YRITYKSEN SISÄINEN MOBIILISTRATEGIA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, syksy 2016

Johan Fabricius

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Visamäki
Tietojenkäsittely

Tekijä Johan Fabricius **Vuosi** 2016

Työn nimi Yrityksen sisäinen mobiilistrategia

TIIVISTELMÄ

Työskenteleminen on muuttumassa yhä enemmän ja enemmän paikasta, ajasta ja laitteista riippumattomampaan suuntaa. Näihin tarpeisiin vastaaminen on monessa yrityksessä IT:n vastuulla ja siihen liittyy myös riskejä. Mahdollisimman aikaisessa vaiheessa tulisi rakentaa joustava ja ketterä mobiilistrategia, jolla näihin haasteisiin pysytään vastaamaan ja riskejä vähintäänkin pienentämään. Tämän opinnäytetyön tarkoituksena olikin luoda mobiilistrategia, sekä pohja, jonka avulla mobiilistrategiaa voi lähteä työstämään omaan yritykseen.

Opinnäytetyö toteutettiin kehitysprojektina, jonka tuotoksena saadaan tietoa nykytilasta, suuntaviivat sille mihin pyritään sekä mobiilistrategia, jota aletaan jalkauttaa. Teoriapohjan kasaamisessa käytettiin hyväksi monenlaista IT-alan sekä strategiakirjallisuutta ja erilaisia internetlähteitä. Tekijällä on myös pitkä työkokemus IT-alalta järjestelmäkehityksen, prosessienkehityksen sekä erilaisten laitehallintajärjestelmien parista.

Kehitysprojektin aikana selväksi kävi, että kehitettävää on jokaisella osa-alueella. Tämän opinnäytetyön tuotokset ovat vasta ensimmäiset hapuilevat askeleet kohti paremmin toimivaa mobiilia ympäristöä. Kaikkia niitä ongelmia, jotka projektin aikana havaittiin, ei pystytä korjaamaan heti. Näiden ongelmien korjaamiseksi on todennäköisesti käynnistettävä uusia kehitysprojekteja, joiden avulla saadaan muutoksia aikaiseksi.

Avainsanat Strategia, mobiliteetti, mobiililaitteiden hallinta, mobiiliapplikaatioiden hallinta, IT-riskienhallinta.

Sivut 28 s. + liitteet 3 s.

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Visamäki
Degree Programme in Business Information Technology

Author Johan Fabricius **Year** 2016

Subject of Bachelor's thesis Company's internal mobile strategy

ABSTRACT

Working is getting more and more free from chains that lock us to some place, time or device. This creates demands and IT-risks that IT-departments need to take care of. There should be a mobile strategy in place as early as possible to tackle these challenges and mitigate the risks. The purpose of the thesis is to create a mobile strategy and basis that can be used as a model for creating mobile strategies.

This thesis was executed as a development project. The end results will give information about the present state, guidelines to where the company wants to go and the actual mobile strategy which will be implemented. The theory part of the thesis reclines to IT- and strategy literature and different internet sources. The author has a long and wide working experience from IT system development, IT process development and different IT device management systems.

During the development project, it could be clearly seen that improvements are needed on all sectors. This thesis gives the first steps towards a better and more functional mobile environment. All problems that were found during the project cannot be fixed immediately. To fix these problems and gain changes new development projects need to be started.

Keywords Strategy, mobility, mobile device management, mobile application management, IT risk management.

Pages 28 p. + appendices 3 p.

KÄSITELUETTELO

App Store
Applen julkinen sovelluskauppa.

B2B
Business-to-business. Yritykseltä yritykselle.

B2C
Business-to-customer. Yritykseltä asiakkaalle.

B2E
Business-to-employee. Yritykseltä työntekijälle.

CRM
Customer relationship management, eli asiakkuudenhallintajärjestelmä.

EMM
Enterprise Mobility Management. Pitää sisällään muun muassa MDM-, MAM- ja MCM-tuotteet / teknologiat.

Gartner
Gartner on kansainvälinen ICT-alan tutkimus- ja konsultointiyritys.

Google Play -kauppa
Googlen julkinen sovelluskauppa.

IoT
Internet of Things. Esineiden internet. Internetin laajeneminen fyysisiin koneisiin ja laitteisiin, joiden toimintaa voidaan mitata ja ohjata internet-verkon yli.

MacOS / OS X
Applen kehittämä käyttöjärjestelmä Macintosh-tietokoneille.

MAM
Mobile Application Management. Mobiilisovellustenhallinta. Koostuu seuraavista osista: sovellusten jakelu, lisensointi, asetustenhallinta, elinkaarenhallinta ja käytön seuranta.

MCM
Mobile Content Management. Mobiilisisällönhallinta. Tietoturvallisen pääsynhallinnan ja tiedon käsittelyn mobiililaitteille mahdollistava teknologia.

MDM
Mobile Device Management. Mobiililaitteidenhallinta. Mahdollistaa sovellusten, asetusten ja tiedon jakamisen mobiilipäätelaitteille.

PC
Personal computer. Henkilökohtainen tietokone, esimerkiksi työasema, kannettava tai pöytätietokone.

PIN

Personal identification number. PIN-koodi. Salasanana käytettävä luku, jolla tunnistaudutaan järjestelmään.

Provisiointi

Valmistelu. Esimerkiksi mobiililaiteen liittäminen mobiililaitehallinnan piiriin.

RFID

Radio Frequency IDentifcation. Radiotaajuinen etätunnistus tietojen etälukuun ja -tallentamiseen tageja käyttämällä.

SaaS

Software as a service. Sovelluksen hankkiminen kolmannelta osapuolelta pilvipalveluna. Ei vaadi omalta organisaatiolta ylläpitoa tai palvelinta.

SLA

Service-level agreement, eli palvelutasosopimus. Asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritetään palvelulle halutut tasot.

SPOC

Single point of contact. Keskitetty palvelupiste.

UEM

Unified Endpoint Management. Yhtenäinen päätelaitteiden hallinta. Yhdellä työkalulla voidaan hallita kaikki mahdolliset päätelaitteet.

Vendor lock-in

Toimittaja- tai valmistajariippuvuus. Aiheutuu esimerkiksi, kun jokin järjestelmä toimii pelkästään tietyn käyttöjärjestelmän päällä.

Windows-kauppa

Microsoftin sovelluskauppa.

WLAN / Wi-Fi

Wireless local area network. Langaton lähiverkko, johon päätelaitteita voidaan kytkeä ilman kaapeleita. Langaton lähiverkko voi olla suojaamaton tai suojattu. Suojaukseen voidaan käyttää salasanoja tai sertifikaatteja.

KUVALUETTELO

TAULUKKOLUETTELO

SISÄLLYS

Liite 1 Laitekartoitus lomake
Liite 2 Nykytilankartoitus lomake

1 JOHDANTO

Tablettien ja älypuhelinten räjähdysmäinen yleistyminen tuo suuria paineita sekä työnantajille, että yritysten IT-osastoille modernisoida työntekijöille tarjottavia työvälineitä. Työntekijät ovat entistä tietoisempia uusimmista markkinoille tulleista laitteista sekä teknologioista. He ovat monesti myös tottuneet jo käyttämään jotain tiettyä laitetta tai sovellusta ja omaksuneet sen käytettävyyden ja ominaisuudet. Välttämättä he eivät ole valmiita näistä työkäytössäkään luopumaan. Tätä ilmiötä kutsutaan kuluttajalähtöisyydeksi.

Tällä ilmiöllä on myös haittapuolensa. Yhä useampi työntekijä käyttää nyt myös työssään omaa tablettiaan tai älypuhelintaan tai vähintäänkin vaatii työnantajalta vastaavia laitteita. Muutamia vuosia sitten yritykset tarjosivat työntekijöilleen aina uusimpia ja hienoimpia laitteita, mutta kotona työntekijöillä oli vanhat laitteet. Tänä päivänä tilanne on monesti täysin päinvastainen. Nykytilanne vaatii yrityksiltä ja IT-osastoilta reagointia sekä jonkinlaisia linjauksia.

Kuluttajalähtöisyydellä on erityinen vaikutus yrityksiin, koska kuluttajille suunnatut tekniikat alkavat löytää tiensä yrityksiin. Tämä heijastaa sitä, miten yritykset pystyvät vaikuttamaan ja hyödyntämään uusia teknologioita ja malleja, jotka ovat alun perin kuluttajille suunnattuja. Kuluttajalähtöisyys ei ole strategia tai jotain mikä pitäisi vaan ottaa suoraan käyttöön ja hyväksyä. Kuluttajalähtöisyys voidaan omaksua ja sitä on osattava käsitellä oikealla tavalla, eikä sitä voida pysäyttää.

Kuluttajalähtöisyyden lisäksi mobiliteetti luo jatkuvasti lisää paineita yritysten IT-organisaatioille pysyä kehityksen aallonharjalla ja mukana liiketoiminnan muuttuvissa tarpeissa. Näihin haasteisiin vastaamiseksi olisi hyvä luoda mobiilistrategia, jota vasten myös liiketoiminnan on helpompi peilata omia nykyisiä sekä tulevia tarpeita. Samalla saadaan taklattua monesti myös kuluttajalähtöisyyden mukanaan tuomia haasteita. Mobiilistrategian tulisikin antaa ylätason suuntaviivat kaikelle mobiilille tekemiselle ja toimimiselle.

Mobiliteetti on osa digitalisaatiota, samoin kuin myös esimerkiksi pilvipalvelut, analytiikka, IoT ja Big Data. Digitalisaatiolla onkin tällä hetkellä kova imu ja siihen investoidaan monissa yrityksissä ja yhteisöissä hyvinkin paljon. Digitalisaatiolla pyritään muuttamaan olemassa olevia perinteisesti kankeita liiketoimintamalleja entistä joustavimmiksi ja tehokkaimmiksi.

Tässä työssä ei käydä läpi kaikkia niitä osa-alueita, jotka mobiilistrategiakokonaisuuteen kuuluvat. Työ on myös hyvin tiukasti rajattu koskemaan pelkästään sisäistä asiakasta eli loppukäyttäjää ja siihen liittyviä osia. Työn ulkopuolelle jäävät kaikki ulkoisiin asiakkaisiin liittyvät asiat, sekä monta muutakin asiaa. Valitettavasti kokonaisuudessaan mobiilistrategiaa tämän työn puitteissa ei ole mahdollista tutkia kovinkaan syvällisesti. Työ tulee antamaan vastaukset kysymyksiin: ”Mikä on mobiilistrategia ja miksi se tarvitaan?”, ”Minkälaisilla järjestelmillä mobiililaitteita voidaan hallita?” ja

”Miltä mobiili tulevaisuus näyttää?”. Työn lopputuloksena saadaan yritykselle sisäinen mobiilistrategia. Tätä mobiilistrategiaan vasten voidaan jatkossa peilata kaikkea yrityksen mobiilia toimintaa.

2 STRATEGIA JA IT-RISKIT

Lisäarvon tuottaminen organisaation ulkopuolisille tahoille on kaikkien organisaatioiden toiminnan lähtökohta. Voidakseen tuottaa hyötyä tähän ulkopuoliseen haasteeseen, on organisaation sisällä pystyttävä vastaamaan kysymyksiin: ”Kenelle ja miksi me tuotamme hyötyä?” ja ”Mikä on se hyöty mitä me tuotamme?”. Organisaation tehtävän lähtökohtana tulisi olla se, mitä asiakas haluaa. Toiminnan lähtökohtana ei voi olla, mitä me haluamme tuottaa. (Lindroos & Lohivesi 2004, 17.)

Riippuu organisaatiosta, minkälaisiin haasteisiin sen tulee vastata. Esimerkiksi julkishallinnon ja yritysten haasteet ovat hyvinkin erilaiset. Julkisella sektorilla hyötyjä arvioidaan poliittisesti. Yksityisellä sektorilla taasen asiakkaat ovat ne, jotka päättävät yritysten tarjoamista tuotteista tai palveluista itselleen saamansa hyödyt ja valitsevat näistä sitten sopivimmat. Myöskin syy-seuraus-ketju eroaa näiden kahden välillä hyvinkin paljon. Yritysten osalta se on hyvinkin suoraviivainen, asiakas ostaa itse tuotteen tai palvelun ja arvioi myös siitä saamansa hyödyn. Julkisen sektorin palvelua tai tuotetta käyttävä henkilö ei lähtökohtaisesti maksa itse, vaan nämä tuotteet ja palvelut rahoitetaan julkisista varoista. Tällöin myös hyödyn arviointi on huomattavasti vaikeampaa. (Lindroos 2004, 12–22.)

Organisaatioilla on kolme ydinhaastetta, joihin täytyy pystyä vastaamaan. Nämä kolme haastetta ovat kyky toimia perustehtävän mukaisesti, tuottaa lisäarvoa sekä toimia kannattavasti ja/tai tehokkaasti. Näihin haasteisiin vastaaminen on organisaatioiden toiminnan kannalta kaikkein keskeisintä. Yritysten strategiaprosessin keskeisimmän sisällön muodostaakin näihin haasteisiin vastaaminen, toiminnan suunnittelu, päätöksenteko sekä päätösten toimeenpano. Pysyviin haasteisiin vastauksia etsittäessä täytyy pystyä tekemään valintoja ja ratkaisuja toimintalinjoista (visio ja strategia), ohjauksesta ja sen puitteista (johtaminen ja organisointi), edellytyksistä (resurssit ja toimintaprosessit) sekä taidoista ja haluista (osaaminen ja tahto) (Lindroos 2004, 24).

Menestyvä organisaatio onkin löytänyt vastaukset siitä, miten toiminta on tehokasta ja kannattavaa, sekä miten tuotetaan perustehtävän mukaista lisäarvoa. Nämä vastaukset eivät ole pysyviä, vaan ne ovat jatkuvassa muutoksessa. (Lindroos 2004, 25.)

Jotta voidaan määrittää strategia, tulee ensin hahmotella ja määritellä visio. Visio on näkemys siitä, miksi halutaan tulla tai mitä halutaan tehdä. Visio määritetään tietyksi ajanjaksoksi ja arvioidaan uudelleen tuon ajanjakson päätyttyä. Vision tulisi olla kannustava sekä haasteellinen. (Lindroos 2004, 26–27.)

Strategialla pyritään saavuttamaan visiossa määritellyt päämäärät. Usein kaikkia eteen tulevia haasteita ei nähdä strategiaa laadittaessa ja näihin haasteisiin on sitten tavalla tai toisella vastattava. Voidaan esimerkiksi tarkastella strategiaa säännöllisin väliajoin, laatia erilaisia skenaarioita tai muutetaan strategiaa jopa ”lennossa”. (Kostamo 1999, 128–129)

2.1 Strategian vaiheet

Strategian luonnin yhteydessä tulisi käydä läpi viisi vaihetta, joista lopullinen strategia sitten saa muotonsa. Ensimmäisenä tulisi kerätä ja analysoida ne tiedot, joiden perusteella strategiaa lähdetään rakentamaan ja miksi strategia tulisi laatia. (Lindroos 2004, 31–42.)

Toisessa vaiheessa luodaan kokonaiskatsaus ensimmäisen vaiheen tietojen perusteella siitä, minkälaisia päätöksiä ja minkälaisia tavoitteita toiminnalle asetetaan. Vision perusteella pitäisi pystyä määrittämään tavoitteet, jotka ovat toteutumisen seurannan kannalta riittävän konkreettiset. Näitä tavoitteita ei tulisi olla neljää enempää. Strategian tulisi selkeästi määrittää ne toimenpiteet, joilla visiossa määritetyt päämäärät voidaan saavuttaa ja mitä lisäarvoa ne tuovat. (Lindroos 2004, 42–45.)

Kolmannessa vaiheessa ennen toteutukseen siirtymistä tulee määrittää keskeiset kehitysprojektit. Jotta halutut muutokset voidaan saavuttaa, tulee tunnistaa, minkälaisia muutoksia täytyy saada toteutettua. Osa kehitysprojekteista saattaa olla niin pitkäkestoisia, että ne eivät ehdi edes valmistua kyseisen strategiajakson aikana. (Lindroos 2004, 46.)

Neljäs vaihe koostuu vuosittaisista toimintasuunnitelmista. Nämä toimintasuunnitelmat sisältävät tarkasti määritellyt keinot ja tavoitteet, joilla varsinainen toteutus saadaan aikaan. Strategiaa ei voida saavuttaa, ilman jokapäiväistä käytännön tekemistä. Ylimmän johdon tulee sitoutua strategian toteuttamiseen ja johtamiseen. (Lindroos 2004, 47–48.)

Viidenteen vaiheeseen kuuluu seuranta, arviointi ja strategian päivittäminen. Säännöllisin väliajoin tulisi arvioida ovatko tehdyt linjaukset edelleen valideja ja voidaanko niiden toteuttamista jatkaa vai olisiko tarpeen tehdä tarkennuksia tai jopa hakea uusia suuntia. Joskus saattaa olla jopa tarpeen määrittää kokonaan uusi strategia. Strategiaa ei koskaan saisi määrittää liian tiukaksi ja joustamattomaksi, koska mahdollisiin muutoksiin reagoiminen voi muutoin käydä ylivoimaisen vaikeaksi. (Lindroos 2004, 48–49.)

Yksi suurimmista riskeistä strategiaa luotaessa on ajattelun lukittautuminen johonkin tiettyyn moodiin. Tulisikin osata ajatella luovasti ja kirkkaasti. Tarvittaessa tulisi uskaltaa myös toimia ja ajatella tarvittaessa toisin, kuin mitä alun perin oltiin ajateltu. Tarpeesta riippuen myös vanhoissa linjauksissa pysyminen on hyvä asia, jos se on tavoitteena. Jos näin ei kuitenkaan ole, tulisi uskaltaa tehdä asioita myös ensimmäistä kertaa ja oppia sitä kautta uusia asioita. Useasti huominen poikkeaa huomattavastikin tästä päivästä ja varsinkin silloin hyppäys tuntemattomaan on oikea ratkaisu. (Lindroos 2004, 54.)

Kehitettäessä mobiilistrategiaa tulisi käyttää asiakaspalvelulähtöistä toimintatapaa, koska asiakas on kuitenkin päivittäin tavalla tai toisella mukana tässä toiminnassa. Tällöin tulisi tuntea asiakkaan nykyiset ja mahdolliset tulevat tarpeet. Tulisi pystyä luomaan myös uusia vielä tällä hetkellä tunnistamattomia tarpeita. Näistä edellä mainituista syistä tulisikin tehdä erittäin tiivistä yhteistyötä asiakkaan kanssa. (Lindroos 2004, 64.)

2.2 IT-riskien hallinta

Riskien hallinta on myös tärkeä osa mobiilistrategiaa. Mobiililaitteilla on pääsy yrityksen kannalta kriittiseenkin tieto-omaisuuteen, joka vääriin käsiin joutuessaan voi aiheuttaa dramaattisia ongelmia yrityksen kilpailukykyyn ja toimintaan. Nykyisin tietotekniikka on myös erittäin tärkeä osa liiketoimintaa, mutta siinä esiintyviin häiriöihin on harvoin varauduttu riittävällä tavalla. (Jordan & Silcock, 2005, 1–3.)

Valitettavan usein yritysten johto ei ole riittävän sitoutunut IT-riskeihin ja niiden hallintaan, vaan tuijotetaan liikaa pelkästään tuotto- ja kustannuslaskelmia. Harvoin myöskään on asianmukaisia keinoja tai työkaluja IT-riskien hallintaan. IT-riskejä ei saisi koskaan jättää huomiotta. (Jordan 2005, 4–6.)

IT-riskien hallinnan tulisi pitää sisällään projektit, it-palvelut, tieto-omaisuus, palveluntarjoajat ja toimittajat, sovellukset, infrastruktuuri, strategiset riskit ja tulevaisuuden uhat sekä IT ja muut yritysriskit. Nämä kaikki kuuluvat myös osaksi mobiilistrategiaa. Jos näistä jokin tai pahimmassa tapauksessa useampi konkretisoituu, voi se aiheuttaa pahimmassa tapauksessa jopa yrityksen toiminnan loppumisen. Kaikkia näitä riskejä tulisi käsitellä IT-riskien portfoliossa, jolloin riskien hallinta on helpompaa. Monesti myös yhteen osa-alueeseen kohdistuva ongelma heijastuu myös muille osa-alueille ja mahdollisen ongelman aiheuttaja on helpompi löytää ja identifioida, kun kaikki IT-riskit ovat omassa portfoliossaan. Portfolion avulla voidaan myös helposti nähdä, onko riskien vähentäminen hallittua. (Jordan 2005, 12–23.)

2.2.1 IT-palvelut

IT-palvelut ovat monesti hyvinkin tiukasti kytköksissä yrityksen liiketoimintaan. Pahimmillaan häiriöt IT-palveluissa voivat lamauttaa koko yrityksen liiketoiminnan ja pahimmillaan voi johtaa jopa ihmishenkien menetyksiin. Palvelut tulisi priorisoida, jotta mahdollisessa katastrofitilanteessa voitaisiin jopa vähillä resursseilla keskittyä kriittisimpien palveluiden ylläpitämiseen. Tulisi pystyä rakentamaan toimintasuunnitelmat erilaisista uhkista selviytymiseen. Näitä suunnitelmia tulisi myös testata ja harjoitella säännöllisesti ja jokaisen IT-osaston työntekijällä tulisi olla selvillä oma roolinsa eri uhkaskenaariossa. (Jordan 2005, 15–17.)

2.2.2 Tieto-omaisuus

Tieto-omaisuutta ei ole monestikaan mitenkään rahallisesti arvotettu ja suojaaminenkin on monesti hoidettu vähän sinnepäin, jos ollenkaan. Yksi kohtuullisen helppo keino informaation suojaamiseksi olisi kunnollisen tietojen luokittelujärjestelmän käyttöönottaminen. Tällöin ainoastaan ne henkilöt, joilla on oikeus käsitellä tietoa, pääsisivät siihen käsiksi. Tieto-omaisuuteen liittyvät riskit voidaan ehkäistä, kun tiedon kadottaminen, tahallinen väärinkäyttö sekä varastaminen on estetty. Myöskin lait ja asetukset määrittävät esimerkiksi, kuinka ihmisten henkilökohtaisia tietoja tulee säilyttää ja miten

niitä saa käsitellä. Monessa yrityksessä riski saataisiin hallintaan ottamalla käyttöön ISO-standardin mukaiset toimenpiteet informaation turvalliseen hallintaan. (Jordan 2005, 17–18.)

2.2.3 Palveluntarjoajat ja toimittajat

Palveluntarjoajista on tullut monelle yritykselle ulkoistamisen takia erittäin kriittinen kumppani. On lähes mahdotonta tuottaa IT-palveluita ilman kolmannen osapuolen apua. Koskaan ei pitäisi kuvitella, että ulkoistamalla IT-toimintoja yritys pääsee eroon myös niihin liittyvistä riskeistä. Yrityksen koko liiketoiminta saattaa pahimmillaan vaarantua riskin konkretisoituessa, kun palveluntarjoajalla kolhu voi korkeintaan tuntua maineessa ja kassavirrassa. Toimittajien ja palveluntarjoajien kautta mahdollisesti aiheutuvat riskit liittyvät huonoon palvelun seurantaan, huonosti laadittuihin sopimuksiin tai tieto-omaisuuden vaarantumiseen. (Jordan 2005, 18–19.)

2.2.4 Sovellukset

Sovelluksien osalta riskit monesti tulevat konkreettisesti esille jonkin sovelluksen uusimisen tai uuden sovelluksen käyttöönottamisen jälkeen. Vanhoja tietoja ei löydykään uudesta sovelluksesta tai jotain toimintoa ei löydy ollenkaan. Seuraavat ongelmat tulevat vastaan siinä kohtaa, kun sovellusta on hetken aikaa käytetty ja saatu kunnon rasitusta aikaan. Tässä kohtaa vasta nähdään todellisesti, kuinka resursseja käytetään, minkälaisiin vasteaikoihin päästään ja mikä todellinen suorituskyky kokonaisuudessaan on. Myöskin yritysfuusiot aiheuttavat useasti ongelmia, koska IT-järjestelmien yhteensopivuutta ei monestikaan osata huomioida riittävän ajoissa. Viimeisenä, mutta ei todellakaan vähäisimpänä riskinä ovat elinkaarensa päässä olevat sovellukset. Joitakin saatetaan tekohengittää jopa vuosia, ennen kuin sovellus uusitaan tai sen käyttö lopetetaan kokonaisuudessaan. (Jordan 2005, 19–20.)

2.2.5 Infrastruktuuri

Infrastruktuuriin liittyvät investoinnit ovat yleensä hyvinkin suuria ja monesti suoranaista hyötyä liiketoiminnalle näistä ei ole. Monesti kuitenkin infrastruktuurin vaikutus koko yrityksen toiminnalle on hyvinkin kriittinen. IT-infrastruktuuri voi pahimmillaan olla rakenteeltaan sopimaton niiden sovellusten ja palveluiden tuottamiseen, joiden päällä sen pitäisi toimia. Kapasiteetti voi olla väärin mitoitettu tai huoltotoimenpiteet on unohdettu tai tarkoituksella jätetty tekemättä – säästetty kustannuksissa – ja näistä sitten voi aiheutua suuriakin ongelmia sovellusten ja palveluiden toimintaan. Näiden lisäksi on saatettu tehdä vääriä valintoja standardeja valittaessa, komponentit voivat olla yhteen sopimattomia ja tuen kanssa saattaa tulla ongelmia ennakoimattomien tai tulevaisuudessa tarvittavien sovellusten kanssa. Infrastruktuurin romahtaessa kaikki ne palvelut ja sovellukset, jotka ovat siitä riippuvaisia ovat myös vaarassa. Infrastruktuurin kanssa onkin aikamoista tasapainoilua uusien ja vanhojen systeemien välillä, koska molemmissa on omat riskinsä. Vanhojen osalta kustannukset kasvavat koko ajan ja ylläpito on kaikin puolin hankalampaa. Toisaalta taas uusiminen vanhasta

taas saattaa tuoda yhtä suuret riskit kuin vanhan ylläpitäminenkin. (Jordan 2005, 21–22.)

2.2.6 Strategiset riskit ja tulevaisuuden uhat

Monesti väitetään, että IT-strategiat on sovitettu muihin yrityksen strategioihin, mutta harvoin tämä kuitenkaan pitää paikkaansa. IT-osaston ja yrityksen strategioista päättävien osapuolten tulisi olla tiiviissä yhteistyössä toistensa kanssa strategioita mietittäessä. Tällöin voitaisiin välttää tilanteet, joissa IT ei voi tukea yrityksen strategian onnistumista. Jos yrityksen strategioita valmistelevat tahot eivät osaa huomioida IT:n vaatimuksia ja mahdollisuuksia tulee strategia todennäköisesti epäonnistumaan. Pääsääntöisesti joustava IT-arkkitehtuuri mahdollistaa ketteryyden ja reagointikyvyn uusiin haasteisiin ja saattaa nopeuttaa myös uusien tuotteiden markkinoille saamista. Standardeja tiukasti seuraavalla arkkitehtuurilla taasen pystytään vähentämään kuluja heti, jolloin katteet ovat paremmat. Toisaalta taas pitäisi pystyä katsomaan isompaa kuvaa ja varautua tulevaisuuden haasteisiin. IT-arkkitehtuuri määrittää hyvinkin pitkälti uusien teknologioiden käyttöönottamiseen liittyvät haasteet. (Jordan 2005, 22–23.)

2.2.7 IT ja muut yritysriskit

IT-riskejä ei voi erottaa yrityksen muusta toiminnasta. Joitakin riskejä voidaan jopa vähentää IT:n avulla. Kaikkia organisaatiota uhkaavia riskejä voidaan pyrkiä hallitsemaan riskienhallintaan erikoistuneella tietojärjestelmällä (RMIS). Toki tähänkin liittyy riskejä. Järjestelmällä ei välttämättä pystytä huomioimaan kaikkia tärkeitä riskiluokkia. RMIS on lähinnä käytössä vakuutustoiminnassa, jossa sillä pystytään valvomaan konkreettista omaisuutta. IT-järjestelmiä pystytään käyttämään toki myös muissa organisaation riskienluokkien hallintaan liittyvissä tehtävissä. Petosten ja kavallusten havaitsemiseen voidaan käyttää esimerkiksi erilaisia lokitiedostoja. Tietotekniikan käyttäminen saattaa altistaa yrityksen myös brändiin tai maineeseen liittyviin riskeihin. Järjestelmät saattavat lähettää kirjeitä tai sähköpostia kuolleille asiakkailleen tai aiheettomia karhukirjeitä, jos järjestelmiä ei ole suunniteltaessa ei ole huomioitu asiakkaan näkökulmaa. Näistä voi aiheutua yrityksen imagolle suuriakin vahinkoja. Markkinointikin olisi syytä ottaa mukaan IT-riskien käsittelyyn, koska he edustavat asiakkaita ja brändiä. Useiden erilaisten näkökulmien huomioimisella saadaan kattavasti katettua erilaisten riskienarviointia ja pystytään myös osallistamaan osaajia monilta eri osastoilta. (Jordan 2005, 24 – 25.)

2.3 Mobiilistrategia Gartnerin mukaan

Mobiilistrategian tulisi olla linjassa sekä kehittyä yrityksen strategian kanssa, kuten kaikkien IT-strategioiden. Mobiilistrategian tulisi kuvata, kuinka mobiliteetti auttaa yritystä saavuttamaan tavoitteensa. Toisen sukupolven mobiilistrategia laajentuu IT:n (B2E) ja markkinoinnin (B2B tai B2C) alueille. (Gartner 2012.)

Mobiilistrategian tulisi vastata näihin kolmeen osioon ja niihin liittyviin kysymyksiin:

- Vaatimukset – Minkälainen mobiilikokemus asiakkaille, työntekijöille ja kumppaneille halutaan tarjota? Miten he asioivat, miten heitä informoidaan ja palvellaan?
- Tarjonta – Mitkä teknologiat, resurssit ja kumppanit tuottavat mobiilin kokemuksen?
- Hallintomalli ja riskit – Keitä täytyy osallistaa, kuka rahoittaa ja kuinka riskit minimoidaan?

(Gartner 2012.)

2.3.1 Vaatimukset

Tämän osion tulisi alkaa kappaleella, joka kuvaa minkälaisia vaatimuksia käyttäjille tuotettavat palvelut aiheuttavat ja kuinka suuresta käyttäjä- / laitemäärästä puhutaan (Gartner 2012).

2.3.2 Tarjonta

Tämän osion tulisi tuoda vastaukset siihen, kuinka vaatimukset-osiossa esitetyt vaatimukset saadaan täytettyä. Tulisi ottaa kantaa vähintäänkin käyttäjien omistamiin laitteisiin ja niihin liittyviin käytäntöihin sekä tehdä rajaukset siihen, mitkä ovat yrityksen järjestelmiin ja verkkoihin sallittuja laitteita ja mitkä eivät. Tekniset vaatimukset, kuten alustaan, arkkitehtuuriin, integraatioihin, testausmenetelmiin sekä käyttäjäkokemukseen liittyvät asiat tulisi huomioida. Myöskään osaamiseen, henkilöstön kouluttamiseen tai yhteistyökumppaneihin liittyviä asioita ei tulisi unohtaa. (Gartner 2012.)

2.3.3 Hallintomalli ja riskienhallinta

Näissä kahdessa viimeisessä osiossa täytyy määrittää päätöksentekoon ja hyväksyntään liittyvät sidosryhmät ja henkilöt, riippuvuudet muihin strategioihin, kertaluonteisista ja jatkuvista kuluista vastaava taho ja kuinka pystytään vähentämään tietoturvaan, talouteen ja asiakkaisiin liittyviä riskejä. Myös ne riskit, jotka ollaan valmiit hyväksymään tulisi kirjata tähän osioon. (Gartner 2012.)

Monet yritykset ovat siirtymässä yrityksen omistamista laitteista sekaympäristöön, jossa on sekä yrityksen omistamia, että käyttäjien omistamia laitteita. Tämän takia tulisi luoda selkeät pelisäännöt sille, mikä on sallittua ja mikä ei. Nämä säännöt tulisi myös selkeästi jalkauttaa työntekijöille ja yksiköille. Tulisi myös olla selkeät suunnitelmat rahoituksen ja kustannusten jakamiseen, käyttäjätukeen, huoltoon ja ääni sekä datapalveluihin liittyen. Näitä ohjeistuksia tulisi myös täydentää keskeisillä viesteillä, jotka korostavat arvon- ja valinnanvapautta, jonka IT-organisaatio tarjoaa yrityksen käyttöön. (Gartner 2012.)

Täytyisi olla selvillä, kuka on vastuussa esimerkiksi BYOD-suunnitelman ylläpidosta ja sen jalkauttamisesta, koska markkinat kehittyvät jatkuvasti ja saataville tulee uusia laitteita ja myöskin hallintajärjestelmät kehittyvät. Jos

on määritettynä jotkin kustannuskatot, niiden täytyisi olla myös selkeästi yksiköihin asti viestittynä. Lisäksi tulisi olla selvillä, mitkä nämä rajat ovat, ja kuka ylimääräiset kulut maksaa. (Gartner 2012.)

Uudet teknologiat ja prosessit luovat myös uusia riskejä muun muassa turvallisuuteen liittyen. Monesti voidaan olla tilanteessa, jossa käyttäjät käyttävät omia laitteitaan, ostavat omia sovelluksia, käyttävät kolmannen osapuolen tiedostojen synkronointiohjelmia sekä käyttävät sovelluksia, jotka tallentavat esimerkiksi sijaintitietoja. Nämä sijaintitiedot voivat olla hyvinkin arkaluonteisia. Myöskin teknologian tai kumppanin katoamista varten tulisi olla jonkinlainen suunnitelma. Kaikki edellä mainitut riskit tulisi olla huomioituna ja niiden varalle tulisi olla suunnitelma. (Gartner 2012.)

3 MOBIILISTRATEGIAN LAATIMINEN

Mobiilistrategia on hyvinkin olennainen osa yrityksen liiketoimintaa tuottavuuden kehittämisen osalta. Mobiilistrategian tulisi ottaa kantaa siihen, mitä laitteita yrityksessä nähdään mobiililaitteina, minkälaisille alustoille yritys tuottaa mobiilisovelluksia sekä mitä palveluita yrityksen työntekijöille ja asiakkaille tarjotaan mobiilisti. Mobiilistrategia vaikuttaa strategisella, taktisella ja operatiivisella organisaatiotasolla. Mobiilistrategia tulisi luoda liiketoiminnan tavoitteiden ja digitaalistrategian perusteella. (Nieminen 2014.)

Kuva 1. Mobiilistrategian vaikutukset eri organisaatiotasoilla (Nieminen 2014).

3.1 Liiketoiminnan tarpeet ja vaatimukset

Mobiilistrategian suunnittelussa tulee huomioida erilaiset liiketoiminnan tarpeet ja vaatimukset. Vaatimuksia saattaa tulla vaikkapa jonkin valitun järjestelmän osalta, välttämättä kaikille alustoille ei ole saatavilla järjestelmän käyttämiseen tarvittavaa natiivisovellusta. Liiketoiminta saattaa myös olla suuntaamassa kehitystä esimerkiksi IoT-järjestelmiin, josta luonnollisesti seuraa mahdollisesti vaatimuksia ja tarpeita yrityksen IT-infrastruktuuria kohti. (Microsoft 2015, 3–5.)

3.2 Laitteiden omistajuus

Laitteiden omistajuus on myös yksi asia, joka tulisi huomioida hyvinkin varhaisessa vaiheessa, mielellään jo ennen kuin mitään yrityksen järjestelmiä julkaistaan saataville mobiilisti. Jos sallitaan esimerkiksi työntekijöiden omat laitteet (BYOD), pitää miettiä, tuleeko niihin olla tiukemmat tai kenties löyhemmät politiikat määritettynä tai sallitaanko niiden kautta pääsyä yrityksen järjestelmiin ollenkaan. Jälkikäteen voi olla hyvinkin hankala alkaa määrittää esimerkiksi politiikkaa, jolla rajataan käyttö tiettyihin laitteisiin tai ottaa kantaa laitteiden tietoturva-asetuksiin. (Microsoft 2015 3, 6–8.)

3.2.1 Kuluttajalähtöisyys

Vuonna 2013 3StepIT:n tekemän tutkimuksen mukaan lähes puolet suomalaisista yrityksistä salli työntekijöiden omien laitteiden käyttämisen työtehtävien hoitamiseen. Suuri enemmistö tietohallintojohtajista kuitenkin suhtautuu kuluttajalähtöisyyteen hyvinkin negatiivisesti. Suurimmat syyt tämän negatiivisuuden takana ovat huoli tietoturvasta, loppukäyttäjätuen kasvamisesta, laitteiden ja sovellusten yhteensopivuudesta ja näiden myötä kustannusten kasvamisesta. Modernit työvälineet ja joustava nykyaikainen työskentely ovat kuitenkin kilpailuvaltti, eikä kuluttajalähtöisyyttä pystytä enää pysäyttämään. Onkin mielenkiintoista nähdä, kuinka uusien laitteiden käyttö yrityksissä kehittyy ja kuinka yritykset kuluttajalähtöisyyden haasteisiin pystyvät vastaamaan. Monissa yrityksissä omien laitteiden käyttöä ei ole sallittu, mutta sitä ei myöskään ole mitenkään teknisesti tai muutoinkaan estetty ja näin ollen omia laitteita saatetaan käyttää ”salaa”. (Vikkula 2013.)

3.2.2 BYOD, CYOD ja yrityksen omistamat laitteet

BYOD tulee sanoista Bring Your Own Device. Se on malli, jossa käyttäjä itse hankkii laitteen ja käyttää sitä työasioidensa hoitamiseen. Tässä mallissa ongelmia voi aiheutua vanhoista sovelluksista, jotka eivät toimi käyttäjän laitteella tai tietoturvaan liittyvistä asioista. Toisaalta sitten taas käyttäjä voi valita laitteen jonka haluaa ja jota osaa jo valmiiksi käyttää, jolloin tukeakaan ei juurikaan tarvita. Työskentely on joustavaa ajasta ja paikasta riippumatonta. (Jääskeläinen 2016.)

CYOD tulee sanoista Choose Your Own Device. Se taas on malli, jossa käyttäjä valitsee laitteen yrityksen määrittämästä laitevalikoimasta. Tämän mallin voi toteuttaa useammalla hankintamallilla. Yritys voi maksaa laitteen kokonaisuudessaan, maksaa osan laitteesta ja käyttäjä maksaa lopun tai käyttäjä maksaa laitteen kokonaisuudessaan. Tukeen liittyvät kulut ovat yleensä hyvinkin samalla tasolla, kuin yrityksen omistamissa laitteissa. Tässä mallissa voidaan myös työtehtävän mukaisesti määrittää laitteet, joita käyttäjälle tarjotaan. (Jääskeläinen, 2016.) Tällä mallilla on havaittu olevan lisäksi positiivista vaikutusta käyttäjien työhyvinvointiin ja tyytyväisyyteen työnantajaa kohtaan (Hietamäki 2016).

Yritys ostaa laitteet ja tarjoaa työntekijälle laitteen työtehtävien hoitamiseen. Tässä mallissa käyttäjä ei pääse vaikuttamaan siihen, millä laitteella työtehtäviä hoidetaan. Tämä malli on kustannusten osalta kallein tuki ja laitteistokulujen vuoksi. Pääsääntöisesti laitevalikoima tässä mallissa on suppea ja siitä johtuen sovellustestaukseen ei tarvitse käyttöjärjestelmä- tai tietoturvapäivitysten yhteydessä käyttää paljoa aikaa. Loppukäyttäjätukea tulee sitten vastaavasti tarjota kaikille valikoimissa oleville laitteille, mikä nostaa kuluja. (Microsoft 2015.)

3.3 Sovellukset

On olemassa kolmenlaisia sovelluksia mobiililaitteille. Natiivi-, HTML5 Web- ja hybridisovellukset. Sovelluksia voidaan hankkia valmiina sovelluskaupoista tai tehdä räätälöityjä sovelluksia joko itse tai jonkin kumppanin toimittamana. Sovelluskaupoissa saatavilla olevat sovellukset ovat ilmaisia, maksullisia, tai sisältävät sovelluksen sisäisiä ostoja. (Vuorinen 2014.)

Natiivisovellukset ovat laitealustakohtaisia sovelluksia, jotka on ohjelmoitu toimimaan kyseisellä alustalla erilaisia kehitystyökaluja käyttäen. Uusimmilla sovelluskehitysvälineillä pystytään tekemään natiivisovellus yhdellä kertaa kaikille alustoille, toki pieniä alustakohtaisia muutoksia koodiin yleensä vaaditaan. Natiivisovelluksia voidaan jaella asiakkaille sovelluskauppojen (App Store, Google Play -kauppa, Windows kauppa) kautta ja ne voivat olla joko ilmaisia, maksullisia tai tarjota ostoja sovelluksen sisällä. Natiivisovellusten etuna voidaan pitää helppoa pääsyä laitealustan tarjoamiin rajapintoihin ja toimintoihin, kuten kameraan, kiihtyvyysantureihin, yhteystietoihin, viesteihin jne. Niiden suorituskyky on myös hyvä paljon grafiikkaa sisältävissä sovelluksissa. (Vuorinen 2014.)

Web-sovellusten etuna voidaan pitää helppoa ja yksinkertaista kehittämistä ja yhdellä kertaa saadaankin valmis sovellus kaikille alustoille. Sovelluskehittäjiä löytyy myös huomattavasti enemmän, koska kehittämiseen käytetään HTML, CSS ja JavaScript -tekniikoita, eli samoja, joilla normaaleja verkkosivuja ja –palveluita rakennetaan. Niitä ei myöskään tarvitse jaella minkään virallisen jakelukanavan läpi, vaan julkaisun voi tehdään suoraan internettiin. Huonoihin puoliin taas lukeutuu se, että kaikki rajapinnat ja laitteen toiminnot eivät välttämättä ole käytettävissä. Tosin suurinta osaa pystytään käyttämään JavaScript-rajapintoja hyödyntäen. (Vuorinen 2014.)

Hybridisovelluksissa yhdistyvät molempien edellä mainittujen hyvät ominaisuudet. Ne voivat hyödyntää kaikkia laitteen rajapintoja ja toimintoja, kuten natiivisovelluksetkin. Niissä on WebView-näkymä, joka on sovellukseen sisäänrakennettu internet-selain ilman osoitepalkkia ja muita selaimen toimintoja. Sovellukset saadaan jaeltua virallisia kanavia pitkin ja halutessa ne voidaan pitää maksullisina. Sovellus, joka laitteelle on asennettuna, on myös käyttäjälle helpompi vaihtoehto, kuin internetissä oleva web-sovellus. Tarvitsee vain avata sovellus ikonista ja aloittaa sovelluksen käyttäminen. (Vuorinen 2014.)

Mobiiliapplikaatioihin kohdistuu myös tietoturvaan liittyviä ongelmia. Applikaatioissa voi olla haavoittuvuuksia, joiden avulla voidaan päästä pahimmillaan kaikkeen laitteessa olevaan tietoon käsiksi. (Ponemon Institute 2015, 2)

Applikaatioita ei tulisi asentaa muualta, kuin virallisista kaupoista. Näitä ovat Google Play -kauppa (Googlen sovelluskauppa), App Store (Applen sovelluskauppa) sekä Microsoft Store (Microsoftin sovelluskauppa). Tosin F-Securen mukaan eniten haittaohjelmia Android-alustaan tulee juurikin Google Play -kaupan kautta (F-Secure 2016).

3.4 Mobiililaitteet

Mobiilistrategian tulisi määrittää myös mitkä laitteet yritys näkee mobiililaitteina. Viime aikoina mobiililaitteen määrittäminen on ehkä hiukan hämärtynyt. Hyvin laaja ryhmä henkilökohtaisia elektronisia laitteita voidaan luokitella mobiililaitteiksi. Luokitteluun voidaan ottaa mukaan kaikki laitteet aina viivakoodinlukijoista älypuhelimiin ja tabletteihin. Pääsääntöisesti mobiililaiteet voidaan erottaa kolmen tunnusmerkin avulla muista laitteista, jotka voivat muistuttaa mobiililaitetta, mutta eivät sitä kuitenkaan ole. Tunnusmerkit ovat siirrettävyys, pieni koko ja langaton kommunikaatio. (Callahan 2014).

Mobiililaitteita voidaan siirtää paikasta toiseen usein ja helposti. Laitteen tulee pystyä toimimaan siirrettäessä riippumatta virtalähteestä tai fyysisestä internet yhteydestä. Mobiililaitteet tyypillisesti sisältävätkin jonkin sisäisen virtalähteen, jonka avulla ne toimivat useita tunteja ilman verkkovirtaa. (Callahan 2014.)

Mobiililaitteet ovat kädessä pidettäviä laitteita, kämmentietokoneita tai älypuhelimia. Tyypillinen mobiililaite mahtuu keskikokoisen aikuisen kämmenelle tai taskuun. Mobiililaite on tyypillisesti yhdellä kädellä käytettävissä, eli laitetta pidetään kämmenellä tai sormilla, ja peukalolla voidaan sitten varsinaisesti käyttää laitetta. Miniläppäreita ja pieniä kannettavia tietokoneita saatetaan toisinaan pitää mobiililaitteina, mutta sitä ne eivät ole, jos yhdellä kädellä käytettävyys on mittarina. (Callahan 2014.)

Mobiililaitteet pystyvät tyypillisesti keskustelemaan toisten samanlaisten laitteiden, pöytätyöasemien ja järjestelmien sekä verkkojen ja kannettavien puhelinten kanssa. Mobiililaitteilla pystytään muodostamaan yhteys internettiin Bluetooth- tai Wi-Fi-verkkojen kautta ja monissa laitteissa on myös sisäänrakennettuna yhteysmahdollisuus matkapuhelin- ja/tai langattomiin verkkoihin. Sähköpostit ja tekstiviestit ovat standardeja viestintäkeinoja, joskin jotkin laitteet kommunikoivat suoraan järjestelmän kanssa, kuten RFID- ja viivakoodinlukijat. (Callahan 2014.)

Markkinaosuuksista katsottuna markkinoilla on tällä hetkellä kolme käyttöjärjestelmää, Android, iOS ja Windows Phone / Windows Mobile (IDC 2016a).

Taulukko 1. Älypuhelinten käyttöjärjestelmien markkinaosuudet elokuussa 2016 (IDC 2016a)

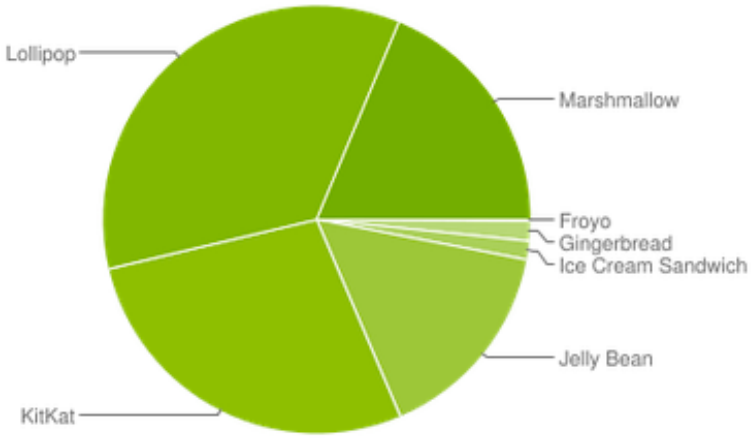
Period	Android	iOS	Windows Phone	Others
2015Q3	84.3%	13.4%	1.8%	0.5%
2015Q4	79.6%	18.6%	1.2%	0.5%
2016Q1	83.4%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%

Source: IDC, Aug 2016

3.5 Tietoturva

Tietoturva koostuu monesta erillisestä osa-alueesta, jotka kaikki tulisi huomioida. Tulisi ottaa huomioon käyttöjärjestelmään ja laitteeseen liittyvä tietoturva, sovellukset ja niiden tietoturva, sekä itse tietoon liittyvä tietoturva. (Oliver 2008, 6–7)

Androidin heikkoutena voidaan varsinkin yrityskäytössä pitää tietoturvaa ja käyttöjärjestelmän päivittymistä silloin, kun käytetään muita kuin Googlen Nexus- tai Samsung laitteita. Heinäkuussa 2016 tietoturva yhtiö Duo Labs suositteli Android-alustalla toimivista laitteista pelkästään Google Nexus- ja Samsung laitteita. Näissä kahdessa on tietoturvaan panostettu enemmän kuin muissa Android-pohjaisissa laitteissa. Tosin Samsung tuottaa päivityksiä vain osalle laitteista. Nexus-laitteille päivitykset ovat saatavilla heti, kun Google tietoturva- tai käyttöjärjestelmäpäivityksiä julkaisee. Muiden osalta on täysin laitevalmistajan käsissä, tuotetaanko laitteeseen tietoturva- tai käyttöjärjestelmäpäivityksiä, Googlen päivitysten pohjalta. Varsinkaan halvimman hintaluokan kuluttajalaitteille päivityksiä ei julkaista ja nämä tulisikin täysin ohittaa, kun mietitään laitteita yrityskäyttöön. (Tech Times 2016.)



Kuva 2. Android käyttöjärjestelmät 5.9.2016 (Android developers 2016)

Taulukko 2. Android käyttöjärjestelmät 5.9.2016 (Android developers 2016)

Version	Codename	API	Distribution	Release Date	Support Status
2,2	Froyo	8	0.1%	20.5.2010	Discontinued
2.3.3 - 2.3.2007	Gingerbread	10	1.5%	6.12.2010	Discontinued
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.4%	18.10.2011	Discontinued
4.1.x	Jelly Bean	16	5.6%	9.7.2012	Discontinued
4.2.x		17	7.7%		
4,3		18	2.3%		
4,4	KitKat	19	27.7%	31.10.2013	Security Updates Only
5	Lollipop	21	13.1%	12.11.2014	Supported

5,1		22	21.9%		
6	Marshmallow	23	18.7%	5.10.2015	Supported

Taulukossa 2 on kuvattuna Android laitteissa asennettuna olevien käyttöjärjestelmien tilanne 5. syyskuuta 2016. Tiedot kerätty laitteista, jotka ovat viimeisen 7-päivän aikana olleet yhteydessä Google Play -kauppaan. Tässä vaiheessa oli jo julkaistuna Nougat, uusin julkisesti saatavilla oleva Android-käyttöjärjestelmä. Taulukossa ei näy alle 0,1% osuuden käyttöjärjestelmiä, joihin Nougatkin tuolla hetkellä kuului. (Android developers 2016.)

Vastaavasti iOS -käyttöjärjestelmän asennettuina olevat versiot näyttävät tältä.

Last Updated: Oct 09, 2016 05:32:04

Adoption Trends

All Platforms:

10.X	62.4%
9.X	29.6%
8.X	3.4%
7.X	2.4%
6.X	1.7%
5.X	0.5%
4.X	0.0%

Kuva 3. iOS käyttöjärjestelmät 9.10.2016 (iOS Version Stats 2016)

3.6 Mobiililaitehallinta

EMM-teknologia joka on kehitetty mobiililaitteiden, sovellusten ja sisällön suojaamiseen ja hallitsemiseen. Se pitää sisällään MDM-, MAM- ja MCM-tuotteet. (IDC 2016.)

MDM:n eli mobiililaitehallinnan avulla voidaan laite liittää hallinnan piiriin. Voidaan määrittää esimerkiksi yhteensopivuuskäytäntö, joka asettaa tietynlaiset minimivaatimukset, jotka laitteen tulee täyttää, jotta se voidaan liittää hallinnan piiriin ja päästään käsiksi yrityksen tietoihin ja järjestelmiin. Tällaisia vaatimuksia voivat olla esimerkiksi tietty käyttöjärjestelmäversio, tai että salasana tai PIN täytyy olla asetettuna ja sen tulee täyttää sille määritetyt minimivaatimukset. (Microsoft, 2016.)

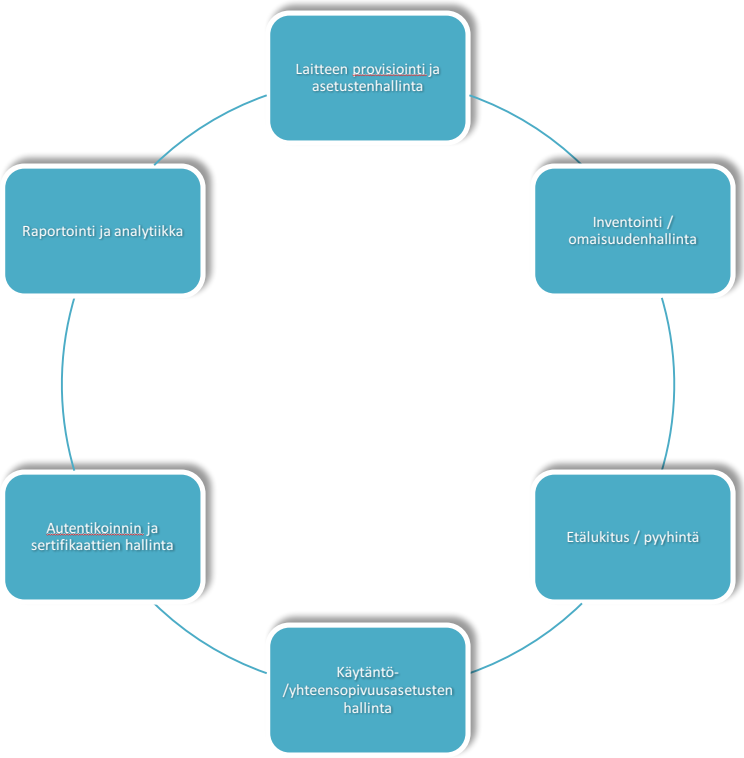
MDM-järjestelmän avulla liitettyyn laitteeseen voidaan määrittää erilaisia asetuksia tai asentaa vaikkapa sovelluksia. Asetusten kautta voidaan automaattisesti tuoda vaikkapa sähköpostiprofiili, WLAN-profiili tai erilaisia sähköisiä varmenteita. (Microsoft 2015, 28–39.)

Järjestelmän avulla laiteelle voidaan katoamis- tai varkaustapauksissa suorittaa niin sanottu tietojen pyyhkiminen joko osittain tai kokonaan yrityksen tietojen turvaamiseksi. Osittainen pyyhkiminen poistaa vain sen tiedon,

joka järjestelmän avulla laitteelle on tuotu. Osittaista pyyhkimistä voidaan myös käyttää esimerkiksi BYOD-laitteiden osalta, kun käyttäjä syystä tai toisesta poistuu yrityksen palveluksesta. Täysi pyyhkiminen tarkoittaa laitteen palauttamista tehdasasetuksiin, eli se poistaa kaiken tiedon joka laitteella on ollut. (Microsoft, 2015 46–51.)

Laitteita ja käyttäjiä voidaan myös ryhmitellä erilaisten parametrien perusteella omiin ryhmiinsä. Näille ryhmille voidaan sitten tarjota automaattisesti erilaisia asetus- ja sovelluskokonaisuuksia. (Microsoft 2015, 15.)

Keskeisimmät MDM-toiminnallisuudet ovat:



Kuva 4. Keskeisimmät MDM toiminnallisuudet (IDC 2016.)

MAM viittaa ratkaisuun, jolla IT-organisaatio voi tiettyjä sovelluksia hallita, suojata ja jakaa. Tiettyihin sovelluksiin tai sovellusryhmiin voidaan kohdistaa mobiilisovellusten hallintakäytäntöjä, jotka voivat vaikuttaa sovelluksen asetuksiin, tietoturvaan tai vaikkapa mahdollistavat kertakirjautumisen. Sovelluksen voidaan esimerkiksi sallia tiedon jakaminen pelkästään toisten hallittujen sovellusten kesken, voidaan estää varmuuskopiointi tai salataan hallitun sovelluksen tiedot. (IDC 2016.)

MCM on ratkaisu, jonka avulla IT voi tarjota käyttäjille suojatun pääsyn mobiililaitteilta yrityksen tietovarastoihin. Näiden järjestelmien avulla IT voi määrittää, kuka pääsee käsiksi mihinkin informaatioon, milloin ja millä laitteilla tai sovelluksilla. MCM-järjestelmät voivat myös olla kytkettynä olemassa oleviin identiteetin- tai oikeuksienhallintajärjestelmiin. Tietovuotojen estäminen on näiden järjestelmien päätehtävä ja sen ne toteuttavat tarjoamalla työkaluja, joiden avulla IT voi määrittää tiedonkulkua sisään ja

ulos suojatuista sovelluksista sekä suojata liikenteen sovellusten välillä. Järjestelmät voivat sijaita joko pilvessä tai yrityksen omissa tiloissa ja voivat tarjota pääsyn joko pilvitiedostoihin tai palomuurin takana sijaitseviin tiedostoihin. (IDC 2016.)

3.7 Mobiililaitteiden hallinnan tulevaisuus

Mobiililaitteidenhallinnan voidaan nähdä olevan jonkinlaisessa murroksessa parhaillaan. Esimerkiksi Microsoftin Windows 10 -käyttöjärjestelmä tarjoaa mahdollisuuden hallintaan MDM-rajapinnan kautta Windows 10 -käyttöjärjestelmällä varustetuille työasemille, kannettaville, tableteille sekä puhelimille (Microsoft 2016a). Sama on ollut mahdollista Mac OS X -käyttöjärjestelmässä versiosta 10.8 lähtien (Apple 2016). Yhdellä ja samalla hallintatuotteella pystyy hallitsemaan sekä perinteiset työasemat, että mobiililaitteet (Microsoft 2016b).

UEM tulee olemaan lähitulevaisuudessa seuraava askel hallinnan osalta. Sen avulla pystytään hallitsemaan kaikki mobiililaitteet, perinteiset PC-laitteet sekä älylaitteet, jotka voidaan osittain ryhmitellä myös IoT-laitteisiin. Älylaitteista voitaisiin esille nostaa Apple TV, tulostimet ja älykellot. (Gartner 2016.)

4 MOBIILISTRATEGIA KÄYTÄNNÖSSÄ

Varsinaista mobiilistrategiaa luotaessa tulisi kaikki edellä mainitut asiat käydä läpi ja hahmottaa kokonaiskuva yrityksen omista tarpeista. Lisäksi tulisi pohtia, minkälaisia haasteita omassa ympäristössä mahdollisesti kohdataan ja miten ne voidaan ratkaista. Tähän täytyisi löytää jonkin ketterä malli, jolla ensimmäisen ”harjoituksen” jälkeen voidaan nopeasti tarvittaessa muuttaa suuntaa, joko jonkin yksittäisen alueen tai vaikka kaikkien osalta. Yksi hyvistä ja kantavista voimista, joka mobiilistrategiaa luotaessa tulisi muistaa on se, että käyttäjän tulisi olla lähtökohtaisesti keskiössä. Mobiilistrategian avulla tulisi tarjota käyttäjälle työkalut tuottavampaan työskentelyyn ja samalla yrityksen tietojen tulisi olla suojattuna ja saatavilla.

Tässä opinnäytetyössä kuvataan mobiilistrategian elementit ja osa-alueet, joiden pohjalta yritykset ja organisaatiot voivat alkaa hahmotella omia strategioitaan. Opinnäytetyön taustalla on asiakasyrityksen projekti, jossa luodaan kyseiselle yritykselle mobiilistrategia. Tietoturvan ja liiketaloudellisten seikkojen takia tämä työ ei esittele yrityksen varsinaista strategiaa, vaan opinnäytetyön tuloksena syntyy mobiilistrategian viitekehys ja malli, jota käytetään myös asiakasyrityksen mobiilistrategiaa laadittaessa.

4.1 Strategian omistaja

Strategialla tulisi olla omistaja, joka huolehtii strategian ajantasaisuudesta. Ennalta sovituin väliajoin strategian jalkautumista tulisi tarkastella sovittujen mittareiden avulla. Lisäksi strategiaa itseään tulisi tarkastella ja mahdollisesti tehdä muutoksia määritettyjen ajanjaksojen jälkeen. Kehityksen ollessa tällä hetkellä hyvinkin nopeaa, mobiilistrategian tarkasteluvälin tulisi olla maksissaan 12 kuukautta. Mobiilistrategiaa on aivan turha tehdä kolmen tai viiden vuoden ajanjaksolle, koska tällöin joudutaan aivan varmasti tekemään muutoksia kesken strategiajakson.

4.2 Riippuvuudet muihin strategioihin

Mobiilistrategia voi vaikuttaa suoraan tai välillisesti muihin yrityksen strategioihin. Siihen voivat vaikuttaa myös muut yrityksessä jo käytössä olevat strategiat. Näitäkin tulisi tarkastella heti alkuvaiheessa ja kartoittaa kaikki mahdolliset riippuvuudet. Jos nämä riippuvuudet jätetään kartoittamatta, saatetaan tehdä päällekkäisiä ja/tai toisiaan pois sulkevia päätöksiä.

4.3 Nykytilan kartoitus

Mobiilistrategiaa mietittäessä tulisi lähteä liikkeelle siten, että on selkeä kuva heti alussa siitä, mihin ollaan menossa. Eli selkeä visio siitä, mitkä ovat tavoitteet. Täytyisi pystyä muodostamaan iso kuva siitä, mitä kaikkea mobiilistrategia pitää sisällään, mihin se vaikuttaa ja mitkä asiat vaikuttavat siihen. Ei voida lähteä liikkeelle siitä, että miten voimme tukea Apple iPad -laitteita. Ensimmäisenä tulee ymmärtää, mitä yritys pyrkii saavuttamaan käyttämällä tabletteja, älypuhelimia sekä muita mobiililaitteita? Minkälaisia rajapintoja käyttäjillä on yrityksen järjestelmiin ja palveluihin nyt?

Luoko mobiliteetti uusia mahdollisuuksia yritykselle ja jos, niin miten nämä mahdollisuudet voidaan hyödyntää? Onko jotain uusia applikaatioita tai rajapintoja, joita tulisi kehittää? Täytyykö prosesseja kehittää tai jopa suunnitella uudelleen? Ja tarvitseeko nykyistä infrastruktuuria päivittää tai tuleeko sen olla paremmin hallittavissa oikean kokemuksen tuottamiseksi käyttäjille?

Kun ollaan saatu luotua jonkinlainen visio siitä, mihin pyritään ja mitä halutaan, tulisi aloittaa nykytilan kartoitus. Tällä kartoituksella pyritään löytämään kaikki ne asiat, jotka vaikuttavat mobiilistrategian luomiseen. Kartoituksessa käytetty lomake löytyy liitteestä 2.

Kaikkea nykytilaan vaikuttavaa ei välttämättä pystytä heti muuttamaan. Sen takia onkin erittäin tärkeää tunnistaa kaikki tällä hetkellä olemassa olevat tarpeet. Voi esimerkiksi olla, että johonkin taustajärjestelmään pääsee käsiksi pelkästään jollain tietyllä käyttöjärjestelmällä varustetulla mobiililaitteella ja siihen asennetulla natiivisovelluksella. Jos päästään aloittamaan niin sanotusti puhtaalta pöydältä, niin silloin nykytilan kartoitus voidaan unohtaa ja siirtyä suoraan seuraaviin vaiheisiin. Nykytilan kartoitus tarjoaa pohjan, jonka päälle rakennetaan kaikki muu.

Asiakasyrityksen nykytilan kartoituksen aikana selvisi, että lähtötilanne oli melko huono. Yrityksellä ei ollut käytössään mobiililaitteiden hallintajärjestelmää. Yrityksen mobiililaitteiden osalta ei ollut myöskään mitään käyttöomaisuudenhallintaa. Myöskään mobiilistrategian vaatimia prosesseja ei oltu määritetty eikä kuvattu. Projektin aikana nykytilaa kartoitettiin eri osapuolten kanssa. Kartoituksen yhteydessä tunnistettujen käyttäjäryhmien edustajilta tiedusteltiin laitteiden käyttötarkoitusta, käyttöjärjestelmää, merkkiä sekä mallia, sovelluksia, käyttäjien työroolia ja käyttäjämääriä. Kyselyssä käytetyt kysymykset ovat nähtävillä liitteessä 1.

4.4 Liiketoiminnan vaatimukset

Liiketoiminnan tulisi olla hyvinkin tiiviisti mukana mobiilistrategian luomisessa. Liiketoiminta on yksi suurimmista mobiilistrategiaan vaikuttavista tekijöistä. Liiketoiminnalla saattaa olla vaatimuksia sille, mitä kaikkea mobiililaitteilla täytyy pystyä tekemään.

Projektissa asiakasyrityksen uusi toiminnanohjausjärjestelmä asetti vaatimuksia myös mobiilistrategialle. Lähtökohtana oli se, että mobiiliin toimintaan päästään toiminnanohjausjärjestelmällä. Järjestelmä pitää saada asennettua ja päivitettyä mobiililaitteisiin ja laitteet tulee saada suojattua.

4.5 Tietoturva

Tietoturvanäkökulma riippuu hyvinkin pitkälti siitä, onko käytössä CYOD- ja/tai BYOD-malli vai pelkästään yrityksen omistamat laitteet. CYOD- ja BYOD-mallit tarvitsevat enemmän huomiota tietoturvankin osalta, koska laitteet ovat enemmän tai vähemmän käyttäjän omistuksessa ja esimerkiksi tietosuojasyistä ne eivät voi olla aivan samalla tavalla yrityksen hallinnassa,

kuin yrityksen omistamat laitteet. Tulee miettiä, miten esimerkiksi varkaustapauksissa toimitaan. On päätettävä, onko yrityksellä oikeus tyhjentää käyttäjän omistama laite kokonaisuudessaan ja samalla poistaa myös käyttäjän henkilökohtaiset tiedostot kuten vaikkapa kuvat. Laitteesta tietojen poistamiseen vaikuttaa myös se, miten hallintaa suoritetaan – ovatko laitteet perinteisesti MDM-hallinnan piirissä vai hallitaanko pelkästään sovelluksia MAM-käytäntöjen avulla. Tähän valintaan vaikuttaa sekin, että kaikkia sovelluksia ei vielä pystytä MAM-käytäntöjen avulla suojaamaan. Hallintamalleja voi olla erilaisia eri mallien välillä. Esimerkiksi kaikki yrityksen omistamat laitteet voivat olla kokonaisuudessaan MDM-hallinnan piirissä. Tällöin laitetta hallitaan erilaisten käytäntöjen avulla, sovelluksia voidaan jakaa pakotettuna laitteille, MAM-käytännöillä hallitaan sovelluksia ja tyhjennys voidaan suorittaa varkaus tai katoamistapauksissa täydellisenä, jolloin kaikki laitteen tiedot poistetaan. BYOD- / CYOD-laitteita taas voitaisiin hallita pelkillä MAM-käytännöillä. Tällöin sovellusten tulee olla saatavilla julkisista sovelluskaupoista, kuten App Storesta, Google Play -kaupasta tai Windows-kaupasta. Pelkkä MAM-käytännöillä sovellusten määritysten hallinta, kun ei tarjoa mahdollisuutta asentaa sovelluksia laitteille.

Asiakasyrityksen työntekijöistä iso osa tekee liikkuvaa työtä ja tästä syystä tietoturva on mobiilistrategiassa tärkeässä osassa. Mobiililaitteiden suojaukseen tuleekin kiinnittää erityisesti huomiota.

4.6 Laitteet, omistajuus ja elinkaari

Heti alkuvaiheessa tulisi määrittää mitkä laitteet yrityksessä luokitellaan mobiililaitteiksi. Onko rajaus hyvin tiukka ”viralliseen” mobiililaitteen määritykseen nähden, siten että mobiililaitteita ovat pelkästään älypuhelimet ja tabletit ja muut yhdellä kädellä käytettävissä olevat laitteet. Laajimmillaan mobiililaitteiksi voidaan määritellä kaikki ne laitteet, joilla päästään tavalla tai toisella käsiksi yrityksen järjestelmiin tai tietoihin ajasta ja paikasta riippumatta. Tällöin huomioitavien asioiden määrä kasvaa huomattavasti ja myöskin vaatimuksen monen asian suhteen ovat suuremmat ja vaativat enemmän huomiota sekä suunnittelua. Todennäköisesti myöskin kulut ovat suuremmat. Pelkästään kulujen takia yhtään laitetta tai järjestelmää ei kuitenkaan pitäisi jättää ulos strategiasta. Pahimmillaan tällainen ajattelumalli aiheuttaa yrityksen tietojen vaarantumisen ja vuotamisen, kun kaikkia mahdollisia laitteita ei ole huomioitu, politiikkaa määritetty tai niiden käyttämistä ei ole estetty. On myös mahdollista pilkkoa strategiaa pienempiin paloihin esimerkiksi siten, että määritetään mobiililaitteiksi älypuhelimet ja tabletit ja näille määritetään oma strategiansa. Tämän lisäksi määritetään oma strategiansa IoT-laitteilla ja niin edelleen. Näillä on hyvinkin todennäköisesti riippuvuuksia toisiinsa, eli nykytilan analyysissä sekä visiossa tulisi käydä kaikki kuitenkin läpi. Mobiililaitemääritys saattaa myös vaikuttaa jo olemassa oleviin laitteisiin ja niiden käyttöön.

Laitteiden lisäksi tulisi määrittää ne käyttöjärjestelmät joita laitteissa tulee olla käytettävissä. Käyttöjärjestelmien suhteen voi tulla vaatimuksia jo nykytilan kartoituksen kautta. Jokin käytettävä järjestelmä saattaa esimerkiksi tuottaa valmiiksi tietyille alustoille natiivisovelluksen. Jos ei olla valmiita

räätälöimään sovellusta muille alustoille ja/tai panostamaan sovelluskehitykseen, niin tästä saattaa ainakin tietyiltä osin aiheutua niin sanottu vendor lock-in tilanne. Eli on pakko käyttää tiettyä käyttöjärjestelmää vähintäänkin jollain tietyllä osa-alueella. Käyttöjärjestelmämäärityksen lisäksi tulisi määrittää mitä käyttöjärjestelmäversioita tuetaan. Tuetaanko pelkästään uusinta versiota käyttöjärjestelmästä vai erimerkiksi uusinta ja sitä edeltävää. Tällä määrityksellä saattaa olla suuriakin vaikutuksia laitteiden elinkaareen. Varsinkin Android laitteet saavat todella huonosti käyttöjärjestelmä- ja tietoturvapäivityksiä ja liian tiukka määritys saattaa aiheuttaa jopa tilanteen, jossa laitteet joudutaan vaihtamaan puolenvuoden välein uusiin ja tästä taas voi seurata suuriakin kustannuksia.

Laitteet, jotka mobiililaitteiksi on määritetty, tulee tarjota loppukäyttäjien saataville jollakin tavalla. Valittava malli vaikuttaa hyvinkin paljon myös kaikkeen muuhun tavalla tai toisella. Valitun mallin mukaan täytyy vielä miettiä mitä kaikkea sen tulee pitää sisällään. Mitkä laitteet tarjotaan saataville, kuka laitteen omistaa, jäävätkö laitteet elinkaaren jälkeen yrityksen vai käyttäjän omistukseen, miten tiedot pyyhitään ja niin edelleen. CYOD-mallia voidaan esimerkiksi tarjota kahdella eri tavalla, toisessa laitteen omistaa yritys ja toisessa elinkaaren lopussa käyttäjä voi lunastaa laitteen itselleen. Nämä kaikki ovat asioita, joita tulee miettiä ja mielellään vielä pidemmällä tähtäimellä, koska siirtyminen erilaisten mallien välillä ei varmasti ainakaan lisää käyttäjien tyytyväisyyttä ja työtehoa. Myöskään hybridimallin valitseminen ei ole pois suljettua. Voidaan tarjota jollekin osalle työntekijöistä vaikkapa CYOD-mallia ja toisille pelkästään yrityksen omistuksessa olevia laitteita, hyvinkin suppealla valikoimalla. Hybridimallilla saattaa joissakin tapauksissa olla työhyvinvointia heikentävä vaikutus, jos/kun tieto erilaisten mallien olemassa olosta kiirii toisen ryhmän tietoon. Näin myös hyvinkin todennäköisesti käy, jos ryhmät työskentelevät tiiviisti toistensa kanssa.

Laitteet voidaan hankkia suoraan yrityksen omistukseen tai vaikkapa jonkin kumppanin kautta vuokraamalla laitteet tietyksi ajaksi yrityksen käyttöön. Pääsääntöisesti kumppanin kanssa toimimalla saavutetaan etuja, joita ei muuten saada. Kumppani voi huolehtia esimerkiksi laitteiden esiasennuksista, laitteiden omaisuudenhallinnasta ja elinkaarenhallinnasta kokonaisuudessaan. Helpoimmillaan yritys määrittää pelkästään laitteet, joita se käyttäjilleen jonkin mallin mukaisesti tarjoaa ja kaiken muun hoitaa kumppani, aina tilausportaalista lähtien siihen, että laite on elinkaaren lopussa tuhottu tietoturvallisesti. Tämän hetkisen korkotason johdosta laitteiden vuokraaminen voi jopa olla omistamista halvempi vaihtoehto ja varsinkin suurilla volyymeillä kustannussäästöt voivat olla merkittäviä.

4.7 Mobiililaitehallinta

Markkinoilla on useita mobiililaitteiden hallintaan tarkoitettuja työkaluja. Näissä työkaluissa on jonkin verran eroavaisuuksia ominaisuuksien osalta, pääsääntöisesti kaikissa on samat perustoiminnallisuudet. Perustoiminnallisuuksiin voidaan lukea sovellusten asentaminen laitteille, laitteen pyyhkiminen varkaustapauksissa ja erilaisten käytäntöjen pakottaminen käyttäjä/laiteryhmäkohtaisesti. Työkaluja löytyy Microsoftilta (Intune/SCCM),

VMwarelta (Airwatch), Mobile Ironilta, IBM:ltä (Maas360), Citrix (XenMobile) ja niin edelleen. Kaikkiaan työkaluja löytyy sadoilta toimittajilta. Kuvassa 4 näkyy Gartnerin näkemys suurimpien toimijoiden suhteista toisiinsa.

Kuva 5. Gartner Magic Quadrant for Enterprise Mobility Management Suites 2016 (Gartner 2016)

Osa työkaluista on saatavilla SaaS-mallilla, osa on yrityksen omille palvelimille asennettavissa ja joistakin on saatavilla myös hybridijärjestelmiä. Toiset ovat saatavilla lisensointimielessä ”kaupanpäällisinä” jonkin lisenssipaketin mukana ja siten halvempia, kuin erikseen hankittavat. Toisissa lisenssimalleissa on erilaisia portaita, joissa saadaan alennuksia hankittavien lisenssimäärien mukaan – mitä enemmän ostetaan, sitä suurempi alennus saadaan. Joissakin hankitaan lisenssit omistukseen ja niiden päälle maksetaan ylläpidosta ja toisissa taas maksetaan pelkästään käytöstä ja ylläpito kuuluu hintaan.

Malli ja tuote on valittava omien tarpeiden mukaan. Tässäkin tulee miettiä myös tulevia tarpeita ja tehdä päätöksiä niiden perusteella. Tuotteesta toiseen vaihtaminen ei käy ihan käden käänteessä. Laitteilta on poistettava ensin nykyinen hallintaprofiili ja sen jälkeen liitettävä laite toisen hallintatuotteen piiriin. Nämä toimenpiteet eivät välttämättä kaikilta käyttäjiltä onnistu omatoimisesti.

Tällä hetkellä näyttää siltä, että laitehallinta kokonaisuudessaan on menossa enemmän ja enemmän UEM suuntaan, eli kaikkia mahdollisia päätelaitteita

hallittaisiin yhdellä keskitetyllä hallintatuotteella. Esimerkiksi Windows 10 tarjoaa saman MDM-rajapinnan, jota mobiililaitteissa on käytetty jo pidemmän aikaan. Sama rajapinta on ollut jo pidemmän aikaa Mac OS X-käyttöjärjestelmässä. Tämän rajapinnan kautta ei kuitenkaan ainakaan tällä hetkellä pystytä vielä suoraan toteuttamaan kaikkea sitä hallintaa, joka perinteisillä menetelmillä edelleen voidaan toteuttaa. Suunta on kuitenkin selvästi muuttumassa ja lieneekin ainoastaan ajan kysymys, kun kaikki hallinta tehdään MDM-rajapinnan kautta.

Asiakasyrityksessä käytiin läpi eri vaihtoehtoja mobiililaitehallintaa varten ja vertailtiin niiden ominaisuuksia ja kustannuksia. Näiden vertailujen jälkeen tehtiin valinta, hankittiin lisenssit ja aloitettiin käyttöönottoprojekti.

4.8 Sovellukset

Nykytilan kartoituksen perusteella saadaan tietoon ne sovellukset, jotka jo ovat käytössä. Näiden lisäksi tulisi pyrkiä tunnistamaan ne sovellukset, jotka tulevat käyttöön lyhyen ajan sisällä. Jos tätä ei kyetä tekemään, tulisi vähintäänkin määrittää se, minkälaisia sovelluksia jatkossa hyväksytään yrityksen mobiililaitteille. Eli tuleeko jokaisesta sovelluksesta olla natiivisovellus vai riittääkö web- tai hybridisovellus. Jos valitaan natiivisovellus, niin tehdäänkö aina suoraan kaikille alustoille vai pelkästään jollekin tietylle, sama koskee hybridisovelluksia. Joitakin sovelluksia voi olla mahdollista julkaista vaikkapa etätyöpöytäyhteyden kautta.

Jos mahdollista, kannattaa tässä kohtaa valita jokin malli, jota tullaan jatkossa käyttämään kaikissa tulevissa projekteissa ja vaatimaan vaikkapa järjestelmätoimittajia tuottamaan tietynlainen sovellus. Jos valitaan websovellus, ei tarvitse lukittua mihinkään tiettyyn laitteeseen tai käyttöjärjestelmään. Tosin tässä vaihtoehdossa saatetaan menettää osa laitteen mahdollisesti tuottamista hyödyistä, kuten osa rajapinnoista tai vaikkapa kiihtyvyysantureiden tuottamat tiedot.

4.9 Tukimallit

Mobiililaitteisiin ja niihin liittyviin sovelluksiin tulisi olla tarjolla tukea tavalla tai toisella. Kaikista helpoin käyttäjän kannalta olisi, jos tuki olisi saatavissa SPOC-mallin mukaisesti. Eli olipa ongelma tietokoneen, mobiililaitteen, sovelluksen tai jonkin muun asian kanssa, niin aina voisi ottaa yhteyttä yhteen ja samaan pisteeseen. Tämä tukipiste ottaa vastaan kaikki yhteydenotot ja välittää ne sitten eteenpäin taustalla oleviin tukipalveluihin. Tausta tiimit ratkaisevat ongelman ja toimittavat valmiin ratkaisun käyttäjälle.

Erilaisten tukimallien miettiminen on myös erittäin tärkeässä roolissa mobiilistrategiaa luotaessa. Tukimallin kokonaisuus riippuu hyvinkin paljon siitä, minkälainen laitekanta ja toimintapa laitteiden tarjoamiseen valitaan. Jos tarjotaan BYOD- tai CYOD-malleja saattavat tukikustannukset olla pienemmät, kuin yrityksen omistamien laitteiden osalta. Tähän vaikuttaa se, miten tuki BYOD- ja CYOD-mallien osalta rajataan. Voidaan rajata malli

niinkin suppeaksi, että BYOD- ja CYOD-laitteiden käyttäjät ovat laitteidensa osalta omillaan ja yritys tarjoaa tukea pelkästään sovellusten osalta. Jos sotketaan malleja keskenään esimerkiksi siten, että tietyille osastoille tarjotaan vaikkapa toista mallia kuin toisille, niin sitten alkaakin olla jo aikamoinen miettiminen myös tuen osalta. Ongelmaksi saattaa muodostua miten tukipiste erottaa käyttäjät toisistaan – kenelle mikäkin tuki kuuluu. Tämä on ongelma, varsinkin jos käytössä ei ole hyvää taustajärjestelmää joka on ajantasainen.

Jos ajatellaan paikasta ja ajasta riippumatonta työskentelyä, niin periaatteessa tuenkin pitäisi olla käytettävissä 24/7. Tästähän taas aiheutuu huomattavia kuluja ja jokin suppeampi tukimalli on monesti järkevämpi kustannus mielessä. Lisäksi erilaisten SLA-vasteiden määrittäminen voi olla hyvinkin raskas prosessi. On toki mahdollista hankkia koko paketti ulkoistettuna joltakin kumppanilta, joka hoitaa laitteiden elinkaarenhallinnan kaikilta osiltaan, myös tuen osalta.

4.10 Käytännöt

Yrityksellä tulisi olla myös erilaisia käytäntöjä ja ohjeistuksia. Jos näitä ei ole, ne tulee luoda mobiilistrategian yhteydessä.

Vähintäänkin jonkinlainen tietoturvakäytäntö olisi oltava. Tässä tulee määrittää, mitkä tiedot mobiililaitteissa tulee olla suojattuna ja kuinka ne suojataan. Lisäksi tulee määrittää, vaaditaanko laitteen salaaminen kokonaisuudessaan vai riittääkö pelkästään yrityksen tietojen salaaminen niiden sovellusten osalta, joissa niitä käsitellään. Määritettävä on myös, tuleeko laitteelle pääsyyn olla jonkinlainen tunnistautuminen ja niin edelleen. Tietoturvakäytäntöjä voi olla useita erilaisia, käyttäjäryhmille kohdistettuina tai yksi joka soveltuu kaikille. Joissakin tapauksissa on tarpeen tehdä tietoturvamielessä esimerkiksi yrityksen johdolle tiukempi tietoturvakäytäntö kuin työntekijöille. Tällöin saadaan paremmin suojattua yrityksen kannalta kriittiset tiedot. Tässäkin on toki pidettävä mielessä se, että yrityksen kannalta kriittistä tietoa voi olla aivan siellä kentällä työskentelevän työntekijänkin laitteessa. Eli tätä rajanvetoa voi olla hyvinkin hankala tehdä. Esimerkiksi jonkin asiakkaan ovikoodit voivat olla työntekijän mobiililaitteessa ja jos suojausta ei ole oikein toteutettu, ovat nämä kaikki tiedot varkaan saatavilla ja siten eteenpäin myytävissä. Tai myyjällä voi olla koko CRM-kanta laitteellaan ja ilman suojausta kaikki asiakastiedot ovat varkaan ulottuvilla.

Myös BYOD-käytäntö on oltava. Sen tulee minimissään täysin estää BYOD-laitteiden käyttäminen yrityksen tiedon käsittelyssä – jos näin halutaan määrittää. Tilanne jossa BYOD-käytäntö ja siihen liittyvät tekniset määritykset puuttuvat on kestämätön, koska käyttäjät tulevat varmasti käyttämään omia laitteitaan, ellei niiden käyttämistä ole teknisesti estetty.

Sellaisia käytäntöjä ei myöskään pidä tehdä, joita ei voida pakottaa. Lisäksi yrityksen johdon tulisi olla täysin sitoutuneita käytäntöjen mukaiseen toimintaan. Jos johdolla on erivapauksia ja tämä huomataan alemmissa portaissa, ei sielläkään tulla sitoutumaan määritettyihin käytäntöihin.

Asiakasyrityksen mobiilistrategiaprojektissa tehtiin ohjeet kaikille käytössä oleville alustoille: iOS, Android ja Windows Mobile. Ohje pitää sisällään laitteen liittämisen mobiililaitehallintaan ja Outlook-applikaation määrittämisen sähköpostia varten.

4.11 Prosessit

Mobiilistrategian tulisi tuottaa myös prosesseja erilaisia tapauksia varten. Tällaisia ovat muun muassa prosessit, kuinka toimitaan, jos laite katoaa tai se varastetaan, käyttäjä lähtee talosta tai miten uusi laite otetaan käyttöön. Edellä mainitut prosessit voivat erota toisistaan sen mukaan, onko käytössä yrityksen omistamat, BYOD- ja CYOD-mallin mukaiset laitteet.

4.12 Tulevaisuus

Mobiililaitteet ovat kehittyneet viime vuosina hurjaa vauhtia. Sellaisia laitteita, joita ei ollut vielä muutamia vuosia sitten, on alkanut putkahdella markkinoille. Esimerkiksi virtuaalilasit ovat tuomassa uusia ulottuvuuksia erilaisiin suunnittelutehtäviin. Niillä voi vaikkapa tutustua rakenteilla olevaan kotiin tai matkustaa ympäri maailman omalta kotisohvalta. Älykellot ovat myös ottaneet suuren harppauksen muutaman vuoden aikana. Näiden avulla voidaan lukea vaikkapa sähköpostia suoraan ranteesta tai asiakkaalle siirryttäessä käyttää navigointia suoraan kellon kautta. Lisää sovelluksia ja erilaisia käyttökohteita löydetään jatkuvasti.

Kaikki nämäkin laitteet ja niiden mahdolliset variaatiot tulisi jollain aikavälillä saada hallintaan ja ottaa osaksi yrityksen mobiilistrategiaa. Jos näitä ei huomioida tai muutoin ole yrityksen tietoja suojattu, tarjoavat nämäkin laitteet mahdollisuuden tietojen menettämiseen.

Yksi suuri muutos, joka varmasti vaikuttaa myös yritysten erilaisiin strategioihin – myös mobiilistrategiaan – on uusi EU:n yleinen tietosuoja-asetus. Uusi asetus on 14.4.2016 hyväksytty lopullisesti Euroopan parlamentin ja neuvoston päätöksillä ja se astuu voimaan 25.5.2018. Tästä aiheutuu monissa tapauksissa suuria muutoksia sille, miten ja missä tietosuoja-aineistoa käsitellään. Suurimpana ”motivaattorina” uudessa tietosuoja-asetuksessa on sen rikkomisesta seuraava sakko. Sakko on suurimmillaan jopa 4% yrityksen globaalista vuoden liikevaihdosta tai 20M€, riippuen siitä kumpi on suurempi. Eli jos yrityksen globaalista vuotuisesta liikevaihdosta 4% on yli 20M€ sakko määräytyy tämän mukaan ja jos alle, niin sakko on 20M€. Tämä on suurin sakko, joka voidaan määrätä kaikkein vakavimmista tietosuoja-asetuksen rikkomisista. Kun taas puhutaan pienemmistä rikkomuksista, sakko on 2% yrityksen globaalista vuoden liikevaihdosta. Tällöin kyseessä voi olla esimerkiksi tilanne, jossa rekisterit eivät ole ajan tasalla tai ilmoitusvelvollisuus valvontaviranomaiselle ja rekisteröidylle mahdollisessa tietosuojaluokkauksessa on laiminlyöty. Ilmoitusvelvollisuus tietosuojaloukkauksissa on 72 tuntia siitä, kun loukkaus on tapahtunut. Puhutaan siis todella suurista summista, joilla voi olla suuria – jopa katastrofaalisia vaikutuksia yrityksen toimintaan. Pahimmillaan tämä voi johtaa jopa yri-

tystoiminnan loppumiseen. Mobiilistrategian kannalta tämä tulisi huomioida tietojenkäsittelyn ja suojaamisen osalta. Ne tiedot ja laitteet, joilla tietosuoja-asetuksen mukaista tietoa käsitellään, tulee suojata niin, että tietosuojaluokkauksia ei pääse syntymään. Tietosuoja-asetus vaikuttaa myös siihen, minkälaista tietoa yritys saa asiakkaistaan kerätä ja ketkä näitä tietoja saavat käsitellä. Asetus tuo uusia oikeuksia myös asiakkaille. Kaikkien näiden huomioiminen ja järjestelmien muuttaminen voi aiheuttaa suuria kustannuksia ja nämä olisi syytä huomioida vuosibudjettien suunnittelussa tulevalle sekä seuraavalle vuodelle. Jos asioihin ei vielä olla alettu panostaa, nyt alkaa olla jo todella kiire, asetuksen voimaan astumiseen on aikaa tällä hetkellä noin 550 päivää ja se ei ole paljon näin suuressa muutoksessa.

5 YHTEENVETO

Opinnäytetyön tavoitteena oli rakentaa mobiilistrategian pohja yritysten käyttöön. Pohjaa hyödynnettiin myös asiakasyrityksen mobiilistrategiaprojektissa. Strategiatyötä ohjasi vahvasti uuden toiminnanohjausjärjestelmän käyttöönottoprojekti, jonka yhteydessä mobiililaitteille asennettavalla sovelluksella kentällä työskentelevät henkilöt pystyvät ottamaan vastaan uusia töitä sekä kirjaamaan tehtyjä töitä reaaliaikaisesti. Sovelluksen jakelua sekä päivittämistä ja myös laitteiden suojaamista varten, oli tarve saada käyttöön myös jokin MDM- / EMM-järjestelmä. Tästä syntyi ajatus, että olisi ehkä hyvä tässä kohtaa määritellä myös mobiilistrategia, jolla voidaan jatkossa helpottaa kaikkea yrityksen mobiililaitteisiin tai mobiilisovelluksiin liittyviä päätöksiä sekä tehdä ylätason linjaukset mobiiliasioihin liittyen.

Lähtötilannetta voisi lyhykäisyydessään kuvata sanalla katastrofaalinen, käytössä ei ollut mitään mobiilistrategian elementtejä. Ei minkäänlaista mobiililaitteiden hallintajärjestelmää, ei minkäänlaista käyttöomaisuudenhallintaa mobiililaitteiden osalta, eikä mitään prosesseja miten eri tilanteissa toimitaan ja niin edelleen. Hyvinkin pienillä asioilla asiat siis olivat muutettavissa huomattavasti parempaan suuntaan.

Työn edistyessä selvisi myös se, että nykytilanteesta hyvään ja hallittuun malliin siirtyminen vaatii hyvinkin suuria ponnisteluja ja pitkäjänteistä työtä muutoksen saavuttamiseksi. Laitteita on tällä hetkellä kentällä kuitenkin useita tuhansia ja kenelläkään ei ole selkeää kuvaa näiden laitteiden elinkaaren tilanteesta. Strategian määrittelyn jälkeen suurimpana tehtävänä on strategian jalkauttaminen ja siihen kirjattujen toimenpiteiden ja määritysten seuraaminen. Aivan perus prosessejakin täytyy tuottaa huima määrä ja ne on saatava käyttöön mahdollisimman nopeasti tilanteen oikaisemiseksi. Projekti on edennyt tällä hetkellä vaiheeseen, jossa mobiilistrategia on lähestulkoon valmiina ja mobiililaitehallinta on jo osittain käyttöönotettuna. Käyttöönottoa edelsi eri järjestelmien kartoittaminen. Kartoituksen perusteella pyydettiin tarjoukset ensin kolmen eri järjestelmän valmistajilta. Tämän jälkeen valitun järjestelmän käyttöönottoa toteuttaviin kumppaneihin oltiin yhteydessä ja pyydettiin käyttöönotosta tarjoukset. Valitun kumppanin kanssa käyttöönotto aloitettiin elokuussa 2016 ja ensimmäiset laitteet olivat hallinnan piirissä noin kaksi viikkoa käyttöönottoprojektin aloittamisesta. Myöskin MAM-käytäntöjä on otettu käyttöön ja ne ovat kohdistettuina kaikkiin tällä hetkellä MDM-hallinnan piirissä oleviin laitteisiin, niiden sovellusten osalta, jotka näitä käytäntöjä tukevat. Lisäksi on olemassa pilottikäyttäjiä varten omat MAM-käytännöt, jotka voidaan kohdistaa käyttäjiin ja laitteisiin, ilman että laitteita tarvitsee liittää MDM-hallinnan piiriin. Erilaisia prosesseja on myös tuotettu useampia ja niistä osa on myös jalkautettu. Projekti onkin siis vielä suhteellisen alussa ja sen lopulliset tulokset ovat nähtävissä todennäköisesti vasta muutaman vuoden kuluttua.

Kaikkiin alussa asetettuihin kysymyksiin löydettiin vastaukset. Ehkä tärkeimpänä johtopäätöksenä voitaisiin nähdä, että mobiilistrategian tulisi olla mahdollisimman joustava. Se on erittäin tärkeää laatia mahdollisimman aikaisessa vaiheessa tai se voi johtaa suuriin ongelmiin. Näiden ongelmien

korjaaminen myöhemmissä vaiheissa on hyvinkin vaikeaa ja kallista. Jos strategiaa ei haluta jostain syystä laatia, niin vähintäänkin tulisi määrittää käytännöt ja prosessit joiden mukaan toimitaan. Käytännöt ja prosessit tulisi myös jalkauttaa ja niiden käyttöä tulisi seurata. Mobiililaitteidenhallintajärjestelmällä on suuri rooli tietoturvanäkökulmasta. Se miten tietoturvaa järjestelmän avulla toteutetaan, onkin sitten aivan eri kysymys. Tätä kysymystä tulee miettiä monelta kantilta ennen kuin päätöstä tehdään ja kannattaa myös huomioida mahdolliset tulevat tarpeet. On helpompi jättää useampia vaihtoehtoja käyttöön, kuin päätyä yhteen ja yrittää sitten myöhemmin tehdä muutoksia.

Mobiilistrategiaan on myös hyvinkin paljon erilaisia tulokulmia, joiden kautta asioita voi lähteä miettimään ja työstämään. Yleensä paras lopputulos saavutetaan, kun keskiöön asetetaan käyttäjä ja tämän ympärille rakennetaan kaikki tarvittava. Yhtä ja samaa mallia ei voida käyttää eri yritysten välillä, vaan kaikkien on luotava oma mallinsa omien tarpeidensa perusteella. Optimaalinen mobiilistrategia tarjoaa käyttäjille kaikki laitteet ja sovellukset käyttöön helposti ja nopeasti tietoturvaa unohtamatta.

Olemassa olleen kokemuksen ja osaamisen päälle tuli vielä roppakaupalla uutta työn edistyessä. Monia erilaisia uusia näkemyksiä on nyt repussa ja tulevaisuutta silmällä pitäen tästä harjoituksesta, oli varmasti monessakin mielessä paljonkin hyötyä.

LÄHTEET

Android developers, (2016). Dashboards. Haettu 7.10.2016 osoitteesta https://developer.android.com/about/dashboards/index.html#Screens

Apple, (2016). MacOS Deployment Reference. Haettu 19.10.2016 osoitteesta https://help.apple.com/deployment/macos/#/ior07301dd60

Callahan, R., (2014). Characteristics of Mobile Devices. Haettu 13.7.2016 osoitteesta https://www.techwalla.com/articles/characteristics-of-mobile-devices

F-Secure, (2016). Suojautuminen nykyaikaisilta tietoturvauhilta. Webinaari 21.10.2016, Atea Finland

Gartner, (2012). *CIO's Next-Generation Mobile Strategy Checklist*. Haettu 30.10.2016 osoitteesta https://www.gartner.com/doc/1998618/cios-next-generation-mobile-strategy-checklist

Gartner, (2016). Magic Quadrant for Enterprise Mobility Management Suites. Haettu 16.8.2016 osoitteesta https://www.gartner.com/doc/reprints?id=1-390IMNG&ct=160608&st=sb

Hietamäki, A., (2016). 6 keinoa, joiden avulla lisäät työtehoa ja onnellisuutta it-päätöksillä. Haettu 29.10.2016 osoitteesta https://www.3stepit.com/fi/blog/6-keinoa-lisata-tyotehoa-it-paatoksilla/

IDC, (2016). Securing productivity in the borderless enterprise. Haettu 12.7.2016 osoitteesta https://info.microsoft.com/EMS-SecuringProductivityintheBorderlessEnterprise.html?ls=Blog&lsd=BA-series

IDC, (2016a). *Smartphone OS Market Share, 2016 Q2*. Haettu 1.10.2016 osoitteesta http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Jordan, E., Silcock L., (2006). *Strateginen IT-riskien hallinta* Helsinki: Edita

Jääskeläinen, T., (2016). BYOD, CYOD ja firman laitepolitiikka. Haettu 30.10.2016 osoitteesta http://blogi.mpy.fi/byod-cyod-ja-firman-laitepolitiikka

Kostamo E, (1999). *Strateginen ajattelu, selviydy tietoyhteiskunnassa*. Helsinki: Multiprint

Lindroos J., Lohivesi K, (2004). *Onnistu strategiassa* 2. painos. Juva: WS Bookwell

Microsoft, (2015). Mobile device management design considerations guide. Haettu 13.5.2016 osoitteesta https://gallery.technet.microsoft.com/Mobile-Device-Management-

7d401582/file/141695/1/MDM%20Design%20Considerations%20Guide%20V2.pdf

Microsoft, (2016). Intune datasheet. Haettu 18.7.2016 osoitteesta http://download.microsoft.com/download/4/b/f/4bf2842c-2b15-44e5-87b4-2c2949a81de9/microsoft_intune_datasheet.pdf

Microsoft, (2016a). Manage Windows 10 in your organization – transition to modern management. Haettu 20.7.2016 osoitteesta https://technet.microsoft.com/en-us/itpro/windows/manage/manage-windows-10-in-your-organization-modern-management

Microsoft, (2016b). Hybrid mobile device management (MDM) with System Center Configuration Manager and Microsoft Intune. Haettu 7.10.2016 https://docs.microsoft.com/en-us/sccm/mdm/understand/hybrid-mobile-device-management

Nieminen, P., (2014). *Digitaali- ja mobiilistrategia liiketoiminnan tuottavuuden kehittäjänä*. Haettu 16.7.2016 osoitteesta http://www.slideshare.net/niemipet/mobiilistrategia

Nieminen, P., (2015). *Digitalisaatio ja mobiliteetti toiminnan kehittäjänä*. Haettu 17.7.2016 osoitteesta http://www.slideshare.net/niemipet/digitalisaatio-ja-mobiliteetti-toiminnan-kehittjn

Oliver, M., (2008). Mobile device management for dummies. Haettu 12.6.2016 osoitteesta http://www.club-cmmc.it/lettura/mobile.pdf

Ponemon Institute, (2015). The state of mobile application insecurity. Haettu 19.10.2016 osoitteesta https://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03074usen/WGL03074USEN.PDF

Smith, D., (2016). iOS Version Stats. Haettu 11.10.2016 osoitteesta https://david-smith.org/iosversionstats/

Tech Times, (2016). Only Nexus and Samsung Android smartphones are safe to use, security firm says. Haettu 16.7.2016 osoitteesta http://www.techtimes.com/articles/168332/20160704/only-nexus-and-samsung-android-smartphones-are-safe-to-use-security-firm-says.htm

Vikkula, K., (2013). Tietotekniikan kuluttajistuminen haastaa työnantajat. Haettu 15.9.2016 osoitteesta http://www.talouselama.fi/tebatti/tietotekniikan-kuluttajistuminen-haastaa-tyonantajat-3356450

Vuorinen, C., (2014). Kolme tapaa kehittää mobiilisovellus. Haettu 15.9.2016 osoitteesta http://w3.fi/kolme-tapaa-kehittaa-mobiilisovellus/

Liite 1

Laitekartoitus lomake

LAITEKARTOITUS LOMAKE

Päivämäärä:
Vastaaja:
Käyttäjäryhmä jota kartoitus koskee:
Käytössä olevat laitteet:
- **Merkki:**
- **Malli:**
- **Käyttöjärjestelmä:**
- **Määrä:**

Laitteiden käyttötarkoitus:

Käytössä olevat sovellukset:

Käyttäjien työroolit:

Muuta huomioitavaa:
(käytettävien sovellusten vaatima käyttöjärjestelmä, erityisvaatimuksia kameralle, salama tms.)

NYKYTILANKARTOITUS LOMAKE

Päivämäärä:
Tekijä:

Laitteet (jos useampia laitteita, kopioi alla olevaa osiota)

Merkki:
Malli:
Käyttöjärjestelmä:
Määrä:
Omistajuus: ☐ **Yrityksen** ☐ **CYOD** ☐ **BYOD**

Sovellukset (jos useampia sovelluksia, kopioi alla olevaa osiota)

Sovellukseni nimi:
Sovelluksen tyyppi: ☐ **Natiivi** ☐ **Hybridi** ☐ **Web**
Käyttöjärjestelmä jolla toimii: ☐ **Android** ☐ **iOS** ☐ **Windows Mobile**

Käyttäjäprofiilit

Sovellusmatriisi:

Käyttäjäprofiilit	*Sovellus 1*	*Sovellus 2*	*Sovellus 3*	*Sovellus 4*	*Sovellus 5*
Profiilli 1					
Profiili 2					
Profiili 3					
Profiili 4					
Profiili 5					

Laitematriisi:

Käyttäjäprofiilit	Laite 1	Laite 2	Laite 3	Laite 4	Laite 5
Profiilli 1					
Profiili 2					
Profiili 3					
Profiili 4					
Profiili 5					

Järjestelmät joihin tarvitaan pääsy mobiililaitteilla:

Nykyiset kyvykkyydet pääsynhallintaan ja -valvontaan:

Nykyiset käytännöt ja prosessit:

Riippuvuudet muihin strategioihin / vaikutus muihin strategioihin

Strategia johon vaikuttaa:

Strategia joka vaikuttaa:

Muuta huomioitavaa: