HAAGA-HELIA
ammattikorkeakoulu

iPadin etähallinnointi

Niina Jäppinen

Opinnäytetyö

Tietojenkäsittely

19.5.2013

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

19.5.2013

Tietojenkäsittely

Tekijä Niina Jäppinen	**Aloitusvuosi** 2009
Raportin nimi iPadin Etähallinnointi	**Sivu- ja liitesivumäärä** 27 + 2
Ohjaaja Tuomo Ryynänen	

Tämän opinnäytetyön aiheena on iPadin etähallinnointi.

Teoriaosuudessa käsitellään, mitä etähallinnointi on, mistä kaikeista se koostuu, ja mitä asioita on otettava huomioon etähallinnoinnissa. Yksi oleellisimmista tekijöistä on toimiva tietoturva. Tietoturvan eri osa-alueita käsitellään etähallinnoinnin näkökulmasta.

Teoriaosuuden jälkeen paneudutaan tarkemmin siihen mitä iPadin etähallinnointi on, ja miten sitä voi toteuttaa käytännössä. Tutkimuksen tavoitteena on myös miettiä miten iPadin etähallinnointia voisi kehittää paremmaksi.

Oppinnäytetyöhön kuuluu myös kysely, jossa selvitetään kokevatko laitteen käyttäjät etähallinnoin tarpeelliseksi, sekä millaisia kokemuksia heillä on laitteen käytöstä sekä etähallinnoinnista. Kyselyssä selvitään myös mihin iPadia pääasiassa käytetään.

Asiasanat
iPad, etähallinnointi, MDM, etätyö

HAAGA-HELIA
University of Applied Sciences

Abstract

19.5.2013

Degree programme

Author Niina Jäppinen	**Year of entry** 2009
The title of thesis iPad's remote control	**Number of report pages and attachment pages** 27+2
Advisor Tuomo Ryynänen	

The purpose of this thesis was to find out how to improve the remote contol on iPads. The study focused on clarifying users' opinions about the remote control and whether it is a necessary concept in the first place. In addition, various remote control solutions were looked into and it was also investigated how and what the people use their iPads for.

In the theoretical part of the thesis, the concept of a remote control was explained. One main factor was operational information security. In the empirical part of the thesis, a survey was conducted among iPad users to gain further insight on how people perceive the remote control.

Key words
iPad, remote control, MDM, remote work

Sisällysluettelo:

Sanasto

Apple ID

Kirjautumistunnus jolla voi käyttää Applen eri palveluita. Tunnuksella voi esimerkiksi ladata ohjelmia iPadiin, AppStoresta Applen omasta sovelluskaupasta. Ilman Apple ID.tä ohjelmien ostaminen/lataaminen tai muiden Applen palveluiden käyttö ei onnistu.

AppStore

Appstore on sovelluskauppa, jonka kautta voi ostaa tai ladata ilmaiseksi sisältöä iPadiin. Esimerkiksi erilaisia pelejä sekä ohjelmia.

Jailbreak

Suljetun laitekäyttöjärjestelmän murtaminen, jotta laitteelle voi esimerkiksi asentaa kolmannenosapuolen sovelluksia. iPadin kohdalla tämä tarkoittaa käytännössä sitä, että laitteeseen pystyy asentamaan ohjelmia muualtakin kuin AppStoresta.

uTorrent

On BitTorrent vertaisverkon asiakasohjelma. uTorrent ohjelmaa voidaan käyttää tiedostojen siirtämiseen sekä erilaisten asioiden lataamiseen Internetistä. Ohjelma tunnetaan ympäri maailmaa. Se tunnetaan ehkä parhaiten laittomien tiedostojen lataus ja levyskanavana.

iPad mikä se on?

iPad on kosketusnäyttöllinen mobiilaite. Se ei kuitenkaan ole älypuhelin, vaikka siinä samanlaisia toimintoja kuin älypuhelimissa. iPad on kooltaan huomattavasti isompi kuin älypuhelin. Ensimmäinen versio laitteesta on julkaistu vuonna 2010 ja laite on Applen valmistama. iPadissa toimiiApplen omalla iOS käyttöjärjestelmällä.

1 Johdanto

Opinnäytetyöni aiheena on tutkia mitä iPadin etähallinnointi on. Päätutkimuskysymykseni on ”Mitä etähallinnointi on?”. Avustavia tutkimuskysymyksiä on ”Mitä etähallinnoinnista on, Mitkä ovat etähallinnoinnin uhat ja riskit? sekä Miten etähallinnoidaan?” Näiden neljän tutkimuskysymyksen ympärille olen rakentanut tämän opinnäytetyön.

2 Teoria

Teoriaosuus käsittelee mitä etähallinnointi on käytännössä. Aloittaessani tutkimaan ja etsimään kirjallisialähteitä etähallinnoinnista huomasin, että aiheesta ei varsinaisesti ole olemassa kirjallisuutta. Etähallinnointi ei kuitenkaan ole uusi keksintö. Jo Windows XP käyttöjärjestelmässä on ollut etähallinnointi ominaisuus. Kirjallisuutta, joka käsittelee etähallinnointi, oli todella vaikea löytää. Tästä syystä päätin lähteä tutkimaan millaiset tekijät vaikuttavat etähallinnointiin.

Yksi tekijä joka vaikuttaa etähallinnnointiin, on tietoturva. Analysoin tietoturvan eri osa-alueita ja käsittelen tietoturvaa etähallinnoinnin näkökulmasta. Etähallinnoinnista saa parhaimman kuvan käytännönläheisten esimerkkien avulla. Tästä syystä olen koonnut muutamia etähallinnointi tapauksia, joihin olen törmännyt työelmässä.

2.1 Mitä etähallinta on?

Etähallinta on jonkin laitteen esimerkiksi tietokoneen käyttämistä etänä ilman, että on fyysisesti kosketuksissa hallinnoitavaan koneeseen. Perusidea on siis ottaa laitteelta A yhteys laitteeseen B internetin välityksellä, ja käyttää laitetta B etänä. Laitteet A ja B voivat olla samassa verkossa tai esimerkiksi täysin eri puolilla maailmaa toisistaan. Tälläistä toimintoa kutsutaan etätyöpöydän käyttämiseksi. (What is remote managemet? http://www.wisegeek.com/what-is-remote-management.htm)

On olemassa erilaisia ohjelmia joiden avulla pystyy etähallinnoimaan laitteita. Kaikissa etähallinnointiohjelmissa on sama perusidea, mutta ohjelmien välillä on joitain eroja. Eroja on mm. ohjelmien toiminnoissa, lisäominaisuuksissa, ja onko etähallinnointiohjelma käyttöjärjestelmä sidonnainen sekä mitä kaikkia laitteita ohjelmalla voi etähallinoida.

Esimerkiksi jotkut ohjelmat vaativat erikseen jokaisella etäyhteyden muodostus kerralla käyttäjän erillisen suostumuksen, ennen kuin koneelle voi muodostaa etäyhteyden. Osassa ohjelmista käyttäjä ei pysty estämään etähallinnointia muuta kuin katkaisemalla koneestaan Internetyhteyden.

Etähallinnointi mahdollistaa etätyöpöydän käytön lisäksi etähallinnointiohjelmasta riippuen mm. koneen teknisten tietojen keräämisen eli mitä ohjelmia koneella on käynnissä parhaillaan, ohjelmistojen versiotiedot, muistinkulutuksen, tietoliikenne määrät ja kuka käyttäjä on kirjautuneena parhaillaan. Etähallinnoinnilla voidaan suorittaa myös erilaisten päivityspakettien tai ohjelmien asentamiset tai varmuuskopioinnin. Kaikissa etähallinnointiohjelmissa ei kuitenkaan ole etätyöpöytä ominaisuutta. (Valtiovarainministeriö, 5.1 Mitä etähalinnointi mahdollistaa? https://www.vahtiohje.fi/web/guest/144)

Etähallinnointiohjelmat voidaan jakaa karkeasti kahteen eri ryhmään. Ensimmäisen ryhmän ohjelmien avulla etähallinnointi tapahtuu etätyöpöytäyhteyttä käyttämällä, jolloin käyttäjä voi nähdä mitä koneella tehdään ja hän voi myös itse esimerkiksi näyttää etäyhteyden muodostajalle millainen ongelma koneessa on. On myös mahdollista, että etähallinnoitsija voi lukita käyttäjältä ruudun jolloin käyttäjä ei pysty tekemään koneella mitään niin kauan kuin etäyhteys on muodostettu. Jälkimmäistä ominaisuutta ei ole kaikissa etähallinnointi ohjelmissa.

Hyviä etähallintaohjelmia on mm. TeamViewer ja Remote Desktop. TeamViewer on käyttöjärjestelmä riippumaton etähallinnointiohjelma ja siitä on saatavilla maksullinen yritysversio sekä ilmainen versio yksityiskäyttäjille. Ohjelma on hyvin käyttäjäystävällinen, koska koneelle ei voi ottaa etäyhteyttä ilman että TeamViewer ohjelma on käynnis-

tetty ja että käyttäjä on kertonut ohjelman antaman ID-numeron etäyhteyden muodostajalle.

Remote Desktop etähallinnointiohjelma on Microsoftin tuote ja se on hyvin tietoturvallinen, koska ohjelman kautta voi etähallinnoida vain niitä koneita jotka ovat samassa verkossa koneen kanssa josta yritetään muodostaa etäyhteys. Remote Desktopista on omat versiot Mac ja Windows koneille.

Ohjelmassa on enemmän ominaisuuksia kuin esimerkiksi TeamViewerissä. Remote Desktop ohjelmassa etähallinnoitsija voi mm. tarkkailla käyttäjän työpöytää ilman että käyttäjä on asiasta tietoinen. Ohjelmalla voi myös lukita käyttäjän ruudun siksi aikaa kun konetta etähallinnoidaan. Remote Desktopilla etähallinnointaessa käyttäjältä ei erikseen tarvite pyytä hyväksyntää, jotta yhteyden voi muodostaa.

TeamViewerillä sekä RemoteDesktopilla pystyy hallinnoimaan perustyöasemia sekä palvelimia. TeamVieweristä on saatavilla myös iPadille oma verio. iPad version avulla käyttäjä pystyy etätyöpöydän avulla käyttämään omaa tietokonettaa iPadilta.

Toisen tyyppiset etähallinnointiohjelmat kuin edellä mainitut, ovat sellaisia joilla etähallinnointi tapahtuu taustalla. Tälläisillä etähallinnointiohjelmilla hallinnointaessa käyttäjä ei pysty näkemään etähallinnointia. Käyttäjä korkeintaan saattaa havaita koneen hidastuneen hieman. Etähallinnoinnista johtuva välikainen hitaus ilmenee vain kun koneen taustalla asentuu päivityksiä tai uusia ohjelmia. Etähallinnointiohjelma jolla näin voi tehdä on esimerkiksi Abosulute Manage. Ohjelman avulla voidaan päivitysten ja uusien ohjelmien asennuksen lisäksi kerätä koneesta teknillisiä tietoja.

2.1.1 Miten tietoturva vaikuttaa etähallinnointiin?

Tietoturva on yksi olennaisimmista asioista liittyen etähallintaan. Jos tietoturva ei ole kunnossa etähallinnoinnin tietoturvariskit kasvavat. Kun tietoturva on kunnossa, on etähallinnointikin paljon riskittömämpää, koska uhkatekijöitä on huomattavasti vähemmän. Käsittelen tietoturvaa yleisellä tasolla ja nimenomaan etähallinnoinnin näkökulmasta.

Kuten aikaisemmin mainitsin, etähallinnointiin käytetään yleensä valmiita ohjelmia, joita on erilaisia. Ohjelmia on kaupallisia yritystarkoituksiin sekä ilmaisia yksityiskäyttöä varten.

Tietoturvan tavoitteet on jaettu seuraaviin tietoturvan periaatteisiin:

- luottamuksellisuus
- autenttisuus, oikeellisuus
- kiistämättömyys
- eheys
- käytettävyys

(Ruohonen, 2002, 2.)

Edellä mainitut kuusi tietoturvan periaatetta toteutuessaan luovat tietoturvaa niin yrityksille kuin tietotekniikan käyttäjille. Onnistunut tietoturva helpottaa, parantaa sekä nopeuttaa työskentelyä. (Ruohonen, 2002, 2.)

2.1.2 Tietoturvan päätavoitteet

Tietoturvan periaatteet muodostavat tietoturvan, joka suojaa järjestelmiä sekä ohjelmia mahdollisimman monilta odotetuilta sekä odottamattomilta uhilta sekä riskeiltä. Tietoturvan päätavoite on varmistaa, että ohjelmat sekä tietokoneet joissa ohjelmia käytetään

tekevät aina sen mitä niiden on tarkoitus tehdä. Tietoturvalla voidaan mm. määritellä oikeuksien avulla keillä kaikilla on pääsy tiettyihin tietoihin ja keillä ei. Oikeuksilla voidaan varmistaa myös, että tiedostoihin pääse käsiksi silloin kun se on tarpeellista. (Ruohonen, 2002, 2.)

Alla on kerrottuna tarkemmin, mitä tietoturvan periaatteiden tavoitteena on. Luottamuksellisuuden tavoitteena on varmistaa, että tietoturvan alaisiin tietoihin pääsee käsiksi vain ne käyttäjät joilla on siihen käyttöoikeudet. Jos jokin ulkopuolinen käyttäjä pääsee näihin tietoihin käsiksi, on luottamuksellisuus tällöin menetetty. (Ruohonen, 2002, 2.)

Autenttisuuden tavoitteena on varmistaa että kaikki tietojärjestelmän osat voidaan tunnistaa jollain tapaa luotettaviksi. Mikäli joku järjestelmän käyttäjä onnistuu kirjautumaan tietojärjestelmään joillain muulla kuin henkilökohtaisella käyttäjätunnuksellaan on tällöin autenttisuus menetetty. (Ruohonen, 2002, 2.)

Käyttäjäntunnistamiseen voidaan käyttää myös muitakin menetelmiä kuin perinteistä käyttäjätunnusta ja salasanaa tai sormenjälkeä. Näitä ovat mm, verkkopankkitunnukset (joilla voi esimerkiksi tunnistautua veroviraston sivuille) tai sirullisella henkilökortilla. (Ruohonen, 2002, 3.)

Kiistämättömyyden tavoitteena on pystyä todistamaan tietojärjestelmissä tehdyt tapahtumat luotettaviksi. Esimerkiksi jos käyttäjä onnistuu tilamaan jostain verkkokaupasta tuotteen ja myöhemmin kiistää tilanneensa mitään verkkokaupasta. Tällaisessa tilanteessa verkkokaupan kiistämättömyys on menetetty. (Ruohonen, 2002, 3.)

Eheyden tavoitteena on, ettei mitkään tietojärjestelmän tiedoista pääse muuttuman vahingossa tai ilman että niitä muuttaa käyttäjä jolla on käyttöoikeudet jotka mahdollista-

vat muutosten teon. Jos tietojärjestelmään päästään tekemään muutoksia luvattomasti, kyseisen tiedoston tai viestin eheys on menetetty. (Ruohonen, 2002, 3.)

Käytettävyyden tavoitteena on, että tietojärjestelmään tallennetut tiedot ovat aina käyttäjien käytettävissä. Käyttäjän kannalta tämä tietoturvapalvelu on kaikkein näkyvin sekä tärkein palvelu tietojärjestelmässä. Ylläpitäjän kannalta tämä on kaikkein monimutkaisin sekä vaikeimmin saavutettavissa oleva palvelu. (Ruohonen, 2002, 3.)

2.1.3 Tietoturvan osa-alueet

Tietoturva on tietoturvan periaatteiden lisäksi jaettu erilaisiin osa-alueisiin, jotka jaetaan yleensä seuraaviin osa-alueisiin.

- tietoaineiston turvallisuus
- ohjelmistoturvallisuus
- tietoliikenneturvallisuus
- fyysinen turvallisuus
- laitteistoturvallisuus
- henkilöturvallisuus
- käyttöturvallisuus
- hallinnollinen turvallisuus

(Ruohonen, 2002, 4.)

Yllä mainituista tietoturvan osa-alueista kaikki eivät ole etähallinnoinnin näkökulmasta oleellisia. Tästä syystä käsittelen vain etähallinnoinin kannalta oleellisimman osa-alueet.

Tietoaineistonturvallisuus on tietoturvan ilmeisin osa-alue ja tarkoittaa tietojen sekä tiedostojen suojaamista. Joskus tietoturvan ajatellaan koostuvan vain tästä osasta. Tapoja joilla tietoaineiston turvallisuutta voidaan parantaa, on erilaisia. Näitä ovat esimerkiksi: toimiva virustorjuntaohjelma, säännöllisten varmuuskopioiden ottaminen (laiterikkojen tai laitteiston katoamisen varalta) sekä oikeanlaisten käyttöoikeuksien määritteleminen käyttäjille. (Ruohonen, 2002, 4.)

Jos ajattelee tietoaineistoturvallisuutta etähallinnanriskien kannalta, olisi hyvä kun käyttäjän aloittaessa arkaluontoisten tiedostojen käsittelemisen tulisi hänen syöttää tunnistetietonsa ennen kuin hän pääsee tiedostoihin käsiksi. Esimerkiksi yleensä yritykset säilyttävät kaiken datansa verkkolevyillä ja jokaisella käyttäjällä on omat henkilökohtaiset tunnuksensa joilla on tietynlaiset pääsyoikeudet näihin datoihin. Kun käyttäjä ottaa verkkolevylle yhteyden työkoneeltaan ensimmäisen kerran kysyy kone käyttäjän tunnuksia. Yleensä koneen muistiin voi tallettaa sekä verkkolevyn osoitteen että käyttäjätunnuksen ja salasanan, jotta jatkossa kun käyttäjä yhdistää verkkolevylle hänen tunnuksia ei kysytä enää uudeleen. Tämä on hyvin käyttäjäystävällinen ratkaisu, mutta jos koneelle pääsee tunkeutumaan ulkopuolinen käyttäjä. Tällöin hänki pääsee samoihin verkkolevyn tiedostoihin joihin koneen käyttäjäkin pääsee.

”Ohjelmistoturvallisuudella tarkoitetaan tietojärjestelmässä käytettyjen ohjelmien lisenssien ylläpitämistä sekä näiden ohjelmien suojaamista luvattomalta käytöltä. ” Lisenssien ylläpito on tärkeää koska lisenssien ollessa kunnossa voidaan olla varma että ohjelmisto on aito sekä hankittu luotettavalta toimittajalta. Tällöin ohjelmat todennäköisesti eivät sisällä haittaohjelmia, eivätkä ne lakkaa toimimasta yllättäen. Vikatilanteissa on mahdollista olla yhteydessä valmistajan tukeen ja saada apua. (Ruohonen, 2002, 4.)

Mikäli tietojärjestelmissä käytetään laittomia ohjelmistokopioita, se riskeeraa tietoturvan esimerkiksi seuraavasti: jos ohjelma on ladattu laittomasti netistä uTorrentin kautta, ohjelma saattaa sisältää erilaisia haittaohjelmia sekä ohjelma ei välttämättä toimi kunnolla. Jos ohjelma sisältää haittaohjelmia tietojärjestelmään saattaa päästä etänä ulkopuolisia, jotka voivat tehdä järjestelmään tuhoja.

2.1.4 Henkilö- ja käyttöturvallisuus etähallinnoinnin näkökulmasta

Henkilöturvallisuuden tarkoituksena on suojata tietojärjestelmiä käyttäjien aiheuttamilta uhilta. Käyttäjien tekemiä vahinkoja ei voi täysin estää, mutta tahattomia vahinkoja voidaan yrittää vähentää käyttäjiä ohjeistamalla miten käyttää ja liikkua tietojärjestelmissä oikein. Tahallisia vahinkoja voidaan vähentää pitämällä huolta siitä, että kaikilla käyttäjillä on vain ne oikeudet joita he oikeasti tarvitsevat. (Ruohonen, 2002, 5.)
Etähallinnan kannalta esimerkkiuhka voisi olla että käyttäjä asentaa jonkin ei työntekoon liittyvän ohjelman koneellensa, joka sisältää viruksen jonka avulla hakkeri pääsee yrityksen tietojärjestelmään etänä käsiksi. Tämä voidaan ehkäistä tiukentamalla käyttäjien oikeuksia niin että vain it-osastolla on oikeudet asentaa koneille ohjelmia.

Käyttöturvallisuuden tarkoituksena on, että tietojärjestelmää käytetään turvallisesti. Käyttöturvallisuus liittyy suoraan henkilöturvallisuuteen, koska jos tietojärjestelmää käytetään huolimattomasti tai väärin on se iso uhka koko tietojärjestelmälle. Esimerkiksi jos käyttäjillä on liian helposti murrettavat salasanat tietojärjestelmään tai etähallinnointiin käytettävät tunnukset eivät koskaan vaihdu tai nekin liian helposti murrettavissa. (Ruohonen, 2002, 5.)

Hallinnollinen turvallisuuden tavoitteena on johtaa kaikkia tietoturvan osa-alueita ja varmistaa, että kaikki nämä osa-alueet ovat riittävän hyvin hoidettu. Hallinnollisen tietoturvallisuus myös luo tietoturvaa sekä kehittää tietoturvasuunnitelmaa.
(Ruohonen, 2002, 5.)

2.1.5 Salasanan tärkeys etähallinnoinnissa

Yleensä etähallinnoinnin suorittaa yrityksessä toimiva it-tukihenkilö, joka hoitaa myös it ylläpitotoimenpiteet. Heillä on joko yhteinen järjestelmänvalvojatunnus tai henkilökohtaiset tunnukset joilla on järjestelmänvalvojan oikeudet. Etähallinnointiin voi olla olemassa täysin omat tunnuksensa tai etähallinnointi voidaan suorittaa samoilla tunnuksilla kuin muutkin ylläpitotoimenpiteet. Tämä riippuu täysin yrityksen toimintatavoista ja

etähallinnointiin käytettävistä ohjelmista. Joka tapauksessa hallinnointitunnuksen salasana jolla pääsee etähallinnoimaan, täytyy olla erittäin hyvä ja vaikeasti ulkopuolisen selvitettävissä. Salasanan täytyy olla hyvä, koska aina kun aloitetaan etähallinnointi tarvitaan ainakin salasana jotta etäyhteyden voi muodostaa kohdelaitteeseen.

2.1.6 Millainen on toimiva salasana?

Hyvässä salasanassa, tulisi olla isoja ja pieniä kirjaimia, numeroita, erikoismerkkejä. Ja näitä merkkejä tulisi olla vähintään 8 merkkiä mielellään enemmän. Salasana ei saa olla minkään kielen sana joka löytyy sanakirjasta, se ei myöskään saa olla johdettua käyttäjätunnuksesta mitenkään, se ei myöskään saa olla sellainen sana jonka voi helposti yhdistää käyttäjään (harrastukset, lemmikkiin tai perheenjäsenen nimi, syntymäpäivä jne..). (Ruohonen, 2002, 151.)

Hyvän salasanan luominen yllä mainittujen ohjeiden mukaan on haastavaa, mutta helppoja tapoja parantaa salasanan turvallisuutta on muutama. Esimerkiksi helppo tapa parantaa salasanan turvallisuutta on keksiä ensin jokin sana, kirjoittaa sana ylös ja muokata sanaa erikoismerkkien, isojen kirjaimien ja numeroiden avulla ja lopuksi piilottaa tämä sana satunnaisen merkkijonon sisälle. (Ruohonen, 2002, 152.)

Yleisesti sanotaan, ettei salasanaa saisi koskaan kirjoittaa mihinkään ylös, mistä hakkeri tai jokin muu ulkopuolinen voi sen löytää. (Ruohonen, 2002, 152.) Etähallinnan kannalta salasanan sijainti esimerkiksi näppäimistön alla ei ole oleellinen, koska etänä työskentelevä hakkeri ei sitä löydä.

Salasanaa ei koskaan saisi kertoa kenellekään eikä kirjoittaa ylös selkokielisenä. Vaihtamalla salasanan tarpeeksi usein saa lisättyä paljon tietoturvaa. Salasana olisi hyvä vaihtaa myös aina silloin jos on syytä epäillä sen vuotaneen vääriin käsiin. (Ruohonen, 2002, 152.)

2.2 Etätyön ja etähallinnoinnin uhat ja riskit

Etänä tehtävä työ on tietoturvan kannalta haasteellista. Etätyö termin voi ymmärtää monella eri tavalla. Monelle etätyön teko tarkoittaa työntekoa esimerkiksi kotoa käsin. Tässä opinnäytetyössä kun puhun etätyöstä tarkoitan sillä it-tukihekilön tekemää etähallinnointityötä työpaikalla. Jos etähallinnointi tapahtuu yrityksen tiloissa eli käytännössä suojatussa sisäverkossa on uhat ja riskit pystytty paremmin minimoimaan kuin julkisessa verkossa tapahtuva etätyö tai etähallinnointi. Yrityksen sisäinen verkko on suljettu verkko johon ulkopuolisten tahoja on vaikeampi päästä käsiksi. (Järvinen, 2002, 119.)

2.2.1 Uhka ja Riski

Mitä termit "uhka" ja "riski" tarkoittavat? Sivistyssanakirja määrittelee sanan "uhka" seuraavasti "mahdollisesti toteutuva epämieluisa, pelottava tai vahingollinen seikka". (Sivistyssanakirja, http://www.suomisanakirja.fi/uhka .)

Sivistyssanakirja määrittelee sanan "riski" seuraavasti "negatiivisen seurauksen ja tämän seurauksen todennäköisyyden tulo (esim. onnettomuuteen tai sairauteen)". (Sivistyssanakirja, http://www.suomisanakirja.fi/riski .)

Riski on uhan ilmentymisen todennäköisyys. Uhka sisältää mitä tapahtuu ja mitä uhasta aiheutuu, jos se toteutuu. Uhkia ja riskejä on etähallinnoinnin kannalta monenlaisia ja niitä on paljon. On myös monenlaisia keinoja suojautua ja varautua niihin. Yritykset tekevät uhka kartoituksia ja riskianalyyseja, jotta voivat varautua uhkiin ja pienentää uhkasta seuraavia riskejä.

Miten tällainen kartoitus sitten tehdään? Ensiksi täyty määritellä mitä halutaan turvata, jotta voidaan miettiä mahdollisia uhkia ja uhista seuraavia riskejä. (Järvinen, 2002, 113.)

2.3 Esimerkkejä etähallinnoinnin uhista

Etähallinnoinnissa kuten kaikessa on omat riskinsä. Etähallinnoinninriskit liittyvät tietoturva-asioihin, koska etähallinnointi ei toimi jos tietoturva-asiat eivät ole kunnossa. Helpoin ja selkein tapa kertoa etähallinnoinnin uhista (uhat johtavat riskeihin) on mielestäni kertoa ne esimerkkien avulla. Olen listannut tähän uhkia ja riskejä joihin olen itse törmännyt työelämässä etähallinnointi toimenpiteitä suorittaessani.

Tapaus 1. Etäyhteyden muodostus väärään laitteeseen. Ennen etäyhteyden muodostusta on selvitetty mihin laitteeseen tai laitteisiin etäyhteys muodostetaan. Uhka voi olla että otetaan vahingossa väärään laitteeseen etäyhteys. Esimerkiksi etähallinnoitavan laitteen ip-osoite on kirjoitettu väärin. Tällöin riskinä on että etäyhteys tulee laitteen käyttäjälle yllätyksenä, jolloin auki olevat tiedostot paljastuvat. Tämän uhkan todennäköisyys riippuu pitkältä siitä millaista etähallinnointi tuotetta käytetään.

Tapaus 2. Käyttäjä on tietoinen, että hänen laitteeseensa otetaan kohta etäyhteys. Uhkana voi kuitenkin olla, että etäyhteydenmuodostus tapahtuu liian aikaisin kohdelaitteeseen. Jos etäyhteys muodostetaan liian aikaisin kohde laitteeseen, riskinä tässäkin tapauksessa on, että kohde laitteen tiedostot paljastuvat, koska laitteen käyttäjä ei ole välttämättä ehtinyt sulkea tiedostoja ennen etäyhteyden muodostumista.

Tapaus 3. Haittaohjelma etäyhteyden kohdelaitteessa. Kohde laitteessa saattaa olla haittaohjelma joka tallentaa etäyhteydenmuodostajan kaikki näppäinpainallukset. Tällöin järjestelmänvalvojan salasanat saattavat vuotaa ulkopuolisille. Riskinä on, että koko yrityksen tietoturva vaarantuu vakavasti, koska vuotaneilla tunnuksilla saa halutessaan tuhoa aikaan.

Tapaus 4. Hidas Internet yhteys etäyhteydessä olevien laitteiden välillä. Mikäli internet yhteys, jonka avulla muodostetaan etäyhteys, on liian hidas tai muuten heikko saattaa etähallinnointi olla haastavaa. Riskinä on, että etähallinnointia ei voi suorittaa jolloin laiteen luoda täytyy erikseen käydä.

2.4 Etähallinnoinnin hyödyt

Etähallinnoinnin onnistuttua IT-ympäristön ylläpitoa on huomattavasti helpompaa, tehokkaampaa ja nopeampaa. Ongelmatilanteiden ratkaiseminen on usein nopeampaa koska aikaa ei mene laitteet luokse siirtymiseen ja samanaikaisesti it-tukihenkilö voi ratkaista monen eri käyttäjän ongelmia. Esimerkiksi jos isossa ympäristössä pitää asentaa kaikille koneille kriittisiä päivityksiä, etähallinnoinnin avulla käyttäjien työaikaa menee vähemmän hukkaan, koska he saavat päivityksen nopeammin ja jos päivitykset pystymään vielä ajamaan taustalla tällöin käyttäjä voi samanaikaisesti tehdä töitä. Etähallinnointi on myös käyttäjän kannalta todella hyvä hyödyllinen, koska nykypäivänä tehdään paljon etätöitä joko kotoa käsin tai työmatkalla ollessa. Yrityksellä jossa työntekijä työskentelee saattaa olla monia eri toimipisteitä ja jokaisessa niissä ei välttämättä ole omaa it-tukea joten etähallinnointi mahdollistaa sen, että käyttäjä voi saada it-tukea riippumatta siitä missä päin käyttäjä on.

3 iPadin etähallinnointi

3.1 iPadin etähallinnoinnin merkitys

iPadin etähallinnoinnin tarpeellisuus riippuu täysin siitä mihinkä tarkoitukseen iPad on hankittu. Esimerkiksi jos se hankittu vain perheen viihdekäyttöön, jolloin laitteeseen ei tallenneta mitään yrityssalaisuuksia tai muita arkaluontoisia asioita, etähallinnoinnilla ei niinkään ole merkitystä eikä siitä ole kovin suurta hyötyä.

Mikäli laite on hankittu sekä työ että viihde käyttöön, olisi hyvä jos etähallinnointi on käytössä. Esimerkiksi käyttäjä on asentanut laitteeseen työsähköpostinsa, jotta hän voi lukea sähköposteja kotona tai työmatkoilla. Laitteen kadotessa esimerkiksi työmatkalla se voi joutua ulkopuolisten käsiin jolloin sähköpostissa olevat yrityssalaisuudet saattavat paljastua. Jos iPadin on hankkinut yritys työntekijälleen työn tekoa varten, etähallinnointi on välttämätöntä. Työsähköpostin lisäksi laitteessa saattaa olla tässä tapauksessa muitakin yrityksen salaisia dokumentteja jotka voivat paljastua jos laite katoaa.

Toimivalla etähallinnoinnilla voidaan ehkäistä joissain tapauksissa mm. yrityssalaisuuksien vuodot jos laite katoaa tai varastetaan. Jos laitteen omistaa yritys etähallinnoinilla myösvoidaan helpottaa laitteen ylläpitoa ja täten vähentää it-tuen työmäärää.

3.2 iPadin etähallinnointi käytännössä

iPadin etähallinnoin tärkeimmät kaksi toimintoa ovat etätyhjennys ja laitteen paikannus. Tapoja joilla iPadin voi tyhjentää etänä on muutama, mutta itse etähallinnointiohjelmia ei ole kovin montaa markkinoilla tällä hetkellä.

3.2.1 iPadin etähallinnointiin tarkoitetut ohjelmat

iPadin etähallinnointia varten ei ole vielä montaa ohjelmaa olemassa. Tästä syystä päätin tutkia kokevatko laitteen käyttäjät etähallinnoinnin tarpeelliseksi. Samalla tutkin mihin kaikkeen laitetta yleensä käytetään, sekä ovatko käyttäjät kokeilleet laitteen valmistajan omaa etähallinnointi tuotetta. Käyttäjien kokemuksista kerron lisää tutkimus luvussa.

AppStoresta löytyy tällä hetkellä vain yksi sovellus jolla voi etähallinnoida iPadia. Ohjelman nimi on ”Etsi iPhone” ja se on ilmainen Applen oma tuote. Tällä ohjelmalla pystyy hallinnoimaan iPadin lisäksi Applen muitakin tuotteita mm iPhoneja sekä Mac tietokoneita. Ohjelman käyttöliittymä on selkeä, hyvä ja käyttäjäystävällinen, joten laitteen etähallinnointi on helppoa, jopa peruskäyttäjille. Sovelluksen toimintoja ovat laitteen paikannus, tyhjennys, laitteen lukitseminen, viestien lähettäminen kadonneeseen laitteeseen, hälytysäänen aktivoiminen. iPadia voi etähallinnoida niin kauan kunnes laitteessa on virtaa jäljellä ja niin kauan kuin laite on Internet yhteyden päässä.

Toinen tuote tai pikemminkin tapa jolla iPadin etähallinnointi onnistuu ilmaiseksi, on Microsoftin Exchange sähköposti-serveri. Exchange-serverin kautta onnistuu ainoastaan etätyhjennys jos laite on Internet yhteyden päässä ja jos laitteeseen on lisätty Exchange sähköpostitili. Etätyhjennys onnistuu myös Microsoft Office 365, sähköpostipalvelun kautta.

4 iPadin etähallinnointi MDM palvelulla

MDM (mobile device management) palvelun tarkoitus on helpottaa ja mahdollistaa mobiililaitteiden valvontaa, laitehallinnointia ja etenkin etähallinnointia. MDM palveluilla voi hallinnoida iOS, Android sekä Windows alustalla toimivia mobiililaitteita. Voi

kuitenkin olla, ettei kaikilla markkinoilla olevilla MDM palveluilla pysty hallinnoimaan kaikkia edellä mainitsemiani käyttöjärjestelmiä.

MDM palveluntarjoajia on markkinoilla useita. Appella on mm. tarjolla oma MDM palvelunsa. Kaikissa markkinoilla olevissa MDM palveluissa perusidea on sama. MDM.n idea on helpottaa mobiililaitteiden hallinnointia, pitää laitteiden käyttöjärjestelmä ja sovellukset ajan tasalla sekä varmistaa että tietoturva-asiat ovat kunnossa. Opinnäytetyössäni olen tutkinut N-able Technologies yrityksen MDM palvelua joka on nimeltään N-central.

N-central on alun perin tarkoitettu työasemien, palvelimien sekä aktiivilaitteiden tarkkailuun sekä etähallinnointiin. Nyt palveluun on tullut uutuutena lisäosa joka mahdollistaa myös mobiililaitteiden valvonnan sekä etähallinnoinnin. Lisäosalla pystyy hallinnoimaan iOS ja Android käytöjärjestelmällä toimivia mobiililaitteita. Tämän hetkisessä N-centralin lisäosan versiossa Windows alustalla toimivien mobiililaitteiden hallinnointi ei ole vielä mahdollista.

N-central palvelussa laitteiden hallinnointi tapahtuu selaimen kautta joten ei ole väliä millaiselta laitteelta itse hallinnointi tehdään. Jotta N-centralin palvelu toimii hallinnoitavaan laitteeseen täytyy ensiksi asentaa etähallintaohjelma. Tämän lisäksi laite pitää vielä rekisteröidä asentamalla iPadiin MDM profiili. Näiden toimenpiteiden jälkeen iPadi tulee jonkun ajan päästä näkyviin N-central palveluun.

4.1 N-centralin MDM ja sen toiminnot

N-centralin MDM palvelu muistuttaa perustoiminnoiltaan hyvin paljon Applen omaa ilmaista Etsi iPhone sovellusta. Perustoiminnoilla tarkoitan seuraavia toimintoja etätyhjennys, paikannus, etälukitus, pääsykoodin nollaus sekä kadonnut-tilan aktivointi. Näi-

den toimintojen lisäksi palvelussa on paljon enemmän toimintoja kuin Etsi iPhone sovelluksessa.

Kun laite on liitetty MDM palveluun, kerää palvelu laitteesta ylläpidon kannalta tärkeitä tietoja. Näitä ovat mm. laitteen sarjanumero, tieto onko takuu voimassa, paljonko laitteessa on akkua jäljellä sillä hetkellä, miten paljon laitteessa on käytettyä ja vapaata muistia, mikä käyttöjärjestelmäversio laitteessa on ja onko laite jailbreakattu.

Perustoimintojen ja tärkeiden tietojen keräyksen lisäksi N-centralin MDM palvelussa on lisää muitakin toimintoja. Näitä toimintoja ovat mm. tiedostojen lähettäminen laitteeseen, varmuuskopiointi, ohjelmien etäasennus sekä laitteen skannaus haittaohjelmien varalta.

Etähallinnoinnin sekä tietojen keräyksen lisäksi N-centralin palvelulla voidaan tarvittaessa rajoittaa iPadin käyttöä. Palvelun avulla voidaan estää haluttujen sovellusten toiminta laitteessa kokonaan.

Estotoiminto on hyödyllinen sellaisissa tilanteissa joissa iPad on hankittu johonkin tiettyyn käyttötarkoitukseen. Esimerkiksi työnantaja hankkii iPadeja työntekijöilleen työntekoa varten tai jonkin oppilaitos hankkii iPadeja opetusvälineiksi. Kummassakin tapauksessa laitteen omistaja pystyy halutessaan estää kaikkien viihdekäyttöön tarkoitettujen sovellusten toimimisen laitteessa, käyttämällä mdm palvelua. Viihdesovelluksi on mm. Spotify ja Netflix.

4.1.1 N-centralin MDM palvelun käyttöönotto käyttäjän näkökulmasta

MDM palvelun käyttöönotto on helppoa. iPadiin tai mobiililaitteeseen täytyy ladata ensin MDM etähallinnointiohjelma. Kun etähallinnointiohjelma on asennettu laitteeseen, etähallinnointi voi alkaa eikä käyttäjän tarvitse itse murehtia laitteen ylläpidosta. Palvelun asennusprosessi on helppo ja käyttäjä pystyy tarvittaessa tekemään sen itse.

Olen piirtäny prosessikaavion MDM etähallinnointiohjelman asennus- ja käyttöönotto-prosessin. Prosessikaavio löytyy liitteestä 1.

Kun iPadin käyttäjä haluaa ottaa MDM etähallinnointipalvelun käyttöön, pitää hänen ensin tilata palvelu. Myynti ilmoittaa uudesta tilauksesta ja uuden käyttäjän tiedot ServiceDeskille. ServiceDesk vastaanottaa tiedon ja luo uudelle käyttäjälle tilin MDM palveluun. Kun tili on luotu, lähettää ServiceDesk MDM palvelun kautta uudelle käyttäjälle sähköpostitse kutsun palveluun. Kutsun voi lähettää myös tekstiviestillä jos N-centraliin ostettu tällainen lisätoiminto.

Lähetetyssä sähköpostissa on selkeät ohjeet miten palvelu otetaan käyttöön. Ohjeiden lisäsi sähköpostissa tulee latauslinkki jonka kautta käyttäjä saa ladattua iPadiin MDM etähallinnointiohjelman. Palvelua ei siis voi ottaa käyttöön ilman, että on saanut kutsun palveluun.

Latauslinkki johtaa N-centralin MDM palvelun sivulle, jossa on kaksi erillistä linkkiä. Ensimmäinen linkki johtaa AppStoreen, josta saa ladattua MDM etähallinnointiohjelman. Ladattava ohjelma on ilmainen, mutta käyttäjällä pitää olla käytössä Apple-ID tunnus jotta lataus onnistuu. Kun ohjelma on ladattu ja sen pikakuvake on ilmestynyt iPadiin pitää vielä toisen latauslinkin kautta rekisteröidä iPadi erikseen.

Rekisteröinnissä iPadille latautuu MDM palvelun profiili. Profiili täytyy erikseen asentaa laitteelle. Profiilin asennus tapahtuu muutamalla klikkauksella. Mikäli käyttäjällä on pääsykoodi iPadissa käytössä hänen täytyy syöttää se asennuksen yhteydessä. Edellä mainittujen toimenpiteiden jälkeen etähallinnointipalvelu on käytössä.

4.2 N-centralin MDM palvelun hyvät ja huonot puolet

Palvelussa on hyviä sekä huonoja puolia. Hyviä puolia on mm. se että palvelu kerää laitteesta hyödyllisiä tietoja. Nämä tiedot helpottavat iPadin ylläpitotoimenpiteitä. Esimerkiksi ylläpito saa kätevästi tietoonsa laitteen sarjanumeron tai takuutiedot, ilman että laitteeseen täytyy päästä fyysisesti käsiksi tai ilman että takuutietoja joutuu tarkistamaan Applen sivuilta. N-centralin palvelun tarjoamat hallinnointitoiminnot ovat huomattavasti laajemmat kuin esimerkiksi Applen omassa Etsi iPhone sovelluksessa.

Hyvää palvelussa on myös, vaikka iPadin joutuisi tyhjentämään etänä, jää laitteen tiedot silti MDM palveluun, jollei kyseistä laitetta poista erikseen hallintasivulta. Tietojen pysymisestä on hyötyä esimerkiksi silloin kun laitteen katoamisesta joutuu tekemään rikosilmoituksen poliisille tai vahinkoilmoituksen vakuutusyhtiölle.

Huonoa N-centralin MDM palvelussa on joidenkin toimintojen toimimattomuus tai se että toiminnot toimivat vain osittain. Esimerkiksi laitteen paikannus ei toimi nykyisessä versiossa lainkaan. Myöskään laitteen tiedot eivät päivity palveluun jatkuvasti jostain syystä. Näitä tietoja on mm. paljonko akkua tai muistia on vielä jäljellä sekä paljonko laitteessa on muistia käytettynä.

Mainitsemiini puutteisiin vaikuttaa todennäköisesti nyt käytössä oleva iPadin käyttöjärjestelmä versio ja N-centralin version yhteensopimattomuusongelmat. Täytyy myös muisaa se, että testissä ollut mobiilaitteiden tarkkailu ja etähallinnointi lisäosa on ensimmäinen versio lisäosasta.

Voi olla, että kaikkia toimintoja, jotka toimivat työasemien, palvelimien sekä aktiivilaitteiden kanssa ei saada toimimaan kunnolla mobiililaitteiden kanssa. Tämä selviää kuitenkin vasta myöhemmin jos lisäosasta julkaistaan uusia versioita. Onneksi markkinoilla on muitakin MDM palveluita tarjolla joiden avulla mobiililaitteiden etähallinnointi sekä tarkkailu onistuu.

iPad sekä mobiililaitteet ylipäätänsä eivät ole enää uusi keksintö. Niitä on myyty paljon yrityksille sekä yksittäisille kuluttajille. Tulevaisuudessa veikkaisin mobiilaitteiden käytön lisääntyvän entisestään etenkin yritysmaailmassa. Jos yritysmaailmassa iPadien käyttö työnteossa lisääntyy entisestään N-centralin MDM:n kaltaisille etähallinnointi ja valvonta palveluille tulee enemmän tarvetta. Mikäli näin tapahtuu sovelluskehittäjät huomaavat toivottavasti kysynnän, markkinoille tulee lisää vastaavanlaisia tuotteita ja kilpailu tuotteiden välillä lisääntyy. Jos kilpailu kiristyy tarpeeksi, mobiililaitteiden etähallinnointi tuotteet kehittyvät entisestään.

4.3 Miten N-centralin MDM palvelua voisi kehittää?

Nykyisten toimintojen puutteet olisi hyvä korjata seuraavassa versiossa. Tuotetta testatessani ja aikaisemman etähallinnointiohjelmien käyttökokemuksien perusteella sain idean. MDM palveluun voisi lisätä etätyöpöytä ominaisuuden. Ylläpitäjän ja käyttäjän käyttömukavuutta voisi parantua, jos etähallinnoitsija voisi ottaa iPadiin etätyöpöytäyhteyden. Esimerkiksi kun laitteeseen asennetaan etänä ohjelma, etätyöpöytä ominaisuuden avulla ylläpitäjä voisi itse testata toimiiko juuri asennettu ohjelma oikein. Ongelmatilanteissa ylläpitäjä voisi etätyöpöydän avulla ohjeistaa käyttäjää etänä. Voi kuitenkin olla ettei tällaista etätyöpöytä ominaisuutta saada toimimaan mobiililaitteissa etenkään iPadissa, johtuen iPadin käyttöjärjestelmän rajoituksista.

5 SWOT analyysi iPadin etähallinnointipalvelusta

On erilaisia tapoja toteuttaa iPadin etähallinnointipalveluna. Teoriaosuudessa olen käsitellyt millaisia asioita on hyvä ottaa huomioon kun lähdetään toteuttamaan etähallinnointia. N-centralin MDM palvelunkuvauksessa kerroin millainen kyseinen palvelu on,

ja miten se eroaa Applen omasta etähallinnointipalvelusta. Kummassakin tuotteessa oli hyviä sekä huonoja puolia.

Tässä luvussa käsittelen iPadin etähallinnointipalvelua SWOT analyysin avulla. Olen miettinyt iPadin etähallinnointipalvelun vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia yleisellätasolla.

Mikä on SWOT analyysi? SWOT analyysi on yksinkertainen ja yleisesti käytetty analysointimenetelmä, jonka avulla voidaan selvittää asioiden vahvuudet, heikkoudet sekä tulevaiduuden mahdollisuudet ja uhat. SWOT on lyhenne sanoista; strength (vahvuus), weakness (heikkous), opportunity (mahdollisuus) ja threat (uhka).
(SWOT analyysi, http://www.qualitas-forum.fi/Laadunty%C3%B6kalut/SWOTanalyysi/tabid/132/Default.aspx .)

5.1 Vahvuudet

iPadin etähallinnointipalvelun vahvuudet.

- Käyttäjäystävällinen
- Helppo toteuttaa
- Helppoa rahaa
- Helppo ottaa käyttöön

Käyttäjäystävällinen, koska kun etähallinnointipalvelu otetaan käyttöön, käyttäjän ei itse tarvitse enää tehdä mitään. Palvelun ollessa käytössä, käyttäjän ei tarvitse murehtia laitteen käyttöjärjestelmän tai sovellusten ylläpidosta.

Toimivan tuotteen avulla etähallinnointi on helppo toteuttaa. Toimivalla tuotteella tarkoitan tuotetta, jossa on tarvittavat ominaisuudet ja ne toimivat niinkuin pitääkin. Toimiva tuote on myös helppo ottaa käyttöön, jolloin itse asennukseen ei mene turhaa aikaa. Käyttäjä voi itse suorittaa asennuksen tai tukihenkilö voi tehdä sen käyttäjän puolesta.

Helppoa rahaa yritykselle silloin kun palvelu on hinnoiteltu oikein. Palvelu myös tuottaa tällöin hyvin, koska samanaikaisesti voidaan hallinnoida montaa iPadia yhtä aikaa, ja silti jokaisesta hallinnointavasta laitteesta saadaan laskutusta erikseen.

5.2 Heikkoudet

iPadin etähallinnointipalvelun heikkoudet.

- Jos laite ei ole Internetin päässä, etähallinnointi on mahdoton toteuttaa.
- Maksullinen palvelu, josta ilmainen versio kaikkien saatavilla.
- Käyttäjä ei voi itse hallinnoida laitettaan etänä.
- Kaikki toiminnot eivät välttämättä toimi heti tai lainkaan.
- Jos etähallinnointia tarvitaan toimistoajan ulkopuolella, sitä ei ole mahdollista saada heti.
- Asiakkaista eivät vielä ole kiinnotuneita tai tietoisia palvelusta.

Etähallinnointipalvelun heikkouksia on vielä paljon ja niihin ei pysty välttämättä vaikuttamaan mitenkään tällä hetkellä. Asiakkiden kiinnostuksen puute tai tietämättömyys palvelun olemassa olosta. Tähän kohtaan voidaan vaikuttaa oikeanlaisella markkinoinnilla.

5.3 Mahdollisuudet

- Oikein myytynä, helppoa rahaa
- Asiakkaat eivät vielä tiedä palvelusta

Mainitsin kohdan palvelun huono tunnettavuus myös heikkouksissa. Se on heikkous mutta samalla mahdollisuus, koska jos käyttäjät eivät ole aikasemmin kuulleet iPadin etähallinnointipalvelusta, heillä ei todennäköisesti ole palvelusta negatiivista mielikuvaa. Tällöin markkinoinnissa tai sen avulla ei tarvitse yrittää poistaa negatiivista kokemusta tai mielikuvaa etähallinnointipalvelusta.

5.4 Uhat

- Applen ilmainen tuote sekä muut kilpailevat tuotteet.
- Asiakkaat eivät innostu tai koe palvelua tarpeelliseksi.

Jotta Applen ilmainen tuote ei olisi uhkana, käyttöön valittavan tuotteen pitäisi olla parempi kuin Applen tarjoama tuote. Valitun tuotteen pitäisi pystyä tarjoamaan etähallinnointipalvelun ostajalle enemmän hyötyä kuin vastaava ilmainen tuote. Tuotteen hinnoittelun pitää myös olla kunnossa. Tuotetta täytyy myös osata kaupata ostajalle oikein. Esimerkiksi korostamalla tarpeeksi kaikkia ominaisuukia joita ilmaisessa tuotteessa ei ole. Täytyy muistaa, että asiakas tyytyy helposti mielummin ilmaiseen kuin maksaa samanlaisesta palvelusta.

Yllämainittujen kohtien avulla sekä tekemieni kahden eri kyselyn perusteella mietin kehitysehdotukset luvussa miten iPadin etähallinnointipalvelua voisi ja miten sitä kannattaisi kehittää nykyisestä.

6 Käyttäjätutkimus

Ennen kuin tein weblomakkeella kyselyn iPadin käyttäjille, kartoitin muutamien it-tukihenkilöiden kokemuksia iPadien tai muiden mobiililaiteiden etähallinnoinnista.

Lähetin sähköpostitse kyselyn kaikille lähituessa tai ServiceDeskissä työskenteleville henkilöille. Esitetyt kysymykset olivat ”Onko teistä kukaan joutunut mitenkään etähallinnoimaan asiakkaiden mobiililaitteita? Esimerkiksi paikantamaan tai tyhjentämään laitteita etänä kun laite on varastettu tai kadonnut? Jos on, niin mitä laitteelle on tehty etänä ja mitä tuotetta on käytetty etähallinnointiin (iCloud, Exchange…) ?”

Vastauksia tuli vain muutama. Kaikki vastaajat olivat joskus yrittäneet etähallinnoida jotain mobiililaitetta. Mobiililaiteiden etähallinnointitapauksia ei kuitenkaan ollut kovin montaa. Puhelimia oli enemmän etähallinnoitu kuin iPadeja. Syynä iPadien vähempi etähallinnoinnin tarve oli se, että asiakkaista jotka omistavat iPadin olivat hankkineet laitteen itse. Jos työntekijä on hankkinut laitteen itse, laitteen etähallinnointi ei kuulu työnantajan ostaman it-tuen piiriin. Tällöin kadonneista tai varastetuista iPadeista ei välttämättä kerrota lainkaan it-tukihenkilölle.

Etähallinnointi jota mobiililaitteille oli tehty, oli pääasiassa paikannus tai laitteen tyhjentämistä etänä. Osa mobiilaitteille tehdystä etähallinnoinnista ei ollut onnistunut, koska tieto kadonneesta laitteesta oli tullut it-tukihenkilölle liian myöhään. Laitteesta oli ehditty katkaisemaan virta tai siitä oli akku ehtinyt loppumaan. Etähallinnointia oli tehty iCloudin tai Exchage-serverin kautta.

6.1 Kyselyn tiedot

Vastauksia kyselyyn tuli yhteensä 44 kappaletta. Vastausaika kyselyyn kesti vain viisi päivää aikataulullisista syitä. Julkaisin kyselyn maanantai iltana 13.5 ja kysely sulkeutui perjantaina 17.5 puolen yön aikaan.

Alun perin kysely piti tehdä iPadin käyttäjille, jotka olivat ostaneet laitteen työnantajaltani. Tämä ei kuitenkaan ollutkaan mahdollista joten jouduin ottamaan varasuunnitelman käyttöön. Julkaisin linkin kyselyyn omalla facebook seinälläni sekä lähetin kyselylinkin niille tutuilleni joiden tuttavapiirissä tai töissä käytettiin iPadeja.

Kysymykset löytyvät liitteestä 2.

6.2 Tulosten analysointi

Kyselyä miettiessäni halusin ensimmäisenä selvittää mihin iPadia käytetään sekä kuka laitteen on hankkinut. Saatujen vastausten perusteella laitetta käytetään pääasiassa omaan käyttöön eli viihdekäyttöön sekä töiden tekemiseen. Suurin osa vastaajista vasta-

si, että on hankkinut iPadin itse, mutta myös työnantajan hankkimia laitteita oli paljon. Tarkentavina kysymyksinä olisi voinut olla, onko työnantaja hankkinut laitteen työntekijälle työntekoa varten vai lahjaksi omaan käyttöön, sekä montako iPadia käyttäjällä on käytössään. Vastaajista osa saattaa käyttää iPadia töissä töiden työjuttuihin sekä omistaa samanlaisen laitteen itse.

Kahden ensimmäisen kysymyksen vastausten perusteella voisi sanoa, että vaikka suurin osa on hankkinut iPadinsa itse omaan käyttöön, niin silti laitetta käytetään jollain tavalla työntekemiseen. Jos iPadiin synkronoidaan työsähköposti ja laite katoaa saattaa se olla yritykselle riski, mikäli työsähköpostit päätyvät vääriin käsiin. Tällä perusteella yrityksille tarjottavaa mobiilaitteiden etähallinnointia voisia laajentaa myös työntekijöiden itse ostamiin laitteisiin jos niissä on työsähköposti synkronoituna.

Kaksi ensimmäistä kysymystä selvitti millaiseen käyttöön iPad oli hankittu, mutta etähallinnoinnin kannalta on myös tärkeä tietää minkälaista dataa laitteessa on. Seuraavilla kahdella kysymyksellä halusin selvittää; onko iPadiin synkronoitu työsähköposti sekä jos laite katoaisi olisi se riski työnantajalle. Suurin osa vastaajista ei ollut lisännyt työsähköpostia laitteeseen eikä pitänyt laitteen katoamista riskinä työantajalle. Näiden vastausten perusteella voisi sanoa, että yritys ei välttämättä hyötyisi juurikaan mobiilaitteiden etähallinnointipalvelun laajentamisesta työntekijöiden itse hankkimiin mobiililaitteisiin. Kuitenkin kannattaa muistaa, että iPadien ja muiden mobiililaitteiden käyttö lisääntyy koko ajan joten etähallinnoinnin tarve saattaa hyvinkin kasvaa.

Kyselyllä halusin selvittää myös sen, että miten suosittu Applen tarjoaman ilmainen etähallinnointipalvelu on iPad käyttäjien keskuudessa. Suurinmalla osalla kyselyyn vastaajista oli Applen oma etähallinnointipalvelu käytössä ja suosituimmat toiminnot joita oli käytetty oli varmuuskopiointi sekä paikannus. Vastauksien perusteella hirveän moni ei ollut onneksi joutunut käyttämään laitteen etätyhjennystä. Oli posiitivista huomata, että yli puolet vastaajista piti etähallinnointia tärkeänä. Etähallinnointipalvelun tulevaisuuden kannalta tämä on todella hyvä juttu.

Olin todella positiivisesti yllättynyt siitä, että vastaajista vajaa puolet käytti iPadissa pääsykoodia. Samalla yllätyin siitä, että kaikki vastaajat eivät olleet tietoisia, että laitteen saa lukittua pääsykoodilla.

Koska opinnäytetyöni yksi tarkoitus oli selvittää miten etähallinnointipalvelua voisia kehittää kysyin kyselyssä, että haluisivatko käyttäjät että heidän ei tarvitsisi itse huolehtia laitteensa päivityksistä. Yli puolet vastaajista vastasi, ettei haluisi päivitysten asentuvan automaattisesti. Tämä vastaus on hieman ristiriidassa sen tiedon kanssa, että vastaajat pitivät etähallinnointia tärkeänä. Olisi mielenkiintoista tietää, että millaista etähallinnointia vastaajat pitävät tarpeellisena.

Kyselyn viimeiset kaksi kysymystä käsitteli laitteen käyttöä ja mahdollisia kommetteja ongelmatilanteista. Näihin kysymyksiin ei ollut pakko vastata. Halusin tietää ongelmantilanteista, koska ongelmista olisi voinut saada ideoita etähallinnointipalvelun kehittämiseen. Saadut vastaukset olivat sellaisia joihin etähallinnoinnista ei olisi ollut apua.

Tekemäni kyselyn perusteella sai jonkilaisen kuvan siitä, olisiko etähallinnointipalvelulle tarvetta. Joidenkin kysymysten vastauksista sai hieman ristiriitaisia vastauksia, joita voi tulkita monella tapaa. Paremman kuvan olisi saanut jos vastaajia olisi ollutt enemmän ja jos tarkentavia kysymyksiä olisi ollut lisää.

Kyselyn perusteella sanoisin, että etähallinnointipalvelulle on tulevaisuudessa paljon enemmän tarvetta kuin tällä hetkellä. Ne jotka tarvitsevat tällä hetkellä iPadiinsä etähallinnointia pärjää hyvi Applen omalla tuotteella.

7 Johtopäätökset

Testailin N-central MDM etähallinnointiohjelman eri toimintoja. Sain tuloksia, joita en osannut etukäteen odottaa. Aluksi ohjelma vaikutti todella lupaavalta ja kätevältä etähallinnointityökalulta. Ohjelmassa on paljon hyödyllisiä toimintoja, joiden avulla voidaan etähallinnoida laitetta. Ohjelma olisi hyvä tuote ja siitä saisi todennäköisesti hyvän palvelun jos se toimisi niin kuin pitäisi. Suurin osa ohjelman toiminnoista ei kuitenkaan toimi lainkaan.

Ohjelman toimimattomuuden takia en lähtisi kehittämään etähallinnointipalvelua kyseisellä tuotteella. Kyseisessä ohjelmassa on vielä liian paljon kehitettävää. Jos tuotteen seuraavassa versiossa on korjattu kaikki puutteet, voisin harkitan ohjelman testaamista uudelleen. N-central MDM etähallinnointiohjelmassa on siis potenttiaalia, mutta myös todella paljon kehitettävää.

Uskoisin, että tulevaisuudessa vastaavanlaiselle etähallinnointipalvelulle on kysyntää. Etähallinnointipalvelu on sellainen josta moni mobiilaitteen käyttäjä ei todennäköisesti ole vielä kuullut mitään. Käyttäjät eivät todennäköisesti osaa vielä kaivata tällaista palvelua.

Tietokoneeseen verrattuna, iPadin käyttö on vielä vähäistä, mutta veikkaisin, että iPadien ja mobiililaitteiden käyttö ylipäätänsä lisääntyy tulevaisuudessa etenkin yritysmaailmassa. Tällä hetkellä töissä käytettävillä iPadeillä mm. luetaan ja lähetetään sähköpostejan, surffaillaan Internetissä, pidetään kokouksissa mukana muistiinpanovälineenä. Mikäli mobiililaitteiden käyttö lisääntyy työelämässä, myös etähallinnointipalvelun tarve lisääntyy. Etenkin jos iPadia tai mobiililaitteita alettaan käyttämään työnteossa kuten tietokoneita.

iPadin hyviä puolia on mm. laitteena se on helppo ja miellyttävä käyttää. Sitä pystyy käyttämään lähes missä vain, ja sitä on helppo kantaa mukana kaikkialle. iPadille ke-

hitellään koko ajan lisää erilaisia sovelluksia joilla voi tehdä yhä enemmän erilaisia asioita.

Huonoa laitteeessa on se, että vaikka sitä on helppo käyttää, siihen joutuu silti asentamaan erilaisia ohjelmia ja siihen tulee ihan samalla tavalla ohjelmistopäivityksiä joita tietokoneeseenkin täytyy asentaa. Huonoa on myös se, että sen kiintolevylle ei pysty tallentamaan suuria määriä dataa. Laitteelle tallennettuihin datoihin ei yleensä pääse käsiksi, kuin vain sillä ohjelmalla jolla tiedot on laitteeseen tallennettu.

Pilvipalveluiden käyttö yritysmaailmassa on lisääntymässä koko ajan. Uskon sen vaikuttavan iPadin ja muiden mobiililaitteiden läpimurtoon työvälineenä, joka korvaa tietokoneen käyttöä. Pilvipalvelut mahdollistavat sen, että mobiilalaitteilla voidaan tehdä tulevaisuudessa enemmän samoja työtehtäviä mitä nyt tehdään vain tietokoneella. Pilvipalvelut mahdollistavat myös sen ettei laitteille tarvitse enää välttämättä tallentaa fyysisesti dataan, vaan datan voi tallentaa suoraan pilveen.

Itse tulen tulevaisuudessa tutkimaan lisää iPadien käyttöä ja miten sitä voisi hyödyntää vielä enemmän työnteossa. Odotan innolla miten iPadien ja muiden mobiililaitteiden käyttö kehittyy ja mahdollisesti lisääntyy.

Lähteet

Järvinen, P. 2002. Tietoturava & Yksityisyys. Docendo Finland Oy. Porvoo

Ruohonen, M. 2002. Tietoturva. Docendo Finland Oy. Porvoo

http://www.suomisanakirja.fi/riski

http://www.suomisanakirja.fi/uhka

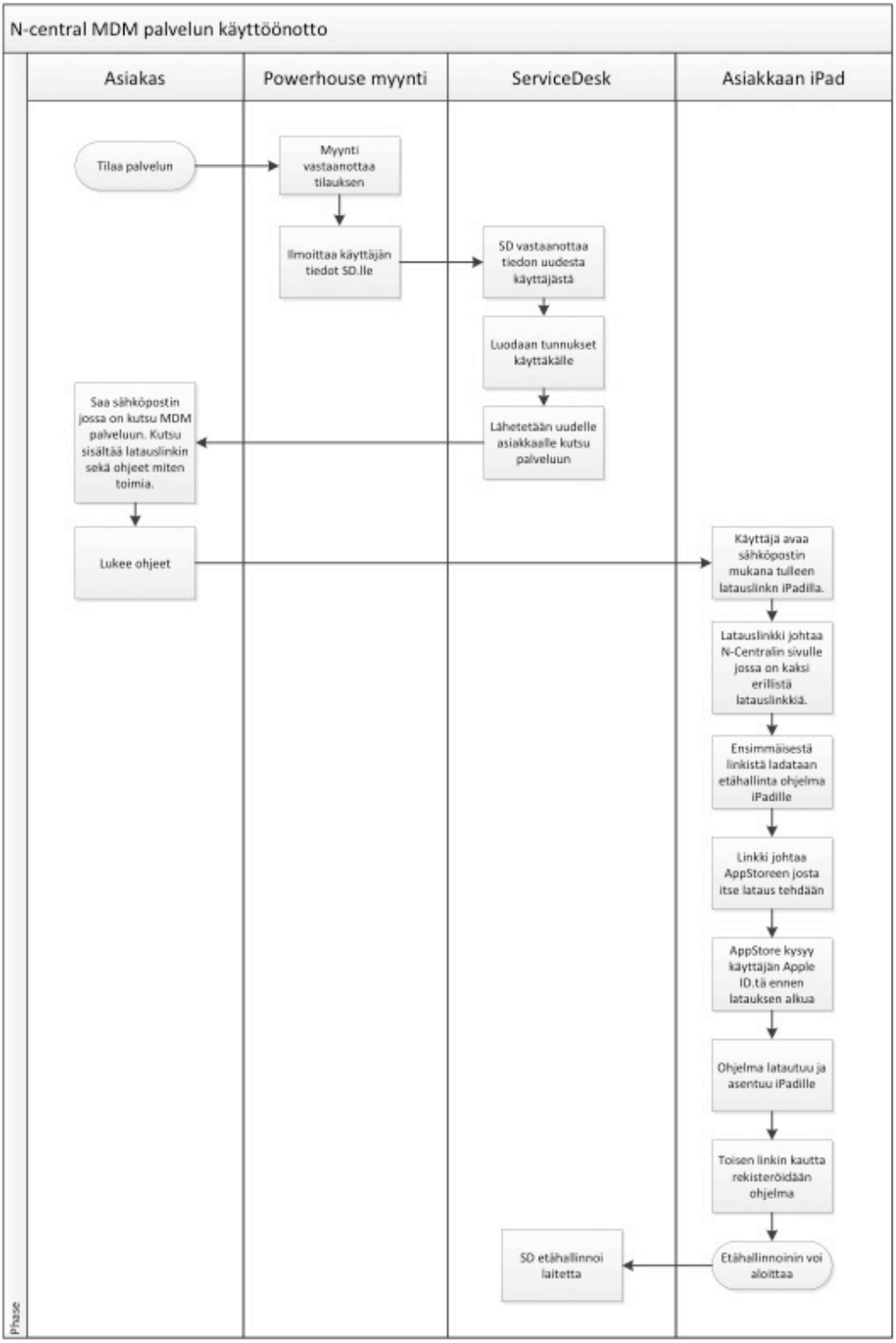
https://www.vahtiohje.fi/web/guest/144

http://www.wisegeek.com/what-is-remote-management.htm

http://www.qualitas-forum.fi/Laadunty%C3%B6kalut/SWOTanalyysi/tabid/132/Default.aspx

Liitteet

Liite 1. Prosessikaavio



Liite 2. Käyttäjäkyselyn kysymykset

1. Mihin käytät iPadia? *

- ◯ Töiden tekemiseen
- ◯ Omaan käyttöön (viihdekäyttöön tms)
- ◯ Kumpaankin

2. Kuka iPadin on hankkinut? *

- ◯ Työnantaja
- ◯ Minä itse
- ◯ Joku muu

3. Oletko lisännyt iPadiin työsähköpostisi? *

- ◯ Kyllä
- ◯ Ei

4. Jos iPadisi katoaisi tai se varastettaisiin, olisiko se riski työnantajellesi? (Sisältääkö iPadi sellaista dataa, joka joutuessaan ulkopuolisten tietoon vahingoittaisi jotenkin yritystoimintaa.) *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

5. Oletko ottanut iCloudin käyttöön? *

- ◯ Kyllä
- ◯ EI
- ◯ En tiedä mikä se on

6. Mitä seuraavia iCloudin toimintoja olet joskus käyttänyt tai testannut? *

- ☐ Varmuuskopiointi
- ☐ Laitteen paikannus
- ☐ Hälytysäänen aktivointi
- ☐ Laitteen etätyhjennys
- ☐ En ole käyttänyt iCloudia koskaan

7. Koetko iPadin etähallinnan tärkeäksi? *

- ◯ Kyllä
- ◯ En

8. Käytätkö iPadissa pääsykoodia? *

- ◯ Kyllä
- ◯ En
- ◯ En ole ollut tietoinen pääsykoodi toiminnosta

9. Haluaisitko, että iPadiisi asentuisi päivitykset automaattisesti, ilman että sinun tarvitsisi itse päivittää laitetta? *

- ◯ Kyllä
- ◯ Ei

10. Onko sinulla ollut teknisiä ongelmia iPadin käyttöönoton tai käyttämisen kanssa?

11. Onko sinulla mitään kommentoitavaa liittyen iPadiin tai iPadin etähallinnointiin? (Ruusut, risut, kehitysehdotukset)