Ida Koskinen

MITEN TIETOISUUS ÄLYLAITTEIDEN TIETOTURVAUHKISTA VAIKUTTAA ÄLYLAITTEIDEN KÄYTTÖÖN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Koskinen, Ida
Miten tietoisuus älylaitteiden tietoturvauhkista vaikuttaa älylaitteiden käyttöön
Jyväskylä: Jyväskylän yliopisto, 2020, 58s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Makkonen, Pekka

Tämän tutkielman tarkoituksena oli tutkia sitä, miten tietoisuus älylaitteiden tietoturvauhkista vaikuttaa älylaitteiden käyttöön ja tietoturvauhkilta suojautumiseen. Älylaitteet lisääntyvät jatkuvasti esineiden internetin myötä ja nykyään jopa kodinkoneet ovat yhdistettyinä internetiin. Tämän myötä myös tietoturvauhkat voivat kohdistua perinteisten tietokoneiden, älypuhelimien ja tablettien lisäksi myös kodinkoneisiin. Tutkimuksen aluksi toteutettiin kirjallisuuskatsaus siitä, millaisia tietoturvauhkia älylaitteisiin kohdistuu. Tämän pohjalta pystyttiin suunnittelemaan tutkimuksen empiirisen osuuden haastattelu, ja haastatteluun valittiin kirjallisuuden mukaan yleisimmät älylaitteiden tietoturvauhkat. Empiirisen osuuden tutkimus toteutettiin kvalitatiivisena tutkimuksena ja haastattelu puolistrukturoituna haastatteluna. Haastattelussa pyrittiin kartoittamaan haastateltavien tietämystä älylaitteisiin kohdistuvista tietoturvauhkista ja heidän kokemustansa omasta tietoturvastaan. Lisäksi haastattelussa esiteltiin muutama yleisin älylaitteisiin kohdistuva tietoturvauhka ja tarkisteltiin, miten esitellyt uhkat vaikuttivat haastateltavien vastauksiin. Haastateltaviksi valittiin tavallisia älylaitteiden käyttäjiä sekä pari IT-alalla työskentelevää, jotta pystytään vertailemaan vastauksia keskenään. Tutkimuksen tulokset osoittavat, että mitä enemmän käyttäjällä on osaamista ja tietoa uhkista, sitä motivoituneempi hän on suojautumaan erilaisilta uhkilta ja käyttää älylaitteita huolellisemmin. Lisäksi tutkimuksen tuloksista huomattiin se, että mitä enemmän käyttäjällä on tietoa uhkista ja mitä enemmän hän on tehnyt tietoturvaa parantavia toimia, sitä huolestuneempi hän on omasta tietoturvastaan. Sen sijaan käyttäjät, jotka eivät olleet tehneet minkäänlaisia tietoturvaa parantavia toimia, kokivat omat tietonsa parhaiten turvatuiksi, eivätkä näin ollen kokeneet tietoturvaratkaisuita tarpeellisiksi.

Asiasanat: älylaitteet, esineiden internet, tietoturva, tietoturvauhkat, käyttäjien kokemus

ABSTRACT

Koskinen, Ida
How awareness of information security issues in smart devices affects the use of smart devices
Jyväskylä: University of Jyväskylä, 2020, 58 pp.
Information Systems, Master's Thesis
Supervisor: Makkonen, Pekka

The aim of this study was to find out how awareness of information security issues in the internet of things and smart devices affect how devices are used and what actions users have done to improve information security. The number of smart devices is increasing all the time as a result of internet of things. Therefore, not only computers, smart phones and tablets are prone to information security issues, but also household appliances such as fridge and heating system. First step of this study was to write a literature review on what kind of information security issues are there for smart devices. Based on literature review, the interviews could be planned for study's empirical part. The most common information security threats for smart devices were selected for the interviews from literature. The empirical research was implemented as qualitative research and interviews as semi-structured interviews. The aim of the interview was to take a closer look of how much interviewees know about information security threats for smart devices and what are their experiences about their own information security. Furthermore, during the interviews few most common information security threats were introduced to interviewees and researched how these threats affect to interviewees' answers. Normal smart device users were selected for the interviews and also a couple of professionals from the IT field were selected so that their answers could be compared to normal users' answers. The main finding of this study is that the more user has a knowledge of threats, the more motivated he is to do actions to protect his information and the more careful he is when using smart devices. Furthermore, the more user has a knowledge of threats and the more he has done actions to improve his information security, the more concerned he is about his information security. Instead the users who haven't done any improvements for their information security were thinking that their information is well secured, and they didn't think they need any actions to improve security.

Keywords: smart devices, internet of things, information security, information security threats, user experience

KUVIOT

KUVIO 1 Esineiden internetin arkkitehtuuri (Mahmoud ym., 2015) 11

TAULUKOT

TAULUKKO 1 Älylaitteisiin kohdistuvat tietoturvahyökkäykset..... 18
TAULUKKO 2 Kuinka turvassa haastateltavat kokevat tietojensa olevan..... 36
TAULUKKO 3 Kuinka turvassa haastateltavien tiedot ovat ennen ja jälkeen tietoturvauhkien esittelyä..... 38
TAULUKKO 4 Haastateltavien näkemys 5 yleisimmän uhkan uhkaavuudesta 40

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

TAULUKOT 4

SISÄLLYS 5

1 JOHDANTO 7

2 INTERNET OF THINGS 10
2.1 Esineiden internetin määrittely 10
2.2 Älylaitteet 12

3 TIETOTURVA 14
3.1 Tietoturvan merkitys älylaitteissa 14
3.2 Älylaitteisiin kohdistuvat tietoturvauhkat 16
3.2.1 Fyysiset hyökkäykset 18
3.2.2 Verkkoon kohdistuvat hyökkäykset 19
3.2.3 Sovellushyökkäykset 21
3.2.4 Salaushyökkäykset 22
3.3 Yleisimmät älylaitteiden tietoturvauhkat 23

4 TUTKIMUSMETODOLOGIA 26
4.1 Tutkimusmenetelmän valinta 26
4.2 Tutkimuksen toteutus ja tiedonkeruu 28
4.3 Datan analysointi 29
4.4 Tutkimuksen reliabiliteetti ja validiteetti 30

5 TUTKIMUKSEN TULOKSET 32
5.1 Käyttäjien tietämys tietoturvauhkista 32
5.2 Kokemus tietoturvan tasosta 34
5.3 Reaktiot esiteltyihin uhkiin 36
5.4 Haastateltavien näkemykset esitellyistä uhkista 39

6 POHDINTA 45

7 YHTEENVETO 50

LÄHTEET 53

LIITE 1 HAASTATTELURUNKO.....57

1 JOHDANTO

Teknologian jatkuva kehittyminen luo mahdollisuuksia uusien arkea helpottavien innovaatioiden keksimiselle. Yksi esimerkki tästä ovat älylaitteet, jotka ovat levinneet nopeasti lähes kaikkien tietoisuuteen. Älylaitteita on nykyään joka paikassa aina kodeista kouluihin ja sairaaloihin. Analyytikoiden mukaan vuoteen 2020 mennessä käytössä olevia älylaitteita tulee olemaan 20,4 miljardia, joka on huomattavasti enemmän kuin maapallon väestö (Berte, 2018).

Älylaitteista on hyötyä niin kuluttajille kuin myös organisaatioille. Älylaitteet tuovat kustannuksia alas sekä parantavat kuljetuksen, energiantuotannon, teollisuuden ja opetuksen tehokkuutta (Berte, 2018). Teknologian kehittyminen ja erityisesti älylaitteiden yleistyminen ei ole kuitenkaan täysin ongelmatonta. Älylaitteet ovat tarjonneet mahdollisuuden uudenlaisten tietoturvahyökkäysten toteuttamiseen.

Termi esineiden internet keksittiin ja otettiin ensimmäisen kerran käyttöön vuonna 1999 RFID kehitysyhteisön jäsenen toimesta (Berte, 2018; Patel & Patel, 2016). Termille esineiden internet ei ole olemassa yhtä vakiintuneesti käytössä olevaa määritelmää. Lisäksi termi ’esineiden internet’ on käytössä lähinnä mediassa, korkeakouluissa sekä teollisuudessa, kun taas kuluttajat viittaavat kyseiseen teknologiaan ennemmin termillä ’älykoti’ (Berte, 2018).

Esineiden internet on ollut paljon keskustelua aiheuttanut ilmiö viime vuosina ja aiheesta on tehty myös paljon tutkimuksia. Erityisesti esineiden internetin tietoturva on herättänyt vilkasta keskustelua ja älylaitteiden tietoturvasta on löydetty paljon puutteita. Tästäkin huolimatta tavallisten käyttäjien tietoisuus älylaitteisiin liitetyistä tietoturvauhkista on heikolla tasolla ja moni ei edes osaa pelätä tietojensa puolesta. Tämän tutkielman tarkoituksena on tutkia seuraavia asioita:

1. Mitkä ovat yleisimmät älylaitteisiin kohdistuvat tietoturvauhkat?
2. Miten tietoisuus älylaitteiden tietoturvauhkista vaikuttaa älylaitteiden käyttöön?

Aihetta on syytä tutkia sen vuoksi, että älylaitteet lisääntyvät jatkuvasti ja tämän myötä myös tietoturvauhkat kehittyvät. Aiemmin ei ole tehty tutkimusta siitä, miten tietoisuus älylaitteiden tietoturvauhkista vaikuttaa käyttäjien halukkuuteen käyttää älylaitteita. Vaikka suurin vastuu älylaitteiden tietoturvasta kuuluu laitteiden valmistajalle, pystyvät käyttäjät parantamaan omaa tietoturvaansa monin eri tavoin. Tämä kuitenkin edellyttää tietämystä erilaisista tietoturvauhkista sekä toimista, joilla omaa tietoturvaa voi parantaa.

Tutkimusta lähdettiin toteuttamaan kirjallisuuskatsauksen avulla, jolla vastattiin ensimmäiseen tutkimuskysymykseen. Kirjallisuuskatsauksen avulla pystyttiin luomaan pohja tutkielman empiiristä osuutta varten. Kirjallisuuskatsausta varten kirjallisuutta etsittiin Google Scholarin avulla, jonka kautta löytyikin kiitettävästi tieteellisiä artikkeleita älylaitteisiin kohdistuvista tietoturvauhista. Lähteiden luotettavuutta arvioitiin julkaisufoorumin avulla sekä viittausten määrällä. Tutkimuksen empiirisessä osuudessa toteutettiin kvalitatiivinen tutkimus puolistrukturoitujen haastattelujen avulla. Haastatteluun valittiin pääasiassa tavallisia älylaitteiden käyttäjiä, sekä heidän lisäkseen 2 IT-alalla työskentelevää ammattilaista, jotta vastauksia voidaan vertailla keskenään.

Vastauksena ensimmäiseen tutkimuskysymykseen on se, että älylaitteisiin kohdistuvia tietoturvauhkia on paljon ja ne voidaan jaotella neljään ryhmään: fyysiset hyökkäykset, verkkoon kohdistuvat hyökkäykset, sovellushyökkäykset ja salaushyökkäykset. Eräitä yleisimmistä älylaitteisiin kohdistuvista tietoturvahyökkäyksistä ovat erilaiset virukset sekä palvelunestohyökkäykset ja mies välissä -hyökkäykset.

Vastauksena toiseen tutkimuskysymykseen voidaan pitää sitä, että mitä enemmän käyttäjällä on tietoa älylaitteisiin kohdistuvista tietoturvauhkista, sitä motivoituneempi hän on suojautumaan niiltä. Henkilöt, joilla on kattavasti tietoa erilaisista uhkista, ovat usein tehneet kattavasti erilaisia tietoturvaa parantavia toimia, sillä he kokevat tietonsa olevan uhattuina. Vaikka tietoturvauhkiin perehtyneet henkilöt ovatkin tehneet paljon erilaisia suojautumistoimenpiteitä, kokevat he silti tietonsa olevan uhattuina. Sen sijaan käyttäjät, joilla ei juurikaan ole tietoa erilaisista tietoturvauhkista, eivät yleensä ole tehneet mitään tai vain vähän tietoturvaa parantavia toimia. Tästä huolimatta käyttäjät, joilla on vähän tietoa tietoturvauhkista ja jotka ovat tehneet vähän suojautumistoimenpiteitä, kokevat tietonsa olevan parhaiten turvassa. Nämä käyttäjät turvautuvat teknologian uhkien välttämisteorian mukaisesti tunteisiin keskittyviin suojautumisstrategioihin, eli he uskottelevat itselleen, ettei kukaan ole kiinnostunut heidän tietoistaan ja etteivät uhkat kohdistu heihin.

Tutkielman rakenne on seuraava: Tutkielman toisessa luvussa esitellään esineiden internetiä ja selvitetään, mitä kyseisellä termillä tarkoitetaan. Koska kirjallisuudessa esineiden internetille ei ole olemassa yleisesti käytössä olevaa määritelmää, pyritään luvussa luomaan mahdollisimman kattava määritelmä termille. Tämän jälkeen luvussa esitellään esineiden internetiin liittyviä älylaitteita sekä niiden toimintaperiaatteita. Tutkielman kolmannessa luvussa käsitellään tietoturvaa älylaitteiden näkökulmasta. Luvussa käsitellään sitä, miksi tietoturvaa tarvitaan älylaitteissa ja millaisia eri tietoturvauhkia älylaitteisiin koh-

distuu. Neljännessä luvussa on esitelty tutkimuksessa käytetty tutkimusmetodologia, eli se, miten tutkimus on toteutettu ja saatu data analysoitu. Luvussa pohditaan myös tutkimuksen reliabiliteettia ja validiteettia. Viidennessä luvussa on esitelty tutkimuksessa saadut tulokset. Ensimmäisessä alaluvussa on esitelty käyttäjien tietämys älylaitteisiin kohdistuvista tietoturvauhkista, toisessa alaluvussa kokemus nykyisen tietoturvan tasosta, kolmannessa alaluvussa haastateltavien reaktiot esiteltyihin uhkiin ja neljännessä alaluvussa haastateltavien näkemykset esitellyistä uhkista. Kuudes luku sisältää pohdinnan tutkimuksen tuloksista ja saatuja tuloksia verrataan myös kirjallisuudessa saatuihin tuloksiin. Tutkielman lopussa on vielä yhteenveto tutkielmassa käsitellyistä asioista.

2 INTERNET OF THINGS

Tässä luvussa määritellään esineiden internet ja selvitetään, mitä sillä tarkoitetaan. Ensimmäisessä alaluvussa käydään läpi esineiden internetin määritelmä kirjallisuuteen pohjautuen. Toinen alaluku esittelee erilaisia älylaitteita, jotka ovat osa esineiden internetiä.

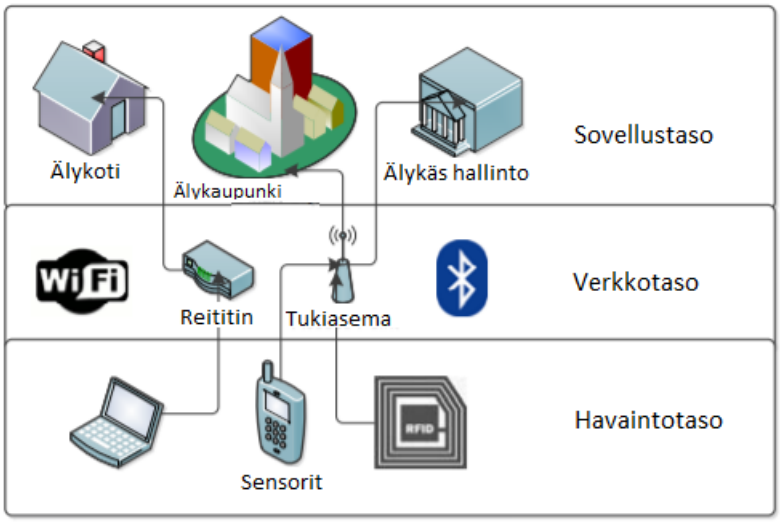
2.1 Esineiden internetin määrittely

Yhä useampi laite ja kodinkone on yhdistetty internetiin ja nämä yhdessä ihmisten ja palveluiden kanssa muodostavat esineiden internetin (internet of things, IoT), joka voi kommunikoida, jakaa dataa ja tietoa yhteisen tavoitteen saavuttamiseksi (Mahmoud, Yousuf, Aloul & Zualkernan, 2015). Esineiden internetin tavoitteena on mahdollistaa esineiden kytkeytyminen milloin tahansa, missä tahansa ja minkä tahansa kanssa, eli muiden esineiden ja ihmisten kanssa (Patel & Patel, 2016). Vaikka termiä esineiden internet käytetään laajasti, ei sille ole olemassa yleisesti käytössä olevaa määritelmää (Wortmann & Flüchter, 2015). Kirjallisuuteen perehtyessä lukijan saattaa olla vaikeaa ymmärtää, mitä esineiden internetillä oikeastaan tarkoitetaan ja mitä sosiaalista, taloudellista ja teknillistä merkitystä sen käyttöönotolla on (Atzori, Iera & Morabito, 2010).

Atzorin, Ieran ja Morabiton (2010) mukaan esineiden internetiin liittyvien määritelmien moninaisuus johtuu termistä ”esineiden internet”. Esineiden internetiä voidaan tarkastella 3 eri näkökulmasta, jotka ovat internetiin suuntautunut, esineisiin suuntautunut ja semanttisesti suuntautunut. Termin ensimmäinen sana eli ’esineiden’ viittaa geneerisiin esineisiin, kun taas jälkimmäinen sana eli ’internet’ viittaa verkkoon. Näin ollen termiä voidaankin tarkastella kummasta vain näkökulmasta, riippuen tarkastelijan intresseistä, tavoitteista tai taustasta. Yhdessä sanat ’esineiden internet’ viittaavat semanttiseen näkökulmaan, joka tuo mukanaan vielä uudenlaisia tapoja tarkastella termiä. (Atzori ym., 2010.)

Yhden määritelmän mukaan esineiden internet on globaali infrastruktuuri tietoyhteiskunnalle, joka mahdollistaa kehittyneet palvelut yhdistämällä toisiinsa fyysiset laitteet ja virtuaaliset ratkaisut (Wortmann & Flüchter, 2015). Gubbi, Buyya, Marusic ja Palaniswami (2013) puolestaan kuvailevat esineiden internetin olevan sensoreiden ja käyttölaitteiden yhteenliittymä, joka tarjoaa mahdollisuuden jakaa tietoa eri alustoilla kehittäen yhteisen toimintakuvan mahdollistamaan innovatiivisen toiminnan. Tämä saavutetaan saumattomalla, laaja-alaisella havaitsemisella, data-analytiikalla sekä tietojen esittämisellä käyttäen havaitsemista ja pilvilaskentaa (Gubbi ym., 2013).

Mahmoud, Yousuf, Aloul ja Zualkernan (2015) kuvailevat artikkelissaan esineiden internetin arkkitehtuuria. Tutkijoiden mielipiteet vaihtelevat sen suhteen, kuinka monta eri tasoa esineiden internetin arkkitehtuurissa nähdään olevan. Suurin osa tutkijoista on kuitenkin sitä mieltä, että esineiden internet toimii lähinnä kolmella eri tasolla, jotka ovat havaitsemisen, verkon ja sovelluksen taso (kuvio 1). (Mahmoud ym., 2015.)



KUVIO 1 Esineiden internetin arkkitehtuuri (Mahmoud ym., 2015)

Havaitsemisen tason tarkoituksena on kerätä dataa ympäristöstä sensoreiden avulla. Kerätty data prosessoidaan ja siirretään verkon tasolle. Havaintotaso koostuu lähinnä sensoreista ja radiotaajuuden tunnistimista (Radio Frequency Identification, RFID). RFID -teknologia mahdollistaa jokaisen laitteen tunnistamisen ja merkinnän. Havaintotason laitteilla on hyvin rajalliset laskennalliset valmiudet, jonka vuoksi niihin on vaikeaa lisätä minkäänlaisia tietoturvaa parantavia salausalgoritmeja. (Mahmoud ym., 2015.) Havaintotasolla tiedon hankinta ja solmujen välinen kommunikointi tapahtuu lyhyellä kantamalla ja paikallisissa verkoissa (Atzori, Iera, Morabito & Nitti, 2012).

Verkkotason tavoitteena on siirtää dataa eri verkkojen välillä (Atzori ym., 2012). Verkon tason tehtävänä on reitittää ja siirtää dataa eri iot -keskuksille ja laitteille hyödyntäen internetiä. Verkon tason laitteet ovat pilvilaskenta-alustoja, internet yhdyskäytäviä, kytkimiä ja reitittimiä ja laitteet käyttävät tiedonsiirtoon WLAN, LTE, Bluetooth, 3G ym. teknologioita. Yhdyskäytävät toimivat

välittäjinä eri iot-solmujen välillä kokoamalla, suodattamalla ja lähettämällä tietoa eri sensoreille. Verkkotason laitteet ovat hyvin monimuotoisia, minkä vuoksi nykyisen verkkoprotokollan käyttäminen on hankalaa, minkä lisäksi myös tehokkaiden suojamekanismien kehittäminen on haastavaa. (Mahmoud ym., 2015.)

Sovellustaso varmistaa datan aitouden, eheyden ja luottamuksellisuuden. Tällä tasolla saavutetaan varsinainen esineiden internetin tavoite eli mahdollistetaan älykäs ympäristö. (Mahmoud ym., 2015.) Sovellustasolla iot-sovellukset yhdistetään ja näin saadaan käyttöön laitteiden toiminnot (Atzori ym., 2012).

2.2 Älylaitteet

Älylaitteilla (smart devices) tarkoitetaan laitteita, jotka ovat yhteydessä internetiin. Älylaitteilla, samoin kuin esineiden internetilläkään, ei ole olemassa yhtä vakiintunutta määritelmää, mutta useimmiten ne määritellään verkkoon liitetyiksi laitteiksi, jotka yhdistävät fyysisen ja virtuaalisen maailman (Ronen & Shamir, 2016). Tänä päivänä yhä useampi laite ja kodinkone on yhdistetty internetiin ja näin ollen älylaitteiden määrä onkin kasvanut valtavalla tahdilla. Suurin ero älylaitteen ja ei-älykkään laitteen välillä on se, että älylaitteet tarjoavat mahdollisuuden sisällyttää kolmannen osapuolen tarjoamia sovelluksia laitteeseen (Suarez-Tangil, Tapiador, Peris-Lopez & Ribagorda, 2014).

Kortuem, Kawsar, Sundramoorthy ja Fitton (2010) jakavat älylaitteet kolmeen ryhmään. Ensimmäisenä ovat toiminnasta tietoiset älylaitteet, jotka voivat tallentaa tietoa esimerkiksi työstä ja laitteen käytöstä. Nämä laitteet ymmärtävät ympäristöään tapahtumien ja toimien kautta, ja ne lähinnä kirjaavat ylös tapahtumia, eivätkä tarjoa interaktiivisia toimia. Toisena ryhmänä ovat menettelytavasta tietoiset älylaitteet. Nämä ovat toiminnasta tietoisia älylaitteita, jotka pystyvät lisäksi tulkitsemaan ympäristön tapahtumia organisaation toimintaperiaatteiden näkökulmasta. Menettelytavasta tietoiset älylaitteet pystyvät ilmoittamaan, jos työntekijät rikkovat organisaation toimintaperiaatteita ja ne voivat antaa varoituksia. Kolmantena ryhmänä ovat prosessista tietoiset älylaitteet, jotka ovat kehittyneimpiä älylaitteita. Nämä laitteet ymmärtävät organisatoriset prosessit ja ne osaavat yhdistää reaalimaailman tapahtumat näihin prosesseihin. Prosessista tietoiset älylaitteet pystyvät esimerkiksi antamaan käyttäjille tietoa tehtävistä ja aikatauluista. (Kortuem ym., 2010.)

Älylaitteet ovat yhteydessä langattomaan sensoriverkkoon (wireless sensor network, WSN), joka koostuu suuresta määrästä sensorisolmuja, jotka valvovat ympäristöään kuten esimerkiksi ääntä, painetta ja lämpötilaa. Keräämänsä tiedot sensorisolmut lähettävät tukiasemalle. Sensorisolmu muodostuu neljästä peruskomponentista, jotka ovat mittausyksikkö, prosessointiyksikkö, lähetinyksikkö sekä virtalähde. (Wahid & Kumar, 2015.) Älylaitteiden akkukapasiteetti sekä laskentateho ovat rajalliset, mikä tarkoittaa sitä, että laitteet käyttävät suurimman osan saatavilla olevasta energiasta ja laskentatehosta varsinaisten

tehtävien suorittamiseen. Tämän vuoksi älylaitteisiin on harvoin mahdollista laittaa minkäänlaista tietoturvaratkaisua. (Mahmoud ym., 2015; Zhang, Cho & Shieh, 2015; Dorri, Kanhere, Jurdak & Gauravaram, 2017.) Tämä altistaa älylaitteet monenlaisille tietoturvauhkille.

Harva osaa pelätä älykkäiden kodinkoneiden tietoturvauhkia, sillä käyttäjät ovat tottuneet miettimään tietoturvaa lähinnä tietokoneiden, tablettien ja älypuhelimien osalta. Verkkoon yhdistetyt kodinkoneet, kuten jääkaapit, pesukoneet ym., ovat kuitenkin paras kohde hyökkääjälle, sillä niissä harvemmin on minkäänlaista tietoturvaa (Ronen & Shamir, 2016). Lisäksi älylaitteita hyödyntämällä on mahdollista saada aikaan paljon tuhoa aiheuttavia hyökkäyksiä, joita esitellään tarkemmin seuraavassa kappaleessa.

3 TIETOTURVA

Tässä luvussa selvitetään, miksi tietoturva on erityisen tärkeää älylaitteissa ja millaiset tiedot voivat olla vaarassa älylaitteita käytettäessä. Toisessa alaluvussa on esitelty erilaisia älylaitteisiin kohdistuvia tietoturvauhkia. Uhkat on jaoteltu seuraaviin kategorioihin: fyysiset hyökkäykset, verkkoon kohdistuvat hyökkäykset, sovellushyökkäykset sekä salaushyökkäykset. Kolmannessa alaluvussa on vielä esitelty kirjallisuuden mukaan yleisimmät älylaitteisiin kohdistuvat tietoturvauhkat.

3.1 Tietoturvan merkitys älylaitteissa

Älylaitteet keräävät jatkuvasti dataa ympäristöstään ja lähettävät sitä eteenpäin. Kun otetaan huomioon se, miten paljon älylaitteita on käytössä, voidaan todeta kyseessä olevan todella suuri määrä dataa. Älylaitteisiin kuitenkin liittyy paljon tietoturvauhkia ja näin ollen kyseessä on laaja-alainen ongelma, joka koskettaa suurta osaa käyttäjistä. Tämän vuoksi tietoturvalla on erittäin tärkeä rooli älylaitteissa.

Tietoturvan tarkoituksena on turvata tiedon luottamuksellisuus, eheys ja saatavuus. Yrityksillä ja organisaatioilla onkin nykyään omat tietoturvapolitiikat tiedon turvaamiselle. Tietoturvapolitiikan avulla työntekijät tietävät, kuinka tietoa pitää käsitellä ja säilöä tietoturvan säilyttämiseksi. (Vroom & Von Solms, 2004.)

Älylaitteet aiheuttavat monessa suhteessa enemmän turvallisuus- ja yksityisyysuhkia kuin tavalliset PC:t. Monet älylaitteet sisältävät lukuisia sensoreita, jotka voivat vuotaa arkaluontoista tietoa käyttäjien sijainnista, eleistä, liikkeistä sekä muista fyysisistä toiminnoista. Tämän lisäksi älylaitteet voivat myös tallentaa ääntä, kuvia ja videota ympäristöstään. (Suarez-Tangil ym., 2014.)

Koska internet on esineiden internetin perusta, lähes kaikki internetiin liittyvät tietoturvauhkat kohdistuvat myös esineiden internetiin. Tämän lisäksi

älylaitteiden nopea kehitys ja laajat käyttömahdollisuudet vaativat tietoturvauhkien havaitsemista ennen laitteiden käyttöönottoa. Vaikka monet yritykset ilmoittavat heidän teknologioiden olevan täysin turvattuja, ovat ne siltikin alttiita monenlaisille tietoturvauhkille. (Andrea, Chrysostomou & Hadjichristofi, 2015.)

Suurin huolenaihe, joka erottaa esineiden internetin tavallisesta internetistä, on Zhangin, Chon ja Shiehin (2015) mukaan skaalautuvuus. Iot:ssä miljardit laitteet ovat yhdistyneet verkkoon ja tämän myötä tapoja laitteiden tunnistamiseen ja todennukseen tulee uudistaa. Tavanomaiset todennusmetodit eivät välttämättä pysty käsittelemään näin suurta määrää laitteita. Lisäksi läpinäkyvyys ja luotettavuus tuottavat ongelmia uusien tunnistus- ja todennusmetodien kehittämiseen. Läpinäkyvyys aiheuttaa ongelmia siten, että käyttäjät eivät jaksa suorittaa monimutkaisia konfigurointivaiheita aktivoidakseen älylaitteensa. Koska konfigurointiasetusten pitäisi olla lähes näkymättömiä käyttäjille, tulee ne suunnitella mahdollisimman yksinkertaisiksi. (Zhang, Cho & Shieh, 2015.)

Luotettavuus on toinen ongelmia aiheuttava asia esineiden internetin tietoturvassa. Rajalliset resurssit ja akun kapasiteetti tekevät älylaitteiden välisestä kommunikoinnista virhealtista. Lisäksi iot-laitteiden epäyhtenäisyys vaikeuttaa entisestään tietoturvaratkaisuiden kehittämistä, sillä laitteiden ja palveluiden toteutus ja arviointi on entistä hankalampaa. Mahdollisten virheiden korjaaminen on näin ollen myös hankalampaa. (Zhang, Cho & Shieh, 2015.)

Zhang, Cho ja Shieh (2015) jakavat esineiden internetin tietoturvauhkat kahteen luokkaan. Ensimmäisessä luokassa hyökkäykset ovat samankaltaisia kuin tavallisessa tietoverkossa ja kohdistuvat tiedon luotettavuuteen, eheyteen ja saatavuuteen. Otettaessa huomioon esineiden internetiin liitettyjen laitteiden määrä ja erilaisuus, ovat tietoturvauhkat huomattavasti monimutkaisempia ja vakavampia kuin perinteiseen verkkoon kohdistuvat. Toisen luokan hyökkäykset hyödyntävät iot-verkon uusia ominaisuuksia ja kohdistuvat älylaitteiden keräämiin arkaluonteisiin tietoihin. Älylaitteet keräävät ympäristöstään monenlaista arkaluonteista tietoa, kuten tietoja käyttäjän sykkeestä, verenpaineesta, kodin lämpötilasta, käyttäjän sijainnista sekä elintavoista. Nämä tiedot ovat alttiita hyökkäyksille ja vaarassa joutua vääriin käsiin. Älylaitteisiin ei ole kuitenkaan mahdollista laittaa perinteistä virusturvaa, koska se veisi liikaa laskentatehoa. (Zhang, Cho & Shieh, 2015.) Näin ollen älylaitteisiin pitäisi kehittää uudenlaisia suojautumiskeinoja tietoturvauhkia vastaan.

Tulevaisuuden internetissä iot tulee olemaan keskeisessä asemassa ja erityisesti tällöin sen tietoturvan merkitys korostuu. Leo, Battisti, Carli ja Neri (2014) korostavat, ettei esineiden internetin tietoturvaa voida nähdä vain yksittäisiin laitteisiin lisättävänä ominaisuutena, vaan ennemmin pitäisi pyrkiä luomaan ympäristö, jossa kuluttajat ja tuottajat voivat tehdä yhteistyötä tietoturvan parantamiseksi. Havaintotasolla tietoturvan tulisi varmistaa se, että solmuja ei ole manipuloitu, ohjailtu tai vahingoitettu sekä se ettei tietoa ole vääristelty, väärennetty tai korvattu luvattomasti. Verkkotasolla tietoturvan tulisi taata välitetyn tiedon luottamuksellisuus, eheys ja aitous. Sovellustasolla puolestaan

tietoturvan tulisi varmistaa tiedon yksityisyys, luottamuksellisuus sekä säilytyksen turvallisuus. (Leo ym., 2014.)

Leon ym. (2014) visio ympäristöstä, jossa kuluttajat myös panostaisivat tietoturvaan saa tukea Liangin ja Xuen (2009) Technology threat avoidance theory (TTAT) eli vapaasti suomennettuna teknologian uhkien välttämisteorialta. TTAT todistaa, että käyttäjät ovat motivoituneita välttelemään haitallista tietotekniikkaa silloin, kun he kohtaavat uhkan ja uskovat, että uhka on mahdollista välttää noudattamalla turvaavia toimia. Jos taas käyttäjät uskovat, ettei uhkaa pysty täysin välttämään turvaavia toimia noudattamalla, ottavat he käyttönsä tunteisiin keskittyvät selviytymisstrategiat. Tunteisiin keskittyvissä selviytymisstrategioissa käyttäjät luovat virheellisiä havaintoja ympäristöstä tekemättä mitään muutoksia siihen. Tunteisiin keskittyviä selviytymisstrategioita käyttäessä käyttäjä saattaa esimerkiksi ajatella, ettei uhka kohdistu häneen tai ettei kukaan ole kiinnostunut hänen tiedoistaan. Tällä tavoin ajattelemalla uhkataso laskee eikä käyttäjä koe tietoturvansa olevan uhattuna. (Liang & Xue, 2009.)

Myös Liangin ja Xuen toinen tutkimus vuodelta 2010 tuo ilmi, että käyttäjät muodostavat uhkakuvan, jos he uskovat, että haitallinen IT tulee todennäköisesti kohdistumaan heihin ja näin tapahtuessa negatiiviset seuraukset tulevat olemaan vakavat. Käyttäjät ovat myös motivoituneita välttelemään uhkaa, jos he kokevat turvaavien toimien olevan tehokkaita, edullisia käyttää ja käyttäjillä on itsevarmuutta sen suhteen, että he osaavat toteuttaa turvaavia toimenpiteitä (Liang & Xue, 2010). Yksi tärkeä syy sille, miksi myös käyttäjät olisi hyvä valjastaa tietoturvan parantamiseen on se, että käyttäjät usein nähdään heikoimpana lenkkinä tietoturvassa. Tämä johtuu siitä, että vahvinkin teknologinen suojaus on mahdollista kiertää, jos hyökkääjä onnistuu manipuloimaan käyttäjän toimimaan haluamallaan tavalla. (Heartfield & Loukas, 2016.)

3.2 Älylaitteisiin kohdistuvat tietoturvauhkat

Älylaitteisiin liittyvät tietoturvauhkat voivat olla aktiivisia tai passiivisia. Aktiivinen hyökkäys pysäyttää älylaitteen tarjoaman palvelun kokonaan, kun taas passiivinen hyökkäys tarkkailee verkossa liikkuvaa tietoa häiritsemättä äylaitteen toimintaa. Eri esineiden internetin tasoihin (sovellus-, verkko- ja havaintotaso) kohdistuu erilaisia hyökkäyksiä. Poikkeuksen tästä tekevät palvelunestohyökkäykset, joita voi esiintyä millä tahansa esineiden internetin tasolla. Palvelunestohyökkäyksellä tarkoitetaan hyökkäystä, joka tekee laitteesta tai verkosta saavuttamattoman valtuutetuille käyttäjille. (Mahmoud ym., 2015.)

Ronen ja Shamir (2016) jakavat älylaitteisiin kohdistuvat hyökkäykset neljään kategoriaan. Ensimmäisenä ovat hyökkäykset, jotka jättävät laitteen toiminnallisuudet huomiotta. Näissä hyökkäyksissä hyökkääjä näkee laitteet vain tavallisina verkkoon yhdistettyinä laitteina, joita pystyy käyttämään esimerkiksi roskapostin lähettämiseen tai bitcoinien louhintaan. Toisena ovat hyökkäykset, jotka pyrkivät rajoittamaan laitteen toiminnallisuuksia. Esimerkkeinä näistä ovat se, ettei tv toimi, jääkaappi ei kylmene tai valot eivät syty. Näiden hyök-

käysten tarkoituksena on mm. ärsyttää yksilöä tai organisaatiota, aiheuttaa taloudellisia menetyksiä tai aiheuttaa laajaa kaaosta. Laitteen toiminnallisuuksia rajoittava hyökkäys voidaan toteuttaa esimerkiksi siten, että hyökkääjä voi laittaa uhrin televisioon näkymään viestin, jossa uhria vaaditaan maksamaan hyökkääjälle bitcoineina, jotta televisio alkaisi taas toimimaan. Nämä hyökkäykset ovat helppoja toteuttaa, sillä älytelevisioissa ei ole minkäänlaisia palomuureja tai virustentorjuntaa ja suurikokoinen televisio on hankalampi kuljettaa korjattavaksi kuin vaikkapa kannettava tietokone. (Ronen & Shamir, 2016.)

Kolmanneksi hyökkäystyypiksi Ronen ja Shamir (2016) ovat nimenneet hyökkäykset, jotka väärinkäyttävät laitteen ominaisuuksia. Yhtenä esimerkkinä näistä hyökkäyksistä on hyökkäys, jossa hyökkääjä pystyy laittamaan päälle kaikki talon valot ja hanat, kun talon omistajat ovat pitkän aikaa poissa kotoa. Tämänkaltaiset hyökkäykset ovat kuitenkin olleet lähinnä yksittäisiä tapauksia eivätkä ne ole aiheuttaneet laajamittaisia vahinkoja. Neljäntenä ovat hyökkäykset, jotka pyrkivät laajentamaan laitteen ominaisuuksia ja aiheuttamaan täten täysin odottamattomia seurauksia. Esimerkkeinä tällaisista hyökkäyksistä voivat olla esimerkiksi tilanne, jossa älykäs ilmastointilaite sytyttää tulipalon tai internetiin yhdistetty robottipölynimuri avaa asunnon oven. Kuten esimerkkihyökkäyksistä huomataan, nämä hyökkäykset vaativat enemmän suunnittelua ja ne ovat haastavampia toteuttaa. (Ronen & Shamir, 2016.)

Esineiden internetiin ja älylaitteisiin kohdistuvia tietoturvauhkia voidaan jaotella eri tavoin ja yleisin tapa jaotella hyökkäykset on jakaa ne neljään kategoriaan, kuten Andrea, Chrystostomou ja Hadjichristofi (2015) sekä Deogirikar ja Vidhate (2017) ovat tehneet. Nämä neljä kategoriaa ovat: fyysiset hyökkäykset havaintotasolla, verkkoon kohdistuvat hyökkäykset verkkotasolla, sovellushyökkäykset sovellustasolla sekä salaushyökkäykset (taulukko 1) (Andrea, Chrysostomou & Hadjichristofi, 2015). Tätä luokittelua käytetään myös tässä tutkielmassa.

TAULUKKO 1 Älylaitteisiin kohdistuvat tietoturvahyökkäykset

Fyysiset hyökkäykset	Verkkoon kohdistuvat hyökkäykset	Sovellushyökkäykset	Salaushyökkäykset
Solmujen väärinkäyttö	Verkkoliikenteen analysointihyökkäys	Tietojenkalastelu	Side channel -hyökkäys
Solmun häirintä	RFID -huijaus	Haittaohjelmat (virukset, vakoiluohjelmat)	Salausanalyysihyökkäys
Haitallisen solmun lisäys (mies välissä -hyökkäys)	RFID -kloonaus	Tilin kaappaus	Mies välissä -hyökkäys
Fyysinen vahingoittaminen	Luvaton pääsy RFID -tunnisteen tietoihin	Salakuuntelu	
Käyttäjän manipulointi	Mies välissä -hyökkäys	Haitallinen komentosarja	
Lepotilaan pääsyn häirintä	Palvelunestohyökkäys	Palvelunestohyökkäys	
Haitallisen koodin lisääminen	Reitityshyökkäys		
	Sybil -hyökkäys		

3.2.1 Fyysiset hyökkäykset

Fyysiset hyökkäykset kohdistuvat iot-järjestelmän laitteiston osiin ja hyökkääjän täytyy olla lähellä iot-järjestelmää, jotta hyökkäys onnistuisi (Andrea, Chrysostomou & Hadjichristofi, 2015). Ensimmäinen fyysisistä hyökkäyksistä on solmujen väärinkäyttö (node tampering). Siinä hyökkääjä aiheuttaa vahinkoa sensorin solmulle joko fyysisesti vaihtamalla koko solmun tai osan sen laitteistosta haitallisiin solmuihin tai laitteistoon. Tällä tavoin hyökkääjä saa oikeuden päästä käsiksi ja muokata arkaluonteisia tietoja, kuten salausavaimia, sekä mahdollisuuden muokata solmujen ohjelmointia. (Perrig, Stankovic & Wagner, 2004.)

Toinen esimerkki fyysisestä hyökkäyksestä on solmun häirintä langattomissa sensoriverkoissa (node jamming). Mpitziopoulos, Gavalas, Konstantopoulos & Pantziou (2009) toteavat solmun häirinnän olevan eräänlainen palvelunestohyökkäyksen muoto. Siinä hyökkääjä häiritsee radiotaajuuksia ja signaaleita, joita käytetään kommunikointiin, sekä estää solmujen välisen kommunikoinnin. Jos hyökkääjä onnistuu häiritsemään tärkeimpiä sensorin solmuja, hän voi estää koko palvelun käytön. (Mpitziopoulos, Gavalas, Konstantopoulos & Pantziou, 2009.)

Myös mies välissä -hyökkäys (man in the middle attack) on mahdollinen fyysisellä tasolla. Tällöin hyökkääjä sijoittaa haitallisen solmun kahden tai useamman solmun väliin, jolloin hän pystyy kontrolloimaan kaikkea tietovirtaa solmujen välillä sekä solmujen toimintaa. Tätä hyökkäystä kutsutaan haitallisen solmun lisäämiseksi. Toinen tapa millä hyökkääjä voi tehdä vahinkoa on fyysisen vahingon tekeminen laitteille. Tämä hyökkäys eroaa solmujen väärinkäy-

töstä siten, että tässä hyökkäyksessä hyökkääjä pyrkii nimenomaan vahingoittamaan esineiden internetiä tarkoituksenaan haitata palveluiden saatavuutta. (Andrea, Chrysostomou & Hadjichristofi, 2015.)

Andrea, Chrysostomou ja Hadjichristofi (2015) luokittelevat käyttäjän manipuloinnin (social engineering) myös fyysiseksi hyökkäykseksi. He perustelevat luokittelua sillä, että käyttäjän manipuloinnissa hyökkääjän täytyy fyysisesti olla vuorovaikutuksessa esineiden internetin käyttäjien kanssa saavuttaakseen tavoitteensa. Käyttäjän manipulointi toimii siten, että hyökkääjä manipuloi käyttäjät jakamaan yksityisiä tietoja tai suorittamaan tiettyjä toimintoja, jotka palvelevat hyökkääjän tavoitteita. (Andrea, Chrysostomou & Hadjichristofi, 2015.)

Yksi tapa haitata älylaitteiden toimintaa on häiritä niiden lepotilaan pääsyä (sleep deprivation attack). Virranhallinta on kriittisessä roolissa sensoriverkkojen toiminnan kannalta, sillä ilman virranhallintaa laitteiden paristot tai akut eivät kestäisi kovin kauaa (Karlof & Wagner, 2003). Näin ollen sensorisolmut on ohjelmoitu menemään lepotilaan säästääkseen pattereita. Älylaitteita vastaan on mahdollista tehdä hyökkäys, joka estää laitteita menemästä lepotilaan. Näin ollen laitteiden patterit tai akut tyhjenevät ja laitteet sammuvat. (Andrea, Chrysostomou & Hadjichristofi, 2015.) Näiden hyökkäysten vahingot mitataan yleensä menetetyn energian muodossa verrattuna tilanteeseen, jossa laitteeseen ei kohdistu hyökkäystä (Dabbagh & Rayes, 2019).

Yksi fyysisistä hyökkäyksistä on haitallisen koodin lisääminen (malicious code injection), joka tapahtuu siten, että hyökkääjä lisää solmuun haitallisen koodin, joka antaa hänelle oikeuden iot-järjestelmään. Tämän myötä hyökkääjä voi saada oikeuden hallita kaikkea solmun toimintaa tai jopa oikeuden hallita koko järjestelmää. (Andrea, Chrysostomou & Hadjichristofi, 2015.)

3.2.2 Verkkoon kohdistuvat hyökkäykset

Verkkoon kohdistuvat hyökkäykset keskittyvät iot-järjestelmän verkkoon ja hyökkääjän ei tarvitse olla lähellä laitteita, vaan hyökkäykset on mahdollista toteuttaa etänä (Andrea, Chrysostomou & Hadjichristofi, 2015). Ensimmäinen verkkoon kohdistuvista hyökkäyksistä on verkkoliikenteen analysointihyökkäys (traffic analysis attack). Siinä hyökkääjä voi saada haltuunsa luottamuksellista tietoa, joka liikkuu RFID -teknologioiden välillä johtuen niiden langattomista ominaisuuksista (Khoo, 2011). Thakur ja Chaudhary (2013) puolestaan toteavat, että lähes kaikissa hyökkäyksissä hyökkääjä pyrkii ensiksi saamaan verkkoon liittyvää tietoa, ennen kuin hän toteuttaa hyökkäyksensä. Tämä toteutetaan käyttämällä jotain urkintasovellusta, kuten pakettien urkintaa (Andrea, Chrysostomou, & Hadjichristofi, 2015).

RFID -huijauksessa (RFID spoofing) hyökkääjä tekeytyy valtuutetuksi RFID -tunnisteeksi saadakseen sen oikeudet (Mitrokotsa, Rieback & Tanenbaum, 2010). Tällöin hyökkääjä voi lähettää omaa dataansa järjestelmään käyttäen alkuperäisen tunnisteen ID:tä ja samalla hän saa täydet oikeudet järjestel-

mään. RFID -kloonauksessa (RFID cloning) puolestaan hyökkääjä kloonaa RFID -tunnisteen kopioiden sen tiedot toiseen RFID -tunnisteeseen. Vaikka tämä hyökkäys onkin varsin samankaltainen kuin RFID -huijaus, ei tässä hyökkäyksessä kuitenkaan käytetä alkuperäisen RFID -tunnisteen ID:tä ja näin ollen on mahdollista tunnistaa alkuperäinen ja kloonattu tunniste toisistaan. RFID -tunnisteisiin liittyy vielä kolmaskin hyökkäys, joka on luvaton pääsy RFID -tunnisteen tietoihin. Tämä hyökkäys mahdollistaa sen, että hyökkääjä voi lukea, muokata tai jopa poistaa RFID -tunnisteen tietoja. RFID -tunnisteissa ei ole kunnollisia todentamismenetelmiä, joka tarkoittaa sitä, että tunnisteisiin pääsee käsiksi kuka vain. (Andrea, Chrysostomou, & Hadjichristofi, 2015.)

Myös verkkotasolla voi esiintyä mies välissä -hyökkäyksiä. Tällöin hyökkääjä onnistuu puuttumaan verkon yli kahden sensorisolmun väliseen kommunikointiin saaden pääsyn salaiseen tietoon. Näin ollen hyökkääjä rikkoo yksityisyyttä seuraamalla, salakuuntelemalla ja kontrolloimalla solmujen välistä kommunikointia. Verkkotason mies välissä -hyökkäys eroaa fyysisen tason haitallisen solmun lisäämisestä siten, että verkkotasolla hyökkääjän ei tarvitse olla paikalla hyökkäyksen toteuttamiseksi vaan hyökkäys onnistuu verkon avulla. (Andrea, Chrysostomou, & Hadjichristofi, 2015.)

Palvelunestohyökkäys (denial of service) on yksi verkkotason hyökkäyksistä. Siinä hyökkääjä lähettää IoT-verkkoon niin paljon verkkoliikennettä, ettei verkko pysty käsittelemään sitä. (Andrea, Chrysostomou, & Hadjichristofi, 2015.) Myös Yu (2014) kuvailee palvelunestohyökkäyksen olevan hyökkäys, jossa suuri määrä tietoliikennettä ohjataan verkkoon, jolloin saadaan esimerkiksi verkon kaistanleveys laskemaan. Tämä joko vaikeuttaa käyttäjän pääsyä palveluun tai jopa kokonaan estää sen (Yu, 2014).

Reitityshyökkäys (routing information attack) on suora hyökkäys, jossa hyökkääjä hankaloittaa verkon toimintaa huijaamalla, muuttamalla tai toistamalla reititystietoja. Tällä tavoin hyökkääjä pystyy luomaan reitityssilmukoita, jolloin paketti jää kulkemaan kahden tai useamman reitittimen väliä. Hyökkääjä voi myös sallia tai hävittää verkkoliikennettä, lähettää vääriä virheilmoituksia tai jopa osittaa verkon. (Andrea, Chrysostomou, & Hadjichristofi, 2015.) Esimerkkeinä reitityshyökkäyksistä ovat mm. hello -hyökkäys sekä musta aukko -hyökkäys. Hello -hyökkäys tarkoittaa tiivistettynä sitä, että hyökkääjä lähettää sensoriverkossa oleville solmuille hello -viestiä, jolloin solmut luulevat hyökkääjän solmun olevan heitä lähimpänä ja alkavat lähettämään paketteja hyökkääjän solmulle (Wahid & Kumar, 2015).

Yksi erityisen haitallinen verkkoon kohdistuva hyökkäys on sybil hyökkäys (sybil attack). Siinä haitallinen solmu esiintyy useampana solmuna. Newsome, Shi, Song ja Perrig (2004) toteavat, että sybil hyökkäyksiä on olemassa useita erilaisia ja ne voidaan toteuttaa eri tavoin. Esimerkiksi solmun identiteetti on mahdollista joko varastaa muilta solmuilta tai hyökkääjä voi luoda täysin uuden identiteetin solmulle. Joissain tapauksissa solmujen identiteetit ovat 32-bittisiä lukuja, jolloin hyökkääjä voi helposti keksiä solmuille mitkä tahansa 32-bittiset luvut identiteeteiksi. Sybil hyökkäystä voidaan myös käyttää aiemmin mainitun reitityshyökkäyksen toteuttamiseen. Yksi mahdollinen sybil hyökkäys

kohdistuu langattomien sensoriverkkojen tekemiin äänestyksiin. Jos hyökkääjällä on käytössään tarpeeksi monta solmuidentiteettiä, voi hän päättää kaikkien äänestysten tulokset. (Newsome ym., 2004.)

3.2.3 Sovellushyökkäykset

Sovelluksiin kohdistuvat hyökkäykset muodostavat suurimman osan tietoturvahyökkäyksistä. Ne hyödyntävät tietojärjestelmiä erilaisilla viruksilla, vakoiluohjelmilla ja haittaohjelmilla, jotka varastavat ja manipuloivat tietoa, estävät yhteydet ja saattavat jopa vahingoittaa laitteita. (Andrea, Chrysostomou, & Hadjichristofi, 2015.)

Tietojenkalastelu eli phishing on yksi sovellushyökkäyksen muoto. Jagatic, Johnson, Jakobsson ja Menczer (2007) kuvailevat tietojenkalastelun olevan yksi käyttäjän manipuloinnin muoto, jossa hyökkääjä yrittää vilpillisesti saada arkaluonteista tietoa uhrilta esiintymällä luotettavana tahona. Erilaisia tietojenkalastelun muotoja on lukuisia ja ne hyödyntävät sekä teknisiä että sosiaalisia haavoittuvuuksia. (Jagatic ym., 2007.) Tietojenkalasteluhyökkäykset toteutetaan useimmiten sähköpostin tai kalastelusivustojen avulla (Andrea, Chrysostomou, & Hadjichristofi, 2015.)

Toinen tapa toteuttaa sovelluksiin kohdistuva hyökkäys on tehdä se haittaohjelmien (malicious software) avulla. Erilaisia haittaohjelmia ovat esimerkiksi virukset, troijan hevonen ja vakoiluohjelmat (Andrea, Chrysostomou, & Hadjichristofi, 2015). Hyökkäys tapahtuu levittämällä haitallista koodia esimerkiksi sähköpostien liitteenä tai ladattavien tiedostojen avulla (Deogirikar & Vidhate, 2017). Troijan hevonen on yksi esimerkki haittaohjelmista. Se ei ole virus mutta käyttäytyy joskus viruksen tavoin. Troijan hevonen toimii siten, että turvalliseksi naamioitu ohjelma käynnistää haitallisen toiminnon, kuten levittää viruksia tai matoja tai aiheuttaa muuta tuhoa järjestelmään. Troijan hevosen avulla voidaan tehdä myös tiedonhankintaa tai tietojen tuhoamista. Troijan hevonen -hyökkäyksiä on useita erilaisia, kuten tietojen lähettämistroijalainen ja tuhoava troijalainen. (Chaudhari & Patel, 2017.)

Tietojenkalastelun ja haittaohjelmien avulla voidaan toteuttaa myös tilin kaappaus (account hijacking), jossa hyökkääjä varastaa uhrin käyttäjätiedot ja pystyy tämän avulla kirjautumaan käyttäjän tileille (Kazim & Zhu, 2015). Näitä tilejä ovat esimerkiksi sähköpostitilit, sosiaalisen median tilit ja pilvipalveluiden tilit. Varastettujen tunnistetietojen avulla hyökkääjä pystyy pääsemään käsiksi käyttäjän tileihin liittyviin tietoihin, kuten sähköpostiviesteihin, yhteystietoihin, pilvipalveluihin tallennettuihin valokuviin, videoihin ja tiedostoihin ym. Sen lisäksi että hyökkääjä pystyy näkemään kaiken tileillä olevan tiedon, hyökkääjä pystyy myös väärentämään tietoja ja lähettämään tietoja eteenpäin muille haitallisille sivustoille. (Bamiah & Brohi, 2011; Kazim & Zhu, 2015.)

Haittaohjelmien avulla pystytään myös salakuuntelemaan älylaitteiden mikrofoneja. Sikder, Petracca, Aksu, Jaeger ja Uluagac (2018) toteavat, että yleisimmin näissä hyökkäyksissä tavoitellaan salasanoja, salausavaimia tai luottokorttitietoja. Salakuuntelu voidaan toteuttaa esimerkiksi älypuhelimen mikro-

fonia kuuntelemalla, kuten Soundcomber -haittaohjelma tekee. Toinen tapa hyödyntää laitteiden mikrofoneja on tehdä se ääniavustajan, kuten Applen Sirin tai Googlen Voice Searchin, avulla. Useimmat iot-laitteet sisältävät nykyään äänihakuohjelmiston, joten hyökkäyksen tekeminen on varsin helppoa. (Sikder ym., 2018.)

Yksi tapa toteuttaa haittaohjelmiin perustuva sovellushyökkäys on tehdä se haitallisen komentosarjan avulla. Tässä hyökkäyksessä tavoitteena on huijata yhdyskäytävää hallinnoiva käyttäjä suorittamaan haitallinen komentosarja, jolla koko järjestelmä voidaan kaataa tai tietoja varastaa (Andrea, Chrysostomou, & Hadjichristofi, 2015).

Lisäksi palvelunestohyökkäys on mahdollinen myös sovellustasolla. Hyökkääjä voi suorittaa hyökkäyksen sovellustasolla, jolloin hyökkäys kohdistuu kaikkiin verkon käyttäjiin. Tämänkaltainen hyökkäys voi estää käyttäjiä pääsemästä sovellustason palveluihin ja antaa hyökkääjälle täyden pääsyn tietokantoihin ja arkaluonteisiin tietoihin. (Andrea, Chrysostomou, & Hadjichristofi, 2015.)

3.2.4 Salaushyökkäykset

Salaushyökkäykset keskittyvät purkamaan salauksen, jota käytetään iot-järjestelmässä. Side channel -hyökkäys tarkoittaa hyökkäystä, jossa hyökkääjä käyttää hyödykseen salauslaitteiden tuottamaa tietoa. Tämä tieto ei ole täysin selväkielistä muttei myöskään salauskieltä, ja se voi sisältää tietoa esimerkiksi laitteen tehosta, ajasta, jonka laite tarvitsee tehtävän suorittamiseen sekä virheiden esiintymistiheydestä. Hyökkääjä käyttää näitä tietoja havaitakseen salausavaimen. Erilaisia side channel -hyökkäyksiä ovat muun muassa ajoitushyökkäykset, erilaiset tehon analyysit sekä vikojen analysointihyökkäykset. Ajoitushyökkäykset ovat riippuvaisia ajasta, jonka laite tarvitsee tehtävien suorittamiseen. Tiedot operointiajoista antavat hyökkääjälle vihjeitä käytetyistä salausmenetelmistä, sillä eri salausmenetelmät salaavat tiedon eri nopeuksilla. Tätä tietoa hyödyntämällä hyökkääjä pystyy saamaan selville käytetyt salausjärjestelmät ja purkamaan ne. (Deogirikar & Vidhate, 2017.)

Salausanalyysi -hyökkäyksen (cryptoanalysis attack) tarkoituksena on löytää salausavain ja purkaa järjestelmän salaus (Andrea, Chrysostomou, & Hadjichristofi, 2015). Hyökkääjä saa salausavaimen haltuunsa joko selkokielen tai salauskielen avulla. Tiedossa on ainakin neljä eri salausanalyysi -hyökkäystä. Ensimmäisessä hyökkääjä pääsee käsiksi salauskieleen ja purkaa salauskielen. Toisessa hyökkääjä tietää joitain kohtia salauskielestä selkokielenä ja pyrkii näiden kohtien avulla selvittämään loput kohdat salauskielestä. Kolmannessa hyökkäyksessä hyökkääjä pystyy kääntämään haluamansa selkokielen salauskieleksi ja käyttämään tätä avukseen salausavaimen selvittämisessä. Neljännessä hyökkäyksessä hyökkääjä saa haltuunsa haluamansa osan salauskielestä selkokielenä ja tätä tietoa hyödyntämällä pystyy selvittämään salausavaimen. (Deogirikar & Vidhate, 2017.)

Salaushyökkäys voidaan toteuttaa myös mies välissä -hyökkäyksenä. Tällöin hyökkääjä onnistuu asettumaan käyttäjien kommunikointikanavan väliin siten, että kaikki käyttäjien välinen kommunikointi kulkee hyökkääjän kautta. Käyttäjät voivat vaihtaa salausavaimia keskenään, jolloin hyökkääjä saa salausavaimet itselleen. Hyökkäyksen kohteeksi joutuneet käyttäjät eivät edes tiedä joutuneensa hyökkäyksen kohteiksi, vaan he luulevat kommunikoineensa keskenään. (Andrea, Chrysostomou, & Hadjichristofi, 2015.)

3.3 Yleisimmät älylaitteiden tietoturvauhkat

Tutkimuksessa toteutettavan haastattelun kannalta on tärkeää löytää esiteltyjen uhkien joukosta yleisimmät uhkat, joihin haastattelussa voidaan keskittyä. Älylaitteisiin kohdistuvia tietoturvauhkia on paljon, eikä olisi järkevää käsitellä niitä kaikkia haastattelussa. Lisäksi haastateltavien pitäisi pystyä sisäistämään saamansa tiedot eri hyökkäyksistä, jolloin on järkevintä pitäytyä muutamassa uhkassa. Näin ollen tässä tutkielmassa esitellyistä tietoturvauhkista on valittu muutama yleisin älylaitteisiin kohdistuva tietoturvauhka.

Sikder ym. (2018) toteavat tietojen vuotamisen esimerkiksi salakuuntelun avulla olevan yleisin iot-laitteisiin ja -järjestelmiin kohdistuva hyökkäys. Yleisimmin näissä hyökkäyksissä tavoitellaan salasanoja, salausavaimia tai luottokorttitietoja. Salakuuntelu voidaan toteuttaa esimerkiksi älypuhelimen mikrofonia kuuntelemalla, kuten Soundcomber -haittaohjelma tekee. (Sikder ym, 2018.) Schlegel ym. (2011) kuvailevat Soundcomberin tavoitteena olevan kerätä pieni määrä korkealaatuista yksityistä tietoa puhelimitse käydyistä keskusteluista ja siirtää tämä tieto haitalliselle taholle. Monet tahot, kuten pankit, kysyvät asiakkailtaan puhelun aluksi arkaluonteisia tietoja, kuten henkilötunnuksen tai osoitteen. Näin ollen Soundcomberin ei tarvitse nauhoittaa koko puhelua, vaan riittää että se nauhoittaa puheluiden alut. Soundcomberin avulla on myös mahdollista nauhoittaa vain tiettyihin numeroihin soitetut puhelut. Käyttäjällä ei yleensä ole mitään tietoa siitä, että hänen puheluitaan nauhoitetaan. (Schlegel ym., 2011.)

Toinen tapa hyödyntää laitteiden mikrofoneja on tehdä se ääniavustajan, kuten Applen Sirin tai Googlen Voice Searchin, avulla. Useimmat iot-laitteet sisältävät nykyään äänihakuohjelmiston, joten hyökkäyksen tekeminen on varsin helppoa. (Sikder ym., 2018.) Diao, Liu, Zhou ja Zhang (2014) esittelevät artikkelissaan kehittämäänsä äänenkaappaukseen soveltuvaa haittaohjelmaa nimeltä VoicEmployer. Hyökkäys tapahtuu siten, että haittaohjelman avulla laitteen ääniavustajalle voidaan antaa erilaisia komentoja, kuten ”Soita numeroon 12345678”, jossa kyseinen numero on haitallinen ja käyttäjää veloitetaan numeroon soittamisesta. Hyökkäyksen avulla voidaan myös saada monenlaista muutakin tietoa selville, esimerkiksi kysymällä ääniavustajalta ”Mikä on minun IP-osoitteeni?” tai ”Mikä on sijaintini?”, jolloin ääniavustaja kertoo vastaukset kysymyksiin ja hyökkääjä saa tällä tavoin kerättyä yksityistä tietoa käyttäjästä ja laitteesta. (Diao ym., 2014.)

Kazimin ja Zhun (2015) mukaan yleisimpinä älylaitteisiin ja erityisesti niiden tarjoamiin pilvipalveluihin liittyvinä uhkina voidaan pitää tietomurtoja, tietojen menetystä, tilin tai palvelun kaappausta sekä palvelunestohyökkäystä. Tietomurrot ja tietojen menetys voivat tapahtua esimerkiksi tietojenkalastelun avulla. Tietojenkalastelu voi tapahtua siten, että hyökkääjä esiintyy jonain luotettavana lähteenä ja pyrkii saamaan uhrinsa luovuttamaan arkaluonteisia tietoja tämän avulla (Chaudhry, Chaudry & Rittenhouse, 2016). Toinen tapa, joka saattaa aiheuttaa tietomurron tai tietojen menetyksen, on haittaohjelmien käyttäminen. Haittaohjelmaan perustuva hyökkäys tapahtuu levittämällä haitallista ohjelmaa esimerkiksi sähköpostin liitteessä tai ladattavien tiedostojen avulla (Deogirikar & Vidhate, 2017). Haittaohjelmien levittäminen tapahtuu usein käyttäjän manipuloinnin avulla, eli hyökkääjä esiintyy luotettavana lähteenä ja kehottaa uhria avaamaan haitallisen ohjelman koneellaan (Chaudhry, Chaudry ja Rittenhouse, 2016).

Tilin kaappauksessa hyökkääjä varastaa uhrin käyttäjätiedot ja pystyy tämän avulla kirjautumaan käyttäjän tileille (Kazim & Zhu, 2015). Myös tämä toteutetaan useimmiten tietojenkalastelua tai haittaohjelmia hyödyntäen. Varastetuilla tunnistetiedoilla hyökkääjä pystyy pääsemään käsiksi käyttäjän tileihin liittyviin tietoihin, kuten sähköposteihin, yhteystietoihin, pilvipalveluihin tallennettuihin valokuviin, videoihin ja tiedostoihin ym. Sen lisäksi että hyökkääjä pystyy näkemään kaiken tileillä olevan tiedon, hyökkääjä pystyy myös väärentämään tietoja ja lähettämään tietoja eteenpäin muille haitallisille sivustoille. (Bamiah & Brohi, 2011.)

Palvelunestohyökkäyksen tarkoituksena on estää oikeutetun käyttäjän pääsy verkkoon, muistiin, tietoihin tai muihin palveluihin. Palvelunestohyökkäykset ovat lisääntyneet vauhdilla viimeisen 5 vuoden aikana. (Kazim & Zhu, 2015.) Palvelunestohyökkäys voidaan toteuttaa esimerkiksi lähettämällä IoT-verkkoon niin paljon verkkoliikennettä, ettei verkko pysty käsittelemään sitä (Andrea, Chrysostomou, & Hadjichristofi, 2015). Hyökkäys kuluttaa laskennallista tehoa, muistia sekä kaistanleveyttä, joka aiheuttaa viivettä palveluihin tai joskus jopa koko palvelun kaatumisen (Kazim & Zhu, 2015). Yksi suurimmista uhkista, jonka esineiden internetin nopea leviäminen on aiheuttanut, ovat bottiverkot. Valtava määrä laitteita yhdistettynä heikkoon tietoturvaan ja valtavaan laskentatehoon tekevät älylaitteista täydellisiä välineitä voimakkaan palvelunestohyökkäyksen toteuttamiseen. Viime aikoina myös hyökkääjät ovat huomanneet, millaista tuhoa tämänkaltaisilla palvelunestohyökkäyksillä on mahdollista saada aikaan. (Habibi, Midi, Mudgerikar & Bertino, 2017.)

Erityisen ongelmallisen palvelunestohyökkäyksistä tekee se, että käyttäjä ei yleensä edes huomaa laitteensa olevan osana palvelunestohyökkäystä, sillä laite toimii normaaliin tapaan. Kun otetaan vielä huomioon se, kuinka paljon älylaitteita jo tällä hetkellä on ja kuinka paljon ne lisääntyvät älykkäiden kodinkoneiden myötä. on älylaitteilla mahdollista tehdä jo yhteiskunnalle haitallisia hyökkäyksiä. Esimerkiksi Vaarama (2019) esittelee artikkelissaan suomalaiseen terveydenhuoltoon kohdistuneen palvelunestohyökkäyksen, jonka avulla terveydenhuollon sivut saatiin kaatumaan. Esitellyssä tapauksessa ei vielä tapah-

tunut mitään peruuttamatonta ja hyökkäyksen epäiltiin olleen kiusantekoa, mutta tämä kertoo kuitenkin siitä, että palvelunestohyökkäyksen avulla on mahdollista lamauttaa esimerkiksi terveydenhuollon järjestelmiä.

Haastatteluun valittiin siis mukaan mikrofonin salakuuntelu, tietojenkalastelu, haittaohjelmat, tilin kaappaus sekä palvelunestohyökkäys. Näihin hyökkäyksiin päädyttiin siksi, että ne on mainittu kirjallisuudessa yleisimmiksi älylaitteisiin kohdistuviksi tietoturvauhkiksi. Lisäksi nämä hyökkäykset ovat sellaisia, jotka kohdistuvat erityisesti käyttäjiin ja heidän tietoihinsa.

4 TUTKIMUSMETODOLOGIA

Tutkimuksen empiirisen osuuden tarkoituksena on selvittää sitä, miten tietoisuus älylaitteisiin kohdistuvista tietoturvauhkista vaikuttaa älylaitteiden käyttöön. Ensiksi luvussa kerrotaan tutkimusmenetelmän valintaan liittyvistä syistä sekä tutkimuksen toteuttamisesta ja tiedonkeruusta. Tätä seuraa datan analysointi sekä tutkimuksen reliabiliteetin ja validiteetin arviointi.

4.1 Tutkimusmenetelmän valinta

Tutkimuksen tavoitteena on selvittää, miten tietoisuuden lisääntyminen älylaitteisiin kohdistuvista tietoturvahyökkäyksistä vaikuttaa käyttäjien haluun käyttää älylaitteita ja kokevatko käyttäjät tietonsa olevan turvassa. Tutkielman teoriaosuuden tutkimusmenetelmänä on käytetty kirjallisuuskatsausta ja empiirisessä osuudessa laadullista tapaustutkimusta. Laadullinen eli kvalitatiivinen tutkimus pyrkii kontekstuaalisuuteen, tulkintaan ja toimijoiden näkökulman ymmärtämiseen. Kvalitatiivisessa tutkimuksessa haastateltavan ja tutkijan nähdään olevan vuorovaikutuksessa. (Hirsjärvi & Hurme, 2008, 22-23.) Tutkija onkin tärkeässä roolissa haastattelun aikana, sillä tutkijan käyttäytyminen, ilmeet, eleet ja puhetyyli vaikuttavat siihen, miten haastateltava haluaa vastata kysymyksiin. Myös haastattelijan asennolla on väliä; jos haastattelija pystyy valitsemaan rennon asennon, esimerkiksi pitämällä kädet rentoina, auttaa se myös haastateltavaa rentoutumaan. (Hirsjärvi & Hurme, 2008, 119.) Lisäksi haastattelijalta vaaditaan taitoa ja kokemusta.

Kvalitatiivinen tutkimus soveltuu käyttäytymisen merkityksen ja sen kontekstin selvittämiseen. Kvalitatiivisen tutkimuksen avulla saadaan selville tutkittavien havainnot tilanteista ja saadaan mahdollisuus huomioida tutkittavien menneisyyten ja kehitykseen liittyviä tekijöitä. (Hirsjärvi & Hurme, 2008, 27.) Hirsjärvi, Remes ja Sajavaara (2009) toteavat kvalitatiivisen tutkimuksen soveltuvan todellisen elämän kuvaamiseen ja tutkimaan kohdetta mahdollisimman kokonaisvaltaisesti. Näin ollen kvalitatiivisen tutkimuksen tavoitteena ei ole

teorian tai hypoteesin testaaminen vaan kerätyn datan yksityiskohtainen tarkastelu. Kvalitatiivisen tutkimuksen tutkimusote on induktiivinen; se etenee tutkijan omista empiirisistä havainnoista, kuten litteroiduista haastatteluista, selitysmalleihin ja teoreettiseen pohdiskeluun (Hirsjärvi, Remes & Sajavaara, 2009, 266).

Tutkimusmenetelmistä on valittu tähän tutkimukseen tapaustutkimus, jolloin tarkastelun kohteena on yksi tai useampi tapaus, joihin tutkimus rajataan kohdistumaan. Esimerkkejä tapauksesta voivat olla yksilö, ryhmä tai organisaatio. Tapaustutkimuksella pyritään laadullisen tutkimuksen tavoin lisäämään tietoa tietystä ilmiöstä, pyrkimättä luomaan yleistettävyyksiä. (Eriksson & Koistinen, 2014.) Lisäksi Erikssonin ja Koistisen (2014) mukaan tapaustutkimus on syytä valita tutkimusmenetelmäksi silloin, jos tutkimuskohteena on jokin tämän ajan elävässä elämässä oleva ilmiö. Tässä tutkielmassa tehty tutkimus on tapaustutkimus siitä, miten tietoisuus älylaitteisiin kohdistuvista tietoturvauhkista vaikuttaa älylaitteiden käyttöön.

Tutkimuksen empiirisen osuuden data on kerätty puolistrukturoidulla teemahaastattelulla. Haastattelu on yleisimmin käytetty tiedonkeruumenetelmä laadullisissa tutkimuksissa (Hirsjärvi & Hurme, 2008, 34; Myers & Newman, 2007). Haastattelu on hyvin joustava tutkimusmenetelmä ja sopii siksi hyvin moniin erilaisiin tutkimustarkoituksiin. Haastattelussa ollaan suorassa vuorovaikutuksessa haastateltavan kanssa ja ei-kielelliset vihjeet, kuten eleet ja ilmeet, auttavat ymmärtämään vastauksia paremmin ja joskus jopa havaitsemaan uusia merkityksiä. Haastattelun avulla voidaan syventää saatavia tietoja, kuten pyytää haastateltavia perustelemaan mielipiteensä ja esittää lisäkysymyksiä. Haastatteluun tiedonkeruumenetelmänä liittyy myös haasteita. Haastatteluun liittyy esimerkiksi monia virhelähteitä, haastattelija voi vaikuttaa haastateltavan vastauksiin tai haastateltava saattaa antaa vain sosiaalisesti hyväksyttäviä vastauksia. (Hirsjärvi & Hurme, 2008, 34-35; Hirsjärvi, Remes & Sajavaara, 2009, 206.) Lisäksi haastatteluiden toteuttaminen vie aikaa ja haastatteluiden analysointi, tulkinta ja raportointi tuottaa ongelmia, sillä valmiita malleja ei ole (Hirsjärvi & Hurme, 2008, 34-35).

Puolistrukturoidussa haastattelussa kysymykset on laadittu etukäteen valmiiksi, mutta kysymysten järjestystä voidaan vaihdella ja valmiiden kysymysten lisäksi on mahdollista kysyä myös ennalta suunnittelemattomia kysymyksiä. Näin ollen haastateltavat saavat vastata hyvin vapaasti kysymyksiin ja haastattelijan on mahdollista kysyä tarkentavia kysymyksiä heiltä. Teemahaastattelu onkin lähempänä strukturoimatonta kuin strukturoitua haastattelua. Muissa puolistrukturoiduissa haastatteluissa kysymykset ja niiden muoto ovat kaikilla samat. (Hirsjärvi & Hurme, 2008, 47-48.)

Haastattelun aluksi haastattelijan tulee saada haastateltavan suostumus kerätyn aineiston käyttöön tutkimuksessa. Tämä kuitenkin aiheuttaa usein päänvaivaa tutkijoille Hirsjärven ja Hurmeen (2008, 20) mukaan, sillä liian tarkka tietämys tutkimuksen tavoitteista saattaa vinouttaa haastattelulla saatavia tuloksia tai muuttaa tutkittavan käyttäytymistä.

4.2 Tutkimuksen toteutus ja tiedonkeruu

Tutkielman empiirisen osuuden tutkimus toteutettiin siis kvalitatiivisena tutkimuksena ja tutkimuksen data kerättiin puolistrukturoitujen haastattelujen avulla. Näin ollen haastatteluissa käytettiin valmista haastattelurunkoa (liite 1), jonka mukaisesti kaikilta haastateltavilta kysyttiin samat kysymykset. Puolistrukturoitu haastattelu antaa kuitenkin mahdollisuuden esittää tarvittaessa selventäviä lisäkysymyksiä esimerkiksi tilanteessa, jossa haastateltava vastaa kysymykseen vain yhdellä sanalla avaamatta vastaustaan sen enempää. Tällöin haastattelijan tulee huolehtia siitä, etteivät esitetyt lisäkysymykset ole johdattelevia, jotta ne eivät vaikuta tutkimuksen luotettavuuteen.

Tutkimuksessa käytettyjen haastattelujen rakenne oli seuraavanlainen: haastattelun aluksi kartoitetaan sitä, millaisia älylaitteita haastateltavalla on käytössään, onko haastateltava tietoinen älylaitteisiin kohdistuvista tietoturvauhkista ja millaisia tietoturvaa parantavia toimia haastateltava on tehnyt. Lisäksi selvitetään, onko haastateltava kuinka huolissaan omasta tietoturvastaan. Tämän jälkeen haastateltaville tullaan esittelemään viisi tutkielman teoriaosuudessa yleisimmiksi todettua älylaitteisiin kohdistuvaa tietoturvauhkaa. Uhkat tullaan esittelemään pääpiirteissään ja siten yksinkertaisesti, että tavallinen käyttäjä pystyy ne ymmärtämään. Lisäksi haastateltaville tullaan kertomaan siitä, millaiset tiedot ovat vaarassa esiteltyjen uhkien vuoksi. Uhkien esittelyä varten jokaisesta uhkasta on luotu lyhyt esittelypaperi, joiden avulla haastateltava voi lukea omaan tahtiinsa viidestä uhkasta.

Kun haastateltava on saanut luettua paperit ja kokee sisäistäneensä asiat, siirrytään haastattelun seuraavaan vaiheeseen, jossa haastateltavia pyydetään arvioimaan sitä, aikovatko he muuttaa älylaitteiden käyttöä tulevaisuudessa, kun he tietävät enemmän niihin liittyvistä tietoturvauhkista. Haastateltavilta kysytään myös uudestaan sitä, kuinka huolissaan he ovat omasta tietoturvastaan nyt. Lisäksi haastateltavia pyydetään laittamaan esitellyt uhkat uhkaavuusjärjestykseen uhkaavimmasta vähiten uhkaavaan. Haastateltavia pyydetään myös perustelemaan järjestystä. Haastattelun lopuksi haastateltavilta vielä kysytään, kokevatko he omaavansa riittävän tietotaidon pitääkseen tietonsa turvassa, sekä kysytään sitä, pitäisikö tietoturvauhkista puhua enemmän.

Kvalitatiivisessa tutkimuksessa harvemmin valitaan otosta, vaan yleensä otetaan harkinnanvarainen näyte. Tällä tarkoitetaan sitä, että haastattelija itse valitsee haastateltavat eikä haastateltavia valita satunnaisotoksella. Tämä siitä syystä, että kvalitatiivisella tutkimuksella pyritään ymmärtämään jotakin tapahtumaa syvemmin, ei tekemään tilastollisia yleistyksiä. (Hirsjärvi & Hurme, 2008, 58-59.) Näin ollen haastateltaviksi on valittu tavallisia älylaitteiden käyttäjiä, joilla ei ole erityistä tietämystä älylaitteiden tietoturvauhkista. Tavalliset käyttäjät valikoituivat haastateltaviksi siitä syystä, että heidän kohdallaan on helpompi huomata, millaisia reaktioita lisääntyvä tietoisuus älylaitteiden tietoturvauhkista aiheuttaa ja millaisia toimia käyttäjät aikovat toteuttaa tämän myötä. Jos tutkimuksessa olisi haastateltu ainoastaan tietotekniikan ammattilai-

sia, olisi heillä luultavimmin ollut jo tietämystä tietoturvauhkista, eikä tutkimus olisi tarjonnut uutta tietoa. Tutkimukseen on kuitenkin pyritty saamaan mukaan myös muutama IT-alan ammattilainen, jotta heidän vastauksiaan voidaan verrata tavallisien käyttäjien vastauksiin. Mielenkiintoista tässä on nähdä se, miten paljon IT-alan ammattilaisilla on tietämystä tietoturvauhkista sekä se, ovatko IT-alan ammattilaiset esimerkiksi suojautuneet tietoturvauhkilta paremmin kuin tavalliset käyttäjät.

Haastattelut tulee aina suunnitella huolellisesti etukäteen. Tutkijan tulee päättää ainakin haastattelujen ajankohdat, paikat, likimääräiset kestot sekä haastatteluun käytettävä välineistö. Tutkijan pitää esimerkiksi suunnitella, missä haastattelut toteutetaan ja miten haastattelu tullaan tallentamaan. Haastattelupaikka saattaa vaikuttaa vastausten laatuun esimerkiksi tapauksessa, jossa koehenkilöitä haastatellaan työpaikkaan liittyvistä asioista työpaikalla. Tällöin koehenkilöt eivät välttämättä uskalla vastata täysin rehellisesti kysymyksiin. (Hirsjärvi & Hurme, 2008, 126-127.) Tässä tutkimuksessa haastatteluiden pitopaikalla ei ole vaikutusta vastausten laatuun, joten haastattelut voidaan pitää paikassa, joka sopii haastateltaville parhaiten. Haastattelupaikan pitää kuitenkin olla riittävän rauhallinen, jotta haastateltavat pystyvät keskittymään haastatteluun kunnolla eikä paikassa saa olla liikaa taustahälyä, joka saattaa heikentää tallennuksen laatua. Näin ollen tämän tutkimuksen haastattelut pidettiin vaihtelevasti joko haastattelijan kotona, haastateltavan kotona, haastateltavan työpaikalla tai Skype-videopuhelun avulla. Haastattelujen aikaan haastattelupaikassa oli vain haastattelija sekä haastateltava. Lisäksi haastattelupaikka oli hiljainen, eikä näin ollen taustahäly vaikuttanut haastatteluihin.

Haastattelut pyrittiin myös pitämään mahdollisimman rauhallisina, ja haastateltavien annettiin vastata kysymyksiin omaan tahtiinsa. Haastateltaviksi päätyi lopulta 14 henkilöä eli H1 28-vuotias mies, H2 50-vuotias nainen, H3 37-vuotias IT-alalla työskentelevä mies, H4 49-vuotias mies, H5 40-vuotias IT-alalla työskentelevä mies, H6 40-vuotias mies, H7 62-vuotias nainen, H8 54-vuotias nainen, H9 59-vuotias nainen, H10 21-vuotias nainen, H11 20-vuotias nainen, H12 28-vuotias nainen, H13 44-vuotias nainen ja H14 27-vuotias nainen.

4.3 Datan analysointi

Haastattelussa kerättävän aineiston analysointi alkaa jo haastattelun aikana, jolloin haastattelija tekee havaintoja haastateltavista ja esille tulleista asioista. Jotta haastatteluilla saatavaa dataa voitaisiin analysoida, tulee haastattelut tallentaa ja tämän jälkeen litteroida eli kirjoittaa tekstiksi. Litterointi tulisi tehdä mahdollisimman pian haastattelun jälkeen. Tämä siitä syystä, että haastattelun ollessa vielä tuoreessa muistissa, on helpompi välttää mahdollisia epäselvyyksiä ja täydentää tai selventää puuttuvia tietoja. (Hirsjärvi & Hurme, 2008, 135.) Tässä tutkimuksessa litterointi tehtiin joko haastattelupäivänä tai haastattelua seuraavana päivänä. Haastattelut nauhoitettiin puhelimen nauhoitusohjelman

avulla. Haastatteluiden aluksi haastateltavilta kysyttiin lupa haastattelun nauhoittamiseen.

Haastatteluiden litterointi voidaan toteuttaa usealla eri tavalla. Hirsjärven ja Hurmeen (2008, 138) mukaan koko haastattelu voidaan kirjoittaa sanatarkasti auki tai aineistosta voidaan valikoida litteroitavaksi esimerkiksi vain teemaalueet tai haastateltavien vastaukset. Aineiston litteroinnin tarkkuudesta ei ole olemassa yleispätevää ohjetta ja litteroinnin tarkkuus riippuu tutkimustehtävästä. Sanasta sanaan litteroinnin kirjoittaminen on työlästä ja aikaa vievää. Erityisesti keskusteluanalyysiä käyttävät tutkijat litteroivat haastattelut pikkutarkasti aina taukoja, huokauksia ja jopa äänenpainoja myöten. (Hirsjärvi & Hurme, 2008, 138-140.) Tässä tutkielmassa päädyttiin litteroimaan haastattelut kokonaisuudessaan, mutta haastatteluista litteroitiin ainoastaan haastateltavien puheenvuorot täysin, haastattelijan puheenvuoroista litteroitiin vain tarvittavat osuudet eli kysymykset sekä mahdolliset lisäkysymykset. Tutkimuksen tavoitteen kannalta ei ole tärkeää tehdä keskusteluanalyysiä, joten litterointiin otettiin mukaan vain haastateltavien puheet ilman äänenpainojen, taukojen ja huokausten litterointia.

Litteroitua aineistoa ei voi analysoida, jos sitä ei ensiksi lue. Aineisto tulee lukea huolella ja useita kertoja. Aineiston analysointi kvalitatiivisessa tutkimuksessa on hyvin pitkälti tutkijan omaa ajattelua ja aineiston erittelyä ja luokittelua. (Hirsjärvi & Hurme, 2008, 143.) Teemahaastattelun aineiston analysointi voidaan toteuttaa monella eri tavalla, esimerkiksi teemoittelemalla, tyypittelemällä ja laskemalla. (Hirsjärvi & Hurme, 2008, 172-176.) Tässä tutkimuksessa tulokset analysoitiin teemoittelun avulla.

Hirsjärvi ja Hurme (2008, 173) toteavat teemoittelun tarkoittavan sellaisia aineiston analysointivaiheessa ilmi tulevia piirteitä, jotka ovat yhteisiä useille haastateltaville. Teemoittelussa haastatteluista saatuja vastauksia vertaillaan, pilkotaan pienempiin osiin, käsitteellistetään ja etsitään säännönmukaisuuksia, joista voidaan muodostaa teemoja (Ritchie & Spencer, 2002).

4.4 Tutkimuksen reliabiliteetti ja validiteetti

Kaikissa tutkimuksissa pyritään välttämään virheiden syntyminen ja tämän vuoksi tutkimuksissa arvioidaan tutkimuksen luotettavuutta. Luotettavuutta voidaan arvioida monin eri tavoin, mutta käytetyimmät luotettavuuden mittarit ovat reliabiliteetti ja validiteetti. (Hirsjärvi, Remes & Sajavaara, 2009, 231.)

Reliabiliteetilla tarkoitetaan mittaustulosten toistettavuutta eli tutkimus ei saisi antaa sattumanvaraisia tuloksia. Reliabiliteetti voidaan todeta monin eri tavoin, esimerkiksi jos kaksi tutkijaa päätyy samanlaiseen tulokseen, voidaan tutkimusta pitää reliaabelina. Toisena esimerkkinä on tilanne, jossa samaa henkilöä tutkitaan eri tutkimuskerroilla ja tullaan samaan tulokseen, jolloin kyseinen tulos on myös reliaabeli. (Hirsjärvi, Remes & Sajavaara, 2009, 231.)

Validius puolestaan tarkoittaa tutkimuksen pätevyyttä eli valitun tutkimusmenetelmän kykyä mitata juuri sitä, mitä sen pitääkin. Tutkijan tulee valita tutkimukselleen parhaiten sopiva tutkimusmenetelmä, mutta validiteettiin liittyy muutakin. Valitut mittarit tai menetelmät eivät aina vastaa sitä todellisuutta, mitä tutkija ajattelee niiden tutkivan. Tästä esimerkkinä toimii tilanne, jossa kyselylomakkeen kysymyksiin on saatu paljon vastauksia, mutta vastaajat ovat saattaneet käsittää kysymykset aivan väärin, jolloin tutkimuksella saadut tulokset eivät välttämättä olekaan päteviä. Valittu tutkimustapa eli kyselylomake aiheuttaa siis tuloksiin virhettä. (Hirsjärvi, Remes & Sajavaara, 2009, 231-232.)

Reliabiliteetin ja validiteetin nähdään usein kuuluvan kvantitatiiviseen tutkimukseen, mutta kaikkien tutkimusten luotettavuutta ja pätevyyttä pitäisi pystyä arvioimaan jollain tavoin. Kuitenkin monet reliabiliteetin ja validiteetin arviointiin kehitetyt mittarit ovat soveltumattomia kvalitatiivisen tutkimuksen arviointiin, ovathan esimerkiksi ihmistä ja kulttuuria koskevat kuvaukset aina ainutlaatuisia. (Hirsjärvi, Remes & Sajavaara, 2009, 232.)

Laadullisissa tutkimuksissa on usein ratkaistu tämä ongelma siten, että tutkija kertoo mahdollisimman tarkasti, mitä hän on tutkimuksessa tehnyt ja miten saatuihin tuloksiin on päädytty. Tutkijan tarkka selostus tutkimuksen toteuttamisesta kohentaa tutkimuksen luotettavuutta ja tarkkuus koskeekin tutkimuksen kaikkia vaiheita. Tutkijan on siis syytä muistaa kertoa kaikissa tutkimuksen vaiheissa tarkasti siitä, mitä hän on tehnyt. Esimerkkeinä haastattelijan tulisi kertoa haastatteluiden olosuhteista ja paikoista, haastatteluihin käytetty aika, mahdolliset häiriötekijät sekä haastattelijan itsearviointi tilanteesta ja mahdollisista virhetulkinnoista. Lisäksi kun tutkija esittää tulkintoja, tulee hänen kertoa, mihin tulkinnat perustuvat. Laadullisessa tutkimuksessa tulkintojen perusteluna toimii se, että tutkija lisää tulkintojensa oheen haastatteluotteita. (Hirsjärvi, Remes & Sajavaara, 2009, 232.)

Tässä tutkielmassa reliabiliteettia ja validiteettia on toteutettu siten, että tutkimuksen eri vaiheet on pyritty kuvaamaan mahdollisimman tarkasti tässä tutkielmassa. Haastattelut nauhoitettiin ja ne litteroitiin huolellisesti. Haastattelut pidettiin rauhallisissa ja hiljaisissa tiloissa, joissa ei ollut haastattelijan ja haastateltavan lisäksi muita henkilöitä. Haastateltaville annettiin myös aikaa vastata kysymyksiin rauhassa. Kysymykset olivat samat jokaiselle haastateltavalle ja kysymykset oli muotoiltu niin, etteivät ne johdattelisi haastateltavia. Lisäksi tutkimuksen tuloksia esiteltäessä tulkintojen oheen on liitetty haastatteluotteita, jotka osoittavat, että tehdyt tulkinnat perustuvat saatuihin tuloksiin.

5 TUTKIMUKSEN TULOKSET

Tässä luvussa käydään läpi tutkimuksella saadut tulokset. Haastatteluiden avulla selvitettiin sitä, kuinka tietoisia käyttäjät ovat älylaitteisiin kohdistuvista tietoturvauhkista, mitä ajatuksia uhkat herättävät käyttäjissä ja miten käyttäjät aikovat jatkaa älylaitteiden käyttöä. Ensiksi tässä luvussa käydään läpi käyttäjien tietämys älylaitteisiin kohdistuvista tietoturvauhkista, käyttäjien tekemät tietoturvaa parantavat toimet sekä käyttäjien kokemus oman tietoturvansa tasosta. Lopuksi esitellään haastateltavien reaktiot esiteltyihin uhkiin ja se, miten tietoisuus älylaitteisiin kohdistuvista tietoturvauhkista vaikuttaa älylaitteiden käyttöön.

5.1 Käyttäjien tietämys tietoturvauhkista

Haastatteluissa tuli ilmi se, että kaikki haastateltavat tietävät tietoturvauhkien olemassaolon. Tietoturvauhkia ei kuitenkaan välttämättä osata nimetä tai kuvailla juuri mitenkään. Osa haastateltavista sanoivat suoraan, etteivät he osaa nimetä uhkia.

> ”No siis käytännössä perus virukset, muista nyt ei oo sillein tietookaan, että en oo perehtyny.” (H6)

> ”No en minä, siis on tämmösiä varmaan mut emmä tiiä minkälaisia.” (H9)

> ”No, enhän mä mitään muuta tiiä kun mitä noista lehistä lukee ja et varmaan vähän semmonen fiilis tulee siinä että pelotellaan, mut emmä oo ainakaan minkään hyökkäyksen kohteeksi joutunut, että niin. Kyllä se varmasti ihan vakava asia on ja tärkee, mutta ei sitä ehkä osaa ihan sillein, minä ainakaan ymmärtää tota, enkä osaa pelätäkkään mutta tuota, niin. No kyllähän sitä tänä päivänä voi tapahtua ihan mitä vaan.” (H8)

Moni kuitenkin osasi nimetä ainakin muutamia erilaisia uhkia.

> ”No semmosia että, toisten niinkun, tai ihmisten tietoja niinkun kurkitaan, että jos jotenkin se hakkeri tai joku saa tietää niinkun mun salasanat tai jotain niin sehän pääsee sitten niillä tunnuksilla kattoon vaikka mun potilastietoja jos vaikka mun pankkitunnukset joutuis vääriin käsiin tai sitten niinkun, sit aina noihin pankkeihin paljon niitä tapahtuu, minusta niitä, eihän ne saa ehkä ihmeellisemmin tietää mutta niihin ainakin yritetään niin kun, ja sit varmaan näihin kotikoneisiin ja kotitietokoneisiin jos ei oo niitä tietoturvaohjelmia niin minusta varmaan niihin voivat hyökätä.” (H2)

> ”No tuota ihan voi olla tämmöisiä jos on kyseessä kännykkä niin siihenhän voi tulla tota tietysti ihan sähköpostien kautta voi tulla hyökkäyksiä, ja sitten voi tietysti olla että sä menet jollekin sivustolle jossa sä avaat jonkinlaisen tiedoston, siitä voi tulla, ja sitten nämä, mulla on tuo reititinkin tuossa, että jos mulla ei olis tuossa salasanaakaan niin siihen on mahdollista ulkopuolisenkin tulla ja iskeä sitä kautta kaikkiin laitteisiin mitkä mulla on yhteydessä tuohon reitittimeen. Tällaisia nytten pääpiirteittäin tiiän, en sitten mitään yksityiskohtaisempaa tiiä.” (H1)

> ”No ainakin, no just sillein et ne voidaan kaapata periaatteessa, joku muu voi periaatteessa käyttää sun tietokonetta tai sitten voi niin kun, saaha sieltä tietoja just, salasanoja ja muita. No meillä on se Google Home niin periaatteessa et jos sen joku hakkeroi niin sit voi kuunnella puhetta koko ajan.” (H12)

Parhaiten haastateltavien tiedossa älylaitteisiin kohdistuvista tietoturvauhkista ovat virukset, käyttäjätunnusten sekä tilien kaappaukset ja tietojenkalastelu. Sen sijaan IT-alalla työskentelevät osaavat nimetä huomattavasti kattavammin erilaisia älylaitteisiin liittyviä tietoturvauhkia.

> ”No vaikka mitä, että esimerkiks Wifin kautta voi kuunnella sitä dataa aika helposti, sitten tota tämmöset valheelliset nettisivut, jotka on tehty näyttämään oikeelta voi ottaa käyttäjätunnuksia ja sitten esim SQL injektiot niin tota datan hallintaa vaikka myös. Itse pyöritän nettisivuja ja siellä on serveri niin sieltä voidaan yrittää saada tietoa sitä kautta. Sitten ihan hakkerointi, kuten force, eli yritetään arvata salasanaa laskemalla ja tämmösiä.” (H3)

> ”No tietysti käyttäjän urkinta, ja sitten tietysti virukset, takaportit, ja tota, no siinä ne varmaan suurin osa on että tota, no joo, mennään nyt niillä alkuun, monen näköistä.” (H5)

Suurin osa haastateltavista osaa nimetä tietoturvahyökkäyksien kohteiksi lähinnä tietokoneet, tabletit ja älypuhelimet, mutta esimerkiksi älykelloja ja muita älykkäitä kodinkoneita ei nähdä alttiiksi hyökkäyksille. Osa haastateltavista ajattelee tietoturvauhkien kohdistuvan yksinomaan tietokoneisiin eikä esimerkiksi älypuhelimien nähdä olevan uhattuina.

> ”No älypuhelimiin ja tuota niin tietokoneisiin.” (H4)

> ”Kyllä mä nyt luulisin että ne ois enemmän puhelimeen ja sitten tablettiin tai tietokoneeseen.” (H9)

> ”No läppäri käytännössä.” (H6)

”Tietokoneisiin etupäässä.” (H2)

Kysyttäessä haastateltavilta, millaiset tiedot hyökkäyksissä ovat uhattuina, 12 haastateltavaa vastasi ensimmäisenä henkilötiedot. Henkilötietojen lisäksi yleisiä vastauksia olivat erityisesti pankkitunnukset ja käyttäjätunnukset esimerkiksi sähköpostiin.

”No henkilötiedot, ne ja ihmisten omaisuus.” (H6)

”Varmaan henkilötietoja, henkilötunnukset varmaan on semmoset.” (H9)

”No varmaan ihan just omat henkilötiedotkin.” (H10)

”No henkilötiedot, kaikki niin kun maksutiedot, pankkikorttien numerot ja tilitiedot, mitäs muuta siellä vois olla… Melkein mikä vaan, missä sä oot töissä, mitä sä oot tehnyt netissä, ja onhan siinä siis sitten varsinkin jos sulla on kamera kännykässä tai sit niin kun tietokoneessa niin nehän voi senkin kaapata ja sit saa kuvaa, niin kun livekuvaa susta, niin tota siis kaikki tämmönen, mitä sä teet siinä, miltä sä näytät, onko sulla likanen paita päällä, siis kaikki tämmöset, hyvin paljon.” (H14)

”Nämä, ne voi mennä niin kun pankkiohjelmassa tilille, vievät rahat, sitten ne voi käyttää henkilötietoja mihin lie, mistä mä tiiän, ihan mihin tahansa kun ne osaa kuitenkin sen, ne nyt on ne mitkä nyt mieleen tulee.” (H7)

5.2 Kokemus tietoturvan tasosta

Kun haastattelun aluksi oli saatu kartoitettua käyttäjien nykyinen tietämys tietoturvauhkista, siirryttiin selvittämään sitä, millä tasolla käyttäjät kokevat oman tietoturvansa olevan. Ensiksi haastateltavilta kysyttiin, kuinka huolestuneita he kokevat olevansa omasta tietoturvastaan ja ovatko heidän tietonsa turvassa. Tämän kysymyksen vastaukset erosivat jo selkeästi toisistaan ja vastaukset vaihtelivat ääripäästä toiseen; osa haastateltavista koki tietojensa olevan turvassa omien toimiensa ansiosta, osa puolestaan olivat hyvinkin huolestuneita omasta tietoturvastaan.

”Ei, ei ole turvassa, että mulla ei oo riittävää viruksentorjuntajärjestelmää, mulla on pankkitoiminnot suojattu (F-securella), että niihin mä oon ottanu viruksentorjuntaohjelman mutta, ne pankkitoiminnot on musta niitä tärkeimpiä juttuja mitä ylipäätänsä mä tietokoneella teen, niin ne on suojattu mutta kyllä mä olen huolestunut noin niin kuin jos liikkuu ettimässä vaikka, ettimässä jotain tietoo niin saattaa virus ollakin siinä esimerkiks tulee, se on ihan ilkeyksissään tehtyjä viruksia, jotka on tehty haitaks vaan, niistä ei oo mitään hyötyä sille tekijälle mutta ne saa jotain mielihyvää siitä.” (H4)

”Tällä hetkellä kyllä koen, koska oon ite varovainen.” (H1)

> ”No en mä osaa olla kun, jos mä aattelen et jos mä vähänkään selväpäisenä pysyn niin enhän mä anna mitään tietoa mihinkään niin en mä sillon koe kauheen uhattuna olevani sitten.” (H8)

> ”En oo hirveen huolestunut, kyl mä pääsääntösesti oletan että ne on turvassa.” (H6)

Seuraavaksi haastateltavilta kysyttiin, ovatko he tehneet joitain tietoturvaa parantavia toimia ja jos ovat, millaisia. Jälleen vastaukset erosivat hyvinkin voimakkaasti, osa vastaajista kertoi, ettei ole tehnyt oikeastaan mitään tietoturvaa parantavia toimia koska tarvittava tietotaito puuttuu. Osa taas osasi nimetä useitakin toimia, joilla he ovat parantaneet omaa tietoturvaansa.

> ”Tietokoneessa on virustorjunnat ynnä muut nämä palomuurit ja semmoset ja kyllä ne on tossa puhelimessakin.” (H7)

> ”Itse asiassa en oo tehny, multa puuttuu se tietotaito siihen. Ilmeisesti netistä sais esimerkiks ilmaisia viruksentorjuntaohjelmia mutta mä en osaa asentaa niitä.” (H4)

> ”—jos selaa nettiä semmosilla sivuilla joita en käytä normaalisti niin mä käytän esimerkiks Kali Linuxia, joka on tietoturvatestaajien käytössä. Ja en, älylaitteilla esim noilla tableteilla tai puhelimilla en lataa niitä uusimpia sovelluksia mitä tulee kaupasta että sitten vasta kun ne on arvosteltu jossakin luotettavalla sivulla.” (H3)

> ”No en.” (H8)

Vastauksista tuli ilmi myös se, että osa haastateltavista kokee tietojensa olevan turvassa, vaikkei ole tehnyt mitään tietoturvaa parantavia toimia. Esimerkiksi H8 sanoi tietojensa olevan turvassa, koska hän ei jaa tietojaan mihinkään epäilyttäviin paikkoihin ja näin ollen hän ei myöskään kokenut tarvitsevansa mitään tietoturvaa parantavia toimia. Lisäksi useampikin haastateltava (H2, H4 ja H7) ajatteli, ettei ketään kiinnosta heidän tietonsa eikä heidän tarvitse tämän vuoksi olla erityisen huolestuneita tietoturvahyökkäyksistä. Tähän liittyy jo aiemmin esitelty TTAT eli teknologian uhkien välttämisteoria, jonka mukaan käyttäjät saattavat luoda virheellisiä havaintoja ympäristöstään tekemättä mitään muutoksia siihen. Käyttäjä voi esimerkiksi ajatella, ettei uhka kohdistu häneen tai ettei kukaan ole kiinnostunut hänen tiedoistaan. (Liang & Xue, 2009.) Näin ollen käyttäjä kuvittelee tietojensa olevan turvassa eikä koe tarvetta tehdä tietoturvaa parantavia toimia, joka kuitenkin altistaa käyttäjän suuremmalla todennäköisyydellä tietoturvauhkille. Samaan aiheeseen liittyy myös käyttäjillä oleva yleinen uskomus siitä, että omalla varovaisuudella voi välttää kaikki tietoturvauhkat. Tämä ei kuitenkaan enää nykyään pidä paikkaansa, kun tietoturvahyökkäykset jatkuvasti kehittyvät yhä vaikeammin havaittaviksi.

> ” No kyllä ne on turvassa jos ne niin kun mun takana on.” (H8)

Seuraavaksi haastateltavia pyydettiin arvioimaan asteikolla 1-10 kuinka turvassa kokee omien tietojensa olevan, kun numero 1 tarkoittaa että tiedot eivät ole ollenkaan turvassa ja 10 tarkoittaa tietojen olevan täysin turvassa. Seuraavassa

taulukossa (taulukko 2) on esitetty haastateltavien numerovastaukset tähän kysymykseen.

TAULUKKO 2 Kuinka turvassa haastateltavat kokevat tietojensa olevan

Haastateltava	Arvio, kuinka turvassa tiedot ovat asteikolla 1-10
H1	9
H2	7
H3	5
H4	6
H5	8
H6	8
H7	8
H8	8
H9	9
H10	7
H11	8
H12	7
H13	8
H14	8

Taulukosta huomataan, että haastateltavat ovat yleisesti ottaen varsin luottavaisia oman tietoturvansa tasoon. Yleisin vastaus on 8 ja keskiarvo vastauksista on 7,57. Ainoastaan yksi haastateltava arvioi tietoturvansa tasoksi 5 ja yksi 6. Alhaisimman arvion, eli arvosanan 5, omalle tietoturvalleen antanut haastateltava eli H3 on itse IT-alalla töissä ja hän oli tehnyt haastateltavista eniten tietoturvaa parantavia toimia. Siltikin hän arvioi tietoturvansa tason kaikista huonoimmaksi.

5.3 Reaktiot esiteltyihin uhkiin

Haastattelun seuraavassa vaiheessa haastateltaville esiteltiin viisi erilaista kirjallisuudessa yleisimmiksi nimitettyä tietoturvauhkaa. Nämä olivat tietojenkalastelu, mikrofonin salakuuntelu, haittaohjelmat, tilin kaappaus sekä palvelunestohyökkäys. Uhkat esiteltiin pääpiirteittään ja haastateltavat saivat rauhassa lukea uhkista tehdyt tiivistelmät. Tämän jälkeen haastateltavilta kysyttiin ensimmäiseksi sitä, millaisia ajatuksia esitellyt uhkat herättivät. Haastateltavien vastaukset vaihtelivat suuresti, osa koki esitellyt uhkat hyvinkin pelottaviksi, kun taas toiset olivat jo ennestään tietoisia esitellyistä uhkista eivätkä uhkat herättäneet heissä sen suurempia tunteita.

> ”No aikamoista pelkoa.” (H2)

> ”No siis ihan tuttua kauraa, näistä lukee lehessä paljon ja tuota, ei herätä mitään uutta mitä en tietäis.” (H6)

> ”No ne on kaikki semmosia mitä niin kun on kyllä tiedostanut mutta ei niitä sillein aina tuu aateltua, mutta on sillein, oon kuullut.” (H12)

> ”No huolestuttavia että kaikkiin tota kodinkoneisiinkin pääsee tuota niin hakkerit tuollasia ilkivaltaisia viruksia (laittamaan) ja pääsee kuuntelemaan ehkä puheluita ja muita että tosi huolestunut olin kun luin ton että ei tuu joka päivä ees mieleenkään tommoset asiat että tota, noi on tosi ovelia, en tiiä syytä sitten mistä johtuu että näitä haittaohjelmia ja tämmösiä on näin paljon, että ei ollut hyvä.” (H4)

Seuraavaksi haastateltavilta kysyttiin, kuinka huolestuneita he kokevat olevansa omasta tietoturvastaan nyt. Ensiksi haastateltavia pyydettiin vapaasti kertomaan omasta tietoturvansa tasosta nyt kun heille on esitelty erilaisia uhkia. Jälleen kerran vastauksissa esiintyi hajontaa ja osa haastateltavista koki tietojensa olevan alttiimpia erilaisille hyökkäyksille, kun taas toiset pitivät tietoturvansa tasoa edelleen samana.

> ”No, en sen huolestuneempi kun äskenkään, että kyllä mä mielestäni pidän siitä hyvää huolta.” (H5)

> ”No sillein että nehän koko ajan varmaan tulee uusia juttuja, että varmaan kun mennään eteenpäin niin varmaan tuun olemaan jossain vaiheessa paljon enemmän huolestunut siitä kun nytten.” (H9)

> ”Kyllä se siis joo, kyllä mä ehkä vähän niin kun huolestuneempi oon kun tää niin kun herätteli tavallaan nää kaikki tiedot mitä tässä oli niin tota, vähän huolestuneempi, en nyt mitenkään hirveän huolestunut edelleenkään mut sillein jonkin verran.” (H14)

Vastauksissa korostui useammankin haastateltavan kohdalla (H5, H6, H11, H13) luotto omiin kykyihin pitää tiedot turvassa. Tämän jälkeen haastateltavia pyydettiin arvioimaan uudestaan oman tietoturvansa tasoa asteikolla 1-10, jossa 1 tarkoittaa että tiedot eivät ole ollenkaan turvassa, 10 tarkoittaa tietojen olevan täysin turvassa. Nämä vastaukset on koottu seuraavaksi esitettävään taulukkoon (taulukko 3). Taulukon toisessa sarakkeessa olevat numerot ovat samat kuin taulukossa 2 eli haastateltavien arviot oman tietoturvan tasosta ennen kuin heille esiteltiin yleisimpiä uhkia, ja kolmannen sarakkeen numerot kertovat haastateltavien arvion oman tietoturvan tasosta uhkien esittelyn jälkeen.

TAULUKKO 3 Kuinka turvassa haastateltavien tiedot ovat ennen ja jälkeen tietoturvauhkien esittelyä

Haastateltava	Arvio ennen uhkien esittelyä	Arvio uhkien esittelyn jälkeen
H1	9	5
H2	7	4
H3	5	5
H4	6	5
H5	8	8
H6	8	8
H7	8	8
H8	8	8
H9	9	9
H10	7	6
H11	8	8
H12	7	7
H13	8	8
H14	8	6

Taulukosta huomataan, että suurin osa numeroista on pysynyt samana eli haastateltavat eivät koe esiteltyjen uhkien vaikuttaneen heidän tietoturvansa tasoon. Haastateltavista 5 (H1, H2, H4, H10 ja H14) koki tietoturvansa laskeneen esiteltyjen uhkien myötä. Suurimmat laskut tietoturvansa tasossa kokivat H1, jonka arvio putosi numerosta 9 numeroon 5, sekä H2, jonka arvio putosi numerosta 7 numeroon 4.

Seuraavaksi haastateltavilta tiedusteltiin sitä, aikovatko he muuttaa älylaitteiden käyttöä jollain tavalla. Vastaukset olivat keskenään hyvin samansuuntaisia eli haastateltavat aikovat jatkossakin käyttää älylaitteita samaan tapaan kuin tähänkin asti.

> ”Kyllä se taitaa jokseenkin samalla tavalla mennä eteenpäin, tietysti tossa vaihtelee esimerkiksi kokoajan salasanoja vahvempiin ja aiemmin, voin sanoa että aiemmin käytin noita, netissä on näitä satunnaisia salasanantekogeneraattoreita ja käytin niitä aiemmin ja sitten tulin miettineeks että niin, entä jos tää tallentaa tää sivusto nää, nämä generoidut salasanat, ja osaa yhistää sen tähän käyttäjään niin mä oon lopettanut niiden käytön, se oli vasta vähän aikaa sitten. Mutta jos nyt sanotaan, tällä hetkellä niin ei mun tarvitse varmaan muuttaa nyt pahemmin mitään.” (H1)

> ”En usko.” (H7)

Vaikka haastateltavat suunnittelevat jatkavansa älylaitteiden käyttöä samaan tapaan tulevaisuudessakin, useampikin totesi, ettei ole kovin halukas hankkimaan enää enempää älylaitteita. Nykyinen laitteiden määrä koettiin riittäväksi eikä uusille älylaitteille nähty mitään tarvetta.

Osa haastateltavista suunnitteli tekevänsä joitain tietoturvaa parantavia toimia jatkossa ja jotkut kommentoivat haastattelun muistuttaneen heitä tietoturvan tärkeydestä.

> ”Öö, en, en, että sillä mennään, että se ois ensimmäisenä työtehtävänä se jonkinlaisen virustorjuntaohjelman saanti että se nyt ois ensimmäinen askel niin kuin turvallisempaan suuntaan.” (H4)

> ”No ei se välttämättä siihen hankkimiseen vaikuta mutta ehkä enemmänkin siihen miten sitten suojaa tulevaisuudessa ne.” (H10)

> ”Siis oonhan mä nyttenkin arka et enhän mä, jos on jotain liitteitä niin jossain näkyy niin emmä niitä avaa tai tämmösiä näin, että kyllähän mä nyttenkin oon varovainen, että kyllä mä jatkossa varmaan samanlailla tuun toimimaan sitten.” (H9)

> ”Ei, kyllä ihan varmaan ennallaan suunnilleen, mut kyllä sitä niin kun täytyy muistaa vaan näitä asioita ja suojata sitten tietoja.” (H13)

5.4 Haastateltavien näkemykset esitellyistä uhkista

Haastattelun lopuksi haastateltavia pyydettiin laittamaan viisi esiteltyä tietoturvauhkaa järjestykseen uhkaavimmasta vähiten uhkaavaan. Haastateltavia pyydettiin miettimään uhkaavuutta itsensä näkökulmasta eli mikä uhkista on itselle eniten uhkaavin ja mikä vähiten. Lisäksi haastateltavia pyydettiin perustelemaan valintansa. Vastaukset tähän kysymykseen on esitelty ensiksi alla olevassa taulukossa (taulukko 4) ja tämän jälkeen käydään läpi haastateltavien perusteluja valinnoilleen. Taulukossa numero 1 tarkoittaa uhkaavinta uhkaa ja 5 vähiten uhkaavaa.

TAULUKKO 4 Haastateltavien näkemys 5 yleisimmän uhkan uhkaavuudesta

	Tietojenkalastelu	Mikrofonin salakuuntelu	Haittaohjelmat	Tilin kaappaus	Palvelunestohyökkäys
H1	4	2	3	1	5
H2	1	5	2	3	4
H3	1	2	4	3	5
H4	3	5	2	1	4
H5	1	3	4	2	5
H6	1	3	4	2	5
H7	4	5	2	1	3
H8	3	5	2	1	4
H9	5	3	2	1	4
H10	5	4	2	1	3
H11	1	2	4	5	3
H12	2	4	1	3	5
H13	2	4	5	1	3
H14	5	4	1	2	3

Taulukon mukaan tietojenkalastelun uhkaavuuden keskiarvo on 2,71, mikrofonin salakuuntelun keskiarvo on 3,64, haittaohjelmien keskiarvo 2,71, tilin kaappauksen keskiarvo 1,92 ja palvelunestohyökkäyksen 4. Keskiarvoja tarkistelemalla voidaan tehdä helposti päätelmä, että haastateltavat kokevat tilin kaappauksen selvästi uhkaavimmaksi uhkaksi. Toiseksi uhkaavimmiksi tulivat samalla keskiarvolla sekä tietojenkalastelu että haittaohjelmat, näiden jälkeen mikrofonin salakuuntelu ja vähiten uhkaavin on palvelunestohyökkäys. Pelkät numerot eivät kuitenkaan vielä kerro riittävästi haastateltavien näkemyksistä esitellyistä uhkista. Sen vuoksi haastateltavia pyydettiin perustelemaan antamiaan arvosanoja.

Tilin kaappaus oli haastateltavien mielestä selvästi uhkaavin. Haastateltavista peräti puolet eli 7 henkilöä nimesi tilin kaappauksen uhkaavimmaksi hyökkäykseksi.

> ”No varmaan tää on just semmonen että, tähän ei aina pysty ite vaikuttamaan sillein että, kun pystyy osaamaan hakkeroimaan sen vaikka oliskin joku tietoturva tai jotain niin.” (H10)

> ”Kyllä se on tuo tilin kaappaus. Se on kerran tapahtunut just Spotifyn kautta niin kuin sanoin niin kyllä se on, silloin se on päällimmäisenä. En tiedä mitä kautta siinä on sitten se että on saanu tiedot mutta en haluis että tulis uudestaan millekkään tärkeämmälle profiilille.” (H1)

Ainoastaan yksi haastateltava laittoi tilin kappauksen vähiten uhkaavaksi. Hän perusteli valintaa sillä, ettei tiedä miten tilin kaappaus käytännössä vaikuttaisi häneen.

> ”Ja kyllähän just tuo tilin kaappauksesta ei oo oikein sillein kokemusta että en oikein tiiä et minkä- tai miten se sit oikein pystyy sit kovin vaikuttamaan kovin paljon.” (H11)

Toiseksi uhkaavimmaksi haastateltavat kokivat samalla keskiarvolla sekä tietojenkalastelun että haittaohjelmat. Tietojenkalastelu selvästi hajautti haastateltavia; samalla kun osa valitsi tietojenkalastelun uhkaavimmaksi, oli se joidenkin mielestä vähiten uhkaavin. Haastateltavat, jotka olivat valinneet tietojenkalastelun uhkaavimmaksi, perustelivat valintaansa mm. sillä, että uhkan kohteena ovat omat henkilökohtaiset tiedot ja osa oli tietoinen myös nykyään hyvin kehittyneistä tietojenkalastelutavoista.

> ”No sanotaanko näin että, ehkä semmonen mikä menis läpi että ite opiskelijana on tullut Kelan kanssa hirveesti, niin sitä ei välttämättä tiedosta että jos se, saatais näkymään että soitetaan vaikka 020 -alkuisesta numerosta niin eihän sitä tiiä että onko se oikeesti Kelan virkailija. Siinä vois olla semmonen mistä saattais saaha mun tiedot.” (H3)

Osa haastateltavista taas perusteli laittaneensa tietojenkalastelun vähiten uhkaavaksi, koska haastateltavat uskovat tunnistavansa mahdolliset tietojenkalasteluhyökkäykset eivätkä näin ollen antaisi tietojaan hyökkääjälle. Lisäksi haastateltavat olivat nähneet paljon uutisointia lisääntyneestä tietojenkalastelusta ja he kokivat olevansa varovaisia omien tietojensa kanssa.

> ”Sen takia koska nehän mun mielestä pitää olla minuun henkilökohtaisesti yhteydessä, kyllä mulla sen verran vielä pää toimii että en anna salasanoja enkä käyttäjätunnuksia.” (H9)

> ”Koska, ite ainakin tietää siitä että ei mee antamaan kellekkään mitään pankkitunnuksia, ja tällein just kuullu uutisissa sen verran paljon tästä että on sitä tapahtunut niin kuitenkin tietoinen siitä sen verran paljon että osaa olla varovainen eikä anna mihinkään omia tietojansa.” (H10)

Haastateltavat sijoittivat haittaohjelmat hyvin pitkälti keskimmäisille arvosanoille eli arvosanoille 2-4, minkä johdosta haittaohjelmat ylsivät jaetulle toiselle sijalle tietojenkalastelun kanssa. Haastateltavat kokivat haittaohjelmat siis uhkaaviksi, mutta eivät kuitenkaan kaikista uhkaavimmiksi. Haastateltavat perustelivat haittaohjelman sijoitusta mm. sillä, että ne keräävät uhrien henkilökohtaisia tietoja, minkä lisäksi laitteella voi olla haittaohjelma käyttäjän huomaamatta. Erityisesti haittaohjelmien huomaamattomuus huoletti haastateltavia, sillä niihin ei pysty itse vaikuttamaan, jos ei edes tiedä laitteella olevan haittaohjelman. Lisäksi tietokone- ja mobiilipelejä pelaavat haastateltavat olivat hyvinkin tietoisia peleihin piilotetuista haittaohjelmista.

> ”No tää on vähän sama kun tuo tilin kaappaus et tavallaan näitä ei aina huomaa sitten jos onkin jotain tämmösiä haittaohjelmia.” (H10)

> ”Haittaohjelmat, en nytten tiedä tuota että, en tuu ladanneeks mitään omasta mielestäni mitään haittaohjelmia, oon tosi varovainen siinä, mutta ei sitä tiedä kun esimerkiksi peleissä on nykyään näitä tietojenkeräysohjelmia esimerkiksi piilotettuna, se oli yks kohu tuossa vuosi takaperin Steamissa, että kun selvisi että muutamiin peleihin oli laitettu salaa semmosia tietojenkeräysohjelmia, niin tota sehän oli semmonen että eihän sitä tiiä jos sä asennat jonkun ohjelman että onko siihen asennettu joku takaportti tai jonkinlainen lisäohjelma.” (H1)

> ”No ite tykkään pelailla esim mobiilipelejä että jos sieltä tulis joku uus peli ja se oliskin haittaohjelma niin se olis semmoinen.” (H3)

Mikrofonin salakuuntelu sai keskiarvoksi 3,64 ja näin ollen se sijoittui neljänneksi uhkaavimmaksi uhaksi. Moni koki, ettei mikrofonin salakuuntelulla heistä saada mitään tärkeitä tietoja selville eivätkä he tämän vuoksi kokeneet mikrofonin salakuuntelua erityisen uhkaavaksi. Kukaan haastateltavista ei laittanut mikrofonin salakuuntelua uhkaavimmaksi ja se sijoitettiinkin useita kertoja vähiten uhkaavimmaksi.

> ”No, mun, mä en sellasia niin kuin puheluita esimerkiks soita enkä käy keskusteluita puhelimessa etteikö niitä vois vaikkapa kuunnellakin, että mua ei haittaa se ollenkaan, että kyllä mun puheluita voi kuunnella, mä en koe sitä sillä tavalla mitenkään, tai en nyt mitenkään mutta koen sen vähiten haittaavana.” (H4)

Kuitenkin osaa huoletti mikrofonin salakuuntelu siitä syystä, että sille voi altistua esimerkiksi ystävän kanssa jutellessa. Tällöin ystävän laitteella saattaa olla haittaohjelma, joka salakuuntelee mikrofonia, ja haastateltava altistuu mikrofonin salakuuntelulle, vaikka olisi itse ollut kuinka huolellinen oman tietoturvan osalta.

> ”No koska sitä ei välttämättä tiedä ite että mikrofonia kuunnellaan, että sehän ei välttämättä edes ole omalta laitteelta, sehän voi olla myös vaikka jos juttelet kaverin kanssa niin sen kaverin laite. Siinä ei auta se vaikka itellä ois mitenkä suojattu.” (H3)

Vähiten uhkaavimmaksi haastateltavat kokivat palvelunestohyökkäyksen keskiarvolla 4. Kukaan haastateltavista ei laittanut palvelunestohyökkäystä uhkaavimmaksi tai toiseksi uhkaavimmaksi uhaksi. Haastateltavat perustelivat palvelunestohyökkäyksen sijoitusta mm. sillä, että palvelunestohyökkäyksessä omat tiedot tai rahat eivät ole uhattuina, vaan palvelunestohyökkäys ainoastaan estää pääsyn tiettyyn palveluun. Haastateltavat kokivat myös, että tietyn palvelun saavuttamattomuus ei ole niin suuri ongelma, vaan heillä on aikaa odottaa, että palvelu tulee taas saataville.

> ”Itelläni ei oo mitään palvelua muuta kun ehkä ne nettisivut on mutta se on semmonen että jos ne kaatuu niin se ei vie rahaa eikä mitään että, siellä ei oo mitään henkilökohtaisia tietoja, se ei haittaa siinä mielessä.” (H3)

Kaiken kaikkiaan haastateltaville esitellyt uhkat olivat melko hyvin jo ennestään tuttuja eivätkä haastateltavat kokeneet esiteltyjen uhkien suuremmin vaikuttavan älylaitteiden käyttöön jatkossa. Osa kuitenkin sanoi haastattelun toimineen ikään kuin muistutuksena siitä, että tietoturvaohjelmisto kannattaa päivittää ja muutenkin miettiä jatkossa tarkemmin, ettei esimerkiksi luettele pankkitunnuksiaan ääneen. Moni toi kuitenkin haastattelun lomassa ilmi huolensa esimerkiksi vanhempia ihmisiä kohtaan ja siitä, miten vanhemmilla ihmisillä ei välttämättä ole minkäänlaisia tietoturvaohjelmistoja ja silti esimerkiksi pankkipalvelut siirtyvät verkkoon, jolloin myös vanhemmat ihmiset joutuvat käyttämään niitä vaikkei heillä ole minkäänlaista tietämystä tietoturvasta. Useampi haastateltava myönsi myös suoraan, ettei heidän omakaan tietämyksensä tietoturvasta ole riittävällä tasolla ja että käyttäjiä pitäisi enemmän informoida erilaisista suojautumiskeinoista. Kun haastateltavilta kysyttiin, kokevatko he oman tietämyksensä olevan riittävällä tasolla tietoturvan kannalta, olivat vastaukset varsin saman suuntaisia; suurin osa koki, että parannettavaa olisi vaikka jonkinlainen tietämys tietoturvasta löytyykin.

> ”No kyllä mä oon luullut niin että kykenen mutta jos mun telkkariakin pitää ruveta pelkäämään niin emmä sitten kyllä enää tiiä.” (H8)

> ”Ei varmaankaan tietsä oo.” (H9)

> ”No ei nyt ehkä välttämättä riittävä, mutta kyllä nyt kuitenkin jonkinlainen.” (H10)

> ”No kyllä se varmaan parempikin vois olla sinänsä, sitä vaan luottaa että sitten kun on asennettuna niitä erinäisiä laitteita ja sit kun ite miettii mitä tekee netissä niin et se riittää mutta voishan tota osaamista toki enemmänkin olla.” (H13)

Viimeiseksi haastattelussa kysyttiin sitä, pitäisikö tietoisuutta tietoturvauhkista lisätä ja jos pitäisi, niin kenelle. Haastateltavien vastauksissa toistui erityisesti huoli vanhemmista ihmisistä ja haastateltavat kokivat, että vanhemmille käyttäjille olisi tärkeää kertoa kattavammin tietoturvan tärkeydestä ja opastaa tietoturvatoimista. Toinen ryhmä, jolle tietoturvasta olisi hyvä kertoa haastateltavien mielestä ovat lapset ja nuoret. Joidenkin mielestä kaikki hyötyisivät siitä, että uhkista kerrottaisiin enemmän ja erityisesti haastateltavat toivoivat, että asioista kerrottaisiin sen verran selkeästi, että ne on helppo ymmärtää.

> ”No aikalailla kaikille, mut etenkin niin kun vanhoille ihmisille.” (H12)

> ”Ja sitten esimerkiks kun pankitkin on, enää ei moneenkaan pankkiin saa oikeestaan ees mennä kun ajanvarauksella niin pankit ei oo koskaan kysyny ainakaan minulta että onko mulla mitään tietoturvaa ja minkälaisilla laitteilla mä hoidan mun rahaasioita ja kuitenkin kukas sen sitten vastaa jos se tili tyhjenee? Niin sitä mä vaan ihmettelen.” (H2)

Käyttäjä nähdään yleisesti heikoimpana lenkkinä tietoturvan kannalta ja tämän vuoksi paras tapa suojella käyttäjiä tietoturvauhkilta, on varmistaa, että heillä on riittävästi tietämystä erilaisista uhkista. Lähes kaikki vastaajat olivat sitä

mieltä, että tiedotusta erilaisista uhkista pitäisi lisätä ja tiedotuksen pitäisi olla sen verran selkeää, että kaikki varmasti ymmärtävät sen. Moni tähänkin tutkimukseen osallistunut totesi suoraan, ettei omaa riittävää tietotaitoa suojellakseen omia tietojaan tarpeeksi.

6 POHDINTA

Tässä luvussa käydään tarkemmin läpi vastaukset tutkimuskysymyksiin, joihin on haettu vastauksia sekä kirjallisuuskatsauksen että empiirisen osuuden haastatteluiden avulla. Tutkimuksen tuloksia vertaillaan kirjallisuuteen ja arvioidaan kriittisesti. Lisäksi luvussa tuodaan ilmi myös tutkimukseen mahdollisesti vaikuttaneet rajoitteet.

Tutkielman tavoitteena oli vastata kahteen tutkimuskysymykseen, jotka ovat:

1. Mitkä ovat yleisimmät älylaitteisiin kohdistuvat tietoturvauhkat?
2. Miten tietoisuus älylaitteiden tietoturvauhkista vaikuttaa älylaitteiden käyttöön?

Vastauksia tutkimuskysymyksiin haettiin kirjallisuuskatsauksen sekä tutkielman empiirisen osuuden haastatteluiden avulla. Ensimmäiseen tutkimuskysymykseen vastattiin kirjallisuuskatsauksen perusteella, jotta saatiin rakennettua pohja haastatteluja varten. Kirjallisuuskatsauksessa kävi ilmi, että älylaitteisiin liittyy valtava määrä tietoturvauhkia ja älylaitteet ovat monessa suhteessa jopa alttiimpia erilaisille tietoturvauhkille kuin perinteiset tietokoneet. Tämä selittyy sillä, että älylaitteet sisältävät erilaisia sensoreita, jotka keräävät valtavan määrän dataa sekä ympäristöstä että käyttäjästä. Myös skaalautuvuus sekä älylaitteiden rajalliset resurssit sekä akun kapasiteetti hankaloittavat tietoturvan toteuttamista älylaitteille.

Älylaitteisiin kohdistuvia tietoturvauhkia voidaan jaotella monin eri tavoin, mutta tässä tutkielmassa uhkat jaettiin 4 kategoriaan kuten Andrea, Chrystostomou ja Hadjichristofi (2015) sekä Deogirikar ja Vidhate (2017) ovat tehneet. Nämä neljä kategoriaa ovat: fyysiset hyökkäykset havaintotasolla, verkkoon kohdistuvat hyökkäykset verkkotasolla, sovellushyökkäykset sovellustasolla sekä salaushyökkäykset. Tietoturvauhkien jatkuvasti kehittyessä kaikkia mahdollisia uhkia ei ollut mahdollista käydä tässä tutkielmassa läpi. Sen vuoksi tutkielmassa päädyttiin esittelemään jokaisesta kategoriasta muutama yleisin uhka. Fyysisistä uhkista käytiin läpi solmujen väärinkäyttö, sol-

mun häirintä, haitallisen solmun lisäys eli mies välissä -hyökkäys, fyysinen vahingoittaminen, käyttäjän manipulointi, lepotilaan pääsyn häirintä sekä haitallisen koodin lisääminen. Verkkoon kohdistuvista hyökkäyksistä esiteltiin verkkoliikenteen analysointihyökkäys, RFID-huijaus, RFID-kloonaus, luvaton pääsy RFID-tunnisteen tietoihin, mies välissä -hyökkäys, palvelunestohyökkäys, reitityshyökkäys ja sybil -hyökkäys. Sovellushyökkäyksistä käytiin läpi tietojenkalastelu, haittaohjelmat, tilin kaappaus, salakuuntelu, haitallinen komentosarja sekä palvelunestohyökkäys. Viimeisestä kategoriasta eli salaushyökkäyksistä esiteltiin side channel -hyökkäys, salausanalyysihyökkäys sekä mies välissä -hyökkäys.

Koska esiteltyjä uhkia on edelleen liian paljon haastattelua varten, päätettiin kirjallisuudesta etsiä muutama yleisin älylaitteisiin kohdistuva tietoturvauhka. Lopulta haastatteluun asti valituiksi uhkiksi tulivat tietojenkalastelu, mikrofonin salakuuntelu, haittaohjelmat, tilin kaappaus ja palvelunestohyökkäys. Nämä uhkat valittiin sen vuoksi, että kirjallisuuden mukaan ne ovat yleisimpiä, mutta myös siitä syystä, että nämä uhkat kohdistuvat erityisesti käyttäjien arkaluonteisiin tietoihin, kuten henkilötietoihin ja pankkitunnuksiin.

Kirjallisuuden pohjalta onnistuttiin vastaamaan hyvin ensimmäiseen tutkimuskysymykseen. Erilaisista älylaitteisiin kohdistuvista tietoturvauhkista oli helposti löydettävissä paljon tietoa ja tiedot oli julkaistu laadukkaissa lähteissä, joten niitä voidaan pitää myös todenmukaisina. Kuitenkaan tässä tutkielmassa ei ollut mahdollista esitellä kaikkia älylaitteisiin kohdistuvia tietoturvauhkia, vaan tutkielmassa keskityttiin selvittämään erityisesti yleisimmät älylaitteisiin kohdistuvat tietoturvauhkat.

Tämän tutkielman toisen tutkimuskysymyksen avulla pyrittiin selvittämään sitä, miten käyttäjien tietoisuus älylaitteisiin kohdistuvista tietoturvauhkista vaikuttaa älylaitteiden käyttöön. Kirjallisuuskatsauksen avulla löydettiin hyvin tietoa yleisimmistä älylaitteisiin kohdistuvista tietoturvauhkista, joten sen pohjalta pystyttiin suunnittelemaan empiirisen tutkimuksen rakenne. Lisäksi kirjallisuuskatsauksen avulla voidaan vertailla empiirisessä osuudessa saatuja tuloksia kirjallisuudessa esitettyihin havaintoihin.

Haastateltavien tietämys älylaitteisiin kohdistuvista tietoturvauhkista vaihtelee henkilöiden välillä, jotkut osaavat luetella lukuisia erilaisia tietoturvauhkia, kun taas toiset eivät osaa nimetä suoraan mitään uhkia. Yleisimpien uhkien esittelyn jälkeen lähes kaikki silti totesivat ainakin kuullensa joskus uhkista nimeltä. Suurin osa haastateltavista kokee tietoturvauhkien kohdistuvan ainoastaan tietokoneisiin, älypuhelimiin ja tabletteihin, eikä esimerkiksi älykkäitä kodinkoneita tai älykelloja pidetä uhattuina. Osa varsinkin vanhemmista haastateltavista uskoo uhkien kohdistuvan yksinomaan tietokoneisiin. Lähes kaikki haastateltavat osasivat nimetä tietoturvauhkien kohdistuvan erityisesti henkilötietoihin. Näiden lisäksi mainittiin myös mm. pankkitunnukset ja sähköpostien tunnukset.

Haastateltavien vastaukset siitä, kokevatko he omien tietojensa olevan turvassa, erosivat jo selkeästi toisistaan. Osa kokee tietojensa olevan hyvin turvassa ja luottavansa omiin taitoihin pitää tiedot turvassa, kun taas jotkut koki-

vat, etteivät tiedot kovin hyvässä turvassa ole ja ettei heillä riitä tietotaito tietoturvan parantamiseen. Haastateltavien tekemät tietoturvaa parantavat toimet erosivat voimakkaasti toisistaan, osa kertoi tehneensä kattavasti erilaisia toimia aina virusturvista vahvoihin salasanoihin, välttävänsä uusimpien sovellusten lataamista sovelluskaupoista sekä käyttämällä tietoturvatestaajien suosimaa Kali Linuxia, kun taas osa ei ollut tehnyt minkäänlaisia tietoturvaa parantavia toimia.

Mielenkiintoisinta tässä on kuitenkin se, että vastaajat, jotka kokivat tietojensa olevan turvassa koska he luottavat omiin kykyihinsä pitää tiedot turvassa, eivät olleet kuitenkaan tehneet juuri mitään tietoturvaa parantavia toimia. Tätä selittävät Liangin ja Xuen (2009, 2010) tutkimukset Technology threat avoidance theory (TTAT) eli vapaasti suomennettuna teknologian uhkien välttämisteoriasta. TTAT todistaa, että käyttäjät ovat motivoituneita välttelemään haitallista tietotekniikkaa silloin, kun he kohtaavat uhkan ja uskovat, että uhka on mahdollista välttää noudattamalla turvaavia toimia. Jos taas käyttäjät uskovat, ettei uhkaa pysty täysin välttämään turvaavia toimia noudattamalla, ottavat he käyttönsä tunteisiin keskittyvät selviytymisstrategiat. Tunteisiin keskittyvissä selviytymisstrategioissa käyttäjät luovat virheellisiä havaintoja ympäristöstä tekemättä mitään muutoksia siihen. Tunteisiin keskittyviä selviytymisstrategioita käyttäessä käyttäjä saattaa esimerkiksi ajatella, ettei uhka kohdistu häneen tai ettei kukaan ole kiinnostunut hänen tiedoistaan. Tällä tavoin ajattelemalla uhkataso laskee eikä käyttäjä koe tietoturvansa olevan uhattuna. (Liang & Xue, 2009; Liang & Xue, 2010.)

Tunteisiin keskittyvät selviytymisstrategiat selittävät juuri sitä, miksi osa haastateltavista kokee tietojensa olevan turvassa ilman minkäänlaisia tietoturvaa parantavia toimia. Käyttäjät uskottelevat itselleen, etteivät uhkat kuitenkaan kohdistu heihin tai ettei kukaan ole kiinnostunut juuri heidän tiedoistaan, ja tällä tavoin käyttäjät luottavat virheellisesti omien tietojensa olevan turvassa.

Kun haastateltaville oli esitelty yleisimpiä älylaitteisiin kohdistuvia tietoturvauhkia, heiltä kysyttiin uudestaan, kuinka huolissaan he ovat oman tietoturvansa tasosta nyt. Moni koki tietoturvansa olevan edelleen samalla tasolla, mutta muutaman haastateltavan kokemus oman tietoturvansa tasosta oli laskenut. Lisäksi tässäkin vaiheessa tuli ilmi peräti 4 haastateltavan kohdalla haastateltavan omat kyvyt pitää tietonsa turvassa. Useampikin haastateltava suunnitteli aikovansa tehdä joitain tietoturvaa parantavia toimia nyt kun haastattelun myötä tietoturva-asiat tulivat puheeksi.

Haastattelun viimeisessä osiossa, jossa haastateltavia pyydettiin laittamaan esitellyt uhkat uhkaavuusjärjestykseen ja perustelemaan järjestys, tuli jälleen useita kertoja ilmi haastateltavien kyky huolehtia itse, että omat tiedot pysyvät turvassa. Haastateltavat kokivat, että kunhan he eivät itse laita tietojaan epäilyttäville sivustoille, ovat heidän tietonsa turvassa. Tämähän ei kuitenkaan enää nykyään pidä paikkaansa tietoturvauhkien moninaisuuden vuoksi. Lisäksi moni perusteli, ettei kukaan kuitenkaan ole kiinnostunut heidän tiedoistaan. Tässä pääsemme jälleen Liangin ja Xuen (2009, 2010) teknologian uhkien välttämisteoriaan. Jos käyttäjät uskovat, ettei uhkaa pysty täysin välttämään,

ottavat he käyttöönsä tunteisiin keskittyvät selviytymisstrategiat, ja kuvittelevat, ettei uhka kohdistu heihin.

Lisäksi Liang ja Xue toivat ilmi vuoden 2010 tutkimuksessaan myös sen, että käyttäjät ovat motivoituneita välttelemään uhkaa, jos he kokevat turvaavien toimien olevan tehokkaita, edullisia käyttää ja käyttäjillä on itsevarmuutta sen suhteen, että he osaavat toteuttaa turvaavia toimenpiteitä. Kysyttäessä haastateltavilta, kokevatko he omaavansa riittävän tietotaidon tietoturvan kannalta, useampikin haastateltava totesi, ettei hänellä ole tarvittavaa tietotaitoa. Näissä olivat mukana myös ne haastateltavat, ketkä aiemmin haastattelussa totesivat tietojensa olevan turvassa ilman mitään tietoturvaratkaisuita, kuten H8. Näin ollen haastatteluissa tuli ilmi teknologian uhkien välttämisteorian mukaan, että haastateltavat tiedostavat, etteivät he omaa tarvittavaa osaamista tietoturvan parantamiseksi ja tämän vuoksi he turvautuvat tunteisiin keskittyviin selviytymisstrategioihin. Tutkimuksen tulokset tukevat näin ollen Liangin ja Xuen (2009, 2010) tutkimuksia teknologian uhkien välttämisteoriasta.

Toinen mielenkiintoinen seikka, joka tuli esiin tämän tutkimuksen myötä, on se, että IT-alan ammattilaiset ovat enemmän huolissaan omasta tietoturvastaan kuin tavalliset käyttäjät. Tämä on mielenkiintoista erityisesti siitä syystä, että IT-alalla työskentelevät olivat kuitenkin tehneet kattavasti erilaisia tietoturvaa parantavia toimia. He perustelivat pelkoaan sillä, että he tietävät, kuinka tiedot voivat vuotaa ulkopuolisille, vaikka itse olisi kuinka huolellinen. Esimerkiksi H3 kertoi, ettei luota siihen, että koulussa tai Kelassa olevat tiedot pysyisivät välttämättä turvassa erilaisten tietovuotojen vuoksi, Lisäksi hän oli tietoinen siitä, kuinka kehittyneitä nykyiset tietojenkalasteluhyökkäykset ovat, ja uskoi voivansa itsekin tulla huijatuksi tällaisissa. Hän myös huomautti, että ystävän laitteella voi olla esimerkiksi mikrofonia salakuunteleva haittaohjelma, jolloin ystävän luona kyläillessä myös omat tiedot ovat vaarassa, jos sattuu puhumaan jotain henkilökohtaisempaa.

Tämä huomio tukee myös teknologian uhkien välttämisteoriaa. Henkilö, joka omaa mielestään riittävän tietotaidon tietoturvan parantamiseksi, on motivoitunut tekemään kattavasti erilaisia tietoturvaa parantavia toimia. Tällainen henkilö myös tiedostaa sen, että uhkat voivat kohdistua itseen ja tämän vuoksi tietoturvatoimet ovat tärkeitä. Tutkimuksen tarkoituksena oli myös tarkistella sitä, miten IT-alalla työskentelevät ovat suojautuneet tietoturvauhkilta verrattuna tavallisiin käyttäjiin. Tutkimuksen myötä tuli ilmi, että IT-alalla työskentelevät ovat paremmin selvillä erilaisista tietoturvauhkista ja näin ollen myös paremmin suojautuneita. Teknologian uhkien välttämisteorian mukaisesti heillä on riittävä luotto omiin kykyihin kyetä suojautumaan uhkilta, joten he tekevät näin. He myös myöntävät tosiasiat itselleen eli sen, että uhkat saattavat kohdistua heihin itseensä ja tämän vuoksi he ovat motivoituneita tekemään tietoturvaa parantavia toimia.

Tutkimuksen tuloksista kävi ilmi, että esitellyistä uhkista huolestuttavimpina haastateltavat pitivät tilin kaappausta, tietojen kalastelua ja haittaohjelmia. Sen sijaan mikrofonin salakuuntelu ja palvelunestohyökkäykset koettiin vähiten uhkaavimmiksi. Nämä tulokset saavat tukea myös tutkimuksesta, jonka ovat

tehneet Makkonen ja Siakas (2019). Sen mukaan haitalliset ohjelmat ja ohjelmistot sekä tietojenkalastelu koettiin uhkaavimmiksi, kun taas palvelunestohyökkäykset ja käyttäjän manipulointi koettiin vähemmän uhkaavaksi (Makkonen & Siakas, 2019). Tutkimusten tulokset siis tukevat hyvin toisiaan.

Tämän tutkimuksen tulokset tukevat näin ollen aiempia tutkimuksia ja sen vuoksi saatuja tuloksia voidaan pitää luotettavina. Tutkimuksen otos on kuitenkin melko pieni, vain 14 haastateltavaa, joten kovin laajoja yleistyksiä ei tämän tutkimuksen tiimoilta voi tehdä. Tutkimuksen avulla saatiin kuitenkin selville yksittäisten älylaitteiden käyttäjien mietteitä tietoturvasta ja heidän tekemiä tietoturvaa parantavia toimia. Lisäksi tuloksista pystyttiin huomaamaan se, että IT-alalla työskentelevät ovat suojautuneet parhaiten mutta kokevat silti samanaikaisesti olevansa eniten uhattuina. Tässäkin tapauksessa pitää kuitenkin huomioida otoksen koko, yhteensä haastateltavia oli 14 ja heistä ainoastaan 2 työskenteli IT-alalla. Näin ollen saatuja tuloksia ei voi yleistää koskemaan suurempia ryhmiä. Saadut tulokset kuitenkin tukevat kirjallisuudessa esiteltyjä tutkimuksia ja olivat yhteneväisiä kirjallisuuden kanssa, joten tämän vuoksi tuloksia voidaan silti pitää luotettavina. Lisäämällä haastateltavien määrää, olisi mahdollista saada vielä tarkempaa tietoa siitä, kuinka paljon tavallisilla käyttäjillä on tietämystä älylaitteisiin kohdistuvista tietoturvaongelmista ja kuinka turvassa he kokevat omien tietojensa olevan.

Tämän tutkielman pohjalta tulee ilmi monia jatkotutkimusaiheita. Tutkimus voitaisiin toteuttaa laajempana, jolloin tulokset olisivat yleistettävämpiä ja saataisiin kattavampaa tietoa tavallisten käyttäjien tietämyksestä älylaitteisiin kohdistuvista tietoturvauhkista. Jos tutkimukseen saataisiin enemmän mukaan myös IT-alalla työskenteleviä, saataisiin yleistettävämpää tietoa siitä, kuinka tavallisten käyttäjien ja IT-alalla työskentelevien tietämykset eroavat tietoturvasta ja kuinka paljon tehdyt tietoturvaa parantavat toimet eroavat toisistaan. Laajemmalla haastateltavien määrällä voitaisiin tutkia myös laajemmin teknologian uhkien välttämisteorian toteutumisen tasoa eli sitä, kuinka monen kohdalla TTAT toteutuu.

7 YHTEENVETO

Esineiden internet ja älylaitteet ovat saavuttaneet viime vuosina valtavan suosion, ja ne ovatkin levinneet lähes kaikille elämän osa-alueille. Tämän tutkielman tarkoituksena oli tutkia sitä, miten tietoisuus älylaitteisiin kohdistuvista tietoturvauhkista vaikuttaa älylaitteiden käyttöön. Ensimmäisenä tutkimuskysymyksenä oli, mitkä ovat yleisimmät älylaitteisiin kohdistuvat tietoturvauhkat. Tähän haettiin vastausta kirjallisuuskatsauksella. Kirjallisuuskatsauksessa esiteltiin tarkemmin, mitä esineiden internetillä ja älylaitteilla tarkoitetaan ja millaisia tietoturvauhkia älylaitteisiin liittyy. Lisäksi tutkielmassa selvitettiin sitä, millainen merkitys tietoturvalla on älylaitteissa.

Älylaitteista hyötyvät niin kuluttajat kuin organisaatiotkin. Kuluttajien elämää älylaitteet helpottavat monella tavalla ja organisaatioita puolestaan älylaitteet auttavat tuomalla kustannuksia alas ja parantamalla tehokkuutta. Esineiden internet ja älylaitteet eivät kuitenkaan ole täysin ongelmattomia, vaan niihin kohdistuu paljon erilaisia tietoturvauhkia. Tämän tekee erityisen haitalliseksi se, että älylaitteet keräävät käyttäjistä valtavan määrän arkaluonteista tietoa eikä älylaitteiden tietoturvaan ole juurikaan panostettu tähän mennessä. Näin ollen kaikki älylaitteiden keräämä data onkin vaarassa päätyä vääriin käsiin.

Älylaitteiden monimuotoisuus ja nopea kehitys luovat haasteita tietoturvaratkaisuiden kehittämiselle. Myös laitteiden rajallinen laskentateho ja akun kapasiteetti tuottavat ongelmia, sillä laitteet tarvitsevat lähes kaiken laskentatehon ja energian toimintojen suorittamiseen. Tämän vuoksi älylaitteita on helppo käyttää hyökkäysten toteuttamiseksi, ja älylaitteisiin kohdistuvat tietoturvauhkat lisääntyvätkin jatkuvasti. Tällä hetkellä älylaitteisiin kohdistuvia tietoturvauhkia on olemassa valtava määrä ja tässä tutkielmassa on pyritty esittelemään niistä keskeisimmät. Älylaitteisiin kohdistuvat tietoturvauhkat voidaan jakaa neljään kategoriaan: fyysiset hyökkäykset, verkkoon kohdistuvat hyökkäykset, sovellushyökkäykset ja salaushyökkäykset. Eräitä yleisimmistä älylaitteisiin kohdistuvista tietoturvahyökkäyksistä ovat erilaiset virukset sekä palvelunestohyökkäykset ja mies välissä -hyökkäykset. Älylaitteisiin kohdistuvilla hyökkäyksillä pyritään moniin eri asioihin: hyökkääjä saattaa yrittää varastaa

arkaluonteisia tietoja, saada taloudellista hyötyä tai aiheuttaa organisaatioille tappioita urkkimalla yrityssalaisuuksia ja levittämällä niitä eteenpäin. Esineiden internetiin ja älylaitteisiin kohdistuvat tietoturvahyökkäykset saattavat aiheuttaa myös vakavaa vaaraa: jos esimerkiksi hyökkääjä onnistuu estämään internetiin liitettyjen lääkinnällisten laitteiden toiminnan sairaalassa, saattavat seuraukset olla tuhoisat (Ronen & Shamir, 2016). Älylaitteiden tietoturvaan tulisikin kiinnittää enemmän huomiota tulevaisuudessa.

Kun kirjallisuuskatsauksella oli saatu selvitettyä yleisimmät älylaitteisiin liittyvät tietoturvauhkat, siirryttiin empiirisen tutkimuksen pariin. Tutkielman toisena tutkimuskysymyksenä oli, miten tietoisuus älylaitteiden tietoturvauhkista vaikuttaa älylaitteiden käyttöön. Laadullinen tutkimus toteutettiin haastatteluiden avulla. Haastateltaviksi valittiin tavallisia älylaitteiden käyttäjiä ja heidän lisäksi pari IT-alan ammattilaista, jotta vastauksia voitaisiin vertailla toisiinsa. Tutkielman keskeisenä tuloksena voidaan pitää sitä, että mitä enemmän käyttäjällä on tietoa älylaitteisiin kohdistuvista tietoturvauhkista, sitä motivoituneempi hän on suojautumaan niiltä. Henkilöt, joilla on kattavasti tietoa erilaisista uhkista, ovat usein tehneet kattavasti erilaisia tietoturvaa parantavia toimia, sillä he kokevat tietonsa olevan uhattuina. Vaikka tietoturvauhkiin perehtyneet henkilöt ovatkin tehneet paljon erilaisia suojautumistoimenpiteitä, kokevat he silti tietonsa olevan uhattuina. Sen sijaan käyttäjät, joilla ei juurikaan ole tietoa erilaisista tietoturvauhkista, eivät yleensä ole tehneet mitään tai vain vähän tietoturvaa parantavia toimia. Tästä huolimatta käyttäjät, joilla on vähän tietoa tietoturvauhkista ja jotka ovat tehneet vähän suojautumistoimenpiteitä, kokevat tietonsa olevan parhaiten turvassa. Nämä käyttäjät turvautuvat teknologian uhkien välttämisteorian mukaisesti tunteisiin keskittyviin suojautumisstrategioihin, eli he uskottelevat itselleen, ettei kukaan ole kiinnostunut heidän tietoistaan ja etteivät uhkat kohdistu heihin.

Käyttäjää pidetään yleisesti tietoturvan kannalta heikoimpana lenkkinä. Näin ollen paras tapa suojella käyttäjiä tietoturvauhkilta, olisi lisätä heidän tietoisuuttaan erilaisista uhkista ja vahvistaa heidän tietotaitoaan suojautua tietoturvauhkilta. Teknologian uhkien välttämisteorian mukaisesti käyttäjä on motivoitunut suojautumaan uhkilta, jos hän omaa riittävän tietotaidon uhkilta suojautumiseen. Tutkielmassa saadut tulokset tukivat siis hyvin kirjallisuudessa esiteltyjä tuloksia ja näiltä osin tutkimuksen tuloksia voidaan pitää luotettavina. Tutkimuksessa oli kuitenkin mukana vain 14 haastateltavaa, joten saadut tulokset eivät ole laajasti yleistettävissä. Lisäksi tutkielmassa verrattiin sekä tavallisten käyttäjien että IT-alan ammattilaisten vastauksia toisiinsa. Tässäkin saadut tulokset saavat tukea kirjallisuudesta, joten niitä voidaan pitää pätevinä. IT-alan ammattilaisia oli kuitenkin vain 2 mukana tutkimuksessa, joten kovin laajoja yleistyksiä ei tästäkään voi tehdä.

Laajentamalla tutkimuksen otantaa, saadaan useita mahdollisia jatkotutkimusaiheita esiin. Suuremmalla otannalla saataisiin luotettavampaa ja yleistettävämpää tietoa siitä, millä tasolla tavallisten käyttäjien tietämys on tietoturvasta. Jos tutkimukseen saataisiin lisää myös IT-alalla työskenteleviä, saataisiin varmempaa tietoa siitäkin, kuinka IT-alan ammattilaisten ja tavallisten käyttä-

jien tietämys tietoturvauhkista eroaa ja millaisia eroja näiden ryhmien välillä on suojautumiskeinoissa. Myös teknologian uhkien välttämisteorian kannalta voisi tutkia tarkemmin suuremmalla otannalla sitä, millä tasolla TTAT toteutuu eri käyttäjien kohdalla. Jokainen käyttäjä on kuitenkin oma yksilönsä ja näin ollen esimerkiksi tehdyt tietoturvaa parantavat toimet eroavat suuresti eri käyttäjien välillä, joten olisi mielenkiintoista tutkia sitä, miten turvassa tietonsa kokevat olevan esimerkiksi henkilöt, jotka tietävät melko paljon tietoturvauhkista ja ovat tehneet useampia tietoturvaa parantavia toimia.

LÄHTEET

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *Computers and Communication (ISCC), 2015 IEEE Symposium on* (s. 180-187). IEEE.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer networks*, *56*(16), 3594-3608.

Bamiah, M. A., & Brohi, S. N. (2011). Seven deadly threats and vulnerabilities in cloud computing. *International Journal of Advanced engineering sciences and technologies*, *9*(1), 87-90.

Berte, D. R. (2018, May). Defining the IoT. In *Proceedings of the International Conference on Business Excellence* (Vol. 12, No. 1, s. 118-128). Sciendo

Chaudhari, F., & Patel, S. (2017). A Survey: Trojan horse Detection Techniques in Network.

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, *10*(1), 247-256.

Dabbagh, M., & Rayes, A. (2019). Internet of things security and privacy. In *Internet of Things From Hype to Reality* (s. 211-238). Springer, Cham.

Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: a survey. In *I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on* (s. 32-37). IEEE.

Diao, W., Liu, X., Zhou, Z., & Zhang, K. (2014, November). Your voice assistant is mine: How to abuse speakers to steal information and control your phone. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices* (s. 63-74). ACM.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on* (s. 618-623). IEEE.

Eriksson, P., & Koistinen, K. (2014). Monenlainen tapaustutkimus. Kuluttajatutkimuskeskus.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

Habibi, J., Midi, D., Mudgerikar, A., & Bertino, E. (2017). Heimdall: Mitigating the internet of insecure things. *IEEE Internet of Things Journal*, *4*(4), 968-978.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, *48*(3), 37.

Hirsjärvi, S. & Hurme H. (2008). Tutkimushaastattelu – Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita. (15. uud. painos). Helsinki: Tammi.

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

Karlof, C., & Wagner, D. (2003, May). Secure routing in wireless sensor networks: Attacks and countermeasures. In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on* (s. 113-127). IEEE.

Kazim, M., & Zhu, S. Y. (2015). A survey on top security threats in cloud computing.

Khoo, B. (2011, October). RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. In *Internet of Things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*(pp. 709-712). IEEE.

Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2010). Smart objects as building blocks for the internet of things. *IEEE Internet Computing*, *14*(1), 44-51.

Leo, M., Battisti, F., Carli, M., & Neri, A. (2014, November). A federated architecture approach for Internet of Things security. In *Euro Med Telco Conference (EMTC), 2014* (s. 1-5). IEEE.

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), 394-413.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In *Internet* Technology *and Secured Transactions (ICITST), 2015 10th International Conference for* (s. 336-341). IEEE.

Makkonen, P., & Siakas, K. (2019). Three quality attributes - availability, performance and security : of social media services used in higher education. In K. Graziano (Ed.), SITE 2019 : *Proceedings of the 30th International conference of Society for Information Technology and Teacher Education* (s. 1964-1969). Chesapeake: Association for the Advancement of Computing in Education (AACE). https://www.learntechlib.org/p/207915/

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classification of RFID attacks. *Gen*, *15693*, 14443.

Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials*, *11*(4).

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004, April). The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks* (s. 259-268). ACM.

Patel, K. K., & Patel, S. M. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, *6*(5).

Ritchie, J., & Spencer, L. (2002). Qualitative data analysis for applied policy research. In *Analyzing qualitative data* (s. 187-208). Routledge.

Ronen, E., & Shamir, A. (2016, March). Extended functionality attacks on IoT devices: The case of smart lights. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on* (s. 3-12). IEEE.

Schlegel, R., Zhang, K., Zhou, X. Y., Intwala, M., Kapadia, A., & Wang, X. (2011, February). Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In *NDSS* (Vol. 11, s. 17-33).

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2018). A survey on sensor-based threats to internet-of-things (iot) devices and applications. *arXiv preprint arXiv:1802.02041*.

Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2014). Evolution, detection and analysis of malware for smart devices. *IEEE Communications Surveys & Tutorials*, *16*(2), 961-987.

Vaarama, V. (2019, 11. helmikuuta). Verkkohyökkäys voi lamaannuttaa sairaalan – esimerkkejä löytyy jo Suomestakin. Haettu 16.1.2020 osoitteesta https://yle.fi/uutiset/3-10640642

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198.

Wahid, A., & Kumar, P. (2015). A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network. *International Journal for Innovative Research in Science and Technology*, *1*(8), 189-196.

Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, *57*(3), 221-224.

Yu, S. (2014). Distributed denial of service attack and defense (s. 15-29). Springer New York.

Zhang, Z. K., Cho, M. C. Y., & Shieh, S. (2015, April). Emerging security threats and countermeasures in IoT. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (s. 1-6). ACM.

LIITE 1 HAASTATTELURUNKO

Haastateltavien taustatiedot (ikä, sukupuoli, ammatti) lupa äänittämiseen

Tutkimuksen tavoitteen kertominen

Termin älylaitteet määrittely tässä tutkimuksessa: Laitteita, jotka ovat yhteydessä internetiin ja jotka yhdistävät fyysisen ja virtuaalisen maailman. Mm. älypuhelimet, tabletit, kannettavat tietokoneet, älykellot, tulostimet, älykkäät kodinkoneet kuten jääkaapit ja älytelevisiot, autojen tietokoneet, älykodit kuten lämmitysjärjestelmät, jätehuolto ym.

Mitä älylaitteita käytössä

Nykyinen tietämys älylaitteisiin kohdistuvista tietoturvahyökkäyksistä -> Mitä hyökkäyksiä tiedät olevan olemassa? Mihin laitteisiin hyökkäykset kohdistuvat? Mitkä tiedot ovat hyökkäyksissä uhattuina?

Kuinka huolestunut olet omasta tietoturvasta? -> Koetko tietojesi olevan turvassa? Miksi/miksi et?

Oletko tehnyt joitain tietoturvaa parantavia toimia? Millaisia?

Arvio asteikolla 1-10 kuinka turvassa kokee tietojensa olevan, 1=ei ollenkaan turvassa, 10=täysin turvassa

Yleisimpien uhkien esittely (mikrofonin salakuuntelu, tietojenkalastelu, haittaohjelmat, tilin kaappaus, palvelunestohyökkäys)

Mitä ajatuksia uhkat herättivät?

Kuinka huolestunut olet omasta tietoturvastasi nyt? Mitkä omista tiedoistasi koet olevan turvassa/uhattuina?

Arvio nyt asteikolla 1-10 kuinka turvassa kokee tietojensa olevan, 1=ei ollenkaan turvassa, 10=täysin turvassa, vaikuttiko saatu tieto?

Aiotko muuttaa älylaitteiden käyttöä tulevaisuudessa? -> Jos kyllä, miten/ jos et, miksi et?

Minkä esitellyistä uhkista koet uhkaavimmaksi ja miksi?

➔ Laita hyökkäykset järjestetykseen uhkaavimmasta vähiten uhkaavaan

Koetko, että omaat tarvittavat tiedot/taidot tietoturvauhkilta suojautumiseen?

Pitäisikö tietoisuutta tietoturvauhkista lisätä? Kenelle pitäisi erityisesti suunnata?