Emppu Kinnaslampi

NYKYAIKAISTEN MOBIILILAITTEIDEN TIETOTURVA YRITYSKÄYTÖSSÄ

Case: Etelä-Savon Tietohallinto Oy

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma

Joulukuu 2012

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** **30.11.2012**
Tekijä(t) Emppu Kinnaslampi	**Koulutusohjelma ja suuntautuminen** **Tietojenkäsittelyn koulutusohjelma**

Nimeke
Nykyaikaisten mobiililaitteiden tietoturva yrityskäytössä
Case: Etelä-Savon Tietohallinto Oy

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli tutkia, minkälaisia tietoturvauhkia nykyaikaisiin mobiililaitteisiin, kuten älypuhelimiin ja tabletteihin kohdistuu erityisesti yrityskäytössä, ja miten näitä uhkia voidaan torjua ja ennaltaehkäistä. Työssä pyrin selvittämään, miten sekä organisaatio että käyttäjä itse voivat mobiililaitteidensa tietoturvaa aktiivisesti omilla toimillaan parantaa sekä minkälaiset valmiudet nykyään merkittävimmissä mobiilikäyttöjärjestelmissä Androidissa, iOS:ssä, Windows Phonessa ja Symbianissa itsessään tietoturvauhkien torjumiseen on.

Mobiililaitteet ovat kehittyneet yhä monipuolisemmiksi ja suorituskykyisemmiksi, joten niillä voidaan hoitaa yhä enemmän asioita, jotka ennen on totuttu tekemään lähinnä PC-työasemilla. Näin ollen mobiililaitteet sisältävät usein suuren määrän yritykselle tärkeitä luottamuksellisia tietoja, joiden menettäminen tai joutuminen vääriin käsiin, joko tahallisesti tai tahattomasti, vaarantaa yrityksen tietoturvan. Uhkia tulee lisää päivä päivältä, joten myös suojautumiskeinojen tulisi olla ajan tasalla.

Opinnäytetyön toimeksiantajana toimi Etelä-Savon Tietohallinto Oy, joka on ICT-palveluita kuntasektorille tarjoava, Kuntien Tiera Oy:n alainen tytäryhtiö. Yrityksellä on asiakkaina mm. Mikkelin kaupunki ja Etelä-Savon Työterveys, joiden mobiililaitteita yritys hallinnoi. Toimeksiantajan asiakkaille tein verkkokyselylomakkeella toteutetun tutkimuksen, jossa selvitin, miten he älypuhelimiaan käyttivät ja miten he ottivat huomioon laitteidensa tietoturvan.

Työn lopputuloksena syntyi mobiilitietoturvadokumentaatio työn toimeksiantajan asiakkaille. Dokumentaation tarkoituksena on lisätä käyttäjien tietoturvatietoisuutta, antaa käytännön vinkkejä hyvän tietoturvan ylläpitämiseksi ja auttaa käyttäjiä saamaan laitteidensa tietoturvaominaisuuksista mahdollisimman paljon irti.

Asiasanat (avainsanat)
tietoturva, tietosuoja, mobiililaitteet, älypuhelimet, tabletit, käyttöjärjestelmät

Sivumäärä	**Kieli**	**URN**
77 sivua + liitteet 8 sivua	Suomi	http://www.urn.fi/URN:NBN:fi:amk-2012120518483

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi	**Opinnäytetyön toimeksiantaja**
Janne Turunen	Etelä-Savon Tietohallinto Oy

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Date of the bachelor's thesis** **30 November 2012**
Author(s) Emppu Kinnaslampi	**Degree programme and option** Business Information Technology

Name of the bachelor's thesis

The security of modern mobile devices in an enterprise environment
Case: Etelä-Savon Tietohallinto Oy

Abstract

Modern mobile devices, such as smartphones and tablets, have become increasingly more versatile and efficient enough to handle tasks that users have previously been able to do mainly with PC workstations. Thus, in an enterprise environment, the mobile devices can contain vital data that is highly confidential to the enterprise. That places the enterprise vulnerable to potential security threats, as losing the confidentiality, integrity or availability of the data held in its mobile devices could ultimately result even in significant financial losses.

My goal in this thesis was to study what the major threats were, and what kind of counter measures could be taken to prevent them. I tried to take into account all the general measures that users themselves could do to actively improve their mobile security. I also studied what kind of security features some of the major mobile operating systems of today, Android, iOS, Windows Phone and Symbian offered to the end user.

My thesis was done for Etelä-Savon Tietohallinto Oy, a subsidiary of Kuntien Tiera Oy, a domestic company offering a wide range of ICT services mainly for the municipal sector. For example, the company handled the mobile device management for the employees of the city of Mikkeli and Etelä-Savon Työterveys Oy. I made a survey to study how these employees operated their smartphones, and how they took into account the security of their mobile devices.

Based on the results, I was able to design a mobile security documentation for Etelä-Savon Tietohallinto Oy to hand out to their clients. Its purpose is mainly to raise information security awareness among the users and to offer some practical advice to maintain a good level of mobile security, and to hopefully get the most out of the security features in their devices.

Subject headings, (keywords)

Information security, data protection, mobile devices, smartphones, tablets, operating systems

Pages	**Language**	**URN**
77 + 8 appendix pages	Finnish	http://www.urn.fi/URN:NBN:fi:amk-2012120518483

Remarks, notes on appendices

Tutor	**Bachelor's thesis assigned by**
Janne Turunen	Etelä-Savon Tietohallinto Oy

SISÄLTÖ

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on tutkia, minkälaisia tietoturvauhkia nykyaikaisiin mobiililaitteisiin, kuten älypuhelimiin ja tabletteihin kohdistuu erityisesti yrityskäytössä, ja miten näitä uhkia vastaan voidaan varautua ja niitä torjua. Pyrin selvittämään, minkälaiset valmiudet eri mobiilikäyttöjärjestelmissä itsessään näiden uhkien torjumiseen on ja miten sekä organisaatio että käyttäjä itse voivat tietoturvaansa aktiivisesti omilla toimillaan parantaa.

Älypuhelimet ovat kehittyneet yhä monipuolisemmiksi ja suorituskykyisemmiksi ja niillä voidaan hoitaa yhä enemmän asioita, jotka ennen on totuttu tekemään lähinnä PC-työasemilla. Yrityksen työntekijät käyttävät älypuhelimia tänä päivänä pelkän kommunikoinnin lisäksi yhä enemmän erilaisten työtehtävien ja askareiden hoitamiseen, kuten vaikkapa sähköpostiin, kalenterikutsuihin ja internetin selaamiseen. (M&M 2012.) Näin ollen älypuhelimet sisältävät usein suuren määrän yritykselle tärkeitä luottamuksellisia tietoja ja näiden tietojen hukkuminen, tuhoutuminen tai joutuminen vääriin käsiin, joko tahallisesti tai tahattomasti, pelkästään huolimattomuudesta johtuen, vaarantaa yrityksen tietoturvan, joka voi johtaa pahimmillaan merkittäviin tappioihin (Lookout Mobile Security 2012a). Lisäksi älypuhelinten tietoturvaa uhkaavat mm. erilaiset haavoittuvuudet ja haittaohjelmat (Symantec 2011, 1 – 3). Lieneekin selvää, että nämä asiat tekevät älypuhelinten tietoturvasta merkittävän, ajankohtaisen ja vakavasti otettavan asian.

Opinnäytetyön toimeksiantaja on Etelä-Savon Tietohallinto Oy, joka on ICT-palveluita kuntasektorille tarjoavan Kuntien Tiera Oy:n alainen tytäryhtiö. Yrityksellä on asiakkaina mm. Mikkelin kaupunki ja Etelä-Savon Työterveys, joiden mobiililaitteita yritys hallinnoi. Tein asiakkaille kyselytutkimuksen selvittääkseni mm. heillä käytössä olevat mobiilikäyttöjärjestelmät, miten he niitä käyttävät sekä millainen on heidän tietoturvatietoisuutensa ja oma arvionsa mobiililaitteisiinsa kohdistuvista uhkista.

Olen pyrkinyt jakamaan opinnäytetyöni selkeästi neljään isompaan lohkoon ja aloitan määrittelemällä, mitä on tietoturva ja analysoin sen merkityksen yleisesti ottaen. Lisäksi tuon esille, millaiset asiat voivat periaatteessa uhata yrityksen tietoturvaa, tutkien

samalla olemassa olevia käytäntöjä ja ohjeita uhkien torjuntaan ja hyvän tietoturvan toteuttamiseen sekä organisaatio- että käyttäjätasolla. Aihepiiri on laaja ja esitellyt menetelmät melko kokonaisvaltaisia, mutta ne vaikuttavat suoraan myös mobiililaitteiden tietoturvaan, kuten myöhemmin tässä työssä tullaan huomaamaan.

Seuraavaksi käyn läpi nykyään merkittävimmät mobiilikäyttöjärjestelmät ja selvitän niiden merkittävimmät erot tietoturvaominaisuuksien osalta, jotta saan muodostettua kokonaisvaltaisen käsityksen siitä, millä tavoin tietoturva eri käyttöjärjestelmissä toteutuu ja minkälaiset valmiudet niissä itsessään tietoturvauhkien torjumiseen on. Tämän olen rajannut niihin asioihin ja ominaisuuksiin, jotka sisältyvät käyttöjärjestelmään vakiona ja virallisesti, eli jotka valmistaja suoraan käyttäjälle tarjoaa. Työssä ei siis ole käsitelty mitään mahdollisia kolmansien osapuolten sovelluksia tai MDM-ratkaisuja, koska tällöin ei enää vertailtaisi pelkästään käyttöjärjestelmien välisiä konkreettisia eroja, vaan puhuttaisiin jo kokonaisten ekosysteemien välisistä eroista ja niiden teoreettisemmista mahdollisuuksista, joka vaatisi vielä laajemman ja ehkä hieman erityyppisen tutkimuksen.

Tämän jälkeen vielä selvitän, millaisia riskejä kaikkiin mobiililaitteisiin käyttöjärjestelmästä riippumatta voi kohdistua ja mitkä ovat uhkista merkittävimpiä, käyttämällä lähdemateriaalina mm. eri tietoturvayhtiöiden tekemiä tutkimuksia ja raportteja aiheesta.

Lopuksi perehdyn opinnäytetyöni toimeksiantajaan, Etelä-Savon Tietohallinto Oy:hyn toimintaympäristönä ja esittelen, perustelen sekä käyn läpi toimeksiantajan asiakkaille tekemäni kyselytutkimuksen lopputuloksineen.

Edellä mainittujen osioiden johtopäätösten pohjalta on opinnäytetyön lopputuloksena tarkoitus toteuttaa käyttäjäläheinen ja konkreettinen dokumentaatio hyvän tietoturvan ylläpitämiseksi ja parantamiseksi nykyaikaisissa älypuhelimissa ja tableteissa. Dokumentaation on tarkoitus tulla Etelä-Savon Tietohallinto Oy:n käyttöön.

2 TIETOTURVA YRITYSTOIMINNASSA

Jotta voidaan ymmärtää tietoturvan merkitys, täytyy ensin määritellä mitä tietoturva on ja mistä se koostuu. Tietoturva-käsitteen määrittelyyn on olemassa useita eri variaatioita riippuen siitä, mitä julkaisua tai standardia mukaillaan. Kaikki lähtevät kuitenkin yleensä liikkeelle siitä oletuksesta, että tieto on tärkeää omaisuutta, jota halutaan suojella pitämällä se luotettavana, käytettävänä, oikeassa muodossa olevana ja vain siihen oikeutettujen henkilöiden saatavana. (Hakala ym. 2006, 4.)

2.1 Klassinen määritelmä

Tietoturva voidaan siis yksinkertaisimmillaan jakaa kolmeen suurimpaan osa-alueeseen klassisella tiedon arvoon perustuvalla määritelmällä. Ne ovat luottamuksellisuus, käytettävyys ja eheys. (Hakala ym. 2006, 4.) Kansainvälisesti tämä on usein tunnettu nimellä CIA-triad, eli CIA-malli, joka muodostuu termeistä Confidentiality, Integrity ja Availability (Perrin, 2008). Pyrin selvittämään mitä nämä osa-alueet tarkoittavat ja miten ne toteutuvat.

Luottamuksellisuus tarkoittaa sitä, että tietojärjestelmän sisältämiin tietoihin pääsevät käsiksi vain henkilöt, joilla on niihin oikeus. Tätä pyritään varmistamaan suojaamalla tietoja sisältävät laitteet ja järjestelmät käyttäjätunnuksien ja salasanojen avulla sekä tarvittaessa kryptaamaan tiedot erilaisilla salausmenetelmillä. (Hakala ym. 2006, 4 – 5.) Jos tieto on salattu tarpeeksi turvallisesti, se pysyy turvassa, vaikka tiedonsiirtoyhteys joutuisikin salakuuntelun kohteeksi tai tallennusmedia varastettaisiin. (Järvinen 2002, 22.)

Käytettävyys on sitä, että tiedot ovat tarvittaessa saatavilla oikeassa muodossa ja tarpeeksi nopeasti. Jotta käytettävyys pysyisi hyvällä tasolla, tulisi huolehtia siitä, että tietoja sisältävät laitteet ja järjestelmät ovat tarpeeksi tehokkaita, ja että tietojen käsittelyyn käytettävät ohjelmistoratkaisut ovat mahdollisimman hyvin käyttöön soveltuvia ja näyttävät tiedot oikeassa muodossa. (Hakala ym. 2006, 4 – 5.) Mikäli tärkeät tiedot on sijoitettu esimerkiksi verkkopalvelimelle ja niitä käytetään sieltä useiden, esimerkiksi kannettavien päätelaitteiden, kuten älypuhelimien kautta myös normaalien toimistoaikojen ulkopuolella, tulee palvelinten luonnollisesti olla päällä ja käytettävissä 24 tuntia vuorokaudessa joka päivä. Tietojen saatavuus saattaisi estyä esimerkiksi

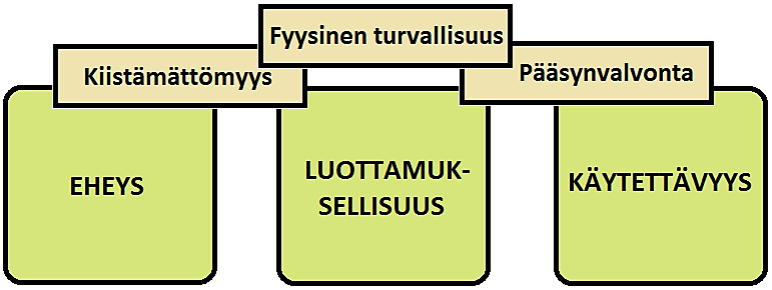
palvelun tarkoituksellisen ylikuormittamisen, eli palvelunestohyökkäyksen johdosta. (Järvinen 2002 24.)

Eheys merkitsee yleisesti ottaen sitä, että tiedot ovat paikkansapitäviä, eikä niiden sisällössä ole virheitä. Siihen vaikuttavat lähinnä ohjelmistopohjaiset asiat. Eheys voidaan ohjelmistotasolla pyrkiä varmistamaan esimerkiksi käyttämällä erilaisia tiedonsyötön rajoitteita ja tarkistuksia sekä tallennus- ja tiedonsiirto-operaatioiden varmistussummia ja tiivisteitä. Laitteistotasolla eheyttä parantavia ratkaisuja ovat mm. virheenkorjaavat muistimoduulit. (Hakala ym. 2006, 4 – 5.) Mahdollisia uhkia tiedon eheydelle voivat olla vaikkapa haittaohjelmat tai verkkosivustoihin murtautuvat ja niiden sisällön töhrivät ns. haktivistit. Myös tahaton asia, kuten laitteistovika tai tallennusmedian korruptoituminen voi tuhota tiedon eheyden. (Järvinen 2002, 22.)

2.2 Laajennettu määritelmä

Jotta otettaisiin paremmin huomioon myös tiedon omistajan identiteetti ja laitteistojen sekä tietojärjestelmien arvo, voidaan klassisen kolmikannan päälle lisätä vielä kolme muuta osatekijää, jotka ovat kiistämättömyys, fyysinen turvallisuus ja pääsynvalvonta (kuva 1). Kiistämättömyydellä tarkoitetaan sitä, että tietojärjestelmä kykenee toimimaan luotettavasti tunnistaessaan tai tallentaessaan sitä käyttävän henkilön tietoja. Pääsynvalvonta on tietojärjestelmän käytön rajoittamista, jolla pyritään estämään laitteiden sekä järjestelmien luvaton ja tarpeeton käyttö niin ulkopuolisten, kuin yrityksen oman henkilökunnankin toimesta. Tietojärjestelmien suorituskyky voi heikentyä, mikäli yrityksen henkilökunta käyttää laitteita omiin tarkoituksiinsa. (Hakala ym. 2006, 5 – 6.)

Fyysisellä turvallisuudella huolehditaan siitä, että yrityksen käyttämät laitteet ja järjestelmät on asianmukaisesti suojattu erilaisia fyysisiä uhkia vastaan, jollaisia voivat olla vaikkapa ilkivalta, murtautuminen, vesivahinko, tulipalo tai sähkön saannin katkeaminen. Paraskaan ohjelmistopohjainen tietojärjestelmä ei ole tietoturvallinen, mikäli sitä ajavat laitteet jätetään alttiiksi fyysisille vahingoille. (Hakala ym. 2006, 11.)



KUVA 1. Tietoturvan osatekijät - Laajennettu tietoturvallisuuden määritelmä (Hakala ym. 2006, 6.)

Petteri Järvinen muistuttaa kirjassaan Tietoturva & yksityisyys (2002, 24) myös todentamisen tärkeydestä. Jotta luottamuksellisuus toteutuu, tulisi todentamisen olla luotettavalla tasolla. Todentamisella tarkoitetaan sitä, että mikä tahansa olio, eli tässä tapauksessa vaikkapa käyttäjä, laite tai tiedon alkuperä pystytään todentamaan aidoksi ja alkuperäiseksi. Olion todentaminen onkin mahdollista vain, jos oliolla on jokin yksilöllinen ominaisuus tai tunnistetieto, joka erottaa sen selkeästi muista. Käyttäjien osalta todennus tehdään yleensä salasanan perusteella ja laitteiden osalta niihin sisällytettyjen tunnistetietojen perusteella, mutta esimerkiksi verkkotiedon todentaminen aidoksi ja oikeelliseksi tai ohjelmakoodin todentaminen alkuperäiseksi saattaa monesti olla vaikeaa. (Järvinen 2002, 24 - 26.)

2.3 Viranomaisten ohjeet ja lainsäädäntö

Tietoturva on sidoksissa tietosuojaan, jota tietoturvan keinoin ylläpidetään. Tietosuoja merkitsee erityisesti henkilön yksityisyyden ja tiedollisen itsemääräämisoikeuden suojaamista, jolle on laadittu myös oma lainsäädäntönsä. Vaikka Suomessa ei ole varsinaista erillislainsäädäntöä tietoturvalle, asettaa Suomen lainsäädäntö kuitenkin tietoturvan toteutukselle joitakin velvoitteita, jotka ovat tosin pääasiassa yleisluontoisia ja tarkoitettu lähinnä ohjenuoraksi, jättäen käytännön tietoturvallisuuden tarkemman määrittelyn yrityksille. Yrityksille tärkeintä on lähinnä, että viranomaiset ohjeistavat ja ottavat kantaa asioihin, joita yritysten tulisi tehdä tietoturvansa eteen. Näin yritykset paremmin tietävät, ovatko heidän käyttämänsä menetelmät lainmukaisia ja parhaiten kaikkien osapuolten intressejä palvelevia. (Laaksonen ym. 2006, 17 – 21.)

Euroopan Unioni on säätänyt useita tietoturvaa koskevia direktiivejä, joista tärkeimpinä voidaan mainita henkilötietojen suoja, 95/46/EY sekä sähköisen viestinnän tie-

tosuoja, 2002/58/EY. EU velvoittaa suojaamaan henkilötietojen käsittelyn sekä toteaa, että henkilötietojen liikkuvuus Euroopan yhteisön alueella on lähtökohtaisesti vapaata. Sähköisen viestinnän tietosuojadirektiivillä pyritään taas lähinnä varmistamaan perusoikeudet ja vapaudet sähköisen viestinnän alalla. Se velvoittaa myös sähköisiä palveluntarjoajia pitämään huolta riittävästä tietoturvasta, jotta viestinnän luvaton käyttö voidaan estää. (Laaksonen ym. 2006, 26 – 27.)

Suomen perustuslain 10. pykälä sanelee mm. kirjesalaisuuden loukkaamattomaksi, kirjeen ollessa tässä tapauksessa mikä tahansa vastaanottajalle kohdistettu yksityinen tietoliikenneviesti. Laki kuitenkin antaa viranomaisille itselleen oikeuden viestintäsalaisuuden ohittamiseen, mikäli sitä edellytetään väärinkäytösten tai rikosten tutkinnan yhteydessä. Käytännössä kirjesalaisuuden loukkaamattomuutta voidaan ylläpitää mahdollisimman hyvän tietoturvan avulla. Tähän erityisiä ohjeita teleyrityksille ja muille sähköisille toimijoille voi antaa Viestintävirasto. (Laaksonen ym. 2006, 28 – 29.)

Tietoturvaan liittyy läheisesti myös henkilötietolaki, 523/1999, joka antaa velvoitteet sille, miten esimerkiksi yritysten tietojärjestelmissä olevia, käyttäjiä yksilöiviä tietoja voidaan käyttää ja miten niiden tulisi olla suojattu. Mikäli yritysten tietojärjestelmät sisältävät henkilötietorekisteriksi määriteltäviä tietojoukkoja, pidetään näitä tietoja hallinnoivaa tahoa rekisterinpitäjänä, jonka velvollisuus on pitää rekisterin tietoturva riittävän hyvällä tasolla. Henkilötietorekisteriksi voidaan esimerkiksi lukea asiakasrekisteri, joka sisältää asiakkaiden henkilötietoja tai Windowsin Active Directory hakemistopalvelu, joka sisältää yrityksen työntekijöiden henkilötiedot. (Laaksonen ym. 2006, 31 – 36.) Henkilötietolain 32. pykälä velvoittaa rekisterinpitäjää suojaamaan rekisterin siten, että siihen ei päästä laittomasti käsiksi. Laki ei määrittele sinänsä, mikä on riittävä tietoturvan taso, vaan sen määrittelee rekisterinpitäjä itse. (Laaksonen ym. 2006, 42.)

Liian heikosti toteutetulla tietoturvalla voi olla myös juridisia seurauksia. Esimerkiksi kesäkuussa 2012 tapahtunut massiivinen salasanavuoto verkostoitumispalvelu Linkedin:ssä poiki haasteen oikeuteen ja yli 5 miljoonan dollarin korvausvaatimukset. Yksityisen henkilön alulle laittamassa joukkokanteessa syytetään Linkedin:iä liian lepsusta salasanojen suojauksesta, jossa palvelun salasanoja ei oltu ns. ”suolattu” asianmukai-

sesti. Palvelu joutui verkkomurron kohteeksi, jonka seurauksena palvelusta varastettiin n. 6,5 miljoonaa käyttäjäsalasanaa. (Linnake 2012a.)

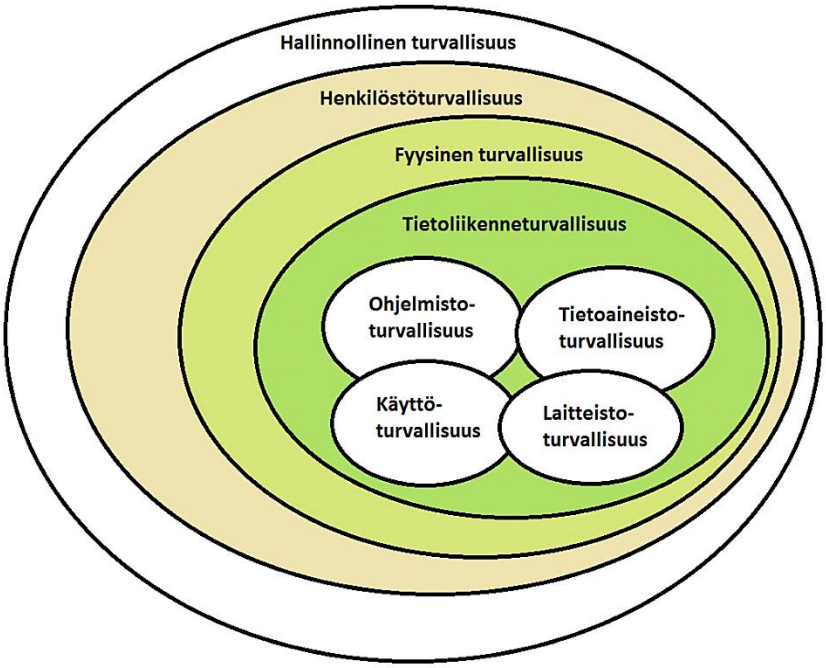
2.4 Tietojärjestelmien turvaaminen VAHTI-ohjeiston mukaisesti

Valtionhallinnon tietoturvallisuuden johtoryhmä, eli VAHTI on Suomen Valtiovarainministeriön ylläpitämä elin, jonka vastuulla on ohjata ja kehittää Suomen valtion tietoturvaa. Sen tavoitteena on parantaa valtionhallinnon tietoturvan luotettavuutta, laatua ja varautumista mahdollisiin uhkiin. Se toimii yhteistyössä mm. valtioneuvoston kanssa, pyrkien valmistelemaan ja yhteen sovittamaan valtioneuvoston ja valtiovarainministeriön hallinnon tietoturvaa koskevia linjauksia. Se pyrkii myös osaltaan edistämään tietoturvakulttuuria, tietoturvatietoisuutta, valtion IT-strategiaa ja kansainvälistä tietoturvayhteistyötä. VAHTI tarjoaa ajankohtaisia ja laajoja ohjeistoja, suosituksia ja tavoitteita tietoturvan suunnitteluun ja toteutukseen, jotka ovat julkisesti saatavissa Valtiovarainministeriön verkkosivuilta. (Valtiovarainministeriö 2012.) VAHTI-aineistoissa on otettu huomioon OECD:n jo vuodesta 1992 lähtien antamat ohjeistukset tietojärjestelmien ja tietoverkkojen tietoturvaperiaatteista, jotka OECD on jäsenvaltioidensa hyväksi laatinut. (Laaksonen ym. 2006, 23 – 24.)

VAHTI on laatinut valtionhallinnon organisaatioiden esimiesasemassa oleville henkilöille tarkoitetun oppaan, nimeltä Johdon tietoturvaopas, joka on julkaistu vuonna 2011. Se esittelee kaikki tärkeimmät seikat, jotka organisaation johdon tulisi tietoturvajohtamisessa ottaa huomioon. Vaikka ohjeet on laadittu lähinnä valtionhallintoa varten, ovat ne yhtä päteviä myös yksityisen sektorin organisaatioissa. (Valtiovarainministeriö 2011.)

VAHTI on laatinut myös oman mallinsa tärkeimmistä tietoturvan osatekijöistä. Se on esillä Valtionvarainministeriön verkkosivuilla olevassa dokumentaatiossa valtionhallinnon keskeisten tietojärjestelmien turvaamiseksi. (Valtiovarainministeriö 2004.) Koska malli on varsin monitasoinen ja laaja, voidaan se myös tiivistää ns. sipulimalliksi (kuva 2), jonka pääkohdat pyrin seuraavaksi käymään pääpiirteiltään läpi. Lisäksi olen poiminut sen yhteyteen Johdon tietoturvaoppaasta (Valtiovarainministeriö 2011) mielestäni tärkeimmät, pääkohtia tukevat seikat.

Tämä sipulimalli koostuu neljästä eri päätasosta, jotka ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoliikenneturvallisuus. Lisäksi tietoliikenneturvallisuuden alle voidaan sijoittaa ohjelmistoturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus ja laitteistoturvallisuus. (Valtiovarainministeriö 2004, 27 – 80.)



KUVA 2. Sipulimalli. Mukaillen (Valtiovarainministeriö 2004, 27 – 80.)

Hallinnollinen turvallisuus on sipulimallin ylin kerros ja se viittaa niihin hallinnollisiin keinoihin, jotka organisaation johto voi tehdä tietoturvan edistämiseksi. Tällaisia keinoja ovat mm. asianmukaiset organisaatiojärjestelyt, vastuiden määrittely sekä henkilöstön koulutus ja ohjeistus. Se edellyttää, että johto noudattaa tietoturvaa ohjaavia säädöksiä ja velvoitteita sekä laatii organisaatiolle mahdollisimman hyvän tietoturvastrategian ja politiikan. Tietoturvapolitiikan noudattamiseksi tulisi laatia dokumentaatio, joka sisältää kaikki suojattavat tietojärjestelmät. Tätä varten vaaditaan myös riskianalyysi. (Valtiovarainministeriö 2004, 27.)

Organisaation johdon sitoutuminen tietoturvan kehittämiseen on avain sen onnistumiseen. Johdon tulee olla mahdollisimman tietoinen organisaatiossa käytössä olevista tietojärjestelmäkokonaisuuksista ja niihin liittyvistä riskeistä. Tietoturvan hallinta tulisi nähdä kokonaisuutena, jossa otetaan huomioon tietoturvaa koskevat tavoitteet ja tehtävät koko organisaatiossa. Tietoturvatyö tulisi olla myös tarpeeksi avointa, jotta

sen asettamat tarpeet ja sen tarjoamat mahdollisuudet tulisivat huomioitua mahdollisimman laajasti. (Valtiovarainministeriö 2004, 30 – 31.)

VAHTI on koonnut myös yksinkertaisen muistilistan, johon on listattu johdon keskeiset tietoturvavelvoitteet. (Valtiovarainministeriö 2011, 21.)

- Lainmukaisuuden varmistaminen
- Riskienhallinnan- ja hallintajärjestelmän toteuttaminen
- Tietoturvapolitiikkaan sitoutuminen
- Tietoturvajohtaminen
- Tietoturvavastuuhenkilön nimeäminen
- Tietoturvallisuuden organisointi

Henkilöstöturvallisuus käsittää kaikki henkilöstöön liittyvät riskit ja niiden hallinnan. Siihen kuuluvat mm. henkilöstön soveltuvuus, toimenkuvat, käyttöoikeudet, turvallisuuskoulutus ja valvonta. Uuden työntekijän henkilöllisyys, taustat sekä soveltuvuus olisi aina syytä selvittää mahdollisimman hyvin. Lisäksi työntekijän toimenkuva tulisi rajata mahdollisimman tarkasti, jotta työntekijän vastuut, oikeudet ja velvollisuudet olisivat selvät kaikille osapuolille. Työntekijällä ei tulisi olla käyttöoikeuksia sellaisiin tietojärjestelmiin, jotka eivät ole hänen työtehtävänsä kannalta välttämättömiä. (Valtiovarainministeriö 2004, 39 – 42.)

Fyysisen turvallisuuden toteutusta varten VAHTI painottaa riittävää suojautumista mm. tunkeutumista, ilkivaltaa, sähkökatkoa, tulipaloa, lämpöä, savua, vettä ja pölyä vastaan sekä kulunvalvontaa ja asianmukaista henkilöstön koulutusta mahdollisten fyysisten uhkien varalta. (Valtiovarainministeriö 2004, 47 – 48.)

Tietoliikenneturvallisuuteen sisältyvät mm. laitteiden ja siirtoyhteyksien ylläpito, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta, ongelmatilanteiden kirjaaminen, viestinnän salaus ja varmistaminen sekä tietoliikennejärjestelmien testaus ennalta. (Valtiovarainministeriö 2004, 54 – 55.)

Sipulimallin alimpaan kerrokseen, tietoliikenneturvallisuuden alle voidaan koota vielä neljä kohtaa, jotka ovat laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. (Valtiovarainministeriö 2004, 61 – 94.)

Laitteistoturvallisuus takaa kaikkien organisaation tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden ja toimivuuden. Laitteiden tulisi olla käytettävissä kaikissa olosuhteissa ja niiden mahdolliseen huoltotarpeeseen tulisi olla varauduttu asianmukaisesti. Laitteiden tulisi olla myös mahdollisimman hyvin suojattuna haittaohjelmilta tai muilta ulkoisilta uhkilta, jotka voivat vaarantaa niiden tietoturvan. (Valtiovarainministeriö 2004, 61 – 66.)

Ohjelmistoturvallisuus sisältää menetelmiä ja toimenpiteitä, jotka liittyvät organisaation laitteiden käyttöjärjestelmien ja ohjelmistojen tietoturvaan. Kaikissa työasemissa tulisi olla mahdollisimman vakioitu käyttöympäristö ja lisäksi kaikki turhat ja tarpeettomat toiminnallisuudet tulisi karsia pois. Käytettävät tietoturvaohjelmistot tulisi pitää aina ajan tasalla ja niiden tulisi olla mahdollisimman hyvin yhteensopivia sekä testattuja. Ohjelmistojen toimittajilla tulisi olla tarvittaessa valmius kolmannen osapuolen suorittamiin auditointeihin. Ohjelmistojen asennuksia varten tulisi olla olemassa erilliset testi- ja tuotantoympäristöt, jonne uudet sovellukset voidaan ennen jakelua viedä vakiointia varten. (Valtiovarainministeriö 2004, 67 – 70.)

Kaikkien asiakirjojen, tiedostojen ja muiden aineistojen turvaamista kutsutaan tietoaineistoturvallisuudeksi. Siihen sisältyvät mm. aineistojen luettelointi ja luokittelu sekä tarvittaessa ohjeistettu hallinta ja käsittely. Pääasia on, että tietoaineisto on tarvittaessa helposti löydettävissä ja siihen voidaan luottaa. (Valtiovarainministeriö 2004, 79 – 80.)

Käyttöturvallisuus tarkoittaa sitä, että kaikelle käytössä olevalle tietotekniikalle on olemassa toimiva tuki, ylläpito ja huolto. Jotta käytön suhteen ei tule ongelmia, tulisi riittävä dokumentaatio olla myös tarvittaessa olemassa. Käyttöturvallisuuden piiriin voidaan lukea mm. huoltosopimukset, palvelutasosopimukset, valmiussuunnitelmat ja käytönvalvonta. Esimerkiksi joidenkin palveluiden tai toimintojen ulkoistaminen saattaa aiheuttaa haasteita, esimerkiksi jos palvelun käyttö estyy tai sen tietoturva vaarantuu, palvelun hallinnan ollessa jollain ulkopuolisella taholla. Tällaisiin tilanteisiin tulisi varautua jo ennalta yhteistyössä palveluntarjoajan kanssa, jotta toimintamallit poikkeustilanteissa ovat molemmille osapuolille selvät. Myös etäyhteyksien tietoturvasta huolehtiminen kuuluu käyttöturvallisuuden piiriin. Kaikkien keskeisten järjestelmien etäkäyttöön tulisi olla pääosin tiukka käyttöpolitiikka. Etäkäytössä tulisi mielellään käyttää vain siihen käyttöön omistettuja laitteita ja yhteyksien muodostamiselta vaadi-

taan vahvaa käyttäjätodennusta ja liikenteen salausta. (Valtiovarainministeriö 2004, 86 – 94.)

2.5 Yksilön vastuu

Asianmukaisestikin turvatun järjestelmän loppukäyttäjällä on kuitenkin aina oma vastuunsa riippumatta siitä, onko kyseessä työ- vai vapaa-ajan -tarkoitukseen laitettaan käyttävä käyttäjä. Erityisesti etätyö ja jatkuvasti saatavilla olevat verkkoyhteydet asettavat omia vaatimuksiaan tietoturvan toteutumiselle. Monesti käyttäjä mieltää verkon kautta suoritettavat asiat jokseenkin abstrakteiksi, eikä välttämättä aina ymmärrä niiden tosimaailmallisia seurauksia ollessaan huolimaton. Huolimattomuudella voi pahimmassa tapauksessa olla myös juridisia seurauksia. Esimerkiksi valveutumaton käyttäjä saattaa kokea vähäpätöiseksi ladata laitteeseensa verkosta ilman tekijänoikeuden haltijan lupaa saataville asetettua, tekijänoikeuden suojaamaa materiaalia, vaikkapa musiikkikappaleen tai jonkun muun digitaalisen tuotteen, välttämättä ymmärtämättä sen olevan rikos. Tapaushan voi olla rinnastettavissa siihen, että henkilö varastaa tuotteen kaupasta, mutta kun rikos tapahtuu verkossa, ei käyttäjä välttämättä edes koe tekevänsä mitään väärää. Lisäksi verkkokäyttäjän riski jäädä kiinni tekijänoikeusrikoksesta on erittäin pieni. (Järvinen 2002, 32 – 35.) Kuten VAHTI henkilöstön tietoturvaohjeessa ilmoittaa, käyttäessään organisaation verkkoa, laitetta, tai sähköpostia, käyttäjä esiintyy periaatteessa tällöin organisaation edustajana. (Valtiovarainministeriö 2006, 9 – 10.)

Kimmo Rousku kirjoittaa tieto- ja viestintätekniikasta uutisoivan Tietoviikko-lehden julkaisemassa artikkelissa (2012) organisaation tietoturvallisuuden vastuiden jakautumisesta. Periaatteessa viime käden vastuun organisaatiossa ottaa aina organisaation ylin johto, mutta ylin johto harvoin yksin vastaa tietoturvan käytännön toteutuksesta, vaan tehtäviä delegoidaan yleensä eteenpäin, esimerkiksi tietoturvapäällikölle, jonka tehtävä puolestaan on valvoa, miten hänen alaisensa tietoturvasta huolehtivat. Tietoturvasta huolehtiminen on siis aina myös loppukäyttäjän harteilla. Rousku kirjoittaakin, että organisaatio on niin terve ja hyvinvoiva, kuin kaikki sen yhdessä kokevat ja tietoturva on osa organisaation asennetta ja kulttuuria, joka on läsnä kaikkialla. Siksi siitä tulisikin huolehtia kaikkien yhteisesti. (Rousku 2012.)

Näkisin, että yksi keskeisimmistä käyttäjän vastuulla olevista asioista on henkilökohtaisen salasanan valinta ja siitä huolehtiminen, sillä kuten olen edellä jo maininnut, salasana on yleensä avain käyttäjien todentamiseen ja luottamuksellisiin tietoihin pääsyyn. IT-yritys Google määrittelee vahvan salasanan sisällön siten, että sen tulisi olla ainakin kahdeksan merkkiä pitkä, eikä se saisi sisältää mitään ilmauksia, jotka perustuvat käyttäjän henkilökohtaisiin tietoihin. (Google 2012.) Tällainen ilmaus voisi olla vaikkapa käyttäjän nimen sisällyttäminen salasanaan.

Salasana on sitä vaikeampi murtaa mitä enemmän erilaisia merkkejä siinä käytetään. Näitä ovat pienet ja isot kirjaimet, numerot sekä symbolit. Lisäksi salasanassa tulisi välttää käyttämästä yksinkertaisia ilmauksia, kuten ”salasana” tai ”sisäänkirjaus” ja näppäimistökaavoja tai merkkisarjoja, kuten ”qwerty” tai ”abcd1234”. Vaikka salasana olisi sisällöltään vahva, on myös suositeltavaa käyttää eri palveluissa ja eri tileissä yksilöllisiä salasanoja. (Google 2012.)

Tietoturvayhtiö F-Securen ohje useita eri palveluita käyttäville käyttäjille on erottaa eri palveluissa käytetyt salasanat esimerkiksi lisäämällä jokaiseen salasanaan erilaisen, palvelukohtaisen yksilöivän osan. Esimerkiksi Amazon.com -sivuston salasanaan voi sisällyttää ilmauksen AMA, joka on huomattavasti tietoturvallisempi tapa, kuin käyttää täysin samaa salasanaa joka paikassa. (F-Secure 2009.)

Valtionvarainministeriön VAHTI-ryhmä on julkaissut Johdon tietoturvaoppaan lisäksi myös organisaation henkilöstölle kohdistetun ohjeistusteoksen, nimeltään Henkilöstön tietoturvaohje, joka on julkaistu vuonna 2006. Sen tarkoituksena on toimia yleisohjeena henkilöstön tietoturvatyölle ja kehittää sitä. (Valtiovarainministeriö 2006.)

Koska organisaation merkittävimmät tietoturvauhkat on jo tämän opinnäytetyön aiemmissa luvuissa esimerkkeineen käyty läpi, ei liene syytä käsitellä niitä uudestaan, vaan tämän luvun loppuun olen poiminut Henkilöstön tietoturvaohjeen mielestäni keskeisimmät käyttäjän tietoturvaa tukevat asiat, jotka tuon seuraavassa tiivistetysti esiin. (Valtiovarainministeriö 2006, 9 – 28.)

- Seuraa tietoturvallisuuteen liittyviä tiedotteita ja ohjeita, ja toimi niiden mukaan sekä osallistu sinulle tarjottuun koulutukseen.
- Älä anna tietokonettasi ulkopuolisten käyttöön

- Älä säilytä salassa pidettävää aineistoa työpöydällä.
- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi tai salasanojasi kellekään toiselle henkilölle.
- Pyri pitämään tietokoneesi näyttö ja näppäimistö suojassa ulkopuolisten katseilta, kun käsittelet niillä arkaluontoista tietoa, tai kun syötät käyttäjätunnuksia ja salasanoja
- Muista vaihtaa salasanasi riittävän usein, tai aina, jos epäilet niiden paljastuneen.
- Muista vastuusi organisaation verkkoa, laitetta, tai sähköpostia käyttäessäsi, sillä esiinnyt tällöin aina organisaation edustajana.
- Tallenna tekemistäsi töistä varmuuskopiot organisaatiosi verkkopalvelimelle, mikäli mahdollista
- Kun lopetat työaseman käytön, kirjaudu aina tietojärjestelmästä ulos ja sammuta laitteet saamiesi ohjeiden mukaisesti.
- Ilmoita aina havaitsemistasi tietoturvaongelmista tai uhkista organisaatiosi tietoturvavastaavalle
- Pyydä aina tarvittaessa neuvoa organisaatiosi asiantuntijoilta.

3 MOBIILIKÄYTTÖJÄRJESTELMÄT JA NIIDEN TIETOTURVA

Tässä luvussa käyn läpi tämän hetken markkinaosuuksilla mitattuna merkittävimmät mobiilikäyttöjärjestelmät erityisesti tietoturvanäkökulmasta. Pyrin käymään läpi jokaisen käyttöjärjestelmän omasta mielestäni käyttäjän kannalta tärkeimmät tietoturvaominaisuudet sekä tekemään lyhyen pintaraapaisun niiden takana toimivaan tekniikkaan ja arkkitehtuuriin. Tarpeettoman monimutkaisesti en eri käyttöjärjestelmien tarkkoja toimintaperiaatteita kuitenkaan niiden laajuuden vuoksi käy läpi, vaan pyrin tuomaan esille pääasiassa vain eri alustojen huomattavimmat erityispiirteet, siltä osin kuin niillä mielestäni on merkitystä loppukäyttökokemukseen.

3.1 Älypuhelimen määritelmä

Koska tässä opinnäytetyössä tutkimuksen kohteena olevat mobiililaitteet ovat älypuhelimia ja taulutietokoneita, eli tabletteja, on hyvä aloittaa määrittelemällä, mikä erot-

taa älypuhelimen tavallisesta matkapuhelimesta ja miten tabletit eroavat älypuhelimista.

Yksi maailman ensimmäisistä älypuhelinvalmistajista, Nokia, määritteli joitain eroja älypuhelimen ja tavallisen puhelimen välillä jo vuonna 2004. Nokian mukaan ei ole olemassa yhtä ainutta tapaa määritellä älypuhelinta, mutta joitain sen tunnusmerkkejä ovat esimerkiksi, että se perustuu kaupalliseen käyttöjärjestelmään, joka mahdollistaa kolmansien osapuolien sovelluskehityksen laitteelle, suuri näyttö ja graafinen käyttöliittymä, suuri tai laajennettavissa oleva sisäinen muisti, yhteydet lähi- ja ulkoverkkoon ja liitettävyys tietokoneeseen. (Nokia 2004, 1.)

Älypuhelimet sisältävät puhelintoiminnon lisäksi käytännön ominaisuuksia ja sovelluksia, kuten kalenterin, yhteystietoluettelon, muistilistan, internetselaimen, sähköpostin, kameran, mediatoistimen, FM-radion ja muita hyöty- tai ajanvietesovelluksia. Älypuhelimet ovatkin käytännössä syrjäyttäneet aiemmin erityisesti yrityskäytössä suositut PDA-laitteet, joiden lyhenne tulee nimestä Personal Digital Assistant, joka voisi vapaasti suomennettuna olla vaikkapa henkilökohtainen digitaalinen avustin. Lisäksi älypuhelimista on tullut merkittävä alusta pelien kehittäjille. (Nokia 2004, 1 – 2.)

Taulutietokone, eli tabletti eroaa älypuhelimesta lähinnä fyysisiltä ominaisuuksiltaan. Tabletti on kosketusnäyttötietokone, jossa ei ole fyysistä näppäimistöä. Tabletit voidaankin luokitella älypuhelinten ja kannettavien tietokoneiden välimaastoon (Sutter 2010). Vaikka tabletista puhutaan tietokoneena, se lienee kuitenkin lähempänä älypuhelinta, kuin kotitietokonetta, joskin nykyaikaisten käyttöjärjestelmien myötä myös raja itse tietokoneen ja älypuhelimen välillä on hämärtynyt. Tabletin näkyvin tunnusmerkki on huomattavasti älypuhelimia suurempi ja tarkempi näyttö, joka vaatii tuekseen myös suurempikapasiteettisen akun. (Tietoviikko 2011.) Vaikka näistä ominaisuuksista voi olla etua älypuhelimiin verrattuna, toistaiseksi voitaneen kuitenkin sanoa tablettien olevan älypuhelimille enemmänkin jatke, kuin korvaaja, sillä älypuhelimilla on edelleen keskeisempi asema työtehtävien hoidossa. (M&M 2012.)

3.2 Tietoturvallisen käyttöjärjestelmän perusperiaatteet

Kun tutkitaan mobiilikäyttöjärjestelmiä, lienee hyvä myös määritellä, millaiset suunnitteluratkaisut puoltavat ohjelmiston, kuten käyttöjärjestelmän tietoturvallisuutta. Jerome H. Saltzerin ja Michael D. Schroederin, jo vuonna 1975 luoma määritelmä tietokoneohjelmistojen tietoturvan toteutuksesta pätee mielestäni monessa asiassa myös tänä päivänä. Saltzer ja Schroeder esittelivät tietoturvallisen ohjelmistokehityksen perusperiaatteet, joiden pääkohdat seuraavassa lyhyesti esittelen ja pyrin selittämään ymmärrettävästi, tarvittaessa käytännön esimerkein. (Saltzer, Schroeder 1975.)

Mekanismin taloudellisuus (Economy of mechanism) tarkoittaa, että käyttöjärjestelmä tulisi aina pitää malliltaan mahdollisimman yksinkertaisena ja pienenä. Mitä yksinkertaisemmista osista käyttöjärjestelmä voidaan rakentaa, sitä vähemmän se on altis kuormittumiselle.

Turvallisuusolettamus (Fail-safe defaults) tarkoittaa, että käyttöjärjestelmä tulisi aina perustua sille olettamukselle, että sen resursseihin ei oletusarvoisesti ole lupaa päästä käsiksi. Yksinkertaistettuna, vahva suojaus on tärkeämpää, kuin pääsyn helppous.

Täydellinen välitys (Complete mediation) tarkoittaa, että jokainen käyttö-oikeuden valtuutus jokaiseen objektiin täytyy voida varmistaa. Esimerkiksi, jos jokin käyttöjärjestelmän sovellus pyytää lupaa suorittaa jonkin toiminnon, tulisi käyttöjärjestelmän aina voida tarkistaa, onko sillä oikeutta siihen.

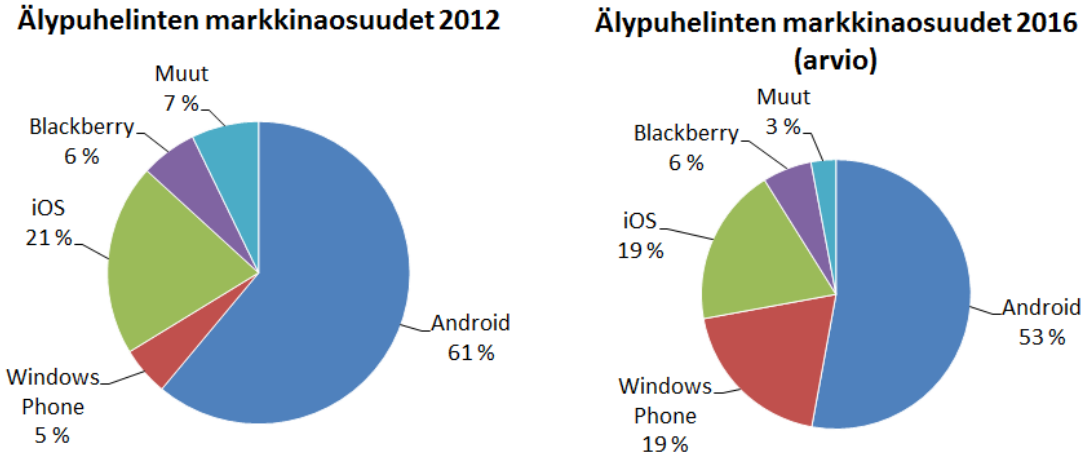
Avoin suunnittelu (Open design) tarkoittaa, että käyttöjärjestelmän ei tulisi olla suunnitteluperiaatteiltaan salamyhkäinen, vaan suunnitteluratkaisujen tulisi olla selkeitä, ja tietoturvan perustua nimenomaan käyttöoikeuksien ja salasanojen toimivuuteen, eikä tarpeettomaan vaikeaselkoisuuteen.

Pienimmät mahdolliset oikeudet (Least privilege) tarkoittaa, että jokaisen käyttöjärjestelmän osan tai käyttäjän tulisi voida suorittaa työnsä pienimmillä mahdollisilla käyttöoikeuksilla.

Psykologinen hyväksyttävyys (Psychological acceptability) tarkoittaa, että käyttöjärjestelmän käyttöliittymän tulisi olla riittävän helppokäyttöinen, jotta käyttäjät pystyvät käyttämään suojamekanismeja rutiininomaisesti oikein ja virheittä.

3.3 Markkinaosuudet

Tutkimusyhtiö IDC:n Kesäkuussa 2012 julkaisemista tuloksista nähdään, että Googlen kehittämä Android on edelleen tämän hetken suosituin mobiililaitteissa käytetty käyttöjärjestelmä, Applen iOS:n ollessa toisena. IDC:n arvion mukaan Microsoftin Windows Phone -alusta on kuitenkin hyvässä kasvussa ja tulee jatkossa nousemaan entistä merkittävämmäksi alustaksi, kun taas Androidin markkinaosuuden odotetaan hieman kaventuvan suhteessa muihin, Symbianin ollessa katoamassa markkinoilta lähes kokonaan. (IDC 2012.)



KUVA 3. Älypuhelinten käyttöjärjestelmien markkinaosuudet (IDC Worldwide Mobile Phone Tracker 2012.)

Kuluttajatutkimusyhtiö Kantar Worldpanel ilmoitti lokakuussa 2012, että Windows Phone -laitteiden osuus erityisesti Euroopan suurimmissa maissa, kuten Italiassa ja Ranskassa on kasvanut viime aikoina merkittävästi. Windows Phone on siis nuoresta iästään huolimatta nousemassa jo Euroopan kolmanneksi suurimmaksi mobiilikäyttöjärjestelmäksi, ohi RIM Blackberryn. (Kantar Worldpanel 2012.)

Näiden tietojen valossa, olen rajannut tässä opinnäytetyössä käsitellyt käyttöjärjestelmät Androidiin, iOS:ään, Windows Phoneen (kuva 4) sekä Symbianiin, koska se on edelleen laajamittaisessa käytössä tämän työn toimeksiantajalla, Etelä-Savon Tietohal-

linto Oy:llä. Katsoin parhaaksi rajata RIM Blackberryn pois, sillä Suomen markkinoilla sillä ei juuri ole ollut kysyntää ja RIM toikin virallisesti Blackberryt saataville Suomessa vasta keväällä 2012 (Lehto 2012a.)

KUVA 4. Kolmen suuren ekosysteemin laitteet vasemmalta oikealle: Windows Phone 8.0, Android 4.0 ja iOS 6 (Bonetti 2012.)

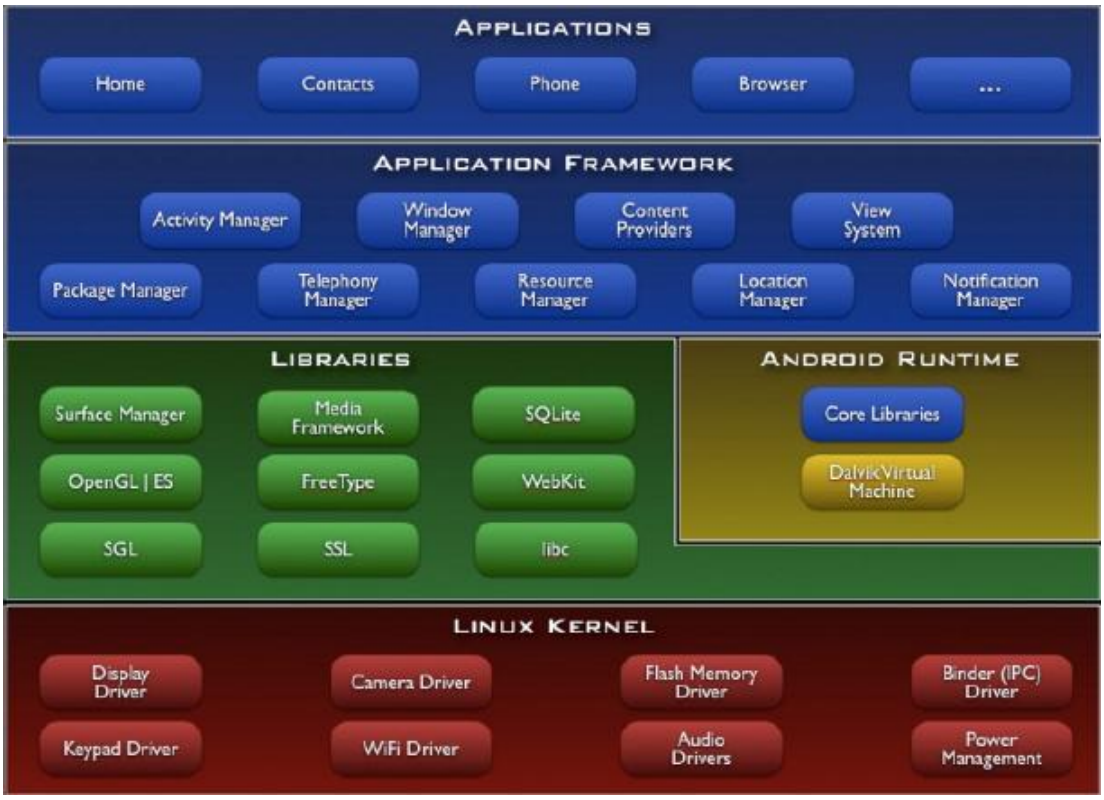
3.4 Android

Android on Googlen kehittämä, avoimeen lähdekoodiin ja Linux-ytimeen perustuva käyttöjärjestelmä älypuhelimille ja tableteille. (Beavis 2008.) Alun perin iOS:n ja Symbianin kilpailijaksi suunniteltu käyttöjärjestelmä on noussut nopeasti maailman suosituimmaksi mobiilialustaksi, markkinaosuuksilla mitattuna. (IDC 2012.)

Uusin Android-versio on 4.1 ”Jelly Bean” (Android 2012a). Google on julkaissut uusia ohjelmistopäivityksiä tasaisin väliajoin, mutta niiden saatavuus laitteisiin on laitekohtaista ja jakelu on laitevalmistajien vastuulla. Tämä johtuu siitä, että laitevalmistajat usein tekevät omia muutoksia laitteidensa Android-käyttöjärjestelmiin, joka merkitsee sitä, että myös Googlen ohjelmistopäivitykset täytyy räätälöidä erikseen laitteille sopiviksi. Tämä välivaihe hidastaa monien Android-laitteiden päivitysten saatavuutta. (Cunningham 2012.)

Android pohjautuu Linux-ytimeen ja Dalvik-nimiseen, Java-pohjaiseen ohjelmistoalustaan. Jokainen sillä ajettava sovellus toimii erillisenä prosessinaan oman virtuaalikoneen päällä, joka takaa sen, ettei yksikään prosessi pääse käyttämään toisen käynnissä olevan prosessin resursseja. (Symantec 2011, 10.)

Androidin tietoturvamalli koostuu teknisesti neljästä pääkerroksesta, jotka ovat sovellustaso, sovelluskehystaso, ohjelmistokirjastotaso sekä Linux-ydin, eli Kernel-taso (kuva 5). Tässä mallissa laitteen eri toiminnot ja sovellukset toimivat näillä eri tasoilla, joille kaikille on olemassa erilliset käyttöluvat. Käytännössä se tarkoittaa sitä, että jokainen sovellus tarvitsee käyttäjän hyväksynnän päästäkseen käsiksi eri tasoilla mahdollisesti oleviin, yksittäisiin käyttölupiin, kuten vaikkapa GPS-paikannukseen. Tämän mallin ongelma on kuitenkin siinä, että jos sovelluksen kehittäjä on asettanut sovelluksen kysymään lupaa päästä käsiksi kerralla useisiin ominaisuuksiin, jotka eivät ole sen toiminnan kannalta välttämättömiä, ja käyttäjä antaa luvan yhdellä klikkauksella, sen kummemmin tarvittaviin lupiin perehtymättä, saattaa käyttäjän tietoturva vaarantua. (Alonso-Parrizas 2011.) Tällainen tilanne voisi mahdollistaa esimerkiksi kolmannen osapuolen tietojenkeruun, josta on mainittu myös myöhemmin tässä luvussa.

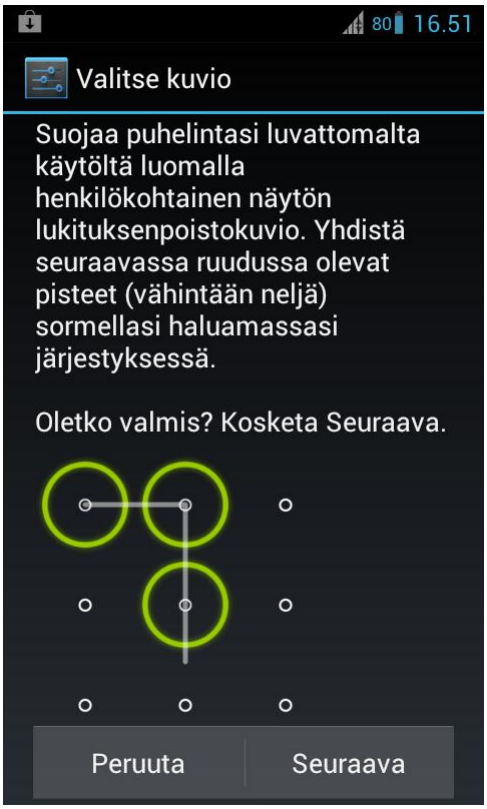


KUVA 5. Android-arkkitehtuuri (Alonso-Parrizas 2011, 6.)

Androidin tietoturvaominaisuuksiin kuuluu perinteisen aakkosnumeerisen salasanasuojauksen lisäksi mahdollisuus asettaa laite lukkiutumaan halutun joutenoloajan jälkeen automaattisesti, jonka jälkeen laite kysyy salasanaa, käyttäjän jälleen ak-

tivoidessa laitteen näyttölukituksesta. Lisäksi voidaan määrittää, monta epäonnistunutta kirjautumisyritystä laite sallii, ennen kuin se pyyhkii kaikki tiedot muististaan luvattoman käytön estämiseksi. Salasanalle voi myös asettaa päivämäärän, jolloin se umpeutuu, jonka jälkeen se täytyy vaihtaa uuteen. (Symatec 2011, 11.)

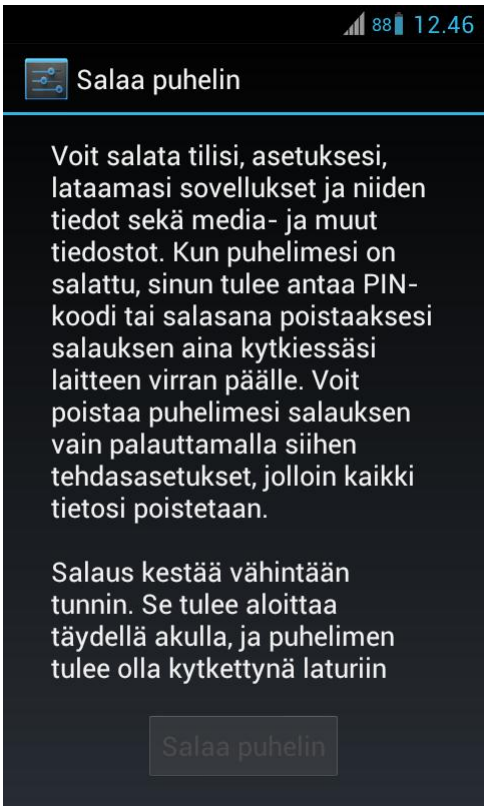
Näyttölukitus voidaan myös avata käyttämällä ruudulla näkyvää, yhdeksästä pisteestä koostuvaa matriisia, eli ns. Pattern-Screen Lock -lukituksenpoistokuviota, johon käyttäjä voi määrittää vähintään neljän pisteen kautta kulkevan yhtenäisen kuvion, jonka piirtämällä laite avaa näyttölukituksen. (kuva 6) Tämä lukituksenpoistokuviomenetelmä on osoittautunut yllättävänkin tehokkaaksi, sillä edes Yhdysvaltain keskusrikospoliisi FBI ei omissa testeissään onnistunut lukuisista yrityksistä huolimatta avaamaan näyttölukitusta. (Kravets 2012.)



KUVA 6. Kuvakaappaus Androidin Pattern-Screen Lock -ominaisuudesta omistamassani Huawei U8800 -älypuhelimessa (Android 4.0.4 ”Ice Cream Sandwich”) (Android 2012b.)

Android on versiosta 3.0 lähtien tukenut vakiona laitteen sisäisen muistin sisältämien tietojen salausta (kuva 7). Kun laitteen sisältö on salattu, kysyy laite joka käynnistyksen yhteydessä käyttäjän asettamaa turvakoodia, eikä koko käyttöjärjestelmä lähde

käyntiin, ellei koodia syötetä oikein. (Whitwam 2012.) Android ei kuitenkaan tue muistikortilla olevien tietojen salausta vakiona, joten muistikortille mahdollisesti tallennettuihin tietoihin pääsee helposti käsiksi yksinkertaisesti poistamalla kortin laitteesta, vaikka itse laite olisikin suojattu salasanalla. (Symatec 2011, 11.). Muistikortin sisältämien tietojen salausta varten Android-käyttäjä joutuukin turvautumaan mahdollisiin kolmansien osapuolten sovelluksiin.



KUVA 7. Kuvakaappaus Androidin salausominaisuudesta omistamassani Huawei U8800 -älypuhelimessa (Android 4.0.4 ”Ice Cream Sandwich”) (Android 2012b.)

Testaamani uusin Android versio 4.1 ”Jelly Bean” (Android 2012a), ei tue vakiona laitteen etälukitusta tai etätyhjennystä, joten tätäkin varten Androidin käyttäjä joutuu turvautumaan kolmansien osapuolten sovelluksiin.

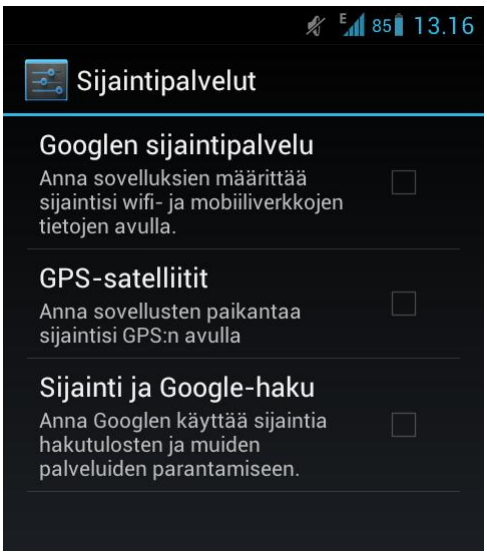
Android ei sisällä vakiona myöskään varsinaista tiedostojen varmuuskopiointi- tai pilvitallennusmahdollisuutta, mutta sisältää toiminnon, jolla käyttäjä voi varmuuskopioida ja palauttaa Gmail-tiliinsä yhdistetyt yhteystiedot, asetukset, kalenterin ja sähköpostin, aina jos vaihtaa laitetta, tai palauttaa sen tehdasasetukset. (Vaknin 2011.) Halutessaan varmuuskopioida koko laitteen sekä muistikortin sisältämät tiedostot,

joutuu käyttäjä sen sijaan turvautumaan kolmansien osapuolten sovelluksiin, tai erikseen asennettavaan Googlen omaan Google Drive -palveluun, jonka voi hankkia ilmaiseksi Googlen sovelluskaupasta. (Cipriani 2012a.)

Osittain sen suosiosta johtuen, Androidista on tullut verkkorikollisten ja haittasovellustehtailijoiden pääasiallinen kohdealusta. Toinen tätä tukeva seikka on Androidin melko liberaali sovelluspolitiikka. Androidin sovelluskauppa Google Play on avoin, eikä sovellusten julkaiseminen vaadi muuta kuin kauppapaikkaan rekisteröitymisen sovelluskehittäjänä. Näin kuka tahansa voi julkaista kauppapaikassa omia sovelluksiaan käyttäjien ladattaviksi melko helposti, jolloin riski myös haitallisten ohjelmien leviämiseen on olemassa. Ennen kuin Google ehtii reagoida asiaan, saattavat miljoonat laitteet jo olla altistuneita haittaohjelmalle. (Reisinger 2011.) Lisäksi, Android-laitteeseen voidaan asentaa myös kauppapaikan ulkopuolisia sovelluksia, mikäli käyttäjä sallii laitteen asetuksista sovellusten asentamisen tuntemattomista lähteistä. Oletettavasti takeet kauppapaikan ulkopuolisten sovellusten turvallisuudesta ovat vielä vähäisemmät, kuin kauppapaikan sovellusten. (Symantec 2011, 14.)

Eräs huolta aiheuttanut seikka Androidissa on sen tapa kerätä tietoja käyttäjästään. Joulukuussa 2010 tekemänsä tutkimuksen pohjalta, The Wall Street Journal syytti Googlea ja Applea käyttäjän sijaintitietojen keruusta. Tiedonkeruun syyksi se epäilee yhtiöiden keskinäistä kilpailua massiivisten käyttäjätietokantojen rakentamisesta, joiden avulla käyttäjä voidaan tarvittaessa paikantaa tarkasti älypuhelimen kautta (kuva 8). Googlen virallinen kanta asiaan on, että se käyttää sijaintietoja parantaakseen liikennekarttojensa tarkkuutta. (Munchbach 2011.)

Tietoturva-analyytikko Samy Kamkar paljastaa, että esimerkiksi älypuhelinvalmistaja HTC:n Android-pohjaiset laitteet keräävät käyttäjän sijaintiedon, nimen, laitteen ID:n ja matkapuhelinverkon signaalin vahvuuden muutaman sekunnin välein, ja lähettävät tiedot Googlelle useaan kertaan tunnin sisällä. (Angwin, Valentino-Devries 2011.)



KUVA 8. Kuvakaappaus Googlen sijaintipalveluvalikosta omistamassani Huawei U8800 -älypuhelimessa (Android 4.0.4 ”Ice Cream Sandwich”) (Android 2012b.)

Tämän johdosta, esimerkiksi Venäjän hallitus on päätynyt Android-pohjaisten tablettien käyttöönoton sijaan suunnittelemaan täysin oman taulutietokoneen, koska se uskoo Googlen laitteisiinsa sisällyttämän tiedonkeruun vaarantavan oman tietoturvansa, ja pelkää, että Android-laitteet asettavat venäläiset tietoliikenneyhteydet alttiiksi salakuuntelulle erityisesti Yhdysvaltojen toimesta. (Kinder 2012.)

Amerikkalaisen MDM- sekä muita mobiililaitepalveluita tarjoavan Fiberlink yrityksen teknologia- ja tuotekehitysjohtaja Clint Adams onkin sanonut, että Android on tietoturvassa pahnan pohjimmaisena, koska sitä ei yksinkertaisesti ole kehitetty täysin tietoturvan ehdoilla, jonka vuoksi parempia tietoturvaominaisuuksia on pultattu siihen hitaasti vasta jälkeenpäin. Adamsin mielestä myös Android-laitteita tarjoavien operaattorien kiinnostus keskittää intressinsä pääasiassa kuluttajamarkkinoille, yritysmarkkinoiden sijaan, on osaltaan vaikuttanut Androidin tietoturvan tasoon. (Reisinger 2011.)

Toisaalta, Androidin lähdekoodin ollessa avointa, voidaan se nähdä kaksiteräisenä miekkana. Siinä missä avoin lähdekoodi voidaan hyökkääjän toimesta nähdä heikkoutena, voidaan se myös nähdä siten, että kun alusta on avointa koodia, on myös kolmansilla osapuolilla mahdollisuus tunnistaa uhkia paremmin ja parantaa alustan tietoturvaa sekä kehittää sille tietoturvasovelluksia nopeammin ja ketterämmin, kuin suljetuissa järjestelmissä, joiden tietoturvauhkiin reagointi on yksin valmistajan varassa. (Google Play 2012.) Tietoturvayritys Symantecin mukaan, Android-alustasta itsestään

on löydetty sen julkaisun jälkeen vain parisen kymmentä haavoittuvuutta, jota se pitää hyvin vähäisenä määränä. (Symantec 2011, 10.)

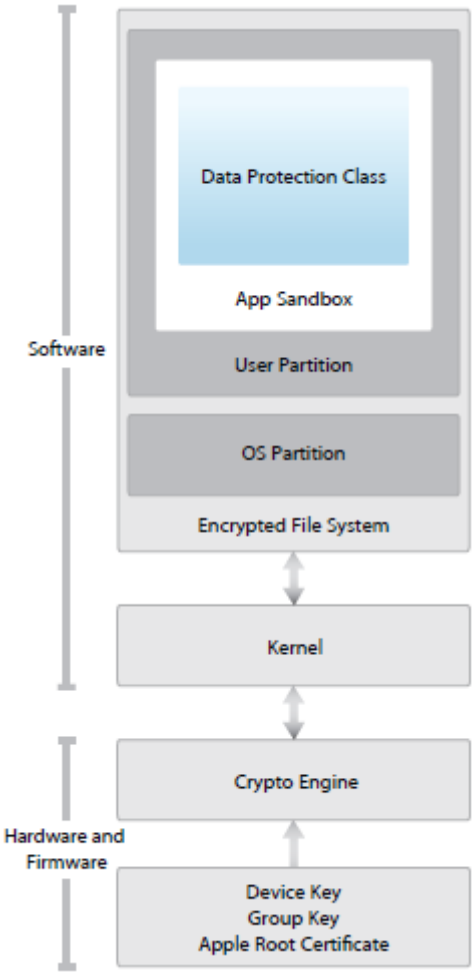
3.5 iOS

iOS on Applen kehittämä mobiilikäyttöjärjestelmä ja toisin kuin Android, iOS on suljetun lähdekoodin käyttöjärjestelmä. iOS pohjautuu Unix-ytimeen, ja se voidaankin nähdä kuin kevennettynä versiona Applen OSX -työpöytäkäyttöjärjestelmästä. (Symantec 2011, 4.) Uusin versio, iOS 6, julkaistiin 19. Syyskuuta 2012. Uusimman iPhone 5 -älypuhelimen ja viidennen sukupolven iPod Touch -mediatoistimen lisäksi se on saatavilla maksuttomana päivityksenä iPhone 4S, 4, 3GS – älypuhelimille, neljännen sukupolven iPod Touch:lle sekä toisen ja kolmannen sukupolven iPad – tableteille. (Linnake 2012b.) Nämä Applen iOS-laitteilleen julkaisemat ohjelmistopäivitykset ovat ladattavissa laitteisiin suoraan verkon yli (Sadun 2012).

iOS käyttää Androidin tavoin ns. Sandboxing-tyyppistä mallia ajaessa sovelluksia, joka tarkoittaa sitä, että yksittäiset sovellukset eivät pääse käsiksi, eivätkä pysty vaikuttamaan toisen sovelluksen dataan, eivätkä sovellukset itse asiassa ole edes tietoisia toisistaan. Sovellukset eivät pääse käsiksi käyttöjärjestelmän ytimeen, eivätkä voi korvata mitään järjestelmän osia tai ajureita. Lisäksi iOS antaa järjestelmän kannalta välttämättömille sovelluksille korkeamman prioriteetin kolmannen osapuolen sovelluksiin verrattuna, ja mikäli käyttöjärjestelmän resurssit uhkaavat loppua kesken tai jokin kolmannen osapuolen sovellus uhkaa viedä resursseja järjestelmäprosesseilta, sammutetaan kolmannen osapuolen sovellukset automaattisesti. Sovelluksilla ei myöskään ole mahdollisuutta päästä käsiksi puhelimen tekstiviesti- tai sähköpostiominaisuuksiin, ilman käyttäjän komentoa. Toisaalta, sovelluksilla on oikeudet päästä käsiksi mm. yhteystietoihin, kalenteriin, laitteen ID-tunnisteeseen, puhelinnumeroon, kuva- ja mediatiedostoihin, Internet-selaimen historiatietoihin ja jopa laitteen videokameraan, ilman käyttäjän erikseen antamaa valtuutusta. (Symantec 2011, 6.)

iOS:n tietoturvamalli koostuu neljästä pääkerroksesta (kuva 9), jonka ohjelmistotason kerroksiin kuuluvat kryptattu tiedostojärjestelmä ja Kernel, eli järjestelmän ydin. Laitteistotason kerrokseen sisältyy kryptausmoottori sekä lohko, joka sisältää Applen allekirjoittamat digitaaliset varmenteet ja muita työkaluja, joiden tehtävänä on tarkistaa ajettavien prosessien aitous. (Apple 2012c, 4 – 5.)

Secure Boot Chain on iOS:n tapa varmistaa, että järjestelmä on eheä, ja että kaikki käyttöjärjestelmän käynnistyksen yhteydessä ajettavat sovellukset, prosessit ja ajurit ovat varmasti alkuperäisiä, eikä niitä ole haitallisesti modifioitu. Mikäli järjestelmä havaitsee, että jokin sen komponentti ei ole alkuperäinen, lopetetaan käyttöjärjestelmän lataaminen, ja pyydetään käyttäjää liittämään laite tietokoneeseen USB-kaapelilla, jotta laite voi yhdistää itsensä Applen iTunes-ohjelmistoon ja palauttaa alkuperäiset tehdasasetukset. (Apple 2012c, 4.)



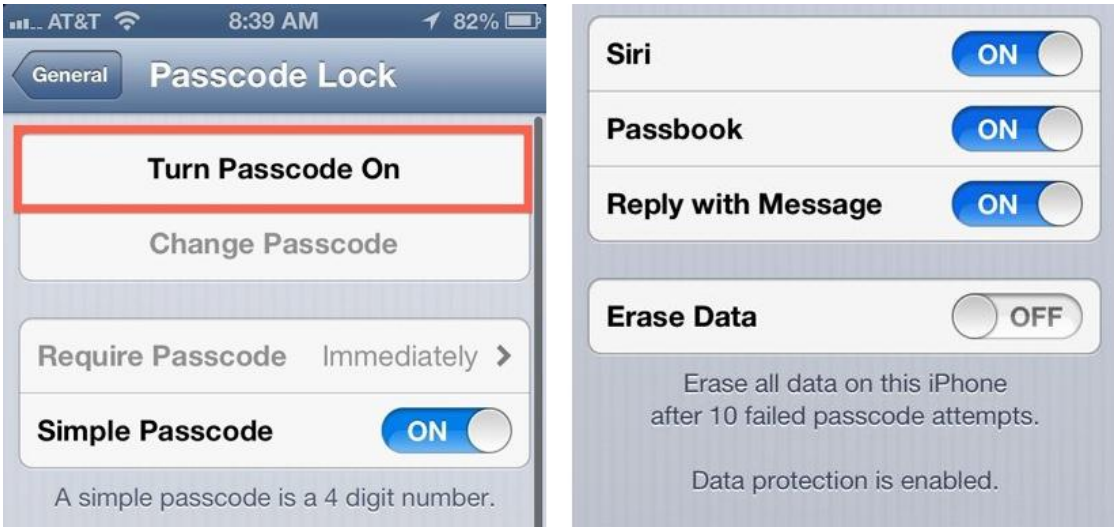
KUVA 9. iOS tietoturva-arkkitehtuuri (Apple 2012c, 3.)

Androidista poiketen, iOS ei tue muistikorttien käyttöä, vaan käyttää ainoastaan laitteeseen rakennettua sisäistä muistia, jota uusimmassa iPhone 5:ssä on saatavilla 16 - 64 gigatavua (Apple 2012a). Tämä tosin lienee lähinnä Applen suunnitteluratkaisu iPhonelle, eikä niinkään käyttöjärjestelmän sanelema ominaisuus. Se on kuitenkin tietoturvallisempi ratkaisu, sillä laitteen sisäisessä muistissa oleviin tietoihin ei pääse helposti käsiksi, muuta kuin itse laitteen kautta. Lisäksi iOS salaa muistissa olevat tiedot automaattisesti 256-bittisellä AES – kryptauksella. (Apple 2012b, 3.)

Näihin tietoihin voidaan silti päästä käsiksi ilman käyttäjän salasanaa, ns. jailbreak -menetelmällä, joka vaatii kuitenkin huomattavasti vaivaa ja taitoa (Symantec 2011, 5). iOS:ssä on kuitenkin vielä tämän lisäksi ylimääräinen toisen tason salauskerros, jonka takana ovat mm. käyttäjän sähköpostit liitteineen. Tätä toisen tason kerrosta on käytännössä mahdoton murtaa ilman käyttäjän salasanaa, joten voidaan sanoa laitteen paikallisen tietosuojauksen olevan erittäin hyvällä tasolla. (Symantec 2011, 5 – 6.)

Kuten Androidissa, myös iOS:ssä on mahdollisuus asettaa laitteelle aakkosnumeerinen salasana umpeutumispäivämäärän kera sekä määrittää, kuinka monta epäonnistunutta kirjautumista vaaditaan, ennen kuin laite tyhjentää tiedot muististaan. (Symatec 2011, 4.) iOS käyttää kuitenkin oletuksena yksinkertaista, vain neljän numeron turvakoodia, jonka käyttäjä voi vaihtaa laitteen asetuksista, ja asettaa haluamansa aakkosnumeerisen salasanan ja joutenoloajan, jonka jälkeen laite kysyy salasanaa. (Van Wyk 2012.)

iOS 6 sisältää Siri-puheohjausominaisuuden. Sirin avulla laitetta voidaan käyttää antamalla sille puhekomentoja. Tunnistettuaan komennon, laite suorittaa halutun toiminnon. iOS 6:n tietoturva-asetuksissa on kuitenkin oletuksena määritelty, että Siri on käytettävissä myös laitteen ollessa lukittu (kuva 10). Tämä mahdollistaa sen, että kuka tahansa voi antaa laitteelle puhekomentoja, ilman salasanan syöttämistä tai edes laitteeseen koskemista. Sirin kautta kenen tahansa on mahdollista kysyä laitteelta esimerkiksi käyttäjän kalenteriin merkittyjä tapaamisia (Van Wyk 2012) tai lähettää viestejä sosiaaliseen mediaan, kuten Twitteriin ja Facebookiin laitteen käyttäjän nimissä. (Mills 2012.)



KUVA 10. iOS 6:n tietoturva-asetuksia (Purcell 2012.)

iOS on sisältänyt versiosta 5 lähtien vakiona pilvitallennus- ja varmuuskopiointipalvelun, jota Apple kutsuu nimellä iCloud. Käyttäjältä kysytään käyttöjärjestelmän ensimmäisen käynnistyksen yhteydessä, haluaako hän ottaa käyttöön iCloud-palvelun. Tämän jälkeen laite varmuuskopioi automaattisesti mm. käyttäjän sähköpostin, yhteystiedot ja kalenterin. Lisäksi käyttäjä voi halutessaan valita palvelun tallentamaan käyttäjän kaikki laitteen muistissa olevat tiedostot Applen palvelimille, josta ne voidaan tarvittaessa palauttaa. (Duffy 2011.) Täydellinen varmuuskopio voidaan tehdä myös tietokoneelle asennettavan iTunes-ohjelmiston kanssa, yhdistämällä laite tietokoneeseen USB-kaapelin avulla. (Apple 2012d.)

iOS tukee vakiona myös laitteen etätyhjennystä sekä etäpaikannusta. Mikäli laite katoaa tai se varastetaan, voi käyttäjä iCloud-palvelun kautta lähettää laitteeseensa komennon, että se tyhjentää kaikki tiedot muististaan. (Hamburger 2011.)

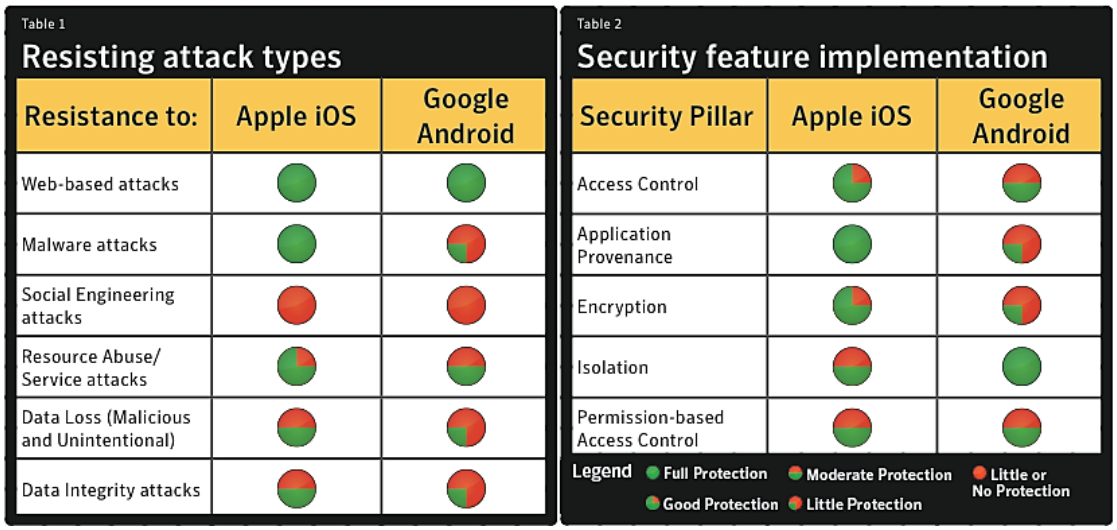
Myös Apple on herättänyt huomiota käyttäjien tietojenkeruulla. The Wall Street Journalin tutkimuksen mukaan, monet iOS- ja Android-sovellukset keräävät tietoja, kuten käyttäjän nimen, puhelinnumeron, puhelimen ID:n ja laitteen sijainnin. Osa sovelluksista erityisesti iOS:llä, lähettää kerättyjä tietoja eteenpäin mm. mainostajille, sillä perusteella, että kerättyjen tietojen avulla voitaisiin esittää mahdollisimman hyvin kategorioituja mainoksia käyttäjälle. (Thurm, Kane 2010.) Esimerkiksi iPhonen musiikkisovellus Pandora lähetti tutkimuksen mukaan käyttäjän tietoja jopa kahdeksalle eri yritykselle, joiden joukossa olivat mm. Apple/Quattro, Google/Adsense, Medialets, Facebook, Weeklyplus ja Yahoo. Toisena esimerkkinä, iPhone-peli Pumpkin Maker

lähettää käyttäjän tietämättä ja lupaa kysymättä laitteen sijaintitiedot erinäisille mainostajille. Apple ei kysyttäessä halunnut kommentoida tapausta mitenkään. (Thurm, Kane 2010.)

Helmikuussa 2012 tuli ilmi, että Applella ja sen laitteiden sovelluskehittäjillä on mahdollisuus myös päästä käsiksi iPhonen käyttäjien yksityisiin valokuviin, sovellustensa kautta. New York Timesin teknologiareportteri Nick Biltonin mukaan on mahdollista, että sovellukset pystyvät käyttäjän tietämättä kopioimaan koko käyttäjän valokuvagallerian. Bilton siteeraa artikkelissaan ohjelmistokehitysyritys Curion perustajaa David E. Cheniä, jonka mukaan laitteen kameralla otettujen kuvien perusteella pystytään tallentamaan tarkkoja tietoja käyttäjän sijainnista, ja kokoamaan näistä tiedoista tietokantoja, joiden leviäminen ei ole enää käyttäjän tai Applen hallussa, siinä vaiheessa, kun tiedot päätyvät kolmansien osapuolten verkkopalvelimille. Apple ei ole halunnut kommentoida tätäkään tapausta. (Bilton 2012.)

Apple on kuitenkin pyrkinyt reagoimaan asiaan lisäämällä iOS6:n asetuksiin yksityisyysvalikon, josta käyttäjä voi hallita sovelluskohtaisia lupia tietojensa käyttöön. Sen kautta voidaan määrittää tietojenkeruuluvat kategorisesti tai per sovellus. Tämä antaa käyttäjälle mahdollisuuden tarvittaessa tarkastaa sovellukselle asennuksen yhteydessä annettuja lupia myös jälkikäteen. (Cipriani 2012b.)

iOS:n tietoturva on saanut myös jonkin verran kehuja alan ammattilaisilta (kuva 11). Tietoturvayhtiö Symantec julkaisi kesäkuussa 2011 A Window Into Mobile Device Security -nimisen raportin, jonka mukaan Applen iOS olisi turvallisempi käyttöjärjestelmä, kuin Googlen Android. Tutkimus paljasti, että iOS on erityisesti turvallisempi haittaohjelmia vastaan sekä sen salausmenetelmät tarjoavat riittävän vahvan suojauksen saapuvan sähköpostin ja mukana mahdollisesti tulevien liitteiden turvaamiseksi. (Symantec 2011, 10.)



KUVA 11. Mukaillen iOS vs. Android: Security Overview (Symantec, A Window Into Mobile Device Security 2011.)

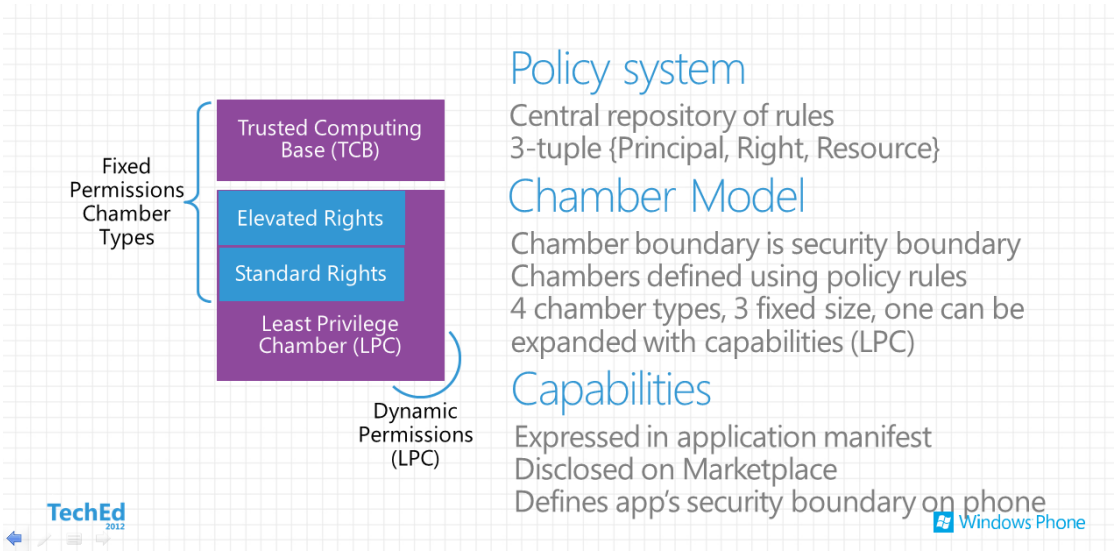
Applen tiukka tapa hallita sen sovelluskauppaa, App Storea, tekee Symantecin mukaan siitä Androidin sovelluskauppaa turvallisemman. Sovelluksen julkaisu App Storessa on kaksiosainen. Ensimmäinen osa edellyttää sovelluksen kehittäjiltä sovelluksen digitaalista allekirjoitusta, joka voidaan suorittaa vain Applelta saatavilla työkaluilla. Tämän jälkeen sovellus lähetetään Applelle arvioitavaksi, ja jos sovellus täyttää Applen vaatimat kriteerit, se ilmestyy myyntiin App Storeen. (Symantec 2011, 4.) Apple on ilmoittanut, että 95 % sille arvioiduksi lähetetyistä sovelluksista läpäisee tarkastusprosessin ja julkaistaan kauppapaikassa kahden viikon sisällä sovelluksen vastaanottamisesta. Sovellus voidaan hylätä esimerkiksi, jos Apple katsoo sen vaarantavan loppukäyttäjän yksityisyyden. (Joseph 2011) Lisäksi sovelluskehittäjät joutuvat maksamaan Applelle vuotuista maksua sen sovelluskauppapalveluiden käytöstä. (Symantec 2011, 4.)

Myös tietoturvayhtiö F-Securen tutkimusjohtaja Mikko Hyppönen on kehaissut iOS:n tietoturvaa. Hyppönen kommentoi kesäkuussa 2012 mikroblogipalvelu Twitterin kautta, että vaikka iPhone on jo 5 vuotta vanha, niin siitä huolimatta koko aikana ei ole tullut vastaan yhtäkään merkittävää haittaohjelmatapausta, josta hän onnittelee Applea. (Hyppönen 2012.)

3.6 Windows Phone

Windows Phone on Microsoftin kehittämä mobiilikäyttöjärjestelmä ja jatkoa vanhemmille Windows Mobile -käyttöjärjestelmille. Se on Microsoftin vastaus Applen ja Googlen hallitsemille älypuhelinmarkkinoille ja vielä melko nuori, sillä sen ensimmäinen versio, 7, esiteltiin ensimmäisen kerran Barcelonan Mobile World Congress – tapahtumassa, Tammikuussa 2010. (Polimenov 2009.)

Windows Phone käyttää sovelluksien osalta tietoturvamallia, jossa sovelluksesta riippuen, sille voidaan myöntää eritasoiset oikeudet laitteen toimintoihin. Microsoft kutsuu eri oikeustasoja kammioksi, ja laitteen tietoturvamallia nimellä Chamber model, eli kammiomalli, koska siihen kuuluu neljä eri kammiotyyppiä (kuva 12). Tällä pyritään estämään esimerkiksi tapaukset, joissa sovellus pääsee käyttäjän tietämättä käsiksi toimintoihin, jotka eivät ole sen käytön kannalta mitenkään välttämättömiä tai tarkoituksenmukaisia ja saattavat vaarantaa laitteen tietoturvan. (Meeus 2012.)



KUVA 12. Windows Phone 7 tietoturvamalli (Meeus 2012.)

Kuten Android ja iOS, myös Windows Phone tukee väliajoin vanhentuvaa aakkosnumeerista salasanaa (Meeus 2012). Käyttäjä voi myös määrittää (kuva 13) laitteen kysymään salasanaa aina halutun joutenoloajan jälkeen (Halsey 2011).

KUVA 13. Windows Phone 7.5 lukitusasetukset (Halsey 2011.)

Windows Phone tukee vakiona Microsoft Exchange Server -käyttäjätilien käyttämistä laitteessa, joka mahdollistaa mm. useamman käyttäjätilin samassa laitteessa sekä muita erityisesti yrityksille suunnattuja toimintoja. Lisäksi voidaan määrittää salasana-asetukset hyvin tarkasti, ja esimerkiksi on määritettävissä, kuinka monta kertaa salasana voidaan syöttää väärin, ennen kuin laite tyhjentää sisäisen muistinsa. (Microsoft 2010.)

Windows Phone tukee laitteen etäpaikannusta ja sisäisen muistin etätyhjennystä. Mikäli laite katoaa, tai varastetaan, voi käyttäjä virallisen windowsphone.com -verkkosivuston kautta paikantaa, etälukita, tai etätyhjentää laitteen. (Windows Phone 2012b.)

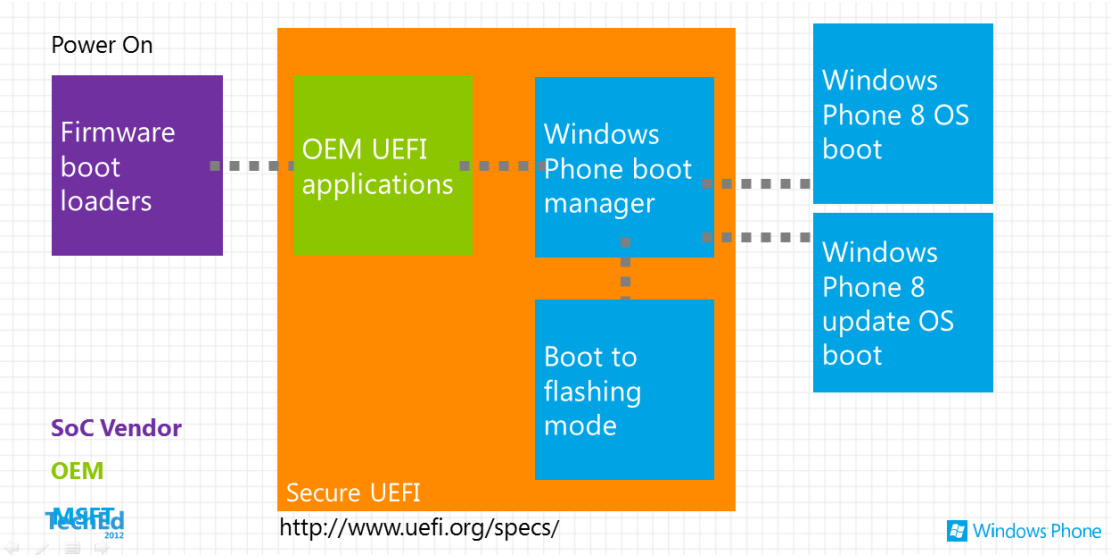
Windows Phone käyttää vakiona Skydrive-pilvitallennuspalvelua, joka toimii pääperiaatteiltaan melko samantyyppisesti kuin Applen iCloud. Skydrive antaa käyttäjän varmuuskopioida pilveen mm. yhteystiedot, sähköpostin, kalenterin sekä on läsnä monissa laitteen vakiosovelluksissa, kuten Microsoft Office -toimistosovelluksissa, joilla käsitellyt dokumentit voi varmuuskopioida pilveen, ja käyttäjän kuvagalleriassa, joka voidaan synkronoida pilveen automaattisesti. Nämä ovat käyttöjärjestelmän perustoimintoja, mutta Microsoft tarjoaa myös erillistä Skydrive-sovellusta, joka antaa käyttäjälle mahdollisuuden selata pilveen tallentamiaan tietoja vielä monipuolisemmin. (Edmonds 2012.) Myös tietokoneelle tehtävä varmuuskopio kaikesta puhelimen sisäl-

löstä onnistuu asentamalla tietokoneelle Microsoftin Zune-ohjelmiston ja liittämällä laite tietokoneeseen USB-kaapelilla. (Windows Phone 2012c.)

Microsoft mukailee Applen mallia sovelluskauppatarjontansa suhteen. Kaikki Windows Phone Marketplacen kautta saatavilla olevat sovellukset edellyttävät Microsoftin digitaalista allekirjoitusta, jonka Microsoft voi myöntää testattuaan sovelluksen ennen niiden julkaisua ja varmistettuaan, että sovellus täyttää Microsoftin asettamat laatu-, yhteensopivuus- ja tietoturvastandardit. (Windows Phone 2012a.)

Microsoft esitteli uusimman version, Windows Phone 8:n kesäkuussa 2012 ja ensimmäisten sitä käyttävien laitteiden on tarkoitus tulla markkinoille vielä vuoden 2012 aikana. (Lehto 2012b.)

Microsoftin Alan Meeus esitteli Windows Phone 8:n merkittävimpiä tietoturvauudistuksia TechEd Europe 2012 -konferensissa, kesäkuussa 2012. Meeuksen mukaan Windows Phone 8 käyttää Applen iOS:n tyyppistä, Secure Boot -nimistä käynnistysmenetelmää, joka tarkistaa joka käynnistyskerralla käyttöjärjestelmän eheyden ja varmistaa, ettei käyttöjärjestelmän ytimen yhteydessä käynnisty mitään ylimääräisiä, haitallisia prosesseja, jotka eivät ole Microsoftin digitaalisesti allekirjoittamia (kuva 14). Tällä voidaan estää mm. laitteen murtaminen ns. jailbreak-menetelmällä. (Meeus 2012.)



KUVA 14. Windows Phone 8:n Secure Boot -käynnistysmenetelmä (Meeus 2012.)

Toinen Windows Phone 8:n merkittävä tietoturvauudistus on tuki laitteen sisältämien tietojen salaukselle, joka on käytössä laitteissa oletuksena. Kryptausmenetelmä on Microsoftin mukaan sama, kuin sen työpöytäkäyttöjärjestelmissä käyttämä BitLocker. Salaus ei kuitenkaan ulotu SD-muistikorttien sisältöön, vaan ainoastaan laitteen sisäinen muisti on kryptattu. (Meeus 2012.)

Windows Phone 8 tukee myös verkon yli laitteeseen ladattavia ohjelmistopäivityksiä. (Sams 2012.)

Lisäksi esiteltiin Windows Phone 8:n uutta MDM-politiikkaa ja tapoja, jolla laitteita voidaan hallita organisaation toimesta, käyttäen samoja työkaluja, kuin Windowsin työpöytäympäristössä, kuten vaikkapa Exchangea. (Meeus 2012.)

Windows Phone 8:n mukana lanseerataan myös uusi Internet Explorer 10 internet-selain, joka tukee Microsoftin työpöytäkäyttöjärjestelmistä tuttua SmartScreen-suodatinta, joka päällä ollessaan estää pääsyn Microsoftin haitalliseksi luokittelemille verkkosivuistoille (Meeus 2012). SmartScreen-suodattimen haitallisten sivustojen tietokantaa Microsoft on kehittänyt ainakin jo vuodesta 2008 lähtien. (Mediati 2008.)

Tietoturvayhtiö F-Securen asiantuntija Sean Sullivanin mukaan Windows Phonen tietoturva on hyvällä tasolla, sillä hän ei ollut 2011 Marraskuuhun mennessä havainnut vielä yhtäkään Windows Phone -haittaohjelmaa. Hän näkee kuitenkin Microsoftin .NET Framework -ohjelmistokirjaston mahdollisena houkuttelevana kohteena haitta-ohjelmien tekijöille, sillä .NET Frameworkia käytetään Windows Phonen lisäksi myös työpöytäkäyttöjärjestelmä Windows 7:n ja Xbox Live -pelipalvelun sovellusten alustana. Sullivan mainitsi myös olevansa erittäin vakuuttunut Nokian hyvästä maineesta Symbian-laitteidensa tietoturvan suhteen ja uskoo, että ainakin Nokia ottaa Windows Phone laitteidensa tietoturvan tosissaan. (Linnake 2011.)

Windows Phone on kuitenkin edelleen varsin nuori käyttöjärjestelmä, ja mm. maksujärjestelmäyritys Realex Paymentsin tietoturvajohtaja David Rook on ilmaissut huolensa siitä, että toisin kuin Android ja iOS, Windows Phone ei välttämättä ole vielä tarpeeksi kypsä kaikille yrityksille. Hän kritisoi mm. siitä puuttuvaa VPN-tukea. Kritiikin kohteeksi joutui myös Windows Phonen toimintamalli, joka ei salli sovelluksien

päästä käsiksi toisten sovellusten käsittelemään dataan. Tätä ominaisuutta hän ei usko Microsoftin muuttavan. (Leyden 2012.)

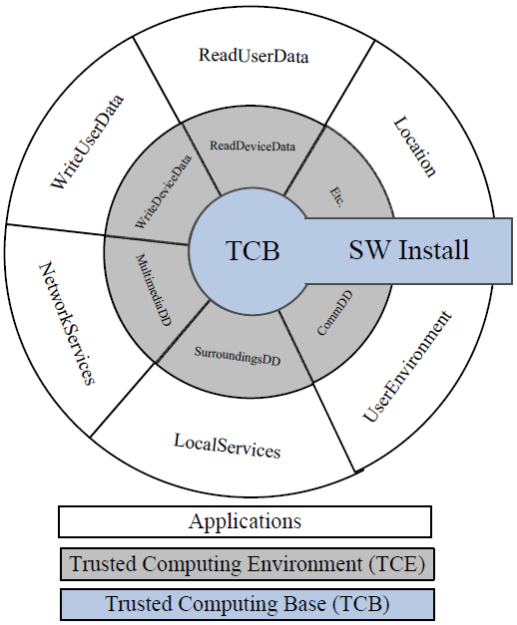
3.7 Symbian

Vanhahko Symbian on pääasiassa vain Nokian älypuhelimissaan käyttämä käyttöjärjestelmä, jonka kuolinisku oli käytännössä Nokian päätös tehdä strateginen yhteistyösopimus Microsoftin kanssa, ja korvata Symbian pikkuhiljaa Microsoftin Windows Phone käyttöjärjestelmällä. Symbian oli pitkään maailman käytetyin mobiilikäyttöjärjestelmä ja 2000-luvun puolivälissä sen osuus kaikista järjestelmistä oli peräti 70 prosenttia. (Turney 2011.) Tänä vuonna sen markkinaosuus on romahtanut peräti alle kymmenesosaan tuosta, ollen alle 7 % (IDC 2012). Nokia on kuitenkin julkaissut yhä uusia Symbian-laitteita Windows Phonea käyttävän Lumia-lippulaivamallistonsa rinnalla. Se odottaa myyvänsä vielä satoja miljoonia Symbian-laitteita tulevien vuosien aikana. Käyttöjärjestelmän tulevaisuuteen ei tiettävästi silti enää investoida merkittävästi. (Turney 2011.) Viimeisin Symbian versio Belle, julkaistiin Elokuussa 2011 (Lehto 2011).

Vaikka Symbian onkin menettänyt ylivaltansa ja on pikkuhiljaa putoamassa markkinajohtajien rinnalta, on sen osuus erityisesti yrityspuhelimista edelleen merkittävä, joten sitä ei voida tässäkään yhteydessä jättää huomioimatta (Pietarinen 2011). Koska Symbian on elinkaarensa ehtoopuolella oleva käyttöjärjestelmä, ei tässä opinnäytetyössä paneuduta juurikaan sen mahdollisuuksiin, tai siihen mahdollisesti kohdistuviin uhkiin, vaan se on otettu mukaan vertailuun lähinnä sen vuoksi, jotta nähdään miten se ominaisuuksiensa ja tekniikkansa osalta eroaa uudemmista mobiilikäyttöjärjestelmistä. Näin saadaan toivottavasti käsitys siitä, missä asioissa uudet kilpailijat ovat mahdollisesti menneet Symbianista edelle.

Symbianin tietoturvamallia kutsutaan nimellä Trusted Computing Platform, joka perustuu nimensäkin mukaisesti eri luottamustason omaaviin kerroksiin. Se rakentuu kolmesta pääkerroksesta, jotka ovat Trusted Computing Base (TCB), Trusted Computing Environment (TCE) sekä sovelluskerros (kuva 15). Käyttöjärjestelmän keskeisin osa on TCB-kerros, joka sisältää järjestelmän ytimen, F32-tiedostopalvelimen sekä sovellusten asennusohjelman, jotka on luokiteltu kaikkein luotetuimmiksi toiminnoiksi. TCE-kerros sisältää käyttöjärjestelmän ytimen päällä ajettavia toimintoja ja sovel-

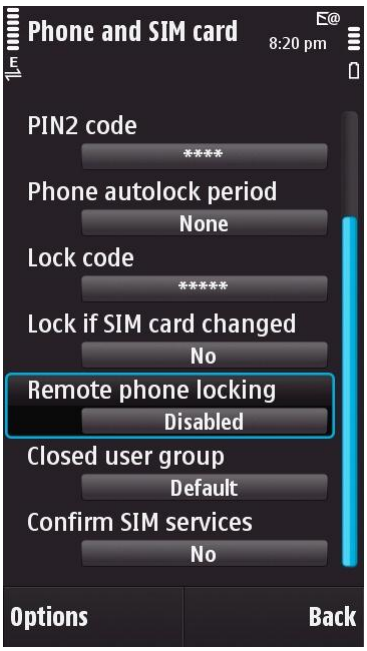
luksia, kuten käyttöliittymän tai muita laitteen valmistajan lisäämiä toimintoja, joita ei ole luokiteltu yhtä luotettavaksi, kuin TCB-kerroksen toimintoja. Sovelluskerroksella ajetaan kaikki kolmansien osapuolten sovellukset, joille ei ole annettu pääsyoikeutta syvemmän tason järjestelmätoimintoihin. Lisäksi sovellustasolla ajettavia sovelluksia voi olla kahta eri tyyppiä, digitaalisesti allekirjoitettuja tai allekirjoittamattomia sovelluksia, joista ensimmäiseksi mainitut on luokiteltu luotettavammiksi. (Li ym. 2010.)



KUVA 15. Symbianin Trusted Computing Platform -tietoturvamalli (Li ym. 2010.)

Symbian tukee aakkosnumeerista salasanaa, halutun joutenolon jälkeen tapahtuvaa salasanan kyselyä (Vinu 2009) sekä laitteen lukitusta ja tyhjennystä etäyhteydellä, Exchange ActiveSyncin kautta. Etälukitus (kuva 16) toimii myös siten, että kun lukittavaan puhelimeen lähetetään ennalta määritetty tekstiviestikomento, laite lukitsee tämän jälkeen itsensä ja pyytää avattaessa suojakoodia. (Nokia 2012b, 125.)

Myös Nokia tarjoaa kolmansien osapuolten sovelluksia omasta sovelluskaupastaan Nokia Storesta. Sovelluskauppaan tarjolle tulevien sovellusten on läpäistävä Nokian itse määrittelemä arviointiprosessi, ennen niiden saataville asettamista. (Prince 2009.)



KUVA 16. Nokia N97 -laitteen tietoturva-asetuksia (Vinu 2009.)

Symbian-laitteissa tietojen automaattinen varmuuskopiointi on hoidettu Nokia Sync -sovelluksella, joka varmuuskopioi laitteen yhteystiedot, kalenterin ja muistiinpanot verkon yli, josta ne ovat tarvittaessa palautettavissa. Palvelun käyttöönottamiseksi vaaditaan rekisteröityminen Nokian verkkopalveluun. (Lehtiniitty 2008.) Mikäli käyttäjä haluaa tehdä täydellisen varmuuskopion, eli varmuuskopioida kaikki laitteen sisältämät tiedostot, täytyy käyttää tietokoneelle asennettavaa ohjelmistoa, jolla synkronointi tapahtuu manuaalisesti, yhdistämällä laite tietokoneeseen USB-kaapelilla. Käytettävä ohjelmisto on laitteesta riippuen joko Nokia Suite tai Ovi Suite. (Makwana 2012.)

Symbian tukee vakiona puhelimen sisäisten tietojen sekä erillisen muistikortin sisällön salausta, joka ei ole vakiona käytössä, mutta sen saa asetettua päälle laitteen asetuksista. (Nokia 2012b, 125.) Nokia tarjoaa myös Symbian-laitteille verkon yli ladattavat ohjelmistopäivitykset, ja laitteen voi asettaa ilmoittamaan aina kun uusi päivitys on saatavilla. (Nokia 2012b, 117 - 118.)

3.8 Johtopäätökset ja vertailu

Edellä käsiteltyjen asioiden pohjalta, olen koonnut seuraavaan taulukkoon (taulukko 1) em. mobiilikäyttöjärjestelmien mielestäni käyttäjän kannalta merkittävimmät, jok-

seenkin vertailtavissa olevat tietoturvaominaisuudet. Tässä on siis otettu huomioon vain ominaisuudet, jotka ovat virallisia ja käyttöjärjestelmän vakiona tukemia.

TAULUKKO 1. Android-, iOS-, Windows Phone- ja Symbian – käyttöjärjestelmien merkittävimmät erot tietoturvaominaisuuksissa.

Tietoturvaominaisuudet vakiona	Android (4.1, "Jelly Bean")	iOS (6.0)	Windows Phone (8.0, "Apollo")	Symbian (10.1, "Belle")
Aakkosnumeerinen salasana	kyllä	kyllä* (oletuksena 4-numeroinen)	kyllä	kyllä
Salasanan asettaminen vanhentuvaksi	kyllä	kyllä	kyllä	ei
Laitteen tyhjennys, jos väärä salasana syötetään liian monta kertaa	kyllä	kyllä	kyllä* (*käytettäessä Exchange-tiliä)	ei
Laitteen aikalukitus	kyllä	kyllä	kyllä	kyllä
Laitteen etälukitus	ei	kyllä	kyllä	kyllä
Laitteen etätyhjennys	ei	kyllä	kyllä	ei
Sovelluskaupan sovellukset digitaalisesti allekirjoitettuja	ei	kyllä	kyllä	kyllä
Laitteen sisäisen muistin salaus	kyllä	kyllä	kyllä	kyllä
Muistikortin sisällön salaus	ei	ei tue muistikortteja	ei	kyllä
Varmuuskopiointi pilveen automaattisesti	kyllä* (*vain perustiedot)	kyllä	kyllä* (*perustiedot ja valikoidut sovellukset)	kyllä* (*vain perustiedot)
Varmuuskopiointiohjelmisto tietokoneelle	ei	kyllä (iTunes)	Kyllä (Zune)	kyllä (Nokia Suite)
Ohjelmistopäivitykset verkon yli suoraan laitteeseen	kyllä	kyllä	kyllä	kyllä

Tämän vertailun valossa näkisin, että merkittävimpien tietoturvaominaisuuksien osalta monipuolisimmat käyttöjärjestelmät ovat iOS ja Windows Phone, jotka ovat ominaisuuksiltaan melko lähellä toisiaan. Nämä olivat myös ainoat käyttöjärjestelmät, jotka tukivat muistikortin sisällön salausta lukuun ottamatta kaikkia muita listattuja ominaisuuksia edes jollain tasolla. Tosin iOS:n kohdalla muistikortin salausta ei kuitenkaan voida tässä ottaa huomioon, sillä iOS-laitteissa ei yksinkertaisesti ole mahdollisuutta käyttää muistikortteja ollenkaan.

Android osoittautui ominaisuuksiltaan rajoittuneimmaksi. Mielestäni merkittävimmät erot Androidissa verrattuna muihin ovat varmuuskopiointimahdollisuuksien, etälukitus- ja tyhjennysmahdollisuuksien puute sekä ehkä liian liberaali sovelluskauppapolitiikka.

Symbian sisältää iästään huolimatta kohtuullisen monipuoliset tietoturvaominaisuudet, mutta en näe sen silti olevan enää uusimpien käyttöjärjestelmien tasolla. Koska Symbian on markkinoilta pikkuhiljaa poistumassa oleva käyttöjärjestelmä, niin ei liene myöskään todennäköistä, että sen tietoturvaominaisuuksia tulevaisuudessa enää paljoa kehitettäisiin.

Ominaisuudet, joita kaikki käyttöjärjestelmät tukivat ja joissa ei ollut merkittäviä eroja, olivat aakkosnumeerinen salasana, laitteen aikalukitus, laitteen sisäisen muistin salaus sekä verkon yli laitteeseen tarjoiltavat ohjelmistopäivitykset.

Käyttöjärjestelmien yksilöllisiä arkkitehtuurillisia ja muita järjestelmätason toteutuseroja en taulukkoon sisällyttänyt, koska ne ovat taulukon keinoin melko vaikeasti vertailtavissa. Toisaalta näkisin, että kaikilla niillä kuitenkin tähdätään käyttäjän kannalta mahdollisimman tietoturvalliseen käyttökokemukseen, jota tässä työssä lähinnä olen pyrkinyt selvittämään.

4 YLEISESTI MOBIILILAITTEISIIN KOHDISTUVIA RISKEJÄ

Kaikkiin mobiililaitteisiin kohdistuu riskejä käyttöjärjestelmästä riippumatta. Markkinatutkimusyhtiö Dimensional Research suoritti Check Point Software Technologies Ltd:n sponsoroimana tutkimuksen mobiililaitteiden merkityksestä tietoturvalle, ni-

mikkeellä The impact of mobile devices on information security: A survey of IT professionals, ja tulokset julkaistiin Check Pointin verkkosivustolla Tammikuussa 2012. (Dimensional Research 2012, 1.)

Tutkimuksessa kysyttiin 768 IT-ammattilaiselta ympäri maailman heidän mielipiteitään mm. mobiilitietoturvauhkien kasvusta, vakavuudesta ja niihin vaikuttavista tekijöistä. Yksi keskeisimmistä havainnoista oli, että jopa 71 % vastaajista näki mobiililaitteiden vaikuttaneen tietoturvatapausten kasvuun. Tutkimuksen perusteella Applen iOS mobiilikäyttöjärjestelmää käyttää 30 % vastaajista, joka tekee siitä täpärästi tutkimuksen käytetyimmän käyttöjärjestelmän, RIM Blackberryn ollessa lähes yhtä suosittu 29 prosentilla. Vastaajista 21 % ilmoitti käyttävänsä Androidia ja 18 % Windows Phonea, Symbianin käyttäjien jäädessä kolmeen prosenttiin. Vastaajien mielestä Googlen Android muodostaa suurimman uhkan tietoturvalle. (Dimensional Research 2012, 4.)

Tutkimuksen mukaan suurin syy mobiililaitteiden tietoturvauhkiin 62 % mielestä löytyy laitteiden käyttäjistä ja yrityksen tietoturvapolitiikan tiedostamisen puutteesta. Muita listattuja syitä olivat mm. turvaton internet-selaaminen, turvattomat WLAN-verkot, kadonneet tai varastetut yrityksen tietoja sisältävät mobiililaitteet, laitteisiin ladatut haittaohjelmat, eri palveluntarjoajien riittämättömät tietoturvapäivitykset ja laitteiden nopea vaihtuvuus. Mobiililaitteiden sisältämiä yritykselle tärkeitä tietoja olivat tutkimuksen mukaan mm. sähköpostit, yrityskontaktit, asiakastiedot ja verkon käyttäjätunnustiedot. (Dimensional Research 2012, 5.)

4.1 Laitteiden hukkuminen

Mobiililaitteiden ollessa kyseessä, on fyysinen turvallisuus nykypäivänä avainasemassa. Yksi ehkä kaikkein merkittävin tietoturvariski mobiililaitteille on laitteen hukkuminen. Katoamisen vaara korostuu, koska älypuhelimet ovat pieniä ja niitä käytetään liikkeellä ollessa, monesti huolimattomasti. Tämän seurauksena laitteen sisältämät tärkeät tiedot voidaan menettää, mikäli niistä ei ole kopiota muualla sekä yritykselle arvokkaat tiedot voivat joutua ulkopuolisten käsiin, jolla voi olla pahimmassa tapauksessa jopa merkittäviä taloudellisia vaikutuksia yritykselle. Nokian tuotetietoturvajohtaja Janne Uusilehto kertoo, että mm. taksien penkeille jää valtava määrä puhelimia, joita omistajat eivät edes kysy takaisin. (Pietarinen 2011.)

Tietoturvayhtiö Lookout Mobile Securityn kokoamien maailmanlaajuisten tilastojen (2012a) mukaan mobiililaite hukataan yleisimmin yöaikaan, yleisimpien katoamispaikkojen ollessa baareja ja yökerhoja. Erityisesti Yhdysvalloissa myös kahvilat, toimistot ja ravintolat ovat yleisiä paikkoja kadottaa älypuhelin. Kaikkein eniten laitteita kuitenkin katoaa erilaisten festivaalien ja juhlien aikana. (Taylor 2012.)

Lookout Mobile Security on arvioinut hukattujen laitteiden suoriksi kustannuksiksi maailmanlaajuisesti vuonna 2012 yhteensä jopa 2,5 miljardia dollaria, mutta laitteiden sisältämien menetettyjen tai ulkopuolisille paljastuneiden tietojen kustannusten yrityksille on arvioitu tänä vuonna olevan jopa 30 miljardia dollaria. (Taylor 2012.)

Suomessa katoaa vuosittain kymmeniä tuhansia kännyköitä. Soneran vuonna 2008 tekemän selvityksen mukaan, Suomessa hukkuu vähintään 15 000 - 20 000 mobiililaitetta vuodessa, joista noin viiden tuhannen arvioitiin olevan yrityskännyköitä. Nykyään lukemat lienevät vieläkin suuremmat. (Tietokone-lehti 2008.)

4.2 Varmuuskopioinnin laiminlyönti

Laitteen kadotessa kaikki ei ole kuitenkaan vielä menetetty, mikäli varmuuskopioinnista on huolehdittu. Kuten tässä työssä aiemmin selvitin, tarjoavat kaikki esittelemäni mobiilikäyttöjärjestelmät vakiona jonkinasteisen mahdollisuuden varmuuskopioida laitteen tiedot automaattisesti pilveen, mutta lienee sanomattakin selvää, että tästä mahdollisuudesta ei ole mitään hyötyä, mikäli sitä ei osata tai muisteta käyttää. Automaattisissa varmuuskopiointiratkaisuissa on kuitenkin eroja, ja vain iOS:n iCloud-palvelu varmuuskopioi vakiona laitteen sisältämät tiedot kokonaisuudessaan pilveen (Duffy 2011). Siksi näkisinkin, että perinteinen, vanha varmuuskopiointitapa kaapelin kautta PC:lle on edelleen omaksumisen arvoinen asia.

Tietoturvayhtiö F-Securen tutkimusjohtaja Mikko Hyppösen mielestä mobiililaitteiden tietoturva ei ole varmuuskopioinnin osalta yrityksissä vielä tarpeeksi hyvällä tasolla. Hyppönen vertaa mobiilitietoturvan toimia pakovakuutukseen, joka hommataan vasta kun talo on jo palanut. Varsinkin älypuhelinten sisältämien tietojen varmuuskopioinnista on huolehdittu kehnosti, väittää brittiläinen tutkimusyhtiö Goode Intelligence. Viestintäviraston tietoturvayksikön päällikkö Erka Koivunen arvioi matkapuhelinten olevan yritysten tietohallinnolle lähinnä ylimääräinen riesa, ja varmuuskopiointi jäte-

täänkin yleensä käyttäjän itsensä vastuulle. Käyttäjä sen sijaan jättää yleensä varmuuskopiot tekemättä, koska sen tekeminen on aikaa vievää puuhaa, jota varten tarvitaan erillinen tietokone ja kaapeli. (Pietarinen 2011.)

Mikko Hyppönen näkee, että Applen iPhonea käyttävien työntekijöiden laitteiden tietoturva on parhaimmalla tasolla, koska iPhone varmuuskopioi aina sisältämänsä tiedot, jos se on asetettu tekemään niin. Lisäksi se sisältää valmiiksi verkkopalveluun yhdistetyn etälukitus- ja tyhjennysmahdollisuuden, jota ei ole vakiona mm. kilpailevissa Nokian Symbian- tai Googlen Android -alustaa käyttävissä laitteissa. Tämä korostuu erityisesti Suomessa, koska yritykset suosivat edelleen Nokian älypuhelimia. (Pietarinen 2011.)

4.3 Pilvitallennuspalvelut – mahdollisuus, mutta myös uhka?

Mukana kulkevien laitteiden kasvun ohella myös erilaisten pilvitallennuspalveluiden käyttö ja kysyntä ovat kasvaneet. Koska tärkeää dataa käsitellään yhä suuremmalla määrällä laitteita eri paikoissa ja tilanteissa, tulisi datan olla tarvittaessa saatavilla sijainnista tai päätelaitteesta riippumatta. Pilvipalvelut tarjoavat yksinkertaisen ja helpon tavan datan varmuuskopiointiin ja kopion nopeaan saatavuuteen, sitä tarvittaessa. (Rousku 2010.)

Käytännössä pilvi tarkoittaa verkon yli jaettavia ohjelmapalveluita, jonka perusajatus on, että tieto ja ohjelmat tallentuvat palvelimille, joihin päätelaitteella päästään käsiksi mistä tahansa, sijainnista riippumatta. Tällöin päätelaitteen fyysiset rajoitukset eivät tule vastaan. Pilvipalveluita voi olla laidasta laitaan, ja englanninkielinen termi cloud computing viittaa mihin tahansa pilvessä ajettavaan sovellukseen, eikä pelkästään tiedon etävarastointiin. (Rousku 2010.)

Pilven kautta toteutettavat tallennus- ja varmuuskopiointipalvelut eivät kuitenkaan ole yksistään autuaaksi tekeviä ratkaisuja, vaan niiden käyttöön liittyy myös potentiaalisesti vakavia riskejä, jotka on syytä ottaa huomioon. Siinä vaiheessa kun yritys varastoi tietojaan pilveen, luovuttaa se samalla kyseisen tiedon itsestään riippumattoman tahon haltuun ja suojaan, eikä yrityksen oma tietoturvakontrolli enää pilveen tallennettujen tietojen osalta päde. Tietoturvayhtiö Nixun johtava konsultti Kim Westerlund näkee, että pilvipalvelut houkuttelevat yrityksiä tekemään päätöksiä harkitsematto-

masti. Erityisen ongelmallisia ovat esimerkiksi henkilötiedot, joiden käsittelyssä tulee ottaa huomioon mahdolliset lainsäädännölliset velvoitteet, mikäli niitä aiotaan säilöä esimerkiksi fyysisesti ulkomailla sijaitseviin pilvipalveluihin. (Siltala 2010.)

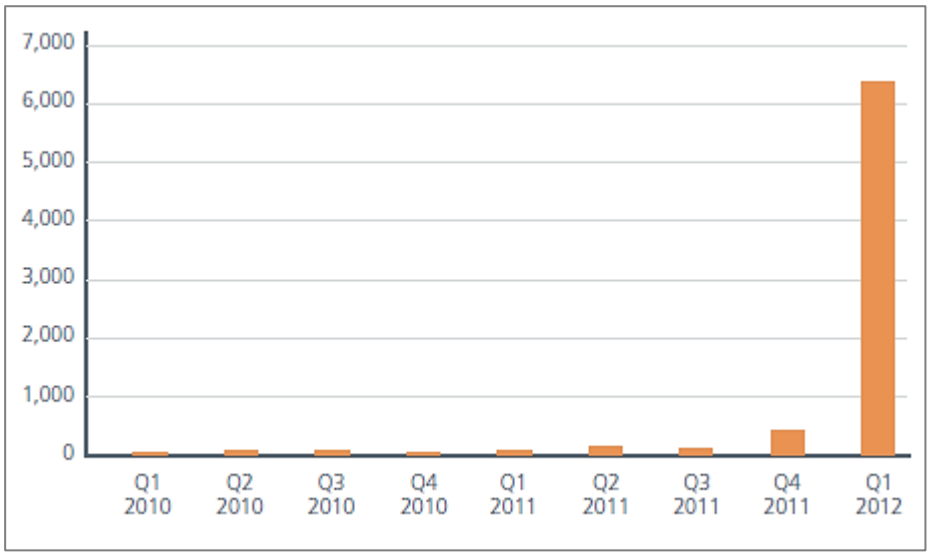
Käytännössä pilvitallennuspalvelun käyttöönottoa voidaan ajatella palvelun ulkoistamisena. Pilvipalvelun käyttöönotto on kuitenkin hyvin helppoa ja mm. käyttöönottosopimuksiin ei useinkaan perehdytä riittävästi. Pilvipalveluntarjoajat jättävät usein kertomatta sopimusseikoista ja palvelutasosta tarpeeksi tarkasti. Westerlundin mielestä ei ole oikein, että pelkästään palveluntarjoaja sanelee salasanan riittävyyden tietojen suojaamiseen, tai suojauksen ohittamisen tietämällä oikean vastauksen turvakysymyksiin. (Siltala 2010.)

Palveluntarjoajat eivät myöskään voi tai halua aina ottaa täyttä vastuuta siitä, että käyttäjien palveluun tallennetut tiedot ovat varmasti aina saatavilla ja turvassa. Esimerkiksi Apple mainitsee iCloud-palvelunsa käyttöehdoissa, että se ei takaa ettei käyttäjän palveluun tallentama data voisi korruptoitua, vahingoittua tai yksinkertaisesti hävitä. Apple muistuttaa, että on käyttäjän vastuulla huolehtia omien varmuuskopioidensa riittävän hyvästä ylläpidosta. (Apple 2012e.) Näin ollen käyttäjä ei voi koskaan täysin varmuudella tietää, onko hänen pilvipalveluunsa sisällyttämä data varmasti turvattu, jolloin ainut varma keino on huolehtia varmuuskopioiden ottamisesta ja säilömisestä itse.

4.4 Haittaohjelmat

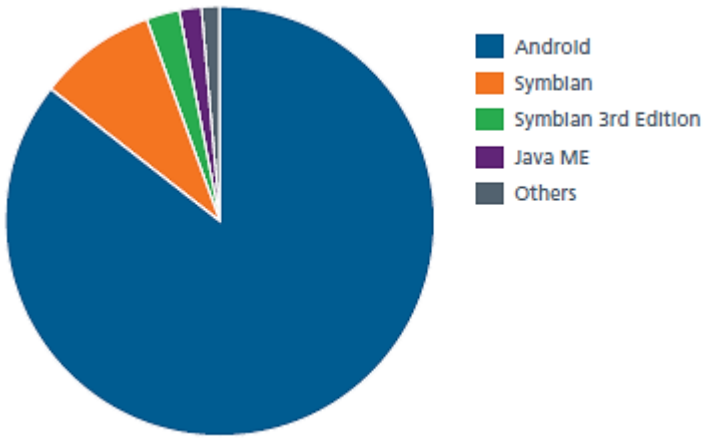
Haittaohjelmiksi luokitellaan sellaiset ohjelmat, jotka aiheuttavat joko tahallisesti tai tahattomasti mitä tahansa ei-toivottuja, eli haitallisia tapahtumia tietojärjestelmiin. Esimerkiksi Spyware-haittaohjelmat, eli ns. vakoiluohjelmat tutkivat tietojärjestelmien sisältämiä tietoja ja lähettävät niitä eteenpäin ulkopuolisille tahoille. (Viestintävirasto 2007.)

Tietoturvayhtiö McAfreen mukaan mobiililaitteiden haittaohjelmat ovat kasvaneet räjähdysmäisesti juuri vuoden 2012 ensimmäisellä neljänneksellä (kuva 17). Suurin osa mobiililaitteita kohtaan tehdyistä hyökkäyksistä ja haittaohjelmista on McAfeen mukaan peräisin Venäjältä ja Kiinasta. (McAfee Labs 2012, 4 - 5.)



KUVA 17. Mobiilihaittaohjelmien kasvu vuodesta 2010 vuoteen 2012 vuosineljännesten tarkkuudella (McAfee Labs 2012, 4.)

Vaikka kasvu koskee erityisesti Android-laitteille tehtyjä haittaohjelmia, koskee haittaohjelmien uhka kaikkia mobiilikäyttöjärjestelmiä (kuva 18). Lukumäärä on noussut vuoden 2011 sadoista haittaohjelmista nyt tuhansiin. Toiseksi eniten haittaohjelmia McAfee on havainnut Symbianille, muiden käyttöjärjestelmien osuuden ollessa toistaiseksi kuitenkin melko marginaalinen. (McAfee Labs 2012, 5.)



KUVA 18. Eri mobiilikäyttöjärjestelmien osuudet kaikista haittaohjelmista (McAfee Labs 2012, 5.)

Suomalainen tietoturvayhtiö F-Secure julkaisi 6.8.2012 raportin vuoden 2012 ensimmäisen neljänneksen mobiililaitteisiin kohdistuvista tietoturvauhkista, nimellä Mobile threat report Q2 2012. Myös siinä todetaan Androidille tehtyjen haittaohjelmien lisääntyneen merkittävästi. Toisen vuosineljänneksen aikana F-Secure havaitsi And-

roidille yhteensä 5033 erilaista haitallista sovelluspakettia, eli APK:ta. Tämä on 64 % enemmän, kuin vuoden ensimmäisellä neljänneksellä. Kaikista havaituista haittaohjelmista peräti 81 % on luokiteltu troijalaisiksi. (F-Secure 2012, 5 – 8.)

Eräs merkittävimmistä uusista uhkista oli drive-by-latausmetodiksi nimetty haittaohjelmatyyppi, josta ensimmäisen tapauksen F-Secure havaitsi Toukokuussa 2012. Android-laitteessa tartunnan saaminen on helppoa, jos käyttäjä on hyväksynyt laitteen asetuksista sovellusten asentamisen tuntemattomista lähteistä. Mikäli käyttäjä tämän jälkeen erehtyy esimerkiksi vierailemaan haittaohjelman sisältävällä verkkosivustolla, on mahdollista, että sivusto lähettää laitteeseen asennuspaketin. Tämän jälkeen käyttäjälle esitetään kysymys vaikkapa tietoturva- tai ohjelmistopäivityksen asentamisesta, ja jos käyttäjä hyväksyy asennuksen, voi haittaohjelma käyttää laitetta välityspalvelimena ja liittää sen osaksi bottiverkkoa. (F-Secure 2012, 5.)

Drive-by-metodin lisäksi, toinen merkittävä F-Securen toisella vuosineljänneksellä havaitsema uusi uhka on Twitteriä hyväksi käyttävä, Cawitt.A-niminen tietojenurkintaohjelma, joka pystyy urkkimaan mm. laitteen tunnistetiedot, IMEI-tunnuksen, puhelinnumeron ja lähettämään laitteesta tekstiviestejä saatuaan komennon emopalvelimeltaan. (F-Secure 2012, 17.)

F-Secure on julkaissut ajantasaisia mobiililaitteiden tietoturvauhka-katsauksia aina vuoden jokaisella neljänneksellä. (F-Secure 2012.)

Suurin syy haittaohjelmatehtailuun on yleensä niiden avulla mahdollisesti saatava rahallinen hyöty. Ehkä tuottavimpia tapoja tehdä rahaa mobiilihaittaohjelmilla ovat erilaiset Toll Fraud -tyyppiset ratkaisut, jotka perustuvat siihen, että haittaohjelma yhdistää tartunnan saaneen laitteen maksulliseen palveluun, joka voi olla mikä tahansa puhelinlaskulla laskutettava palvelu, kuten tekstiviestin lähettäminen maksulliseen palvelunumeroon ilman käyttäjän lupaa. (Lookout Mobile Security 2012b, 10.)

5 MOBIILILAITTEIDEN HALLINTA YRITYSTOIMINNASSA – CASE: ETELÄ-SAVON TIETOHALLINTO OY

Tämän opinnäytetyön toimeksiantaja on Etelä-Savon Tietohallinto Oy. Se on toiminut Kuntien Tiera Oy:n sataprosenttisena tytäryhtiönä toukokuusta 2011 lähtien. Etelä-Savon Tietohallinto Oy on perustettu virallisesti tammikuussa 2007 ja varsinainen toiminta alkoi vuoden 2008 alusta. Sen toimipiste sijaitsee toimistotalo Jääkäri 1:ssä, Mikkelissä. Nykyinen emoyhtiö Kuntien Tiera Oy on perustettu syksyllä 2010 ja se on suomalainen toimija, joka tarjoaa monipuolisia ICT-palveluita kuntasektorille verkostomaisesti, yhteistyössä kuntien sekä muiden julkisten ja kaupallisten toimijoiden kanssa. Se on täysin kuntakentän omistuksessa, joka mahdollistaa mm. kuntien suorahankinnat suoraan yhtiöltä. Omistajina on tällä hetkellä 199 kuntatoimijaa ja yli 30 kuntayhtymää, laskennallisen väestöpeiton ollessa yli 46 %. (Tiera 2012.)

Työn luettavuuden selkeyttämiseksi, tulen käyttämään yrityksen nimestä tästä eteenpäin lyhennettä ESTH.

Toimeksiantoprosessi lähti käyntiin, kun otin puhelimitse yhteyttä ESTH:n projektipäällikkö Jarkko Sanisaloon tiedustellakseni, onko heidän organisaatiollaan kiinnostusta toimia toimeksiantajana. Vinkin ESTH:n mahdollisesta kiinnostuksesta sain opinnäytetyöni ohjaajalta, Mikkelin Ammattikorkeakoulun Janne Turuselta. ESTH osoitti kiinnostusta, joten sovimme tapaamisen heidän toimipisteeseensä keskiviikolle 13.6.2012. ESTH:n edustajina paikalla olivat projektipäällikkö Sanisalon lisäksi organisaation ICT-asiantuntija Raine Koste. Esittelin heille opinnäytetyöni idean ja alustavan suunnitelman, ja he kertoivat hieman ESTH:sta toimintaympäristönä ja siitä, miten heillä mobiililaitteiden hallinta on toteutettu.

ESTH hallinnoi Kuntien Tieran asiakkaisiin kuuluvan Mikkelin kaupungin sekä Etelä-Savon Työterveyden työntekijöiden älypuhelimia. Mikkelin kaupungin käyttäjäkunta koostuu mm. sosiaali- ja terveystyöntekijöistä, oppilaitosten henkilökunnasta sekä kaupungin tekniikan ja infrastruktuurin työntekijöistä. Etelä-Savon Työterveys työllistää hoito- ja terveyspalvelualan työntekijöitä.

ESTH:lla on käytössä Syncshield-ohjelmistoalusta, joka on eräänlainen mobiililaitteiden hallintajärjestelmä. Haastatteluhetkellä Syncshieldin alaisuuteen oli liitettynä 267

älypuhelinta, jotka koostuvat pääasiassa Symbian-, Android-, ja iOS-laitteista. Joitakin Windows Phone-laitteita oli myös jo käytössä sekä muutamia tabletteja, pääasiassa Applen iPadeja. Nokian puhelimista erityisesti E7-malleja on runsaasti. Koska ESTH on vasta hiljattain siirtynyt Kuntien Tieran alaisuuteen, on suurin osa puhelimista Mikkelin kaupungin omistamia laitteita, jotka on jatkossa vähitellen tarkoitus korvata Tiera-konsernin laitteilla. Vanhojen laitteiden tuki on ESTH:lla itsellään, mutta kaikkien helmikuun 2012 jälkeen hankittujen laitteiden tuki on MPY:llä, eli Mikkelin Puhelin Oyj:llä, joka valikoitui laitteiden toimittajaksi ja MDM-palveluntarjoajaksi Mikkelin kaupungin kilpailutettua eri palveluntarjoajia. Puhelinoperaattorina ja mobiiliverkkoyhteyksien tarjoajana toimii Sonera.

Laitteiden tietoturvasta on huolehdittu Syncshieldin lisäksi myös standardoidulla elinkaarimallilla, jossa laitteiden elinkaaren pituus on 36 kuukautta, eli kolme vuotta. Elinkaaren loputtua laitteiden hävittämisestä ja loppusijoituksesta vastaa MPY, joka tarjoaa palvelun sellaisenaan. Käytössä on myös ollut F-Secure virustorjuntaohjelmiston mobiiliversio, mutta siitä ollaan luopumassa, koska sitä ei enää koeta tarpeelliseksi. Sähköpostiohjelmistona toimii Microsoft Exchange. Laitteissa ei ole pakkoa vakioiduille sovelluksille ja käyttäjät voivat halutessaan asentaa laitteisiinsa mitä tahansa sovelluksia esimerkiksi kunkin laitteen omasta sovelluskaupasta. Laitteilla voidaan käyttää verkkoyhteyksiä vapaasti, joko hyödyntäen Soneran mobiililaajakaistaa tai WLAN-verkkoja. ESTH:n toimipisteessä tarjolla on suojattu WLAN-verkko.

Yrityksen historiasta ei löydy toistaiseksi merkittäviä, vahinkoa aiheuttaneita tietoturvatapauksia. Muutama laitteen katoamistapaus on ollut, jonka vuoksi kadonneita laitteita on jouduttu tyhjentämään etäyhteydellä.

ESTH;lla ei toistaiseksi ole laadittuna minkäänlaista laitteen käyttöön tai käyttöönottoon liittyvää dokumentaatiota, jossa ohjeistettaisiin käyttäjiä hyvään tietoturvaan laitteidensa kanssa ja parannettaisiin heidän tietoturvatietoisuuttaan, joten suunnittelimme, että tämän opinnäytetyön pohjalta saisin sellaisen heille laadittua.

5.1 Kyselytutkimus ESTH:n asiakkaille

Tein ESTH:n älypuhelimia käyttäville asiakkaille kyselytutkimuksen, selvittääkseni mm. mitä älypuhelimia asiakkaat käyttävät, miten käyttävät, millä tavoin he ottavat

huomioon tietoturvan ja mikä on heidän oma arvionsa mobiililaitteisiinsa kohdistuvista uhkista.

Tutkimus on toteutettu pääasiassa kvantitatiivisin menetelmin, koska katsoin sen parhaaksi tavaksi tiedonkeruun ja -esittämisen helppouden kannalta, joskin mukana on myös muutama kysymys, johon sai vastata avoimesti. Kvantitatiivisellä menetelmällä tarkoitetaan siis määrällistä tutkimustapaa, jossa käytetään tarkkoja, laskelmallisia mittausmenetelmiä, kun taas kvalitatiivisellä, eli laadullisella tutkimustavalla annetaan sijaa vastaajien omille, vapaamuotoisemmille vastauksille (Tilastokeskus 2012).

Kysely oli vastaajille täysin anonyymi, sillä mitään käyttäjiä yksilöiviä henkilötietoja ei tässä tutkimuksessa ollut tarvetta kerätä. Pyrin saateviestissäni lyhyen selitteen lisäksi painottamaan myös sitä, että vastaaminen vie aikaa vain hetken ja mitä useampi kyselyyn vastaisi, niin sitä laadukkaampi kysely saataisiin.

Tuloksilla oli tarkoitus saada lisää selvyyttä siihen, miten käyttäjän omat teot ja valinnat voivat mahdollisesti vaikuttaa tietoturvaan, eli mikä on käyttäjän rooli tietoturvan toteutumisessa. Pyrin rajaamaan kysymykset siten, että ne olisivat mahdollisimman hyvin ymmärrettäviä ja suoraviivaisia, jotta kaikki osaisivat niihin vastata. Kyselyä tehdessä täytyi ottaa huomioon, että kaikki vastaajat eivät välttämättä ole kokeneita älypuhelimen käyttäjiä. Lähtökohtana oli siis käyttäjäystävällinen kysely. Tällä pyrin takaamaan, että mahdollisimman moni pystyy vastaamaan kyselyyn, ja että vastauksiin voidaan luottaa. Lienee selvää, että asiakkailta kerättyjen tietojen määrällä ja luotettavuudella on suora korrelaatio siihen, kuinka hyvin heidän tarpeitaan vastaavan mobiilitietoturvadokumentaation pystyn ESTH:lle toteuttamaan.

Ennen kyselyn käynnistämistä konsultoin vielä ESTH:n edustajia siitä, mitä mieltä he olivat suunnittelemistani kysymyksistä ja olisivatko he halunneet vielä lisätä jotain sekä olisivatko he halunneet rajata jotenkin kyselyn jakelua. He olivat kysymyksiin tyytyväisiä ja sitä mieltä, että kysely kannattaa lähettää koko henkilöstölle, eikä pelkästään heidän Syncshield-järjestelmäänsä rekisteröidyille älypuhelinkäyttäjille.

Toteutin kyselyn datan analysointi- ja verkkokyselytyökalu Webropolin avulla, jonka kautta lähetin ESTH:n asiakkaiden sähköpostiin linkin kyselyyn. Kyselyyn vastaaminen tapahtui HTML-lomakkeen kautta ja siihen vastasi yhteensä 40 henkilöä. ESTH

suositteli toteuttamaan kyselyn elokuun puolivälin jälkeen, jolloin mahdollisimman moni heidän asiakkaistaan olisi jo palannut lomilta. Siispä avasin kyselyn ja lähetin linkin kyselylomakkeeseen 28.8.2012. Vastausaikaa oli 10 päivää, joskin kaikki 40 vastausta tulivat jo ensimmäisten kolmen päivän aikana.

Itse HTML-kyselylomake löytyy tämän työn liitteistä (liite 2).

5.2 Tutkimustulosten läpikäynti

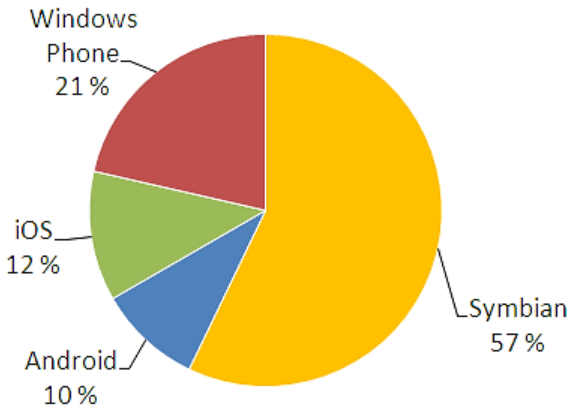
Kyselyssä oli yhteensä 11 kysymystä, jotka seuraavassa käyn tuloksineen läpi ja pyrin samalla analysoimaan niiden merkityksen.

Ensimmäisenä kysymyksenä oli luonnollisestikin selvittää, mitä ESTH:n hallinnoimia laitteita käyttäjillä on käytössään, ja tämän vuoksi kysyin merkkiä ja mallia. Päätin asetella kysymyksen näin sen sijaan, että olisin kysynyt suoraan, mikä käyttöjärjestelmä käyttäjän laitteessa on, sillä uskoin käyttäjien tietävän puhelimensa merkin ja mallin paremmin kuin puhelimensa käyttöjärjestelmän nimen. Merkki ja malli kuitenkin riittivät, sillä niiden perusteella pystyin tarkistamaan suoraan, mikä käyttöjärjestelmä laitteessa on.

Suurimmalla osalla vastaajista oli käytössään Symbian-pohjainen laite, joita oli yhteensä 24 kappaletta. Windows Phone -laitteita oli 9 kappaletta, iOS-laitteita 5 kappaletta ja Android-laitteita 4 kappaletta (kuva 19). Kaikista laitteista peräti 32 oli Nokian valmistamia.

Toisena kysymyksenä oli, onko heillä käytössään myös taulutietokone, eli tabletti ja jos, niin mikä.

Viisi henkilöä ilmoitti käyttävänsä tablettia, mutta vain neljä oli osannut ilmoittaa laitteensa merkin. Ilmoitetut merkit olivat Apple iPad2, määrittelemätön Applen tabletti, Samsung Galaxy Tab II 7.0 sekä määrittelemätön ZTE:n tabletti.



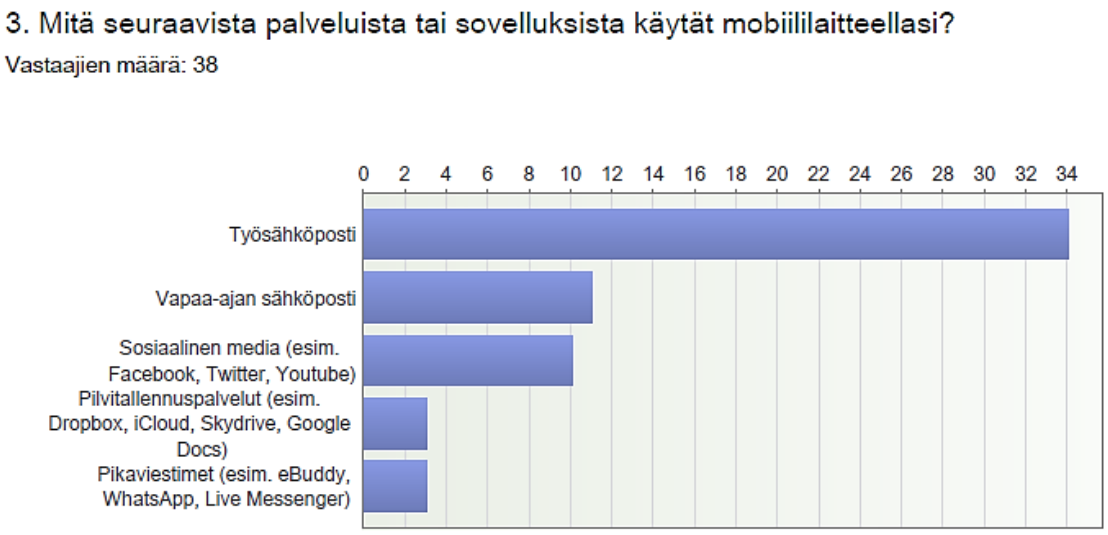
KUVA 19. Kyselyyn vastanneiden ESTH:n asiakkaiden käyttämät mobiilikäyttöjärjestelmät, sisältäen älypuhelimet sekä tabletit

Vaikka reilusti yli puolet vastaajien laitteista olikin Nokian Symbian-puhelimia, on Windows Phone-laitteiden osuus silti jo 21 %, siitä huolimatta, että se on näistä käyttöjärjestelmistä nuorin. Yhtä Samsungia lukuun ottamatta, myös kaikki Windows Phone-laitteet olivat Nokian puhelimia. Sen merkitys ei tämän tutkimuksen kannalta liene kovin merkittävää, mutta olisi silti mielenkiintoista tietää, ovatko Windows Phone-laitteiden omistajat valinneet laitteensa käyttöjärjestelmän vai laitteen valmistajan, Nokian perusteella, ehkäpä todettuaan, ettei uutta Nokian Symbian-laitetta välttämättä kannata enää hankkia.

Kolmannessa kysymyksessä kysyin, mitä palveluja tai sovelluksia käyttäjät laitteellaan käyttävät. Annetut vaihtoehdot olivat työsähköposti, vapaa-ajan sähköposti, Sosiaalinen media (esim. Facebook, Twitter, Youtube), pilvitallennuspalvelut (esim. Dropbox, iCloud, Skydrive, Google Docs) sekä pikaviestimet (esim. eBuddy, WhatsApp, Live Messenger). Valitsin vaihtoehdot sen perusteella, mitkä katsoin olevan oman kokemukseni perusteella yleisimpiä mobiililaitteilla käytettyjä palveluita ja sovelluksia sekä sen perusteella, millä palveluilla ja sovelluksilla katsoin ensisijaisesti olevan tietoturvan kannalta merkitystä.

Vastaajista 34 ilmoitti käyttävänsä laitteellaan työsähköpostia (kuva 20). Vapaa-ajan sähköpostia ilmoitti käyttävänsä 11 henkilöä, sosiaalista mediaa 10 henkilöä, pilvitallennuspalveluita 3 henkilöä sekä pikaviestimiä 3 henkilöä.

Tällä kartoituksella nähdään, minkä palveluiden ja sovellusten osalta tietoturva-asiat tulee ensisijaisesti ottaa huomioon. Kuten oli ennakoitavissa, suurin osa vastaajista käyttää laitteellaan työsähköpostia, joka merkitsee sitä, että laite sisältää mahdollisesti yritykselle luottamuksellisia tietoja. Kuten olen aiemmin todennut, on äärimmäisen tärkeää pitää nämä tiedot ja niitä sisältävät laitteet vain niihin oikeutettujen henkilöiden hallussa. Myös osa vastaajista käyttää vapaa-ajan sähköpostia ja sosiaalista mediaa laitteellaan.

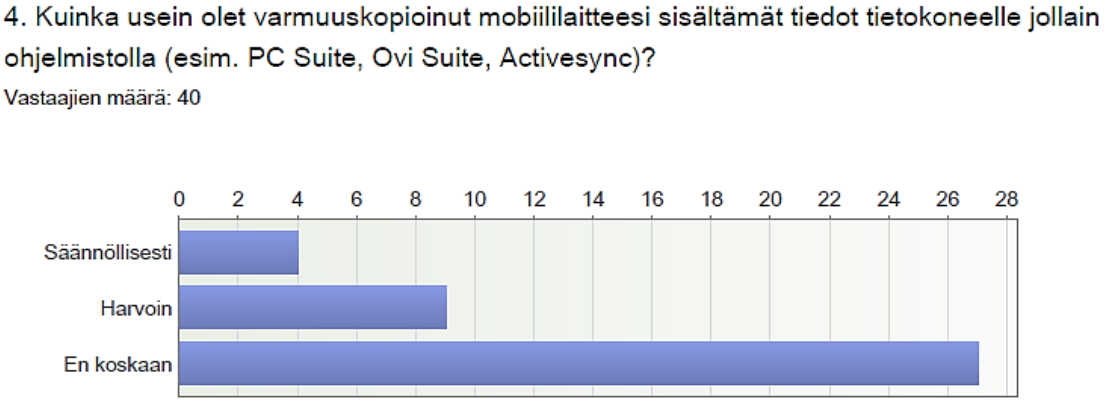


KUVA 20. Laitteella käytetyt palvelut ja sovellukset

Neljännessä kysymyksessä kysyin, kuinka usein käyttäjät ovat varmuuskopioineet mobiililaitteensa sisältämät tiedot tietokoneelle jollain ohjelmistolla (esim. PC Suite, Ovi Suite, Activesync).

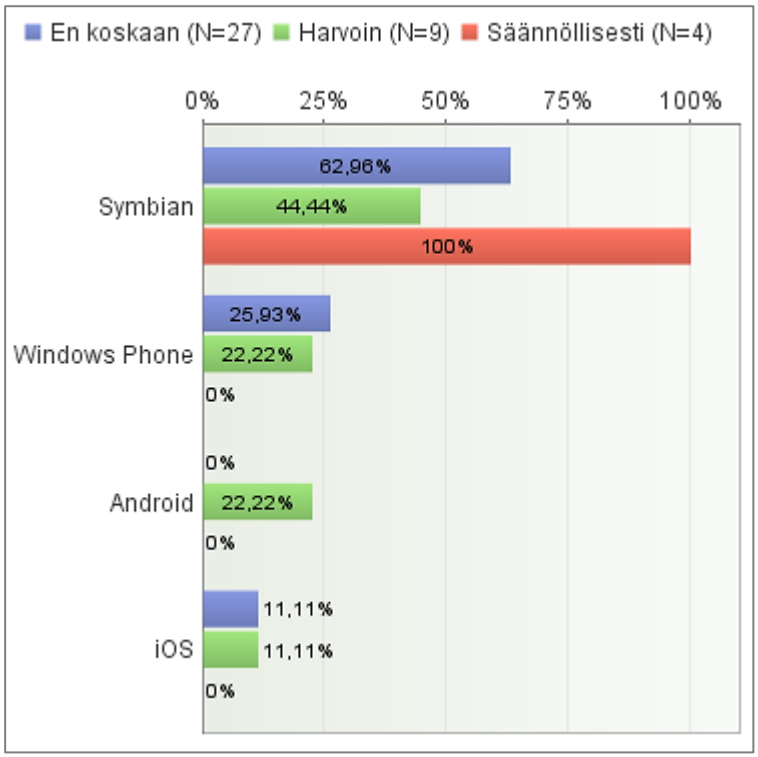
Ainoastaan neljä vastaajaa ilmoitti varmuuskopioivansa tiedot säännöllisesti (kuva 21). 9 vastaajaa varmuuskopioi tietoja harvoin, ja peräti 27 vastaajaa ei ole varmuuskopioinut tietoja koskaan.

Kysyin tätä, koska kuten todettua, varmuuskopiointi on yksi tärkeimmistä yrityksen tietoturvaan liittyvistä asioista. Lisäksi halusin nähdä, miten eri käyttöjärjestelmien käyttäjät varmuuskopioinnin kanssa menettelevät.



KUVA 21. Varmuuskopioinnin säännöllisyys

Kun kysyttiin nimenomaan käyttäjän suorittamasta varmuuskopioinnista tietokoneelle, voisin olettaa, että siihen syntyy tarve, mikäli käyttöjärjestelmä ei vakiona tue verkkoyhteyden yli tapahtuvaa, automaattista pilveen synkronointia. Siihen liittyen huomattavaa oli, että yksikään Windows Phone, Android, tai iOS -käyttäjä ei ilmoittanut varmuuskopioivansa laitteen sisältöä tietokoneelle säännöllisesti, vaan kaikki säännöllisesti varmuuskopioivat olivat Symbianin käyttäjiä (kuva 22). Voisin kuvitella tähän osasyyn olevan sen, että toisin kuin esimerkiksi iOS:stä, Symbianista puuttuu mahdollisuus synkronoida kaikki laitteen sisältämät tiedot automaattisesti pilveen. Myöskään Androidissa ei vakiona tätä mahdollisuutta ole ja kaikki Android-käyttäjät ilmoittivat varmuuskopioivansa tietokoneelle harvoin.

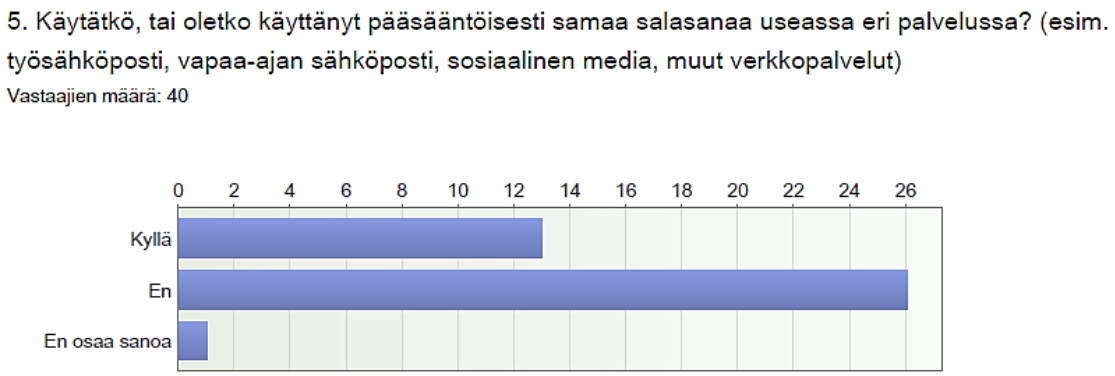


KUVA 22. Varmuuskopioinnin säännöllisyys per käyttöjärjestelmän käyttäjä

Viidennessä kysymyksessä tiedustelin käyttäjiltä, käyttävätkö tai ovatko he pääsääntöisesti käyttäneet samaa salasanaa useassa eri palvelussa, kuten työsähköpostissa, vapaa-ajan sähköpostissa, sosiaalisessa mediassa, tai muissa verkkopalveluissa.

Suurin osa (26) ilmoitti, ettei käytä pääsääntöisesti samaa salasanaa, kun 13 ilmoitti käyttävänsä (kuva 23). Yksi käyttäjä vastasi kysymykseen ”En osaa sanoa”. Tämän vastausvaihtoehdon jätin lähinnä takaportiksi sille, jos joku käyttäjistä ei halua paljastaa onko käyttänyt samaa salasanaa vai ei, joskin lienee myös mahdollista, ettei vastaaja yksinkertaisesti tiennyt tai muistanut.

Syy miksi kysyin tätä, liittyy oleellisesti kolmanteen kysymykseen, jossa kysyin mitä eri palveluita ja sovelluksia käyttäjät laitteillaan käyttävät. On selvää, että mikäli käyttää samaa salasanaa työsähköpostissa sekä esimerkiksi vapaa-ajan sähköpostissa tai jossain sosiaalisen median palvelussa, niin selvittämällä yhdessä palvelussa käytettävän salasanan, voidaan samalla salasanalla tällöin päästä käsiksi myös muihin henkilökohtaisiin käyttäjätileihin.

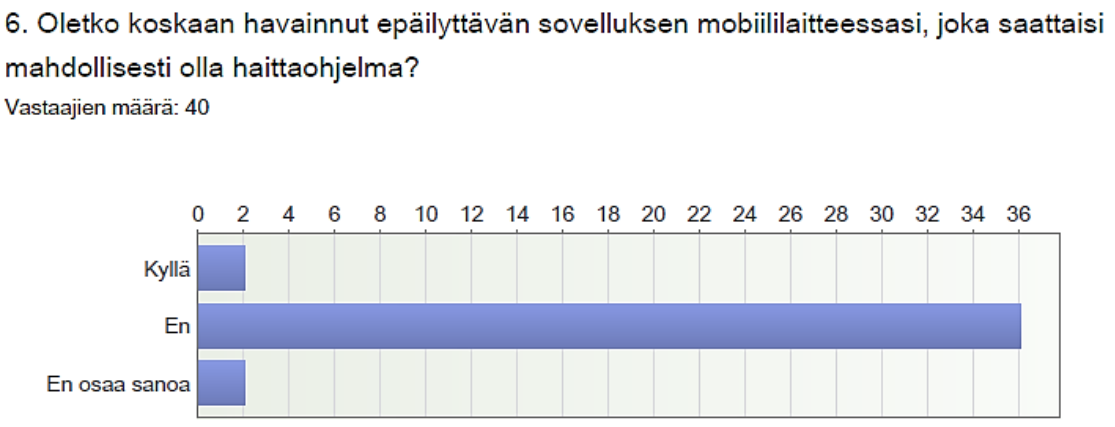


KUVA 23. Saman salasanan käyttö useassa eri verkkopalvelussa

Kuudennessa kysymyksessä tiedustelin, ovatko käyttäjät koskaan havainneet laitteessaan sovellusta, joka on heidän mielestään ollut epäilyttävä tai mahdollisesti haitallinen.

Vain kaksi vastaajaa oli mielestään havainnut tällaisen ohjelman (kuva 24). Vastaajista 36 ei ollut havainnut mitään epäilyttävää ja kaksi ei osannut varmuudella sanoa.

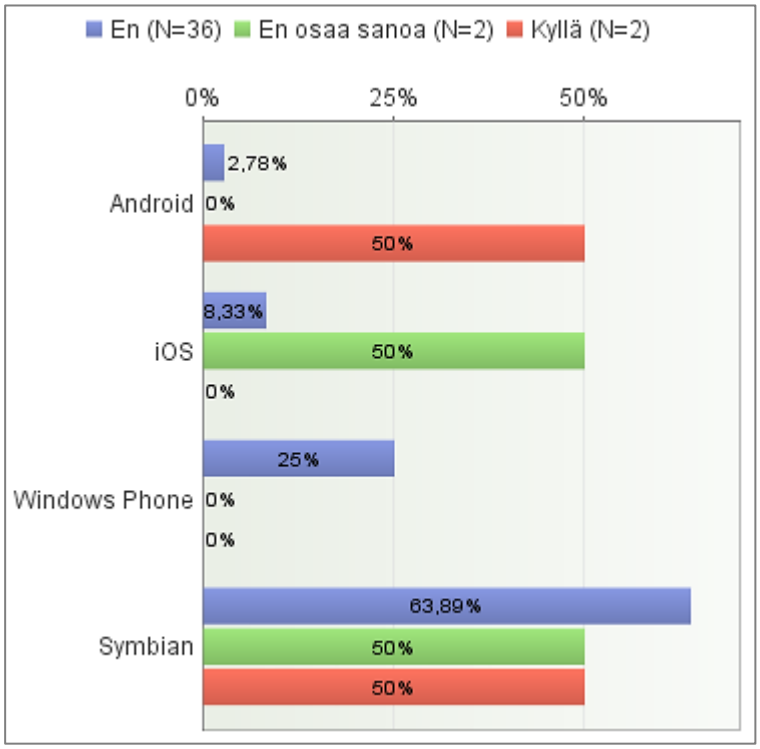
Kysymyksellä pyrin selvittämään, minkälaisia kokemuksia käyttäjillä on haittaohjelmien osalta. Kysymys perustuu käyttäjän omaan arvioon, sillä en halunnut kysyä suoraan, onko käyttäjän laitteessa koskaan ollut varmasti haitallista sovellusta, sillä epäilen, että harva käyttäjä sitä varmuudella voi tietää.



KUVA 24. Käyttäjän mielestä epäilyttävän ohjelman havaitseminen laitteessa

Vaikka vain kaksi oli huomannut mielestään epäilyttävän sovelluksen laitteessaan, niin merkille pantavaa tuloksissa oli mielestäni se, että henkilöistä, jotka olivat epäilyttävää toimintaa havainneet, toinen oli Android-käyttäjä ja toinen Symbian-käyttäjä (kuva 25). Windows Phonea tai iOS:ää käyttävät henkilöt eivät olleet huomanneet

laitteissaan mitään epäilyttävää. Koska kysymyksessä kysyttiin nimenomaan käyttäjän mielestä mahdollisesti epäilyttävästä sovelluksesta, niin ei voida tietenkään varmuudella päätellä, oliko kyseessä varmasti haitallinen sovellus, mutta lienee silti hyvä huomioida varsinkin eri käyttöjärjestelmien käyttäjien toisistaan poikkeavat havainnot.



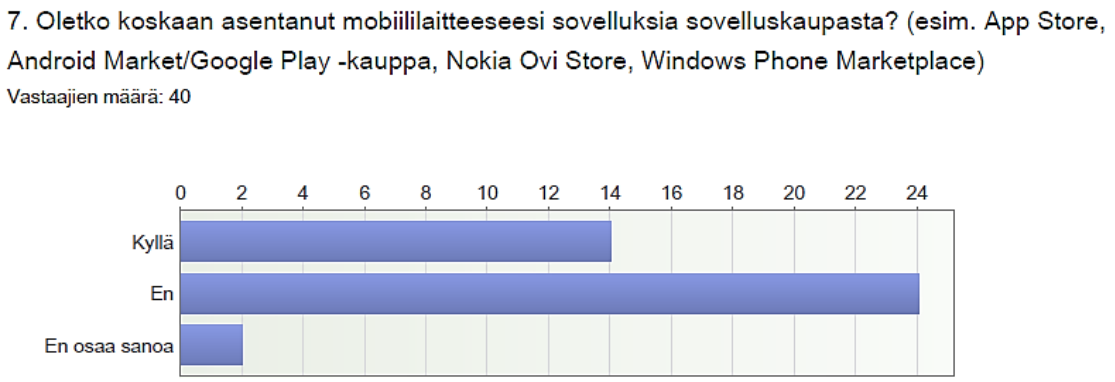
KUVA 25. Epäilyttävän ohjelman havaitseminen laitteessa per käyttöjärjestelmän käyttäjä

Seitsemännessä kysymyksessä kysytään, onko käyttäjä koskaan asentanut laitteeseensa sovelluksia sovelluskaupasta, kuten App Storesta, Google Play -kaupasta, Nokia Ovi Storesta, tai Windows Phone Marketplacesta. Esitin kysymyksen, koska ESTH ilmoitti, että heillä laitteiden pääsyä valmistajien sovelluskauppaan ei ole mitenkään rajoitettu. Syy miksi katsoin tämän kysymyksen olevan merkittävä laitteeseen mahdollisesti kohdistuvan uhkan kannalta, on se, että kuten aiemmin tässä työssä olen todennut, on sovelluskaupasta mahdollista ladata sovelluksia, jotka saattavat olla haitallisia.

Vastaajista 24 ei ollut ilmoittanut käyttäneensä sovelluskauppoja, 14 ilmoitti käyttäneensä ja kaksi vastasi ”En osaa sanoa” (kuva 26). Kun kuitenkin melko suuri osa vastaajista ilmoittaa käyttävänsä sovelluskauppoja, voidaan siitä päätellä ainakin se, että haittasovelluksen saaminen laitteeseen sovelluskaupan kautta on mahdollista, jos-

kaan en pidä tätä opinnäytetyössä aiemmin esiteltyjen tietojen valossa kaikkein merkittävimpänä tietoturvauhkana.

Lisäksi voidaan mainita, että kaikki iOS- ja Android-käyttäjät ilmoittivat ladanneensa sovelluksia sovelluskaupasta, kun taas suurin osa Symbianin käyttäjistä ei ollut käyttänyt sovelluskauppaa, Windows Phone-käyttäjien vastausten jakautuessa melko tasaisesti.



KUVA 26. Sovelluskaupasta ladattujen sovellusten asentaminen

Kahdeksannessa kysymyksessä kysyin, onko käyttäjän mobiililaite koskaan ollut pidemmän aikaa kadoksissa. Vaihtoehdot olivat ”Kyllä, eikä sitä enää löytynyt”, ”Kyllä, mutta se löytyi myöhemmin”, ja ”Ei”. Kukaan neljästäkymmenestä vastaajasta ei ollut koskaan kadottanut laitettaan.

Kuten jo aiemmin olen todennut, on laitteiden fyysinen hukkuminen yksi merkittävimpiä, ellei jopa se kaikkein merkittävin yksittäinen tietoturvariski mobiilaitteille. ESTH:n asiakkaat ovat kuitenkin olleet erityisen huolellisia tai sitten vaan onnekkaita, kun yksikään ei ilmoittanut koskaan hukanneensa laitettaan.

Yhdeksännessä kysymyksessä halusin tietää, kuinka todennäköistä käyttäjien mielestä olisi, että heidän laitteeseensa kohdistuisi jokin tietoturvauhka. Vastausvaihtoehtona oli numeroasteikko yhdestä viiteen, jossa ykkönen vastaa erittäin epätodennäköistä, kakkonen melko epätodennäköistä, kolmonen yhtä paljon todennäköistä, kuin epätodennäköistä, nelonen melko todennäköistä ja vitonen erittäin todennäköistä.

Kaikkien vastaajien keskiarvo oli 2,63, eli keskimäärin käyttäjät kokivat, että heidän laitteisiinsa kohdistuva tietoturvauhka on hieman enemmän epätodennäköistä, kuin

todennäköistä (kuva 27). Havainnollistamisen vuoksi piirsin kuvan alle vielä liukusäätimen, josta näkee mihin kohtaan vastausten keskiarvo asteikolla suunnilleen asettuu.

Kysymyksen esittäminen oli mielestäni oleellista, koska sillä miten käyttäjät tietoturvan henkilökohtaisesti kokevat, lienee suora vaikutus siihen, miten käyttäjät laitteitaan käyttävät ja miten tosissaan he sen tietoturvan ottavat. On huomattavaa, että yksikään vastaaja ei pitänyt tietoturvauhkaa erittäin todennäköisenä.

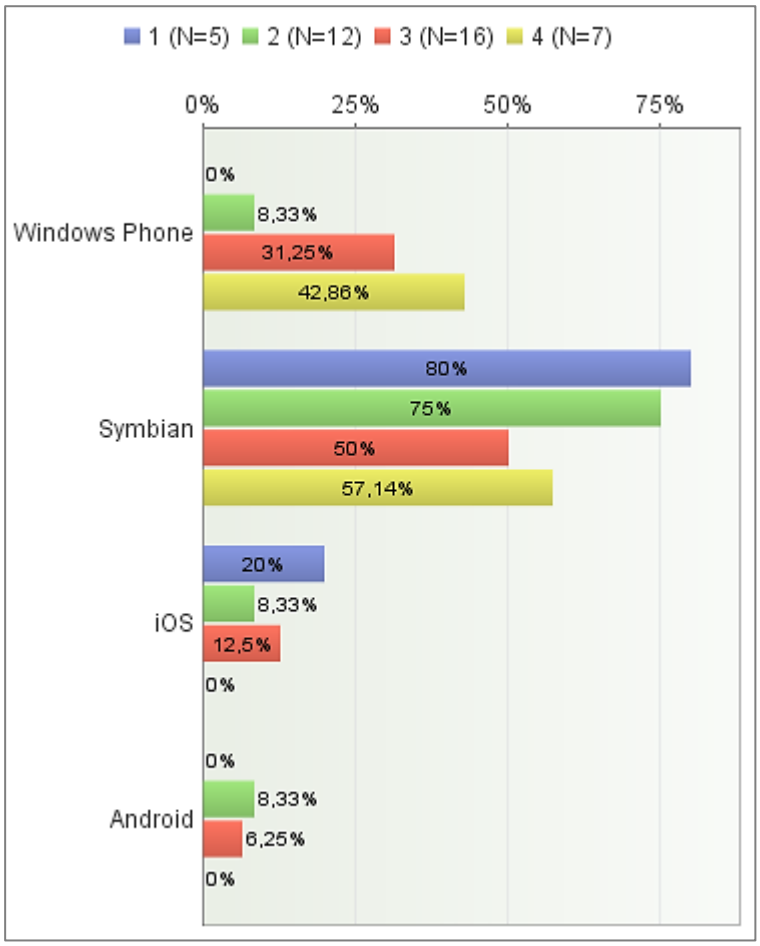
9. Asteikolla 1-5, kuinka todennäköisenä pidät, että mobiililaitteeseesi kohdistuisi jokin tietoturvauhka?

Vastaajien määrä: 40

	1	2	3	4	5		Yhteensä	Keskiarvo
Epätodennäköistä	5	12	16	7	0	Todennäköistä	40	2,63

KUVA 27. Käyttäjän oma arvio hänen laitteeseensa mahdollisesti kohdistuvan tietoturvauhkan todennäköisyydestä asteikolla 1-5

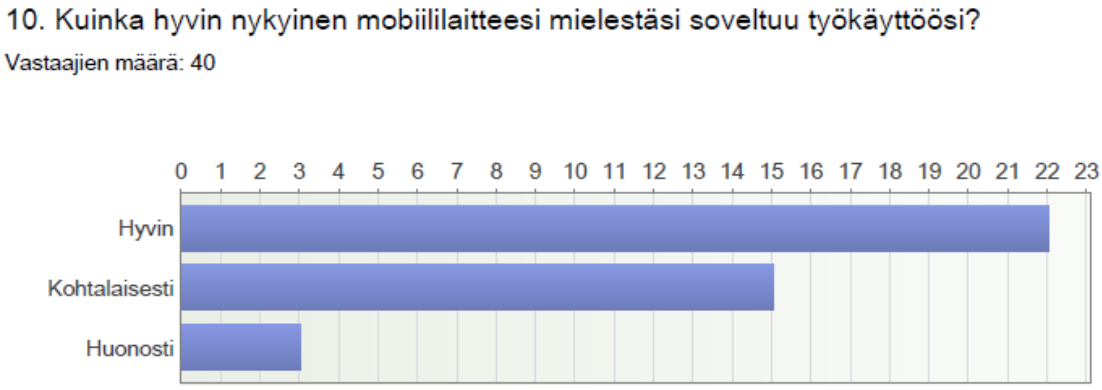
Kun katsotaan vastaajien arvioita tietoturvauhkan todennäköisyydestä käyttöjärjestelmäkohtaisesti, huomataan, että tietoturvauhkaa kaikkein epätodennäköisimpänä pitivät erityisesti iOS-käyttäjät ja Symbian-käyttäjät, eli he kokivat olevansa suhteellisesti parhaiten turvassa tietoturvauhkilta (kuva 28). Suhteellisesti kaikkein todennäköisimpänä tietoturvauhkaa pitivät Windows Phone -käyttäjät, Androidin sijoittuessa lähimmäs kaikkien vastaajien keskiarvoa. Tästä voitaneen päätellä, että ehkä Windows Phone käyttäjät ovat joko kriittisempiä juuri omia laitteitaan kohtaan, tietoturvatietoisempia tai mahdollisesti molempia.



KUVA 28. Arvio tietoturvauhkan todennäköisyydestä asteikolla 1-5 per käyttöjärjestelmän käyttäjä

Viimeiseksi esitetyt kysymykset 10 ja 11 olivat eräänlaisia ylimääräisiä kysymyksiä, joiden vastaukset auttanevat lähinnä Etelä-Savon Tietohallinto Oy:tä arvioimaan heidän asiakkaidensa käytössä olevien laitteiden tasoa ja soveltuvuutta työtehtäviin. Kysymyksessä 10 pyysin käyttäjiä arvioimaan, kuinka hyvin heidän nykyiset mobiililaitteensa heidän mielestään soveltuvat työkäyttöön. Vastausvaihtoehdot olivat ”Hyvin”, ”Kohtalaisesti”, ja ”Huonosti”.

Yli puolet vastaajista (22) oli sitä mieltä, että nykyinen laite soveltuu heille hyvin, 15 sitä mieltä, että soveltuu kohtalaisesti ja vain 3 sitä mieltä, että soveltuu huonosti (kuva 29).



KUVA 29. Käyttäjän tyytyväisyys laitteeseensa työkäytössä

Kysymys 11 oli avoin kysymys, jossa pyysin vastaajia kirjoittamaan vapaasti, mitä puutteita heidän nykyisissä laitteissa heidän omasta mielestään on. Tämä liittyi osaltaan edelliseen kysymykseen ja tarkoituksena oli antaa lopuksi käyttäjille vapaa sana, mikäli heillä oli jotain erityistä huomautettavaa laitteistaan. Kommentit olivat enimmäkseen laitteen yleiskäyttöön liittyviä, mutta myös muutamia laitteen tietoturvaan liittyviä, tai sitä jokseenkin sivuavia kommentteja esitettiin (kuva 30).

Nokia Lumia 710 -laitetta käyttävä vastaaja oli sitä mieltä, että hänen laitteessaan oleva Windows Phone -käyttöjärjestelmä on siitä huono, että hänen mielestään Bluetooth-yhteyden suojauksia tai näkyvyyttä ei voi juurikaan säädellä. Nokia E7 Symbian-puhelinta käyttävä vastaaja ilmoitti, että hänen puhelintaan ei ole päivitetty, eikä hän tiedä miten se hoituu, koska hän ei itse saa sitä tehdä. Nokia E71 Symbian-puhelinta käyttävä vastaaja kertoi, että hänen mielestään puhelin lukkiutuu liian nopeasti ja jatkuva suojakoodin näpyttely on rasittavaa. Nokia C6 Symbian-puhelinta käyttävä vastaaja ilmoitti, että puhelimessa on välillä ongelmia sen jälkeen kun hän vaihtaa sähköpostinsa salasanan.

Avoimet kommentit eivät siis olleet kovin tarkkoja tai syvällisiä, mutta niistä voinee ainakin päätellä sen, että kaikki käyttäjät eivät olleet täysin tyytyväisiä laitteidensa tietoturvaominaisuuksiin tai eivät osanneet käyttää niitä riittävän hyvin. Nämä kokemukset myös osaltaan auttanevat opinnäytetyön lopputuloksena tehtävän tietoturvadokumentaation suunnittelua mahdollisimman hyvin kohderyhmälle sopivaksi.

11. Voit kirjoittaa tähän mitä puutteita laitteessasi mielestäsi on:

Vastaajien määrä: 14

- Puhelintoiminnot huonot, puhelut katkeavat, vaikea löytää numerot yms.
- Hyvin toimivat...
- Windows-käyttöjärjestelmä on huomattavasti Symbian-käyttöjärjestelmää karumpi. Esim. Bluetooth-yhteyden suojauksia tai näkyvyyttä ei voi enemmälti säädellä.
- mm. liiaan pieni näyttö, etenkin liitetiedostojen lukemiseen
- Laite hyvä, palvelut eivät vielä auki (mm.työsähköposti), joten toimii ihan vaan puhelimena. Koska käytössä puhelu/tekstiviesti ei tietoturvariski ole vielä suuri.
- Hankala käyttää =monimutkainen ottaa käyttöön, musiikin lataaminen/kuunteleminen hankalaa, kalenteri surkea
- Puhelintani ei ole päivitetty enkä tiedä miten se hoituu, koska en sitä itse saa tehdä.
- En käytä työssäni älypuhelinta, tämä on oma. Työssä on joku Nokian halkoversio.
- Osaamisessa on puutteita uuden Nokian suhteen
- Nettikävttö iotenkin kankeaa. Asiaa voisi auttaa. ios lukisi kävttöohieet. mutta´kuten asia usein on... Näytön tekstin koko on kankeasti muutettavissa/säädettävissä oman aikuisnäön vaatimusten mukaiseksi.
- Ohjeita eri toiminnoista jonkin verran.
- Puhelin lukkiutuu aika nopeasti ja jatkuva suojakoodin näpyttely on rasittavaa...
- Viestien kirjoittamisen hankaluus, koska näppäimet kosketusnäytössä suht. pienet. Yleinen tietämättömyys, tarvitsisi kurssitusta, miten puhelinta voisi käyttää mahdollisimman hyvin.
- - Välillä puhelimessa ongelmia, esim. sen jälkeen kun vaihdan salasanan s-postiin

KUVA 30. Käyttäjien avoimet kommentit laitteidensa mahdollisista puutteista

5.3 Johtopäätökset tutkimustuloksista

Lähetin kyselyn Webropolin kautta suoraan n. 2400:lle ESTH:n asiakkaalle. Kun tiedossa oli, että näistä asiakkaista ESTH:n hallinnoimien älypuhelinten käyttäjiä oli n. 267 ja osallistujia kyselyyn saatiin yhteensä 40, niin saadaan osuudeksi pyöristettynä n. 15 % kaikista käyttäjistä. Vaikka 15 % ei itsessään ole järin suuri otanta, niin näkisin, että määrällisesti 40 vastaajaa on kuitenkin riittävä otanta tukemaan tätä työtä ja siitä tehtyjä johtopäätöksiä, varsinkin kun vastauksissa edustettuina ovat kuitenkin kaikki tässä työssä käsitellyt mobiilikäyttöjärjestelmät.

Kyselyn tulosten perusteella voidaan kaiketi sanoa, että ESTH:n asiakkaiden mobiililaitteiden tietoturva on keskimäärin jo melko hyvällä tasolla, mutta joitain puutteita löytyy. Erityisesti positiivisena asiana voisin mainita laitteiden fyysisestä turvallisuudesta huolehtimisen, sillä laitteet ovat pysyneet hyvin tallessa, kun kukaan vastaajista ei myöntänyt koskaan hukanneensa mobiililaitettaan.

Huomiotani herätti kuitenkin yleinen tietoturvatietoisuus, sillä käyttäjien suhtautuminen tietoturvaan oli ehkä jopa yltiö-optimistista, eivätkä kaikki käyttäjät välttämättä suhtaudu mobiililaitteidensa tietoturvaan asiaankuuluvalla vakavuudella. Yksikään vastaaja ei pitänyt minkäänlaista tietoturvauhkaa erittäin todennäköisenä, vaan suurin

osa piti tietoturvauhkia enemmän epätodennäköisenä, kuin todennäköisenä. Tietoturvauhka on kuitenkin monisäikeinen käsite ja kuten olen tässä työssä aiemmin maininnut, käyttäjä ei välttämättä tule aina ajatelleeksi, että laitteeseen voisi kohdistua jokin tietoturvauhka myös hänen itsensä toimesta. Eli yksikään vastaaja ei pitänyt erittäin todennäköisenä esimerkiksi sitä mahdollisuutta, että saattaisi vahingossa hukata laitteensa.

Eräs merkittävimmistä havainnoista lienee myös se, että neljäsosa vastaajista ilmoitti käyttävänsä laitteellaan myös vapaa-ajan sähköpostia ja sosiaalista mediaa, ja n. kolmasosa vastaajista ilmoitti käyttävänsä pääsääntöisesti samaa salasanaa eri palveluissa. Kun 90 % vastaajista käyttää laitteellaan myös työsähköpostia, on mahdollista, että moni käyttää samaa salasanaa sekä työsähköpostissa että esimerkiksi sosiaalisessa mediassa, mikä osaltaan voi asettaa yrityksen tietoturvan osittain itsestään riippumattomaksi. Mikäli henkilö käyttää samaa salasanaa sekä sosiaalisen median palvelussa että työsähköpostissa, on kenen tahansa periaatteessa mahdollista päästä luvatta käsiksi kyseisen henkilön työsähköpostiin ja sen mahdollisesti sisältämiin luottamuksellisiin tietoihin, jos henkilön käyttämään sosiaaliseen median palveluun kohdistuisi esimerkiksi sen käyttäjien salasanat paljastava tietovuoto.

Vapaa-ajan sähköpostin tai sosiaalisen median käyttö laitteella merkitsee myös sitä, että käyttäjä hoitaa yrityksen hallinnoimalla laitteella myös henkilökohtaisia tai työtehtäviin mahdollisesti kuulumattomia asioita. Tämä on toki odotettua, mutta se asettaa kuitenkin käyttäjälle tiettyjä vastuita. Kuten aiemmin todettu, käyttäessään organisaation verkkoa, laitetta tai sähköpostia, käyttäjä esiintyy periaatteessa tällöin organisaation edustajana, joka kannattaa muistaa erityisesti, jos kirjoittelee sosiaaliseen mediaan, kuten Facebookiin tai Twitteriin tilapäivityksiä.

Myös eri mobiilikäyttöjärjestelmien käyttäjien välillä oli eroja siinä, millainen heidän käyttökokemuksensa tietoturvan osalta on ollut. Esimerkiksi Symbian-käyttäjät olivat ainoita, jotka kertoivat varmuuskopioivansa laitteidensa sisältämät tiedot säännöllisesti, kaikki Android- ja iOS-käyttäjät olivat ladanneet sovelluskaupasta kolmansien osapuolten sovelluksia laitteisiinsa ja Windows Phone -käyttäjät pitivät tietoturvauhkia kaikkein todennäköisimpänä. Pelkästään tämän kyselyn perusteella on kuitenkin vaikea määritellä minkä käyttöjärjestelmän käyttäjien tietoturva on parhaimmalla tasolla, koska kysely painottui enemmänkin käyttötottumuksiin, kuin absoluuttisiin eroihin eri

käyttöjärjestelmien tietoturvallisuuden välillä, johon taas pyrin paremmin vastaamaan tämän työn kolmannessa luvussa ”Mobiilikäyttöjärjestelmät ja niiden tietoturva”.

Kaiken kaikkiaan kyselyn perusteella on selvää, että käyttäjillä olisi mahdollisuus omilla toimillaan vielä parantaa laitteidensa tietoturvaa, ja mahdollisesti käyttää niiden tietoturvaominaisuuksia tehokkaammin. Siksi jonkinlaisesta mobiilitietoturvaan liittyvästä dokumentaatiosta voisi olla käyttäjille ja viime kädessä koko organisaatiolle hyötyä.

6 PÄÄTÄNTÖ

Tämän opinnäytetyön tekeminen alkoi kesäkuussa 2012 ja asetin tavoitteeksi saada sen valmiiksi marraskuun puoliväliin mennessä. Aikaa toteutukseen oli siis n. viisi kuukautta, joka hyvän lopputuloksen saamiseksi tarkoitti melko tiivistä työskentelytahtia. Aiheen valinta ja rajaus syntyi lopulta melko vaivattomasti, lähinnä omasta kiinnostuksesta älypuhelimiin ja tietoturva-aiheeseen. Työ eteni mutkattomasti omalla painollaan, ja sen edetessä opin myös itse paljon lisää erityisesti eri älypuhelinalustojen tietoturvaominaisuuksista, joten opinnäytetyöprosessi oli myös siinä mielessä mielenkiintoinen ja hyödyllinen kokemus, vaikka itse olenkin jo pitkäaikainen älypuhelinten käyttäjä.

Työn tavoite ja lähtökohta kiteytettynä yhteen virkkeeseen oli siis selvittää, minkälaisia tietoturvauhkia nykyaikaisiin mobiililaitteisiin kohdistuu erityisesti yrityskäytössä ja selvityksen perusteella tutkia ja kehittää keinoja näiden uhkien torjuntaan ja ennaltaehkäisyyn.

Tämä onnistui, ja työn lopputuloksena syntyi työn toimeksiantajalle, Etelä-Savon Tietohallinto Oy:lle mobiilitietoturvadokumentaatio, jossa yhdistyivät lopulta kaikki käsittelemäni asiat. Annoin dokumentaatiolle nimen ”Tietoturvavinkkejä älypuhelinten käyttäjille” ja olen sisällyttänyt sen tämän opinnäytetyön liitteeksi (liite 1). Kaikki tämän työn eri luvuissa esittämäni johtopäätökset ja tulokset tukivat osaltaan dokumentaation syntyä, ja pystyin suunnitellusti yhdistämään kaikki työssä käsitellyt eri osa-alueet yhdeksi selkeäksi kokonaisuudeksi.

Pyrin tekemään dokumentaatiosta mahdollisimman käyttäjäystävällisen ja käytännönläheisen, jotta siitä olisi mahdollisimman paljon konkreettista hyötyä lukijalle, riippumatta siitä onko kyseessä kokenut älypuhelinkäyttäjä vai aloittelija. Sen tarkoituksena on eritoten lisätä lukijan tietoturvatietoisuutta ja antaa vinkkejä siihen, miten älypuhelimen käyttäjä voi omilla toimillaan ylläpitää ja parantaa mobiililaitteensa tietoturvaa. Se sisältää muutamia tietoturvaan yleisesti liittyviä asioita sekä lisäksi erityisesti käyttöjärjestelmäkohtaisia vinkkejä, joiden avulla käyttäjät toivottavasti saavat laitteidensa tietoturvaominaisuuksista enemmän irti. Dokumentaatiossa esitettyjä menetelmiä ei ole kuitenkaan varsinaisesti rajattu pelkästään toimeksiantajan asiakkaille, vaan uskon, että niistä on hyötyä kenelle tahansa nykyaikaisen älypuhelimen tai tabletin käyttäjälle.

Toimeksiantajan edustajat ilmaisivat olevansa lopputulokseen tyytyväisiä. Projektipäällikkö Sanisalon mielestä dokumentaatio oli varsin hyvä ja selkeä. ICT-asiantuntija Koste piti dokumentaatiota erittäin hyvänä, yleismaailmallisena ja kokonaisarvoltaan oleellisena.

Tietoturva, mobiililaitteet ja niiden käyttöjärjestelmät ovat epäilemättä sellaisia aiheita, joita on käsitelty aiemminkin eri opinnäytetöissä ja tutkimuksissa, asiayhteyksiltään joko suoraan tai epäsuorasti toisiinsa liittyen. Tämä opinnäytetyö pyrkii kuitenkin uudistamaan näitä aiheita olemalla ajankohtainen ja konkreettinen. Halusin siis tehdä opinnäytetyön, jossa otetaan huomioon nykyaikaisten mobiilikäyttöjärjestelmien käyttö tämän päivän yritysympäristössä ja tutkitaan, mitkä laitteiden ja käyttöjärjestelmien kehityksen tietoturvalle asettamat vaatimukset konkreettisesti ovat. Jo alusta alkaen minulle oli selvää, että vaikka aihepiiri olikin laaja, niin halusin työn silti olevan järkevä ja koherentti kokonaisuus, eikä tarpeettoman monimutkainen tai epäolennaisuuksiin keskittyvä. Pyrin käyttämään lähteitä monipuolisesti ja vertaillen, jotta sain mielestäni tärkeimmät asiat otettua huomioon mahdollisimman laaja-alaisesti ja riittävän tarkasti, käyttäen kuitenkin tervettä kriittisyyttä lähteiden luotettavuuden suhteen.

Näkisin, että sain opinnäytetyössäni käsiteltyä kaikki mielestäni tärkeimmät asiat ja näin ollen asetetut tavoitteet saavutettiin ja olen myös itse lopputulokseen tyytyväinen. Aina löytyy toki parannettavaakin, ja koska aihepiiri oli melko laaja ja jakautunut, olisi enemmällä ajalla saanut luultavasti aihetta käsiteltyä vielä syvällisemmin, mutta on eri asia, olisiko se vaikuttanut merkittävästi työn lopputulokseen.

Työ on kuitenkin aihepiiriltään sellainen, että siihen liittyvät asiat, kuten mobiililaitteet, niiden tietoturva ja eri mobiilikäyttöjärjestelmät niiden ympärille rakennettuine ekosysteemeineen ovat jatkuvasti kehittyviä ja ajan hermoilla eläviä asioita. Käyttäjämäärä, palveluiden määrä, laitekirjo ja niihin kohdistuvat uhkat jatkanevat edelleen kasvuaan, joka voi merkitä vain sitä, että mobiililaitteiden tietoturva tulee jatkossakin olemaan ajankohtainen ja vakavasti otettava asia.

LÄHTEET

Mika Hakala, Mika Vainio, Olli Vuorinen 2006. Tietoturvallisuuden käsikirja. Suomi: WSOY.

Mika Laaksonen, Tervo Nivasalo, Karri Tomula 2006. Yrityksen tietoturvakäsikirja. Suomi: Edita.

Järvinen, Petteri 2002. Tietoturva & yksityisyys. Suomi: Docendo.

Perrin, Chad 2008. The CIA Triad. Verkkojulkaisu.
http://www.techrepublic.com/blog/security/the-cia-triad/488
Kirjoitettu 30.6.2008. Luettu 10.6.2012

Tietokone-lehti 2008. Tuhansia yrityskännyköitä katoaa vuosittain Suomessa. Verkkojulkaisu.
http://www.tietokone.fi/uutiset/2008/tuhansia_yrityskannykoita_katoaa_vuosittain_suomessa
Kirjoitettu 26.2.2008. Luettu 11.7.2012

Pietarinen, Harri 2011. Älypuhelinten suojaus on retuperällä. Verkkojulkaisu
http://www.digitoday.fi/tietoturva/2011/03/19/lypuhelinten-suojaus-on-retuperalla/20113874/66
Kirjoitettu 18.3.2011. Luettu 11.7.2012

Linnake, Tuomas 2012a. LinkedIn oikeuteen – vaatimuksena viiden miljoonan korvaukset. Verkkojulkaisu. http://www.itviikko.fi/uutiset/2012/06/21/linkedin-oikeuteen--vaatimuksena-viiden-miljoonan-korvaukset/201232028/7
Kirjoitettu 21.6.2012. Luettu 5.10.2012

Valtiovarainministeriö, VAHTI 2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Suomi: Edita.

Valtiovarainministeriö, VAHTI. Julkisen hallinnon ICT, Tietoturvallisuus. Verkkojulkaisu. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp
Luettu 26.7.2012

Valtiovarainministeriö 2011. Johdon tietoturvaopas. Verkkojulkaisu.
https://www.vahtiohje.fi/web/guest/2/2011-johdon-tietoturvaopas
Kirjoitettu 02/2011. Luettu 26.7.2012

Valtiovarainministeriö 2006. Henkilöstön tietoturvaopas. Verkkojulkaisu.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061127Henkil/name.jsp
Kirjoitettu 27.11.2006. Luettu 3.10.2012

Rousku, Kimmo 2012. Johtaja – kanna vastuu ja määritä politiikka. Verkkojulkaisu.
http://www.tietoviikko.fi/blogit/turvasatama/johtaja++kanna+vastuu+ja+maarita+politiikka/a761965
Kirjoitettu 24.1.2012. Luettu 3.10.2012

Jerome H. Saltzer, Michael D. Schroeder 1975. The Protection of Information in Computer Systems. Verkkojulkaisu.
http://www.cs.virginia.edu/~evans/cs551/saltzer/
Luettu 4.10.2012

IDC, Worldwide Mobile Phone Tracker, 6.6 2012. Verkkojulkaisu.
http://www.idc.com/getdoc.jsp?containerId=prUS23523812
Kirjoitettu 6.6.2012. Luettu 3.8.2012.

Dimensional Research, The impact of mobile devices on information security: A survey of IT professionals 2012. Verkkojulkaisu.
http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf
Kirjoitettu 01/2012. Luettu 6.8.2012.

Kantar Worldpanel 2012. Windows makes progress in Europe. Verkkojulkaisu.
http://www.kantarworldpanel.com/global/News/Windows-makes-progress-in-Europe
Kirjoitettu 1.10.2012. Luettu 3.10.2012

Tiera, Kuntien Tiera Oy 2012. Verkkojulkaisu. http://www.tiera.fi/
Luettu 28.8.2012.

Siltala, Tiina 2010. Pilvipalvelujen tietoturva kuntoon. Verkkojulkaisu.
http://www.tietoviikko.fi/edut/pilvi/pilvipalvelujen+tietoturva+kuntoon/a400099
Kirjoitettu 1.6.2010. Luettu 31.8.2012.

Rousku, Kimmo 2010. Mikä ihmeen pilvi? Cloud computingin alkeet peruskäyttäjälle. Verkkojulkaisu.
http://www.tietoviikko.fi/edut/pilvi/mika+ihmeen+pilvi+cloud+computingin+alkeet+peruskayttajalle/a394325
Kirjoitettu 22.4.2010. Luettu 31.8.2012

F-Secure 2012. Mobile threat report Q2 2012. Verkkojulkaisu.
http://www.f-
se-
cure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q2%202012.pdf
Kirjoitettu 6.8.2012. Luettu 3.9.2012

Nokia 2004. Backgrounder – Smartphones. Verkkojulkaisu
http://www.nokia.com/NOKIA_COM_1/About_Nokia/Press/Press_Events/zz_Announcement/smartphonebackgroundersep2004final_final.pdf
Kirjoitettu: 04/2004. Luettu: 4.9.2012

Tietoviikko, 2011. 3 käyttäjää kertoo taulutietokoneestaan. Verkkojulkaisu
http://www.tietoviikko.fi/tablet/3+kayttajaa+kertoo+taulutietokoneestaan/a587465
Kirjoitettu 6.8.2011. Luettu 5.9.2012

Sutter, John D 2010. What is a tablet, anyway? Verkkojulkaisu.
http://articles.cnn.com/2010-01-09/tech/ces.tablet.computers_1_tablet-touch-screen-keyboard?_s=PM:TECH
Kirjoitettu 9.1.2010. Luettu 5.9.2012

Beavis, Gareth 2008. A complete history of Android. Verkkojulkaisu
http://www.techradar.com/news/phone-and-communications/mobile-phones/a-complete-history-of-android-470327
Kirjoitettu 23.9.2008. Luettu 11.9.2012

Reisinger, Don 2011. Smartphone, Tablet Security: 10 Lessons to Learn. Verkkojulkaisu. http://www.eweek.com/c/a/Security/Smartphone-Tablet-Security-10-Lessons-to-Learn-463120/
Kirjoitettu 8.12.2011. Luettu 11.9.2012

Turney, Drew 2011. The best mobile OS: security showdown. Verkkojulkaisu.
http://www.zdnet.com/the-best-mobile-os-security-showdown-1339314044/
Kirjoitettu 23.5.2011. Luettu 12.9.2012

Lehto, Tero 2011. Iso yllätys: Symbian Belle tuo huiman parannuksen. Verkkojulkaisu. http://blogit.tietokone.fi/tietojakoneesta/2011/09/iso-yllatys-symbian-belle-tuo-huiman-parannuksen/
Kirjoitettu 23.9.2011. Luettu 12.9.2012

Google Play 2012. Security on Android. Verkkojulkaisu.
http://support.google.com/googleplay/bin/answer.py?hl=en&answer=1368854
Luettu 12.9.2012.

Kinder, Lucy 2012. Russia snubs Google for Android-style tablet. Verkkojulkaisu.
http://www.telegraph.co.uk/technology/9516850/Russia-snubs-Google-for-Android-style-tablet.html#
Kirjoitettu 3.9.2012. Luettu 12.9.2012

Android 2012a. Android 4.1 Jelly Bean. Verkkojulkaisu
http://www.android.com/about/jelly-bean/
Luettu 3.9.2012

Android.2012b. Introducing Android 4.0. Verkkojulkaisu.
http://www.android.com/about/ice-cream-sandwich/
Luettu 3.9.2012

Scott Thurm, Yukari Iwatani Kane 2010. Your Apps Are Watching You. Verkkojulkaisu.
http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html
Kirjoitettu 17.12.2010. Luettu 13.9.2012

Munchbach, Andrew 2011. Android gathering location data too, researcher develops harvesting tool. Verkkojulkaisu. http://www.bgr.com/2011/04/22/android-gathering-location-data-too-researcher-develops-harvesting-tool/
Kirjoitettu 22.4.2011. Luettu 14.9.2012

Julia Angwin, Jennifer Valentino-Devries 2011. Apple, Google Collect User Data. Verkkojulkaisu.
http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html
Kirjoitettu 22.4.2011. Luettu 14.9.2012.

Bilton, Nick 2012. Aple Loophole Gives Developers Access to Photos. Verkkojulkaisu. http://bits.blogs.nytimes.com/2012/02/28/tk-ios-gives-developers-access-to-photos-videos-location/
Kirjoitettu 28.2.2012. Luettu 17.9.2012

Symantec 2011. A Window Into Mobile Device Security. Verkkojulkaisu.
http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf
Kirjoitettu 06/2011. Luettu 17.9.2012

Apple 2012a. iPhone 5 Tech Specs. Verkkojulkaisu.
http://www.apple.com/iphone/specs.html
Luettu 20.9.2012

Apple 2012b. iOS Security Introduction. Verkkojulkaisu
http://images.apple.com/iphone/business/docs/iOS_Security_Introduction_Mar12.pdf
Luettu 20.9.2012

Polimenov, Anton 2009. WP7: What is Windows Phone 7. Verkkojulkaisu
http://www.silverlightshow.net/items/WP7-What-is-Windows-Phone-7.aspx
Kirjoitettu 10.11.2009. Luettu 20.9.2012

Linnake, Tuomas 2011. F-Secure: Windows Phone -viruksia ei näköpiirissä. Verkkojulkaisu. http://www.digitoday.fi/tietoturva/2011/11/30/f-secure-windows-phone--viruksia-ei-nakopiirissa/201118090/66
Kirjoitettu 30.11.2011. Luettu 24.9.2012

Kravets, David 2012. FBI Can't Crack ANdroid Pattern-Screen Lock. Verkkojulkaisu
http://www.wired.com/threatlevel/2012/03/fbi-android-phone-lock/
Kirjoitettu 14.3.2012. Luettu 24.9.2012.

Meeus, Alan 2012. Windows Phone: Security Deep Dive. Verkkojulkaisu
http://channel9.msdn.com/Events/TechEd/Europe/2012/WPH304
Kirjoitettu 27.6.2012. Luettu 25.9.2012

Windows Phone 2012a. Application Certification Requirements for Windows Phone. Verkkojulkaisu.
http://msdn.microsoft.com/en-us/library/windowsphone/develop/hh184843%28v=vs.92%29.aspx
Kirjoitettu 26.7.2012. Luettu 25.9.2012

Mediati, Nick 2008. Internet Explorer 8 Beta 2: Can It Outfox Firefox?. Verkkojulkaisu. http://www.pcworld.com/article/150385/ie8b2.html
Kirjoitettu 27.8.2008. Luettu 26.9.2012.

Lehto, Tero 2012a. Blackberry tulee viimein Suomeen. Verkkojulkaisu.
http://www.3t.fi/artikkeli/uutiset/teknologia/blackberry_tulee_viimein_suomeen
Kirjoitettu 20.2.2012. Luettu 11.10.2012.

Lehto, Tero 2012b. Windows Phone 8 –julkistus toi yllätyksiä. Verkkojulkaisu.
http://www.3t.fi/artikkeli/blogit/tero_lehto/windows_phone_8_julkistus_toi_yllatyksia
Kirjoitettu 20.6.2012. Luettu 26.9.2012

Windows Phone 2012b. Find a lost phone. Verkkojulkaisu.
http://www.windowsphone.com/en-us/how-to/wp7/basics/find-a-lost-phone
Luettu 26.9.2012

Windows Phone 2012c. Make room on my computer for phone updates. Verkkojulkaisu. http://www.windowsphone.com/en-us/how-to/wp7/basics/make-room-on-your-computer-for-phone-updates
Luettu 17.10.2012

Hyppönen, Mikko 2012. Twitter / mikko: iPhone is 5 years old today. Verkkojulkaisu.
https://twitter.com/mikko/status/218329213420322817
Kirjoitettu 28.6.2012. Luettu 26.9.2012.

Joseph, Chris 2011. iPhone App Approval Process. Verkkojulkaisu
http://www.ehow.com/info_12147582_iphone-app-approval-process.html
Kirjoitettu 17.10.2011. Luettu 26.9.2012.

Alonso-Parrizas, Angel. 2011. Securely deploying Android devices. Verkkojulkaisu
http://www.sans.org/reading_room/whitepapers/sysadmin/securely-deploying-android-devices_33799
Kirjoitettu 22.9.2011. Luettu 26.9.2012.

Apple 2012c. iOS Security. Verkkojulkaisu
http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf
Kirjoitettu 05/2012. Luettu 27.9.2012.

Apple 2012d. iOS: How to back up. Verkkojulkaisu
http://support.apple.com/kb/ht1766
Kirjoitettu 20.8.2012. Luettu 17.10.2012

Apple 2012e. iCloud terms and conditions. Verkkojulkaisu.
http://www.apple.com/legal/icloud/en/terms.html
Kirjoitettu 13.9.2012. Luettu 18.10.2012

Linnake, Tuomas 2012b. iOS6 pyytää laskeutumislupaa iPhoneen. Verkkojulkaisu.
http://www.digitoday.fi/data/2012/09/19/ios-6-pyytaa-laskeutumislupaa-iphoneen/201238155/66
Kirjoitettu 19.9.2012. Luettu 27.9.2012

Whitwam, Ryan 2012. How to properly secure your iPhone or Android device. Verkkojulkaisu. http://www.extremetech.com/computing/116635-how-to-properly-secure-your-iphone-or-android-device/2
Kirjoitettu 2.2.2012. Luettu 27.9.2012

Android 2012. Android 4.1, Jelly Bean. Verkkojulkaisu
http://www.android.com/about/jelly-bean/
Luettu 20.9.2012

Halsey, Mike 2012. How to Secure Windows Phone with a Delayed Password. Verkkojulkaisu. http://www.ghacks.net/2011/10/27/how-to-secure-windows-phone-with-an-delayed-password/
Kirjoitettu 27.10.2011. Luettu 28.9.2012

Leyden, John 2012. Windows Phone 7 ’not fit for big biz … unlike Android, iOS’. Verkkojulkaisu. http://www.theregister.co.uk/2012/04/30/window_mobile_7_security/
Kirjoitettu 30.4.2012. Luettu 28.9.2012

Purcell, Kevin 2012. How to Set a Passcode on Lock Screen of iPhone 5. Verkkojulkaisu. http://www.gottabemobile.com/2012/09/27/how-to-set-a-passcode-on-lock-screen-of-iphone-5/
Kirjoitettu: 27.9.2012. Luettu 1.10.2012

Vaknin, Sharon 2011. How to back up your Android phone. Verkkojulkaisu. https://play.google.com/store/apps/details?id=com.rerware.android.MyBackupPro Kirjoitettu 15.4.2011. Luettu 1.10.2012

Hamburger, Ellis. 2011. Here's The More Serious iPhone Security Problem Facing many Users. Verkkojulkaisu. http://www.businessinsider.com/find-my-iphone-2011-10?op=1
Kirjoitettu 20.10.2011 Luettu 18.10.2012

Cipriani, Jason 2012a. How to use Google Drive on Android. Verkkojulkaisu. http://howto.cnet.com/8301-11310_39-57420195-285/how-to-use-google-drive-on-android/
Kirjoitettu 24.4.2012. Luettu 1.10.2012

Duffy, Jill 2011. Optimize iCloud for iPhone in 6 Simple Steps. Verkkojulkaisu http://www.pcmag.com/article2/0,2817,2394702,00.asp
Kirjoitettu 14.10.2011. Luettu 1.10.2012

Van Wyk, Kenneth 2012. Shutting down security gotchas in iOS 6. Verkkojulkaisu. http://www.computerworld.com/s/article/9231627/Kenneth_van_Wyk_Shutting_down_security_gotchas_in_iOS_6?taxonomyId=17&pageNumber=1
Kirjoitettu 24.9.2012. Luettu 1.10.2012

Microsoft 2010. Windows Phone 7 and Microsoft Exchange Server. Verkkojulkaisu. http://www.abc-computers.com/wp-content/uploads/2010/12/Windows_7_Phone_and_Exchange_DataSheet.pdf
Kirjoitettu 2010. Luettu 17.10.2012

Edmonds, Rich 2012. Making the most of cloud storage with SkyDrive on your Windows Phone. Verkkojulkaisu.
http://www.wpcentral.com/making-most-cloud-storage-skydrive
Kirjoitettu 10.5.2012. Luettu 1.10.2012

Cipriani, Jason 2012b. How to control your privacy settings on iOS6. Verkkojulkaisu. http://howto.cnet.com/8301-11310_39-57507698-285/how-to-control-your-privacy-settings-on-ios-6/
Kirjoitettu 19.9.2012. Luettu 18.10.2012

Bo Li, Elena Reshetova, Tuomas Aura 2010. Symbian Os Platform Security Model. Verkkojulkaisu. http://c59951.r51.cf2.rackcdn.com/5678-73507-li.pdf
Kirjoitettu 08/2010. Luettu 2.10.2012

Nokia 2012a. Nokia Belle – Suojaa tietosi. Verkkojulkaisu. http://www.nokia.com/fi-fi/tuotteet/nokia-for-business/nokia-belle/security/symbian-security/
Luettu 3.10.2012

Nokia 2012b. Nokia 808 Pureview -käyttöohje. Verkkojulkaisu. http://download.fds-ncom.nokia.com/supportFiles/phones/files/pdf_guides/devices/808/Nokia_808_UG_fi_FI.pdf
Luettu 11.10.2012

Vinu, Thomas 2009. Remote phone lock for your N97. Verkkojulkaisu. http://myportableworld.com/posts/remote-phone-lock-for-your-n97/
Kirjoitettu 27.8.2009. Luettu 4.10.2012

Lehtiniitty, Markus 2008. Nokian Ovi Sync –synkronointipalvelu avautui. Verkkojulkaisu. http://www.puhelinvertailu.com/uutiset.cfm/2008/08/28/nokian_ovi_sync_synkronointipalvelu_avautui
Kirjoitettu 28.8.2008. Luettu 4.10.2012

Makwana, Samir 2012. How to Backup contacts using Nokia Suite. Verkkojulkaisu. http://www.themobileindian.com/news/8403_How-to-Backup-contacts-using-Nokia-Suite
Kirjoitettu 17.9.2012. Luettu 4.10.2012

McAfee Labs 2012. McAfee Threats Report: First Quarter 2012. Verkkojulkaisu. www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf
Kirjoitettu 23.5.2012. Luettu 11.10.2012

Tilastokeskus 2012. 1.4 Kvantitatiivinen ja kvalitatiivinen tutkimus. Verkkojulkaisu. http://www.stat.fi/tup/verkkokoulu/data/tt/01/04/index.html
Luettu 17.10.2012

Taylor, Kate 2012. Where you (probably) lost your phone. Verkkojulkaisu. http://www.tgdaily.com/mobility-features/62272-where-you-probably-lost-your-phone
Kirjoitettu 23.3.2012. Luettu 18.10.2012

Prince, Brian 2009. Nokia Ovi Store Lays Out Security Policy for Third-Party Apps. Verkkojulkaisu. http://www.eweek.com/c/a/Security/Nokia-Ovi-Store-Lays-Out-Security-Policy-for-ThirdParty-Apps-348402/
Kirjoitettu 26.5.2009. Luettu 18.10.2012

Lookout Mobile Security 2012a. Mobile Lost & Found. Verkkojulkaisu. https://www.lookout.com/resources/reports/mobile-lost-and-found/billion-dollar-phone-bill
Kirjoitettu 2012. Luettu 18.10.2012

Lookout Mobile Security 2012b. State of Mobile Security 2012. Verkkojulkaisu. https://www.lookout.com/_downloads/lookout-state-of-mobile-security-2012.pdf
Kirjoitettu 2012. Luettu 18.10.2012

Viestintävirasto 2007. Haittaohjelmat. Verkkojulkaisu. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/haittaohjelmat.html
Kirjoitettu 24.9.2007. Luettu 18.10.2012

Bonetti, Pino 2012. Benchmarking mobile maps. Verkkojulkaisu. http://conversations.nokia.com/2012/09/20/benchmarking-mobile-maps/
Kirjoitettu 20.9.2012. Luettu 18.10.2012

Google 2012. Fiksun salasanan valinta. Verkkojulkaisu.
http://support.google.com/accounts/bin/answer.py?hl=fi&answer=32040
Luettu 29.10.2012

Mills, Elinor 2012. iOS 6 allows tweets, Facebook posts from locked device. Verkkojulkaisu. http://news.cnet.com/8301-1009_3-57517364-83/ios-6-allows-tweets-facebook-posts-from-locked-device/
Kirjoitettu 20.9.2012. Luettu 1.11.2012

Sadun, Erica 2012. Updating to iOS6: Using over-the-air update. Verkkojulkaisu.
http://www.tuaw.com/2012/09/19/updating-to-ios-6-using-over-the-air-update/
Kirjoitettu 19.9.2012. Luettu 1.11.2012

Cunningham, Andrew 2012. What happened to the Android Update Alliance? Verkkojulkaisu. http://arstechnica.com/gadgets/2012/06/what-happened-to-the-android-update-alliance/
Kirjoitettu 28.6.2012. Luettu 1.11.2012

Sams, Brad 2012. Windows Phone 8 updates to be OTA, 18 month support guaranteed. Verkkojulkaisu. http://www.neowin.net/news/windows-phone-8-updates-to-be-ota-18-month-support-guaranteed
Kirjoitettu 20.6.2012. Luettu 1.11.2012

F-Secure 2009. Put Your Passwords on a Post-It. Verkkojulkaisu. http://www.f-secure.com/weblog/archives/00001691.html
Kirjoitettu 26.5.2009. Luettu 11.11.2012

M&M 2012. Ruotsissa tabletti on jo työkäytössä – suomalainen sinnittelee vielä älypuhelimella. Verkkojulkaisu.
http://www.marmai.fi/uutiset/ruotsissa+tabletti+on+jo+tyokaytossa++suomalainen+sinnittelee+viela+alypuhelimella/a2154294
Kirjoitettu 7.11.2012. Luettu 10.11.2012

Tietoturvavinkkejä älypuhelinten käyttäjille

Tämän ohjeen tarkoituksena on antaa vinkkejä siihen, miten älypuhelimen käyttäjä voi omilla toimillaan ylläpitää ja parantaa laitteensa tietoturvaa. Se sisältää muutamia tietoturvaan yleisesti liittyviä asioita, sekä lisäksi erityisesti laitekohtaisia vinkkejä, joilla saat laitteesi tietoturvaominaisuuksista toivottavasti enemmän irti.

Mihin tietoturvalla pyritään?

Kun puhutaan tietoturvasta, lähdetään yleensä liikkeelle siitä oletuksesta, että tieto on tärkeää omaisuutta, jota halutaan suojella pitämällä se luotettavana, käytettävänä, oikeassa muodossa olevana ja vain siihen oikeutettujen henkilöiden saatavana. Tietoturvatoimenpiteillä tähdätään siis tiedon suojelemiseen, jotta siihen mahdollisesti kohdistuvat uhat eivät aiheuttaisi merkittävää riskiä yksilölle tai yhteisölle.

Miten tietoturva liittyy älypuhelimiin?

Älypuhelimia kehitetään yhä monipuolisemmiksi ja suorituskykyisemmiksi, jotta niillä voitaisiin hoitaa yhä enemmän asioita, jotka ennen on totuttu tekemään lähinnä työasemilla. Tämä tekee älypuhelinten tietoturvasta merkittävän ja ajankohtaisen asian, johon kannattaa kiinnittää huomiota, sillä älypuhelimet sisältävät usein suuren määrän yritykselle tärkeitä luottamuksellisia tietoja. Näiden tietojen hukkuminen, tuhoutuminen tai joutuminen vääriin käsiin, joko tahallisesti tai tahattomasti, vaarantaa yrityksen tietoturvan. Uhkia tulee lisää päivä päivältä, joten myös suojautumiskeinojen tulisi olla ajan tasalla.

Miten voin vaikuttaa tietoturvaan?

On sanottu, että organisaatio on niin terve ja hyvinvoiva, kuin kaikki sen yhdessä kokevat ja tietoturva on osa organisaation asennetta ja kulttuuria, joka on läsnä kaikkialla. Siksi siitä tulisikin huolehtia kaikkien yhteisesti.

Kannattaa muistaa erityisesti seuraavat asiat:

- Pidä henkilökohtaiset käyttäjätunnukset ja salasanat ulkopuolisten ulottumattomissa
- Älä säilytä luottamuksellista aineistoa paikoissa, joissa ne ovat helposti ulkopuolisten saatavilla
- Pyri suojaamaan laitteesi näyttö ulkopuolisten katseilta, kun käsittelet niillä arkaluontoista tietoa
- Älä anna laitteitasi ulkopuolisten käyttöön
- Harkitse millaisia tietoja haluat laitteessasi säilyttää ja käsitellä
- Epäselvissä tilanteissa, ota yhteys organisaatiosi IT-tukeen

Tietoturvavinkkejä älypuhelinten käyttäjille

Käytä vahvaa salasanaa

Käyttäessäsi laitteellasi kirjautumista vaativia palveluita ja sovelluksia, suosi salasanaa, joka on vähintään 8 merkkiä pitkä ja sisältää mahdollisimman monta erilaista merkkiä kuten:

- pieniä ja ISOJA kirjaimia
- numeroita
- symboleja ja erikoismerkkejä, kuten # $! @

On myös suositeltavaa käyttää eri palveluissa ja eri tileissä eri salasanaa. Tämä onnistuu vaivattomimmin lisäämällä salasanaan jokin palvelukohtainen yksilöivä ilmaus. Esim. käyttäessäsi Facebook-yhteisöpalvelua, voit sisällyttää salasanan yhteyteen vaikkapa ilmauksen FB.

Esimerkkisalasana: **At3s!7V8** (perusosa)

Esimerkkisalasana Facebook-palvelussa: **At3s!7V8FB** (perusosa + yksilöivä ilmaus)

Mikäli epäilet, että salasanasi on paljastunut ulkopuolisille, kannattaa se vaihtaa välittömästi uuteen.

Varmuuskopioi säännöllisesti

Aina on mahdollista, että laite katoaa, hajoaa tai sen sisältämät tiedot menetetään esimerkiksi huolimattomuuden johdosta. Kaikki ei ole kuitenkaan menetetty, mikäli laitteen sisältämien tietojen varmuuskopioinnista on huolehdittu. Onkin sanottu, että varmuuskopiointi on kuin palovakuutus, eli siitä ei ole mitään hyötyä enää sen jälkeen, jos talo on jo palanut, eli tässä tapauksessa tärkeät tiedot menetetty. Kaikki nykyaikaiset älypuhelimet tukevat vakiona jonkinasteista varmuuskopiointia ja useimmissa laitteissa se onnistuu myös automaattisesti verkon yli.

Vältä epämääräisten sovellusten asentamista

Älypuhelimille tehdyt haittaohjelmat ovat nykyään jo varsin yleisiä ja ne voivat aiheuttaa monenlaista riesaa käyttäjälle. Monet sovellukset voivat urkkia käyttäjän henkilökohtaisia, laitteeseen tallennettuja tietoja tai sijaintitietoja ja lähettää niitä eteenpäin kolmansille osapuolille. Vakavimmillaan haittaohjelmat pystyvät jopa aiheuttamaan rahallisia kustannuksia, sillä jotkut niistä voivat käyttäjän tietämättä soittaa tai lähettää viestejä maksullisiin palveluihin, jotka laskutetaan käyttäjältä operaattorin puhelinlaskussa.

Haittaohjelman voi laitteeseensa saada esimerkiksi sovelluskaupasta ladatun sovelluksen kylkiäisenä. Tämän vuoksi kannattaa olla erityisen tarkka millaisia sovelluksia laitteeseensa asentaa ja välttää asentamasta suotta sovelluksia, joita ei tarvitse.

Tietoturvavinkkejä älypuhelinten käyttäjille

Harkitse salasanasuojattua näyttölukitusta

Mikäli laitteessasi ei ole käytössä salasanasuojattua näyttölukitusta, on kenen tahansa mahdollista käyttää ja selata laitteen sisältämiä tietoja huomaamattasi. Näin voi käydä erityisesti, mikäli unohdat tai kadotat laitteesi johonkin tai se varastetaan.

Estääksesi muita käyttämästä laitettasi luvatta, voit määrittää laitteen asetuksista sille salasanan ja asettaa sen lukkiutumaan halutun joutenoloajan jälkeen, jolloin laite pyytää aina käyttäjän salasanaa näyttölukitusta avattaessa. Tämän ikävänä puolena on kuitenkin se, että jos salasanan kyselyvälin asettaa varsin lyhyeksi, on laitteen käyttö vaivalloisempaa, kun salasanaa joutuu syöttämään jatkuvasti. Siksi kannattaakin kokeilla mikä on itselle sopiva aikaväli, jotta salasanan syöttö ei häiritse liikaa laitteen käyttöä, mutta suojaa kuitenkin luvattomalta käytöltä. Kaikista nykyaikaisista älypuhelimista löytyy vakiona näyttölukitustoiminto.

Pidä laitteesi käyttöjärjestelmä ajan tasalla

Käyttämällä uusinta saatavilla olevaa käyttöjärjestelmän ohjelmistoversiota varmistat, että laite sisältää kaikki uusimmat parannukset ja korjaukset mm. mahdollisten tietoturvahaavoittuvuuksien osalta. Kaikissa nykyaikaisissa älypuhelimissa on mahdollisuus päivittää laitteen ohjelmisto uusimpaan versioon langattomasti verkon yli.

Ennen käyttöjärjestelmäpäivityksen asentamista kannattaa vielä varmistaa, että olet tehnyt varmuuskopion kaikesta laitteen tärkeästä sisällöstä, sillä riippuen laitteesta, päivitys saattaa vaatia laitteen palautuksen tehdasasetuksiin.

Joitakin laitekohtaisia vinkkejä

Oheen on koottu muutamia laitekohtaisia käytännön vinkkejä ja toimia, joilla voit parantaa laitteesi tietoturvaa. Ominaisuuksissa on kuitenkin eroja eri laitteiden ja käyttöjärjestelmäversioiden välillä, joten mikäli tarvitset tarkempia ohjeita tässä ohjeessa esiteltyjen vinkkien toteuttamiseen, löydät lisätietoa laitteesi käyttöoppaasta.

Ohjeessa on huomioitu seuraavia käyttöjärjestelmiä käyttävät laitteet:

- **Symbian** (mm. Nokia C-, E- ja N-sarjan mallit)
- **Windows Phone** (mm. Nokia Lumia – mallit ja Samsung Omnia –mallit)
- **iOS** (mm. Apple iPhone 3GS, 4, 4S, 5)
- **Android** (mm. Samsung Galaxy – mallit, HTC One – mallit ja ZTE Blade –mallit)

Tietoturvavinkkejä älypuhelinten käyttäjille

Symbian

Varmuuskopiointi: Symbian-laitteiden sisällön, kuten yhteystietojen, viestien, kalenterin, kuvien ja kaikkien tallennettujen dokumenttien täydellinen varmuuskopiointi onnistuu yhdistämällä laite tietokoneeseen USB-kaapelilla ja käyttämällä Nokia Suite- tai Ovi Suite -ohjelmistoa, puhelinmallista riippuen. Tällä tavoin laitteeseen tallennettu tärkeä sisältö pysyy tallessa, vaikka itse laite hukkuisi tai hajoaisi.

Tietojen salaus: Uusimmissa Symbian-laitteissa on mahdollisuus salata laitteen sisältämät tiedot, joka tarkoittaa sitä, että mikäli laite joutuu vääriin käsiin, ei sen sisältämiä henkilökohtaisia tietoja päästä selaamaan ilman oikean salasanan syöttämistä. Salauksen voi ottaa käyttöön laitteen asetuksista ja salata voi sekä sisäisessä muistissa, että muistikortilla olevan sisällön.

Windows Phone

Varmuuskopiointi: Windows Phone-laitteista löytyy vakiona Skydrive -palvelu, joka varmuuskopioi käyttäjän yhteystiedot, sähköpostin, kalenterin, kuvat, sekä mm. Office-dokumentit automaattisesti verkon yli, sitä mukaa kun uutta sisältöä laitteeseen tallennetaan. Skydrive-varmuuskopiointi voidaan määrittää sovelluskohtaisesti kunkin sovelluksen asetuksista. Skydrive ei kuitenkaan ole läsnä kaikissa sovelluksissa, joten on suositeltavaa myös tehdä laitteen sisällöstä täydellinen varmuuskopio kytkemällä laite tietokoneeseen USB-kaapelilla ja käyttämällä Microsoftin Zune-ohjelmiston varmuuskopiointitoimintoa.

Kadonneen laitteen paikantaminen: Mikäli Windows Phone-laite katoaa, on laite mahdollista paikantaa windowsphone.com-sivuston kautta, kirjautumalla sivustolle samalla käyttäjätilillä, jota laitteessa on käytetty. Sivuston kautta on mahdollista paikantaa laite kartalla, soittaa laitteeseen, sekä etälukita tai etätyhjentää laite, jotta ulkopuoliset eivät pääsisi käsiksi sen sisältämiin tietoihin.

iOS

Aakkosnumeerinen salasana: iOS-laitteet käyttävät oletuksena vain neljästä numerosta koostuvaa suojakoodia, mutta sen voi laitteen asetuksista vaihtaa myös pidemmäksi salasanaksi, joka sisältää kirjaimia ja numeroita. Paremman tietoturvan vuoksi kannattaa ehdottomasti harkita suojakoodin vaihtamista aakkosnumeeriseksi laitteen lukitusasetuksista. Lisäksi voidaan määrittää kuinka monta epäonnistunutta salasanansyöttöyritystä vaaditaan, ennen kuin laite tyhjentää kaikki käyttäjän tiedot sisäisestä muististaan.

Puheohjaus laitteen ollessa lukittu: Uusimmat iOS-laitteet sisältävät Siri-puheohjausominaisuuden, jonka avulla laitetta voidaan käyttää antamalla sille puhekomentoja. Tämä mahdollistaa sen, että kuka tahansa voi antaa laitteelle puhekomentoja, ilman salasanan syöttämistä tai edes laitteeseen koskemista. Sirin kautta kenen tahansa on mahdollista kysyä laitteelta esimerkiksi käyttäjän kalenteriin merkittyjä tapaamisia tai lähettää viestejä sosiaaliseen mediaan, kuten Twitteriin ja Facebookiin laitteen käyttäjän nimissä. Tämän vuoksi kannattaa harkita, haluaako Sirin olevan käytettävissä laitteen ollessa lukittu. Ominaisuuden saa pois päältä laitteen tietoturva-asetuksista.

Varmuuskopiointi: iOS-laitteista löytyy vakiona iCloud-palvelu, joka varmuuskopioi kaikki laitteen tiedot automaattisesti verkon yli sitä mukaa kun uutta sisältöä laitteeseen tallennetaan. Laite kysyy käyttäjältä

palvelun käyttöönottoa ensimmäisen käynnistyskerran yhteydessä, mutta jos sitä ei ole vielä tällöin otettu käyttöön, voidaan se kytkeä myöhemmin päälle myös laitteen asetuksista. Asetuksista voidaan myös määritellä halutaanko palvelun varmuuskopioivan kaiken laitteen sisällön vai vain pelkästään tietyt asiat. Varmuuskopion laitteen sisällöstä voi myös tehdä paikalliselle tietokoneelle, kytkemällä laitteen tietokoneeseen USB-kaapelilla ja käyttämällä Applen iTunes-ohjelmiston varmuuskopiointitoimintoa.

Android

Lukituksenpoistokuvio: Android-laitteiden näyttölukituksessa voidaan käyttää salasanasuojauksen sijasta myös ns. lukituksenpoistokuviota, joka on helppo ja nopea, mutta silti turvallinen tapa lukita laite. Lukituksenpoistokuvio on yhdeksästä pisteestä koostuva matriisi, johon käyttäjä voi määrittää vähintään neljän pisteen kautta kulkevan, yhtenäisen kuvion, jonka piirtämällä laite avaa näyttölukituksen. Se löytyy laitteen suojausasetuksista.

Tietojen salaus: Uusimmissa Android-laitteissa on mahdollisuus salata laitteen sisäisessä muistissa olevat tiedot, joka tarkoittaa sitä, että mikäli laite joutuu vääriin käsiin, ei sen sisältämiä henkilökohtaisia tietoja päästä selaamaan ilman oikean salasanan syöttämistä. Laitteen muistikortille tallennettuja tietoja ei kuitenkaan ole mahdollista vakiona salata. Salauksen voi asettaa päälle laitteen suojausasetuksista, mutta siihen kannattaa varata aikaa ja laitteen akkuun virtaa, koska salaus saattaa kestää pitkään.

Varmuuskopiointi: Android-laitteissa on mahdollisuus varmuuskopioida kaikkien laitteessa käytettävien tilien tiedot automaattisesti verkon yli. Tilit voivat sisältää mm. sähköpostin, kalenterin, kuvat ja yhteystiedot. Valitsemalla laitteen asetuksista "tilit ja synkronointi", on mahdollista määrittää erikseen, mitkä kaikki tiedot käyttäjä haluaa varmuuskopioida. Suurin osa Android-laitteista ei kuitenkaan tarjoa vakiona ohjelmistoa, jolla puhelimen sisällöstä voisi tehdä täydellisen varmuuskopion tietokoneelle, joten tätä varten täytyy hankkia jokin kolmannen osapuolen sovellus Google Play -sovelluskaupasta.

Kyselylomake Etelä-Savon Tietohallinto Oy:n asiakkaille

Kysely älypuhelinten käyttäjille

Hei,

Olen Mikkelin Ammattikorkeakoulun tietojenkäsittelyn opiskelija, ja teen opinnäytetyötäni Etelä-Savon Tietohallinto Oy:lle (Tiera), aiheena mobiililaitteiden tietoturvariskit yritystoiminnassa. Tarkoituksenani on selvittää millaisia uhkia älypuhelimiin yrityskäytössä mahdollisesti kohdistuu, ja miten laitteiden tietoturvaa voitaisiin parantaa entisestään.

Mikäli teillä on hetki aikaa, toivoisin, että vastaisitte alla olevaan käyttötottumuskyselyyn. Tämä kysely koskee vain älypuhelimia ja tabletteja, jotka on toimittanut teille työnantajanne ja joita hallinnoi Etelä-Savon Tietohallinto Oy. Kysely on täysin vapaaehtonen, eikä mitään henkilötietoja kysytä, eikä kerätä. Kyselyyn vastaaminen vie vain hetken ja mitä useampi vastaa, sitä laadukkaampi tutkimus saadaan.

Pääsette kyselyyn klikkaamalla tämän viestin alla olevaa "Vastaa kyselyyn"-painiketta. Kiitän ajastanne!

Emppu Kinnaslampi
Mikkelin Ammattikorkeakoulu
emppu.kinnaslampi@mail.mamk.fi

Vastaa kyselyyn

English summary: I'm a IT-student in Mikkeli University of Applied Sciences and I'm making my thesis for Etelä-Savon Tietohallinto Oy dealing with the subject of mobile security threats in corporate environment. This survey is for smartphone and tablet users only. The survey is completely voluntary and anonymous. Please note that the survey is only in Finnish. If you wish to participate, you can open the survey from the link above. Thank you for your time!

LIITE 2(2).

Kyselylomake Etelä-Savon Tietohallinto Oy:n asiakkaille

Kysely älypuhelinten käyttäjille

1. Älypuhelimesi merkki ja malli:

2. Onko käytössäsi myös taulutietokone eli tabletti?

- ○ Kyllä, mikä?
- ○ Ei

3. Mitä seuraavista palveluista tai sovelluksista käytät mobiililaitteellasi?

- ☐ Työsähköposti
- ☐ Vapaa-ajan sähköposti
- ☐ Sosiaalinen media (esim. Facebook, Twitter, Youtube)
- ☐ Pilvitallennuspalvelut (esim. Dropbox, iCloud, Skydrive, Google Docs)
- ☐ Pikaviestimet (esim. eBuddy, WhatsApp, Live Messenger)

4. Kuinka usein olet varmuuskopioinut mobiililaitteesi sisältämät tiedot tietokoneelle jollain ohjelmistolla (esim. PC Suite, Ovi Suite, Activesync)?

- ○ Säännöllisesti
- ○ Harvoin
- ○ En koskaan

5. Käytätkö, tai oletko käyttänyt pääsääntöisesti samaa salasanaa useassa eri palvelussa? (esim. työsähköposti, vapaa-ajan sähköposti, sosiaalinen media, muut verkkopalvelut)

- ○ Kyllä
- ○ En
- ○ En osaa sanoa

6. Oletko koskaan havainnut epäilyttävän sovelluksen mobiililaitteessasi, joka saattaisi mahdollisesti olla haittaohjelma?

Kyselylomake Etelä-Savon Tietohallinto Oy:n asiakkaille

7. Oletko koskaan asentanut mobiililaitteeseesi sovelluksia sovelluskaupasta? (esim. App Store, Android Market/Google Play -kauppa, Nokia Ovi Store, Windows Phone Marketplace)

- ○ Kyllä
- ○ En
- ○ En osaa sanoa

8. Onko mobiililaitteesi koskaan ollut pidemmän aikaa kadoksissa?

- ○ Kyllä, eikä sitä enää löytynyt
- ○ Kyllä, mutta se löytyi myöhemmin
- ○ Ei

9. Asteikolla 1-5, kuinka todennäköisenä pidät, että mobiililaitteeseesi kohdistuisi jokin tietoturvauhka?

	1	2	3	4	5	
Epätodennäköistä	○	○	○	○	○	Todennäköistä

10. Kuinka hyvin nykyinen mobiililaitteesi mielestäsi soveltuu työkäyttöösi?

- ○ Hyvin
- ○ Kohtalaisesti
- ○ Huonosti

11. Voit kirjoittaa tähän mitä puutteita laitteessasi mielestäsi on:

Lähetä