Aleksi Kivelä

TIETOTURVAN YLLÄPITÄMISEN HAASTEET KOTIKONTEKSTISSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Kivelä, Aleksi
Tietoturvan ylläpitämisen haasteet kotikontekstissa
Jyväskylä: Jyväskylän yliopisto, 2016, 25 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Koskelainen, Tiina

Tietoturva on tärkeä aihe, koska internetin käyttäjien määrä kasvaa yhä ja tietoturvauhat eivät ole vähenemässä. Päinvastoin, uusia uhkia havaitaan vuosittain tuhansia. Tietoturvan ylläpitämisessä tärkeä lenkki ohjelmistojen lisäksi on tietojärjestelmän käyttäjä itse. Paraskaan virustentorjunta ei välttämättä pelasta, jos käyttäjä lankeaa kalasteluhyökkäykseen. Tästä syystä tutkielmassa yritetään ymmärtää käyttäjiä, miten he toimivat ja miksi, jotta tietoturvaa voidaan parantaa ja kaikki voivat nauttia turvallisemmasta internetistä tulevaisuudessa. Tässä tutkielmassa huomataan, että iso osa käyttäjistä ei varaudu uhkiin erityisen hyvin ja monet suojakeinot jäävät käyttämättä. Lisäksi käyttäjiltä puuttuu tarvittavat tietotaidot itsensä oikeaoppiseen suojelemiseen eivätkä käyttäjät vaikuta motivoituneilta opiskelemaan tietoturvaa itsenäisesti. Tietoturvakäyttäytymisen teoriat osoittavat, että käyttäytymiseen vaikuttavat tottumukset, suojakeinon kustannukset ja tehokkuus, aiemmat kokemukset, henkilökohtainen vastuuntunto, muiden mielipiteet, itseluottamus, tietoturvauhan vakavuus ja alttius uhalle. Tietoturvan parantamiseksi, kirjallisuudessa on ehdotettu tietoturvaportaalia ja erilaisten psykologisten ilmiöiden ottamista huomioon järjestelmiä ja ohjelmistoja suunnitellessa. Tutkimus on suoritettu kirjallisuuskatsauksena käyttäen enimmäkseen lähteinä tieteellisiä artikkeleita ja konferenssijulkaisuja.

Asiasanat: tietoturva, virustentorjuntaohjelmat, haittaohjelmat, mobiililaitteet, käyttäytyminen

ABSTRACT

Kivelä, Aleksi
Challenges of maintaining information security in home context
Jyväskylä: University of Jyväskylä, 2016, 25 p.
Information Systems, Bachelor's Thesis
Supervisor: Koskelainen, Tiina

Information security is an important subject because the amount of internet users is still growing and the number security threats is not dropping. Quite the opposite. Thousands of new threats are detected each year. Together with software, the user is one important factor in maintaining information security. Even the best security software might not save you if you fall for a phish. For that reason, in this thesis, I will try to understand users, how they act and why, so that information security can be improved and everyone can enjoy safer internet in the future. In this thesis, I find that majority of users do not utilize the safeguards available to them and therefore they are not well prepared against security threats. Users also lack the necessary know-how to protect themselves and users don't seem motivated to educate themselves about information security. Security behavior theories have proven that factors affecting behavior include: habit strength, safeguard costs and effectiveness, previous experiences, personal responsibility, self-efficacy, threat severity and threat susceptibility. To improve information security, a security portal has been suggested and better understanding of psychological theories when developing new systems and software has been called for. This research was conducted by means of literature review and most of the used source material is scientific articles and conference publications.

Keywords: data security, antivirus software, malware, mobile devices, behaviour

KUVIOT

SISÄLLYS

1 JOHDANTO

International Telecommunication Union arvioi, että internetillä on vuoden 2015 loppuun mennessä n. 3,2 miljardia käyttäjää ja luvun uskotaan kasvavan vielä. Täten voidaan todeta, että tietoturva koskettaa todella isoa ihmismassaa. Vuonna 2014 Symantec havaitsi 46 uutta haittaohjelmalajia Android -laitteille, mikä kertoo sen, että uusia hyökkäyskeinoja kehitetään jatkuvasti, jolloin tietoturvan ylläpitäminen on tärkeää. (Symantec Internet Security Threat Report 2015).

Tietoturvaan on monta näkökulmaa, mutta tämä tutkimus on rajattu tietoturvakäyttäytymiseen, koska käyttäytyminen on tärkeä osa tietoturvaa. Tietoturvaohjelmistot eivät voi tehdä juuri mitään, jos käyttäjä itse jää, esimerkiksi kalasteluhyökkäyksen uhriksi. (Hong, 2012). Lisäksi tutkimus on rajattu kotikontekstiin ja kotikäyttäjiin, koska kotikäyttäjiin kohdistuvat ovat yleisiä ja onnistuneet hyökkäykset heikentävät tietoturvaa myös muille internetin käyttäjille. Tämä johtuu siitä, että saastuneet koneet saattavat liittyä bottiverkkoihin, joiden teho kasvaa uusien koneiden myötä. Kotikäyttäjälle käytän seuraavaa määritelmää: Kotikäyttäjä on henkilö, joka käyttää tietojärjestelmiä omaan käyttöönsä työympäristön ulkopuolella. Kotikäyttäjällä on pääsy internetiin ja hän itse vastaa laitteistonsa tietoturvasta. (Kritzinger & von Solms, 2010.). Muut käyttäjät ovat henkilöitä, jotka yhdistävät internetiin työpaikoilla olevien laitteiden kautta. He todennäköisimmin ovat saaneet tietoturvakoulutusta ja heitä koskevat organisaation ohjeistukset ja määräykset tietoturvan suhteen. (Kritzinger & von Solms, 2010.).

Tutkimus toteutettiin kirjallisuuskatsauksena ja tavoitteena oli löytää vastaukset seuraaviin kysymyksiin:

- Millaisia tietoturvauhkia kotikäyttäjät kohtaavat?
- Miten tietoturvauhkia vastaan varaudutaan ja mitkä tekijät henkilön tietoturvakäyttäytymiseen vaikuttavat?
- Millaisia tietoturvauhkia on mobiililaitteilla ja miten käyttäjät varautuvat niihin?

Tutkimuksen lähdemateriaalina käytän enimmäkseen tieteellisiä artikkeleita ja konferenssijulkaisuja. Sen lisäksi käytössä on tietoturva-aiheisia e-kirjoja ja alaan erikoistuneiden organisaatioiden kyselyjä ja tilastoja. Myös organisaatioiden internetsivuilta löytyviä tietoja käytetään hyödyksi. Lähteiden etsimiseen käytin Googlen normaalia hakukonetta ja Googlen Scholar-hakukonetta. Tieteellisten artikkeleiden ja konferenssijulkaisujen julkaisijoiden arviointiin käytin Julkaisufoorumia. Kirjojen ja verkkosivujen arviointi tapahtui silmämääräisesti. Tutkielmassa käytettyjen tieteellisten julkaisijoiden vähimmäisvaatimuksena on pyritty pitämään taso 2 (johtava taso). Kahdestakymmenestä käytetystä tieteellisestä artikkelista tai konferenssijulkaisusta, 14 ansaitsi tason kaksi tai kolme (paras taso).

Tutkimuksessa havaitaan, että käyttäjät kohtaavat moninaisia tietoturvauhkia haittaohjelmista palvelunestohyökkäyksiin – mobiililaitteilla ja tietokoneilla. Iso osa käyttäjistä ei ole kuitenkaan hyvin valmistautunut näitä uhkia kohtaamaan. Joillain käyttäjillä ei ole suojausta laitteessaan lainkaan ja suurella osalla käyttäjistä suojaus on puutteellinen. Käyttäjillä ei ole myöskään tarvittavaa tietotaitoa tehdäkseen oikeita ratkaisuja tietoturvansa suhteen. Huomattavaa on myös se, että käyttäjillä ei vaikuta olevan motivaatiota tietotaitonsa parantamiseen. Tutkielmassa pohditaankin joitain keinoja parantaa käyttäjien tietoturvaosaamista. Parannuskeinoiksi on esitetty tietoturvaportaalia ja parempaa psykologian teorioiden ymmärtämistä järjestelmiä ja ohjelmistoja kehittäessä. Lisäksi tietoturvakäyttäytymiseen vaikuttavia tekijöitä tutkitaan teoreettisten mallien kautta. Lopputuloksena havaitaan, että käyttäytymiseen vaikuttavat: tottumukset, suojakeinon kustannukset ja tehokkuus, aiemmat kokemukset, henkilökohtainen vastuuntunto, muiden mielipiteet, itseluottamus, tietoturvauhan vakavuus ja alttius uhalle.

Tutkielman sisältö on jaettu kahteen päälukuun. Ensimmäisessä luvussa tutkitaan tietokoneilla ja mobiililaitteilla esiintyviä tietoturvauhkia ja näiden uhkien mahdollisia seurauksia käyttäjille. Toisessa luvussa tutkitaan tietoturvakäyttäytymiseen vaikuttavia tekijöitä teorian kautta, käyttäjien tietoisuutta tietoturvaan liittyvissä asioissa, tietoturvakäyttäytymistä mobiililaitteiden sovelluskaupoissa, käyttäjien varautumista uhkiin ja tietoturvan parannusehdotuksia. Viimeinen luku sisältää tulosten yhteenvedon ja pohdintaa tuloksista ja tutkielman sisällöstä.

2 TIETOTURVAUHAT KOTIKÄYTTÄJILLE

Tässä luvussa esitellään ensin tietoturvan perusteita ja sen jälkeen yleisimpiä tietoturvauhkia, joita kotikäyttäjät kohtaavat tietokoneilla ja mobiililaitteilla. Lisäksi luvussa tuodaan esille haittoja, joita tietoturvauhat voivat käyttäjille aiheuttaa.

2.1 Tietoturvauhan määrittely

Tietoturva on tietojärjestelmien luottamuksellisuuden (confidentiality), eheyden (integrity) ja saatavuuden (availability) turvaamista. (Guttmann & Roback, 1995). Eheyden turvaaminen tarkoittaa sitä, että tiedon luvaton muokkaaminen ja tuhoaminen tehdään mahdottomaksi. Saatavuus turvataan varmistamalla nopea ja luotettava pääsy tietoon käsiksi. Luottamuksellisuus tarkoittaa tiedon pitämistä salassa ja yksityisyyden ylläpitämistä. (Stallings & Brown, 2015.). Kotikontekstissa tämä voisi tarkoittaa esimerkiksi sitä, että käyttäjä haluaa varmistaa henkilökohtaisten dokumenttien olevan turvassa luvattomalta muokkaukselta ja tuhoamiselta ja tietokoneen halutaan toimivan riittävän nopeasti. Käyttäjä itse määrittää laitteessaan olevalle datalle, ohjelmistolle ja itse laitteistolle arvon, mikä vaikuttaa tietoturvaan liittyvissä valinnoissa.

Pfleeger, Pfleeger ja Margulies (2015) määrittelevät uhan olevan joukko tilanteita ja olosuhteita, jotka voivat aiheuttaa haittaa. Uhat voidaan jakaa tahattomiin ja tahallisiin uhkiin. Esimerkkeinä tahattomasta uhasta, käyttäjä voi poistaa tiedostoja vahingossa tai laite voi pudota lattialle ja särkyä. Tahalliset uhat ovat niitä, joissa ihminen tietoisesti yrittää aiheuttaa haittaa. Tahallista haitan aiheuttamista kutsutaan hyökkäykseksi. Hyökkäyksiä on kahta tyyppiä: satunnainen hyökkäys ja kohdistettu hyökkäys. Satunnainen hyökkäys voi olla haitallinen koodi nettisivulla, jonka uhriksi voi joutua kuka tahansa. Kohdistetussa hyökkäyksessä pyritään vahingoittamaan esimerkiksi tiettyä konetta tai henkilöä. (Pfleeger ym., 2015.).

Uhkia vastaan käytettään suojakeinoja, jotka voivat olla tekoja, laitteita, käytäntöjä, tekniikoita tai ohjelmistoja. Ne vähentävät uhista, haavoittuvuuksista tai hyökkäyksistä koituvia haittoja tai ilmoittavat niistä, jotta tarvittaviin toimenpiteisiin voidaan ryhtyä. Tietoturvan yhteydessä puhutaan usein myös haavoittuvuuksista, millä tarkoitetaan järjestelmästä löytyvää heikkoutta, jota voidaan käyttää hyväksi ja aiheuttaa sen avulla haittaa. (Pfleeger ym., 2015.). Esimerkiksi järjestelmä ei vahvista käyttäjän henkilöllisyyttä oikein, jolloin dataan voi olla mahdollista tehdä luvattomia muutoksia.

2.2 Tietoturvauhkia kotikäyttäjille

Yksi tietoturvauhkien tyyppi on haitallinen ohjelmakoodi. Haitallista ohjelmakoodia on montaa eri tyyppiä ja jokaisella on omat erityispiirteensä. Virukset, troijalaiset, madot, vakoiluohjelmat ja rootkitit ovat esimerkkejä haitallisesta ohjelmakoodista. Yleisesti haitallista ohjelmakoodia sisältävää ohjelmaa kutsutaan haittaohjelmaksi. Seuraavaksi annan lyhyen kuvauksen yleisimmistä haittaohjelmatyypeistä ja niiden erityispiirteistä. Tiedot on otettu F-Securen ja Symantecin verkkosivuilta.

Virus on haitallinen ohjelma, joka integroi omaa ohjelmakoodiaan toiseen ohjelmaan tai tiedostoon käyttäjän sitä tiedostamatta. Virukset leviävät saastuttamalla muita järjestelmän tiedostoja ja virus yleensä aiheuttaa vahinkoa tiedostoille. Osa viruksista hyökkää tiedostoja kohtaan, toiset laitteen käynnistyssektorille ja jotkin virukset kohdistuvat erilaisiin makro skripteihin. Viruksen erottaa madosta se, että mato pystyy kopioimaan itseään ja leviämään ilman käyttäjän toimia. Troijalaiset ovat tietokoneohjelmia, jotka näyttävät hyödyllisiltä ja aidoilta, mutta ovatkin todellisuudessa haitallisia, jopa tuhoisia. Troijalaiset usein kantavat mukanaan jonkinlaisen haitallisen ominaisuuden. Vakavimmat troijalaiset tuhoavat tai varastavat tiedostoja. Lisäksi ne avaavat takaportin tietokoneeseen, minkä kautta henkilökohtaista ja luottamuksellista dataa voidaan varastaa. Vakoiluohjelmat tekevät sitä, mitä nimen perusteella voi olettaa. Ne asentuvat tietokoneelle käyttäjän luvalla tai ilman sitä ja alkavat kerätä tietoja käyttäjästä. Kerättyyn tietoon voi kuulua esimerkiksi näppäinten painallukset tai vieraillut verkkosivut. Lähes minkälainen tieto tahansa on kerättävissä. Ohjelma lähettää kerättyä tietoa etäkäyttäjälle ja haitallinen vakoiluohjelma voi myös ladata muita haittaohjelmia ja asentaa niitä tietokoneelle. Kaikki haittaohjelmat eivät kuuluu tiettyyn kategoriaan vaan niillä voi olla kykyjä useammasta haittaohjelmatyypistä. Näitä haittaohjelmia kuvaava englannin kielinen termi on blended threat. (How F-Secure classifies threats, The 11 most common computer security threats.).

Toinen tietoturvauhkien tyyppi on tietojenkalastelu. Kalastelussa hyökkääjä yrittää saada itselleen arkaluontoista tietoa uhrilta, tekeytymällä luotettavaksi lähteeksi. (Jagatic, Johnson, Jakobsson & Menczer, 2007). Esimerkiksi hyökkääjä voi lähettää sähköpostin, jossa hän esittää kuuluvansa pankin palvelukseen ja vaatii käyttäjää siirtymään viestissä ilmoitettuun osoitteeseen ja an-

tamaan siellä pankkitunnuksensa. Kalastelutyyppejä on useampia. Yksi niistä on kohdennettu kalastelu, jossa hyökkääjä kerää tietoa kohteestaan etukäteen ja hyödyntää sitä hyökkäyksessä, parantaakseen onnistumismahdollisuuksiaan. (Hong, 2012).

Hyökkäyksiä kohdistetaan myös suoraan selaimiin, koska ne ovat keskeisessä roolissa ihmisten yhdistämisessä internetiin. Lisäksi selaimissa on paljon haavoittuvuuksia, mikä tekee niistä suosittuja hyökkäyksen kohteita. (Pfleeger ym., 2015). Vuonna 2014 suosituimmista selaimista löydettiin 6549 haavoittuvuutta. (Symantec Internet Security Threat Report 2015). Kuten tietojenkalastelussa, hyökkääjät yrittävät saada selaimista arkaluonteista informaatiota kuten salasanoja tai käyttäjätunnuksia.

Kolmas uhka on laitteen menettäminen tai sen rikkoutuminen. Useimpien ihmisten kannettavat tietokoneet ja älypuhelimet sisältävät dataa, jota ei haluta menettää tai sen ei haluta päätyvän vääriin käsiin. Myös itse laitteen menetys aiheuttaa vähintään rahallisen menetyksen. (Stallings & Brown, 2015.).

Neljäs uhka on palvelunestohyökkäys. Sen tarkoituksena on tehdä verkkosivu tai verkkopalvelu saavuttamattomaksi käyttäjälle. Hyökkäykset useimmiten kohdistetaan suuriin yrityksiin, jolloin haitat käyttäjälle ovat melko pienet, mutta myös yksittäiset henkilöt voivat olla palvelunestohyökkäyksen kohteena, esimerkiksi suosittu pelaaja suoratoistopalvelussa. Hyökkäyksen yleinen toteutustapa on hyödyntää saastuneiden koneiden verkostoa, jota ohjataan etänä. Tähän verkkoon kytketyt koneet alkavat pommittaa tiettyä palvelua yhteyspyynnöillä, jolloin palvelun toiminta hidastuu tai lakkaa kokonaan. (The 11 most common computer security threats.).

2.3 Tietoturvauhkia mobiililaitteilla

Haittaohjelmat voivat levitä mobiililaitteilla tekstiviestien, multimediaviestien, bluetooth ja internet yhteyksien avulla. (La Polla, Martinelli & Sgandurra, 2013). La Polla ym. (2013) antavat kolme tyypillistä esimerkkiä mobiilihaittaohjelmista. Ensimmäinen on troijalainen Android älypuhelimille. Kyseinen troijalainen esitti olevansa mediasoitin, joka piti asentaa manuaalisesti ja asennusvaiheessa se kysyi käyttäjältä lupaa lähettää tekstiviestejä. Asennuksen jälkeen, käyttäjän aukaistessa ohjelman, troijalainen alkaa lähettää tekstiviestejä maksulliseen numeroon, jonka kulut käyttäjä joutuu myöhemmin maksamaan puhelinlaskussaan. Toinen esimerkki on Android rootkit, jonka tutkijat kehittivät todistaakseen mitä on mahdollista tehdä haavoittuvuuksia hyödyntämällä. Se aktivoitui, kun puhelimeen soitettiin tietystä numerosta. Rootkit antoi täyden hallinnan laitteeseen mahdollistaen hyökkääjälle tekstiviestien lukemisen, puhelinmaksujen aiheuttamisen ja GPS paikantamisen. (Papatjamasiou & Percoco 2010.). Kolmas haittaohjelma on iSAM, joka on myös tutkijoiden kehittämä haittaohjelma iOS-käyttöjärjestelmälle. Ohjelma pystyy keräämään tietoa, lähettämään haitallisia tekstiviestejä, estämään ohjelmien käynnistämisen, estämään langattomat yhteydet, leviämään muihin laitteisiin ja iSAM on etäohjattavissa.

(Damopoulus, Kambourakis & Gritzalis 2011). Osa haittaohjelmista kykenee taltioimaan videota laitteen kamerasta tai nauhoittamaan ääntä laitteen mikrofonista. Useat haittaohjelmat hyödyntävät käyttäjän tekemiä muutoksia iOS tai Android käyttöjärjestelmään, joilla käyttäjä saa lisää oikeuksia tehdä muutoksia järjestelmään. (La Polla, 2013.).

Perinteisten haittaohjelmien lisäksi, myös mobiililaitteet voidaan liittää bottiverkkoihin, jotka kykenevät palvelunestohyökkäyksiin. Hyökkäyksiä on mahdollista kohdistaa yksittäisiin laitteisiin tai kokonaisiin verkkoihin. Verkkoon kohdistettu hyökkäys ei välttämättä vaadi erityisen isoa laitteiden määrää ja seurauksena voi olla esimerkiksi hätäpuhelupalvelun toiminnan heikentyminen. Yksittäistä laitetta vastaan voidaan tehdä esimerkiksi hyökkäys, jolla pyritään kuluttamaan akku tyhjäksi. (La Polla, 2013.).

Mobiililaitteilla on joitakin tietoturvaan ja haittaohjelmiin liittyviä erityispiirteitä tietokoneisiin verrattuna. La Pollan ym. (2013) mukaan rikollisille rahan tekeminen on helpompaa mobiililaitteilla maksullisista numeroista johtuen. Maksulliset numerot ovat helppoja koska operaattori hoitaa laskutuksen. Tutkimuksen mukaan vuosina 2009-2011, 52 % haittaohjelmista sisälsi toiminnallisuuden maksullisten numeroiden hyödyntämiseen. (Felt, Finifter, Chin, Hanna, Wagner 2011). Samassa tutkimuksessa huomattiin, että haittaohjelmat useimmiten varastavat henkilökohtaista tietoa ja lähettävät roskapostia tekstiviestien muodossa.

Mobiililaitteiden turvaamisessa yksi merkittävä ero ja haaste tietokoneisiin nähden on resurssien vähyys suorituskyvyn ja tehonkulutuksen suhteen. Prosessorin hitaus, keskusmuistin vähyys ja akun kesto rajoittavat mahdollisuuksia perinteisten suojakeinojen tuomiseen mobiililaitteille. Toinen haaste on mobiililaitteiden monissa eri teknologioissa, joiden kautta laitteeseen voi yhdistää ja täten hyökkäysmahdollisuudet ovat monipuoliset.

2.4 Haitat käyttäjälle

Erilaiset uhat voivat aiheuttaa kotikäyttäjälle haittoja pienestä kiusanteosta rahallisiin menetyksiin asti. Jokainen henkilö kokee haitat erilaisella tavalla, koska jokainen määrittää laitteissa olevalle datalle, ohjelmistolle ja komponentille oman arvonsa. (Pfleeger ym., 2015). Seuraavaksi nostan esille esimerkkejä haitoista, joita voi tapahtua, kun tiedon luottamuksellisuus, eheys tai saatavuus menetetään.

Kuten aiemassa luvussa mainittu, luottamuksellisuuden menetys tarkoittaa sitä, että tietoon on päässyt käsiksi henkilö tai ohjelma, jolla ei ole lupaa kyseistä tietoa pitää hallussaan. (Pfleeger ym., 2015). Rikollisten tavoittelemia tietoja identiteettivarkauden tekemiseen ovat nimi, osoite, sosiaaliturvatunnus, pankkikortin numerot, salasanat ja käyttäjätunnukset. (Information Systems and Technology). Yhdysvaltalaisen rikostilastoja tuottavan viraston raportin mukaan arviolta 17,6 miljoonaa yhdysvaltalaista jäi identiteettivarkauden uhriksi vuonna 2014. 14 % uhreista menetti rahaa, joista 51 % menetti yli 100 dolla-

ria. (Harell, 2015). Tietojen menettämisellä voi siis olla merkittävät rahalliset seuraukset yksittäiselle henkilölle. Lisäksi raportissa kerrotaan, että 52 % uhreista selvitti ongelmat vuorokaudessa, mutta joissain tapauksissa selvittely voi kestää kauemmin, mikä voi tuoda mukanaan ahdistusta. Raportin mukaan 10 % tunsi olonsa erittäin ahdistuneeksi rikoksen jälkeen. (Harell, 2015).

Eheys tarkoittaa muun muassa sitä, että tieto on ajan tasalla ja tarkkaa, sitä ei ole muokattu tai tiedon muokkaus on tapahtunut hyväksyttävin keinoin. Yksi tapaus haittaohjelman aiheuttamasta eheyden menetyksestä oli Word ohjelman makro, joka lisäsi englannin kielisiin teksteihin satunnaisesti sanan ”is” jälkeen sanan ”not”, muuttaen täten myönteisiä lauseita kielteisiksi. Ohjelman aiheuttamat haitat ovat helposti kuviteltavissa. (Pfleeger ym., 2015.).

Saatavuudella tarkoitetaan sitä, että pyyntöön vastataan hyväksyttävässä ajassa. (Pfleeger ym., 2015). Esimerkiksi tietokone reagoi näppäimen painallukseen viiveettä ja tiedostot ovat aina käytettävissä. Saatavuuden heikentämiseen erikoistuvat palvelunestohyökkäykset, jotka voivat aiheuttaa käyttökatkoja verkkopalveluihin. Henkilölle aiheutuva haitta määräytyykin sen mukaan, mikä palvelu on kyseessä ja miten tärkeä palvelu on käyttäjälle sillä hetkellä.

3 TIETOTURVAKÄYTTÄYTYMINEN JA -TIETOISUUS KOTIKONTEKSTISSA

Tässä luvussa esitetään ensin teoria tietoturvakäyttäytymiseen vaikuttavista tekijöistä. Sitten tutkitaan tietoturvakäyttäytymistä tietokoneilla ja mobiililaitteilla tutkimustulosten pohjalta. Lopuksi esitetään keinoja suojautua tietoturvauhilta ja ehdotuksia tietoturvakäyttäytymisen parantamiseen.

3.1 Teoria tietoturvakäyttäytymisestä

Liang ja Xue (2009) julkaisivat teorian, joka on luotu usean teorian synteesillä ja sille on annettu nimeksi Technology Threat Avoidance Theory (TTAT). TTAT pyrkii selittämään yksittäisen henkilön tietoturvakäyttäytymistä. Teorian perustana on: Protection motivation theory (PMT), helth belief model ja riskianalyysin tutkimus. Myöhemmin Tsai ym. (2016) testasivat PMT:hen ja TTAT:hen pohjautuvaa teoriaa ja tutkijat totesivat uuden teorian lisäävän selityskykyä viidellätoista prosentilla. Edellisiin teorioihin verrattuna, tähän versioon tuotiin uusia muuttujia, joista käyttäytymiseen vaikuttavia muuttujia oli: aiemmat kokemukset, subjektiiviset näkemykset, tottumusten voimakkuus ja henkilökohtainen vastuu. Seuraavaksi esittelen teorioiden muuttujat, joiden on todettu vaikuttavan tietoturvakäyttäytymiseen.

Technology Threat Avoidance teorian mukaan käyttäjä ensin havaitsee mahdollisten tietoturvauhan ja asettaa sen jälkeen tavoitteen välttää tätä uhkaa. Jos käyttäjä huomaa nykytilanteen olevan liian lähellä uhkakuvaa, hän alkaa toimiin nykytilanteen parantamiseksi, jotta uhka vältetään. Käyttäjä jatkaa toimia, kunnes hän ei tunne olevansa enää uhattu. Tällainen vaaran välttäminen tapahtuu ihmiseltä luonnostaan. (Liang & Xue, 2010.).

Teorian mukaan, käyttäjät käyvät kaksi prosessia läpi: uhan arviointi ja turvautumiskeinojen arviointi. Uhan arviointi prosessissa on kaksi osaa: uhan vaarallisuus (threat severity) ja alttius uhalle (threat susceptibility). Ihmiset arvioivat haittaohjelmia sen pohjalta, miten alttiina he ovat sille ja miten vakava

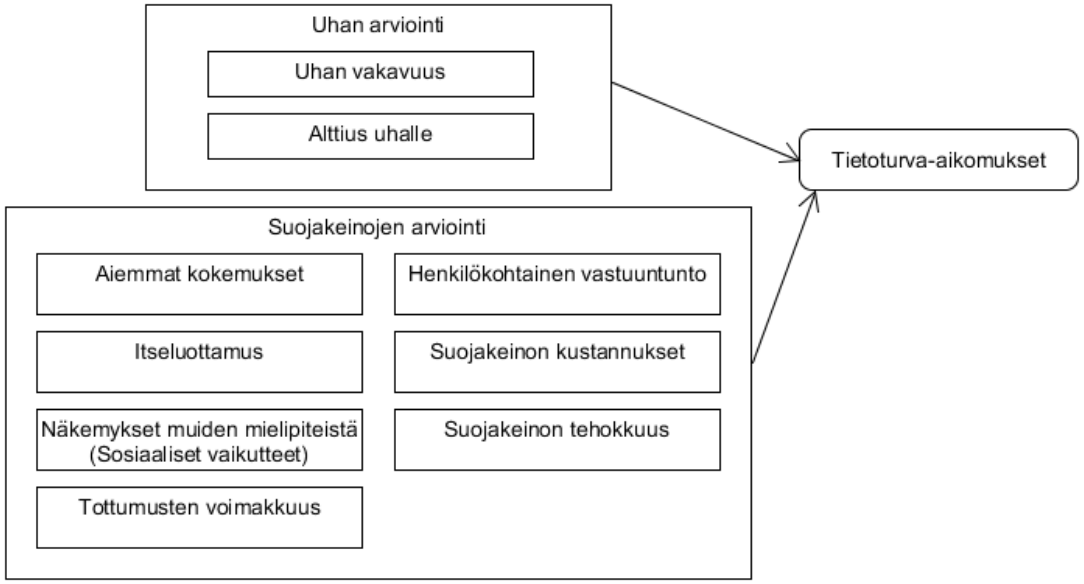
uhka on kyseessä. Ihmisen kokema uhka muodostuu näistä kahdesta asiasta ja jokainen ihminen arvioi uhkia omalla tavallaan. Jos ihminen uskoo, että tietoturvauhalla on olematon riski osua omalle kohdalle, ei hänellä ole motivaatiota toimia tätä uhkaa vastaan. Samoin jos haittaohjelman aiheuttamat haitat hyvin pienet, ei tule tarvetta ehkäistä tätä uhkaa. Esimerkiksi virusta ja mainosohjelmaa vertailtaessa, virus koetaan uhkaavammaksi, koska sen aiheuttamat haitat ovat mainosohjelman pop-up ikkunoiden haittaa suurempi. Käyttäjät siis arvioivat haittaohjelmasta mahdollisesti aiheutuvat haitat ja tähän arvioon perustuen päätetään ryhtyä uhan vastaisiin toimiin, jos siihen on tarvetta. (Liang & Xue, 2010.).

TTAT:n mukaan uhan arviointi tapahtuu aina ennen toimenpiteisiin ryhtymistä, koska vasta uhan todettuaan käyttäjälle muodostuu tunne vaarasta ja halu etsiä turvautumiskeinoja. Vaikka Liang ja Xue (2010) löysivät tutkimuksessaan tukea uhan arviointiprosessin hypoteeseille, Tsai ym. (2016) eivät löytäneet vastaavia todisteita. Toisaalta Vance, Siponen ja Pahnila (2012) tutkivat myös PMT:tä ja he huomasivat, että uhan vaarallisuus vaikutti positiivisesti aikomukseen noudattaa tietoturvasäädöksiä yrityksessä. Tsai ym. (2016) toteavatkin, että heidän tutkimustapansa ei takaa kausaalisuutta ja he ehdottavat jatkotutkimuksissa syvällisempää perehtymistä juuri uhan arvioinnissa vaikuttaviin muuttujiin.

Uhan arvioinnin jälkeen alkaa turvakeinojen arviointiprosessi, jonka tarkoituksena tietoturvauhan välttäminen. Tässä prosessissa tärkeää on arvioida tietyn suojakeinon vaikutusta tiettyyn uhkaan. Esimerkiksi virustentorjuntaohjelmiston vaikutusta virusten uhkaa vastaan. Henkilön mieltämä uhan vältettävyys muodostuu TTAT:ssä kolmesta osasta: kuinka hyvin suojakeinon uskotaan ehkäisevän tietoturvauhkaa (percieved effectiveness), mitkä ovat kustannukset (percieved costs) ja kuinka luottavainen henkilö on omiin kykyihinsä ottaessaan suojakeinon käyttöön (self-efficacy). Suojakienon käyttöönotto vaatii aina käyttäjältä joitain kustannuksia. Suojakeino voi vaatia käyttäjältä esimerkiksi aikaa, rahaa, vaivaa tai osaamista. Nämä vaatimukset voivat luoda esteitä suojakeinon käyttöönotolle silloin kun käyttäjä vertailee suojakeinon hyötyjä siitä koituviin kustannuksiin. Tästä johtuen koetut kustannukset vaikuttavat negatiivisesti suojakeinon arvioituun hyödyllisyyteen. Käyttäjän itseluottamus on vaikuttava muuttuja, koska käyttäjä voi ajatella, että hänen taidot ei riitä suojakeinon hyödyntämiseen, jolloin suojakeinon kustannusten ja tehokkuuden vaikutus ei ole niin suuri. (Liang & Xue, 2010.).

Tsai ym. (2016) lisäsivät suojakeinojen arviointiin luvussa aiemmin mainittuja muuttujia. Tapojen voimakkuus (habit strength) vaikuttaa tietoturvakäyttäytymiseen siten, että henkilö jolla on tapana tehdä turvallisuuta parantavia tekoja, on motivoitunut suojelemaan tietoturvaansa. Mikäli henkilö kokee olevansa vastuussa tietoturvastaan, hän todennäköisemmin käyttää suojakeinoja (personal responsibility). Myös käsitys henkilölle tärkeiden, muiden ihmisten mielipiteistä (subjective norms) vaikuttaa tietoturva-aikomuksiin. Lisäksi henkilön aiemmat kokemukset vaikuttavat. Käyttäjät joilla on aiempaa kokemusta haittaohjelmien torjunnasta, ovat motivoituneempia käyttämään suojakeinoja.

Teorioiden mukaan nämä muuttujat vaikuttavat henkilön tietoturva-aikomuksiin ja lopulta käyttäytymiseen. Seuraavassa kuviossa on koottu tässä luvussa käsiteltyjen teorioiden pohjalta tietoturva-aikomuksiin vaikuttavat tekijät. (kuvio 1).



KUVIO 1 Tietoturva-aikomuksiin vaikuttavat tekijät

TTAT:n mukaan turvautumistapoja on kahta eri tyyppiä: ongelmalähtöinen ja tunnelähtöinen. Ongelmalähtöiseen lähestymistapaan kuuluvat esimerkiksi tietoturvaohjelmistojen asentaminen, salasanan vaihtaminen ja evästeiden kytkeminen pois päältä. Nämä toimet luovat etäisyyttä ei-toivottuun lopputulokseen ja täten turvallisuudentunne lisääntyy. Tunnelähtöinen tapa perustuu siihen, että käyttäjä luo valheellisen kuvan uhasta, jotta negatiiviset tunteet, kuten pelko ja stressi, vähenevät ja itseasiassa mitään konkreettisia toimia ei tehdä. TTAT:n mukaan ihminen valitsee mieluummin tunnelähtöisen lähestymistavan, jos hän ei tunne kontrolloivansa tilannetta tarpeeksi hyvin. Nämä kaksi lähestymistapaa ovat toisiaan vastustavia strategioita eli toisen käyttäminen vähentää tarvetta toiselle. Toisaalta kaikkia tietoturvauhkia ei voi välttää täysin käyttämällä jotain suojakeinoa. Tässä tilanteessa hyödynnetään molempia lähestymistapoja, jotta etäisyys ei-toivottuun lopputilanteeseen saadaan tarpeeksi suureksi. Esimerkiksi jos ihminen tietää, että virustentorjunta ei ole täysin riittävä, hän voi toivoa, että virus ei osu omalle kohdalle tai vaihtoehtoisesti hyväksyä sen, että tietokone jossain vaiheessa saastuu. Teorian mukaan, koetun uhan kasvaessa suuremmaksi, tietoturvauhan välttämisen motivaation kasvu heikkenee. Tämä johtuu siitä, että tunnelähtöistä lähestymistapaa käytettäessä, halu tehdä toimia tietoturvan parantamiseksi ei juuri nouse, vaikka koetun uhan määrä nousisi. Liang ja Xue (2009) viittaavat psykologian tutkimukseen, mikä on osoittanut, että uhan aiheuttaman pelon noustessa tietylle tasolle ihmiset turtuvat pelkotasossa tapahtuville muutoksille. (Liang & Xue, 2010).

Lisäksi TTAT:hen kuuluu riskin sieto ja sosiaaliset vaikuttajat. Tietoturvan kontekstissa riskin sieto tarkoittaa ei-toivotun lopputuloksen ja nykyhetken vähimmäiseroa, jonka käyttäjä sietää. Eli kohdatessaan saman uhan, enemmän riskiä sietävät ihmiset tuntevat olevansa vähemmän uhattuna kuin ne, jotka sietävät riskejä vähemmän. Tutkijat arvelevat, että riskin sieto vaikuttaa negatiivisesti koettuun uhkaan. (Liang & Xue, 2009.).

Kun otetaan huomioon, että yksittäinen käyttäjä voidaan lähes aina liittää johonkin ryhmään, organisaatioon tai yhteisöön, voidaan olettaa muiden ihmisten vaikuttavan päätöksiin myös. (Liang & Xue, 2009). Muilta ihmisiltä voi saada lisää tietoa, mikä on erityisen tärkeää kokemattomille tietokoneiden käyttäjille. Lisäksi ihmisiin kohdistuu painetta yhteisöstä, mikä johtaa siihen, että ihmiset usein haluavat tehdä toimia, jotka ovat sosiaalisesti toivottuja. Tsai ym. (2016) huomasivat, että tietoturvatuen saatavuus ei vaikuttanut aikomukseen parantaa tietoturvaa, mutta käsitys muiden ihmisten mielipiteistä vaikutti.

Liang ja Xue (2010) kiteyttävät tutkimuksensa pohjalta, että käyttäjien motivaatio tietoturvauhkien välttämiseen perustuu uhan havaitsemiseen ja kyseisen uhan vältettävyyteen. Mikäli käyttäjä ei huomaa uhkaa, hän ei ryhdy toimiin. Sama pätee jos uhka on havaittu, mutta ei uskota, että siltä voisi välttyä.

3.2 Käyttäjien tietoisuus ja käyttäytyminen

Furnell, Bryant ja Phippen (2007) suorittivat tutkimuksen Iso-Britanniassa, jossa selvitettiin käyttäjien tietämystä tietoturvaan liittyvissä asioissa. Kyselyyn vastanneet osoittivat ymmärtävänsä suurimman osan tietoturvaan liittyvistä termeistä. Osa käyttäjistä ei kuitenkaan varaudu uhkaan millään tavalla, vaikka osoittaa kyselyssä ymmärtävänsä tietoturvauhat. Furnell ym. (2007) arvelevat, että osa vastaajista ei ymmärrä uhkaa täysin, vaikka niin väittävät tai sitten he eivät pidä uhkaa tarpeeksi varteenotettavana. Vaikka tärkeimmät suojakeinot, kuten virustentorjunta ja palomuuri, olivat yleensä käytössä, vastaajien ymmärrys käytössä olevien suojakeinojen roolista ei ollut erityisen hyvällä tasolla. Neljännes vastaajista ei tiennyt tai ollut varma tietyn suojakeinon roolista.

Tutkimuksessa huomattiin myös se, että vastaajat eivät olleet erityisen hyvin tietoisia sovelluksien, kuten internetselainten, tietoturvaominaisuuksista. Kun kysyttiin vastaajien omia tuntemuksia, kyselyyn vastanneista 63 % uskoi kykenevänsä suojaamaan itsensä huijauksilta internetissä. Tämän joukon ulkopuolelle jää siis merkittävä osuus, joka tuntee olevansa uhattuna. Lisäksi 73 % tunsi olevansa vastuussa omasta tietoturvastaan. Jos käyttäjien oletetaan olevan vastuussa tietoturvastaan, tämän lukeman täytyisi nousta, jotta tietoturva paranisi.

Tietoturvainformaatioon liittyen Furnell ym. (2007) kysyivät myös seuraaviin aiheisiin liittyviä kysymyksiä: mitä käyttäjät tekisivät ongelmatilanteissa, mistä käyttäjät hankkisivat neuvoja ja miten hyvin internetistä löytyvät apusivustot tunnetaan. Vastauksista selvisi, että neuvoja etsitään mieluiten ystäviltä, it-ammattilaisilta tai aihetta käsitteleviltä internetsivuilta. Internetsivujen koh-

dalla huomattiin kuitenkin se, että monet Iso-Britanniassa mainostetut sivustot eivät olleet vastaajille tunnettuja. Vain 33 % vastaajista oli kuullut tunnetuimmasta sivustosta. Tutkijoille herääkin kysymys, mitä lähteitä tiedonhankintaan sitten käytetään, kun valtion panostamat, kotikäyttäjille suunnatut lähteet eivät ole tiedossa. Kun kysyttiin kehen käyttäjä ottaisi yhteyttä hakkerointi tapauksessa, puolet eivät osanneet sanoa, mikä tutkijoiden mukaan vihjaisi siihen, että parempi ohjeistus olisi tarpeen.

Käyttäjien tietoturvatietoisuutta tutki myös Arachchilage ja Love (2014). Heidän tutkimuksensa oli tietojenkalastelulta suojautumisen näkökulmasta. Tutkimuksen tuloksena oli, että tietojenkalastelun uhriksi joutumisen riski kasvaa, kun käyttäjällä ei ole tarpeeksi tietoa. Furnell ym. (2007) huomasivat myös puutteellista tietämystä juuri tietojenkalastelun osalta. Vain 68 % vastanneista tiesi mitä tietojenkalastelu on, kun seuraavaksi pienin osuus oli troijalaisella (83 %). Vaikka tutkimusten välillä on noin seitsemän vuotta aikaa, molemmat toteavat sen, että tietoturvakoulutuksessa on varaa parantaa.

Dhamija, Tygar ja Hearst (2006) tutkivat tietojenkalastelua ja he analysoivat artikkelissaan tietojenkalasteluhyökkäyksissä käytettyjä keinoja. Tutkijat nostavat esille kaksi erilaista tapaa, joilla käyttäjien tiedonpuutetta käytetään hyväksi. Ensimmäinen puute on järjestelmään liittyvissä tiedoissa. Monet käyttäjät eivät tiedä miten käyttöjärjestelmät, ohjelmat, sähköposti ja internet toimivat. Tätä voidaan hyödyntää esimerkiksi käyttämällä URL-osoitetta, joka muistuttaa jollain tavalla aitoa osoitetta, mutta käyttäjä ei sitä osaa erottaa aidosta osoitteesta. Toinen ongelma on turvallisuutta osoittavien vihjeiden huono ymmärrys. Esimerkiksi SSL-yhteyttä kuvaavan riippulukko-symbolin merkitys ei ole kaikille käyttäjille selvää. Kyseinen symbolin oikea paikka on osoiterivillä, mutta hyökkääjät voivat laittaa symbolin myös sivun sisältöön luodakseen vaikutelman luotettavasta sivustosta ja hämätäkseen käyttäjää.

Dhamija, Tygar ja Hearst (2006) suorittivat käyttäjäkokeen, jossa kävi ilmi myös kaksi muuta puutetta käyttäjien tietoturvatietämyksessä. Osa henkilöistä ei tiennyt, että internetissä edes on olemassa huijaussivustoja ja osalla oli virheellisiä käsityksiä siitä, mitkä ovat turvallisen sivuston tunnusmerkkejä. Käyttäjät pitivät hyvinä sivustoja, jotka sisälsivät ammattimaiselta näyttäviä valokuvia, animaatioita ja mainoksia, vaikka näiden asioiden pohjalta ei voi luotettavasti huijaussivustoa erottaa.

Furnell, Tsaganidi, ja Phippen (2008) löysivät haastatteluissaan samoja ongelmia kuten edellisissä tutkimuksissa. Haastateltavat arvioivat olevansa aloittelijoita, mutta aktiivisia internetin käyttäjiä. Haastatteluissa huomattiin, että vastaajat olivat joutuneet haittaohjelmien kanssa tekemisiin, mutta siitä huolimatta he eivät olleet erityisen huolissaan mahdollisista uhista. Vastaajat osoittivat, että he eivät ymmärtäneet mahdollisia seurauksia ja turvallisuuden takaamisen vaadittavia toimenpiteitä. Tässäkään haastattelussa monet vastaajista eivät tienneet, mitä suojakeinoja heillä oli käytössä. Toisessa ääripäässä olivat vastaajat, jotka luottivat liikaa suojakeinojensa riittävyyteen. Haastatteluissa huomattiin, että osa käyttäjistä ei tehnyt mitään täydentääkseen tiedoissaan olevia puutteita, vaikka jotkin asiat olivat epäselviä. Tiedon puutteen vaikutuk-

sen huomasi Wash (2010) haastatteluissaan. Wash huomasi, että palomuuria ei pidetty välttämättömänä, koska palomuurin tehtävää ja hyötyä ei tarkasti tiedetty. Toisaalta kaikki vastaajat tiesivät, että virukset voivat levitä liitetiedostojen avulla ja siksi he uskoivat, että tuntemattomien liitteiden avaamatta jättäminen auttaa torjumaan viruksia. Tämä taas tuo esille sen, miten hyvä tietämys voi auttaa tekemään parempia tietoturvaan liittyviä valintoja.

Tietoturvayhtiö McAfee julkaisi vuonna 2012 raportin, jonka mukaan tietokoneista 17 prosenttia oli täysin suojaamattomia. Tutkimuksessa oli mukana 24 maata ja näistä huonoimmin pärjäsi Singapore, jossa suojaamattomia tietokoneita oli 21.75 % ja parhaiten pärjäsi Suomi, jossa suojaamattomia tietokoneita oli 9.7 %. Tutkimusta varten dataa kerättiin McAfeen Security Scan Plus diagnostiikkaohjelmalla, joka skannasi tietokoneen uhkien varalta ja tarkasti tietokoneen virustentorjunnan ja palomuurin tilanteen. Ohjelma oli ilmainen ja kuluttajat käyttivät sitä vapaaehtoisesti. Maailmanlaajuisesti n. 27-28 miljoonaa skannausta tehtiin kuukausittain.

3.3 Tietoturvakäyttäytyminen mobiililaitteilla

Myös mobiililaitteilla käyttäjien tietoturvaan liittyvät tietotaidot on havaittu puutteellisiksi. Mylonas, Kastania ja Gritzalis (2013) tekivät kyselytutkimuksen, jossa haastateltiin kreikkalaisia mobiililaitteiden käyttäjiä, jotka latasivat sovelluksia puhelimeensa mobiilisovelluskaupasta kuten Google Play. Vastanneista 76 % uskoi sovellusten olevan turvallisia (Mylonas ym., 2013), vaikka todellisuudessa sovellusten turvallisuutta ei ole täysin varmistettu mobiilisovelluskaupoissa. (Mylonas, Tsoumas, Dristas & Gritzalis, 2011). Vastaavia havaintoja tekivät myös Felt ym. (2012) ja Kelley ym. (2012). Kelley ym. (2012) totesivat, että suurin osa käyttäjistä ei ollut huolissaan haittaohjelmista, koska he eivät luottaneet uuteen teknologiaan ja täten eivät uskaltaneet esimerkiksi hoitaa pankkiasioitaan puhelimella, mistä seurasi se, että puhelimen tietoturvaa ei pidetty erityisen tärkeänä. Toinen syy on se, että he luulivat Android sovellusten olevan haittaohjelmien varalta tarkastettuja.

Monien mobiililaitteiden käyttöjärjestelmien turvallisuus perustuu siihen, että käyttäjälle annetaan tarvittava tieto ja käyttäjä tekee sen pohjalta harkitun päätöksen. (Mylonas ym., 2013). Esimerkiksi Androidilla ohjelma voi kysyä käyttäjältä lupaa tiettyihin puhelimen toimintoihin, kuten GPS-paikannukseen tai internetyhteyteen. Felt ym. (2012) toteavat, että sovellusten pyytämiä oikeuksia ei ymmärretä erityisen hyvin. Vain 3 % internetkyselyyn vastanneista ja 24 % laboratoriotutkimukseen osallistuneista tiesi, mitä sovelluksen pyytämät oikeudet tarkoittavat. Kelley ym. (2012) toteavat myös, että käyttäjät eivät ymmärrä termistöä kokonaan, eivätkä he ole lähteneet tätä tietoa itselleen hankkimaan. Käyttäjän tietoturvan kannalta on huono asia, että käyttäjä ei ymmärrä hänelle esitettyä tietoa, mutta tilannetta huonontaa vielä se, että ilmoituksiin ei edes aina kiinnitetä huomiota. Vain 38.6 % luki turvallisuutta koskevat ilmoitukset joka kerta. (Mylonas ym., 2013.) Felt ym. (2012) tekemässä tutkimuksessa

17 % käyttäjistä kiinnitti huomiota lupakyselyihin. Lupakyselyt eivät siis ole yksinään riittäviä suojaamaan käyttäjiä haittaohjelmilta.

Älypuhelinten tietoturvaa parantaakseen käyttäjät eivät ota käyttöön kolmannen osapuolen tietoturvaohjelmistoja, eivätkä käyttäjät pidä näitä ohjelmistoja tärkeinä. 24,5 % käyttää puhelimessaan tietoturvaohjelmistoa, kun vastaava luku tietokoneilla on 85,8 %. Tämän lisäksi puhelimien valmiiksi asennettuja tietoturvaominaisuuksia ei oteta laajalti käyttöön. Käytetyin ominaisuus on salasanalukitus, jota käyttää 64,4 % tutkimukseen vastanneista. Tiedostojen salausta käyttää 22,7 %. Puhelimen etäpaikannusta käyttää 23,1 % ja tietojen etäpoistoa käyttää 15,1 % vastanneista. 27,9 % vastaajista ei käytä mitään edellä mainituista suojakeinoista. Käyttäjät eivät siis varaudu erityisen hyvin haittaohjelmiin tai laitteen menettämiseen. (Mylonas ym., 2013.).

Sovellusten valintaan johtaneet kriteerit edellä mainituissa tutkimuksissa vaihtelivat. Kelley ym. (2012) toteavat, että iso osa käyttäjistä turvautui tähtiluokituksiin, muiden käyttäjien kirjoittamiin arvosteluihin ja muilta kuultuihin kokemuksiin. Myös Felt ym. (2012) tekemässä tutkimuksessa, 88 % vastanneista luki arvosteluja ja 68 % piti arvosteluja tärkeänä. Toisaalta Mylonas ym. (2013) toteavat, että käyttäjistä vain 10 % luki käyttäjäarvosteluita. Lisäksi vain 3.5 % vastaajista piti yksityisyyttä ja turvallisuutta tärkeänä kriteerinä. Sen sijaan ylivoimaisesti tärkeimpänä pidettiin sovelluksen hyödyllisyyttä (58.5 % vastaajista). Hyödyllisyyttä arvostavat käyttäjät todennäköisemmin eivät lukeneet arvosteluja, mikä heikentää tietoturvaa, koska arvosteluissa usein käy ilmi, jos sovelluksessa on tietoturva- tai yksityisyysongelmia. (Mylonas ym. 2013). Syy eroaviin tuloksiin voi olla kulttuurillinen. Kelley ym. ja Felt ym. suorittivat tutkimuksen Yhdysvalloissa, mutta Mylonas ym. suorittivat tutkimuksen Kreikassa.

Virallisten julkaisukanavien lisäksi on mahdollista ladata piraattiohjelmia, joita ladataan epävirallisilta sivustoilta. Vaaralliseksi nämä ohjelmat tekee se, ettei niitä testata. Lisäksi osalla laitteista kyseisten ohjelmien asentamiseksi täytyy kiertää käyttöjärjestelmän suojaus, joka estää piraattiohjelmien asentamisen ja näin yksi suojakerros haittaohjelmia vastaan tulee ohitetuksi. Mylonas ym., (2013) toteavat tutkimuksessaan, että 60.7 % kreikkalaisista tutkimukseen osallistuneista suosi piraattiohjelmia alkuperäisten sijasta. Tämä aiheuttaa suuremman todennäköisyyden joutua haittaohjelman uhriksi. (Mylonas ym., 2013).

Edellä mainittujen tutkimusten loppupäätelmät ovat yhtenevät. Käyttäjillä ei ole riittävää tietotaitoa suojellakseen tietoturvaansa ladatessaan sovelluksia älypuhelimilleen. Lisäksi sovelluskauppojen käyttämät mekanismit tietoturvan parantamiseen eivät ole erityisen tehokkaita, koska käyttäjät sivuuttavat ne tai eivät ymmärrä niiden sanomaa. (Mylonas ym. 2013). Lisäksi oli huomionarvoista, että tietämättömät käyttäjät eivät halunneet tai viitsineet hankkia lisää informaatiota.

3.4 Uhilta suojautuminen ja tietoturvan parannusehdotukset

Kotikäyttäjällä on monia tapoja parantaa tietoturvaansa. Luokittelen suojakeinot ohjelmistoihin ja käyttäytymiseen. Ohjelmistoja haittaohjelmia vastaan on saatavilla ilmaisina ja maksullisina versioina ja niiden tarjoamat toiminallisuudet ovat moninaisia. Tietoturvaohjelmistojen perimmäisenä tarkoituksena on havaita ja poistaa haitallinen ohjelmisto, käyttäen erilaisia tunnistustekniikoita. (Criddle). Useat ohjelmistot tarjoavat esimerkiksi reaaliaikaista haittaohjelmien tunnistusta. Tämän tyyppisten ohjelmistojen lisäksi on mahdollista käyttää palomuuria, joka seuraa ja kontrolloi sisäverkon ja ulkoverkon välistä liikennettä, pyrkien estämään haitallisen liikenteen kulun.

Tietoturvaa voi parantaa myös omalla käyttäytymisellään. Erilaisia tietoturvaa parantavia toimenpiteitä on olemassa lukuisia, mutta tässä kaksi esimerkkiä. Ensimmäiseksi salasanojen käytössä olisi hyvä tapa olla käyttämättä samaa salasanaa useammassa sivustossa. Tällöin salasanan päätyessä vääriin käsiin, ei ole vaarassa menettää useampaa tiliä, jotka ovat saman salasanan takana. Lisäksi salasanan pitäisi olla tarpeeksi monimutkainen, ettei sitä murreta helposti. Toinen tärkeä osa-alue on päivitykset. Ohjelmia ja käyttöjärjestelmiä päivitetään jatkuvasti, jotta tietoturvaongelmia vähennettäisiin, ja siksi parhaan turvallisuuden takaamiseksi ohjelmistojen olisi hyvä olla ajan tasalla. (Abrams, 2004.).

Furnell ym. (2007) tekemä tutkimus osoitti, että 93 % henkilöistä käyttää virustentorjuntaohjelmistoa, 87 % palomuuria, 77% vakoiluohjelmantorjuntaa ja 60 % roskapostintorjuntaa. Suurimmalla osalla oli siis tärkeimmät haittaohjelmien torjuntakeinot käytössä. Kuitenkin näiden sovellusten tehokkuuden takaamiseksi ohjelmistot täytyy pitää päivitettynä. Tutkimuksessa kysyttiin päivittämisen säännöllisyyttä ja 63 % kertoi päivittävänsä virustentorjunnan säännöllisesti, mikä tarkoittaa sitä, että iso osa henkilöistä turvautuu vanhentuneeseen virustietokantaan. Haittaohjelmien torjuntaan tarkoitettuja ohjelmia päivitettiin vielä vähemmän, mikä on itsessään merkittävä haavoittuvuus. (Furnell ym., 2007.). Furnell ym. (2007) huomauttavat, että osa ohjelmistoista päivittyy itsestään, eikä käyttäjä sitä välttämättä tiedosta, jolloin tutkimuksessa saatu lukema saattoi todellisuudessa olla parempi.

Tietoturvan parantamiseksi Kritzinger ja von Solms (2010) ehdottavat tietoturva opastuksen tuomista osaksi kotikäyttäjien internetin käyttöä. Työpaikoilla, joissa internetiä käytetään, työntekijät todennäköisesti saavat jonkin asteista tietoturvakoulutusta ja internetin käyttö voi olla valvonnan alla. Tätä etua kotikäyttäjillä ei ole, vaan he vastaavat turvallisuudestaan suurelta osin itse. Kritzinger ja von Solms haluaisivat tietoturvaopetuksen osaksi internetiin pääsyä ja tätä varten he ehdottavat, että internet-palveluntarjoaja ohjaisi käyttäjät tietoturvaportaaliin, missä käyttäjät saisivat opastusta ja informaatiota.

Pfleeger ja Caputo (2012) analysoivat useiden käyttäytymistutkimusten tulosten ja teorioiden pohjalta asioita, joita pitäisi ottaa huomioon, kun tavoitellaan hyvää tietoturvaa. Ensimmäiseksi tietoturvavaroituksista pitäisi tehdä

käyttäjän kannalta relevantteja, jotta ihmiset kiinnittäisivät niihin huomiota. Huomiota voi lisätä myös pelon avulla, mutta mukana täytyy olla myös ratkaisu pelon tuottavaan ongelmaan. Toisaalta liika pelote voi johtaa fight-or-flight reaktioon, jolloin päätöksiä ei tehdä harkiten. (Elaboration likelihood model). Käyttäjä voi valita parempia tietoturvaratkaisuja, kun mahdolliset negatiiviset vaikutukset tuntuvat abstraktin sijaan konkreettiselta ja henkilökohtaiselta. (Identifiable victim effect). (Pfleeger & Caputo, 2012.).

Kognitiivinen dissonanssi on epämukavuudentunne, joka johtuu tilanteesta, jossa kaksi ristiriidassa olevaa ajatusta on mielessä samaan aikaan. Jotta tietoturvakäyttäytyminen muuttuisi, ihmisten asenteita täytyy muuttaa ensin. Järjestelmä voisi esimerkiksi korostaa käyttäjän tietoturvaa heikentävien toimien hölmöyttä, ja näin saada aikaan dissonanssia. Järjestelmä voi sitten ehdottaa keinoja, joilla tätä dissonanssia voi lievittää käyttäytymistä muuttamalla. Toisaalta ihmiset eivät helposti muuta toimintaansa, ellei toiminnan muuttamiselle ole jotain houkuttelevaa kannustinta. (Status quo bias). (Pfleeger & Caputo, 2012.).

Käyttäjien valintoihin vaikuttaa myös annetun informaation konteksti. Jos valinnat esitetään positiivisessa kontekstissa, käyttäjät todennäköisesti valitsevat sen. Esimerkiksi: palomuuri päästää sisään liikennettä (positiivinen) tai palomuuri estää liikennettä (negatiivinen). Lisäksi ihmiset reagoivat voimakkaammin menetyksiin kuin saatuihin hyötyihin. Esimerkiksi kun jonkin toiminnon kuvataan vähentävän yksityisyyttä, toiminnallisuuden parantamisen sijasta, siihen saatetaan reagoida negatiivisesti. (Framing effects). (Pfleeger & Caputo, 2012.).

Optimisim bias -teorian mukaan ihmisellä on tapana yliarvioida positiivisten tapahtumien todennäköisyyttä ja aliarvioida negatiivisten tapahtumien todennäköisyyttä. Riskiä joutua haittaohjelman kohteeksi aliarvioidaan ja käyttäjät voivat ajatella olevansa immuuneja hyökkäyksille. Tämän takia uhan todennäköisyydet ja mahdolliset vaikutukset pitäisi tuoda käyttäjälle ilmi siten, että uhat pystytään liittämään oikeisiin kokemuksiin. Ihmiset usein myös ajattelevat hallitsevansa lopputulosta paremmin kuin miten he todellisuudessa pystyvät. Esimerkiksi käyttäjä ei välttämättä käytä virusskanneria, koska hän uskoo hallitsevansa tietoturvauhat. (Control bias) (Pfleeger & Caputo, 2012.).

Endownment effect -teorian mukaan ihmisillä on tapana valita jokin näkökulma ja yrittää hankkia tälle näkökulmalle lisää tukea. Tukea hankitaan esimerkiksi kiinnittämällä enemmän huomiota näkökulmaa puoltaviin todisteisiin kuin sitä vastustaviin todisteisiin. Tämä johtaa siihen, että ihmiset eivät ole niin avoimia uusille ideoille kuin he luulevat olevansa. Käyttäjillä voi olla vahva käsitys omasta tietoturvastaan ja tätä käsitystä ei tämän teorian valossa ole helppo muuttaa. Tästä syystä käyttäjiä pitäisi rohkaista muuttamaan käsityksiään antamalla runsaasti todistusaineistoa, jolla vähennettäisiin samalla käyttäjän liiallista itsevarmuutta. (Pfleeger & Caputo, 2012.).

4 YHTEENVETO

Tutkielmassa pyrittiin tuomaan esille erityyppisiä tietoturvauhkia joita kotioloissa kohdataan ja selvitettiin, miten näitä uhkia vastaan varaudutaan ja mitkä seikat henkilön tietoturvakäyttäytymiseen vaikuttavat. Lisäksi tuotiin esille joitain keinoja, joilla tietoturvaa voisi parantaa.

Tutkielmassa selvisi, että yksi merkittävimpiä henkilön puolustuskykyä heikentäviä tekijöitä on käyttäjän tietämys tietoturvasta. Tutkimustulokset olivat sen suhteen yhteneviä. Suurella osalla käyttäjistä ei ole tarvittavaa tietotaitoa tietoturvauhilta varautumiseen. Tästä seurasi käyttäjien jääminen vähäisen suojauksen varaan ja erityisesti tietojenkalastelussa tiedon puutetta pystytään käyttämään hyväksi. Tutkimuksissa huomattiin, että tietotaidoiltaan paremmat käyttäjät hyödyntävät saatavilla olevia suojakeinoja paremmin. Huomattavaa on kuitenkin se, että esittelemissäni teoreettisissa malleissa käyttäjän tietämystä ei otettu huomioon. Tämä johtunee siitä, että tällä hetkellä tutkijoilla ei ole yhtä valmista teoriaa vaan tutkijat pyrkivät kehittämään parempia teorioita jatkuvasti ja yhdessä versiossa ei ole haluttu testata kaikkia mahdollisia muuttujia. Mielenkiintoista olisi nähdä, miten tietämys tietoturvasta voitaisiin implementoida teoreettiseen malliin.

Teoreettisilla malleilla pyritään ennustamaan ja ymmärtämään käyttäjän tekemiä valintoja tietoturvan suhteen. Esittelemissäni teorioissa tuotiin esille monia muuttujia, joiden on todettu vaikuttavan tietoturva-aikomuksiin. Näitä muuttujia ovat: tottumukset, suojakeinon kustannukset ja tehokkuus, aiemmat kokemukset, henkilökohtainen vastuuntunto, muiden mielipiteet, itseluottamus, uhan vakavuus ja alttius uhalle.

Tietoturvauhkiin varaudutaan kohtalaisesti tietokoneilla. 2007 julkaistussa tutkimuksessa 93 % käytti virustentorjuntaa ja 87 % palomuuria. (Furnell ym., 2007) Tilanne oli kuitenkin huonompi 2013, kun McAfeen raportissa 17 % tietokoneista todettiin olevan täysin suojaamattomia. Suomessa vastaava luku oli 9.7 %. Uskon, että nämä lukemat antavat hyvän kuvan tietoturvan nykytilanteesta, koska tutkimus on suhteellisen tuore ja tulokset perustuvat kymmeniin miljooniin skannauksiin. Tämä suojaamattomuus ei pelkästään aiheuta ongel-

mia laitteen omistajalle vaan myös muille internetin käyttäjille, jos suojaamaton kone saastuu ja liittyy bottiverkkoon, mikä tekee palvelunestohyökkäyksiä.

Myös älypuhelimilla on vastaavia tietoturvauhkia, kuten troijalaisia ja muita haittaohjelmia. Älypuhelimissa roskapostia pystyttiin lähettämään tietokoneista poiketen tekstiviesteillä, ja maksullisia numeroita hyödyntäen rikollisen oli helpompi hankkia rahaa tietokoneisiin verrattuna. Mobiilikäyttäjät eivät kuitenkaan varaudu uhkiin erityisen hyvin, sillä älypuhelimissa ei käytetä tietoturvaohjelmistoja tai muita suojakeinoja erityisen laajalti. Mobiilikäyttäjissä huomatiin myös huoletonta ja ymmärtämätöntä käyttäytymistä tutkimuksissa, jotka keskittyivät mobiilisovelluskauppoihin. Monet eivät lue turvallisuutta koskevia varoituksia ja suurin osa ei ymmärrä ohjelmien pyytämiä käyttöoikeuksia. Käyttäjät eivät myöskään tienneet sovelluskauppojen toimintafilosofiaa. Jopa 76 % uskoi sovellusten olevan turvallisia, vaikka sitä ei ole kaupan puolesta varmistettu. (Mylonas ym., 2013). Lisäksi älypuhelimilla käytetään piraattiohjelmia, jotka ovat tietoturvariski jo itsessään.

Kun tietoturvaa halutaan lähteä parantamaan, voidaan tämän tutkielman pohjalta löytää joitain ongelmia, joihin kannattaisi etsiä ratkaisuja. Ensimmäinen ongelma lienee jo siinä, että 17% tietokoneista on suojaamattomia ja älypuhelimien suojakeinoja ei käytetä. Mitkä ovat tähän johtavat syyt ja mitä asialle voisi tehdä? Tämän tutkielman pohjalta voisi päätellä mahdolliseksi syyksi ihmisten tietämättömyyttä, mutta syynä voisi olla myös välinpitämättömyys. Tätä ajatusta tukee, se että käyttäjien ei todettu olevan motivoituneita hankkimaan itselleen lisää tietoa tietoturvasta. Ratkaisu tähän on ihmisten informointi ja motivointi. Yksi käytännön ehdotus ihmisten informointiin on tietoturvaportaali, jonka kautta jokaisen täytyy kulkea päästäkseen internetiin. Toinen tutkielmassa todettu ongelma on mobiilisovelluskauppojen varoitusten tehottomuus. Varoituksista pitäisi saada helpommin omaksuttavia jonkinlaisen opastuksen avulla, koska käyttäjien tiedot eivät riitä varoitusten ymmärtämiseen.

Tätä tutkielmaa rajoittaa tutkimuskysymysten laajuus ja avoimuus. Kun kysymyksiin yrittää vastata kattavasti, ei pysty tämän tekstin puitteissa perehtymään syvällisesti kaikkiin osa-alueisiin. Tutkielmassa käytetyistä lähteistä osa on jo kymmenen vuotta vanhoja, joten tuoreempi tutkimus vastaisi paremmin tämän hetkistä tilannetta. Toisaalta jotkin tietoturvaan liittyvät asiat voivat muuttua hyvin nopeasti, koska kehitystyötä tehdään jatkuvasti, jolloin vain parin vuoden takaiset artikkelitkaan eivät välttämättä pidä täysin paikkansa. Esimerkiksi kun puhutaan sovelluskaupan varoituksista tai toimintatavoista, ne voivat päivittyä milloin tahansa.

Mahdollisista jatkotutkimusaiheista yksi on tietoturvakäyttäytymisen teoriat. Tällä hetkellä teoriat eivät kovin kattavasti pysty selittämään henkilön tietoturvakäyttäytymistä. Parempi ymmärrys tietoturvakäyttäytymisestä voisi jatkossa olla avuksi paremman tietoturvan saavuttamisessa ja siksi sitä kannattaa tutkia. Myös tietoturvakäyttäytymisen parantamiseen keskittyvä tutkimus on perusteltua tämän tutkielman osoittamien puutteiden pohjalta.

LÄHTEET

Abrams, L. (2004, 17. elokuuta). Simple and easy ways to keep your computer safe and secure on the Internet. Haettu 17.6.2016 osoitteesta http://www.bleepingcomputer.com/tutorials/keep-your-computer-safe-online/

Arachchilage, N. A. G. & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

Damopoulos, D., Kambourakis, G. & Gritzalis, S. (2011). iSAM: An iPhone stealth airborne malware. *Future challenges in security and privacy for academia and industry* (s. 17-28) Springer.

Dhamija, R., Tygar, J. D. & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* (581-590). ACM.

Criddle, L. What is Anti-Virus Software? Haettu 17.6.2016 osoitteesta http://www.webroot.com/in/en/home/resources/tips/pc-security/security-what-is-anti-virus-software

Felt, A. P., Finifter, M., Chin, E., Hanna, S. & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices,* (3-14). ACM.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security,* Washington, D.C. (3:1-3:14). New York, NY, USA: ACM.

Furnell, S. M., Bryant, P. & Phippen, A. D. (2007). Assessing the security perceptions of personal internet users. *Computers & Security, 26*(5), 410-417.

Furnell, S., Tsaganidi, V. & Phippen, A. (2008). Security beliefs and barriers for novice internet users. *Computers & Security, 27*(7–8), 235-240.

Guttman, B. & Roback, E. A. (1995). *An introduction to computer security: The NIST handbook.* DIANE Publishing.

Harell, E. (2015, huhtikuu). Victims of Identity Theft, 2014. Haettu 17.6.2016 osoitteesta http://www.bjs.gov/content/pub/pdf/vit14.pdf

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.

How F-Secure classifies threats. Haettu 15.6.2016 osoitteesta https://www.f-secure.com/en/web/labs_global/classification

Information Systems and Technology. Identity Theft. Haettu 17.6.2016 osoitteesta https://ist.mit.edu/security/identity_theft

Jagatic, T. N., Johnson, N. A., Jakobsson, M. & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N. & Wetherall, D. (2012). A conundrum of permissions: Installing applications on an android smartphone. *Financial cryptography and data security* (s. 68-79) Springer.

Kritzinger, E. & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.

La Polla, M., Martinelli, F. & Sgandurra, D. (2013). A survey on security for mobile devices. *Communications Surveys & Tutorials, IEEE, 15*(1), 446-471.

Liang, H. & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly,* 71-90.

Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective*. *Journal of the Association for Information Systems, 11*(7), 394.

McAfee. Consumer Alert: McAfee Finds One in Every Six Personal Computers Have Zero Protection. Haettu 27.5.2016 osoitteesta http://www.mcafee.com/us/about/news/2012/q2/20120530-01.aspx

Mylonas, A., Kastania, A. & Gritzalis, D. (2013). Delegate the smartphone user? security awareness in smartphone platforms. *Computers & Security, 34*, 47-66.

Papathanasiou, C. & Percoco, N. J. (2010). This is not the droid you're looking for... *Def Con, 18*

Pfleeger, C. P., Pfleeger, S. L. & Margulies, J. (2015). *Security in computing* (5. uud. painos). Upper Saddle River, NJ, USA: Prentice Hall Press.

Pfleeger, S. L. & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611.

Stallings, W. & Brown, L. (2015). *Computer security: Principles and practice*. Boston: Pearson.

Symantec Internet Security Threat Report 2015. (2015, huhtikuu). Haettu 27.5.2016 osoitteesta https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

The 11 most common computer security threats. Haettu 27.5.2016 osoitteesta http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J. & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138-150.

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198.

Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security,* (11). ACM.