Janne Lahti

Kodin IoT-laitteet ja tietoturva

Tietotekniikan kandidaatintutkielma

9. toukokuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Janne Lahti

Yhteystiedot: janne.m.lahti@student.jyu.fi

Ohjaaja: Tytti Saksa

Työn nimi: Kodin IoT-laitteet ja tietoturva

Title in English: Home IoT devices and information security

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 20+0

Tiivistelmä: Tässä tutkielmassa käydään läpi kodin IoT-laitteisiin liittyvää tietoturvaa. Kirjallisuuteen perehtymällä määritellään, millaisia esineitä kuuluu kodin IoT-laitteisiin, ja millaisia teknisiä ominaisuuksia niillä on. Laitteiden ja ominaisuuksien avulla hahmotetaan, millaisia suojautumisen keinoja niihin on mahdollista luoda. Suojautumisen ohella eritellään erilaisia vaihtoehtoja kohdistaa hyökkäyksiä IoT-laitteisiin. Lisäksi tutkielmassa tarkastellaan suhtautumista IoT-laitteiden tietoturvaan. Erityisesti valmistajien vastuuta tietoturvasta huolehtimisesta otetaan huomioon. Myös muiden toimijoiden, kuten valtioiden toimenpiteitä tietoturvan osalta eritellään.

Avainsanat: esineiden internet, koti, tietoturva, verkkohyökkäykset

Abstract: This thesis analyzes the information security of home IoT devices. By reviewing the literature, it determines what kind of objects belong to home IoT devices and what technical properties they have. Devices and their features are used to outline what means of security can be created for them. In addition to security, various options to target attacks on IoT devices are specified. Also, the thesis examines the attitude towards the security of IoT devices. In particular, the responsibility of manufacturers for security is taken into account. The measures of other actors, such as states, towards information security are also specified.

Keywords: Internet of Things, home, information security, cyber attacks

Sisällys

1 JOHDANTO 1

2 KODIN IOT-LAITE 3
2.1 Käyttökohteet 3
2.2 Tekniset ominaisuudet 4

3 SUOJAUTUMINEN HYÖKKÄYKSILTÄ 6
3.1 Suojautumisen keinot 6
3.2 Erilaiset hyökkäykset 9

4 VALVONTA 11
4.1 Valmistajan vastuu 11
4.2 Julkiset toimijat 12

5 YHTEENVETO 14

LÄHTEET 16

1 Johdanto

IoT-laitteiksi luokiteltavat tuotteet ovat ilmestyneet monille aloille viimeisten vuosien aikana, ja nykypäivänä niitä löytyy myös tavallisten kuluttajien kodeista. Kodin IoT-laitteet on saatettu kehittää toteuttamaan melko yksinkertaista toimintaa. Yksinkertaisesta toiminnasta huolimatta niillä voi olla monipuolisia ominaisuuksia, esimerkiksi perinteistä tietokonetta muistuttava ohjelmisto sekä yhteys internetiin. Erilaisten ominaisuuksien avulla ne voivat toimia kanavana muihin kodin laitteisiin ja vaarantaa siten omistajansa turvallisuutta ja yksityisyyttä hyvin laajasti.

Tutkielmassa on tarkoitus kartoittaa kodin IoT-laitteiden tietoturvaa. Keskeinen tavoite on selvittää, millaisia ongelmia on havaittu ja miten niitä on yritetty korjata. Haavoittuvuuksia on voinut jäädä erilaisiin osiin laitteissa, ja niiden ympäristössä. Esimerkiksi kun internetyhteys mahdollistaa IoT-laitteen viestimisen muiden laitteiden kanssa, voi uhkia löytyä yhteydestä tai viestinnän muista osapuolista. Kiinnostava näkökulma onkin hahmottaa, millaisia erityisiä piirteitä näihin laitteisiin liittyy, ja onko niiden korjaamisessa ollut erityisiä haasteita.

Aihetta käsitellään kirjallisuuskartoituksena, sillä tietoturvasta on tehty runsaasti tieteellistä tutkimusta. Tietoturva on erittäin tärkeä ominaisuus myös asiakkaalle, ja siksi sitä on syytä tarkastella puolueettomasta näkökulmasta. Laitteiden valmistajat ovat pääsääntöisesti kaupallisia yrityksiä, ja niillä on omat vaihtelevat tavoitteensa. Uusien IoT-laitteiden ilmestyessä markkinoille myös niiden päällimmäiset huomiot liittyvät laitteen keskeisiin hyötyihin. Hyötyjen ohella pitäisi huolehtia haittojen minimoimisesta, esimerkiksi mahdollisuudesta, että laite luo heikkouden ympäristöön, jossa se sijaitsee. Koska tietoturvaa on käsitelty tieteellisissä tutkimuksissa laajasti, keskitytään tässä tutkielmassa luomaan yleinen käsitys laitteiden piirteiden ja haasteiden luonteesta.

Luvussa 2 käydään läpi kodin IoT-laitteita yleisellä tasolla. Luvun tavoite on määritellä tutkielmaa koskevia laitteita niiden käytön, rakenteen ja toimintojen perusteella. Luvussa 3 perehdytään tarkemmin tyypillisiin keinoihin suojautua hyökkäyksiltä ja käsitellään erilaisten haavoittuvuuksien mahdollistamia hyökkäyksiä. Luvussa 4 esitellään erilaisia toimijoita

ja toimenpiteitä, joiden avulla tietoturva voidaan säilyttää korkeammalla tasolla. Luvussa 5 muodostetaan yhteenveto tuloksista ja johtopäätöksistä, joita tutkielman myötä ilmeni. Luvussa pohditaan myös tietoturvaan liittyviä heikkouksia ja mahdollisia tulevia toimenpiteitä.

2 Kodin IoT-laite

Ennen tietoturvaan tarkempaa perehtymistä on syytä määritellä IoT-laitteita, ja niihin liittyviä ominaisuuksia. Ominaisuuksisien avulla saadaan käsitys rakenteista ja malleista joihin hyökkäykset ja hyökkäyksiltä puolustautuminen liittyvät. Tässä luvussa käydään aluksi läpi kodin IoT-laitteiden yleisiä piirteitä. Yleisten piirteiden jälkeen perehdytään tarkemmin laitteiden teknisiin ominaisuuksiin.

2.1 Käyttökohteet

IoT-laitteet ovat tulleet älypuhelimien perässä moniin erilaisiin ympäristöihin. Tästä kertovat esimerkiksi Han, Jeon ja Kim (2015) tutkimuksessaan. Heidän listauksessaan tällaisia ympäristöjä ovat esimerkiksi kodit, kaupungit ja terveydenhuolto. Tässä tutkielmassa perehtydään IoT-laitteisiin juuri kotiympäristössä.

Monimuotoisuutta ilmenee myös kodin IoT-laitteisiin kuuluvien tuotteiden ryhmässä. Erilaisia laitteita listaavat esimerkiksi Bandekar ja Javaid (2017), joiden mukaan niitä voivat olla valaisimet, ilmastointiinvaikuttavat koneet ja keittiön laitteet kuten mikroaaltouuni. Monimuotoisuuden olemassaolon erääksi syyksi Bandekar ja Javaid mainitsevat, että laitteet ovat kooltaan pieniä, ja helposti etänä hallittavia.

Heriadin ja Pamujin kuvaus (Heriadi ja Pamuji 2020) kodin IoT-laitteista korostaa niiden monipuolisuutta samoin kuin Bandekar ja Javaid (2017). Heriadi ja Pamuji (2020) sisällyttävät määritelmään erilaiset kodinkoneet, kuten jääkaapit ja lamput, mutta myös erityyppiset sensorit kunhan ne ovat yhdistettynä internettiin. IoT-laite määritellään heidän artikkelissa myös sellaiseksi laitteeksi, joka kykenee siirtämään dataa verkon yli ilman, että ihmisen tarvitsee tehdä mitään.

Boyes ja Watson (2019) käsittelevät artikkelissaan kodin IoT-laitteina erityisesti sellaisia tuotteita, jotka ohjaavat esimerkiksi kodin valaistusta ja lämmitystä. Tuotteiden pitäisi silloin jossain määrin vaikuttaa kodin energiankäyttöön ja hiilidioksidipäästöihin. Luokittelun osalta Boyes ja Watson jakavat laitteita ruoan valmistukseen ja säilytykseen, sekä siivouk-

seen.

2.2 Tekniset ominaisuudet

IoT-laitteet eivät ole erityisen tehokkaita. Turvallisuutta suunnitellessa olisi hyvä ottaa huomioon, että siihen liittyvät mekanismit saisivat käyttää vähän resursseja (Augusto-Gonzalez ym. 2019). Heriadi ja Pamuji (2020) toteavat myös, että IoT-laitteet ovat tyypillisesti pieniä ja yksinkertaisia. Lisäksi niiden laitteisto on rajallinen esimerkiksi virran ja muistin suhteen, ja ohjelmistosta on tehty minimaalinen. Tämä minimaalisuus saattaa Heriadin ja Pamujin mukaan jättää myös turvallisuuden vastaavalle tasolle. Bandekar ja Javaid (2017) nostavat samoin esiin kodin IoT-laitteiden pienet resurssit, jolla tarkoitetaan tehon vähäisyyttä. Verkkoa ja IoT-laitteita voitaisiin heidän mukaansa suojata lisäämällä verkkoon sitä varten kehitettyä laitteistoa. Laitteisto lisäisi energian kulutusta, ja siksi pienitehoisten IoT-laitteiden kanssa Bandekar ja Javaid ovat halunneet keskittyä ongelmanratkaisuun algoritmin pohjalta.

Kodin-IoT laitteet voivat viestiä muille laitteille käyttäen esimerkiksi internet- ja Bluetooth-protokollia (Augusto-Gonzalez ym. 2019). Internet-protokollien kanssa laite on yhteydessä kotona olevaan yhdyskäytävään, joka puolestaan on yhteydessä muuhun internettiin (Han, Jeon ja Kim 2015). Yhdyskäytävä voi käytännössä olla esimerkiksi reititin tai hubi (Boyes ja Watson 2019). Tämän yhdyskäytävän kautta laite voi olla yhteydessä palvelimeen, joka kerää tietoa erilaisista tapahtumista (Han, Jeon ja Kim 2015). Augusto-Gonzalez ym. (2019) huomioivat artikkelissaan myös yhdyskäytävän osuuden, kun he erittelevät kodin IoT-verkkoa. Yhdyskäytävän suojaamisessa tavoitteena on saada hallintaa verkon IoT-laitteisiin riippumatta niiden käyttämistä protokollista (Augusto-Gonzalez ym. 2019).

Viestinnän lisäksi laitteiden ominaisuuksiin kuuluu erilaisia sensoreja ja antureja. Anturien tarkoitus on yleensä mitata ilman ominaisuuksia, kuten lämpötilaa, kosteutta ja ääntä (Bandekar ja Javaid 2017). Myös esimerkiksi Heriadi ja Pamuji (2020) listaavat kodin IoT-laitteiden ominaisuuksiksi sensorit, mutta he eivät eritelleet tarkemmin niiden mittaamia ilmiöitä.

Kun IoT-laitteet vaikuttavat kodin sähkölaitteiden toimintaan, täytyy niiden suunnittelussa ottaa huomioon menetelmät sähkövirtojen hallinnassa. Boyes ja Watson (2019) kertovat, että nykyiset IoT-järjestelmät ovat sen kannalta yleensä melko yksinkertaisia. Sähkö tulee ver-

kosta, ja IoT-laite voi joko sallia virran kulkemisen tai katkaista sen esimerkiksi valaisimelta. Tulevaisuudessa jos kotona on aurinkopaneeleja, varaavia akustoja ja sähköauton latureita, tulee IoT-laitteen hallittavasta kodin sähköjärjestelmästä heidän mukaansa huomattavasti monimutkaisempi.

Boyes ja Watson (2019) tarkentavat vielä, että kodin IoT-laitteisiin liittyy usein laitekohtainen ohjelma. Ohjelma eli sovellus toimii internet-selaimen välityksellä, tai se ladataan älypuhelimeen sen sovelluskaupasta. Ohjelman keskeinen tehtävä on Boyesin ja Watsonin mukaan tarkkailla ja hallinnoida IoT-laitetta.

3 Suojautuminen hyökkäyksiltä

IoT-laitteet ovat yleensä yhdistettynä internettiin. Heriadi ja Pamuji (2020) toteavat, että internet on luonteeltaan sellainen, että mistä vain voi hyökätä minne vain. Siksi heidän mukaansa kyberturvallisuus on IoT-laitteiden keskeisin haaste turvallisuudessa.

IoT-laitteisiin liittyvä tietoturva on myös ollut esillä jo jonkin aikaa. Babar ym. (2011) käsittelevät artikkelissaan jo vuonna 2011 IoT-laitteisiin liittyvää tietoturvaa. Artikkelin tekstissä nousee esiin samanlaiset tavat tehdä hyökkäyksiä, kuin myöhemmissäkin tutkimuksissa (Heriadi ja Pamuji 2020; Augusto-Gonzalez ym. 2019). Ongelmiksi Babar ym. mainitsevat myös myöhempien tutkimusten tavoin, että suunnitteluvaiheessa ei olla keskitytty tarpeeksi turvallisuuteen.

Hernández-Serrano ym. (2018) huomauttavat, että useimmat IoT-laitteet käsittelevät käyttäjään liittyvää tietoa. Tiedot voivat olla hyvinkin henkilökohtaisia, jolloin yksityisyyden suojelu on tärkeää. Samalla Hernández-Serrano ym. toetavat myös, että tiedon suojelu ei ole yksinkertainen tehtävä, koska IoT-laitteet sisältävät suuren määrän ja merkittävästi vaihtelevaa laitteistoa ja ohjelmistoa.

Tietoturva ei riipu pelkästään IoT-laitteesta itsestään, vaan siihen vaikuttavat myös muut laitteet ja yhteydet (Boyes ja Watson 2019). Boyesin ja Watsonin mukaan erityisesti samassa verkossa olevat muut laitteet voivat vaarantaa IoT-laitteen turvallisuutta. Tilanne muodostuu ongelmalliseksi varsinkin jos IoT-laite vaikuttaa kodin kriittisiin kohteisiin, kuten sähkönkäytön ohjaukseen.

Tämän luvun tarkoitus on eritellä keinoja, joita IoT-laitteiden ominaisuudet mahdollistavat suojautumiseen ja tietoturvan ylläpitämiseen. Suojautumiskeinojen esittelyn jälkeen käydään läpi yleisiä keinoja tehdä hyökkäyksiä.

3.1 Suojautumisen keinot

Tietoturvaa voi parantaa huolellisella suunnittelulla. Tähän Heriadi ja Pamuji (2020) ehdottavat SQUARE-menetelmää, jossa on yhdeksän vaihetta. Menetelmässä aluksi varmistetaan

määritelmät termeille esimerkiksi virukselle. Toisena vaiheena tunnistetaan tavoite, esimerkiksi kyberturvallisuudesta huolehtiminen kodin IoT-laitteiden kanssa. Kolmantena luodaan artefakti ja siihen liittyvät kaaviot. Niiden jälkeen ryhdytään tunnistamaan riskejä. Riskien tunnistuksessa tärkeää on arvioida myös niiden vakavuutta. Viidentenä valitaan tekniikoita turvallisuustarpeen tarkempaan analysointiin, ja tehdään esimerkiksi kirjallisuuden tarkastelua. Seuraavaksi analysoinnin perusteella luodaan lista turvallisuusvaatimuksista. Seitsemännessä vaiheessa vaatimukset luokitellaan sopiviin kategorioihin. Luokittelun jälkeinen vaihe on asettaa tärkeysasteet luokiteltujen kohteiden vaatimuksille. Viimeisenä vedetään vielä yhteen saatuja tuloksia, ja asetetaan toimenpiteet jotta tulokset saavutetaan (Heriadi ja Pamuji 2020).

Suunnittelusta toteutukseen asti päätyneissä verkoissa henkilökohtaiset laitteet ja kotia ohjaavat IoT-laitteet ovat usein samassa ryhmässä (Boyes ja Watson 2019). Tämä ei ole tietoturvan kannalta hyvä tilanne, koska haavoittuvuus tai hyökkäys mihin tahansa laitteeseen vaarantaisi silloin koko verkon kaikki laitteet. Boyesin ja Watsonin mukaan parempi vaihtoehto olisi jakaa laitteet turvallisiin vyöhykkeisiin.

Verkon yksittäisistä laitteista tärkeä suojauksen kohde on yhdyskäytävä, eli laite jonka kautta kodin IoT-laitteet ovat yhteydessä internettiin. GHOST-projektissa, johon Augusto-Gonzalez ym. (2019) artikkeli keskittyy, pyritään huomioimaan tämä osa suojauksessa. Augusto-Gonzalez ym. kertovat, että yhdyskäytävän suojauksessa vaikutetaan sen kautta kulkeviin datapaketteihin. Toiminnan pitäisi silti tapahtua niin, ettei se vaikuta laitteiden suorituskykyyn.

GHOST-arkkitehtuuri voi tarkkailla liikkuvan datan sisältöä (Augusto-Gonzalez ym. 2019). Sisällön avulla voidaan huomata, mikä on hyödyllistä dataa, ja missä on poikkeuksia. Viestinnän poikkeuksiin keskittyminen suojauksessa mahdollistaa sen, että IoT-laitteet voivat olla monimuotoisia. Augusto-Gonzalez ym. toteavat myös että luokitteleva ohjelmisto oppii IoT-laitteiden toimintatapoja verkossa. Opittujen toimintamallien avulla voidaan sitten helpommin löytää poikkeuksia.

Paikallisten toimintojen lisäksi GHOST-alustaan kuuluu pilvipohjainen tietoarkisto (Augusto-Gonzalez ym. 2019). Boyes ja Watson (2019) huomauttavat, että pilvipalveluun nojaaminen ei välttämättä ole hyvä asia. Jos yhteydet katkeavat, tai niihin hyökätään, jäävät kodin IoT-

laitteet ilman niiden taustapalvelua. Tähän Boyes ja Watson ehdottavat, että palvelin toimisi omistajan kotona.

Käyttäjällä on myös mahdollisuus vaikuttaa GHOST-arkkitehtuurin toimintaan (Augusto-Gonzalez ym. 2019). Valintojen perusteella voi esimerkiksi asettaa yhteyden estoja, ja tapahtumiin liittyviä riskejä. Augusto-Gonzalez ym. täsmentävät kuitenkin artikkelissaan, että tavoitteena on käyttäjän puuttuminen toimintaan mahdollisimman harvoin.

Tietoturvaa tarjoavan ohjelmiston on syytä esittää selkeä visualisaatio tilanteestaan (Augusto-Gonzalez ym. 2019). Hyvä visualisaatio mahdollistaa onnistuneen vuorovaikutuksen ihmisen ja tietokoneen välillä. Onnistuneesta vuorovaikutuksesta taas seuraa heidän mukaansa se, että käyttäjällä on mahdollisuus tehdä oikeita valintoja. Hyvän visualisaation myötä käyttäjä voi nähdä esimerkiksi yleistä ja laitekohtaista historiaa, jotka puolestaan mahdollistavat käyttäjän itse havaita poikkeuksia ja mahdollisia uhkia.

Bandekar ja Javaid (2017) nostavat esiin Augusto-Gonzalez ym. (2019) -artikkelin tavoin IoT-laitteiden tietoturvassa esiin ratkaisun, jossa suojaukseen luotu ohjelmisto seuraa dataliikennettä koko verkossa. Tällainen ohjelmisto pystyisi huomaamaan poikkeuksia ja muita epäilyttäviä tapahtumia, joita estämällä verkon laitteet pysyvät turvassa.

Bandekar ja Javaid (2017) toteavat artikkelissaan, että heidän algoritminsa onnistuu suojaamaan laitteita. Algoritmi kykenee huomaamaan ja estämään hyökkäyksen verkossa. Se toimii myös alhaisella virralla, jolloin sen kytkeminen verkkoon ei juurikaan lisää laitteiden virrankulutusta. Bandekar ja Javaid muistuttavat vielä, että vaihtoehtoinen toteutus erillisellä turvallisuutta valvovalla laitteistolla olisi tarvinnut paljon enemmän energiaa. Heidän käyttämänsä ratkaisu ei kuitenkaan ole täydellinen. Tähän liittyen todetaan, että algoritmi ei huomaa kaikkia mahdollisia hyökkäysten keinoja. Tulevaisuuden työnä olisikin Bandekarin ja Javaidin mukaan löytää vastaavanlainen ratkaisu, joka toimisi myös erityyppisissä hyökkäyksissä.

3.2 Erilaiset hyökkäykset

Hyökkäykset voidaan jaotella useisiin luokkiin. Augusto-Gonzalez ym. (2019) esittävät niihin liittyen kolme kategoriaa: fyysiset hyökkäykset, ohjelmistohyökkäykset ja verkon kautta tapahtuvat hyökkäykset. Heriadi ja Pamuji (2020) puolestaan käyttävät viittä erilaista hyökkäystapaa IoT-laitteilla, ja niistä kolme ovat samoja Augusto-Gonzalez ym. (2019) kanssa. Kaksi muuta ovat vielä sivukanava ja kryptoanalyysi hyökkäys. Ensimmäinen molempien mainitsema on fyysiset hyökkäykset. Niihin kuuluu fyysinen toiminta, jota henkilö voi tehdä IoT-laitteelle. Augusto-Gonzalez ym. (2019) luettelevat, että tämä tarkoittaa esimerkiksi laitteen sulkemista tai rikkomista. GHOST-arkkitehtuuri voi havaita tällaisen hyökkäyksen tarkkailemalla liikenteen määrää yhteyspisteellä. IoT-laitteen toiminnan muuttuessa, esimerkiksi sammuessa, sen viestinnän määrä muuhun verkkoon muuttuu selvästi Augusto-Gonzalez ym. mukaan.

Toinen vaihtoehto hyökkäyksille tapahtuu verkon kautta (Augusto-Gonzalez ym. 2019; Heriadi ja Pamuji 2020). Verkossa toimiva hyökkääjä voi yrittää varastaa IoT-laitteen lähettämiä tietoja, tai vaihtoehtoisesti asentaa IoT-laitteeseen ohjelmistoa, joka vaikuttaa laitteen toimintaan haitallisella tavalla. GHOST pystyy tunnistamaan tämäntyyppisiä hyökkäyksiä seuraamalla laitekohtaisesti niiden liikenteessä tapahtuvia muutoksia (Augusto-Gonzalez ym. 2019). Heriadi ja Pamuji (2020) tarkentavat verkkohyökkäykset vielä passiivisiin ja aktiivisiin. Passiivista on esimerkiksi verkkoliikenteen tarkkailu. Aktiivista puolestaan heidän mukaansa on erilaiset toimintaa häiritsevät hyökkäykset verkon laitteisiin.

Kolmas keino Augusto-Gonzalez ym. (2019) sekä Heriadi ja Pamuji (2020) mukaan on ohjelmistohyökkäys. Jos hyökkääjä pääse käsiksi IoT-laitteen ohjelmistoon, hän voi yrittää asentaa siihen viruksia ja muita haittaohjelmia. Hyökkääjän on myös mahdollista käyttää laitteissa olevia aukkoja niiden vaarantamiseen. GHOST-ohjelmisto pystyy näissäkin tilanteissa tarkkailemaan verkon tapahtumia, ja löytämään sieltä epäilyttäviä poikkeuksia riskien vähentämiseksi (Augusto-Gonzalez ym. 2019). Heriadi ja Pamuji (2020) puolestaan tarkentavat, että IoT-laitteen oma ohjelmisto on usein ensisijainen tapa hyökätä.

Näiden kolmen yhteisen lisäksi Heriadi ja Pamuji (2020) mainitsevat vielä kaksi muuta tapaa. Ensimmäinen niistä on sivukanavahyökkäys. Se tarkoittaa käytännössä, että mitataan

vaikkapa johonkin toimintoon kuluvaa aikaa tai sähkövirtaa. Kun tiedetään, että esimerkiksi oikeilla ja väärillä salasanoilla kulutus on erilaista, voidaan Heriadin ja Pamujin mukaan päätellä, milloin jokin kirjautumistieto on oikein.

Viidentenä tapana on vielä kryptoanalyysi hyökkäys (Heriadi ja Pamuji 2020). Kyseisessä hyökkäyksessä tavoitteena on saada jollain tapaa salattu avain, ja sen kautta merkkijono, esimerkiksi salasana josta salaus on tehty. Eräs tällainen hyökkäys, jonka Heriadi ja Pamuji mainitsevat, on niin kutsuttu Man-in-the-middle.

IoT-laitteiden uhat eivät ole jääneet vain teorian tasolle, vaan niitä on myös käytetty hyökkäyksiin. Antonakakis ym. (2017) tutkimus kertoo Mirai botnetin tapauksesta. Yksinkertaisuudessaan Mirai verkkoa käytettiin tekemään suuria palvelunestohyökkäyksiä erilaisiin merkittäviin kohteisiin. Hyökkäystä tehneet laitteet olivat Antonakakis ym. mukaan pääosin IoT-laitteita.

4 Valvonta

Hyökkäysten tunnistaminen ja suojautumiskeinojen löytäminen niitä vastaan on tärkeä osa tietoturvaa. Laitteet jäävät kuitenkin alttiiksi hyökkäyksille, jos niissä ei ole käytössä löydettyjä suojautumiskeinoja. Siksi on erittäin tärkeää, että varmistetaan työkalujen käyttöönotto myös käytännössä.

Tässä luvussa tarkastellaan miten laitteista vastuussa olevat, eli niiden valmistajat ovat huolehtineet tietoturvasta. Valmistajista tehtyjen huomioiden jälkeen katsotaan vielä, millaisia ulkopuolisia valvojia toiminnalla on, ja millaista valvontaa on.

4.1 Valmistajan vastuu

Markkinoilla oleva laite on sen valmistajan käsialaa. Valmistajan vastuuseen kuuluu monien muiden tehtävien ohella kaikenlaisesta turvallisuudesta huolehtiminen. Heriadi ja Pamuji (2020) tarkentavat tätä vielä kertomalla, että kyberturvasta huolehtiminen kuuluu valmistajan ohjelmistokehityksen alueelle. Vaikka tietoturva kuuluu ohjelmistokehityksen alueelle, niin Heriadin ja Pamujin mukaan se olisi syytä tehdä erillään muusta ohjelmistokehityksestä, eikä osana sitä.

Bandekar ja Javaid (2017) puolestaan väittävät, että valmistajat kiirehtivät liikaa kodin IoT-laitteiden kanssa. Heidän mukaansa valmistajan tavoitteena on tuotteen nopea kehitys ja markkinointi, jolloin turvallisuus voi jää liian vähälle huomiolle. Myös Boyes ja Watson (2019) kertovat, että IoT-laitteiden huonosti tehty suunnittelu on aiheuttanut tietoturvaongelmia.

Tuotteiden valmistuksen ohella yritykset ovat tehneet myös tutkimusta laitteisiin liittyen. Esimerkiksi HP-yritystä edustavassa artikkelissa Rawlinson (2014) kertoo, että jopa 70 % kaikista IoT-laitteista olisi haavoittuvaisia. Tutkimuksessa havaittiin, että esimerkiksi salasanoilta ei vaadittu riittävää pituutta tai monimutkaisuutta. Lisäksi verkossa tapahtuva viestintä oli artikkelin mukaan usein puutteellista, koska liikennettä ei salattu ollenkaan.

4.2 Julkiset toimijat

Turvallisuus on tärkeä osa IoT-laitteita, mutta myös monia muita tuotteita. Sen huono toteutus voi aiheuttaa suurta vahinkoa laitteen käyttäjälle, joten siitä huolehtimisesta on syytä jakaa vastuuta ulkopuolisille valvojille. Ulkopuoliset valvojat voivat tarkoittaa lakeja ja muita säädöksiä, tai erillisiä yhtiöitä.

Säädöksiin liittyen Boyes ja Watson (2019) toteavat, että IoT-laitteet ovat melko uusi ja noususssa oleva ala, ja siksi siihen liittyvä lainsäädäntö on osin puutteellista. Vaillinaiset määräykset voivat Boyesin ja Watsonin mukaan johtaa epäilyttävään toimintaan, kun sitä ei ole erikseen kielletty. He myös korostavat, että ihmisten turvallisuuden kannalta on tärkeää, että käytännöt on säännelty tarkasti, eikä ainoastaan luoteta valmistajan hyviin periaatteisiin.

Halusta huolehtia kodin IoT-laitteiden turvallisuudesta myös valmistajien ulkopuolelta löytyy todisteita. Tästä esimerkki ovat Euroopan unionin rahoittamat useat projektit liittyen IoT-laitteiden kehitykseen. Tähän aiheeseen liittyy myös tässä tutkielmassa käsitelty Augusto-Gonzalez ym. (2019) artikkelin GHOST-projekti. Augusto-Gonzalez ym. korostavat, että GHOST-projektin tavoite on luoda kodin IoT-laitteista turvallisia riippumatta laitteiden tarkasta rakenteesta. Toinen hanke on Carrozzo ym. (2018) artikkelissa kuvattu symbIoTe-projekti. Kyseisen projektin tarkoitus on kehittää palvelua, jossa erityyppiset IoT-laitteet voivat olla vuorovaikutuksessa. Palvelussa korostetaan Carrozzo ym. mukaan myös turvallisuudesta huolehtimisesta sen eri osissa.

Valtio voi olla kiinnostunut älykodeista myös sen vuoksi, että niillä voidaan vähentää hiilidioksidipäästöjä, ja tehostaa uusiutuvien energialähteiden käyttöä (Boyes ja Watson 2019). Tehostusta voi tapahtua esimerkiksi niin, että laitteet reagoivat verkossa olevan sähkön määrään. Reagointi tarkoittaa esimerkiksi sitä, että kotona on akkuseinä, jonka käytön osuutta säädellään sen mukaan, kuinka paljon kulutusta verkossa on tai kuinka paljon sähkö maksaa verkossa. Boyes ja Watson toteavat, että Iso-Britanniassa kotien lämmitys luo merkittävän osan käytetystä energiasta, ja sen vuoksi aiheeseen on kiinnostusta hallituksen tasolla.

Iso-Britannian kohdalla valtio on myös asettanut tavoitteita, jotta esimerkiksi kodin IoT-laitteet voisivat vaikuttaa sähköverkon toimintaan (Boyes ja Watson 2019). Tavoitteet ovat seuraavanlaisia: ensiksi, verkkoon ei saa tulla häiriöitä IoT-laitteiden vuoksi. Toiseksi, lait-

teiden täytyy olla kyberturvallisia. Ja kolmas asia on, että datan yksityisyydestä pitää olla huolehdittu. Lisäksi laitteiden hallinnan pitää Boyesin ja Watsonin mukaansa toimia hyvin minkä tahansa verkkoon liittyvän osapuolen toimesta.

5 Yhteenveto

IoT-laitteet ovat tulleet jäädäkseen useille eri aloille. Niiden yleistymisen myötä myös erilaisia kodintoimintoja voidaan sähköistää ja automatisoida. Kodin IoT-laitteet muodostavatkin hyvin monipuolisen ryhmän tuotteita. Laitteisiin kuuluu niin pieniä mittareita, kuin suurempia kodinkoneita. IoT-laitteilla voidaan vaikuttaa kotona esimerkiksi valaistukseen tai lämmitykseen. Keskeinen osa näissä laitteissa ovat niiden anturit ja sensorit.

Teknisesti IoT-laitteista löytyy perinteisen tietokoneen piirteitä, mutta myös eroja niihin verrattuna on. IoT-laitteet ovat erityisesti kooltaan pieniä, ja käyttävät vähän resursseja, eli esimerkiksi muistia ja sähköä. Automaattisen toiminnan lisäksi IoT-laitteita voidaan hallita etänä. Yhteyksiä varten laitteista löytyy tyypillisesti internet- tai Bluetooth-protokollat. Laitteen hallinta etänä tapahtuu internet-selaimen tai älypuhelimen sovelluksen kautta.

Erilaisista käyttötarkoituksista huolimatta kodin IoT-laitteilla on yhteisiä piirteitä. Yhteiset piirteet tulevat hyödyksi, kun lähdetään luomaan suojautumiskeinoja IoT-laitteille. Silloin samoja mekanismeja voidaan käyttää laajalla joukolla laitteita. Erilaisten laitteiden suojaukseen tärkeä keino olisi jakaa verkon toimijat eri vyöhykkeisiin tai sektoreihin. Silloin yhdellä alueella tapahtuva hyökkäys ei altistaisi kaikkia laitteita uhkille.

Tärkeä kohta suojauksessa on yhdyskäytävä, eli esimerkiksi reititin, jonka kautta IoT-laitteet ovat yhteydessä muuhun internettiin. Yhdyskäytävän suojaava ohjelmisto voi tarkkailla läpikulkevaa liikennettä, ja sen myötä oppia tyypillisiä toimintamalleja. Tyypillisen toiminnan avulla voidaan löytää poikkeuksia, jotka voidaan sitten käsitellä mahdollisina uhkina. Yhdyskäytävän ohjelmistoa tukee myös se, että IoT-laitteen tarkalla mallilla ei ole väliä, vaan kaikkia voidaan suojata, kunhan ne vain viestivät yhdyskäytävän kautta.

Kodin IoT-laitteisiin kohdistuu erilaisten hyökkäysten uhkia. Keskeisimpiä näistä ovat fyysiset, verkon kautta tapahtuvat ja ohjelmistohyökkäykset. Fyysisissä hyökkäyksissä hyökkääjällä on fyysinen pääsy laitteelle. Sen myötä laitteen toimintaa voidaan häiritä esimerkiksi sulkemalla se. Verkon kautta tapahtuvissa hyökkäyksissä voidaan tarkkailla liikennettä, tai aktiivisesti häiritä laitteiden toimintaa. Tärkein ryhmä ovat ohjelmistohyökkäykset. Niissä laitteiden tietoturva-aukkoja hyödyntämällä pyritään asentamaan haitallista ohjelmistoa.

Tietoturvan muodostuminen vaatii, että taustalla on teoriaa sopivista suojautumiskeinoista. Turvallisuus jää kuitenkin puuttumaan, jos sen toteutumiseen ei panosteta käytännössä. Suurin tekijä kodin IoT-laitteen turvallisuudessa on sen valmistaja. Hyvän tietoturvan kannalta olisi tärkeää, että tietoturva suunnitellaan ohjelmistokehityksessä, mutta erillisenä osana.

Valmistajan lisäksi tietoturvasta huolehtii muita tahoja, esimerkiksi lainsäädäntö ja organisaatiot kuten EU. Lainsäädännön kohdalla ongelmaksi muodostuu IoT-laitteiden uutuus. Kaikkiin seikkoihin ei ole ehditty tehdä määräyksiä, joten usein joudutaan luottamaan, että valmistaja on hyväntahtoinen ja tietoturvasta on huolehdittu. Näin ei aina ole, vaan toisinaan valmistuksessa kiiruhdetaan liikaa, tai muista syistä suojaukseen on jäänyt aukkoja.

Lähteet

Antonakakis, Manos, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric ym. 2017. "Understanding the Mirai Botnet". Teoksessa *26th USENIX Security Symposium (USENIX Security 17),* 1093–1110. Vancouver, BC: USENIX Association, elokuu. ISBN: 978-1-931971-40-9. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

Augusto-Gonzalez, J., A. Collen, S. Evangelatos, M. Anagnostopoulos, G. Spathoulas, K. M. Giannoutakis, K. Votis ym. 2019. "From Internet of Threats to Internet of Things: A Cyber Security Architecture for Smart Homes". Teoksessa *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD),* 1–6. https://doi.org/10.1109/CAMAD.2019.8858493.

Babar, Sachin, Antonietta Stango, Neeli Prasad, Jaydip Sen ja Ramjee Prasad. 2011. "Proposed embedded security framework for Internet of Things (IoT)". Teoksessa *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE),* 1–5. https://doi.org/10.1109/WIRELESSVITAE.2011.5940923.

Bandekar, Ashutosh, ja Ahmad Y Javaid. 2017. "Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices". Teoksessa *2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER),* 1631–1636. https://doi.org/10.1109/CYBER.2017.8446380.

Boyes, Hugh, ja Tim Watson. 2019. "Towards a secure and resilient IoT architecture for smart home energy management". Teoksessa *Living in the Internet of Things (IoT 2019),* 1–7. https://doi.org/10.1049/cp.2019.0161.

Carrozzo, G., M. Pardi, P. Tedeschi, G. Piro, M. Dobski, K. Leszczyski, A. Carminati ja M. Di Fraia. 2018. "Interoperation of IoT Platforms in Confined Smart Spaces: The SymbIoTe Smart Space Architecture". Teoksessa *2018 Fifth International Conference on Internet of Things: Systems, Management and Security,* 38–45. https://doi.org/10.1109/IoTSMS.2018.8554894.

Han, Jin-Hee, YongSung Jeon ja JeongNyeo Kim. 2015. “Security considerations for secure and trustworthy smart home system in the IoT environment”. Teoksessa *2015 International Conference on Information and Communication Technology Convergence (ICTC),* 1116–1118. https://doi.org/10.1109/ICTC.2015.7354752.

Heriadi, Herman, ja Geraldi Catur Pamuji. 2020. “Cyber Security in IoT communication (Internet of Things) on Smart Home”. Teoksessa *IOP Conference Series: Materials Science and Engineering,* 879:012043. 1. IOP Publishing. https://doi.org/10.1088/1757-899X/879/1/012043.

Hernández-Serrano, Juan, Jose L. Muñoz, Olga León, Lars Mikkelsen, Hans-Peter Schwefel ja Arne Bröring. 2018. “Privacy risk analysis in the IoT domain”. Teoksessa *2018 Global Internet of Things Summit (GIoTS),* 1–6. https://doi.org/10.1109/GIOTS.2018.8534534.

Rawlinson, Kristi. 2014. “HP study reveals 70 percent of internet of things devices vulnerable to attack”. Viitattu 10. maaliskuuta 2022. https://www.hp.com/us-en/hp-news/press-release.html?id=1744676.