resursseja. Zero-touch Enrollment toimii myös niin, että laitteet voidaan keskitetysti rekisteröidä ja ottaa käyttöön, kun Android-laitteeseen on kytketty virta ja se on yhdistetty verkkoon. Näin ollen väärien asetusmäärityksien riski pienenee, kun rekisteröinti tehdään automatisoidusti manuaalisen määrityksen sijaan. ZTE:n avulla myös luvattomien ja tuntemattomien laitteiden liittyminen yrityksen omaan keskitetyn hallinnan ympäristöön voidaan estää. Tämä on tietysti tietoturvan kannalta merkittävä asia, jotta mobiililaitehallinnan ympäristöön kuulumattomat laitteet saadaan pidettyä poissa. (Hexnode 2020.)

Zero-touchin käytölle on tiettyjä edellytyksiä, jotka yrityksen tulee ottaa huomioon ennen palvelun käyttöönottoa. Yrityksen on hankittava laitteet palvelun käyttöä varten Zero-touch -jälleenmyyjiltä tai Google-kumppanilta. Tämän vuoksi normaaleille kuluttajille tarkoitetuista kaupoista ei esimerkiksi voi laitteita hankkia. ZTE:n käyttöä varten käyttöönotettavissa Android-laitteissa tulee myös olla Android Oreo, tai sitä uudempi Android-käyttöjärjestelmän versio. Poikkeuksena Zero-touchia voidaan käyttää myös Pixel-puhelimissa, joissa on Android Nougat -käyttöjärjestelmäversio.

Lisäksi yrityksen tulee varmistaa ennen laitteiden hankintaa, että valitut laitemallit löytyvät Android Zero-touch -laitteiden listasta. Listaan on koottu palvelun käytölle tuetut mallit. Ohjeistuksena Zero-touchissa on myös se, että mobiililaitteessa tulee käyttää yrityksen omaa tiliä tai sähköpostiosoitetta. Esimerkiksi henkilökohtaisia Gmail-tilejä ei siis tule tähän tarkoitukseen käyttää. (Hexnode 2020.)

5 MOBIILILAITEHALLINNAN SUUNNITTELU YRITYKSESSÄ

IT-osaston tulee mobiililaitteiden käyttöönotossa suunnitella aluksi tarkasti, mitkä ovat yritykselle sopivimmat laitteiden hallintatavat ja ohjelmistot. Aluksi tulee siis pohtia, mihin mobiililaitteiden käyttöönotolla yrityksessä pyritään ja mihin osa-alueisiin keskitetään esimerkiksi eniten resursseja. Tietoturva on monelle yritykselle yksi ykkösprioriteetti mobiililaitehallinnan ratkaisuja suunniteltaessa, joten siihen tulee kiinnittää heti alusta alkaen erityistä huomiota.

Tälle työlle ei ollut erillistä tilaajaa, joten mobiililaitehallinnan suunnittelussa käytetään esimerkkiä, jonka mukaisesti yritys voisi edetä. Tässä osassa työtä käydään siis läpi vaiheet, jotka yrityksen tulee suunnitella ennen itse mobiililaitteiden käyttöönottoa. Lisäksi tarkastellaan kolmea mobiililaitteiden hallintajärjestelmää tarkemmin, joista valitaan yksi yrityksen käyttöön.

5.1 Mobiililaitehallinnan suunnittelussa huomioitavat asiat

Tärkeänä lähtökohtana mobiililaitteiden käyttöönotossa ja sen suunnittelussa voidaan pitää tietoturvaa. Kun suuri määrä uusia mobiililaitteita otetaan yrityksessä käyttöön, tietoturvariskit tulee ottaa heti alussa riittävään huomioon. Varmasti jokainen mobiililaitteiden hallintajärjestelmä nykyään on luotu mahdollisimman kattavan tietoturvan piiriin, mutta tietoturvan merkitystä ei voi koskaan korostaa liikaa. Esimerkiksi Android-laitteista löydetään jatkuvasti uusia tietoturva-aukkoja, joihin hakkerit voivat huonon tietoturvan vallitessa iskeä nopeastikin. Mobiililaitteet saattavat joutua helposti vääriin käsiin myös esimerkiksi katoamisen tai varkauden kautta. Esimerkiksi tavallisten työasemien kohdalla varkaustilastot ovat luonnollisesti paljon matalampia kuin mobiililaitteiden kohdalla.

Mobiililaitteiden käyttöönotossa on kiinnitettävä huomio siihen, miten tietoliikenneyhteyksien turvallisuus varmistetaan. Mikäli palomuurin asetukset ja tietoliikenneyhteydet eivät ole tarkkaan määriteltyjä, syntyy suuri riski yrityksen arkaluontoisten tietojen vuotamiselle. Tämän vuoksi yrityksen tulee ottaa VPN (Virtual Private Net-

work) käyttöön viimeistään tässä vaiheessa, kun mobiililaitteita ollaan ottamassa työntekijöiden käyttöön. VPN-yhteyden avulla työntekijät pääsevät yrityksen omaan verkkoon turvallisesti esimerkiksi työskennellessään etänä kotoa käsin. Dataliikenne saadaan salattua VPN-yhteydellä, jotta esimerkiksi yrityksen dataa tai yrityksen omistamien mobiililaitteiden sijaintitietoja ei joudu vääriin käsiin.

Suunnitteluvaiheessa ennen itse laitteiden käyttöönottoa tulee tarkasti kirjata ylös kaikki käyttöönotettavat mobiililaitteet ja niiden lukumäärä. Yritys voi esimerkiksi yksilöidä jokaisen uuden mobiililaitteen omalla tunnisteella. Nämä tunnistenumerot voidaan syöttää yrityksen omaan tietojärjestelmään, jonka kautta jokainen laite löydetään esimerkiksi häiriö- tai katoamistilanteissa nopeasti. Uusiin mobiililaitteisiin voidaan myös esimerkiksi tarralla vielä kiinnittää laitteen tunnistenumero, jotta itse työntekijäkin tietää käytössä olevan laitteensa tunnisteen heti kysyttäessä. Mobiililaitteiden hallinta voidaan ulkoistaa yrityksestä kokonaan ulkopuoliselle toimittajalle, mutta silti yrityksellä itselläänkin on hyvä olla kirjattuna kaikkien omistamiensa laitteiden lukumäärä ja tunnistetiedot omaan järjestelmäänsä.

Kun yritys laajentaa toimintaansa mobiiliympäristöön, tulee tehdä tutkimusta markkinoilla olevista mobiililaitehallinnan ratkaisuista. Yrityksen tuottavuuden maksimoimiseksi on tärkeää löytää yrityksen vaatimuksiin parhaiten sopiva ratkaisu. Mobiililaitehallinnan ratkaisuja on jo nykyään tarjolla paljon, mutta pääpiirteet ratkaisuissa ovat melko samanlaisia ja ne eroavat hyvin vähän toisistaan.

5.2 Mobiililaitehallintaratkaisujen vertailuun valittavat järjestelmät

Mobiililaitteiden hallintaan kehitetyistä järjestelmistä tarkempaan tarkasteluun valikoitui MobileIron, Miradore ja SOTI MobiControl. Nämä kaikki kolme järjestelmää voidaan ottaa käyttöön Android-käyttöjärjestelmän piirissä oleviin laitteisiin. Työssä valittiin kyseiset järjestelmät juuri siksi, että tämä opinnäytetyö keskittyy pelkästään Android-laitteisiin. Edellä mainitut kolme hallintajärjestelmää ovat myös yleisesti tunnettuja, eli näistä ratkaisuista löytyy hyvin tietoa niiden tarkastelua varten. Tälle opinnäytetyölle ei ole erillistä tilaajaa, joka määrittäisi tietyt vaatimukset ja tarvittavat omi-

naisuudet mobiililaitehallintaan valikoitavalle järjestelmälle. Tästä syystä työssä käydään läpi näiden kolmen valikoidun järjestelmän ominaisuuksia ja valitaan näistä vertailun jälkeen omien näkemysten mukaisesti parhaaksi todettu järjestelmä yrityskäyttöön.

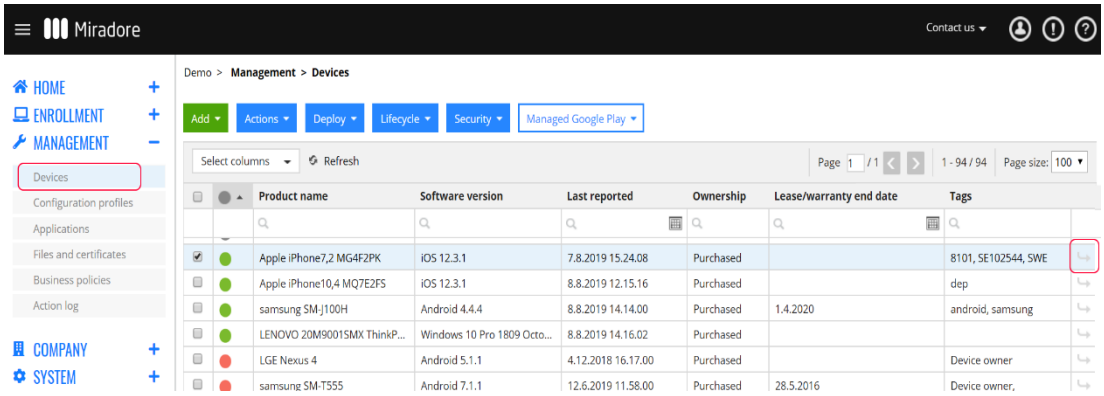
5.2.1 MobileIron

MobileIronilla on merkittävä asema mobiililaitteiden hallintajärjestelmänä, sillä maailman suurimmat yrityksetkin luottavat MobileIroniin perustana omalla yritystoiminnalleen. Kyseessä on kattava liikkuvuuden hallintaratkaisu, jolla voidaan hallita mobiilisovelluksia, sisältöä sekä laitteen hallintaominaisuuksia. MobileIronilla on kuukausittain jopa kaksi miljardia aktiivista laitetta, jotka hyödyntävät tätä hallintaratkaisua. MobileIronin avulla yrityksessä voidaan ottaa käyttöön Android-laitteet ja sovellukset turvallisesti, vaikka laitteita olisi suurikin määrä. Vaikka laitemäärät kasvavat, niin käyttöönotto pystytään pitämään silti riittävän turvallisella tasolla. Hallintajärjestelmän avulla voidaan myös pitää yrityksen data ja yrityksen työntekijän henkilökohtainen data erillään toisistaan, mikäli työntekijällä on käytössään oma laite. MobileIronin haasteena on se, että mobiililaitteiden hallinta pitäisi pystyä turvaamaan kaikille laitteille riittävällä tasolla, vaikka laitteita olisi useilta eri valmistajilta. Yrityksen omistamien laitteiden ja käyttäjien omien laitteiden käyttöönotossa on myös oma haasteensa, sillä molemmissa tapauksissa tietoturva pitää pystyä pitämään tarvittavalla tasolla. (Mobileiron 2015.)

5.2.2 Miradore

Miradore on perustettu vuonna 2006. Yli 10 000 yritystä yli 180 maassa käyttää ohjelmistoa, joten sitä voidaan pitää suosittuna hallintaratkaisujen tarjoajana. Miradore on suomalainen ohjelmistoyritys, joka tarjoaa tehokkaita pilvipohjaisia laitehallintaratkaisuja mobiililaitteille ja työasemille. Android-, iOS, macOS- ja Windows-laitteet ovat tuettuja Miradoren hallintaratkaisun käyttöä varten. Laitteiden hallintaan käytettävää käyttöliittymää käytetään internet-selaimen kautta, josta nähdään esimerkiksi käytössä olevat laitteet ja niiden käyttöjärjestelmät listattuna (Kuva 3). Miradoren

avulla organisaatiot pystyvät hallitsemaan ja suojaamaan käytössä olevia laitteita tehokkaammin. Hallintaratkaisun avulla on helppo hallita esimerkiksi älypuhelimia ja tabletteja, koska siinä on juuri oikeat ominaisuudet tehokasta laitteiden hallintaa varten. Miradoren avulla yrityksen kaikki luottamukselliset tiedot voidaan salata, ottaa käyttöön tietoturvan kannalta turvalliset salasanat ja estää tiettyjen sovellusten käyttö kokonaan. Myös automatisointiominaisuuksien avulla tehostetaan laitteiden käyttöönottoa huomattavasti, sillä laitteiden rekisteröinti ja alkumäärittelyjen tekoon kuluva aika saadaan tämän avulla minimoitua. (Miradore 2020a.)



Kuva 3. Miradoren näkymä käytössä olevista laitteista (Miradore 2020b).

5.2.3 SOTI MobiControl

Kolmas vertailtava mobiililaitteiden hallintajärjestelmä on SOTI MobiControl, joka on myös yksi vaihtoehto yritykselle Android-laitteiden hallinnan toteuttamiseksi. Järjestelmän avulla saadaan mobiililaitteiden hallinta yksinkertaistettua helpon käyttöliittymän kautta. SOTI:n ansiosta jokainen laite määritellään automatisoidusti tietyillä tiliasetuksilla, tarvittavilla sovelluksilla ja VPN-asetuksilla. Yrityksen arkaluontoinen data pysyy näin ollen yhtä turvattuna kuin yrityksen toimistoissa sijaitsevat työasematkin. SOTI:n ratkaisun avulla IT-osaston on myös vaivatonta diagnosoida ja ratkaista ongelmia palveluntarjoajan kanssa, koska sen etätukitoiminnot ovat alan parhaimmistoa. Laitteiden tarkastelu ja hallinta on tehty helpoksi etäältä käsin, minkä vuoksi sovellus- ja laiteongelmat pystytään ratkomaan nopealla aikataululla. (Honeywell 2020.)

SOTI Hub on turvallinen sovellus, jolla pystytään hallitsemaan yrityksen käytössä olevaa dataa. Sovelluksen avulla yrityksen on helppoa hallita sen asiakirjoja ja tiedostoja, jotka halutaan pitää turvassa. SOTI:n hallintajärjestelmässä on myös toinen merkittävä lisäominaisuus, joka on turvallinen mobiiliselain SOTI Surf. Tähän mobiiliselaimeen on määritetty ennalta tietyt ominaisuudet ja suojausasetukset yrityksen tarpeen mukaisesti. Tällä tavoin huomioidaan yrityksen oman liiketoiminnan kannalta keskeisimmät asiat ja myös loppukäyttäjien vaatimukset tulevat huomioiduksi entistä paremmin. SOTI:n hallintajärjestelmää ja sen ominaisuuksia hyödyntämällä yritys voi varmistua siitä, että yrityksen omalle liiketoiminnalle tärkeimmät asiat tulevat huomioiduksi. (Honeywell 2020.)

5.3 Hallintaratkaisun valinta

Käytettäväksi Android-laitteiden hallintaratkaisuksi valikoitui Miradore, koska sen käyttöliittymä ja hallittavuus vaikuttivat sopivimmilta yritysmaailmaan käytettäväksi. Nämä ovat tärkeitä asioita yrityksen liiketoiminnassa, koska tällöin uuden hallintajärjestelmän toimintoihin ja ominaisuuksiin perehtymiseen käytetty aika saadaan minimoitua. Miradore tarjoaa hallintaratkaisulleen neljä erilaista lisenssimallia, jotka tietysti eroavat ominaisuuksiltaan hieman toisistaan. Nämä Miradoren tarjoamat mallit ovat Free, Business, Enterprise ja Enterprise Plus. Näihin malleihin tutustuessa tultiin siihen tulokseen, että yritykselle sopiva suunnitelma olisi käyttää Enterprise-lisenssiä. Enteprise-version hinta on 2 euroa yhdeltä hallittavalta laitteelta kuukaudessa. Tätä hintaa voidaan pitää kohtuullisena, koska Miradoren käyttö helpottaa yrityksen Android-laitteiden laitehallinnassa huomattavasti yrityksen IT-osastoa.

Hallintajärjestelmän käyttöönottavalla yrityksellä tulee olla valmiina suunnitelma siitä, ketkä ottavat vastuun Miradoren hallinnasta. Eli nimetään esimerkiksi tietyt henkilöt, jotka vastaavat Miradoren kautta laitteiden hallinnasta, kun järjestelmä otetaan käyttöön. Tämä tietysti vaatii näiden henkilöiden kouluttamisen, mutta se on varmasti pitkällä aikavälillä yrityksen tehokkuutta lisäävä toimintatapa. Hallintajärjestelmän ylläpitoon valittuja henkilöitä tulee myös olla riittävästi, jotta esimerkiksi sairastapausten aikana toiminta saadaan turvattua. Tämän ratkaisun ansiosta muiden yrityksen työntekijöiden ei tarvitse keskittyä itse mobiililaitehallintaan, vaan he voivat keskittyä

itse laitteiden käyttöön ja sitä kautta olla tuottavia yrityksen liiketoiminnan näkökulmasta. Koko yrityksen henkilöstö on kuitenkin hyvä kouluttaa uuden käyttöönotettavan mobiililaitehallintajärjestelmän peruskäyttöä varten, mutta kaikkien ei tarvitse osata hallintajärjestelmän monipuolista käyttöä.

5.4 Tietoturva

Yrityksen on muistettava Android-laitteita käyttöön otettaessa myös tietoturvan merkitys. Toki jo aiemmin yritykselle valitun Miradoren myötä tietoturva saadaan pidettyä turvattuna, mutta tietyt asiat tulee suunnitella valmiiksi. Esimerkiksi yrityksessä työskentelevien käyttäjien omat laitteet (BYOD-malli) pitää ottaa tarkempaan tarkasteluun, sillä ne eivät tietosuojakäytäntöjen vuoksi ole täysin yrityksen hallinnassa. Yrityksen on suunniteltava valmiiksi esimerkiksi laitteen katoamisen tai varkauden sattuessa toimintatapa tällaiseen tilanteeseen. Suunnitteluvaiheessa on siis tärkeää pohtia, voidaanko esimerkiksi käyttäjän oma laite tyhjentää yrityksen toimesta laitteen katoamistilanteessa. Tilanne on hankala, sillä laitteen täysi tyhjennys merkitsisi tietysti sitä, että käyttäjä menettäisi myös kaiken henkilökohtaisen datansa. Tällaiset tilanteet tulee etukäteen ottaa huomioon, jotta toimintatapa on tiedossa varkauden tai laitteen katoamisen hetkellä.

Tietoturvaa tarkasteltaessa yrityksen on myös syytä hankkia riittävän uudet Android-laitteet, jotta tietoturvapäivitykset ovat varmasti saatavilla tulevaisuudessakin. Esimerkiksi vanhemmissa Android-laitteissa on käyttöjärjestelmäversioita, jotka eivät enää ole uusimpien tietoturvapäivitysten tukemia. Myös laitevalmistajan valintaan on kiinnitettävä huomiota, sillä valmistajienkin kesken laitteiden päivitettävyys vaihtelee. Esimerkiksi Googlen ja Samsungin Android-laitteet ovat hyviä vaihtoehtoja yritykselle, koska ne jakavat tietoturvapäivityksiä laitevalmistajista parhaiten. Google jakaa tietoturvapäivitykset laitteilleen käytännössä saman tien, kun uusi tietoturvapäivitys on saatavilla.

6 YHTEENVETO

Tämän opinnäytetyön tarkoituksena oli tutkia mobiililaitteiden keskitettyä hallintaa Androidille. Työssä käytiin läpi Androidin käyttöjärjestelmää aluksi yleisellä tasolla esimerkiksi historiaa ja Androidin ominaisuuksia tarkastelemalla. Aluksi katsottiin myös, mitä vahvuuksia ja heikkouksia käyttöjärjestelmästä löytyy. Käyttöjärjestelmän esittelyn ja pääpiirteiden tarkastelun jälkeen työssä tarkasteltiin keskitetylle mobiililaitehallinnalle tarjolla olevia työkaluja ja ratkaisuja, joita yritysmaailmassa voidaan ottaa käyttöön. Opinnäytetyössä keskityttiin ainoastaan Android-laitteisiin ja tutkittiin asioita, jotka yrityksen tulee ottaa huomioon, ennen Android-laitteiden käyttöönottoa. Työlle ei ollut erillistä tilaajaa, mutta työssä luotiin suunnitelma, jonka mukaisesti yritys voisi edetä ennen mobiililaitteiden käyttöönottoa. Valittiin myös esimerkkiyritykselle hallintajärjestelmien vertailun jälkeen Miradoren tarjoama mobiililaitehallinnan ratkaisu käyttöön.

Työn aikana mobiililaitehallintaa tutkimalla huomattiin, että yrityksen ottaessa Android-laitteita käyttöönsä on tärkeää suunnitella pienetkin yksityiskohdat riittävän tarkasti. Hyvällä suunnitelmalla itse Android-laitteiden käyttöönotto saadaan varmasti yrityksessä toteutettua nopeammin ja vältytään epäselvyyksiltä käyttöönottovaiheessa. Yritykselle laaditussa suunnitelmassa katsottiin myös tärkeäksi se, että tietty ryhmä/tiimi yrityksen henkilöstön joukosta nimetään vastaamaan käyttöönotettavien Android-laitteiden hallinnasta. Opinnäytetyössä katsottiin tämä toimintamalli sellaiseksi, joka olisi yrityksen toiminnan kannalta tehokkain ratkaisu. Käytiin myös läpi tietoturvan merkitys mobiililaitehallintaa suunniteltaessa. Tietoturvan merkitystä ei voida varsinkaan yrityksen näkökulmasta ikinä korostaa liikaa, sillä arkaluontoisen datan joutuminen väärille tahoille pitää pystyä estämään joka tilanteessa.

Yrityksen tulisi aina varata riittävästi aikaa ja resursseja sille, että uusien käyttöönotettavien mobiililaitteiden hallintaan on perehdytty mahdollisimman tarkasti. Suunnittelemalla työmenetelmät ja käytettävät järjestelmät valmiiksi säästetään varmasti työtunteja laitteiden käyttöönoton jälkeen. Hyvällä suunnittelulla ja mobiililaitehallinnan ratkaisuja hyödyntämällä myös mobiililaitehallinnasta saadaan enemmän hyötyjä irti.

LÄHTEET

Bhasin, H. 2019. SWOT analysis of Android – Android SWOT Analysis. Viitattu 6.4.2020. https://www.marketing91.com/android-swot-analysis/

Callaham, J. 2019. The history of Android OS: its name, origin and more. Viitattu 22.3.2020. https://www.androidauthority.com/history-android-os-name-789433/

Cheuvront, D. 2018. Why UEM Is the New MDM: The Latest Stage in Enterprise Evolution. Viitattu 12.4.2020. https://securityintelligence.com/why-uem-is-the-new-mdm-the-latest-stage-in-enterprise-evolution/

Cipriani, J. 2020. The best Android 10 features you should be using today. Viitattu 1.4.2020. https://www.cnet.com/how-to/the-best-android-10-features-you-should-be-using-today/

Hexnode. 2020. What is Zero Touch Enrollment? Viitattu 22.5.2020. https://www.hexnode.com/mobile-device-management/help/zero-touch-enrollment/

Honeywell. 2020. SOTI MobiControl, Viitattu 22.5.2020. https://www.honeywellaidc.com/products/software/device-management/soti-mobicontrol

Kapko, M. 2017. What is EMM? Enterprise Mobility Management explained. Viitattu 11.4.2020. https://www.computerworld.com/article/3230510/what-is-enterprise-mobility-management-emm.html

Karch, M. 2019. What Is Android? Viitattu 12.5.2020. https://www.lifewire.com/what-is-google-android-1616887

Mearian, L. 2017. What's the difference between MDM, MAM, EMM and UEM? Viitattu 10.4.2020. https://www.computerworld.com/article/3206325/whats-the-difference-between-mdm-mam-emm-and-uem.html

Miradore. 2020a. About Miradore. https://www.miradore.com/about-us/

Miradore. 2020b. Device Inventory Data. https://onlinesupport.miradore.com/hc/en-us/articles/200875261-Device-inventory-data

Mobiili. 2018. Android täytti 10 vuotta - käyttöjärjestelmä osa valtavaa muutosta mobiilialalla. Viitattu 22.3.2020. https://mobiili.fi/2018/09/24/android-taytti-10-vuotta-kayttojarjestelma-osa-valtavaa-muutosta-mobiilialalla/

Mobileiron. 2015. MobileIron for Android. Viitattu 18.5.2020. https://www.mobileiron.com/sites/default/files/Datasheets/Android%20Datasheet/mobileiron-android_v2.0_EN-US.pdf

Raphael, J. 2020. Android versions: A living history from 1.0 to 11. Viitattu 1.4.2020. https://www.computerworld.com/article/3235946/android/android-versions-a-living-history-from-1-0-to-today.html

Robinson, D. 2016. Android Nougat Release Date Set for this August, No Love for Nexus 5 Users. Viitattu 1.4.2020. https://www.nashvillechatterclass.com/android-nougat-release-date-set-august-no-love-nexus-5-users/10761/

Samsung for Business. 2019. What is Knox Mobile Enrollment? Viitattu 5.5.2020. https://insights.samsung.com/2019/02/19/what-is-knox-mobile-enrollment/

Samsung Knox. 2019. Knox Mobile Enrollment. Viitattu 23.5.2020. https://docs.samsungknox.com/admin/knox-mobile-enrollment/welcome.htm

Shiong, A. 2019. As user privacy and MDM become more incompatible – the new guide to BYOD vs company devices. Viitattu 10.4.2020. https://enterprise-cio.com/news/2019/oct/29/user-privacy-and-mdm-become-more-incompatible-new-guide-byod-vs-company-devices/

Tess, H. 2018. Understanding the Difference between MDM, MAM, EMM and UEM. Viitattu 10.4.2020. https://solutionsreview.com/mobile-device-management/understanding-the-difference-between-mdm-mam-emm-and-uem/