Haaga-Helia
ammattikorkeakoulu Oy

Kotitalouksien älykodinkoneiden käyttöohjeet tietoturva-riskeiltä suojautumiseen

Tarja Lehmussaari

Opinnäytetyö
Tietojenkäsittely
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Tarja Lehmussaari

Koulutusohjelma
Tietojenkäsittely

Raportin/Opinnäytetyön nimi
Kotitalouksien älykodinkoneiden käyttöohjeet tietoturvariskeiltä suojautumiseen

Sivu- ja liitesivumäärä
38 + 1

Opinnäytetyön tavoitteena on selvittää älykodinkoneisiin liittyviä tietoturvariskejä ja niiltä suojautumista sekä tutkia mitä tietoturvariskeiltä suojautumiseen liittyvää laitevalmistajat ovat ottaneet huomioon käyttöohjeissaan ja miten niissä ohjeistetaan kuluttajaa.

Opinnäytetyö on laadullinen tutkimus ja rajattu koskettamaan Suomessa markkinoilla olevia älykodinkoneita, joihin löytyy suomenkielinen käyttöohje vapaasti saatavana Internetistä. Tämä opinnäytetyö kertoo älykodinkoneesta ja sitä ympäröivästä integraatiosta, tietoturvariskeistä, tietoturvasta sekä kodinkoneiden käyttöohjeista. Opinnäytetyö auttaa ymmärtämään kokonaisuutta, johon älykodinkone liittyy ja sitä kautta tarvetta käyttöohjeistuksen antamiin neuvoihin tietoturvariskeiltä suojautumiseen. Käyttöohjeista tehty tutkimus on tehty sisältöanalyysilla, lukemalla laitteisiin liittyvät käyttöohjeet ja etsien niistä kuluttajaohjeistusta riskeiltä suojautumiseen. Apuna tutkittaessa käyttöohjeita on käytetty Viestintäviraston antamaa muistilistaa kuluttajalle IoT-laitteen hankinnasta. Näkökulmana opinnäytetyössä on kuluttaja.

Opinnäytetyön keskeisimpiä tuloksina voidaan todeta, että älykodinkoneisiin liittyvät merkittävimmät tietoturvariskit ovat haittaohjelmat ja laitteen käyttö palvelunestohyökkäyksessä, jotka vaikuttavat suuresti älykodinkoneen toimivuuteen sekä välillisesti voivat aiheuttaa vahinkoa kodin muihin laitteisiin ja niissä säilytettäviin tietoihin. Vähimmäisvaatimukset älykodinkoneen suojaukselle ovat automaattiset ohjelmistopäivitykset, asetuksiin pääsyn esto salasanoin sekä salasanojen vaihtamisen mahdollisuus. Käyttöohjeissaan laitevalmistajat ovat ottaneet nämä vaatimukset huomioon vaihtelevasti ja osin puuteellisesti, sillä mainintoja näistä ei löytynyt kaikista tutkituista ohjeista. Käyttöohjeet noudattavat kuluttajaturvallisuuslakia, jossa vaatimuksena on Suomessa myytävien kulutustavaroiden käyttöohjeiden suomenkielisyys.

Opinnäytetyön materiaali on kerätty syksyn 2017 – helmikuun 2018 välisenä aikana ja aiheen ajankohtaisuudesta kertoo se, että haavoittuvuuksia älykodinkoneissa ja sen integraatiossa käytetyistä tekniikoista on löydetty tällä ajanjaksolla kuukausittain.

Asiasanat

Tietoturva, tietoturvariski, käyttöohje, älykodinkone, IoT

Sisällys

1 Johdanto

Internet-verkkoon kytketystä kodinkoneesta käytetään yleisesti nimitystä älykodinkone, joka puolestaan kytkeytyy IoT (Internet of Things) käsitteeseen. Yleisesti IoT-laitteiden ongelmana nähdään niiden heikko tietoturva. Tästä todisteena ovat raportoidut palvelunestohyökkäykset, joiden toteutuksessa on käytetty kodeissa olevia suojaamattomia yhteyksiä ja älylaitteita. (Turvallisuuskomitea 2017, 7-9.) Suojaamattomat älykodinkoneet, verkkoyhteydet ja kodin muut verkkoon kytketyt laitteet yhdessä muodostavat tietoturvariskejä. Näistä mahdollisista tietoturvariskeistä tai niiltä suojautumiseen valmistajat ja myyjät eivät kerro kuluttajalle riittävän selkeästi ja yksinkertaisesti. Kuluttajalle ei välttämättä ole osaamista tai tietoa laitteisiin liittyvien tietoturvariskien arviontiin ja hahmottamiseen. Mikäli kuluttaja haluaa ennen ostopäätöstään tehdä vertailua tai tutustua älykodinkoneen teknisiin ominaisuuksiin, kodinkoneen verkko-ominaisuuksiin, hallintasovelluksiin ja näihin liittyviin riskeihin ja niiltä suojautumiseen, tulisi ne näkyä helposti ja selkeästi laitteen käyttöohjeissa tai tuoteselosteessa.

Uhkat ja tietoturva-aukot kodin älylaitehallinnassa jakaantuvat useaan kodin tekniikan integraation osaan ja tietoturvariskien laajuus riippuu siitä, millaisia laitteita kodin verkkoon on liitetty. Uhkat ja tietoturva-aukot riippuvat myös verkkoyhteyksistä, laitteiden ja ohjelmistojen suojauksesta, miten ja kuka sovelluksia käyttää, millaisia tietoja ladataan sekä mitä tietoa laitteisiin on talletettu. Älykodinkoneiden tietoturvariskit muodostuvat kodin laiteintegraation heikoimman kohdan kautta (älykodinkone, yhteydet, sovellukset, muut älylaitteet tai ihminen). Älykodinkoneen tietoturvariskien todennäköisyyteen vaikuttaa myös suuresti se, ovatko laitteissa toteutetut ratkaisut tietoturvallisia sekä onko laitteille saatavissa puutteita korjaavia päivityksiä. (Norppa & Peltomäki 2015, 126-127.)

Älykodinkoneiden liittyvät tietoturvauhkat ovat usein tietoturva -asiantuntijoiden havaitsemia ja he osaavat arvioida näitä riskejä sekä suojautua niiden varalta. Riskien hallinta on myös haasteellinen tietotekniikan osa-alue, joka vaatii osaamista, aikaa ja pitkäjänniteisyyttä sekä sen on oltava jatkuvaa. Kuluttaja-kotitalous, jolla ei ole tarvittavaa tietoteknistä osaamista, harvoin laatii kodin tietoturvasuunnitelmaa, toteuttaa sellaisen tai ylläpitää sitä säännöllisesti.

Opinnäytetyön tavoitteena on selvittää älykodinkoneisiin liittyviä tietoturvariskejä ja niiltä suojautumista sekä tutkia mitä tietoturvariskeiltä suojautumiseen liittyvää laitevalmistajat ovat ottaneet huomioon käyttöohjeissaan ja miten niissä ohjeistetaan kuluttajaa. Opinnäyte on rajattu koskettamaan Suomessa markkinoilla olevia älykodinkoneita, joihin löytyy

suomenkielinen käyttöohje vapaasti saatavana Internetistä. Älykodinkoneen tietoturvariskeistä selvitetään vain vaikutukseltaan merkittävät, joista on raportoituja haavoittuvuuksia. Näkökulmana on kuluttajakotitaloudet, koska usein tietoturvallisuutta käsitellään vaikeasti ymmärrettävässä muodossa.

Opinnäytetyön teoriaosuus sisältää selvityksen älykodinkoneiden tietoturvariskeistä ja niiltä suojautumista. Tutkimusosa käsittää sisältöanalyysin älykodinkoneiden käyttöohjeista. Teoriaosuus toimii käyttöohjeista tehtävää tutkimusta varten ohjaavana viitekehyksenä. Nämä yhdessä kytketään tuloksina, joista yhteenveto löytyy pohdintaosuudessa. Opinnäytetyön teoriaosuus koostuu kahdesta pääotsikosta: ”Kotitalouksien älykodinkoneet” sekä ”Tietoturvariskit ja niiltä suojautuminen”. Luvussa 2 esitellään yleisellä tasolla älykodinkonetta, sen liittämistä kodin verkkoon sekä keskeisesti älykodinkoneeseen liittyvästä hallinnasta. Luvussa 3 keskitytään tietoturvariskeihin, riskeiltä suojautumiseen sekä käyttöohjeisiin. Käyttöohjeiden tutkimusosio (luku 4) sisältää esittelyn tutkimuksen tavoitteista, kohteista, menetelmistä, aineistosta. Tutkimuksen tuloksissa kerrotaan valittujen älykodinkoneiden käyttöohjeiden sisällöt ennalta määriteltyjen kysymysten avulla. Pohdinnassa esitetään koko opinnäytetyön keskeiset tulokset, pääkysymyksiin vastaukset, johtopäätökset tutkimuksesta sekä koko opinnäytetyön prosessin kulusta.

Opinnäytetyön keskeiset käsitteet ovat IoT, älykodinkone, tietoturvariski, tietoturva ja käyttöohje. IoT (Internet of Things) tarkoittaa laitteiden keskinäistä kommunikointia koko maailmaa käsittävän Internet-verkon yli (Miller 2015, 6-7).

Älykodinkone on kodinkone, joka varsinaisen rutiininomaisten perustoimintojensa lisäksi suorittaa verkkoyhteyden kautta annettuja käskyjä- Verkkoyhteys mahdollistaa laitteen toimintojen ja asetusten ohjaamista muilla älylaitteilla, käytönaikaisen tiedon välittämisen laitetoimittajalle ja laitteen omistajalle sekä kommunikoinnin toisten älylaitteiden kanssa.

Tietoturvariski määritellään Valtionhallinnon tietoturvasanastossa (Valtionvarainministeriö 2008, 111), että se on ”Tietoon, tietoliikenteeseen tai tietojärjestelmään kohdistuva vahingon vaara”.

Tietoturva käsittää suojaustoimenpiteitä, joilla näitä mahdollisia tietoturvariskejä pyritään estämään tai vähentämään.

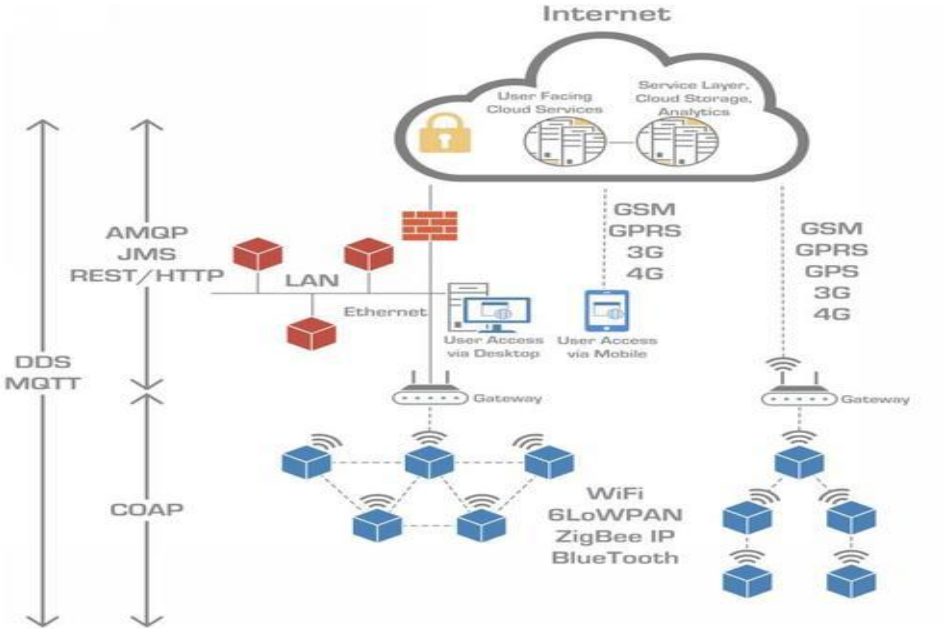
Käyttöohjeella tarkoitetaan kuluttajalle annettavaa dokumenttia, joka ymmärrettävällä tavalla ohjeistaa kuluttajaa asentamaan sekä käyttämään laitetta turvallisesti. Käyttöohje yleisesti sisältää tietoa, varoituksia sekä huomautuksia.

2 Kotitalouksien älykodinkoneet

Suomessa myytäviin kodinkoneisiin, joihin on liitetty Internetin välityksellä tapahtuvaa ohjausta ja monitorointia, ovat tyypillisimmin jääkaappeja, pyykinpesukoneita, kuivausrumpuja, astianpesukoneita, robotti-imureita sekä mikroaaltouuneja (kuva 1).

Kuva 1. Älykodinkoneita (Neato; Bosch; Samsung).

Näitä älykodinkoneita voidaan ohjata ja monitoroida älypuhelimiin asennettavilla -sovelluksilla, jotka laitteen valmistaja tarjoaa laitekohtaisesti ja, jotka ovat vapaasti ladattavissa Internetistä. Laitteiden älyominaisuuksia voidaan ohjata myös suoraan siinä itsessään olevien näyttöjen ja painikkeiden avulla. Osa laitevalmistajista tarjoaa hallintamahdollisuuden samaan laiteperheeseen kuuluvien älylaitteiden avulla. Tällaisia muita älylaitteita voivat olla esimerkiksi älytelevisiot. Jotta kodinkoneesta saadaan älykäs, siihen on rakennettu sulautettu käyttöjärjestelmä sekä komponentti, joka on yhteydessä suoraan tai langattomasti kodin tiedonsiirtolaitteiden välityksellä Internettiin. Älylaitteiden keskinäinen kommunikointi ja integroituminen verkkoon voidaan toteuttaa useilla eri teknologioilla (kuva 2).



Kuva 2. Internet of Things environment (EETimes 2015).

Kuvassa 2 oikealla alhaalla näkyvät laitteet ovat langattomasti yksin tai yhdessä liitettyinä reitittimeen, joka puolestaan ottaa radioyhteyksin yhteyden Internettiin. Keskellä kuvaa nähdään tyypillinen älykodinkoneen integraatio, jossa kodinkone ja muut laitteet ottavat yhteyden kodissa olevaan tukiasemaan, joka puolestaan on yhteydessä langallista verkkoa pitkin verkkoyhteyden tarjoavan palvelun tuottajan kautta Internettiin. Hallintasovelluksia voi olla puhelimien ja muiden päätelaitteiden kautta takaisin älykodinkoneeseen tai suoraan langattomassa verkossa. Vasemmalla kuvassa mainitaan viestintään liittyviä protokollia, joita käytetään tiedonsiirrossa. Seuraavissa alaluvuissa kerrotaan kuvaan liittyvistä osista sekä määritelmistä, jotta älykodinkoneeseen liittyvät haavoittuvuuden osa-alueet tietoturvan näkökulmasta saadaan hahmotettua.

2.1 Älykodinkoneen integrointi kotiverkkoon

Useimmat älykodinkoneet vaativat langattoman verkon ja sitä käyttäen pääsyn Internettiin sekä ohjelmiston, jolla laitteistoa hallitaan ja monitoroidaan. Kotitalouksissa on yleisesti vain yksi tukiasema ja yksi yhteys (kuva 3). Vain siten voisi turvautua tietoturvariskeiltä tehokkaammin ja vahingon laajuutta rajoittaa vain kyseiseen laitteeseen ja siihen kytkettyihin tietoliikenne osiin. Älykodinkone on kuitenkin vain yksi laite kodin muiden verkkoon liitettyjen laitteiden joukossa ja kiinteillä kaapeleilla integraation rakentaminen on käytännössä lähes mahdotonta. Yleisiä Suomessa myytävissä älykodinkoneissa käytettyjä langattomia verkkoyhteyksiä ovat WiFi ja Bluetooth, jotka mainitaan laitteiden myyntiesitteissä. Nämä ovat kaupallisia nimityksiä ja toteutuksia WLAN (Wireless Local Area Network) käsitteen sisällä (Cisco 2014b, 194-197).

Kuva 3. Kotiverkko (MikroPC).

WLAN (Wireless Local Area Network) ja **Bluetooth** ovat yleisiä nimityksiä langattomalle lähiverkolle. Langaton lähiverkko on toteutettu radioaalloilla, joka mahdollistaa sen, ettei laitteesta tarvita fyysistä verkkokaapelia reitittimeen tai modeemiin (Turvallisuuskomitea 2017, 11).

Langattomien yhteyksien kohdalla puhutaan IEEE-standardeista (Institute of Electrical Engineers), jotka käytännössä ovat yhteisesti sovittuja, toteutettuja ja käytettyjä tekniikoita tiedon siirtämiseen radioteitse. Standardeista on useita versioita ja toteutuksia, joita on käytetty erilaisissa kaupallisissa lähiverkko toteutuksissa. Langattomat yhteydet käyttävät tiedonsiirtostandardia IEEE 802.11, IEEE 802.15 tai IEEE 802.16, joiden merkittävin ero on niiden tiedonsiirtonopeudessa ja radiotaajuudessa. Näistä standardeista on myös julkaistu useita versioita, joissa on pyritty tehostamaan tiedonsiirtonopeuksia. (Cisco 2014b, 194-197.)

WiFi käyttää IEEE 802.11 tiedonsiirtostandardia ja riippuen hankitun tiedonsiirto ersioita. Uusimman version tiedonsiirtonopeus on 54 Mbps. Bluetooth käyttää IEEE 802.15 tiedonsiirtostandardia, jonka maksimi tiedonsiirtonopeus on 3 Mbps. (Cisco 2014b, 197.)

Älykodinkoneiden käyttämät langattomat verkot WiFi ja Bluetooth käyttävät tiedonsiirron suojaamiseen salausta, salauksen purkamista sekä tietoihin pääsyn valvontaa. Tällaisia tekniikoita nimeltään ovat WEP (Wired-Equivalent Privacy), WPA (WiFi Protected Access) ja WPA2 (uusin versio WPA:sta) ja niistä puhutaan yleisesti protokollina. Heikoimman langattoman verkon suojauksen antaa yhteys, joka käyttää WEP protokollaa siinä havaittujen puutteiden vuoksi. Käytännössä WPA ja WPA2 ovat uudempia versioita WEP-protokollasta. (Cisco 2014b, 615-616.)

2.2 Älykodinkoneiden hallintasovellukset

Älykodinkoneen hallintasovellusta voidaan käyttää itse älykodinkoneessa sekä muissa kodin älylaitteissa (mobiililaitteet ja älytelevisio) riippuen älykodinkoneesta. Älykodinkoneessa oleva paneelin kautta hallinta yleisimmin rajoittuu lähinnä laitteen käynnistämiseen ja sammuttamiseen, laitteen toiminnan seuraamiseen, verkkoyhteyksien käsittelyyn sekä tehdasasetusten palauttamiseen. Kehittyneemmissä älykodinkoneissa paneelin kautta voidaan käsitellä erilaisia dokumentteja, niissä olevien kameroiden toimintaa sekä vaikkapa musiikin kuuntelua. Hallintasovelluksen pääasiallinen käyttö on kuitenkin tarkoitettu älypuhelimille tai tableteille. Periaatteena on ensin ladata laitteistotoimittajakohtainen sovellus älypuhelimeen tai tablettiin, rekisteröityä ja kirjautua käyttäjätilikohtaiseen palveluun ja tämän jälkeen hallita älykodinkonetta etäyhteyden kautta. Hallintasovellukset pyytävät

syöttämään erilaisia tietoja riippuen laitteesta. Mobiili-sovellus Home Connect (2015) kysyy seuraavia tietoja rekisteröitymisvaiheessa:

- etunimi
- sukunimi
- sähköpostiosoite
- kodinkoneen käyttömaa
- salasana eli käytön suojaus.
- mobiililaitteen kieliasetukset
- kuittaukset käyttöehtojen ja tietosuojalausekkeiden hyväksymisestä
- käyttäjätilin tila (aktivoitu/passivoitu)

Sovellus ja älykodinkone keräävät edellä mainittujen rekisteröitymistietojen lisäksi käytön aikaista tietoa. Tällaisia tietoja ovat esimerkiksi laitetta yksilöivät tiedot kuten merkki, sarjanumero, verkkosovittimen tunniste, kodinkoneen asetukset sekä kodinkoneen toimintojen tilat. (Home-Connect 2015.)

Hallintasovelluksien tietoturvalausekkeita on saatavilla maahantuojien yleisissä tietoturvaselosteissa. Tietoturvalausekkeiden tulkintaa varten tulisi kuluttajan tietää Suomen ja EU:n laissa kerrotut vaatimukset tietojen luovuttamiseen. Tietoja voidaan siis välittää myös sellaisiin maihin, jotka eivät ole tietosuojalain mukaista eikä näin ollen Suomen ja EU:n lainsäädäntö ole enää suojaamassa henkilön yksityisyyttä. Tästä tietojen luovutuksesta ulkopuolisille esimerkkinä seuraava lainaus Home-Connect (2015) tietosuojaselosteesta.

> Sovelluksen ja sen tarjoamien palvelujen järjestämiseksi teemme yhteistyötä erilaisten palveluntarjoajien kanssa. Siinä tapauksessa, että olemme velvoittaneet nämä palveluntarjoajat käsittelemään tietoja tarkasti tietojenkäsittelyn alihankintaa koskevien ohjeiden mukaisesti, sinun suostumustasi tietojenkäsittelyyn näillä palveluntarjoajilla ei tarvita. Muissa tapauksissa, joissa tarvitaan tietosuojasyistä suostumus omien henkilötietojesi luovuttamiseen palveluntarjoajille, ilmoitamme asiasta sinulle erikseen emmekä siirrä tietojasi ilman ennakkosuostumustasi.

3 Tietoturvariskit ja niiltä suojautuminen

Älykodinkoneeseen liittyvät tietoturvariskit eivät ole suoraan lueteltavissa, sillä ensin ne on tunnistettava ja ymmärrettävä mitä riski -sana tarkoittaa. Andrearsson & Koivisto (2013, 41) mainitsevat kirjassaan, että riski terminä voidaan mieltää hyvinkin eri tavoin. Tärkeintä on määritellä riskit käsitteenä ja erotella ne riskitekijästä ja riskivaikutuksista. Älykodinkonetta ajatellen riskivaikutus määritellään tässä yhteydessä riskin aiheuttamaksi vahingoksi. Esimerkiksi laitteen toiminta estyy tai tietoja katoaa ulkopuolisten käsiin. Riskitekijä puolestaan tässä yhteydessä on älykodinkoneen kannalta muu verkon suojaus, kuluttajan tietämättömyys miten suojautua sekä muut laitteet. Riskien tunnistaminen älykodinkoneessa riippuu suuresti siitä, millaisia toimintoja siinä on ja sekä mitä siihen voidaan tallettaa. Toisaalta älylaite voi huonosti suojattuna olla reitti hyvin erilaisten riskien leviämiseen kodin muihin laitteisiin, jolloin kaikissa verkkoon kytketyissä laitteissa oleva tieto on vaarassa. Suomessa ja maailmalla raportoitujen IoT-haavoittuvuuksien perusteella voidaan älykodinkoneiden merkittävimmiksi tietoturvariskeiksi tunnistaa haittaohjelma ja palvelunestohyökkäys. (Turvallisuuskomitea 2017; Viestintävirasto 2015a).

Haittaohjelmia voivat olla esimerkiksi mato ja virus, jotka leviävät koneesta toiseen hidastaen tai estäen verkkoon kytkettyjen laitteiden normaalia toimintaa (Järvinen & Rousku 2017, 178). Haittaohjelma voi olla myös ’ovia’ avaava ohjelma, jolloin se toimii ensin suojauksia purkavana ja luo pääsyn muille tiedon kannalta haitallisemmille ohjelmille. Tällaiset ohjelmat etsivät kaikista suojaamattomista laitteista salasanojen purkua ja pyrkivät pääsemään verkossa kaikkiin laitteisiin sekä käyttäjän salaamiin tietoihin ja esimerkiksi toimivat kiristysohjelmina kodin kannettavissa tietokoneissa. Palvelunestohyökkäys tarkoittaa suurta haitallista tietoliikennemäärää, joka on kohdistettu jollekin palvelun tarjoajan Internet-sivustolle. Tämä haittaa ja estää kyseisten sivujen käytön (esimerkiksi pankkipalveluiden käytön) ja siinä on mukana kotien suojaamattomia laitteita (esimerkiksi älykodinkoneita). Älykodinkoneen kannalta palvelunestohyökkäyksessä mukana olo voi tukkia oman verkkoliikenteen ja teleoperaattori voi sulkea koko yhteyden estäen kaiken liikenteen turvallisuussyistä. Haittaohjelmat hidastavat laitteiden toimintaa ja älykodinkoneessa haittaohjelma voi estää älykodinkoneen normaalitoiminnot (jääkaappi ei ole kylmä, pesukone ei ota vettä)

3.1 Tietoturvariskin suuruuden arviointi

Riskin suuruuteen vaikuttaa sen todennäköisyys ja laajuus. Kuluttajan näkökulmasta suuruuden määrittää se, mitä kaikkea voi menettää ja onko sillä kuluttajalle suuri merkitys sil-

loin, kun riski toteutuu. Älykodinkoneiden tietoturvariskien arviointeja ei ole helposti saatavilla. Jotta riskeiltä suojautuminen olisi tarkoituksenmukaista, tulisi riskit arvioida ja ryhtyä toimenpiteisiin vähintäänkin sellaisten riskien osalta, jotka ovat merkittäviä, todennäköisiä ja vaikutukseltaan suuria. Jotta suojautumisen tarpeellisuutta voitaisiin pohtia, arvioidaan seuraavassa esimerkissä haittaohjelma -riskiä. Riski on arvioitu Valtionvarainministeriön (2017a) julkaiseman riskienhallintatyökalun avulla (kuva 4).

Työkaluun on syötetty riskin tunnistamisen tiedot sekä arvioitu todennäköisyys ja vaikutus. Työkalu laskee riskin suuruudeksi 9 (sietämätön riski), joka tulee työkalun huomautuksen mukaan huomioida toimenpitein. Värit kertovat vakavuudesta. Punainen väri on merkittävin ja oranssi väri kertoo toiseksi suurimmasta arvosta. Värit auttavat työkalun analysoinnissa kiinnittämään huomiota juuri näihin riskeihin.

Riskien tunnistaminen			Riskien tunnistaminen				Riskin merkityksen arviointi			
Riski (riskin nimi)	Syyt ja tekijät riskin taustalla - miksi riski voi toteutua?	Seurauksia riskin toteutumisesta - mitä voi tapahtua?	Todennäköisyys		Vaikutus		Riskin suuruus (T x V)		Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyky)	
Haittaohjelma	Kodin verkko ja älykodinkone suojaamaton. Riskitekijänä kuluttajan tietämättömyys, ohjeiden riittämättömyys, laitteen ohjelmistopäivitysten ja salasanojen puuttuminen tai puhdas vahinko	Haittaohjelma estää älykodinkoneen laiteen toiminnan ja toimii reittinä haittaohjelman levityksessä. Lopulta tärkeitä tietoja voidaan menettää kodin verkkoon kytketyissä laitteissa.	3	Todennäköinen	3	Merkittävä	9	Sietämätön riski	4	Huomioitava riski

Kuva 4. Haittaohjelma riskin suuruuden arviointi Vahtiohjeen riskienarviointityökalussa (Valtionvarainministeriö 2017a)

Valtionvarainministeriön (2017b) Vahtiohjeen todennäköisyyden 3 (todennäköinen) kriteerejä ovat mm:

- Toimintoon tai järjestelmään pääsy on helppoa
- Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa
- Toiminnon ohjeistusta ei ole
- Tapahtuma ilmenee kerran kuukaudessa
- Uhkan toteutuminen on mahdollista suurelle määrälle käyttäjiä

Älykodinkoneen kohdalla edellä mainittuihin kriteereihin vastaukset perusteltuina:

- Toimintoon tai järjestelmään pääsy on helppoa, mikäli laite näkyy suoraan Internettiin tai laitteen sekä verkon suojaus on puutteellinen
- Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa, koska haittaohjelmahyökkäyksiä on jo toteutettu
- Toiminnon ohjeistusta ei ole, sillä ostotilanteessa kuluttajalle ei välttämättä ole tietoa ja käyttöohjeistus ei sisällä ohjeita
- Tapahtuma ilmenee ainakin kerran kuukaudessa, mikäli laite ja sen integraatio ei ole suojattu.
- Uhkan toteutuminen on mahdollista suurelle määrälle käyttäjiä, sillä haittaohjelmien laajuudesta on jo todisteita.

Valtionvarainministeriön (2017b) Vahtiohjeen vaikutuksen 3 (merkittävä) kriteerejä ovat mm:

- Seuraukset koskevat kaikkia tietojen tai palvelujen käyttäjiä
- Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä
- Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin
- Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen
- Toiminta on lainsäädännön velvoitteiden vastaista

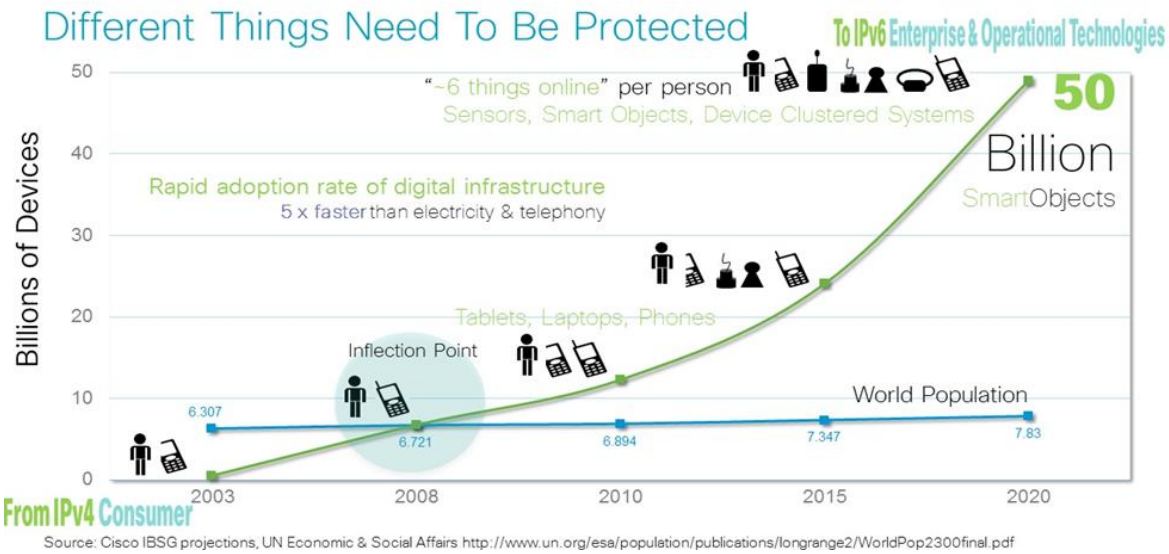
Älykodinkoneen kohdalla edellä mainittuihin kriteereihin vastaukset perusteltuina:

- Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä, koska älykodinkoneiden omistajat ovat saman haavoittuvuuden osallisia
- Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä, sillä haittaohjelma ja sen leviäminen on pyrittävä välittömästi estämään
- Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin on mahdollinen, sillä riippuen haittaohjelmasta se voi estää älykodinkoneen käytön ja kotiverkkoon kytkettyjen kaikkien laitteiden käytön
- Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen on mahdollista, sillä haittaohjelmasta riippuen se on voinut tuhota henkilötietosuojan alla olevia henkilötietoja verkkoon kytketyistä muista laitteista
- Toiminta on lainsäädännön velvoitteiden vastaista, sillä haittaohjelmat ovat rikos

Riskin merkityksen ollessa merkittävä tai suuri, on vähintäänkin niiden osalta ryhdyttävä toimenpiteisiin. Toimenpiteet ovat tietoturvariskeiltä suojautumiseen ovat käsitteenä tietoturva, josta seuraavassa alaluvussa kerrotaan tarkemmin.

3.2 Älykodinkoneisiin liittyvä tietoturvallisuus

Maailmanlaajuisesti älykkäiden koneiden tarjonta ja keskimääräinen henkilön omistama laitteiden määrä kasvaa räjähdysmäisesti (kuva 5). Samalla suojattavien kohteiden määrä kasvaa Ciscon (2014) mukaan ainakin viisi kertaa nopeammin, kuin aikaisemmin on esimerkiksi hankittu puhelimia.



Kuva 5. Älykkäiden koneiden tarjonta (Cisco 2014a)

Samaan aikaan, kun älykodinkoneiden määrä kasvaa maailmalla, kasvaa yksittäisessä kodissa älylaitteiden määrä. Koska älykodinkoneille ei ole välttämättä saatavilla päivityksiä, tulisi jokaisen tehdä toimenpiteitä tietoturvariskeiltä suojautumiseen. Kotitalouksien älylaitteiden ja sitä ympäröivän verkkoon pääsyn mahdollistava tekniikka onkin kaikilta osin suojattava, mikäli haluaa minimoida tietoturvariskien toteutumista (Järvinen & Rousku 2017, 110). Älykodinkone ei ole myöskään tekniikaltaan verrattavissa esimerkiksi älypuhelimiin, josta johtuen laitteiden valmistajat eivät kykene tarjoamaan päivityksiä (Norppa & Peltomäki 2015, 127). Tästä syystä kaikkiin sellaisiin kohtiin, joihin tosiasiallisesti voi vaikuttaa (laitteen ja integraation ohjelmistopäivitykset, virustorjunta, talletetut tiedot, salasanat sekä suostumukset tietojen edelleen käytössä) tulee kiinnittää huomiota. Nämä ovat kohdat ovat tietoturvan kannalta eri osa-alueita ja niitä on kautta-aikojen jaoteltu usealla tavalla. Tietoturva voidaan jaotella tietoturvan osa-alueisiin, jotka ovat luottamuksellisuus, eheys, saatavuus, kiistämättömyys sekä pääsynvalvonta. Tällä jaottelulla pyritään varmistamaan, että kaikkien tietoturvariskien näkökulmat otettaisiin suojauksessa huomioon. (Hakala, Vainio & Vuorinen 2006, 4-5.)

Luottamuksellisuudella tarkoitetaan, että tietojärjestelmässä olevat tiedot ovat vain ja ainoastaan niihin oikeutettujen käytössä eikä niitä luovuteta ulkopuolisille (Hakala, Vainio & Vuorinen 2006, 4). Älykodinkoneessa tällaisia suojattavia tietoja ovat hallintasovelluksessa annettavat laite ja henkilötiedot, joita välitetään laitteiston valmistajalle. Kuluttaja antaa suostumuksen, jos tietoja voidaan välittää edelleen valmistajan yhteistyökumppaneille.

Käytettävyydellä tarkoitetaan, että tiedot ovat saatavilla oikean muotoisina ja silloin kun käyttäjä niitä haluaa tai tarvitsee (Hakala, Vainio & Vuorinen 2006, 4). Käytettävyyttä voi rikkoa esimerkiksi älykodinkoneen tai kodin verkon käyttöönotto muihin tarkoituksiin, jolloin kodinkone ei pysty suorittamaan sen omia tehtäviä. Tällainen riski on esimerkiksi palvelunestohyökkäys, jossa älykodinkonetta käytetään yhtenä resurssina hyökätessä jonkin yrityksen verkkosivuille tai verkossa oleviin palveluihin (Turvallisuuskomitea 2017). Tässä tapauksessa laitteen kapasiteetti on vain tähän hyökkäykseen käytössä eikä sitä pysty hallinnoimaan.

Eheys tarkoittaa laajasti käsitettynä, että tietojen tulee pitää paikkaansa eikä niitä ole muutettu vahingossa tai tahallisesti (Hakala, Vainio & Vuorinen 2006, 4). Eheyttä vaarantavia riskejä ovat esimerkiksi haittaohjelmat. Haittaohjelmat voivat muuntaa ja tuhota kodinkoneen toimintaa ohjaavia tietoja, jolloin tieto ei ole enää alkuperäisessä muodossaan.

Kodinkone ei haittaohjelman vuoksi kykene enää suorittamaan omia toimintojaan tai toiminnot ovat virheellisiä. (Turvallisuuskomitea 2017.)

Kiistämättömyys älylaitehallinnassa liittyy olennaisesti hallintasovelluksiin, joilla älykodinkonetta ohjataan ja joihin annetaan laitteesta sekä käyttäjästä tietoa. Hallintasovellukseen syötetyt tiedot pitää tallentaa ja säilyttää alkuperäisessä muodossa, eikä sitä saa muuttaa (Opetus ja Kulttuuriministeriö). Tämä riski voi toteutua kuluttajalle, mikäli tietoja muutetaan ilman tietojen omistajan toimenpiteitä tai lupaa. Laitevalmistajan on pyydettäessä todistettava, kuka tietoja on tallettanut, mikäli kuluttaja kiistää tietojen oikeellisuuden.

Pääsynvalvonta tarkoittaa, että tunnistetulla käyttäjällä on pääsy ennakolta sovittuihin tietoihin (Hakala, Vainio & Vuorinen 2006, 4). Tässä tapauksessa vain kuluttajalla on pääsy hallintasovellukseen ja omiin syöttämiinsä tietoihin sekä antamiinsa laiteohjaustietoihin ja asetuksiin. Pääsynvalvontaa älylaitteessa rajoitetaan salasanoilla sekä kytkemällä hallintasovellus vain tiettyyn älykodinkoneeseen. Pääsynvalvontaa suorittaa sekä hallintasovellus, laite että koko kodin integraatioon asetetut rajoitukset.

3.2.1 Verkkoon liitetyt muut laitteet

Jokaisessa kodin tietoverkkoon liitetyssä laitteessa tulee vähimmäisvaatimuksena asentaa ohjelmistopäivitykset aina kun se on mahdollista, laatia laitekohtaiset salasanat sekä laitteesta riippuen asentaa virustorjuntaohjelmistot. Tämä koskee kaikkia kotitaloudessa käytettäviä tietokoneita, älypuhelimia, tabletteja, viihde-elektroniikkaa, kodin turvallisuuselektroniikkaa, tietoliikenne tekniikkaa niin kotona kuin talossa tai taloyhtiössä. Tämä on tärkeää sillä, älykodinkoneiden tietoturvapuutteiden vuoksi ne voivat paljastaa laitteen tunnistetiedot Internettiin (Viestintävirasto 2015a). Lähtökohtana IoT-laitteiden kytkennässä tulee Viestintäviraston ohjeistuksen mukaan olla se, että ne eivät näkyisi julkiseen Internettiin vaan niihin olisi pääsy vain kodin sisäverkon puolelta. Mikäli kodissa on useita erilaisia IoT-laitteita, ne kaikki vaativat omanlaisensa hallintasovelluksen ja saattavat käyttää erilaisia tekniikoita kytkeytyessään kotiverkkoon.

3.2.2 Palomuuri

Palomuuri nimensä mukaisesti toimii esteenä haitalliselle tietoliikenteelle, joka uhkaa kodin tietoturvallisuutta. Palomuuri on joko eri laitteiden käyttöjärjestelmiin sisäänrakennettu ohjelmisto tai erillinen fyysinen laite ohjelmistoineen. Yleisimmin kotitaloudessa olevat palomuurit ovat tietokoneissa, reitittimissä ja modeemeissa. Erillisenä fyysisenä laitteena se on harvinainen kotitalouksissa. Palomuurin tehtävänä on suojata verkkoa tai yksittäistä laitetta verkossa, ennalta annettujen sääntöjen (asetusten) mukaisesti. Sen asetuksia voi

muuttaa joko suoraan laitteesta tai sovellusten kautta esimerkiksi älypuhelimella. Koska palomuuri suojaa vain tietoliikennettä ja siihen itseensä voi liittyä puutteitta, palomuuri ei yksin riitä huolehtimaan verkosta tulevia uhkia vastaan. Asentamalla kaikkiin kodin laitteisiin virustorjunta, voidaan näitä palomuuriin liittyviä heikkouksia korjata. (Andrearsson & Koivisto 2013, 24.)

3.2.3 Langaton verkko

Älykodinkoneiden käyttämät langattomat verkot WiFi ja Bluetooth käyttävät tiedonsiirrossaan WEP, WPA tai WPA2 salaus- ja pääsynhallinta protokollaa. Langattoman verkon yhteydessä suojaustoimenpiteenä kuluttaja voi vaihtaa WLAN-tukiasemassa käytettävän salauksen mahdollisimman uuteen, joka tällä hetkellä tarkoittaa WPA2-salausta. Sen lisäksi tukiasemaan syötettävä salasana kannattaa vaihtaa mahdollisimman vahvaksi (mahdollisimman pitkä, ennalta-arvaamaton, erilaisia merkkejä). Tukiasemassa voidaan myös vaihtaa SSID:n (Service Set Identifier) asetuksia. SSID tarkoittaa langattoman verkon tunnistetta esimerkiksi sille annettu nimi. Tämän voi tukiasemassa muuttaa näkymättömäksi, jolloin se ei näy sisäverkosta ulospäin Internet:iin. Tämä sinänsä ei estä tietoverkkoon murtautujia, mutta vähintäänkin hidastaa sitä.

Pelkästään vuoden 2017 syksyllä Viestintävirasto on raportoinut useita haavoittuvuuksia, jotka koskettavat sulautettuja käyttöjärjestelmiä ja salaustekniikoita. Kodinkoneissa käytettyjä salaustekniikoita mainitaan maahantuojien tietoturvaselostuksissa, jotka ovat esimerkiksi WPA2, TSL, AES. Näitä salaustekniikoita käytetään kodin langattomissa yhteyksissä WiFi ja Bluetooth. WiFi-yhteydestä löytyi lokakuussa WPA2-salaustekniikkaan liittyvä haavoittuvuus, joka vaikuttavat sulautettuihin järjestelmiin, reitittimiin, palomuureihin sekä digiboxeihin (Viestintävirasto 2017b). Bluetooth yhteyden toteutusten vanhoista versioista löydettiin syyskuussa haavoittuvuus, joka mahdollistaa ulkopuolisen suorittaa omia komentojaan (Viestintävirasto 2017c).

3.2.4 Älypuhelimet, tabletit

Älykodinkoneiden hallintasovellukset ladataan laitteesta riippuen sovelluksia tarjoavien yritysten sivuilta. Tietoturvan näkökulmasta, on syytä tarkistaa, mistä sovelluksen lataa. Käyttäjän tulee varmistaa, että sivu on ladattu varmuudella juuri älykodinkoneen ohjeistuksen mukaiselta Internet-sivustolta.

Itse älypuhelimet ja tabletit on syytä suojata virustorjuntaohjelmistoilla sekä asentaa ohjelmistopäivitykset aina, kun ne ovat mahdollisia ja tarjolla. Virustorjuntaohjelmistojen asentamisen ongelmana on, ettei kaikille puhelimille ole tarjolla erillisiä suojausohjelmia.

Android-laitteille on tarjolla puhelimeen liitettäviä suojausohjelmia, IPhone-laitteille ei ole tarjolla erillisiä suojausohjelmia, joten niiden suojaus ensisijaisesti perustuu Applen kehittämiin itse laitteessa oleviin suojausmenetelmiin ja tekniikoihin. Turvallisuutta lisää luonnollisesti laitteiden suojaus PIN-koodilla sekä uusimmissa malleissa olevat sormenjälki -tunniste. Sormenjälki toimii suojauksena paremmin, sillä sitä on vaikeampi kopioida. (Mikrobitti 10/2016.)

Uusimmat ja kalleimmat mobiililaitteet ovat suosittuja varkauden kohteita. Laitteen käyttöä tilanteessa, jossa se on varastettu, voidaan estää esimerkiksi Elisan Turvapaketissa olevalla Finder-toiminnolla. Finder-toiminnon avulla voit etsiä kadonnutta laitetta ja toistaa äänekkään hälytyksen laitteessa (Elisa).

3.2.5 Käyttäjät

Käyttäjälle asetetaan IoT-laitteiden hallinnassa luonnollisesti suurin vastuu. Mikäli laite yhdistetään verkkoon, tulee laitteen omistajan tutustua ohjeisiin, sopimuksiin sekä suojata koko verkko. Kaikkien kotiverkkoon kytkeytyvien laitteiden käyttäjien tulee olla tietoisia riskeistä ja esimerkiksi perheen jäsenten käyttämiin mobiililaitteisiin tulisi asentaa suojausohjelmia, joista edellä kerrottiin. Kuluttajan olisi ymmärrettävä kokonaisuus, johon hankittu älykodinkone kuuluu ja perehtyä ensin modeemin, reitittimen ja kaikkien verkkoon liitettyjen laitteiden suojaamiseen käyttöohjeiden mukaisesti. Tämä voi olla vaikeaa, koska kaikki laitteet ja ohjelmistot hankitaan erillisinä, eikä kokonaisuutta välttämättä hahmoteta liitettäessä lisää laitteita kotiverkkoon. Vaikeutta lisää se, ettei älykodinkoneiden käyttöohjeissa tai myyntitilanteessa välttämättä kerrota mahdollisista käytön riskeistä. Lisäksi haasteena on kodin suuri älylaitteiden määrä ja käyttäjinä perheessä on myös lapsia sekä perheessä vierailevia henkilöitä, joiden laitteiden käyttöä silloin kun ne ovat kytkettynä kodin sisäverkkoon tulisi ohjeistaa ja valvoa.

Viestintäviraston johtava tietoturva asiantuntija Huopio esitelmöi Lahdessa 21.9.2017 pidetyssä Teknologiayrittäjyyspäivillä kyberturvallisuudesta (Viestintävirasto 2017c). Esityksessä todetaan, että IoT-laitteen käyttöön liittyvät tietoturvaongelmat ovat vakavia, eivätkä käyttäjät tiedä tai osaa suojautua riskeiltä.

3.2.6 Hallintasovellukset

Kuten aiemmin kerrottiin, älykodinkoneen hallintasovellukset keräävät sekä laitteesta, että käyttäjästä tietoa. Osa tiedoista ovat Suomessa tietosuojan piirissä, mutta antamalla tietoa sovelluksille ja hyväksymällä ehdot, tiedot saattavat siirtyä Suomen ja Eu:n ulkopuo-

lelle maihin, joissa ei ole samanlaista lakiin perustuvaa tietosuojaa kuin Suomessa. Suojautuminen tässä yhteydessä tarkoittaa mobiililaitteen suojausta tarvittavilla virustorjunnoilla, hallintasovellusten päivitysten pitäminen ajan tasalla sekä luovutettavien tietojen ja suostumusten rajoittaminen. Hallintasovellusten avulla älykodinkoneen hallinta voi myös aiheuttaa tahatonta vahinkoa, jolloin vahingon sattuessa ja hallittaessa kaukaa vahinkoja voi olla hankala rajoittaa tai suojata.

3.2.7 Älykodinkoneen hävitys

Yksi IoT-laitteen elinkaaren huomiotta jätetty vaihe on laitteesta luopuminen (myynti tai hävitys). Kun älylaitteesta luovutaan, ei sen hävittämisestä tietoturvariskin kannalta löydy kuluttajalle ohjeistusta, kuten löytyy vaikkapa älypuhelimista ja tableteista. Apple (2017) ohjeistaa verkkosivuillaan: ”Ennen kuin myyt tai luovutat laitteesi, poista siitä kaikki henkilökohtaiset tiedot”. Älykodinkoneeseen voi jäädä muutakin tietoa, kuin edellinen verkon IP-osoite, jos tietoja on voitu syöttää laitteeseen suoraan. Tällaisia tietoja ovat sovellustilin tiedot, käyttäjäasetukset, erillisiä muistioita, valokuvia jne. Älykodinkoneen hävittämisen yhteydessä tai myytäessä laitetta edelleen tulisi muistaa poistaa kaikki henkilökohtainen talletettu tieto sekä tehdastietojen palautus, mikäli se on laitteessa mahdollista.

3.3 Laitetoimittajien ja kuluttajan vastuu tietoturvariskin toteutuessa

Tosiasiassa kaikki vastuu on kuluttajalla, koska itse älykodinkoneen suojaukseen ei juurikaan voi vaikuttaa. Riskin toteutuessa kuluttajalla ei ole käytännössä suojaa, eikä sitä varten pysty hankkimaan Suomessa vakuutusta, toisin kuin yritykset saavat tietojensa häviämisen varten erilaisia toimintansa keskeytymistä varten olevia vakuutuksia. Tällainen vakuutus korvaa tietojen menetyksiä ja laitteiden toimimattomuudesta aiheutuvia toimintakatkoja yritystoiminnassa. Toisaalta todistaminen, mistä älykodinkoneen vahinko tosiasiassa on johtunut voi olla haastavaa kuluttajan kannalta. Kuluttajan on haastavaa todistaa, että älylaite osallistui palvelunestohyökkäykseen ja lakkasi toimimasta. Haittaohjelma on voinut tulla verkkoon suojaamattoman reitittimen kautta, jolloin älykodinkoneen vakuutus ei luultavimmin tällaista korvaisi.

Laitteen valmistajasta riippuen, älylaitteen tietoturvaominaisuudet on voitu toteuttaa omien käytäntöjen mukaisesti. Toteutukseen vaikuttaa myös älykodinkoneissa oleva teknologian yksinkertaisuus, johon ei pystytä vielä lisäämään todellisia tietoturvaa lisääviä osia. Laitevalmistaja voi joutua vastuuseen laitteen omistajasta keräämiensä tietojen osalta, mikäli ne rikkovat tietosuojaa. Tämä vastuu tosin rajoittuu Suomen ja EU:n rajojen sisäpuolelle. Käyttäjältä vaaditaan perustietämystä tietotekniikasta tai luotettavaa palveluntuottajaa, joka voi suojata laitekokonaisuuden kotona.

3.4 Älykodinkoneiden käyttöohjeet

Käyttöohje toimii kuluttajan apuna suojausta rakennettaessa, laitetta asennettaessa sekä koko älykodinkoneen elinkaaren aikana suojauksen ylläpidossa. Älykodinkoneet ovat tulleet markkinoille nopeasti ja käyttöohjeissa oleva älyominaisuus on uutta tietoa ohjeistuksessa. Kun kuluttaja on hankkinut älykodinkoneen, alkaa koneen asennus kotona. Asennusta varten kuluttajalle on laadittu käyttöohjeet, joiden perusteella laitteen turvallinen asennus ja käyttö on mahdollista. Suomen kuluttajaturvallisuuslaissa mainitaan yleisiä velvollisuuksia, joita tuotteiden valmistajan on annettava kuluttajalle. Kuluttajaturvallisuuslain (920/2011) 2 luvun 9 § sääntelee kulutustavaroihin liittyvien tietojen antamisesta kuluttajalle seuraavasti:

> Toiminnanharjoittajan on selkeällä ja ymmärrettävällä tavalla annettava kuluttajille ja kuluttajiin rinnastettaville tarvittavat tiedot, jotta he pystyvät arvioimaan kulutustavaroihin ja kuluttajapalveluihin liittyvät vaarat. Valvontaviranomainen voi vaatia, että toiminnanharjoittaja antaa kuluttajille sopivalla tavalla tavaraan tai palveluun liittyvän vaaran torjumisen tai ehkäisemisen kannalta tarpeellisia käyttö- tai toimintaohjeita, varoituksia tai muuta tietoa.

Vaaroista, joista laissa mainitaan, käsitetään yleisesti henkilön fyysiseen turvallisuuteen liittyvänä. Tällaisia ovat esimerkiksi varoitukset laitteen liittämisestä sähköverkkoon. Lain yhtenä tarkoituksena on myös ehkäistä kulutustavaroista aiheutuvia omaisuusvahinkoja.

Tukes (Turvallisuus- ja kemikaalivirasto) on lupa- ja valvontaviranomainen, joka edistää tuotteiden, palveluiden ja teollisen toiminnan turvallisuutta ja luotettavuutta sekä valvoo ja toimeenpanee niihin liittyvää lainsäädäntöä. Varsinaisten tehtäviensä lisäksi se laatii oppaita ja ohjeistuksia laitteiden valmistajille ja maahantuojille. Käyttöohjeista Tukes (Tukes 2016, 6) on laatinut oppaan, jossa mainitaan vastuusta ja käyttöohjeesta seuraavasti:

> Suomalainen valmistaja, maahantuoja tai jakelija vastaa siitä, että tuote on laillisesti Suomen markkinoilla. Kuluttajansuojalain mukaan vastuu käyttöohjeesta on myyjällä. Kuluttajalla on oikeus saada selkeä käyttöohje suomeksi ja ruotsiksi, ja myyjän velvollisuus on toimittaa se hänelle.

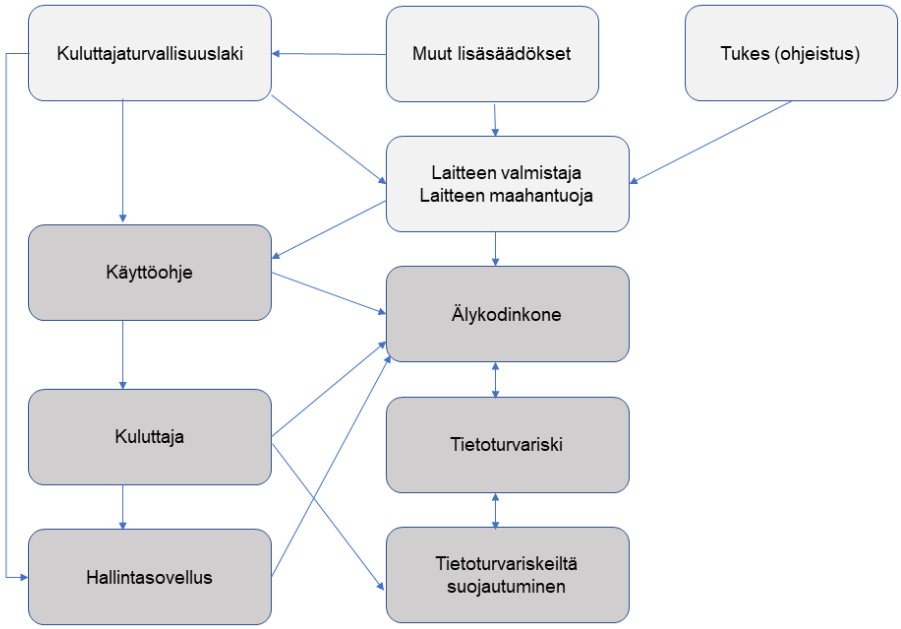
Oppaasta löytyy yleisluontoisia neuvoja siitä, miten käyttöohjeesta saa ymmärrettävän ja helppolukuisen.

Kuten laki ja Tukes kertoo, kuluttajan kannalta käyttöohjeen tulee sisältää ohjeita vaaran ehkäisemiseksi selkeästi kuluttajan äidinkielellä. Lainsäädäntöä käyttöohjeen sisällöstä ei ole, lukuun ottamatta laitteen sähköturvallisuuteen liittyvistä tiedoista ja varoituksista. Standardeja sähkölaitteiden käyttöohjeista on tarjolla laitteiden valmistajille ja maahantuojille ja joita voi tilata esimerkiksi SFS-verkkokaupasta (Suomen Standardoimisliitto SFS ry). SFS toimii Suomessa standardoinnin keskusjärjestönä ja tekee yhteistyötä vastaavien

kansainvälisten järjestöjen kanssa. Standardien sisältöjä ei ole vapaasti luettavissa, josta syystä niiden sisältöä ei tässä yhteydessä käydä lävitse eivätkä ne vielä sisällä tietoturvallisuuteen liittyviä ohjeistuksia. SFS on mukana kansainvälisessä IoT laitteiden starndardoimis hankkeessa, josta tietoa ollaan julkistamassa keväällä 2018. (SFS.)

Kuluttajan näkökulmasta ajatellen älykodinkoneen toiminnoista, hallintasovelluksista ja niiden käytöstä olisi hyvä olla samanlainen sisältö ja rakenne kuin varsinaisen käyttöohjeen muissa osissa on; varoitukset, huomautukset, asennus, toiminnot ja hävitys. Tietoturvan kannalta siinä tulisi olla kaikki sellaiset tiedot, huomautukset ja varoitukset, jotka liittyvät johonkin tiedettyyn uhkaan. Kaikki toiminnot tulisi kertoa ja erotella selkeästi. Laitteessa oleva hallintapaneeli tulee olla omassa osiossa ja hallintasovellukseen liittyvät omassaan, mikäli laitteessa itsessään on myös mahdollisuus hallintasovelluksen käyttöön ja se eroaa mobiilisovelluksen toiminnoista.

Käyttöohje on osa älykodinkoneeseen liittyvää tietoturvallisuutta, sillä se avustaa kuluttajaa antamalla kaiken tarpeellisen tiedon tietoturvariskeiltä suojautumiseen. Käyttöohjeeseen vaikuttavat useat tekijät (kuva 6) ja se toimii yhtenä tärkeimpänä kuluttajaa auttavana dokumentaationa tietoturvariskeiltä suojautumisessa.



Kuva 6. Älykodinkoneeseen liittyvät tekijät.

Kuvasta voidaan nähdä karkeasti, miten edellä käyttöohjeesta kerrotut asiat nivoutuvat yhteen älykodinkoneeseen, tietoturvariskeihin ja niiltä suojautumiseen. Käyttöohje on siis kiinteä ja merkittävä osa älykodinkoneen hallittavuutta myös tietoturvariskeiltä suojaamisessa.

4 Tutkimus älykodinkoneiden käyttöohjeista

Tässä luvussa kerrotaan tutkimusmenetelmästä, aineistosta, toteutuksesta, laitekohtaiset tutkimustulokset sekä yhteenveto tutkimustuloksista.

Opinnäytetyön tavoitteena on selvittää älykodinkoneisiin liittyviä tietoturvariskejä ja niiltä suojautumista sekä tutkia mitä tietoturvariskeiltä suojautumiseen liittyvää laitevalmistajat ovat ottaneet huomioon käyttöohjeissaan ja miten niissä ohjeistetaan kuluttajaa. Älykodinkoneisiin liittyvät tietoturvariskit ja niiltä suojautuminen on esitelty teoriaosuudessa luvussa 3 ja se toimii käyttöohjeen sisältöanalyysille ohjaavana viitekehyksenä. Tutkimus käyttöohjeista on laadullinen eli kvalitatiivinen ja menetelmänä sisältöanalyysi. Laadulliseen tutkimukseen on liitetty erilaisia perinteitä ja useita kymmeniä tunnusmerkkejä, joiden perusteella Tuomen & Sarajärven (2018, 14; 188) mukaan laadullista tutkimusta voidaan pitää kattokäsitteenä ja monitieteellisenä menetelmänä. Tämä helpottaa laadullisen tutkimuksen ja sisältöanalyysin tekoa ja antaa tutkijalle enemmän vapautta tutkittavan aineiston määrän ja tutkimuksen rajauksen suhteen sekä viitekehyksen luomiseen. Laadullinen tutkimus voi olla yhdistelmä määrällistä sekä sanallista, mutta suppean aineiston osalta määrällisiin tuloksiin tähtäävä tutkimus ei ole mahdollista tai ne eivät ole yleistettävissä. Tämä tutkimus käyttöohjeista on sanallinen eikä siinä keskitytä erilaisten esiintymien määrälliseen analysointiin.

Tämän työn sisältöanalyysilla pyritään ymmärtämään älykodinkoneiden käyttöohjeiden sisältöä tietoturvariskin, tietoturvan ja kuluttajan kannalta, joka sopii Kanasen (2014, 56) määritelmään laadullisesta tutkimuksesta. Tutkimuksen viitekehyksenä toimii teoriaosuuden selvitykset älykodinkoneiden tietoturvariskeistä, älykodinkoneen ja siihen liittyvä integraation suojaustarpeista sekä käyttöohjeista valmistajille laadittu lainsäädäntö ja ohjeistus. Käyttöohjeiden sisältöanalyysissa tutkitaan, mitä tietoa niissä on saatavilla kuluttajalle, jotta älykodinkoneeseen liittyviä riskejä voidaan ehkäistä siltä osin kuin se teoriaosuuden mukaan on mahdollista. Älykodinkoneen huomattavimmat riskit ovat laitteessa olevien tietojen menettäminen, haittaohjelmat, niiden käyttö palvelunestohyökkäyksissä sekä haittaohjelmien leviäminen kodin muihin tietoteknisiin laitteisiin ja yhteyksiin. Toisaalta älykodinkoneen kannalta sitä ympäröivän integraation suojaamattomuus aiheuttaa älykodinkoneen suojaukselle vaatimuksia. Käyttöohje puolestaan toimii kuluttajan apuna suojausta rakennettaessa, laitetta asennettaessa sekä koko älykodinkoneen elinkaaren aikana suojauksen ylläpidossa. Tästä syystä on tärkeää, että käyttöohje on laadittu kuluttajalle myös älyominaisuuksien osalta ohjaavaksi ja suojausta ajatellen neuvovaksi, kuluttajan tietoteknisestä tietämyksestä riippumatta. Kun tutkimusmenetelmänä on sisältöanalyysi, tulisi pyr-

kiä objektiivisuuteen, joka on yksi tieteellisen tutkimuksen ehto. Toisin sanoen tutkijana pitäisi olla vaikuttamatta suuresti siihen mitä tuloksia syntyy. Laadullisessa tutkimuksessa tämän säilyttäminen voi olla vaikeaa, sillä tutkija itse analysoi tässä tapauksessa dokumentteja ja näin ollen jotakin subjektiivisuutta jää voimaan. Objektiivisuutta tässä tutkimuksessa on pyritty säilyttämään sillä, että aineistoa on jaoteltu teoriaosuudessa kerrottuun viitekehykseen siitä millaiset asiat vaikuttavat keskeisesti älykodinkoneen suojaukseen sekä miten lainsäädäntö ja Tukes määräävät ja ohjeistavat käyttöohjeiden laadintaa. Tutkimus ei sisällä tutkijan mielipiteitä asiasta ja pohdintaosuudessa olevat päätelmät tehdään yleisellä tasolla pohjautuen tuloksiin aineistoista tutkijan tämän hetkisen tietämyksen tasolla.

4.1 Tutkimusaineisto

Tutkimuksen kohteena on Suomessa myytävien älykodinkoneiden vapaasti verkossa saatavilla olevat käyttöohjeet (liite 1), jotka ovat tutkittavissa kuten julkiset asiakirjat (Kuula 2006, 171). Tämä tarkoittaa, että eettiseltä kannalta niiden anonymiteetin käsittely on helpompaa kuin esimerkiksi henkilöhaastatteluissa. Laadittaessa tätä tutkimusta eettistä puolta on harkittu tarkoin eikä tarkoituksena ole vertailla valmistajia keskenään eikä arvostella valmistajien kykyä tuottaa käyttöohjeita. Keskeisenä tarkoituksena on pyrkiä etsimään tutkittavaa tietoa, koska älykodinkoneet ovat tulleet markkinoille nopeasti ja käyttöohjeissa oleva älyominaisuus on siis uutta tietoa ohjeistuksessa.

Kodinkoneen valinnassa käytettiin kriteerinä, että ne sisältävät langattoman yhteyden (Wifi, Bluetooth), joka mahdollistaa Internet-yhteyden ja tekee kodinkoneesta älykkään. Tutkimuskohteet valittiin myös siten, että mukana olevat laitteet eroaisivat toisistaan perustoiminnoiltaan, hallintasovelluksiltaan sekä valmistajittain. Laitemerkit valittiin suomalaisille kuluttajille kohdistettujen suomenkielisten verkkokauppojen sivustoilta, joten laitteisiin tulee liittää käyttöohjeet suomenkielisenä.

Näillä perustein älykodinkoneista valittuina ovat seuraavat laitteet valmistajittain:

- Jääkaappi, Samsung
- Astianpesukone, Bosch
- Imuri, Neato Botac connected
- Kahvinkeitin, Philips

Samsung jääkaappi sisältää niitä myyvien liikkeiden teknisen tuoteselosteen mukaan WiFi ja Bluetooth ominaisuuden. Sitä voidaan hallinnoida sekä koneessa olevan näytön että siihen liittyvän hallintasovelluksen (Samsung Smart) kautta. Laitteeseen voidaan siirtää kuvia ja tietoa ja se sisältää myös kameran, jolla voidaan nähdä jääkaapin sisältöä. Jää-

kaappia maahantuojana toimii useita erilaisia yrityksiä, jotka tekevät yhteystyötä Samsung:n kanssa. Samsung Electronics Nordic Ab toimii eteläkorealaisen valmistajan Samsung Group sivuliikkeenä Suomessa sekä tarjoaa tietoa tuotteista suomenkielisinä kuluttajille. Sivuliikkeen toimiala on sähköisten kodinkoneiden vähittäiskauppa. (YTJ.)

Bosch Asianpesukone sisältää teknisen tuoteselosteen mukaan WiFi ominaisuuden, jolla kone voidaan liittää langattomaan verkkoon. Sitä voidaan hallinnoida sekä koneessa olevan näytön että siihen liittyvän hallintasovelluksen (Home Connect) kautta. Laitteen hallintaa ovat perustoimintojen käyttö (sammutus, käynnistys, toiminnan seuraaminen). Astianpesukonetta tuodaan maahan useiden erilaisten yritysten kautta. BSH Kodinkoneet Oy toimii Suomeen tuotavien Bosch kodinkoneiden ja kodin sähkölaitteiden tukkukauppana ja se tarjoaa tukkukaupan lisäksi palveluita ja tukea laitteiden käyttöön liittyen. (YTJ.)

Neato Botvac Imuri sisältää WiFi langattoman yhteysmahdollisuuden. Sitä voidaan hallita sekä imurin painikkeilla sekä hallintasovelluksen kautta. Pääasiallinen älyominaisuuksien hallinta tapahtuu hallintasovelluksessa ja itse imurissa on toimintopainikkeita laitteen sammuttamiseen sekä käynnistämiseen. Imurin valmistaja on yhdysvaltalainen Neato Robotics ja Suomen osalta pääasiallisena maahantuojana toimii Idelux Oy. Idelux:n toimialana on viihde-elektroniikan tukkukauppa ja jälleenmyyjinä useita erityyppisiä liikkeitä. Idelux Oy tarjoaa tietoa ja tukea laitteiden hankinnassa. (YTJ.)

Philips Kahvinkeitin sisältää Bluetooth yhteysmahdolliseen langattoman verkon kautta hallintasovellukseen sekä hallintapainikkeita itse keittimessä. Keittimessä on pieni näyttö, josta voidaan nähdä joitakin tietoja (kuten salasana ja keittimen tila). Keittimen hallintaa ovat käynistys ja sammutus sekä erilaisten juomien valinta sekä juomien profilointi eri ihmisille. Kahvinkeittimen valmistaja on alankomaalainen suuryritys Philips ja sitä maahantuo muun muassa suomalainen Philips Oy, joka toimii tukkukauppana myös kodinkoneille ja tarjoaa Philips tuotteista tietoa ja tukea kuluttajille. Jälleenmyyntiliikkeinä toimii useita erilaisia yrityksiä, kuten kodinkoneliikkeet ja tavaratalot. (YTJ.)

4.2 Tutkimuksen toteutus

Tutkimus toteutettiin siten, että haettiin, luettiin ja tutkittiin vapaasti verkossa olevien älykodinkoneiden käyttöohjeet. Laite etsittiin aiemmin kuvatun älykodinkoneen määritelmän perusteella niitä myyvien suomalaisten yritysten verkkosivuilta. Kriteerinä pidettiin, että laitteessa tulee olla verkkoyhteys, joka mahdollistaa edelleen Internet-yhteyden. Älykodinkonetta myyvän yrityksen sivuilta saatiin laitteen tyyppikoodi, jolla käyttöohje etsittiin laitteen

valmistajan tai maahantuojan Internet-sivuilta. Tämän jälkeen jokainen käyttöohje talletettiin sisällön lukemista, muistiinpanoja ja erittelyä varten laitekohtaisiin Word-dokumentteihin koneelle. Kun aineistot olivat käsiteltävissä, ryhdyttiin palastelemaan ja erittelemään käyttöohjeiden sisältöjä teoriaosuuden perusteella. Ensin käyttöohjeiden sisällöt jaettiin yleisiin tietoihin sähkölaitteesta sekä älyominaisuuksista kertovaan osaan. Tässä tutkimuksessa sähkötekniset osat ovat irrotettu tutkittavasta aineistosta kokonaan pois ja keskitytty vain älyominaisuuksista ja hallintasovelluksista kertoviin osioihin. Tutkimuksen kannalta vain nämä ovat tosiasiassa merkityksellisiä, sillä niissä on tietoa tietoturvariskeiltä suojautumiseen laitteen, sen integraation ja käyttäjän kannalta. Älyominaisuudet ja hallintasovelluksista kerrotut aineistot on vielä jaoteltu vastaamaan opinnäytetyön tavoitetta omiin kokonaisuuksiin, joista kerrotaan seuraavissa kappaleissa tarkemmin.

Tutkimuksessa on käytetty Excel-työkalua yleiseen aineiston sisällön hahmottamiseen ja analyysin aikana tapahtuvaan tiedon etsimiseen. Siihen talletettiin vain lyhyesti tietoa, koska varsinaiset jaotellut tekstit ovat laitekohtaisissa Word-dokumenteissa eriteltyinä ja jaoteltuina. Excel-työkalu on kehittynyt tutkimuksen aikana iteroiden tietämyksen kasvaessa ja aineiston sisällön läpikäymisen ymmärtämisen yhteydessä. Työkalua on käytetty myös tulosten yhteenvetoja laadittaessa helpottamaan ja muistamaan keskeisten löydösten raportointia.

Jotta tutkimuksella saadaan vastaus ”Mitä tietoturvariskeiltä suojautumiseen liittyvää käyttöohjeista löytyy”, laadittiin aineiston tarkastelun avuksi kysymyksiä. Apuna kysymysten laadinnassa käytettiin Viestintäviraston (2016) IoT-laitteen hankintaan liittyvää muistilistaa mukaillen ja sitä on käytetty tähän tutkimukseen soveltuvin osin. Kysymykset, jotka käydään jokaisen aineiston kohdalla ovat:

- Onko laitteelle mahdollista saada ohjelmisto tai tietoturvapäivityksiä?
- Mikäli ohjelmistopäivityksiä on saatavilla, asennetaanko ne automaattisesti vai käsin?
- Onko laitteen asetuksiin pääsy suojattu salasanoin?
- Mikäli asetuksiin pääsy on suojattu salasanoin, onko se vaihdettavissa vai onko se kiinteä?
- Mitkä ovat laitteen oletusasetukset?
- Näkyykö laite suoraan Internettiin? Jos näkyy, miten se tapahtuu?
- Löytyykö muuta tietoturvaan liittyvää ohjeistusta?

Kysymykset perustuvat teoriaosuuden tietoon älykodinkoneen suojausmahdollisuuksista. Kolme ensimmäistä kysymystä liittyvät suoraan älykodinkoneeseen. Oletusasetuksilla on merkitystä silloin, jos ne sallivat ennen valintoja esimerkiksi verkkoon pääsyn. Mikäli laite näkyy suoraan Internet-verkkoon, tulisi ohjeista näkyä miten se tapahtuu (laitevalmistajan palvelinten kautta vai muutoin. Mukaan on myös otettu epäsuora kysymys (muuta tietoturvaan liittyvää), jottei suojauksen kannalta tärkeitä osia aineistosta ohitettaisi. Näitä kysymyksiä ja vastauksia varten on luotu Excel-taulukko (kuva 7), jossa laitteen tyyppi on

omalla rivillään ja sarakkeissa otsikkoina ovat varsinaiset kysymykset. Tätä sivua on käytetty tulosten etsimisen yhteydessä sekä lopulta tulosten sanalliseen raportointiin.

Älykodinkone	Ohjelmistopäivitykset saatavilla	Ohjelmisto päivittyy automaattisesti	Onko laitteen asetuksiin pääsy suojattu salasanoin? Mikäli asetuksiin pääsy on suojattu salasanoin, onko se vaihdettavissa vai onko se kiinteä?	Oletusasetukset	Näkyvyys Internetissä	Muuta tietoturvaan liittyvää (Varoitukset ja huomautukset)
Jääkaappi	kyllä	kyllä	kyllä vaihdetaan asennuksen yhteydessä	Oletuksena yhteydet pois päältä. Muusta ei mainintaa	ei mainintaa	kyllä Sisältö Word:ssa kohdassa "Huomioitavaa"
Astianpesukone	ei mainintaa	kyllä	kyllä vaihdetaan asennuksen yhteydessä	ei mainintaa	ei mainintaa	kyllä Sisältö Word:ssa kohdassa "Huomioitavaa"
Imuri	ei mainintaa	ei mainintaa	ei mainintaa	ei mainintaa	ei mainintaa	kyllä Sisältö Word:ssa kohdassa "Huomioitavaa"
Kahvinkeitin	ei mainintaa	ei mainintaa	kyllä suojattu kiinteällä salasanalla	salasana kiinteä	ei mainintaa	kyllä Salasanan syötön yhteydessä Sisältö Word:ssa kohdassa "Huomioitavaa"

Kuva 7. Laitekohtaiset tietoturvakysymykset vastauksineen.

Tutkimuskysymykseen ”Miten käyttöohjeissa ohjeistetaan suojautumaan tietoturvariskeiltä?” käytetään pohjana käyttöohjeisiin liittyvää lainsäädäntöä ja Tukes:n ohjeistusta, joista kerrottiin käyttöohjeen kohdalla luvussa 3.4. Lain mukaan sen on oltava suomenkielinen ja ymmärrettävä. Ymmärrettävyyttä pyritään selvittämään kielisyyden, ikäsuositusten, käyttöohjeen laajuuden (käyttöohjeen pituus ja älyominaisuuden osuus tästä, onko suomenkielinen ohje erillisenä). Lisäksi ymmärrettävyyttä pyritään selvittämään etsimällä ’Huomautus’ ja ’Varoitus’ -kohtia, jotka ovat yleisiä sähkölaitteiden käyttöohjeissa olevia tapoja ilmoittaa erityistä huomiota vaativista kohdista ja näin herättämään kuluttajan kiinnostus niihin. Yhteydenottokanavat antavat kuluttajalle mahdollisuuden kysyä lisää ja ikäsuositus vaikuttaa siihen minkä ikäisenä laitetta voi käyttää ja ymmärtää käytön vaikutuksia. Analysointia varten on laadittu kysymykset edellä mainitun mukaisesti :

- Onko käyttöohje suomenkielinen?
- Kuinka pitkä käyttöohje on kokonaisuudessaan ja mikä on älyominaisuuden osuus?
- Miltä Internet-sivustolta käyttöohje löytyy?
    - sivuston julkaisija
- Mitä muotoa käyttöohjedokumentaatio on?
- Ikäsuositukset
- Onko yhteydenottokanavat ilmoitettu ongelmatilanteita varten?
    - mitkä ne ovat

Excel-taulukkoon (kuva 8) omalle sivulleen on merkittynä laite omalla rivillään ja kysymykset sekä omina sarakkeinaan. Kuva on esimerkki yhdestä käyttöohjeesta työkalussa. Työkalu sisältää myös muita sarakkeita (linkit valmistajan sivulle käyttöohjeeseen, linkki eriteltyyn analyysidokumenttiin sekä huomioita), mutta ne on jätetty tässä esityksessä pois, jotta esimerkin luettavuus säilyisi. Sivu on muodostettu tutkimuksen alussa ja ylläpidetty analyysin aikana. Sivua on käytetty apuna koko tutkimuksen ajan ja tärkeänä osana se on toiminut sanallista yhteenvetoa laadittaessa. Taulukossa on vielä lisäsarakkeina linkki käyttöohjeeseen

Älykodinkone	Hallintasovellus	Ohjeen saatavuus ja muoto	Kielisyys	Käyttöohjeen sivu lkm	Älysivut lkm	Laitteen käytön lkäsuositus	Yhteydenottokanava ongelmatilanteessa
Jääkaappi	Samsung connect	Internet Laitteen valmistajan sivu PDF	englanti saksa italia ranska ruotsi tanska norja suomi	624	14	Aikuiset, alaikäiset vain valvotusti. Ei alle 8 v	live chat puhelimitse sähköposti,

Kuva 8. Laitekohtaiset yleiset tiedot vastauksineen.

Näitä edellä mainittuja Excel-taulukoita ja word-dokumentteja on käytetty yhdessä ja erikseen tutkimustulosten, keskeisten tulosten pohdinnassa sekä johtopäätösten tekemisessä.

4.3 Tutkimustulokset laitteittain

Tutkimustulokset esitellään ensin laitteittain kysymyksittäin sanallisesti sekä esitellään esimerkkejä aineistoista löytyvistä havainnoista. Jokaisen laitteen kohdalla toistuu samat jaottelut ja kysymykset sekä kohdassa 4.3.5 tulokset kootaan yhteen.

4.3.1 Jääkaappi Samsung

Käyttöohje löytyi Samsung.com sivustoilta. Kuluttajan näkökulmasta verkkokauppojen sivuilla ei ollut mainintaa itse käyttöohjeen sijainnista, vaan se täytyy tehdä ensin hakemalla myyjän sivuilta haluttu tuote ja sen jälkeen mennä valmistajan tai maahantuojan suomenkielisille sivustoille ja etsiä käyttöohjetta sieltä tuotteen tyypin tunnuksella. Jääkaapin tyyppikoodi on RR40M71657F/EE. Käyttöohje on julkaistu yhtenä dokumenttina ollen 624 sivua pitkä. Käyttöohjedokumentti on luotu englannin, saksan, italian, ranskan, ruotsin, tanskan, norjan ja suomen kielisinä. Suomenkielinen osuus on ohjeessa viimeisenä. Käyttöohje ei sisällä maakohtaista yleistä sisällysluetteloa, joten dokumentti on selailtava etsien suomenkielistä osiota, mikä tekee käyttöohjeen selaamisesta työlään sen sisältämän sivumäärän vuoksi.

Käyttöohje noudattaa yleistä rakennetta, jossa ensin kerrotaan fyysiseen turvallisuuteen liittyvät ohjeet ja varoitukset, asennusohjeet, toiminnot, huolto ja vianmääritys. Itse älyominaisuuksista kerrotaan kohdassa ”Toiminnot” ja se on pituudeltaan 14 sivua pitkä.

Laitteen asetuksiin ja toimintoihin pääsy: Jääkaapin toimintaa voidaan seurata ja ohjata sekä sen asetuksia voidaan hallita joko jääkaapin näytöltä tai etänä erillisen sovelluksen kautta (Family Hub tai Samsung Connect). Jääkaappi voidaan yhdistää myös tiettyihin muihin Samsung laitteisiin kuten älytelevisioon ja hallita kaappia television kautta Samsung Connect sovellusten kautta. Jääkaapin todennusta voidaan käyttää Samsung Smart TV-sovelluksissa, joiden avulla jääkaapin yksityisyystiedot voidaan jakaa televisioon (Device Authentication / laitteen todennus). Salasanasta ei ole mainintaa toimintojen yhteydessä. Käyttöohjeessa mainitaan, että jotkin valinnat ja asetukset eivät ole välttämättä käytettävissä kaukosäätimessä. Mitään mainintaa siitä, mitä nämä poikkeukset ovat, ei ole saatavilla ohjeessa.

Laitteen ohjelmiston päivittyminen voidaan tehdä automaattisesti eikä täysin manuaalisesta päivityksestä ollut mainintaa. Jääkaapin hallintasovelluksen tai jääkaapin hallintapaneelin asetuksissa tulee ensin valita Software Update -toiminto, jonka jälkeen jääkaappi ilmoittaa onko päivityksiä saatavilla. Kun päivityksiä on saatavilla, laitteessa aktivoituu Update -painike. Painamalla Update -painiketta, ohjelmistopäivitys käynnistyy. Käyttöohje ei mainitse, onko tietoturvapäivityksiä saatavilla tai onko valmistaja sitoutunut julkaisemaan niitä.

Laitteen näkyvyyttä internetissä ei ole kerrottu käyttöohjeessa suoraan. Tähän liittyen kiertäen käyttöohjeessa ilmaistaan, että jos Internetin palvelun tarjoaja on rekisteröinyt modeemin MAC osoitteen tunnistamista varten, jääkaappi ei välttämättä saa yhteyttä Internettiin.

Yhteydenotto ongelmatilanteissa: Käyttöohjeessa mainitaan yhteydenottokanaviksi maakohtaiset asiakaspalvelunumerot sekä maahantuojan sivustot Internetissä (www.samsung.com/fi/support). Internetyhteysongelmissa käyttöohje ohjeistaa olemaan yhteydessä Internetpalveluntarjoajaan tai paikalliseen Samsungin huoltoon tai jälleenmyyjään.

Tietoturvariskeiltä suojautumisen ohjeistus: Käyttöohjeessa ei ole minkäänlaista suoraa mainintaa tietoturvariskeiltä suojautumiseen tai mainintaa siitä, tehdäänkö ohjelmistopäivitysten yhteydessä tietoturvaan liittyviä päivityksiä. Mainintaa ei ole myöskään siitä, voidaanko jääkaappiin asentaa erillisiä tietoturvaan liittyviä ohjelmistoja, kuten virustorjuntaohjelmistoja. Tietoturvaan löyhästi liittyvä varoitus kertoo, että aikuisten on valvottava alaikäisiä näiden käyttäessä palveluita. Tietoturvariskeiltä suojautumiseen voidaan myös liittää Clean Screen Mode -toiminto. Toiminto ehkäisee, ettei sovelluksia käynnistetä vahingossa jääkaapin näytöltä esimerkiksi puhdistuksen yhteydessä.

Lisäksi havaittiin **huomautuksia** tietoturvallisuuteen liittyen, että asetuksien palautusta varten tulee käyttää Factory Data Reset toimintoa, joka palauttaa tehdasasetukset sekä poistaa kaikki käyttäjätiedot pysyvästi. Poistettavia tietoja ovat tilitiedot, muistiot, valokuvat ja käyttäjäasetukset. Tämä kerrotaan asetustoimintojen yhteydessä eikä siinä ole viittausta tilanteeseen, jossa näin tulee tehdä. Käyttöohjeessa mainitaan myös, että sovellusten sisältö tai ulkoasu voi muuttua tai niiden tuki saatetaan lopettaa ilman erillistä ilmoitusta. Yhteyksissä olevista ongelmista mainitaan, että verkkojärjestelmän palomuuriasetukset voivat estää Samsung Smart -jääkaappia yhdistymästä Internettiin. Protokolista ja yhteyksistä on maininta Samsung Smart -jääkaapit tukevat 2,4 GHz:n Wi-Fi-yhteyden IEEE 802.11 b/g/n- ja Soft-AP -protokollaa.

4.3.2 Astianpesukone Bosch

Astianpesukoneen käyttöohje löytyi Bosch-Home.fi sivustolta kohdasta ”Lisäasiakirjat”, josta käyttöohje on vapaasti ladattavissa ja luettavissa. Astianpesukoneen tyyppikoodi on SMA67MD06E, jolla käyttöohjetta etsittiin sivustolta. Käyttöohje on suoraan suomenkielinen 60 sivuinen opas, josta löytyy älyominaisuutta koskevaa tekstiä 5 sivua. Käyttöohje on jaoteltu sisällöltään useaan eri osa-alueeseen, jotka ovat: määritysten mukainen käyttö, turvallisuusohjeet, ympäristön suojelu, tutustu laitteeseen, Home Connect, pesutoiminnot, laitteen käyttö ja huolto, ongelmatilanteet, huoltopalvelu sekä asennus ja liitäntä.

Laitteen asetuksiin ja toimintoihin pääsy: Astianpesukoneen toimintoja voidaan hallita ja asetuksia muuttaa sekä suoraan astianpesukoneen näytöltä, että Home Connect -sovelluksen kautta. Laitteen ohjelmistopäivityksistä ei ole mainintaa käyttöohjeessa eikä itse astianpesukoneen toimintovalikkojen selostuksista löydy tähän viittaavaa toimintovaihtoehtoa. Asetuksiin pääsyä salasanalla ei ole kuvattu käyttöohjeessa.

Laitteen ohjelmiston päivittyminen: Laitteen ohjelmiston päivityksistä ei ole käyttöohjeissa mainintaa. Tietoturvapäivitysten saatavuudesta tai siitä onko laitevalmistaja sitoutunut julkaisemaan niitä, ei mainita käyttöohjeessa.

Laitteen näkyvyyttä Internetissä ei ole kerrottu käyttöohjeessa.

Yhteydenotto ongelmatilanteissa: Käyttöohjeessa mainitaan yhteydenottokanavaksi häitiötilanteessa Suomalainen asiakaspalvelunumero, joka löytyy käyttöohjeen lopusta.

Lisäksi havaittiin **huomautuksia** tietoturvallisuuteen liittyen, että tehdasasetuksena virta katkeaa automaattisesti pesuohjelman päätyttyä. Sitä katkeaako WiFi -yhteys ei kerrota.

Yhteyden Home Connect -palvelimeen voidaan katkaista Home Connect -sovelluksesta, jolloin laite on yhteydessä vain hallintasovellukseen mobiililaitteessa. Tietoturvaan liittyvää huomautusta käsitellään myös kohdassa ”Huoltopalvelu” seuraavasti: ”Huomaa, että huoltopalvelun työntekijät eivät koskaan kysy Home Connect -salasanaasi”. Tietosuojaa koskeva huomautus laitteen yhdistämisestä Home Connect sovellukseen kertoo lyhyesti, mitä tietoja välitetään valmistajan palvelimelle. Astianpesukone välittää laitetunnisteen (laiteavain ja WiFi moduulin MAC-osoitteen), WIFI-moduulin turvallisuussertifikaatin, pesukoneen käytössä olevan ohjelma- ja laiteversion sekä tehdasasetuksen tilan.

Käyttöohjeessa on maininta noudatetuista EU:n direktiiveistä sekä radio- ja telepäätelaitteita koskeva sitoumus.

4.3.3 Imuri Neato

Imurin käyttöohje löytyi Neato.com -sivustolta kohdasta ’Neato botvac connected series documentation’. Tyyppikoodia ei varsinaisesti ollut, vaan sitä etsittiin nimellä botvacD3connected/botvacD5connected. Käyttöohjeita on kolmessa erillisessä dokumentissa, joissa kaikissa on eri sisältö. Varsinainen käyttöohje on 160 sivuinen, jossa on usealla eri kielellä ohjeistukset. Kielisyydet ovat englanti, ranska, espanja, italia, saksa, ruotsi, alankomaat, tanska, norja ja suomi. Suomenkielinen osio löytyy koko dokumentin lopusta ja on 13 sivun mittainen. Käyttöohje on jaoteltu yleisesittelyyn, vinkkeihin, robotin valmisteluun, Neato-sovelluksen ja robotin yhteyden muodostamiseen sekä kunnossapitoon ja huoltoon. Käyttöohjeeseen liittyvät varoitukset ja huomautukset ovat dokumentissa, joka on nimeltään Important Information. Valmistajan sivuilta löytyy erillinen pikakäyttöohje, joka sisältää imurin toimintoja ja näyttöä koskevaa informaatiota, joita ei muissa käyttöohje -dokumenteissa ole. Käyttöohjeistus imurin osalta on siis jaoteltuna kolmeen eri dokumentaatioon, jotka ovat erisisältöisiä.

Laitteen asetuksiin ja toimintoihin pääsy: Robotin toimintoja voidaan hallita ja asetuksia muuttaa sekä suoraan robotin näytöltä että Neato -sovelluksen kautta. Robotti-imuria voidaan käyttää usealla mobiililaitteella ja kirjautuminen samalle tilille on mahdollista (käyttäen sähköpostiosoitetta ja salasanaa). Salasana on muutettava hallintasovelluksessa.

Laitteen ohjelmiston päivittyminen: Laitteen ohjelmistopäivityksistä ei ole mainintaa käyttöohjeessa eikä itse toimintovalikkojen selostuksista löydy tähän viittaavaa toimintovaihtoehtoa. Käyttöohje ei mainitse, onko tietoturvapäivityksiä saatavilla tai onko valmistaja sitoutunut julkaisemaan niitä.

Laitteen suoraa näkyvyyttä Internettiin eri kerrota. Ohjeessa kerrotaan, että yhteysongelmien syynä voi olla tietyt langattoman verkon reitittimen palomuurin ja porttien asetukset, jotka voivat estää yhteyden Neaton palvelimille.

Yhteydenotto ongelmatilanteissa: Käyttöohjeessa mainitaan yhteydenottokanavaksi häitiötilanteessa Neato asiakastuki osoitteessa www.NeatoRobotics.com/support.

Muita tietoturvaan liittyviä huomautuksia tai varoituksia ei löydy käyttöohjeesta.

4.3.4 Kahvinkeitin Philips

Kahvinkeittimen käyttöohje löytyi www.philips.fi -sivustolta laitekohtaiselta sivulta kohdasta ”Tuki, oppaat”. Käyttöohjetta etsitiin tyyppikoodeilla HD8969,HD8977 ja HD8978. Käyttöohje on suoraan suomenkielinen ja on 102 sivua pitkä kokonaisuus sisältäen laajasti perinteiset osiot itse laitteesta sekä vaiheittaiset toiminnot ja asetusten määrittelyt. Älyominaisuudet on kerrottu kolmella sivulla.

Laitteen asetuksiin ja toimintoihin pääsy: Ohjeessa on kerrottu Bluetooth -yhteydestä ja hallintasovelluksesta, jonka voi ladata mobiililaitteeseen. Bluetooth on kytketty tehdasasetuksena päälle ja sen voi asettaa pois päältä itse kahvinkeittimestä. Keitin näyttää 4-numeroisen PIN-koodin, jota käytetään, kun mobiililaite yhdistetään kahvinkeittimeen. Tietoturvariskiin liittyen tässä yhteydessä on varoitus: ’Jos syötät väärän PIN-koodin 5 kertaa peräkkäin, keitin poistaa Bluetooth -yhteyden käytöstä turvallisuussyistä’. Käyttöohjeessa ei kerrota, mihin tuo PIN-koodi 5 kerran yritys on syötetty. Itse laite ei pyydä salasanaa vaan antaa sen näytöllä ja sieltä se on haettavissa tarvittaessa ja käytettävissä kun yhteyttä muodostetaan hallintasovellukselta keittimeen.

Laitteen ohjelmiston päivittyminen: Laitteen ohjelmistopäivityksistä ei ole mainintaa käyttöohjeessa eikä itse toimintovalikkojen selostuksista löydy tähän viittaavaa toimintovaihtoehtoa. Käyttöohje ei mainitse, onko tietoturvapäivityksiä saatavilla tai onko valmistaja sitoutunut julkaisemaan niitä.

Laitteen suoraa näkyvyyttä Internettiin eri kerrota.

Yhteydenotto ongelmatilanteissa: Käyttöohjeessa mainitaan yhteydenottokanavaksi häiriötilanteessa www.saeco.com/support tai ottamaan yhteyttä asuinmaan Philips Saecon -palvelunumeroon. Palvelunumeroa ei kerrota.

Lisäksi havaittiin tietoturvallisuuteen liittyen varoitus, että turvallisuussyistä Saeco Avanti -sovellusta tulee käyttää näköyhteydessä keittimeen. Varoituksella viitataan henkilövammoihin ja -vaaroihin.

Langaton verkkoyhteys (Bluetooth) -toiminto on laitteessa kytketty käyttöön oletuksena.

4.3.5 Käyttöohjeiden tutkimustulosten yhteenveto

Tulokset yleisiin kysymyksiin, jotka perustuvat lakiin, Tukesin ohjeisiin sekä vaikuttavat ymmärtämiseen (ikä, käyttöohjeen pituus, yhteydenottokanava) ovat esitetty taulukossa 1. Älyominaisuuksista ja toiminnoista kerrotaan 14 sivulla ja pienimmillään näistä ominaisuuksista kerrotaan 3 sivulla. Kaikilla käyttöohjeet olivat pdf-muodossa laitteen tyyppikohtaisissa dokumenteissa ja vain yhdellä käyttöohje oli suoraan suomenkielinen. Muilla laitteilla käyttöohje sisälsi ohjeet useilla kielillä pidentäen ohjetta ja pitkittäen suomenkielisen osuuden hakemista. Ikäsuositus löytyy kaikista käyttöohjeista ja jääkaapin yhteydessä se on mainittu myös erikseen hallintasovelluksen yhteydessä. Laitteita ei tule antaa alaikäisten käyttöön ilman aikuisen valvontaa. Yhteydenottokanavat ovat kerrottuina jokaisessa käyttöohjeessa ja ne vaihtelevat.

Yleiset kysymykset (laki ja Tukes sekä käyttäjä)	Vastaukset aineistosta (N/A = ohjeessa ei ole mainintaa)
Ohjeen saatavuus ja muoto?	jääkaappi, astianpesukone, imuri, kahvinkeitin: maahantuojan sivut, PDF
Onko käyttöohje suomenkielinen?	jääkaappi, astianpesukone, imuri, kahvinkeitin
Kuinka pitkä käyttöohje on kokonaisuudessaan ja mikä on älyominaisuuden osuus?	jääkaappi (624, 14), astianpesukone (60,5), imuri (160, 13), kahvinkeitin (120, 3)
Onko yhteydenottokanavat ilmoitettu ongelmatilanteita varten?	- jääkaappi (live chat, puhelimitse, sähköposti) - astianpesukone (puhelimitse, myBosch palvelulla) - imuri (www.NeatoRobotics.com/support) - kahvinkeitin (live chat, puhelimitse, sähköposti) - kahvinkeitin (
Ikäsuositukset	- Jääkaappi (aikuisten valvottava alaikäisiä sovellusta käytettäessä) - astianpesukone (koko laitetta koskeva kielto alle 8 vuotiaat) - imuri (koko laiteta koskeva kielto alle 8 v, alaikäisetlapset yli 8 v valvonnan alla) - kahvinkeitin (koko laitetta koskeva kielto alle 8 vuotiaat)

Taulukko 1. Yleiset kysymykset yhteenveto.

Tulokset tietoturvaan liittyviin kysymyksiin (Taulukko 2) sisältävät vaihtelevuutta enemmän kuin tulokset yleisistä kysymyksistä. Ohjelmistoasennukset ovat mahdollisia ja automaattisia jääkaapissa, muissa laitteissa siitä ei ole mainintaa. Laitteen asetuksiin pääsy on suojattu yksilöllisellä salasanalla imurissa ja kiinteällä salasanalla kahvinkeittimessä, muissa käyttöohjeissa asetuksiin pääsystä ei ole erillistä mainintaa. Kaikki käyttöohjeet ovat suomenkielisiä. Varoituksia tietoturvallisuuteen liittyen ei löytynyt yhdestäkään käyttöohjeesta eikä tietoa siitä näkyykö laite suoraan Internet-verkkoon.

Tietoturvaan liittyvät kysymykset (älykodinkoneen suojaus tietoturvariskeiltä)	Vastaukset aineistossa (N/A = ohjeessa ei ole mainintaa)
Onko laitteelle mahdollista saada ohjelmisto tai tietoturvapäivityksiä?	jääkaappi
Mikäli ohjelmistopäivityksiä on saatavilla, asennetaanko ne automaattisesti vai käsin?	jääkaappi (automaattinen)
Onko laitteen asetuksiin pääsy suojattu salasanoin?	jääkaappi, astianpesukone, imuri, kahvinkeitin
Onko laitteen asetuksiin pääsy suojattu yksilöllisellä salasanalla?	imuri
Onko laitteen asetuksiin pääsy suojattu kiinteällä salasanalla?	kahvinkeitin
Näkyykö laite Internettiin?	N/A
Muita tietoturvallisuuteen liittyviä huomautuksia	jääkaappi, astianpesukone, imuri (tulokset näistä eriteltyinä taulukon 2 jälkeen)
Muita tietoturvallisuuteen liittyviä varoituksia	N/A

Taulukko 2. Tietoturvallisuuteen liittyvät kysymykset yhteenveto.

Muuta tietoturvallisuuteen liittyviä huomautuksia löytyi jääkapin, astianpesukoneen sekä kahvinkeittimen käyttöohjeista (taulukko 3). Yleisesti voidaan todeta, että ne vaihtelevat käyttöohjeittain. Yhteistä jokaiselle käyttöohjeelle on, että niissä ohjeistetaan langattomaan verkkoon kytkeminen. Vaihtelevuus verkkoon kytkennälle tulee laitekohtaisesti esille WiFi-yhteyden oletusasetuksista, jotka ovat suoraan päällä astianpesukoneessa ja kahvinkeittimessä ja muissa laitteissa se asetetaan päälle haluttaessa. Jääkaapin kohdalla palomuuriasetukset voivat estää laitetta pääsemästä Internettiin eikä jääkaapin kohdalla mainita miten palomuuriasetuksia tulee muuttaa ja vaikuttaako se suoraan koko verkon

turvallisuuteen. Muissa käyttöohjeissa tällaista huomautusta ei ole Jääkaapin huomautuksista löytyy myös maininta sen tukemista protokollista, jotka suoraan ovat WiFi-yhteydessä käytetty protokolla, muista käyttöohjeissa tämä puuttuu.

Huomautus	
Wifi-verkkoon kytkeminen ja katkaisu.	Kaikissa ohjeet, kuinka kytkentä ja katkaisu suoritetaan. WiFi oletusasetuksena astianpesukoneessa ja kahvinkeittimessä suoraan päällä. WiFi-yhteys katkeaa automaattisesti astianpesukoneessa, kun pesuohjelma päättyy.
Palomuuri	Palomuurin asetukset voivat estää jääkaapin pääsyn Internet-verkkoon
Käytetyt protokollat	Samsung Smart -jääkaapit tukevat 2,4 GHz:n Wi-Fi-yhteyden IEEE 802.11 b/g/n- ja Soft-AP -protokollaa. Muissa laitteissa ei mainintaa.
Salasanakäytäntöjä	Kahvinkeittimestä katkeaa Wifi-yhteys, jos virheellistä salasanaa yritetään 5 kertaa peräkkäin.
Tehdasasetusten palautus	Tehdasasetukset voidaan palauttaa jääkaapissa, jossa huomautetaan lisäksi ettei muutetuja asetuksia voida palauttaa

Taulukko 3. Muita tietoturvallisuuteen liittyviä huomautuksia.

Varoituksia älyominaisuuksiin tai hallintasovelluksiin liittyen ei löytynyt yhdestäkään käyttöohjeesta.

5 Pohdinta

Opinnäytetyön tavoitteena on selvittää älykodinkoneisiin liittyviä tietoturvariskejä ja niiltä suojautumista sekä tutkia mitä tietoturvariskeiltä suojautumiseen liittyvää laitevalmistajat ovat ottaneet huomioon käyttöohjeissaan ja miten niissä ohjeistetaan kuluttajaa.

Toteutetun tutkimuksen yleisinä keskeisinä tuloksina voidaan todeta, että käyttöohjeet olivat kaikilla saatavilla valmistajan/maahantuojan verkkosivuilla PDF-muodossa, jota on vaikea lukea ohjeen pituudesta riippuen selaamalla sitä viimeiseen suomenkieliseen osioon saakka. Vain yksi käyttöohje oli saatavilla suoraan suomenkielisenä. Jälleenmyyjien sivuilta löytyi älykodinkoneista hyvin yleistä tietoa, jonka perusteella pystyi päättelemään, onko kyseessä älylaite (WiFi tai Bluetooth -yhteys). Käyttöohjeesta jälleenmyyjien sivuilla ei ollut mainintaa, joten se pitää hakea laitekoodin ja merkin perusteella valmistajan tai maahantuojan sivuilta.

Varoituksia tietoturvallisuuteen liittyen ei löytynyt yhdestäkään käyttöohjeesta. Huomautuksia sen sijaan löytyi vaihtelevasti ja vain yksi yhteinen piirre oli WiFi-yhteyden asetusten kytkennän ohjeistus. Käyttöohjeissa kerrottiin miten WiFi-yhteyden saa päälle tai pois ja yhdessä käyttöohjeessa kerrottiin, että yhteys katkaistaan automaattisesti pesuohjelman päätyttyä. WiFi-yhteys on tehdasasetuksena oletuksena päällä kahdessa laitteessa. Tehdasasetusten palauttamisesta oli kerrottu vain yhdessä käyttöohjeessa, muissa tästä ei ollut mainintaa.

Tutkimuskysymyksiin (älykodinkoneisiin liittyvät tietoturvariskit ja niiltä suojautuminen) saatiin seuraavat keskeiset tulokset teoriaosuudessa. Älykodinkoneisiin liittyvät merkittävimmät tietoturvariskit ovat haittaohjelma ja laitteen käyttö palvelunestohyökkäyksessä, jotka vaikuttavat suuresti älykodinkoneen toimivuuteen sekä välillisesti voivat aiheuttaa vahinkoa kodin muihin laitteisiin ja niissä säilytettäviin tietoihin. Älykodinkoneen suojaus tapahtuu asentamalla ohjelmistopäivitykset sekä suojaamalla laite hallintasovellukseen syötettävällä salasanalla. Näiden suojaustoimenpiteet riippuvat täysin laitteesta eikä muita suojaustoimenpiteitä ei voida tehdä. Jotta älykodinkoneen suojaus kokonaisuudessaan on mahdollista, on suojattava laitteeseen liittyvä muu kodin laitteisto ja verkko. Suojattavia laitteistoja ovat kaikki kodin tietoliikenneverkkoon kytketyt muut laitteet, tietokoneet, puhelimet, tabletit, reitittimet, modeemit, palomuurit sekä langaton ja kiinteä tietoliikenneyhteys.

Tutkimuskysymyksiin ”Mitä tietoturvariskeiltä suojautumiseen liittyvää laitevalmistajat ovat ottaneet huomioon käyttöohjeissaan ja miten niissä ohjeistetaan kuluttajaa” saatiin seuraavat keskeiset tulokset käyttöohjeiden sisältöanalyysissa. Tulosten perusteella voidaan

todeta, että kaikki käyttöohjeet löytyvät suomenkielisinä maahantuojien tai valmistajien sivuilta laitekohtaisesti. Kaikki tutkitut käyttöohjeet noudattavat siten lain edellyttämää kielellistä vaatimusta. Ymmärrettävyyttä on käyttöohjeissa pyritty lisäämään erittelemällä toiminnot ja huomautukset omiksi erillisiksi osioiksi. Kaikista käyttöohjeista löytyi myös huomautus laitteen käyttäjän ikään liittyen. Laitteita tulee käyttää vain aikuiset ja alaikäisten käyttöä tulee valvoa. Vähimmäisvaatimukset älykodinkoneen suojaukselle ovat ohjelmistopäivitykset sekä salasanojen vaihtamisen mahdollisuus. Laitevalmistajat ovat ottaneet nämä vaatimukset huomioon vaihtelevasti ja osin puuteellisesti. Ohjelmistopäivityksistä on mainintaa vain yhden laitteen osalta ja siinä ohjelmistopäivitys voidaan asentaa automaattiseksi, joka parantaa laitteen toimivuutta ja mahdollisesti tietoturvallisuutta. Salasanakäytännöt ovat vaihtelevia siten, että ne voidaan joko vaihtaa tai ovat kiinteitä. Osassa salasanoista ei ole mainintaa lainkaan. Älykodinkoneen käyttöohjeissa keskitytään hallintasovellusten asennukseen ja toimintojen vaihtoehtojen selostamiseen eikä niiden yhteyttä tietoturvaan selosteta.

Yleisenä johtopäätöksenä tutkimuksesta on, ettei älykodinkoneiden käyttöohjeissa varsinaisesti opasteta kuluttajaa suojautumaan mahdollisilta tietoturvariskeiltä. Niissä on mainintoja salasanoista ja ohjelmistopäivityksistä, mutta kuluttajan on ymmärrettävä näiden liittyvän tietoturvallisuuteen. Jos asetuksiin pääsee ilman salasanoja, se on todellinen riski kuten on myös riski, mikäli salasanaa ei voi vaihtaa. On myös ymmärrettävä, että ohjelmistopäivitysten kannattaa antaa asentua automaattisesti. Kuluttajan on siis omattava tarvittavat tiedot ja taidot sekä älykodinkoneen, että sitä ympäröivän integraation suojaamiseen mahdollisia tietoturvariskejä kohtaan. Käyttöohjeet ovat älyominaisuuksien osalta vielä alkutekijöissään, kun niitä verrataan käyttöohjeen muihin osiin. Johtopäätöksenä voin myös todeta, että käyttöohjeen laadintaa ei myöskään ole ohjattu sisällön suhteen, mikä näyttäytyi eri laitteiden ohjeissa hyvin erilaisina sisältöinä. Toisin sanoen standardit käyttöohjeiden sisällöistä älyominaisuuksiin liittyen näyttävät puuttuvan kokonaan ja sellaiset olisi hyvä luoda viranomaisten toimesta. Käyttöohjeista voidaan myös päätellä, että tietoturva-aukkoja syntyy laitteesta riippuen hyvin erilaisia. Älyjääkaappi voidaan yhdistää modeemin tai reitittimen lisäksi saman laitevalmistajan muihin elektroniikkalaitteisiin. Tämä mahdollistaa uusia reittejä haavoittuvuuksille. Samoin älykoneisiin liitettävät käyttäjiä voi olla useita, kunhan käyttäjätilin salasanat on jaettu käyttäjille, jolloin kaikilla käyttäjillä pitää olla tieto siitä, kuinka suojata oma mobiililaite ja kuinka käyttää tietoturvallisesti ohjattavaa älykodinkonetta

Asetettu tavoite onnistui mielestäni hyvin, sillä tavoitteen tutkimuskysymyksiin pystyttiin vastaamaan. Teoriaosuudessa kuvattiin kokonaisvaltaisesti älykodinkoneen, tietoturvaris-

kien, tietoturvan sekä käyttöohjeiden merkityksiä sekä keskinäisiä yhteyksiä kuluttajan näkökulmasta. Käyttöohjeiden tutkimusosiossa peilattiin käyttöohjeen sisältöä teoriaosuudessa saatuihin tietoihin ja kokonaisuuteen. Tavoite sinänsä oli epärealistinen käyttöohjeista löytyneiden tulosten näkökulmasta, sillä käytetty käyttöohje otos ei riitä yleistyksiin ja tulokset voidaan julkistaa vain tutkittavien käyttöohjeiden osalta. Tavoitteesta teki haasteellisen myös teoriaosuus, jonka rajaaminen tuntui paikoitellen mahdottomalta. Laitteiden kytkeminen toisiinsa tekee verkostosta ja variaatioista loppumattoman ja sen kuvaaminen innosti liikaa erilaisten vaihtoehtojen tutkimiseen. Oman haasteensa toi myös riittävän objektiivisuuden säilyttäminen, koska tutkiessani käyttöohjeita syntyi monenlaisia mielipiteitä. Olen pyrkinyt kuitenkin aktiivisesti pitämään mielipiteet erossa tutkimusta tehdessä ja asettumaan tutkijan rooliin neutraalina aineiston lukijana. Tässä auttoivat aineistoon tehdyt täsmälliset kysymykset, joihin etsin vastauksia käyttöohjeista.

Jäin myös pohtimaan älykodinkoneiden ajankohtaisuutta kuluttajan, tietoturvallisuuden ja käyttöohjeiden näkökulmista. En löytänyt näistä yhteen liitettyjä tutkimuksia selatessani Internet-sivustoja. Tietoturvasta ja tietoturvariskeistä löytyy runsaasti tutkimuksia, mutta niitä ei ole käsitelty kuluttajalle annettavien käyttöohjeiden kautta. Käyttöohjeet älykodinkoneissa ovat myös uusi alue ja tämä opinnäytetyö on ehkä uusin tutkimus niiden sisällöstä tietoturvallisuuteen liittyen.

Jatkotutkimusehdotuksena esitän, että tämän opinnäytetyön tuloksia voidaan käyttää tutkittaessa maahantuojien tai valmistajien halukkuutta täydentää käyttöohjeita siten, että ne ohjaisivat kuluttajaa suojautumaan älykodinkoneiden mahdollisilta tietoturvariskeiltä. Toisena tutkimusaiheena mieleeni tulee valvontaviranomaisten ja maahantuojien yhteistyö. Voivatko näiden laitteiden maahantuojat yhdessä Suomen valvontaviranomaisten kanssa laatia yhdessä kuluttajaa hyödyntäviä käyttöohjeita varoituksineen. Kolmantena jatkotutkimusaiheena ehdotan standardin luomista käyttöohjeen tietoturvaa käsittelevälle sisällölle.

Opinnäytetyö alkoi innostumisesta aiheesta älykodinkone, koska niistä uutisoitiin eri yhteyksissä niihin liittyvien tietoturvauhkien osalta. Syksyllä 2017 aloitin aineiston etsimisen yleisesti liittyen näihin laitteisiin ja luin useita artikkeleita erilaisista verkkojulkaisuista. Teoriaa työstäessä varsinaisen sisältöanalyysin kohde alkoi hahmottumaan käyttöohjeeksi, sillä se toimii yhtenä tärkeänä riskeiltä suojautumisen dokumenttina kuluttajan näkökulmasta. Teorian täydentyessä aloin peilaamaan teoriaa ja tutkimuskohdetta sekä iteroin tätä vaihetta useita kertoja. Näin pystyin vertailemaan teoriaa ja tutkittavaa osaa keskenään koko prosessin ajan. Aihe älykodinkoneet on ollut todella mielenkiintoinen, mutta samalla erittäin haastava. Haastavuuden tähän on tuonut älykodinkoneissa oleva suuri määrä eri tekniikkaa, standardien puute sekä syvällisen tiedon puute itse laitteista. Aloitin

opinnäytetyön syyskuussa 2017 ja työtäni viimeistellessä nyt maaliskuussa 2018 huomaan, että aineistona käyttämäni lähteet ovat vanhentuneet ainakin siltä osin, mitä niissä on kerrottu turvallisista salaustekniikoista. Toisena haasteena oli käytettyjen Internet-lähteiden muuttuminen prosessin aikana. Esimerkiksi Suomen Valtionvarainministeriön ohjeistuksen linkkien takana olevia sivustoja on ryhdytty uudistamaan, jolloin lähteinä olleet linkit eivät enää toimineet. Älykodinkoneisiin sinänsä ei ole julkistettu tänä aikana tietoturvariskeihin liittyen suojausohjelmia, mutta sen sijaan laitteisiin ja sitä ympäröivän tekniikkaan ja protokolliin liittyen hyökkäyksiä ja tietoturva-aukkoja on löydetty lähes kuukausittain.

Opinnäytetyön prosessin aikana olen oppinut kiinnittämään enemmän huomiota kotonani oleviin älylaitteisiin ja niiden suojaukseen. Opinnäytetyön kirjoittaminen on myös parantanut kykyäni etsiä tietoa viranomaisten sivustoilta sekä jäsentämään saatua tietoa paremmin. Tietoperustan kokonaisuus ja käyttöohjeiden analysointi ovat lisänneet tietämystäni älykodinkoneista siinä määrin, että pystyn ohjeistamaan ja auttamaan tuttaviani sekä perheenjäseniäni näihin liittyvissä kysymyksissä. Työssäni osaan huolehtia osaltani paremmin älylaitteiden käyttöön liittyvien riskien hallinnoimisesta ja havaitsemaan mahdollisia tietoturvallisuuteen liittyvä puutteita. Työhöni ei liity älykodinkoneita, mutta huomaan sellaisia olevan yhteisissä tiloissamme ja näistä olen jo keskustellut laitteista vastaavien kanssa.

Mitä enemmän IoT-laitetta ja sitä ympäröivää tietoturvaan liittyvää problematiikkaa luin, sen laajemmaksi tutkittava kokonaisuus kasvoi. Tietämykseni tason kasvaessa jäin pohtimaan, mitä tietoa kansalaisena ja kuluttajana tarvitsen sekä mistä tuota tietoa pitäisi saada ja missä vaiheessa. Tietoturvariskeiltä suojautuminen on haastavaa, mutta esimerkiksi Viestintäviraston sivuilla on saatavilla runsaasti ohjeistusta, tietoa sekä varoituksia kodin laiteintegraation eri osista, joihin älykodinkone kytkeytyy. Sivuilla olevan tiedon perusteella on helppo aloittaa tietämyksen kasvattaminen ja laajentaa sitä kodin laitekokonaisuudessa laite kerrallaan ottaen yhteyttä laitteen tukipalveluja tarjoaviin tahoihin, ellei käyttöohjeesta ilmene tarpeeksi tietoa.

IoT luo suuria mahdollisuuksia yritysten liiketoiminnalle taloudellisesti. Näkökulmani tässä opinnäytetyössä on ollut kuluttaja eli kuka tahansa meistä, joka ostaa älykodinkoneen. Älykodinkoneissa on jo havaittu puutteita ja niihin on hyökätty tai niitä on käytetty osana hyökkäystä. Tästä syystä olisi sekä yritysten liiketoiminnan että kuluttajan tietoturvallisuuden kannalta hyödyllistä ryhtyä toimenpiteisiin paremman tietoturvan aikaansaamiseksi.

Tulevaisuudelta odotan, että älylaitteiden tietoturvallisuuta koskevat kansainväliset standardit saataisiin valmiiksi, jotta laitevalmistajat parantaisivat älykodinkoneiden suojausta ja noudattaisivat yhteisesti hyväksyttyjä standardeja. Lisäksi odotan, että kuluttajalle annetaan riittävä tietous älykodinkoneiden tietoturvariskeiltä suojautumiseen mahdollisimman ymmärrettävästi käyttöohjeissa tai niihin liitettävissä erillisissä kuluttajille suunnatuissa tietoturvaoppaissa. Tulevaisuus näyttää toteutuvatko nämä.

Lähteet

Andrearsson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tietosanoma. Helsinki.

Apple 2017. Miten toimia ennen iPhonen, iPadin tai iPod touchin myymistä tai luovuttamista. Luettavissa: https://support.apple.com/fi-fi/HT201351. Luettu: 11.1.2018.

Bosch. Kalusteisiin sijoitettavat astianpesukoneet. Luettavissa: http://www.bosch-home.fi/tuotteet/astianpesukoneet/kalusteisiin-sijoitettavat-astianpesukoneet. Luettu: 18.3.2018.

Cisco 2014a. The Internet of Things. Luettavissa: https://www.imda.gov.sg/-/media/imda/files/industry-development/infrastructure/technology/jeffapcar.pdf?la=en. Luettu: 14.11.2017.

Cisco 2014b. Introduction to Networks. Cisco Press. Indianapolis, USA.

EETimes 2015. Juggling Data Connectivity Protocols For Industrial IoT. Luettavissa: https://www.eetimes.com/author.asp?doc_id=1326169. Luettu: 13.11.2017.

Elisa 2017. Elisa Turvapaketti puhelimelle tai tabletille (Android, iOS). Luettavissa: https://elisa.fi/asiakaspalvelu/aihe/matkapuhelinliittymat/ohje/mobiiliturva/. Luettu: 13.12.2017.

Kuluttajaturvallisuuslaki 22.7.2011/920.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. WS Bookwell. Porvoo.

Home Connect 2015. Tietoturva. Luettavissa: http://www.home-connect.com/fi/fi/datenschutz/datenschutz.html. Luettu: 8.1.2018.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturva opas. Alma Talent. Helsinki.

Kananen, J. 2008. Kvalitatiivisen tutkimuksen teoria ja käytänteet. Jyväskylän ammattikorkeakoulu. Jyväskylä.

Kuula, A. 2006. Tutkimusetiikka. Gummerus Kirjapaino Oy. Jyväskylä.

Mikrobitti 10/2016. Opas: Näin huolehdit älypuhelimesi tietoturvasta. Luettavissa: https://www.mikrobitti.fi/2016/10/opas-nain-huolehdit-alypuhelimesi-tietoturvasta. Luettu: 14.11.2017.

MikroPC 11/2014. Näin rakennat kotiverkon. Luettavissa: http://mikropc.net/nettilehti/pdf/2011201446.pdf. Luettu: 15.12.2017.

Miller, M. 2015. The Internet of Things. QUE. Indianapolis, USA. Luettu 15.12.2018.

Norppa, K. & Peltomäki, J. 2015. Rikos meni verkkoon. Talentum. Helsinki.

Neato. Neato botvac connected. Luettavissa: https://www.neatorobotics.com/. Luettu 18.3.2018.

Opetus ja kulttuuriministeriö. Tietoturva. Luettavissa: https://avointiede.fi/tietoturva?inheritRedirect=true). Luettu: 5.1.2018.

Samsung. History. Luettavissa: https://www.samsung.com/us/aboutsamsung/company/history/. Luettu:17.3.2018.

SFS. Suomen Standardoimisliitto SFS Ry. Mikä SFS on? Luettavissa: https://www.sfs.fi/sfs_ry. Luettu: 18.3.2018.

Tietosuojavaltuutetun toimisto 2010. Koti WLAN:n suojaaminen. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpxXsSV/Kotiwlanin_suojaaminen.pdf. Luettu: 1.10.2017.

Tukes 2016. Tuotteiden käyttöohjeet ja turvallista käyttöä koskevat merkinnät. Luettavissa: http://www.tukes.fi/Tiedostot/julkaisut/Tuotteiden_kaytto-ohjeet_opas.pdf. Luettu: 4.1.2018.

Tuomi, J. & Sarajärvi, A. Laadullinen tutkimus ja sisältöanalyysi. Tammi. Helsinki. Luettu: 17.3.2018.

Turvallisuuskomitea 2017. Kodin kyberopas. Luettavissa: https://www.turvallisuuskomitea.fi/index.php/files/10/lataukset/67/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf. Luettu: 1.10.2017.

Valtionvarainministeriö 2008. Valtionhallinnon tietoturvasanasto. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229. Luettu: 2.12.2017.
Valtionvarainministeriö 2017a. Riskienhallintatyökalu – Excel – laajempi versio. Luettavissa: https://www.vahtiohje.fi/web/guest. Luettu 16.3.2018.

Valtionvarainministeriö 2017b. Ohje riskien hallintaan. Luettavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y. Luettu: 2.12.2017.

Viestintävirasto 2015a. Heikosti ylläpidetyt kotireitittimet ovat verkkorikollisten kohteena - osa 1. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2015/10/ttn201510121051.html. Luettu: 12.12.2017.

Viestintävirasto 2015b. Verkkojen ja palvelujen tietoturva. Luettavissa: https://www.viestintavirasto.fi/ohjausjavalvonta/tekninentoimivuusjatietoturva/tietoturva.html. Luettu: 5.10.2017.

Viestintävirasto 2016. Ota esineiden internetin suojauskeinot haltuun. Luettavissa: ttps://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2016/06/ttn201606210934.html. Luettu 5.10.2017.

Viestintävirasto 2017a. Internettiin liitettyjen laitteiden turvallinen käyttö. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/laitteenturvallinenkaytto.html. Luettu: 5.11.2017.

Viestintävirasto 2017b. WPA2-haavoittuvuudet mahdollistavat Wifi-verkkojen salauksen murtamisen. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2017/haavoittuvuus-2017-033.html. Luettu: 20.10.2017.

Viestintävirasto 2017c. Vakavia haavoittuvuuksia Bluetooth-toteutuksissa. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2017/haavoittuvuus-2017-029.html. Luettu 20.10.2017.

Viestintävirasto 2017c. Kyberturvallisuus yritysten arkipäivää. Luettavissa: http://docplayer.fi/56294840-Kyberturvallisuus-yritysten-arkipaivaa.html. Luettu: 15.12.2017.

YTJ. Yritys ja yhteisötietojärjestelmä. Yrityshaku. Luettavissa: https://tietopalvelu.ytj.fi/yrityshaku.aspx?kielikoodi=1. Luettu 17.3.2018.

Liitteet

Liite 1. Käyttöohjeet

Valmistaja	Laite	Internet osoite
Samsung	Jääkaappi RF56M9540SR	http://downloadcenter.samsung.com/content/UM/201708/20170818153539453/T-TYPE_RF9500M_DA68-03460J-04_EN_DE_IT_FR_SV_DA_NO_FI.pdf
Bosch	Astianpesukone SMA67MD06E	http://media3.bosch-home.com/Documents/9001276904_C.pdf
Neato	Imuri botvacD3connected botvacD5connected	https://004ad429deffb6ec831a-519cff0c4aadf0882029ee8826ed368e.ssl.cf5.rackcdn.com/Neato_User_Guide_D3_D5_10-Lang_EMEA_HR_Rev_2.pdf http://5df8aa4b674bc30f90a6-519cff0c4aadf0882029ee8826ed368e.r50.cf5.rackcdn.com/Botvac_Important_Information_Connected_10-Lang_500-0036rev3.pdf https://www.neatorobotics.com/wp-content/uploads/2015/09/botvac-connected-qsg-10-lang.pdf
Philips	Kahvinkeitin CranBaristo Avanti HD8977	https://www.download.p4c.philips.com/files/h/hd8977_01/hd8977_01_dfu_fin.pdf