LAPIN AMK
Lapland University of Applied Sciences

ORGANISAATION MOBIILILAITTEIDEN HALLINTASTRATEGIA

Tapio M. Nykänen

Opinnäytetyö
Tekniikka ja liikenne
Tietotekniikan koulutusohjelma
Insinööri (AMK)

2015

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tekniikka ja liikenne
Tietotekniikan koulutusohjelma

Tekijä Tapio M. Nykänen Vuosi 2015
Ohjaaja Kenneth Karlsson
Toimeksiantaja LapIT Oy
Työn nimi Organisaation mobiililaitteiden hallintastrategia.
Sivu- ja liitemäärä 22 + 1

Tässä opinnäytetyössä raportoidaan mobiililaitteiden hallintastrategian laatimisen avuksi tehdyn ohjeen toteuttaminen toimeksiantona. Toimeksiantaja on rovaniemeläinen LapIT Oy. Ohje on tarkoitettu LapIT Oy:n asiakasorganisaatioiden tieto- ja viestintätekniikasta vastaavalle henkilöstölle.

Opinnäytetyössä avataan käytettävinä käsitteinä organisaatio, mobiililaite sekä hallintastrategia. Teoreettisessa osassa käsitellään mobiililaitteiden hallintastrategian osa-alueina määrittely, turvallisuuskäytännöt, laitehallinta ja tuki sekä oman laitteen käyttö. Työssä myös kuvataan toimeksiannon toteutusta valmistelusta lähtien aina tuotokseen asti.

Toimeksiantona tehty ohje mobiililaitteiden hallintastrategian laatimiseen sisältää aihepiiriin liittyvien lyhenteiden selittämisen, mobiililaitteiden hallintastrategian (MDM) määrittelyn, turvallisuuskäytännöt, laitehallinnan ja tuen sekä oman laitteen käytön. Laitehallinta ja tuki on jaettu hallintajärjestelmän valintaan ja elinkaareen.

Asiasanat mobiililaitteet, hallintastrategia, tietoturva, laitehallinta, elinkaari, BYOD

Abstract of Thesis

LAPIN AMK
Lapland University of Applied Sciences

School of Technology, Communication and Transport
Information Technology Programme

Author Tapio M. Nykänen Year 2015
Supervisor Kenneth Karlsson
Commissioned by LapIT Oy
Subject of thesis Organization's mobile device management strategy.
Number of pages 22 + 1

The subject of this thesis was an organization's mobile device management strategy. The goal was to create a guide for developing the management strategy, which the commissioner could use with their customers. During the research, the main focus was on the contents of the mobile device management strategy and the common best practices. While creating the guide itself, much attention was also paid on the legibility and the layout of the guide.

The research was done by comparing different articles and publications about the subject, searching for the recurring themes and procedures. These best practices were then collected and presented in the guide in an easy to understand way, so that the guide would be useful even if the reader was not an expert in information technology.

The subject for the thesis was chosen based on the commissioner's need for a tool to help their customers with their mobile device management. Enterprise mobility is a globally growing trend, so this was a very topical subject that has not yet been studied too much, though that will most likely change in the future. This thesis helps the commissioner's research and development of enterprise mobility.

Key words mobile devices, management strategy, information security, device management, life cycle, BYOD

SISÄLLYS

1 JOHDANTO

Suoritin ensimmäisen ammattikorkeakouluopintoihini liittyvän harjoittelun LapIT Oy:llä elokuussa 2012. Harjoittelun jälkeen, saman vuoden joulukuussa, minulle tarjottiin palkallista harjoittelijan toimea, minkä jälkeen olen ollut lähes katkeamattomasti työsuhteessa LapIT:llä. Tästä syystä oli luonnollista, että työnantajastani tulisi opinnäytetyön toimeksiantaja.

Tämän opinnäytetyön tuloksena on tarkoitus tuottaa ohje, jota toimeksiantajan asiakasorganisaatiot voivat käyttää apunaan mobiilipäätelaitteiden hallintastrategiaa suunnitellessaan. Ohjeen lisäksi opinnäytetyössä tutustutaan mobiilipäätelaitteiden hallintaan ja sen merkitykseen yritysmaailmassa. Työssä käydään läpi mobiililaitteiden hallintastrategiaan liittyviä tärkeitä ja yleisesti hyväksi koettuja käytäntöjä.

Tutkimusaineistona työssä on käytetty enimmäkseen Internetistä löytyvää mobiililaitteiden hallintaan liittyvää aineistoa. Lisäksi työn aikana on käyty keskusteluja toimeksiantajan työntekijöiden kanssa ohjeen toteutukseen liittyen. Työssä kiinnitetään erityistä huomiota ohjeen luettavuuteen. Yksi iso haaste on kirjoittaa ohjeesta riittävän kattava, mutta toisaalta selkeä, jotta lukijalle olisi siitä mahdollisimman paljon hyötyä.

Mobiilipäätelaitteiden määrä organisaatioissa kasvaa jatkuvasti. Sen lisäksi, että työntekijöille tarjotaan matkapuhelimet työkäyttöön, myös tablettien määrä yrityskäytössä lisääntyy. Enää ei voida vain hankkia uusia laitteita ja jakaa niitä työntekijöille, vaan organisaatiolla pitää olla suunniteltuna strategia, jonka avulla laitteita hallitaan. Organisaation on määritettävä millainen on laitteen elinkaari, mistä ja miten laitteet hankitaan ja kuinka ylläpidetään tarvittavat sovellukset. On tärkeää huomioida, miten tarvittaessa toteutetaan laitteen huolto sekä miten järjestetään riittävä tietoturva.

Opinnäytetyön tavoitteena on aikaansaada ytimekäs ohje, jonka avulla organisaatio voi laatia oman hallintastrategian mobiilipäätelaitteita varten. Tarkoitus ei

ole ottaa kantaa esimerkiksi siihen, minkä valmistajan laitteita tai virustorjuntaohjelmaa organisaatio tulee käyttämään. Ohje esittää organisaatiolle kysymyksiä, joihin vastaamalla organisaatio voi itse luoda strategian.

2 TOIMEKSIANNON TAUSTAA

LapIT Oy on rovaniemeläinen vuonna 2000 perustettu IT-palveluja ja -konsultointia tarjoava yritys, joka työllistää Lapissa yli 70 henkilöä toimipisteillään Rovaniemellä, Kuusamossa, Kemijärvellä, Taivalkoskella, Ivalossa, Pellossa sekä Ylitorniolla. Yritys on pohjoissuomalaisten kuntakonsernien omistama. Suurimpia omistajia ovat Rovaniemen, Kuusamon ja Kemijärven kaupungit sekä Lapin sairaanhoitopiirin kuntayhtymä. LapIT Oy tuottaa asiakkailleen sovellus-, infra-, ja palvelupistepalvelua sekä lähitukipalvelua ja päätelaitteiden hallintapalvelua. (LapIT Oy 2015.) Tämä opinnäytetyö keskittyy näistä palveluista päätelaitteiden hallintapalveluihin.

Päätelaitteiden hallintapalvelut -yksikkö perustettiin vuonna 2014. Yksikkö tuottaa mm. elinkaarenhallintapalvelua, joka pitää sisällään laitteiden hankinnan, esiasennukset ja toimitukset, laiterekisterien ylläpitämisen sekä laitteen tietoturvallisen käytöstä poistamisen. Vuonna 2014 elinkaarenhallintapalveluun otettiin mukaan mobiilipäätelaitteet. (LapIT Oy 2014.)

Näiden muutosten jälkeen opinnäytetyön aihetta tarjottiin Päätelaitteiden hallintapalveluista. Mobiilipäätelaitteiden elinkaarenhallintapalveluun liittymisen myötä yksikön palvelupäälliköllä oli tarjolla toimeksiantona mobiililaitteiden hallintastrategian ohjeistuksen laatiminen. Alkuperäisenä tavoitteena oli kirjoittaa ohje, jonka perusteella LapIT:n asiakkaat voisivat luoda itselleen strategian, johon perustuen he sitten ostaisivat palveluita edelleen LapIT:ltä. Asiakasorganisaatioissa ohjetta lukisivat pääosin asiakkaan tietohallinnosta vastaavat henkilöt. Ohjetta kirjoittaessa on huomioitava lukijoiden vaihteleva tekninen osaaminen.

3 YLEINEN TIETOPERUSTA JA KÄSITTEET

3.1 Organisaatio

Organisaatio voidaan määritellä ryhmäksi ihmisiä, jotka työskentelevät yhdessä saavuttaakseen saman päämäärän. Toiminta vaatii onnistuakseen yhdessä sovittuja toimintatapoja ja sääntöjä (Mäkinen 2003). Tässä opinnäytetyössä organisaatiolla tarkoitetaan LapIT Oy:n asiakkaita tai niihin verrattavia tahoja. LapIT:n asiakasorganisaatioita voivat olla kunta- tai pk-sektorin, julkishallinnon sekä terveydenhuollon toimijat (LapIT Oy 2015). Työtä ei kuitenkaan kohdisteta mihinkään tiettyyn asiakkuuteen, vaan työn tuotos on kaikkien asiakkaiden ja asiakkaiksi haluavien hyödynnettävissä.

3.2 Mobiililaite

Opinnäytetyössä mobiilipäätelaitteista käytetään lyhempää ja käyttäjäystävällisempää termiä *mobiililaitteet*. Valtiovarainministeriön (2013) julkaisemassa Päätelaitteiden tietoturvaohjeessa päätelaitteet määritellään ’laitteiksi, joilla käytetään organisaation tietoja jotka ovat päätelaitteella, sähköisissä tietojärjestelmissä tai muissa palveluissa’. Päätelaitteita ovat sekä perinteiset pöytätyöasemat, kannettavat tietokoneet kuin älypuhelimet ja taulutietokoneet eli tabletit.

Mobiililaitteilla tarkoitetaan tässä työssä nimenomaan älypuhelimia ja tabletteja. Terminä *mobiili* viittaa liikkuvuuteen, joten sen perusteella myös kannettava tietokone tulisi laskea mobiililaitteisiin. Mobiiliopas (2011) määrittelee mobiililaitteet sellaisiksi laitteiksi, joilla pääsee tietoverkkoon ajasta ja paikasta riippumatta.

LapIT Oy ei luokittele kannettavia tietokoneita mobiililaitteiksi, vaikka ne periaatteessa siihen kategoriaan sopisivat. Toisin kuin kannettavat tietokoneet, puhelimia ja tabletteja ei liitetä osaksi yrityksen toimialuetta. (Lisko 2015.) Työn tuloksena oleva ohje on laadittu tästä näkökulmasta, mutta mikään ei estä lukijaa soveltamasta ohjetta halutessaan myös kannettaviin tietokoneisiin, mikäli se sopii paremmin oman organisaation toimintaan.

Kannettavien tietokoneiden erottelu mobiililaitteista toimialueeseen liittämisellä perustellen on jo nyt osoittautumassa ongelmalliseksi. Windows 8 -käyttöjärjestelmällä toimivia tabletteja on ollut markkinoilla jo vuosia, ja ne on mahdollista nostaa toimialueelle. Windows 10 -käyttöjärjestelmän myötä markkinoille on tulossa myös puhelimia, jotka on mahdollista liittää toimialueelle.

3.3 Hallintastrategia

Riitta Viitalan (2007) mukaan strategia on ymmärrettävissä rationaalisena strategia-ajatteluna, johdonmukaisena toimintamallina tai keinovalikoimana. Tämän työn tuotoksena tuleva ohje organisaation mobiililaitteiden hallintastrategian laatimiseen keskittyy erityisesti Viitalan (2007) määritelmään strategiasta johdonmukaisena toimintamallina sekä yrityksen tapana toimia mobiililaitteiden kanssa. Samansuuntaisesti Harri Sjöholm (2006) toteaa organisaation hyötyvän teknologiastrategiasta sisäisen tietoisuuden lisäämisessä.

Mobiililaitteiden hallintastrategiassa (mobile device management strategy eli MDM-strategia) organisaatio määrittelee toimintatapansa, joilla mobiililaitteita hallitaan. Hallintastrategian osa-alueina opinnäytetyössä käsitellään mobiililaitteiden hallintastrategian määrittelyä, turvallisuuskäytäntöjä sekä laitehallintaa ja -tukea. (Grey 2011.) Tarkemmin MDM-strategiaa avataan seuraavassa luvussa.

4 MOBIILILAITTEIDEN HALLINTASTRATEGIA

4.1 Määrittely

Greyn (2011) mukaan hallintastrategiassa tulee määritellä, millaiseen organisaatioon strategiaa ollaan luomassa. Hän listaa määriteltävät asiat kysymysmuotoon seuraavasti:

- Millaisia työntekijöitä?
- Millaisia laitteita?
- Mitä käyttöjärjestelmiä?
- Mitä sovelluksia?
- Millainen tietoturva?
- Kuinka tietotekniikkaa hallitaan?
- Kuka maksaa?

(Grey 2011)

Määrittelemällä ylläolevat asiat organisaatio luo strategialleen lähtökohdat. Samalla strategian laatija muodostaa itselleen käsityksen organisaation ympäristöstä ja tekee valintoja, joilla pyrkii strategialle asetettuihin tavoitteisiin.

4.2 Turvallisuuskäytännöt

Valtiovarainministeriö (2013) listaa erilaisia mobiililaitteisiin kohdistuvia uhkia ja hyökkäystapoja, joihin kuuluu mm. käyttäjän huijaaminen asentamaan haitallisia ohjelmia laitteilleen, laitteiden luvaton käyttäminen varastetuilla tunnuksilla sekä laitteen katoaminen ja varastaminen. Torjuakseen ja vähentääkseen uhkien toteutumista organisaation täytyy tiedostaa tietoturvariskit, joille mobiililaitteet sen toiminnassa altistuvat.

Riskikartoituksen jälkeen on luotava säännöt ja ohjeistus siitä, miten organisaatiossa toimitaan tietoturvallisen toiminnan ylläpitämiseksi sekä riskien toteutuessa. Valtiovarainministeriö (2013) suosittelee mobiililaitteiden hallintaohjelmis-

ton käyttöä. Markkinoilla on useita tuotteita, joiden avulla organisaation mobiililaitteita voidaan hallita keskitetysti. Mobiililaitteiden hallintaohjelmistoja käsitellään myöhemmin.

Mobiililaitteiden hallintastrategiassa organisaatio määrittää, miten laitteet suojataan luvattoman käytön varalta. Perinteisimpiä toimintatapoja ovat salasanakäytännöt ja laitteiden massamuistien salaaminen. Nämä keinot ovat ikään kuin tietoturvan etulinjana. Salasana suojaa laitteen tiettyyn pisteeseen asti, mutta organisaation täytyy seurata turvallisten salasanojen kehitystä. Tänä päivänä riittävän monimutkaisena ja turvallisena pidetty salasana ei enää vuoden päästä välttämättä ole sitä. On tärkeää, että organisaatiossa seurataan tietoturvauutisia ja teknologian kehitystä.

Sen lisäksi, että estetään fyysinen pääsy laitteelle salasanoilla ja salausohjelmilla, myös verkon kautta tapahtuvat tietomurrot on pyrittävä estämään. Käyttäjän on mahdollista asentaa laitteelleen sovelluksia, joiden lähteen luotettavuudesta ei voida olla varmoja. Organisaation on estettävä tällainen toiminta. Mikäli sovellusten asennusta ei ole mahdollista estää teknisesti, se on syytä kieltää hallintastrategiassa. Puhelimien turvallisuusasetuksista on mahdollista kytkeä päälle asetus, jolla estetään sellaisten sovellusten asentaminen joita laitevalmistaja ei ole tunnistanut luotetuiksi. Esimerkiksi Sophoksen (2013) mallistrategiassa yksiselitteisesti kielletään muiden kuin laitevalmistajan hyväksymien sovellusten asentaminen. Kun jotain kielletään, on myös syytä määritellä seuraamukset kiellon rikkomiselle.

4.3 Laitehallinta ja tuki

Grey (2011) kehottaa kiinnittämään mobiililaitteiden hallintastrategiaa suunniteltaessa huomiota laitehallinnan ja tuen määrityksiin. Erityisesti laitteiden hankinta- ja huoltoprosessien sekä laitteiden hallinnan suunnittelu on tärkeää. Käytännössä organisaatio voi tehdä tämän kaiken itse, tai vaihtoehtoisesti ulkoistaa mobiililaitteiden hallinnan elinkaarenhallintapalveluita tarjoavalle yritykselle.

Miten organisaatio tuleekaan toteuttamaan laitteiden hallinnan ja tuen, käyttäjien ohjeistaminen on organisaation vastuulla. Hallintastrategian avulla organisaatio linjaa ja tuo tiedoksi käyttäjille mobiililaitteiden hallinnan vastuujaon. Näin organisaation sisällä on selvillä, kenen puoleen käännytään esimerkiksi kun mobiililaite on lakannut toimimasta tai käyttäjän tehtävät muuttuvat ja hän tarvitsee uusia sovelluksia laitteelleen. Mobiililaitteiden hallintajärjestelmällä on suuri merkitys mobiililaitteiden hallintastrategiassa.

4.4 Oman laitteen käyttö

Udo Waibel (2014) tuo artikkelissaan esille Enterprise Management Associatesin (EMA) analyytikoiden arvion, että nykypäivänä yritysten älypuhelimista 58 prosenttia on käyttäjien omistamia. Artikkelista ei käy ilmi, kattaako EMA:n tutkimus yritykset maailmanlaajuisesti vai ainoastaan Yhdysvalloissa. Oletettavasti voidaan arvioida, että trendi on sama Euroopassa.

Organisaation työntekijöiden omien laitteiden käytöstä on hyötyä sekä organisaatiolle, että työntekijöille (taulukko 1). Huomattavin hyöty lienee työtekijöiden tyytyväisyys, kun heidän ei tarvitse opetella ylimääräisten laitteiden käyttöä.

Taulukko 1. Omien laitteiden käytön mahdolliset edut ja huomioitavat asiat (mukaillen Technology Conference & Expo 2013).

Mahdolliset edut	**Huomioitavaa**
Kustannusten hallinta	Turvallisuus ja sääntöjen noudattaminen
Työntekijöiden tyytyväisyys	Hallinnan puute
Teknologian omaksuminen	Ylimääräisen tuen tarve
Useampia käyttöjärjestelmiä	Yksityisyys
Tuottavuuden lisääminen	Yhteensopivuus
Laajempi mobiilin käyttöönotto	Tiedon häviäminen/vuotaminen
	Työntekijä omistaa laitteen

Omien laitteiden käyttö tuo mukanaan huomioitavia asioita. Koska organisaatio ei omista laitteita, on niiden hallitseminen haastavaa. On tärkeää, että organisaation tietoturvaohjeistukset ovat työntekijöiden tiedossa ja niitä noudatetaan. Organisaatio voi ottaa omien laitteiden käyttöön kantaa mobiililaitteiden hallintastrategiassa niin sanotulla BYOD-politiikalla (Bring your own device, tuo oma laitteesi).

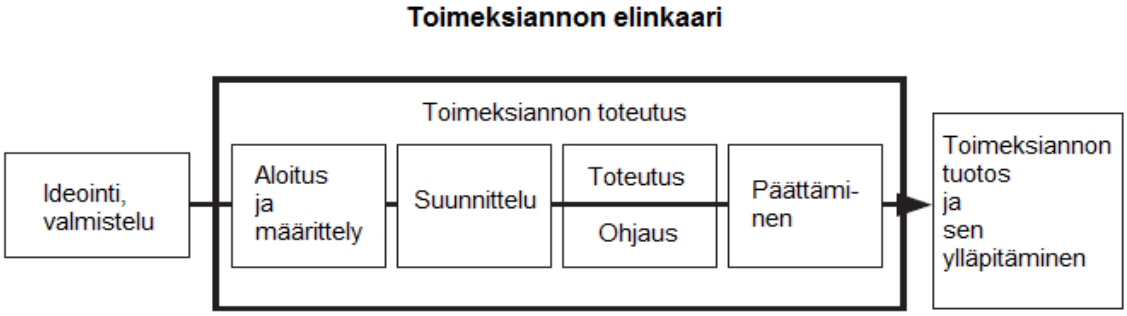
5 TOIMEKSIANNON TOTEUTUS

5.1 Valmistelu

Kun opinnäytetyön tekeminen tuli opinnoissani ajankohtaiseksi, kysyin esimieheltäni LapIT Oy:ssä olisiko yrityksellä tarjolla toimeksiantoja. Mobiililaitteiden hallintastrategia nousi esille, koska mobiililaitteet oli vastikään liitetty osaksi yrityksen tarjoamaa elinkaarenhallintapalvelua. Esittelin toimeksiantoehdotuksen opettajilleni Lapin ammattikorkeakoulussa, ja aiheen hyväksynnän jälkeen aloin työskentelyn.

Tämän työn tekemisessä menetelmänä on periaatteessa käytetty kirjallisuuskatsausta. Ari Salminen (2011) toteaa katsaus-nimityksen olevan ”harhaanjohtava”, koska todellisuudessa kyseessä on myös lähteiden uudelleenarviointi lukijan näkökulmasta. Kuvaileva kirjallisuuskatsaus on ilman tiukkoja sääntöjä toteutettua yleiskatsausta. Sen vuoksi työssä on käytetty monenlaisia, eritasoisia lähteitä.

Kuviossa 1 kuvataan toimeksiannon toteutuksen eteneminen. Aloitus ja määrittely tapahtuivat pitkälti esimiehen kanssa keskustellen. Kävimme läpi toimeksiannon tavoitteen, eli määrittelimme millainen ohje toimeksiannon lopputuloksena tulisi olla. Erityisen tärkeää tässä vaiheessa toimeksiantoa oli määritellä ohjeen lukijakunta. Dokumentin kohdeyleisö vaikuttaa ratkaisevasti siihen, millaista kieltä teksti tulee olemaan.



Kuvio 1. Toimeksiannon elinkaari (mukaillen Artto ym. 2006).

Toimeksiannon määrittelyn jälkeen olivat vuorossa ohjeen suunnittelu sekä lähdemateriaalin kerääminen. Toimeksiannon toteutuksen aikana pidettiin myös tarvittaessa ohjaustapaamisia sekä opinnäytetyön ohjaajan, että toimeksiantajan kanssa. Pääasiassa ohjaus koski lähdemateriaalin keräämistä ja arviointia.

5.2 Teoriasta tuotokseen

Opinnäytetyön raportointi on tapahtunut toimeksiannon toteutuksen rinnalla. Lähdemateriaalista koottu ”hallintastrategian teoria” on kirjattu raporttiin. Toimeksiannon lopputulokseen, eli itse ohjeeseen, on koottu raportin teoriaosuuden kokoamisen aikana havaitut ”best practices”, joiden avulla hallintastrategia muodostuu. Jotta ohje pysyisi tiiviinä ja helposti luettavana, se jaettiin viiteen osa-alueeseen, joita käsitellään tässä luvussa ohjeessa käytettyjen väliotsikoiden mukaisesti.

Lyhenteet

Yksi suurimmista haasteista ohjetta kirjoittaessa oli englanninkielisen ”jargonin” avaaminen ymmärrettävästi. Jo määrittelyvaiheessa todettiin, että liian tekninen kieli tekee ohjeesta luotaantyöntävän. Ohjeessa pyrittiin siis kiinnittämään erityistä huomiota teknisten termien käyttöön.

Mobiililaitteista ja erityisesti niiden hallinnasta kirjoitettaessa tulee väkisin vastaan sellaisia lyhenteitä, joiden käyttämistä ei voi välttää. Jotta ohjeen kieli olisi sujuvaa, tietyt yleisimmät lyhenteet avataan erillisessä Lyhenteet-osiossa. Kohdatessaan entuudestaan oudon lyhenteen lukija voi palata dokumentin alkuun ja selvittää pikaisesti, mistä on kyse. Kaikkia lyhenteitä ei esiinny ohjeessa, mutta ne selitetään joka tapauksessa siltä varalta, että lukija törmää niihin omassa taustatutkimuksessaan.

Määrittely

Ohjeen MDM-strategian määrittely -osiossa organisaatiota ohjeistetaan tekemään strategian taustoitus. Strategian laatijan täytyy tuntea organisaation olemassa oleva mobiiliympäristö, jotta strategian laatimisessa osataan tehdä organisaation toimintaa parhaiten tukevia valintoja. Osiossa lukijalle esitetään luvussa 4.1 esitellyt kysymykset sellaisinaan.

Turvallisuuskäytännöt

Koska mobiililaitteita käytetään vaihtelevissa paikoissa ja tilanteissa, tietoturvallisuus on avainasemassa niiden hallinnassa. Tästä syystä oli luonnollista, että yksi ohjeen osa-alueista koskee organisaation turvallisuuskäytäntöjä. Turvallisuuskäytännöt-osiossa käsitellään niitä huomioitavia asioita, joilla organisaatio turvaa sekä fyysiset laitteensa että niillä käsiteltävän datan.

Osiossa tuodaan esille erilaisia tapoja, joilla organisaatio voi halutessaan ottaa kantaa ja edesauttaa mobiililaitteidensa tietoturvaa. Näitä ovat salasanasääntöjen ja virusturvaohjelmistojen lisäksi myös käyttäjien kouluttaminen. Erityisesi painotetaan organisaation sisäisten ohjeiden selkeyttä ja käyttäjien riittävää kouluttamista ja opastamista. Organisaation on tiedostettava, että kaikille eivät riitä samat ohjeet. Nykypäivänä ihmisten tekninen osaaminen vaihtelee niin paljon, ettei voida luottaa että yksillä ohjeistuksilla saadaan koko organisaation toimimaan. Inhimillinen tekijä (human factor) tulee aina ottaa huomioon tietoturvaa pohdittaessa, sillä virheitä tekevä ihminen on tietoturvan heikoin lenkki (Karlsson 2014).

Laitehallinta ja tuki

Laitehallinta ja tuki -osio jaettiin kahteen osaan. Ensimmäinen osa käsittelee mobiililaitteiden hallintajärjestelmän valintaa. Ohje esittää lukijalle kysymyksiä, joita hänen on syytä ottaa huomioon tuotetta valittaessa. Ei ole järkevää esitellä tai

vertailla erilaisia hallintajärjestelmiä, vaan ohjeessa pikemminkin käsitellään niiden ominaisuuksia yleisellä tasolla. Jos ohjeessa esiteltäisiin jotain tiettyä tuotetta, tiedot olisivat pahimmassa tapauksessa muutamassa kuukaudessa vanhentuneita. Tällaisen ratkaisun jälkeen ohjetta ei tarvitse olla päivittämässä jatkuvasti.

Laitehallinta ja tuki -osion toisessa osassa käsitellään laitteen elinkaarta. Ohjeessa kerrotaan taulukkomuodossa, mitä eri vaiheita laitteen elinkaaressa on ja mitä niissä on hyvä huomioida strategiassa. Osiossa pyritään korostamaan organisaation sisäistä vastuunjakoa sekä käyttäjien ohjeistamista.

Oman laitteen käyttö

Lähdemateriaalin keräämisen ja arvioinnin yhteydessä nousi esiin erityisesti amerikkalaisissa lähteissä toistuva käsitys, että yritysten työntekijät haluavat yhä enemmän käyttää työtehtävissään omaa mobiililaitettaan. Tähän itse suhtaudun kriittisesti. Työssäni LapIT Oy:llä en ole vielä kohdannut asiakasorganisaatioiden työntekijöitä, jotka olisivat käyttäneet omia omistuslaitteitaan työssään. Kaikilla on ollut käytössään työnantajan laite. Tämä tukee käsitystäni siitä, että ainakaan vielä oman laitteen käyttö ei ole Suomessa yleistä, mutta päätin joka tapauksessa sisällyttää ohjeeseen osion ns. BYOD-politiikasta.

6 POHDINTA

Opinnäytetyössäni tavoitteenani oli tehdä ohje organisaation mobiililaitteiden hallintastrategian laatimiseen. Pääsin tavoitteeseen, ja voin toimittaa opinnäytetyön tuotoksena syntyneen ohjeen (liite 1) toimeksiantajalleni tämän opinnäytteen valmistuttua.

Helpoimmaksi tehtäväksi opinnäytetyössä osoittautui lähdemateriaalin kerääminen. Olin varautunut henkisesti, että MDM-strategiasta olisi hankala löytää käyttökelpoisia lähteitä. Yritysten auttaminen tällaisen hallintastrategian laatimisessa on luultavasti rahanarvoista bisnestä konsulttiyrityksille. Oletin, että tästä syystä mobiililaitteiden hallintastrategiasta ei olisi saatavilla ilmaista informaatiota. Aiheesta kirjoitettuja artikkeleita ja vapaassa jaossa olevia mallistrategioita löytyi kuitenkin yllättävän vaivattomasti. Toisaalta eräässä lähdeartikkelikandidaatissa todettiin, että yleisin tapa organisaation MDM-strategian laatimiseen on ”googlaaminen”. Lähdemateriaalia oli tarjolla, joten suurin työnsarka oli hyödyllisen tiedon erottelemisessa tarpeettomasta, sekä kerätyn tiedon esittäminen sellaisessa muodossa, että vähemmän tekninenkin ihminen hyötyy siitä. Tieteellistä tutkimuskirjallisuutta aiheesta ei löytynyt, mikä on toisaalta ymmärrettävää aihepiirin tuoreuden vuoksi.

Opinnäytetyössä haasteelliseksi osoittautui englanninkielisen ammattisanaston kääntäminen suomenkielelle. Ohjeen kieliasu oli tarkoitus pitää mahdollisimman ymmärrettävänä kaiken tasoisille lukijoille.

Kaiken kaikkiaan opinnäytetyöprosessi oli haastavampi kuin etukäteen oletin. Työskentelyssäni vaikeinta oli alkuun pääseminen, mutta kun lähdemateriaalia alkoi löytyä ja kirjoittamisprosessi lähti käyntiin, prosessi alkoi edetä rivakasti. Raportin kirjoittamisessa päädyin tekemään normista poikkeavia ratkaisuja tekstin luettavuuden parantamiseksi. Tekstiosiossa 5.2 käytän ”epävirallisia” väliotsikoita, koska koen että ne helpottavat sisältökokonaisuuksien hahmottamista. Otsikoiden alle ei kuitenkaan välttämättä tullut niin paljon tekstiä, että kolmostason

otsikoiden käyttäminen olisi ollut perusteltua. Lisäksi omasta mielestäni kolmostason otsikot olisivat vaikuttaneet negatiivisesti raportin sisällysluettelon tasapainoon, mikä olisi osaltaan vaikuttanut sisällön hahmottamiseen.

Koska mobiiliteknologia ja -markkinat kehittyvät jatkuvasti, mobiililaitteiden hallintastrategian ohjetta on syytä aina silloin tällöin päivittää. Juuri ajantasaisena pysymisen vuoksi ohjeessa ei esitellä mobiililaitteiden hallintaan liittyviä tuotteita. Parhaaksi koetut toimintatavat erityisesti tietoturvan alalla muuttuvat nopeasti, joten tarve päivittämiselle varmasti tulee. Ohjeen jatkoksi voisi myös laatia LapIT:n oman mallistrategian. Jatkotutkimusaiheena voisi olla toimeksiantajan asiakkaiden MDM-strategioiden kartoittaminen muutaman vuoden päästä. Jos MDM-strategiaa ei ole otettu käyttöön, asiakasta voisi kannustaa sen laatimiseen. LapIT Oy voisi myös myydä mobiililaitteiden hallintastrategian tekemiseen konsultointipalvelua.

LÄHTEET

Artto K., Martinsuo M. & Kujala J. 2006 (2. painos: 2008). Projektiliiketoiminta. WSOY, Helsinki.

Grey, B. 2011. Building an effective mobile device management strategy. Viitattu 24.10.2015 http://www.slideshare.net/fiberlink/building-an-effective-mobile-device-management-strategy

Karlsson, K. 2014. Human factor. Steganography and Digital investigation. Luento 22.4.2014.

LapIT Oy 2014. Toimintakertomus 2014.

LapIT Oy 2015. Viitattu 24.10.2015. http://www.lapit.fi/lapit/

Lisko, M. 2015. Opariin liittyen: onko läppäri mobiililaite? Email markus.lisko@lapit.fi 24.10.2015. Tulostettu 26.10.2015.

Mobiiliopas 2011. Avoimet verkostot oppimiseen (AVO) -hanke. Euroopan sosiaalirahasto (ESR). Viitattu 24.10.2015. https://sites.google.com/site/avomobiiliopas/mobiililaitteet

Mäkinen, S. 2003. Organisaation muisti – käsiteanalyysi. University of Tampere. Department of Information Studies. Research notes 2003/2.

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Opetusjulkaisuja 62. Julkisjohtaminen 4. Vaasan yliopiston julkaisuja.

Sjöholm, H. 2006. Pk-yrityksen liiketoiminnan kehittäminen. Teknologia ja innovaatiot hyödyksi. Tekes Helsinki.

Sophos 2013. Sample Mobile Device Security Policy. A Sophos Whitepaper.

Technology Conference & Expo 2013. Bring your own device. Viitattu 14.11.2015 http://searchcio.techtarget.com/feature/Ensure-mobile-device-security-through-a-mobile-device-management-policy

Valtiovarainministeriö 2013. Päätelaitteiden tietoturvaohje. Valtiohallinnon tietoturvallisuuden johtoryhmä VAHTI 5/2013. Juvenes Print – Suomen Yliopistopaino Oy.

Viitala, R. 2007. Henkilöstöjohtaminen – Strateginen kilpailutekijä. Helsinki: Edita Publishing Oy.

Waibel, U. 2014. 5 key things to consider when developing an enterprise mobility management strategy. Viitattu 15.11.2015. http://www.net-security.org/article.php?id=2122

LIITTEET

Liite 1

Mobiililaitteiden hallintastrategia
Ohjeita MDM-strategian luomiseen

31.10.2015/ Tapio Nykänen

Rantavitikantie 33
96300 ROVANIEMI
Palvelupiste 0201 555 222
Y-tunnus: 1637268-5
ALV-rek

Sisällysluettelo

1. Yleistä

Tämä dokumentti on tarkoitettu organisaation tieto- ja viestintätekniikasta vastaavalle henkilöstölle avuksi mobiilipäätelaitteiden hallintastrategiaa suunniteltaessa. Hallintastrategian avulla organisaatio selkiyttää linjauksiaan työntekijöilleen, hallitsee mobiililaitteiden kustannuksia ja käyttöä sekä vähentää mobiililaitteiden käytöstä aiheutuvia tietoturvariskejä.

Dokumentti ei ota kantaa siihen, mitä nimenomaisia tuotteita organisaation pitäisi ottaa toiminnassaan käyttöön. Organisaation vastuulle jää tutustua esimerkiksi eri mobiilikäyttöjärjestelmien tai virustorjuntaohjelmistojen eroavaisuuksiin. Ohje antaa neuvoja sen suhteen, mitä kannattaa ottaa huomioon päätöksiä tehtäessä.

2. Lyhenteet

Seuraavassa taulukossa selitetään sellaisia lyhenteitä, joita hallintastrategiaa suunnitellessa todennäköisesti tulee vastaan.

Lyhenne	Avattu	Suomennos/selitys
BYOD	Bring Your Own Device	Oman omistuslaitteen käyttö työtehtävissä
MAM	Mobile Application Management	Mobiilisovellusten hallinta
MDM	Mobile Device Management	Mobiililaitteiden hallinta

3. MDM-strategian määrittely

Mobiililaitteiden hallintastrategian laatiminen on syytä aloittaa organisaation nykytilanteen tarkastelusta. Seuraavassa taulukossa on asioita, jotka määrittelemällä saadaan luotua lähtökohdat MDM-strategialle:

Millaisia käyttäjiä?	Minkälaisessa käytössä organisaation toiminnassa olevat laitteet ovat
Millaisia laitteita?	Onko organisaation toimintaympäristössä älypuhelimia ja tabletteja? Vaikuttaa mm. siihen, millaista dataa laitteilla käsitellään ja sitä kautta tarvittavaan tietoturvaan.
Mitä käyttöjärjestelmiä?	Vaikuttaa mm. MDM-järjestelmän valintaan. Mitä useampi käyttöjärjestelmä, sitä monimutkaisempi ympäristö.
Mitä sovelluksia?	Vaikuttaa mm. vaadittavan tietoturvan määrittelyyn
Kuinka tietotekniikkaa hallitaan?	Organisaation sisäinen vastuunjako ja olemassa olevat järjestelmät
Kuka maksaa?	Organisaation sisäinen vastuunjako

4. Turvallisuuskäytännöt

Koska organisaation sisällä työntekijöiden tietotaito mobiililaitteisiin liittyen on hyvin vaihtelevaa, tietoturvan näkökulmasta ketjun heikoin lenkki on viime kädessä laitteen käyttäjä. Organisaation onkin hyvä kiinnittää huomiota tietoturvamääräysten ja -ohjeistusten selkeyteen ja työntekijöiden valistamiseen.

Seuraavassa taulukossa esitetään toimenpiteitä, joilla organisaatio ehkäisee tietoturvariskien toteutumista:

Laitteelle pääsyn suojaaminen	
Salasanakäytännöt	Huomioitava ajantasaiset turvallisen salasanan vaatimukset
Salasanan säännöllinen vaihtaminen	Voiko salasanan vaihtamisen automatisoida kuten tietokoneilla?
Päätös käytettävästä suojausmetodista (pinkoodi, salasana, sormenjälkitunnistus yms.)	Huomioitava laitevalmistajakohtaiset erot
Virusturva	
Antivirus-tuote mobiililaitteille	Haittaohjelmia on jo melkein kaikille isoimmille mobiilialustoille
Tietoturvatasot	
Eriasteisten tietoturvatasojen määrittäminen	Huomioitava laitteen käyttötapaukset, missä ja millaista dataa laitteilla käsitellään. Esim. potilastietojen suojaaminen (otettava huomioon myös mahdolliset lait joita datan käsittelyyn liittyy).
Laitteen salaaminen	
Salaustuotteen valinta	Huomioitava yhteensopivuus käytettävien laitteiden, käyttöjärjestelmien ja hallintajärjestelmien ym. kanssa
Päätös salattavista laitteista	Salataanko kaikki laitteet, vai ainoastaan tietyn tietoturvatason laitteet?
Sallitut sovellukset	
Päätös, mitä sovelluksia organisaation laitteille saa asentaa	Pystytäänkö käyttäjää estämään asentamasta sovelluksia esim. käyttöoikeuksilla?
Päätös toimenpiteistä/seuraamuksista, jos käyttäjän asentama sovellus aiheuttaa tietoturvariskin	Mitä jos käyttäjän asentama sovellus asentaa viruksen tai muuten aiheuttaa laitteen rikkoutumisen?
Käyttäjien kouluttaminen	
Tietoturvallinen työskentely tutuksi	Käyttäjät oppivat tuntemaan tietoturvariskit ja toimet joilla niitä ehkäistään

Geofencing

Geofencing on ohjelmisto-ominaisuus, joka määrittää laitteen GPS:n avulla maantieteelliset rajat mobiilisovelluksille. Organisaatio voi määrittää jonkin tietyn sovelluksen käytettäväksi vain esimerkiksi omalla toimipisteellään tai kunnan alueella. Ominaisuuden hyödyntäminen lisäisi tietoturvaa sellaisten ohjelmistojen ja tietojen kanssa, joita ei ole tarpeen käsitellä kuin tietyssä tarkasti rajattavissa olevassa paikassa.

5. Laitehallinta ja tuki

Organisaation tulee suunnitella mobiililaitteiden elinkaari samalla lailla kuin perinteisten tietokoneiden tietokoneidenkin, kuitenkin huomioiden laitteiden käyttöiät. Mobiililaitteen käyttöikä on usein huomattavasti lyhempi kuin esimerkiksi pöytätyöaseman. Laitteiden elinkaaren aikana niitä on helpoin hallita MDM-järjestelmällä. Tässä osiossa käsitellään MDM-järjestelmän ominaisuuksia sekä mobiililaitteiden elinkaarta.

Hallintajärjestelmän valinta

Hallintatuotetta valittaessa huomioon otettavia ja selvittämisen arvoisia kysymyksiä:

Mitä käyttöjärjestelmiä tuote tukee?	Huomioitava myös käyttöjärjestelmien asettamat rajoitukset. Kaikki käyttöjärjestelmät eivät salli yhtä laajaa hallintaa kuin toiset (vrt. iOS ja Android)
Tukeeko tuote integraatiota organisaation olemassaolevien infrastruktuurielementtien kanssa	Esim. Active Directory
Tukeeko tuote mobiililaitteiden käytäntöjen hallintaa?	Voiko laitteille määritellä/ylläpitää/pakottaa käytäntöjä?
Tukeeko tuote turvallisuudenhallintaa?	Esim. alkuperäisten tai kolmannen osapuolen turvallisuuskontrollien muokkaaminen/pakottaminen, uhkien havaitseminen
Kuinka tuote toteuttaa laitteiden monitoroinnin, raportoinnin ja vianmäärityksen?	Esim. reaaliaikaiset tilannetiedot, hälytykset, lokitiedostot, diagnostiikkatyökalut
Tukeeko tuote mobiilisovellusten hallintaa?	Sovellusten lataaminen laitteelle, asentaminen, hallinta, poistaminen/disablointi
Tukeeko tuote mobiilidokumenttien hallintaa?	Organisaation dokumenttien synkronointi ja turvaaminen
Tukeeko tuote BYOD-laitteiden hallintaa?	Miten client asennetaan laitteelle, paljonko tarvitaan lisenssejä?

Elinkaari

Organisaation ympäristössä voi olla käytössä monenlaisia mobiililaitteita eri käyttötarkoituksissa. Osa laitteista voi olla organisaation omistamia, osa taas leasingsopimuksella hankittuja. On tärkeää suunnitella laitteiden elinkaari ja sen eri vaiheet. Seuraavassa taulukossa mobiililaitteen elinkaari on jaettu kuuteen päävaiheeseen: esikartoitus, hankinta, käyttöönotto, käyttö ja ylläpito, uudelleenkäyttöönotto, käytöstä poisto. Taulukossa listataan asioita, joita elinkaaren eri vaiheissa tulee tehdä tai ottaa huomioon.

Esikartoitus	
Päätelaitekartoitus	Varmistetaan, että markkinoilla on tuotteita jotka täyttävät organisaation tarpeet ominaisuuksiltaan (huomioitava tietoturvavaatimukset).
Päätös tietoturvatasosta	Huomioitava käsiteltävän datan suojaustaso, laitteen käyttöympäristö sekä palvelut joihin kytkeydytään.
Hankinta	
Tietoturvavaatimukset	Huomioitava lait ja esikartoituksessa päätetty tietoturvataso.
Vastuunjako	Kuka hankkii laitteet? Ketä voi konsultoida tarvittaessa? Kuka hankkii ja hallitsee sovelluslisenssejä?
Käyttöönotto	
Miten laite otetaan käyttöön?	Esiasennetaanko sovellukset ym. vai vastaako käyttäjä tarvitsemiensa sovellusten asentamisesta? Salataanko laite?
Tarvittava koulutus laitteen käytöstä	Huomioitava käyttäjien vaihteleva tieto- ja osaamistaso (riittääkö kirjallinen ohje vai tarvitaanko ns. lähiopetusta?)
Käyttö ja ylläpito	
Päivitysten asentaminen	Kuka asentaa ohjelmisto- ja tietoturvapäivitykset sekä käyttöjärjestelmäpäivitykset? Millaisella aikataululla päivitykset asennetaan?
Muutoshallinta ohjelmistoasennuksissa	Kuka vastaa muutosten pilotoinnista ja toteuttamisesta?
Laitteen huoltaminen	Miten käyttäjä toimii laitteen rikkoutuessa? Kuka vastaa laitteen huoltamisesta/huoltoon lähettämisestä? Huomioitava huollosta aiheutuva käyttökatko mm. varalaitteiden määrässä.

Uudelleenkäyttöönotto	
Laitteen tietoturvallinen tyhjentäminen	Kuka vastaa laitteen tietoturvallisesta tyhjentämisestä/tehdasasetuksille palauttamisesta käyttäjän vaihtuessa?
Käytöstä poistaminen	
Tietoturvallisen käytöstä poistamisen toimenpiteiden määritteleminen	Kuka vastaa laitteen tietoturvallisesta käytöstä poistamisesta?

6. Oman laitteen käyttö

Työntekijä saattaa haluta käyttää töissä omaa mobiililaitettaan. Joku voi kokea esimerkiksi useamman puhelimen mukana kantamisen epämiellyttävänä ja haluaisi ennemmin käyttää pelkästään omaa puhelintaan. Organisaatio voi harkita ottavansa käyttöön ns. BYOD-politiikan. Seuraavassa taulukossa esitetään BYOD-laitteiden mahdollisia etuja ja huomioon otettavia seikkoja:

Mahdolliset edut	**Huomioitavaa**
Kustannusten hallinta	Turvallisuus ja sääntöjen noudattaminen
Työntekijöiden tyytyväisyys	Hallinnan puute
Teknologian omaksuminen	Ylimääräisen tuen tarve
Useampia käyttöjärjestelmiä	Yksityisyys
Tuottavuuden lisääminen	Yhteensopivuus
Laajempi mobiilin käyttöönotto	Tiedon häviäminen/vuotaminen
	Työntekijä omistaa laitteen

Omien laitteiden käytössä huomionarvoista on se, että jos käyttäjä haluaa käyttää omistamaansa laitetta työtehtävissään, hän joutuu luopumaan osasta päätäntävaltaa laitteen suhteen. Jotta organisaation toiminnan tietoturva säilyy, on kaikkien sen dataa käsittelevien laitteiden oltava mobiililaitteiden hallintastrategian määrittämien tietoturvavaatimusten piirissä.