OULUN AMMATTIKORKEAKOULU

Tekijä

Timi Myllyaho

IOT-LAITTEET KOTONA JA NIIDEN TIETOTURVA

IOT-LAITTEET KOTONA JA NIIDEN TIETOTURVA

Timi Myllyaho
Opinnäytetyö
Kevät 2020
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittely, järjestelmäasiantuntemus

Tekijä: Timi Myllyaho
Opinnäytetyön nimi: IoT-laitteet kotona ja niiden tietoturva
Työn ohjaaja: Ritva Virkkala
Työn valmistumislukukausi ja -vuosi: Kevät 2020 Sivumäärä: 39

Opinnäytetyössä käsitellään IoT-laitteita kotiolosuhteissa ja niihin liittyviä tietoturvaongelmia. IoT eli Internet of Things tarkoittaa internetin tuomista uudenlaisiin ympäristöihin ja laitteisiin. Idea opinnäytetyöhön tuli IoT-laitteiden räjähdysmäisestä suosion kasvusta ja monesti puutteellisista tietoturvakäytänteistä. Opinnäytetyössä perehdytään IoT:n historiaan ja kuinka se on vähitellen viime vuosina vakiinnuttanut paikkansa markkinoilla ja ihmisten kotona. Työssä selvitetään IoT:n käyttämät yleisimmät tekniikat ja mihin suuntaan IoT on lähitulevaisuudessa kehittymässä. Lopuksi tutkitaan, kuinka ihmiset voivat suojautua jatkuvasti kehittyviä verkkouhkia vastaan. Aineistona työssä käytettiin kirja- ja artikkelilähteitä.

Opinnäytetyön perusteella tietoturva on monesti unohdettu laitteista, sillä nykyteollisuudessa laitemäärä ajaa usein tietoturvan edelle. Uusia laitteita pusketaan markkinoille niin nopeasti, että tietoturvan merkitys unohdetaan. Sittemmin tietoturvaan on alettu panostamaan enemmän muun muassa joidenkin maiden ja järjestöjen taholta. Hakkerit keskittyvät laitteisiin, joiden tietoturva on puutteellista. Siitä syystä IoT-laitteisiin kohdistetaan paljon tietoturvaiskuja. IoT-laitteiden tietoturvan ollessa puutteellista, korostuu käyttäjien tekemät teot sen parantamiseksi. Kotona tehtävät tietoturvaparannukset ovat tärkeitä ja niillä voidaan tehdä hakkerin työstä paljon hankalampaa.

Johtopäätöksenä voidaan pitää tietoturvaa koskevia puutteita ja kuinka ihmiset voivat pienillä, mutta merkittävillä teoillaan tehdä laitteista turvallisempia käyttää. Työssä esiintyviä toimenpiteitä voidaan suositella kaikille, jotka käyttävät IoT-laitteita kotonaan.

Asiasanat: IoT, esineiden internet, tietoturva, kyberturvallisuus, verkkohyökkäykset

ABSTRACT

Oulu University of Applied Sciences
Business Information Systems, Computer Systems Expertise

Author: Timi Myllyaho
Title of thesis: Security of IoT Devices at Home
Supervisor: Ritva Virkkala
Term and year when the thesis was submitted: Spring 2020 Number of pages: 39

This thesis focuses on IoT devices at home and their state of security. The idea for the thesis came from the rapid growth of IoT devices and from a concern regarding their insufficient security. The thesis introduces the history of IoT devices and how they took their place in the market and at homes. The thesis identifies the most common security techniques IoT devices are using, and how the IoT is going to develop in the future. Furthermore, this thesis covers some methods with which normal users could be protected against vulnerabilities from the IoT. The source materials for this thesis were books and online articles.

The results in this thesis show how security is often ignored due to the hectic nature of the markets. New devices are launched so quickly that companies neglect the importance of security. Currently companies are paying more attention to security, and some countries and organizations are focusing more on security aspects. The main targets for hackers are weakly protected devices, like some IoT devices, and this is the main reason why IoT devices receive so many malicious attacks. If security with these devices is insufficient, there are many steps that can be taken to improve it at home. With these steps taken, malicious acts by possible hackers would be made much more difficult, or even impossible.

In conclusion, many IoT devices have insufficient security, but with some steps taken by the users, these security vulnerabilities can be reduced or completely averted. The helpful steps that are presented in this thesis can be recommended to anyone who has an IoT device at home.

Keywords: IoT, Internet of Things, computer security, data security, hacking

SISÄLLYS

KÄYTETYT LYHENTEET (SANASTO)

5G	Viidennen sukupolven mobiilidatayhteys.
Arduino	Yhden piirilevyn mikrokontrolleri.
Blockchain	Alun perin Bitcoinia varten suunniteltu lohkoketjuista muodostuva tietokanta.
Bluetooth	Radiotekniikkaan perustuva langaton tiedonsiirtojärjestelmä.
DDoS	Hajautettu palvelunestohyökkäys.
Honeypot	Keinotekoinen ansa, jolla houkutellaan verkkorikollisia tekemään tietoturvaan kohdistuvia iskuja.
IoT	Internet of Things eli esineiden internet tarkoittaa internetin tuomista erilaisiin laitteisiin.
IP-osoite	Yksilöllinen osoite, jolla laite kommunikoi internetissä muiden laitteiden kanssa.
Käyttölaite	Elektroninen tai mekaaninen laite, joka suorittaa erilaisia fyysisiä toimintoja perustuen sen tulkitsemaan koodiin.
M2M	Machine-to-Machine tarkoittaa useiden laitteiden kommunikointia keskenään internetissä.
Massive MIMO	Usean antennin mahdollistava yhtäaikainen lähettämä ja vastaanottama tekniikka.
NFC	Radioaalloilla toimiva tekniikka, jolla lähekkäin olevat laitteet voivat siirtää dataa keskenään.
Pilvi	Internetissä sijaitseva palvelin/palvelinjoukko, jossa tietoa säilytetään.
Raspberry Pi	Yhden piirilevyn tietokone.
RFID	Radioaalloilla toimiva langaton tekniikka, joka käyttää hyväkseen tägejä.
Sensori	Pienikokoinen anturi, joka havainnoi erilaisia ulkoisia ärsykkeitä.
Wi-Fi	Langaton internet-verkko.

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on perehtyä esineiden internetiin eli IoT:iin (Internet of Things) kotiolosuhteissa. Nimensä mukaisesti internet on tullut useisiin laitteisiin niin kotona kuin sen ulkopuolellakin. Sen räjähdysmäinen kasvu tuo mukanaan paljon haasteita, joista iso osa liittyy tietoturvaan ja sen puutteisiin. Nykyteollisuudessa mennään niin sanotusti laitemäärä edellä tietoturvan tullessa vasta toisena. (McClelland 2020.)

Pohjustuksena IoT-laitteisiin ja tietoturvaan tulen käsittelemään IoT:n historiaa ja kuinka se pikkuhiljaa kehittyi ja levittäytyi yhä useamman kotiin ja työpaikkaan. Opinnäytetyön kohteena on syventyä uusien älylaitteiden tuomiin tietoturvaongelmiin. Tärkeimpinä kohteina ovat erilaiset tietoturvahyökkäykset ja niiltä suojautuminen. Iskujen määrä on kasvanut eksponentiaalisesti. Määrä moninkertaistuu vuosi toisensa jälkeen ja iskut tulevat yhä useammasta lähteestä. (Kaspersky 2020.)

Tärkeänä osana työtä ovat tavat, joilla erilaisia iskuja voitaisiin välttää ja vähentää. Tapoja, joilla voimme suojautua on monia. Tärkeintä on pitää huolta omista fyysisistä laitteista, joilla IoT-laitteita ohjataan, kuten älypuhelimista. (Norton 2020).

Opinnäytetyö käsittelee IoT-laitteiden käyttämiä tekniikoita ja kuinka ne tulevat tulevaisuudessa kehittymään. Kaikki tekniikat pitävät sisällään haasteita myös tietoturvan puolella.

2 IOT YLEISESTI JA SEN HISTORIA

IoT on käsitteenä laaja. Yleisesti sen voi määritellä isoksi joukoksi laitteita, jotka ovat yhteydessä internetiin ja voivat keskustella keskenään. Laite voi olla mitä tahansa hehkulampusta kodin turvaratkaisuihin. Laitteiden kirjo näyttää olevan lähes rajaton. (Gilchrist 2017, 5.)

IoT-laitteilla on kyky oppia tuntemaan käyttäjänsä ja käyttöympäristönsä. Osa näistä tiedoista voi olla henkilökohtaisia ja ne voidaan jakaa laitevalmistajien ja kolmansien osapuolien kanssa. Tämän kaiken toteuttamiseen laitteet tarvitsevat internet- tai Bluetooth-yhteyden tiedon jakamiseen käyttäjiltä palvelimille, joista laitteet hakevat tietonsa. (Ren ym. 2019.)

IoT-laitteet kätkevät yleensä sisälleen sensoreita, kameroita ja mikrofoneja, joilla ne aistivat ympäristöä sekä tulkitsevat erilaisia tapahtumia. Laitteiden sisään asennetut sensorit ja käyttölaitteet toimivat IoT-laitteiden aivoina. Sensori on pieni elektroninen komponentti, joka on tehty aistimaan erilaisia ulkoisia ärsykkeitä, kuten valoa, ääntä, ilmankosteutta, painetta, lämpötilaa, kiihtyvyyttä ja GPS-koordinaatteja. Esimerkiksi nykyiset älypuhelimet ovat täynnä erilaisia sensoreita. (Pathak & Bhandari 2018, 29.)

Käyttölaite (Actuator) on elektroninen tai mekaaninen laite, joka suorittaa toiminnan tai liikkeen (vedon, työnnön tai kierron). Ledit, moottorit ja kaiuttimet ovat esimerkkejä käyttölaitteesta. Sensorit ja käyttölaitteet ovat kuin vastakohdat toisilleen. Sensorit muuttavat fyysisen reaktion sähköiseksi signaaliksi, kun taas käyttölaite tekee sen päinvastoin eli muuttaa sähköisen signaalin fyysiseksi tapahtumaksi. IoT-laitteiden toimintaperiaate perustuu siis hyvin pitkälti näiden kahden eri komponentin toimintoihin. Ne voivat olla sisäänrakennettuja tai jälkeenpäin asennettuja. (Pathak & Bhandari 2018, 29.)

IoT-termin keksi alun perin Kevin Ashton -niminen henkilö vuonna 1999. Hänen aikomuksenaan silloin oli markkinoida RFID-tekniikka (Radio Frequency Identification) omassa esityksessään. Esityksen nimi oli Internet of Things. Myöhemmin termin käyttö on yleistynyt muun muassa Googlen ansiosta. Vuonna 2010 tuli selville, että Googlen käyttämässään Street View -palvelussa se varastoi informaatiota ihmisten Wi-Fi-verkkoihin. Tämä johti keskusteluihin siitä, että Google olisi yrittänyt indeksoida koko internetin ja maailman omaan käyttöönsä. (Lueth 2014.)

Vuonna 2005 ilmestyi Arduino, joka on yhden piirilevyn mikrokontrolleri. Arduino suunniteltiin alun perin oppilaskäyttöön. Tavoitteena oli, että kaikki osaisivat käyttää sitä, vaikka ei omaisi minkäänlaista teknistä pohjaa. Heti levittyään laajempaan käyttöön Arduino alkoi mukautumaan erilaisiin IoT-projekteihin. Laite on suunniteltu niin, että siihen on helppo kytkeä erilaisia sensoreita ja käyttölaitteita, joilla se aistii ympäristöään ja tekee ohjelmoituja käskyjä niiden mukaan. Arduinon etuja ovat halpa hinta, yksinkertainen ohjelmointiliittymä, avoin lähdekoodi sekä järjestelmäriippumattomuus, minkä ansiosta sitä voi ajaa Windowsilla, Macilla tai Linuxilla. (Arduino 2020.)

2000-luvun ensimmäisen vuosikymmenen loppupuolella IoT alkoi yleistymään nopeasti. Ciscon mukaan vuosina 2008-09 oli enemmän internetiin kytkettyjä laitteita kuin maailmassa oli ihmisiä. Vuonna 2010 internetiin kytkettyjä laitteita oli noin 12,5 miljardia, mikä teki silloiseen ihmismäärään suhteutettuna noin 1,84 laitetta/henkilö. Samoihin aikoihin Kiina oli vasta aloittelemassa investointejaan IoT-järjestelmiin. 2011 lanseerattiin IPV6-protokolla, jolloin uusia IP-osoitteita saatiin valtava ja lähes loputon määrä käyttöön. Tarkalleen ottaen 128-bittisessä IPV6-verkossa voi olla noin 340 sekstiljoonaa osoitetta. (Postscapes 2019.)

Vuonna 2012 ICT-alan tutkimus- ja konsultointiyritys Gartner julkisti heidän vuosikatsauksessaan IoT:n mullistavan maailman muutaman vuoden sisällä. IoT tulisi laajentumaan pois älypuhelimista ja tableteista lukemattomiin muihin laitteisiin ja kohteisiin. Myös NFC (Near Field Communication) oli vahvasti asialistalla. Alettiin panostamaan siihen, että maksaminen, julkinen liikenne ja terveydenhuolto hyötyisi NFC:n tuomista hyödyistä. (Postscapes 2019.)

Vuonna 2012 ilmestyi Raspberry Pi. Tämä minikokoinen yhden piirilevyn tietokone piti sisällään prosessorin, keskusmuistin eli RAM:n, grafiikkapiirin sekä erilaisia liitäntöjä, joihin sai kytkettyä hiiren, näppäimistön ja näytön. Lataaminen onnistui matkapuhelimen laturilla. Internetyhteys saatiin kaapelia käyttäen (RJ45). Raspberry Pi kohdennettiin aluksi oppilaskäyttöön ja elektroniikkaharrastelijoille. Se piti sisällään ohjeita erilaisten projektien rakentamiseen. Raspberryn julkaisi voittoa tavoittelematon organisaatio Englannista. (Pathak & Bhandari 2018, 30-32.)

Raspberry Pi:n valttina olivat sen halpa hinta (vain 35 dollaria) sekä kehittynyt järjestelmäpiiri. Koska se oli myös varustettu Ethernet-portilla ja monilla USB-liitännöillä, monet alan harrastajat ottivat sen nopeasti käyttöön omissa pienprojekteissaan. Raspberry Pi ei pidä sisällään sensoreita tai käyttölaitteita (actuator). Sen sijaan siinä on sisäänrakennettuna niin sanotut GPIO-pinnit, jotka

mahdollistavat ulkoisten sensorien tai laitteiden kytkemisen. Käyttöjärjestelmä Raspberryyn asennetaan siihen liitettävään erilliseen Micro SD -korttiin. (Pathak & Bhandari 2018, 30-32.)

Tämän jälkeen useat isot laitevalmistajat alkoivat huomata IoT:n tarjoaman potentiaalin. Mahtiyritykset, kuten Apple, Samsung, Google, Cisco ja General Motors alkoivat panostamaan enemmän IoT-sensoreihin ja laitteisiin. Skaala on iso aina älylaseista itseohjaaviin autoihin. Logistiikka, terveydenhuolto, öljy ja energia, maatalous, myynti ja monet muut alkoivat käyttämään internetiä hyväkseen omissa innovaatioissaan niin yksityisellä kuin julkisella sektorilla. (Khvoynitskaya 2019.)

2.1 IoT-laitteiden käyttämät tekniikat

Vuoteen 2020 tullessa IoT:sta on kasvanut miljardibisnes. IoT Analytics -sivuston mukaan vuoden 2019 lopussa oli noin 9,5 miljardia yhdistettyä IoT-laitetta. Sivusto listaa kolme isointa syytä hurjaan kasvuun. (Lueth 2020.)

- Räjähdysmäinen kasvu älykotilaitteissa.
- Parantuneet matkapuhelin -ja M2M-liittymät.
- Laitemäärän kasvu Kiinassa.

2.1.1 5G

5G-verkko on langattomien yhteyksien viimeisin iso mullistus. Se on yleistynyt 2010-luvun loppupuolella, mutta ei edelleenkään ole käytössä kuin muutamissa maissa. On ennustettu, että vuoteen 2023 mennessä 5G-yhteyksiä on noin 10 prosenttia maailman mobiiliyhteyksistä. (Fisher 2020.)

5G mahdollistaa 4G:tä huomattavasti nopeamman tiedonsiirron. Sen radiotaajuus voi olla noin 28 GHz kun 4G:llä se on väliltä 700 MHz – 2500 MHz. Samalla myös viive pienenee, joten laitteiden suorittamat käskyt nopeutuvat. Viive 4G:ssä on noin 20-30 ms, kun taas 5G:ssä se voi olla parhaimmillaan jopa 1 ms. (Vella 2019.)

5G käyttää hyväkseen millimetriaaltoja, joiden aallon pituus on lyhyt, joten sillä voidaan saavuttaa suuria nopeuksia pienellä säteellä. Kun matka pitenee, millimetriaallon teho heikkenee. Toisekseen sen heikkouksia ovat fyysiset esteen, kuten rakennukset ja niiden seinämät. Tämän takia tukiasemia täytyy olla tiheämmässä verrattuna 4G-verkkoon, jotta 5G-nopeudet pääsisivät huippunopeuksiinsa. 5G ei kuitenkaan käytä pelkästään uusinta millimetriaalto-tekniikkaansa vaan sen tukena ovat vanhemmat tekniikat pidemmillä radioaalloilla, jolloin laitteet käyttävät sen hetkistä tekniikkaa, mikä on nopein. (Heinzman 2019.)

5G käyttää toistakin uutta tekniikkaa nimeltään Massive MIMO (Multiple Input Multiple Output). Siinä langaton verkko käyttää useita antenneja lähettämään ja vastaanottamaan dataa yhtä aikaa useilta päätelaitteilta käyttäen samaa kanavaa. Useat antennit tekevät myös Massive MIMO – verkosta luotettavamman ja häiriövapaamman. (Mundy & Thomas 2019.) Apunaan se käyttää Beamforming-tekniikkaa eli keilanmuodostusta, jolla antennit voivat seurata käyttäjää ja laitteita taatakseen parhaan mahdollisen nopeuden ja viiveen (Villa 2019).

2.1.2 Koneoppiminen eli Machine Learning

Koneoppiminen on nykypäivänä mukana kaikessa, itseohjaavista autoista Applen tuottamaan Siri-puheentunnistuspalveluun. Koneoppimisen avulla voidaan saada tärkeää tietoa esimerkiksi asiakkaiden käytöksestä ostotilanteissa ja niihin johtaneista teoista. Tämän toteutumiseen tarvitaan iso määrä sensoreita, jotka luovat ison kokonaisuuden. Tätä kaikkea dataa IoT pyrkii hyödyntämään. (Lea 2018, 390-391.)

Koneoppimisen perimmäinen ajatus on matkia ihmisen aivoja päätöksenteon yhteydessä. Ihmiset tekevät päätöksensä oppimisen, harjoittelun ja kokemuksen kautta, kun taas koneet tarvitsevat siihen algoritmin. Isoin haaste koneoppimisessa on se, että miten kone voidaan ohjelmoida mukautumaan vaihtuviin olosuhteisiin. Oppiakseen paremmaksi, kone tarvitsee dataa käsiteltäväkseen. Mitä enemmän dataa se käsittelee, sen paremmaksi sen antama palaute kehittyy. (Robertson 2019.)

Esimerkkinä koneoppimisesta voidaan käyttää uusien autojen sensoreita. Niissä on valtava määrä erilaisia sensoreita, jotka havainnoivat ympäristöään estääkseen onnettomuuksia ja tehdäkseen

ajamisesta helpompaa. Auton keskustietokone voi oppia myös kuljettajan tekemistä virheistä tai vaarallisesta ajotavasta, jolloin se tarvittaessa kytkee päälle turvamekanismeja turvatakseen kuljettajan. (Robertson 2019.)

2.1.3 Syväoppiminen eli Deep Learning

IoT-laitteet tuottavat valtavan määrän erilaista dataa. Syväoppimisen tarkoituksena on purkaa dataa ja muuttaa se käyttäjälle ymmärrettäväksi materiaaliksi. Syväoppimisen isoin etu pätee erityisesti vaikeisiin olosuhteisiin, mutta sitä voidaan hyödyntää myös kotiympäristössä. Syväoppimisella on tärkeä rooli muun muassa kuvan tunnistuksessa ja kieliteknologiassa eli luonnollisen kielen käsittelyssä (Natural Language Processing). Sen tarkoituksena on parantaa tietokoneita ymmärtämään ihmisten käyttämiä eri kieliä (Garbade 2018). Syväoppiminen on tärkeä työkalu valtavien datamäärien käsittelyyn. Se on kehitelty parantamaan normaalin koneoppimisen puutteet. Tavallisen koneoppimisen ongelma on, ettei se osaa oppia ympäristöstään vaikeissa ja äänekkäissä olosuhteissa. Tähän ongelmaan on haettu ratkaisua syväoppimisen kautta. (Li & Ota & Dong 2018.)

2.1.4 Reunalaskenta eli Edge Computing

Kasvavien datamäärien käsittelemiseksi tarvitaan tekniikoita, jotta nykyinen pilvikapasiteetti ei ylikuormitu. Vaikka suurin osa liikenteestä sujuu hyvin pilvipalveluiden kautta, kasvavat datamäärät voivat silti aiheuttaa ongelmia viiveen ja suorituskyvyn kanssa. Näitä ongelmia estääkseen on kehitelty reunalaskenta, jossa prosessointi tapahtuu lähellä datan lähdettä, jolloin sitä ei tarvitse lähettää erikseen pilveen tai erimerkiksi erilliselle palvelimelle. Ylimääräisen datan siirron sijaan voidaan keskittyä laitteen nopeuden ja datan käsittelyn parantamiseen. (Premsankar & Di Francesco & Taleb 2018, 1)

5G-verkkojen yleistyminen helpottaa reunalaskennan käyttöönottoa. Erityisesti matala viive ja nopeat ja luotettavat yhteydet helpottavat suurien datamäärien käsittelyä. (Premsankar & Di Francesco & Taleb 2018, 4)

Cisco esitteli vuonna 2014 Fog Computing -termin, jonka on tarkoitus toimia ikään kuin ponnahduslautana reunalaskentaan. Nimensä mukaisesti eli usvana Fog Computing toimii pilven ja päätelaitteiden välissä. Edge ja Fog Computing -tekniikoiden voidaan ajatella olevan sama asia, mutta tosiasiassa Edge Computing -tekniikkaa voidaan pitää käsitteenä ja Fog Computing -tekniikkaa standardina. Fog Computing-tekniikka tekee datan prosessoinnin lähiverkossa, kun taas Edge Computing tekee sen laitteessa tai sensorissa itsessään lähettämättä sitä mihinkään. (Linthicum 2019.)

Yleisesti yllä mainittuja tekniikoita käytetään teollisuudessa ja terveydenhuollossa, mutta niille löytyy tarvetta myös älykodeissa. Lukemattomat erilaiset laitteet monilta eri laitetoimittajilta saattavat tehdä laitteiden kytkennän ja hallinnan monimutkaiseksi, jolloin voi olla tarvetta Fog Computing -tekniikalle. Myös paljon laskentaa ja varastointitilaa vaativat laitteet, kuten esimerkiksi reaaliaikaiset videointijärjestelmät ovat lähes mahdoton toteuttaa ilman pilvipalvelun tai palvelimen apua. (Prabhu 2017.)

2.2 Tulevaisuus

IoT:n odotetaan yleistyvän tulevaisuudessa useissa käyttötarkoituksissa. Ihmisten elämä tulee olemaan yhä riippuvaisempaa internetistä ja siihen kytketyistä laitteista. Arvioiden mukaan IoT-laitteita tulee olemaan yli 75 miljardia kappaletta vuoteen 2025 mennessä. Erilaiset tekniikat ja järjestelmät sulautuvat yhä paremmin toisiinsa, mikä tekee helpompaa uusien laitteiden kytkennästä ja datan käsittelystä. (Alam 2018, 450.)

Tanweer Alam mainitsi seuraavia skenaarioita IoT:n tulevaisuudesta:

- Jopa 85-90% kaikesta IoT:iin liittyvästä datasta on pilvessä vuoteen 2023 mennessä.
- 85-90% kaikista informaatioteknologian yrityksistä tulee kohtaamaan jonkinlaisia ongelmia tietoturvan kanssa.
- 45-50% tietoverkoista kohtaa isoja ongelmia liiallisten datamäärien seurauksena.
- Yrityksillä tulee olemaan omat IoT-ympäristöt.
- Yhä suurempi osa tietoliikenteestä integroituu eli keskustelee keskenään. (Alam 2018, 452.)

On ennustettu, että IoT-laitteet tuottavat jopa 90 tsettabittiä (10^{21}) dataa vuoteen 2025 mennessä. Kaikki data käsitellään isoissa keskitetyissä ympäristöissä, joissa on valtava laskenta- ja varastointikapasiteetti. Näiden ympäristöjen ongelmaksi muodostuvat suurien datamäärien aiheuttama viiveen kasvu sekä herkkyys luonnonkatastrofeille ja hakkereiden iskuille. Muun muassa näiden ongelmien vuoksi datan käsittely siirtyy yhä enemmän päätelaitteiden lähelle. Fog Computingia ja tekoälyä tullaan hyödyntämään entistä enemmän tulevaisuudessa. (Rishi & Saluja 2019.)

Taloudellisesti IoT:sta kasvaa globaali biljoonabisnes. Vuoteen 2025 mennessä koko maailman markkinat voivat olla arviolta jopa 1,1 biljoonaa Yhdysvaltain dollaria. (Rishi & Saluja 2019.)

2.2.1 Satelliitit internetin perustana

Satelliittien rooli IoT-laitteissa muuttuu merkittäväksi lähitulevaisuudessa. Etenkin maatalous ja rahtiliikenteen seuranta helpottuu haja-asutusalueilla. Tutkijat ennustavat, että satelliitit tarjoavat internetyhteyden 24 miljoonalle laitteelle maailmanlaajuisesti vuoteen 2024 mennessä. Nykyinen matkapuhelinverkko kattaa vain noin 20% maapallon pinta-alasta, kun satelliiteilla kattavuus olisi 100%. Toimiakseen satelliitit tarvitsevat maalla sijaitsevan tukiaseman siirtääkseen tietoa päätelaitteiden välillä. Erityisesti lento- ja meriliikenne kokevat vaikeuksia, jolleivat ne ole tukiasemien kantoalueella. (FutureIoT 2019.)

Satelliitit eivät ole uusi keksintö matkapuhelinverkkokäytössä. Niiden keksimisen aikaan 1990-luvulla oli niiden käyttö kuitenkin kallista verrattuna nykyisiin satelliitteihin. Nykyisiä nanosatelliitteja voidaan tuottaa massatuotantona, mikä laskee valmistamiskustannuksia. Kustannuksia laskee myös nanosatelliittien pieni koko. Se voi vaihdella 1-10 kilon välillä, minkä ansiosta niitä voidaan laukaista isoja määriä kerrallaan. (Narayanasamy & Ahmad & Othman 2017, 2.) Nanosatelliitit lähetetään matalan Maan kiertoradalle, joka sijaitsee Maasta katsottuna noin 160-1000 km välisellä alueella. Nanosatelliittien käytännöllisyyttä lisää, ettei niiden tarvitse kulkea koko ajan päiväntasaajan myötäistä linjaa pitkin, vaan ne voivat vaihdella reittiään. Nanosatelliitit kulkevat noin 7,8 kilometriä sekunnissa ja kiertävät Maapallon noin 90 minuutissa. Koska nanosatelliitit liikkuvat nopeasti, ne eivät tarjoa kovinkaan hyvää kattavuutta televiestinnässä. Ongelmaa on pyritty ratkaisemaan lähettämällä satelliitteja avaruuteen iso määrä kerrallaan, jolloin ne kattavat isomman alueen. Tällaista satelliittien keskittymää kutsutaan konstellaatioksi. (European Space Agency ESA.)

Monet yritykset ovat ottaneet tavoitteekseen luoda toimiva ja kattava internet-infrastruktuuri avaruudesta käsin. SpaceX, Amazon, OneWeb ja Telesat ovat näistä esimerkkejä. Yhdessä nämä yritykset laukaisevat jopa yli 46000 satelliittia tulevien vuosien aikana, joista suurin osa SpaceX:n toimesta. (Sheetz & Petrova 2019.)

2.2.2 SpaceX

SpaceX:n perusti Elon Musk vuonna 2002. Yritys valmistaa avaruusraketteja ja satelliitteja, minkä lisäksi se vastaa niiden lähettämisestä avaruuteen. SpaceX on myös Starlink-projektin takana, jonka päämääränä on tarjota halpa internet sellaisille alueille, joissa sitä ei ole saatavilla. Projektin taustalla on lähettää jopa 12000 satelliittia matalan Maan kiertoradalle 550 kilometrin korkeuteen. Tulevaisuudessa satelliittien lukumäärä voi nousta jopa 30000:een. SpaceX:n satelliitit ovat pien-satelliitteja ja painavat noin 227 kiloa. Huhtikuussa 2020 Starlink-satelliitteja on avaruudessa 422 kappaletta. (Mann 2020.)

2.2.3 Wi-Fi 6

Wi-Fi 6 eli IEEE 802.11ax on Wi-Fi-verkkojen uusin standardi, joka on julkaistu vuonna 2019. Kuitenkin vielä huhtikuussa 2020 markkinoilla ei ole montakaan laitetta, jotka tukisivat Wi-Fi 6:n tarjoamia tekniikoita. Wi-Fi 6 -tekniikan yleistymistä jarruttaa myös reitittimien kallis hinta. (Hoffman 2020.)

Wi-Fi 6 tarjoaa jopa neljä kertaa nopeamman suoritustehon kuin vanha 802.11ac-tekniikka. Wi-Fi 6 kykenee toimimaan sekä 2.4GHz:n että 5GHz:n taajuuksilla, joten se tukee samanaikaisesti sekä vanhoja että uusia laitteita. (Aruba 2018.) Isoimpana uudistuksena Wi-Fi 6:ssa on OFDMA (Orthogonal Frequency Division Multiple Access), jossa useiden laitteiden lähettämää dataa voidaan käsitellä yhtä aikaa. OFDMA-tekniikassa langattoman verkon kanaville luodaan alikanavia, joita pitkin päätelaitteet lähettävät dataa. Päätelaitteiden lähettämä data pilkotaan osiin, jotka OFDMA yhdistää ja lähettää päätelaitteille samanaikaisesti. Vanha 802.11ac-tekniikka pystyy käsittelemään ainoastaan yhden päätelaitteen datan kerrallaan. (Network World 2018.)

Tulevaisuudessa OFDMA-tekniikasta on hyötyä myös IoT-laitteissa. Monet IoT-laitteet tarvitsevat vain vähän kaistanleveyttä, jolloin ne voivat samanaikaisesti kommunikoida OFDMA-tekniikan avulla. Tämä vähentää viivettä, jolle monet IoT-laitteet ovat herkkiä. (Network World 2018.)

3 IOT KOTONA

IoT on hiljalleen yleistynyt kodeissa ja työympäristöissä muutamien viime vuosien aikana. Laitteiden määrä on suuri ja internet löytyy nykyään lähes kaikkialta. Älykodin perimmäisenä ajatuksena on helpottaa ja parantaa elämänlaatua. Älykodin ohjaus tapahtuu useimmiten älypuhelinten ja mikrokontrollereiden avulla. Älypuhelimiin asennettavilla sovelluksilla voidaan ohjata koko kodin laitteistoa. (Domb 2019.)

Älykodin toimintaperiaate voidaan jakaa osiin:

- IoT on perustana älylaitteille, sillä se tarjoaa internetin ja etähallinnan, jota voidaan ohjata muun muassa puhelimilla.
- Sensorit ovat yhdistettynä älylaitteisiin. Sensorit ovat IoT-laitteiden aivot. Sensoreiden avulla voidaan tarkkailla kotia ja kodin laitteita, josta syntyy dataa. Tällainen laite voi olla esimerkiksi ilmastointilaite.
- Prosessori eli suoritin suorittaa sensoreiden keräämän datan.
- Data käsitellään ohjelmistorajapinnoissa (API), jossa ulkoiset sovellukset saavat oikeat tiedot käskyjen suorittamiseen.
- Käyttölaitteet (actuator) suorittavat saamansa käskyt teoiksi.
- Lähes kaikki tieto käsitellään pilvessä. Pilvi tarjoaa skaalautuvaa laskentatehoa, varastointitilaa ja sovelluksia. Ohjattavien sovellusten avulla kehitetään, huolletaan ja ohjataan IoT-laitteita mistä ja milloin tahansa. Käsitelty data säilytetään pilvessä tulevaisuutta varten. (Domb 2019.)

IoT-laitteiden tuottama datamäärä on niin valtava, ettei ihminen pysty sitä tulkitsemaan. Siitä syystä tieto käsitellään joko pilvessä tai itse laitteessa. IoT-laitteiden toimintaperiaate perustuu sääntöjen tulkitsemiseen, joita käyttäjällä on mahdollisuus luoda ja muokata. Sääntö muodostuu erilaisista tapahtumaketjuista ja kuvioista. Järjestelmä voi käsitellä ison määrän tapahtumia, suorittaa toimintoja, ohjata ja optimoida käskyjä reaaliajassa. Järjestelmä myös havaitsee ja analysoi poikkeavuudet ja häiriöt, joiden perusteella se luo uusia reagointimalleja. Uusien mallien perusteella voidaan luoda varoituksia tai jopa estää laitteen käyttö. (Domb 2019.)

3.1 Laitteiden kirjo

Älykoti on saanut 2010-luvulla isot mittasuhteet. Vuosikymmenen loppupuolella meidän saataville ovat tulleet muun muassa älypeilit, robotti-imurit, älyvalot, älykkäät lämmitys- ja ilmastointilaitteet, moottoroidut ikkunaverhot sekä automatiikalla toimivat ovet ja ikkunat (Mundle 2019). Kaiken lisäksi kodistamme löytyy yhä useammin älytelevisio ja tietokone sekä mahdollisesti pesukone ja jääkaappi, jotka ovat varustettuja internetillä. Näiden kaikkien laitteiden tarkoitus on helpottaa kodin askareita, parantaa turvallisuutta, säästää aikaa ja pienentää kodin sähkölaskua. (Domb 2019.)

3.2 Tietoturvan rooli

Vuonna 2011 julkistettiin Nest Learning Thermostat eli älylaite, joka oppii säätelemään kodin lämpötilaa käyttäjän vuorokausirytmien perusteella. Pari vuotta myöhemmin Google osti brändin 3,2 miljardilla eurolla. Heti tämän jälkeen useat yritykset halusivat alkaa tuottamaan omia älylaitteitaan. Kun IoT-laitteita alkoi vyörymään markkinoille, tietoturvaan ei juurikaan panostettu. Yrityksien ainoana tavoitteena oli saada laitteet mahdollisimman nopeasti markkinoille, vaikka niiden tietoturvassa saattoi olla puutteita. (Gupta 2019, 2-4.)

Toimintaohjeiden tekijät eivät pysyneet IoT-laitteiden kasvun perässä, eivätkä siksi voineet laatia tiukkoja laatu- ja turvallisuusohjeita. Tähän on tullut muutos vasta 2010-luvun loppupuolella, sillä virastot, kuten GSMA ja FTC (Federal Trade Commission) ovat alkaneet tiukentaa turvallisuus- ja yksityisyyssääntöjään. GSMA toimii globaalisti matkapuhelinoperaattoreiden edustajana ja FTC on Yhdysvaltain kauppakomissio. Vaikka turvallisuuteen on panostettu, IoT-laitteet kärsivät silti tietoturvaongelmista. Sen seurauksena tietoturva-ammattilaisten kysyntä on kasvanut. (Gupta 2019, 2-4.)

4 TIETOTURVA

Palo Alto Networks Unit 42 -tutkijatiimin mukaan jopa 98 prosenttia kaikesta IoT-laitteiden tuottamasta datasta on suojaamatonta. Tämän lisäksi yli puolet kaikista IoT-laitteista on vaarassa joutua keskivakavan tai erittäin vakavan tietoturvaiskun kohteeksi. Iso osa datasta on henkilökohtaista ja yksilöllistä, jota ei suojata millään tavalla. IoT-laitteiden elinkaari on pidempi kuin esimerkiksi puhelimella ja tietokoneella. IoT-laite voi olla käytössä 10-20 vuotta, jonka aikana se ei välttämättä saa lainkaan tietoturvapäivityksiä. Tällainen ongelma on erityisen vakava esimerkiksi terveydenhuollossa. Moni laite käyttää edelleen Windows 7 -käyttöjärjestelmää, jonka tuki päättyi 14.1.2020. Windows 7 -käyttöjärjestelmä ei saa enää tärkeitä tietoturvapäivityksiä, joten se on helppo kohde haittaohjelmille ja erilaisille tietoturvaiskuille. (O'Donnell 2020.)

4.1 Nykymalli

Vuonna 2020 esiintyy edelleen ongelmia tietoturvassa. Tietoisuus siitä lisää monen valtion ja yrityksen haluja tehdä enemmän töitä tietoturvan eteen. Esimerkiksi Ison-Britannian hallitus on jättänyt vuoden 2020 alussa lakiesityksen, jossa vaaditaan laitevalmistajia panostamaan IoT-laitteiden tietoturvaan. Tullessaan voimaan uusi laki koostuisi kolmesta eri kohdasta:

1. Kaikkien uusien IoT-laitteiden salasanojen tulee olla uniikkeja, eikä niitä voi palauttaa tehdasasetuksiin.
2. Laitetoimittajien täytyy ylläpitää asiakaspalvelua, johon kuluttajat voivat tehdä vikailmoituksia.
3. Laitetoimittajien täytyy ilmoittaa jokaiselle laitteelle päivämäärä, mihin asti ne tulevat saamaan tietoturvapäivityksiä. (O'Donnell 2020.)

Myös Yhdysvalloissa on tehty uusia lakimuutoksia. Kaliforniassa ja Oregonissa on tullut voimaan 1.1.2020 uusi laki, jossa laitevalmistajien on lisättävä IoT-laitteiden tietoturvaa. Kaliforniassa voimaan tullut laki vaatii laitevalmistajia lisäämään kaikkiin internet ja Bluetooth -laitteisiin "kohtuullinen" määrä tietoturvaa. Tietoturvaominaisuuksien tulee olla kullekin laitteelle sopivia. Esimerkiksi laitteen keräämät henkilökohtaiset tiedot tulee salata ja käsitellä luottamuksellisesti, eikä ulkopuolisen pidä päästä niihin käsiksi lainkaan. Kalifornian laissa on myös sama salasanavaatimus kuin

Ison-Britannian laissa. Kaikilla laitteilla täytyy olla yksilöllinen salasana. Laitteiden täytyy myös olla ohjelmoituja vaatimaan käyttäjältä uusi kirjautumisen todennusmenetelmä ennen ensimmäistä kirjautumista. Oregonin asettamassa laissa internetiin kytketyt laitteet on rajoitettu pääasiassa kotona käytettäviin henkilökohtaisiin laitteisiin. (Lyon & Taye 2020.)

IoT-laitteet kärsivät monesti laskentatehon puutteesta, joten niiden teho ei välttämättä riitä suorittamaan edes kevytkäyttöisiä tietoturvaohjelmia. Vaikka uusia lakeja onkin tullut tietoturvan lisäämiseksi, on laitteiden turvallisuus edelleen alkeellista. Näin ollen IoT-laitteet ovat oletettavasti tulevaisuudessakin haavoittuvaisia tietoturvaiskuille. Kehitys on kuitenkin menossa oikeaan suuntaan, sillä IoT:n tietoturvaongelmat on huomioitu joidenkin maiden lainsäädännössä. Turvallisuutta pitäisi kuitenkin lisätä muuallakin kuin itse laitteissa. Esimerkiksi internet-operaattoreiden pitäisi panostaa enemmän turvallisuuteen verkkotasolla. (Fernandez 2020.)

4.2 IoT-hyökkäysten historia

Ensimmäinen iso IoT-laitteisiin suunnattu hyökkäys tuli julkisuuteen heinäkuussa 2016. Hyökkäyksen nimi oli Mirai ja se hyödynsi bottiverkkoa (Botnet). Bottiverkko koostuu useista kaapatuista tietokoneista ja älylaitteista, joita ulkopuolinen hakkeri hallitsee. Yleensä käyttäjä ei edes huomaa, että hänen laitettaan käytetään muihin tarkoituksiin. Laajaa bottiverkkoa voidaan käyttää myös DDoS-hyökkäyksessä, johon myös Mirai keskittyi. (Fruhlinger 2018.) DDoS-hyökkäyksessä eli hajautetussa palvelunestohyökkäyksessä useat laitteet ruuhkauttavat palvelimen tai verkon aiheuttaakseen sen romahtamisen. Näin estetään jonkin tietyn internet-sivun tai palvelun käyttö. Kun hyökkäykset tulevat useista laitteista kerrallaan, sitä on mahdoton pysäyttää estämällä liikenne vain yhdestä lähteestä. Useiden lähteiden etsimiseen menee yleensä paljon aikaa ja resursseja. (Impreva 2020.)

Mirai pyrki hyödyntämään IoT-laitteissa olleita tietoturva-aukkoja. Mirai levitti itsestään monistuvaa matoa, joka lisääntyi samalla, kun se etsi ja saastutti haavoittuvaisia IoT-laitteita. Saastuneet laitteet olivat C&C (Command and Control) -palvelimen hallinnassa, jota hakkerit käyttivät bottiverkon luomiseen ja hallintaan. Mirai koostui kahdesta komponentista; replikaatio- ja hyökkäysmoduulista. Replikaatiomoduulin tarkoituksena oli kasvattaa bottiverkon kokoa niin suureksi kuin mahdollista. Tehdäkseen tämän, se käytti hyväkseen 64 tunnetuimman oletuskäyttäjätunnuksen ja -salasanan

yhdistelmää. Tarkoituksenaan Mirailla oli arvata laitteiden oikeat tunnukset ja salasanat, joka lopulta johti yli 600 000 IoT-laitteen kaappaamiseen. Haavoittuneiden laitteiden joukossa oli esimerkiksi kotireitittimiä ja valvontakameroita. (Cloudflare 2017.)

Syyskuussa 2016 Mirain ensimmäiseksi kohteeksi joutui tietoturvajournalisti Brian Krebs, jonka kotisivulle kohdistettiin DDoS-hyökkäys. Kyseinen hyökkäys on yksi historian laajimmista DDoS-hyökkäyksistä. Dataa liikkui tuntien ajan noin 600-700 miljoonaa bittiä sekunnissa, mikä silloin vastasi noin puolta prosenttia koko internetin kapasiteetista. (Storm 2017.)

Mirain toinen tekijä Paras Jha julkaisi 1.10.2016 Mirain lähdekoodin internetiin, jolloin kuka tahansa pystyi lataamaan ja muokkaamaan sitä. Tämän seurauksena IoT-laitteista koostuvat bottiverkot ovat yleistyneet. Mirain tietoturvaiskut vaikuttivat useaan maahan. Esimerkiksi Liberiassa Mirai onnistui kaatamaan osittain koko internetin. Saksassa yli 900 000 asiakasta joutui hyökkäyksen kohteeksi reitittimiin kohdistetun iskun myötä. (Storm 2017.)

Tietoturvaiskut ovat kasvaneet Mirain jälkeen. Tietoturvayhtiö Kaspersky raportoi omassa IoT-raportissaan hyökkäysten kasvaneen merkittävästi vuosien 2017-2019 aikana. Vuoden 2018 ensimmäisen puoliskon aikana yhtiö havaitsi 120 000 erilaista haittaohjelman muunnelmaa. Vuonna 2017 vastaava luku oli noin 30 000. Vuonna 2016 havaittiin vain noin 3000 erilaista haittaohjelmaa. (Kaspersky 2018.)

Tietoturvaiskujen määrä kokonaisuudessaan on paljon suurempi. Vuoden 2019 ensimmäisellä puoliskolla Kaspersky havaitsi yli 100 miljoonaa hyökkäystä 276 000 eri IP-osoitteesta, joiden kohteina olivat älylaitteet. Määrä on seitsemän kertaa enemmän kuin mitä vuonna 2017 rekisteröitiin koko vuoden aikana. Hyökkäykset olivat yleensä DDoS-hyökkäyksiä, jotka useasti pohjautuivat Miraihin. Hakkerit käyttivät myös brute-force -tekniikkaa eli väsytyshyökkäystä, jossa yritetään arvata oikeaa salasanaa niin kauan kunnes oikea löydetään. (Kaspersky 2019.)

Tietoturvayhtiöt käyttävät tietoturvauhkien havaitsemiseen Honeypot eli hunajapurkki -menetelmää. Hunajapurkki matkii normaalia tietokonetta tai palvelinta ja se on erillään muusta laiteympäristöstä. Hunajapurkki voidaan käyttää sekä tunnistamaan että torjumaan hyökkäyksiä. Hunajapurkkien keräämä tieto on tärkeää taistelussa hakkereita vastaan, sillä niiden avulla opitaan hyökkääjistä ja heidän käyttämistään tekniikoista. (The Defence Works 2019.)

Kasperskyn mukaan suurin tietoturvauhka on edelleen Mirai. Vuonna 2019 Kasperskyn hunajapurkkien tulosten perusteella Mirai-pohjaisia hyökkäyksiä oli 39 % kaikista heihin kohdistuneista iskuista. Nyadrop-nimistä hyökkäystä käytettiin 38,57 % tapauksista. Nyadrop käyttää brute-force -tekniikkaa. (Kaspersky 2019.)

Chain Reaction oli akateeminen tutkimus, jossa Philips Hue -älylamput otettiin hallintaan likiverkossa (PAN). Tutkimuksessa kohteina olivat sekä kotona että älykaupungeissa käytettävät älylamput. Hyökkäys tapahtui Philips Huen käyttämän Zigbee-protokollan avulla. Zigbee eli IEEE 802.15.4 on protokolla, joka mahdollistaa useiden pienten laitteiden liittämisen samaan likiverkkoon. (Lea 2018, 431.)

Hyökkäyksessä tutkijat pääsivät käsikseen yhteen Hue-lamppuun, johon asetettiin vahingollinen laiteohjelmisto. Ohjelmisto sääteli lampun kirkkautta ja väriä käyttäjän tietämättä. Saatuaan haltuunsa yhden lampun, onnistuivat tutkijat tämän jälkeen levittämään haittaohjelmiston koko verkkoympäristöön ja jopa oman lähiverkon ulkopuolelle. Murtautuminen tapahtui Huen käyttämän sillan avulla, jolla lamppuja ohjataan puhelimeen asennettavalla sovelluksella. Silta kytketään reitittimeen RJ45-verkkokaapelilla. Helmikuussa 2020 Philips korjasi päivityksessään tutkijoiden löytämän tietoturva-aukon. (Check Point 2020.)

4.3 Olemassa olevat uhat

Vuonna 2020 Mirai-pohjaisia bottiverkkoja käytetään edelleen tietoturvaiskuissa. Yksi monista on Echobot, joka käyttää hyväkseen samoja haavoittuvuuksia IoT-laitteissa kuin Mirai (Kreminchuker & Zavodchik 2019). DDoS-hyökkäysten lisäksi hakkerit käyttävät myös niin sanottua MITM (Man-in-the-middle) eli mies välissä -hyökkäystä. Hyökkäyksessä hakkeri toimii kahden osapuolen välissä lähettäen heille molemmille viestejä esittämällä koko ajan toista osapuolta. Molemmat osapuolet voivat olla täysin tietämättömiä, että he ovat vaihtaneet tietoja hakkerin kanssa. Tällaista MITM-hyökkäystä on käytetty esimerkiksi älyautojen ja älyjääkaappien kaappauksissa. (Simko 2016.)

Älylaitteiden tuottama ja käsittelemä data on ollut aina ongelma tietoturvan kannalta. Käyttäjä ei aina tiedä mitä dataa laite on kerännyt ja minne sitä on lähetetty. Osa laitteista ei tarjoa minkäänlaista asetusvalikkoa, josta käyttäjä voisi hallita yksityisyysasetuksia. Ongelma korostuu sitä mukaa, kun laitemäärät ja datavirrat kasvavat. Voidaankin pitää oletuksena, että tulevaisuudessa kaikki mahdollinen kerättävissä oleva data kerätään älylaitteiden toimesta. (Al-Turjman 2019, 135.)

Kyberturvallisuudessa on kolme tärkeää kohtaa, jotka määrittelevät datan käsittelyä.

- Confidentiality eli luottamuksellisuus on datan suojaamista ja, että vain valtuutetut osapuolet (myös koneet) voivat lukea dataa.
- Authentication eli todennus on datan todistamista käsittelemättömäksi hakkerin toimesta ja oikean lähettäjän varmistamista.
- Access eli käyttöoikeus tarkoittaa valtuutettujen henkilöiden oikeutta päästä käsiksi dataan ja resursseihin. (Lin 2016.)

Luottamuksellisuuden kautta hakkerit pääsevät käsikseen esimerkiksi kodin lämpötila-antureihin, jolloin tiedosta voidaan päätellä, onko talo asutettu vai ei. Tällainen tieto voi altistaa esimerkiksi murtovarkauksille. Todennusongelmat voivat koskea esimerkiksi kodin älylukkoja ja turvajärjestelmiä. Todentamattomat järjestelmän tilaa koskevat hälytykset voidaan tulkita talossa olevan hätätilan avaamalla ovet ja ikkunat hätäpoistumista varten. Todellisuudessa hakkerit ovat aukaisseet ovet päästäkseen taloon tai aiheuttaakseen ilkivaltaa. Käyttöoikeusuhissa hakkerit voivat päästä sisään järjestelmään järjestelmänvalvojan roolissa, joka altistaa lukemattomille haavoittuvuuksille. Hakkerit voivat halutessaan käyttää internetkaistaa ja laukaista esimerkiksi DoS-hyökkäyksen. (Lin 2016.)

4.4 Tulevaisuuden uhat

Kehittyvät internetyhteydet tuovat mukanaan lisää hyökkäyksiä ja haasteita. 5G-yhteydet mahdollistavat nopeammat yhteydet, joita IoT-laitteet tulevat hyödyntämään tulevaisuudessa. Uusi tekniikka tulee kohtaamaan haasteita tietoturvassa, sillä palveluntarjoajat ja laitevalmistajat eivät vielä tiedä, mitä riskejä 5G tuo mukanaan. Haasteita on myös 5G:n ja aikaisempien tekniikoiden eli 4G:n

ja 3G:n sovittaminen yhteen. Silloin kun 5G:tä ei ole saatavilla, laite käyttää toiseksi nopeinta yhteyttä. Erilaisissa testauksissa on todettu esiintyvän tietoturvaongelmia silloin, kun laite joutuu vaihtamaan pois nopeimmasta verkostaan. (Cortese 2020.)

Tulevaisuudessa useat jo olemassa olevat IoT-laitteet tulevat vanhentumaan tietoturvansa osalta. Nykyiset laitevalmistajat valmistavat lisää laitteita nykyisille ja tuleville markkinoille, mutta eivät samaan aikaan panosta vanhojen laitteiden tietoturvaan. Ongelmat koskevat niin laitteita kuin ohjelmistojakin. Vaarassa ovat käyttäjien lisäksi myös laitevalmistajat, sillä arkaluontoisten tietojen vuotaminen vaarantaa jokaisen yksityisyyden. (Shah 2019.)

Ennalta arvattavat tunnukset ja salasanat ovat vaarallinen yhdistelmä, joita moni laitevalmistaja käyttää edelleen oletuksena. Pelkästään tunnuksen tietäminen saattaa antaa hakkerille mahdollisuuden suorittaa brute-force -hyökkäys. Käyttäjien pitäisi itse vaihtaa tunnukset heti laitteen saatuaan, mutta tietämättömyys ja laitevalmistajien tarjoamat puutteelliset ohjeistukset vähentävät toimenpiteitä. Mirai on hyvä esimerkki oletustunnusten käytön vakavuudesta ja mihin se voi johtaa. (Shah 2019.)

4.5 Kenen vastuulla tietoturva on?

Laitevalmistajat kilpailevat aikaa ja toisiaan vastaan julkaisemalla uusia laitteita markkinoille vailla kunnollista tietoturvaa. Siitäkin huolimatta vastuun siirtäminen pelkästään heidän vastuulleen ei ole oikein. Asiakkaan täytyy miettiä omaa vastuutaan eikä luottaa pelkästään laitevalmistajiin. Asiakas ei välttämättä tiedä, mitä kaikkea dataa IoT-laite varastoi ja kelle kaikille sitä lähetetään. Datan suojaaminen on laitevalmistajan vastuulla, mutta asiakas voi parantaa laitteen tietoturvaa esimerkiksi vaihtamalla oletustunnukset. Asiakkaan täytyy ajatella dataa samalla tavalla kuin rahaa, sillä kauppiaat ja hakkerit ajattelevat juuri niin. (Outpost24 2020.)

Valtioilla on valta ja velvollisuus tehdä muutoksia lainsäädäntöihin, kuten Iso-Britannia ja Oregonin ja Kalifornian osavaltiot ovat tehneet. Muutoksella estetään muun muassa IoT-laitteiden käyttämät oletustunnukset. Tietoturvan tulevaisuuden kannalta tämä on merkittävä parannus, sillä IoT-laitteista jopa kolmannes käyttää heikkoja salasanoja. Eräässä tutkimuksessa on todettu ”123456” olevan maailman yleisin käytössä oleva salasana. (Proske 2019.)

4.6 Esimerkkejä haavoittuvaisista laitteista

Luettelo laitteista, jotka ovat erityisen haavoittuvaisia ja aiheuttavat vakavia yksityisyyden loukkaavia tietoturvaongelmia.

- Älyvalvontakamerat ovat aina olleet hakkereiden suosiossa. Muun muassa Mirai käytti hyväkseen valvontakameroita ja niiden heikkoja oletustunnuksia. Googlen Nest Hub ja Amazon Ring -ovikellokamerat ovat myös kohdanneet yksityisyystietovuotoja ja ongelmia laitteidensa turvallisuudessa. Molemmat yhtiöt ovat paikanneet tietoturva-aukot. (Ciso Mag 2020.)
- Älytelevisiot omaavat paljon riskejä yksityisyyteen liittyen. Älytelevisioissa on usein mikrofoni ja kamera, joiden avulla tekoäly tekee television katselemisesta yksilöllisempää. Niiden varjopuolena on kuitenkin datan siirtyminen kolmansille osapuolille, kuten mainostajille ja analytiikkayhtiöille. Datan hallitsematon jakelu lisää tietoturvavuotojen riskiä. (Moghaddam ym. 2019.) Tämän lisäksi hakkerit voivat kuunnella ja katsella ihmisiä heidän kotonaan, mikäli he ovat päässeet tunkeutumaan samaan verkkoon (Ciso Mag 2020).
- Älykellot ja aktiivisuusrannekkeet keräävät paljon henkilökohtaista dataa. Niin sanotut puettavat älylaitteet käyttävät GPS-sijaintipalveluja taatakseen parhaan käyttökokemuksen. Sijaintitiedot voivat olla vaarallisia joutuessaan hakkereiden tietoon. Älykelloja voidaan käyttää myös älylukkojen aukaisuun, jolloin itse laitteen varastetuksi tuleminen voi olla kohtalokasta. (Norton 2020.)
- Älykaiuttimet ohjaavat monia kotona käytettäviä laitteita puheentunnistuksen avulla. Kaiuttimet vastaavat ihmisten esittämiin kysymyksiin, ajastavat tapahtumia, soittavat musiikkia ja ne voidaan asettaa kontrolloimaan erilaisia kodin järjestelmiä, kuten ovien lukkoja ja valaistusta. (Park ym. 2019.) Sekä Amazonin käyttämässä Alexassa että Googlen Home -älykaiuttimissa on havaittu lukuisia haavoittuvuuksia ja ongelmia. Molemmat ovat kohdanneet tietojenkalastelua sekä salakuuntelua hakkereiden toimesta. Laitteet sallivat kolmansien osapuolien pääsyn käyttäjien tietoihin. Nämä kolmannet osapuolet tuottavat useasti palvelut, joilta puheentunnistuslaitteet hakevat tietonsa. (Security Research Labs 2019.)

5 KUINKA SUOJAUTUA?

Nykyaikaiset IoT-laitteet ovat suunniteltuja toimimaan mahdollisimman helposti ja nopeasti suoraan laatikosta purettuna. Tällainen toimintatapa näkyy yleensä huonosti suunnitellussa tietoturvassa tai sitä ei välttämättä ole lainkaan. (Gilchrist 2017, 49.)

IoT-laitteiden myötä tietoturvaiskut ovat muuttuneet entistä henkilökohtaisimmiksi. Ennen IoT:ia yleisin riski oli menettää rahansa tietoturvaiskussa. Sen sijaan IoT:iin kohdistuvat iskut voivat olla jopa ihmishenkeä uhkaavia. (Atlam & Wills 2019, 131.)

5.1 Mitä käyttäjä voi tehdä?

Käyttäjällä on vastuu suojata omat laitteensa ja ohjelmistonsa. Tärkeintä on suojata laitteet fyysisesti, mikäli on mahdollista, että joku ulkopuolinen pääsisi niihin käsiksi (Atlam & Wills 2019, 131). Käyttäjällä on monia muitakin mahdollisuuksia tehdä hakkerin työstä vaikeampaa. Alla lueteltu tehokkaimpia keinoja estää tietomurrot:

- Reitittimien oletustunnusta eli SSID:tä ja salasanaa ei saa käyttää ikinä. Oletussalasanan tilalle pitäisi keksiä tarpeeksi hyvä ja vahva salasana. Ongelmana kotona olevissa reitittimissä on se, että moni käyttäjä saattaa tietää oikeat tunnukset, kuten lapset ja heidän kaverinsa. Heidän kauttaan salasana voi tahtomattaan levitä väärille henkilöille, mikä taas altistaa verkon tietoturvaiskuille. Salasanasta kannattaa tehdä monimutkainen, sillä kerran verkkoon kytketyt laitteet eivät tietoturvasyistä näytä salasanaa. Harva muistaa ulkoa pitkiä ja monimutkaisia salasanoja. (Cooper 2020.)
- Kytkettyjen IoT-laitteiden oletustunnusten vaihtaminen. Yritysten pitäisi ohjelmoida laitteet vaatimaan tunnusten vaihtamista, mutta loppukädessä vastuu on käyttäjällä. (Atlam & Wills 2019, 131.)
- Vaikka salasana on kertaalleen vaihdettu turvalliseksi, se ei tarkoita, etteikö sitä tarvitsisi enää koskaan vaihtaa. Salasanan vaihtoväliin ei ole tiettyä sääntöä, mutta suosituksena on vaihtaa se säännöllisin väliajoin. (Cooper 2020.)

- Käyttäjällä on mahdollisuus luoda vierasverkko, jossa reititin luo oman yhteyspisteen ulkopuolisille käyttäjille. Kotona sijaitsevat älylaitteet toimivat edelleen omassa verkossaan, jolloin ne ovat suojassa mahdollisilta haittaohjelmilta, joita tulisi ulkopuolisten mukana. (Grustniy 2018.) On myös mahdollista luoda vierasverkko pelkästään IoT-laitteille, mikäli niitä on paljon. Tällä voidaan eristää tietoturvaiskuille haavoittuvaiset laitteet omasta kotiverkosta. (Cooper 2020.)
- IoT-laitteiden firmware eli ohjelmistopäivitykset täytyy olla ajan tasalla. Jos laitteita ei ole päivitetty pitkään aikaan, ne ovat helpommin murrettavissa hakkereiden toimesta. Tuoreimmat päivitykset ovat laitevalmistajan vastuulla ja yleensä niitä onkin saatavilla niin pitkään kuin tuotteen elinkaari on voimassa. Myös reitittimen ohjelmistopäivitys on tärkeää ladata aina, kun uusi versio ilmestyy. (Atlam & Wills 2019, 131.)
- Yksi tietoturvaa parantava esimerkki on UPnP (Universal Plug and Play) protokolla, joka auttaa laitteita löytämään verkon ja kommunikoimaan valmistajien kanssa, muun muassa päivitysten osalta. UPnP on tärkeänä osana IoT-laitteiden toimintaa, mutta samalla se voi avata väylän hakkereille päästä tunkeutumaan kotiverkkoon. Esimerkiksi Mirai käytti hyväkseen UPnP:ää. (Green 2020.)

IoT-laitteisiin olisi hyvä perehtyä ennen ostopäätöstä. Iso osa laitteista kerää jonkinlaista dataa, eivätkä kaikki käyttäjät ole tietoisia, mihin kaikkeen dataa käytetään. (Norton 2020.) Vaikka IoT-laite on kykeneväinen käyttämään internetiä, se ei tarkoita, että se täytyisi kytkeä internetiin. Jotkin laitteet toimivat hyvin ilman internetiä, joten voi olla perusteltua jättää laite kytkemättä internetiin. (Viswanathan 2019.)

Vastakohtana on olemassa laitteita, jotka vaativat internetyhteyttä jatkuvasti toimiakseen. Jotkin laitteet eivät välttämättä tuo elämään lisäarvoa, jolloin voi olla perusteltua lopettaa laitteen käyttö. Vanhoissa ja käyttämättömissä laitteissa voi myös piillä tietoturvariskejä, jos niissä ei ole uusimpia päivityksiä asennettuina. (Viswanathan 2019.)

5.2 Tekoäly suojautumiskeinona

Tekoälyn ja koneoppimisen käsittelemää dataa käytetään myös tietoturvan kehittämiseksi. Koneoppimista käytetään vanhojen haittaohjelmien tutkimiseen ja oppimiseen. Kun tietoa erilaisista

hyökkäyksistä on opittu, sitä voidaan hyödyntää tulevaisuudessa. Opitut hyökkäykset estetään välittömästi ennen kuin ne kerkeävät tekemään tuhojaan. (Palmer 2020.)

Tekoälypohjaista verkkomonitorointityökalua voidaan käyttää seuraamaan päivittäistä internetin käyttöä. Niiden tarkoituksena on analysoida liikennettä ja tunnistaa poikkeavuudet ja reagoida niihin välittömästi. Tällainen toimii esimerkiksi sähköpostien kautta leviävissä tietojenkalasteluviesteissä, jolloin järjestelmä huomaa poikkeavuuden ja varoittaa mahdollisesta uhasta. (Palmer 2020.)

Tekoälyä käytetään hakkereiden toimesta myös tietoturvaiskujen pohjana. Se toimii täysin päinvastaisesti kuin hyvää tarkoittava tekoäly. Tietoturvayritykset opettavat tekoälyään paremmaksi syöttämällä niille erilaista dataa, niin normaalia kuin epäilyttävääkin. Ongelmana on se, etteivät ne voi käsitellä oikeisiin henkilöihin perustuvaa arkaluontoista tietoa, koska on olemassa säännöksiä ja lakeja, joilla arkaa tietoa suojellaan. Vastaavasti hakkerit eivät välitä tällaisista laeista, vaan heidän käyttämänään tekoäly oppii paljon enemmän henkilökohtaisesta datasta, jolloin he voivat saada yliotteen. (Chester 2019.)

Tekoäly on tärkeänä osana IoT-laitteiden toimintaa. IoT-laitteet keräävät paljon tietoa ympäristöstä, kuten lämpötilaa, ilmanlaatua, värähtelyä ja ääniä. Tekoäly oppii tunnistamaan poikkeavat tapahtumat normaaleista, jolloin se varoittaa käyttäjää ja estää mahdollisen vaaratilanteen. Tekoälyn tekemät päätökset ovat jopa 20 kertaa nopeampia ja varmempia verrattuna perinteisiin tietovälineihin. (Schatsky & Kumar & Bumb 2017.)

5.3 Tulevaisuuden tekniikat

Lähes kaikki data, mikä nykypäivänä liikkuu yritysten ja käyttäjien välillä on tavalla tai toisella hakkereiden ja rikollisten saavutettavissa. Datan oikeellisuuden toteaminen on vaikeaa keskitetyssä ympäristössä (Reyna ym. 2018, 174). Keskitetty verkko tarkoittaa yleisintä käytössä olevaa mallia eli asiakas/palvelin -mallia, jossa asiakkaat lähettävät kyselyn palveluntarjoajan palvelimelle ja saavat sieltä vastauksen. Keskitetty verkko on altis erilaisille tietoturvaiskuille, sillä se on riippuvainen vakaasta internetyhteydestä. Koko verkkoympäristö voi kaatua, mikäli yksi palvelin lakkaa toimimasta. IoT-laitteiden turvallisuuden kannalta hajautettu verkko on turvallisempi, mutta sen käytössä on myös huonot puolensa, kuten sen monimutkainen hallinta ja viive datan kulussa. Hajautetussa

verkossa jokainen laite toimii omillaan, eivätkä ne nouda tietojaan ulkoiselta palvelimelta. (Seal 2020.)

5.3.1 Blockchain

Yksi tunnetuimmista hajautetun järjestelmän käyttäjistä on kryptovaluutta Bitcoin. Maksutapana kryptovaluutat poikkeavat kaikista muista maksutavoista. Bitcoin toimii täysin digitaalisesti ja globaalisti. Bitcoin ei tarvitse tuekseen kolmansia osapuolia, kuten pankkeja, vaan se toimii itsenäisesti Blockchain-tekniikan avulla. Blockchain perustuu datan suojelemiseen muuttumattomana koko sen elinkaaren ajan. Blockchainin luotettavuutta on käytetty hyväkseen Bitcoinin lisäksi muun muassa erilaisissa sähköisissä äänestyksissä. (Reyna ym. 2018, 174.)

Blockchainin toimivuus kryptovaluutoissa perustuu useiden toisilleen tuntemattomien käyttäjien ylläpitämiin ja vahvistamiin siirtoihin. Blockchain luo täysin muuttumattoman, läpinäkyvän, turvallisen ja jäljitettävän rekisterin eli tietokannan. Kun tapahtumat ovat kirjattu, niistä muodostuu lohkoja. Jokaiseen uuteen lohkoon sisältyy tieto edellisestä lohkosta, jolloin syntyy lohkoketju. Lohkoketjut ovat hajautettuna useille tietokoneille, joten lohkoissa olevia tietoja on mahdoton muokata jälkeenpäin jäämättä siitä kiinni. (Reyna ym. 2018, 174.)

Blockchain voi auttaa tulevaisuudessa IoT:ia parantamaan sen turvallisuutta ja käytettävyyttä. Laitteiden välillä liikkuva data olisi suojattu Blockchainin avulla, mikä tekisi datasta luotettavaa. Valtavia datamääriä ei enää hallitsisi isot yritykset, vaan se olisi hajautettu ympäri verkkoa. Blockchainin käyttäminen lisäisi yhden lisäkerroksen suojaukseen, joka tekisi tietoturvaiskuista lähes mahdotonta. Samalla Blockchain toimii läpinäkyvästi, mikä antaa kaikille oikeutetuille käyttäjille oikeuden päästä näkemään tapahtumahistoriaa. Tämän etuna on datavuotojen nopea ja luotettava paikantaminen. Yrityksille Blockchainin käyttö voisi tarkoittaa kulujen pienentymistä, sillä enää ei tarvitsisi ylläpitää isoja ja kalliita palvelimia. (Mahmood 2019, 98-99.)

5.3.2 Kvanttitietokoneet

Kvanttitietokoneet toimivat kvanttimekaniikalla. Kvanttitietokoneet käyttävät tavallisten bittien sijaan kubittejä. Tavallinen tietokone käyttää laskennassa ykkösiä tai nollia. Kvanttitietokoneen käyttämä kubitti voi sisältää ykkösen, nollan tai molemmat yhtä aikaa. Ykkösen ja nollan yhdistelmää kutsutaan superpositioksi. Superposition ansiosta kvanttitietokoneet voivat tehdä laskentoja miljoonia kertoja nopeammin kuin tavallinen tietokone. (Tegio 2019.)

Kvanttitietokoneiden mahdollistamilla nopeuksilla IoT-laitteet voisivat saada merkittävän hyödyn datan siirrossa. Data käsiteltäisiin nopeampaa ja se olisi nopeammin saatavilla. Arkaluonteisen datan siirto tapahtuisi myös tietoturvallisemmin, sillä kvanttitietokoneet mahdollistavat kvanttisalauksen. Kvanttisalaus käyttää hyväkseen algoritmeja, jotka tarvitsevat kvanttitietokoneiden laskentatehon. Salaustekniikan monimutkaisuus toimisi hyvin hakkereita vastaan. (Tegio 2019.)

Mikäli kvanttitietokoneet yleistyisivät kuluttajamarkkinoilla, se tarjoaisi mahdollisuuden myös hakkereille käyttää niiden ylivertaista laskentatehoa. Europol on varoittanut kvanttitietokoneiden päätymisestä vääriin käsiin. Päätyessään ensin hakkereille, heillä olisi mahdollisuus murtaa nykyiset salausjärjestelmät. (Palmer 2019.)

6 POHDINTA

Opinnäytetyön taustalla oli halu selvittää, kuinka IoT on kehittynyt ja mukautunut jokapäiväisiin askareihin kotiympäristössä. Taustalla olivat IoT:n puutteet tietoturvassa ja kuinka yritykset tietoisesti laiminlyövät sen merkitystä uusissa laitteissa ja vanhojen laitteiden päivityksissä. Tavoitteena oli tutkia IoT:n käyttämät tekniikat ja kuinka ne tulevat mahdollisesti kehittymään lähivuosina. Moni tekniikka tuo käyttäjälle apua, mutta niissä voi piillä myös tietoturvaongelmia. Työssä käsiteltiin tavalliseen käyttäjään kohdistuvia tietoturvaiskuja ja mitä käyttäjät voisivat tehdä kotiolosuhteissa toisin, jotta iskuja voitaisiin vähentää tai estää kokonaan.

Katsaus antoi selvän kuvan siitä, että laitteiden tietoturva on edelleen heikolla tasolla. Ongelman ydin on laitevalmistajissa, sillä he eivät panosta tarpeeksi tietoturvaan. Nykyisten markkinat perustuvat siihen, että laitemäärä pyritään maksimoimaan ja tietoturva jätetään usein toissijaiseksi (McClelland 2020). Tähän on kuitenkin alettu puuttumaan joissain maissa ja järjestöissä. Esimerkkinä työssä mainitut Iso-Britannia sekä Yhdysvaltojen osavaltiot Kalifornia ja Oregon, jotka ovat määränneet lakeja, joissa vaaditaan yrityksiä panostamaan tietoturvaan. Kehitystä on täten tapahtunut ja tällaiset teot motivoivat muitakin maita ja organisaatioita miettimään tietoturvan tärkeyttä.

IoT-laitteet ovat yleensä sellaisessa käytössä, ettei niitä muisteta päivittää, vaikka tärkeitä tietoturvapäivityksiä olisikin saatavilla. Esimerkiksi valvontakamerat voivat olla monta vuotta käytössä ilman, että niitä päivitetään lainkaan. Tällaiset käyttäjän tekemät virheet altistavat laitteet tietoturvaiskujen kohteiksi, eikä siitä voi syyttää ketään muuta kuin huolimatonta käyttäjää. Ehkäistäkseen ongelmia laitteet on pidettävä päivitettyinä.

Tekoäly tarjoaa IoT-laitteille tärkeitä ominaisuuksia, mitä ilman IoT ei olisi lähellekään yhtä kykeneväinen erilaisiin tekoihin kuin mitä se nyt on. Nykyajan ihmiset arvostavat helppoutta ja vaivattomuutta, mitä tekoäly tarjoaa ikään kuin itsestään. Koneet oppivat teoistaan viisaammiksi, minkä seurauksena laitteisiin ei tarvitse erikseen syöttää uusia käskyjä koodin muodossa. Samalla tekoälyn lisääminen kasvattaa huolta arkaluontoisen datan käsittelystä, sillä ihminen ei näe sitä hurjaa datamäärää mitä käsitellään pilvessä tai palvelimilla tekoälyn toimesta. Loppujen lopuksi täytyy muistaa, että tekoäly on vain työkalu muiden joukossa, joten sekään ei ole täydellinen (Chester 2019).

Peruskäyttäjälle voi olla mahdotonta käyttää Honeypotin kaltaisia työkaluja tietoturvaiskujen havaitsemiseksi, mutta yrityksille on tärkeää selvittää hakkereiden käyttämät tekniikat. Kaiken tarkoituksena on tehdä laitteista turvallisempia ja valmiimpia kuluttajamarkkinoille sekä tarjota päivityksiä paikkaamaan tietoturva-aukkoja.

Käyttäjien tekemät teot iskujen estämiseksi osoittautuivat varsin kokonaisvaltaisiksi. Jo pelkästään laitteiden käyttämien oletustunnusten vaihtaminen osoittautui tehokkaaksi keinoksi hankaloittaa verkkorikollisten toimia. Kotona reitittimeen tehtävät muutokset ovat kuitenkin tärkeimmät keinot pienentää iskujen mahdollisuutta.

IoT-laitteiden keräämä datan määrä on valtava. Datan merkitystä käsiteltiin monessa eri asiayhteydessä eikä sen merkitystä voi kiistää. Laitteiden tuottama data kerätään sellaisiin paikkoihin, joihin peruskäyttäjällä ei ole pääsyä. Aina ei voi tietää, mihin kaikkialle data kulkee ja miten sitä käytetään. Datan oikeaoppinen käsittely tulee korostumaan tulevaisuudessa. Dataa voidaan suojella tekemällä kotiverkko mahdollisimman turvalliseksi. Käyttäjän on kuitenkin hyväksyttävä, että dataa lähetään jatkuvasti operaattoreille, yrityksille ja kolmansille osapuolille, vaikka kotiverkkoon tekisi kaikki mahdolliset suojaukset.

Opinnäytetyössä käytettyjen lähteiden määrä oli suuri ja kirjava, joten löydettyjä ongelmia ja niiden ehkäisykeinoja voidaan pitää hyvin luotettavina. Työn luotettavuutta olisi lisännyt kohdentamalla tutkimus IoT-laitteita valmistavaan yritykseen tai tietoturvayritykseen. Toimeksiantajalta olisi saanut hyvät pohjatiedot siihen, kuinka tietoturvaan suhtaudutaan käytännön tasolla. He olisivat voineet myös rajata työtä pienemään osaan sekä antaa hyviä keinoja kehittää sitä.

Katsauksen loppupäätelmänä voidaan todeta, että tavallisen käyttäjän vastuulla on tehdä laitteistaan turvallisempia käyttää. Tietoturvan parantamiseksi on paljon eri keinoja, mutta vastuuta pitäisi saada enemmän tuotteen valmistajille ja verkko-operaattoreille. Tulevaisuudessa verkkoyhteydet ja tekniikat jatkavat kehittymistään, joten IoT-laitteiden tietoturvan merkitys tulee vain korostumaan. Samalla kun tekniikat kehittyvät, myös hakkereiden osaaminen ja heidän käyttämänsä keinot muuttuvat vaarallisimmiksi. Iskut kohdistuvat yhä useammin henkilökohtaiseen dataan, jolla voi olla kohtalokkaita seurauksia.

LÄHTEET

Alam, Tanweer 2018. A Reliable Communication Framework and Its Use in Internet of Things (IoT). s. 450-452. Viitattu 6.4.2020, https://www.researchgate.net/publication/325645304_A_Reliable_Communication_Framework_and_Its_Use_in_Internet_of_Things_IoT

Al-Turjman, Fadi 2019. Security in IoT-Enabled Spaces. CRC Press, USA, s. 135.

Arduino. What is Arduino? Viitattu 27.3. https://www.arduino.cc/en/guide/introduction

Aruba 2018. What Is 802.11ax (Wi-Fi 6)? And Why You Need It. Viitattu 9.4.2020, https://www.arubanetworks.com/assets/so/SO_80211ax.pdf

Atlam, Hany F – Wills, Gary 2019. IoT Security, Privacy, Safety and Ethics. s. 131.

Check Point 2020. The Dark Side of Smart Lightning: Check Point Research Shows How Business and Home Networks Can Be Hacked from a Lightbulb. Viitattu 24.4.2020, https://www.checkpoint.com/press/2020/the-dark-side-of-smart-lighting-check-point-research-shows-how-business-and-home-networks-can-be-hacked-from-a-lightbulb/#

Chester, Dean 2019. AI in IoT Security: Friend of Foe? Viitattu 10.5.2020, https://www.iotforall.com/hackers-using-ai/

Ciso Mag 2020. 10 IoT Security Incidents That Make You Feel Less Secure. Viitattu 27.4.2020, https://www.cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/

Cloudflare. Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis. Viitattu 21.4.2020, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/#toc-k

Cooper, Stephen 2020. How to Secure Your Home Wireless Network. Viitattu 6.5.2020, https://www.comparitech.com/blog/information-security/secure-home-wireless-network/

Cortese, Joseph 2020. Securing IoT in a 5G World. Viitattu 26.4.2020, https://www.cpomagazine.com/cyber-security/securing-iot-in-a-5g-world/

Domb, Menachem 2019. Smart Home Systems Based on Internet of Things. IntechOpen.
ESA. Types of Orbits. Viitattu 7.4.2020, https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits#LEO

Fernandez, Angel 2020. New IoT Security Regulations: What You Need to Know. Viitattu 17.4.2020, https://www.allot.com/blog/new-iot-security-regulations-what-you-need-to-know/

Fisher, Tim 2020. 5G Availability Around the World. Viitattu 27.3.2020, https://www.lifewire.com/5g-availability-world-4156244

Fruhlinger, Josh 2018. The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought the Internet. Viitattu 20.4.2020, https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

FutureIoT 2019. Satellites to Enable 24 Million IoT Connections Globally by 2024. Viitattu 5.4.2020, https://futureiot.tech/satellites-to-enable-24-million-iot-connections-globally-by-2024/

Garbade, Michael J 2018. A Simple Introduction to Natural Language Processing. Viitattu 31.3.2020, https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32

Gilchrist, Alasdair 2017. IoT Security Issues. Walter de Gruyter, USA, s. 5, 49.

Green, Andy 2020. What Is UPnP & Why Is It Dangerous? Viitattu 7.5.2020, https://www.varonis.com/blog/what-is-upnp/

Grustniy, Leonid 2018. What's a Guest Wi-Fi Network, and Why Do You Need one? Viitattu 6.5.2020, https://www.kaspersky.com/blog/guest-wifi/23843/

Gupta, Aditya 2019. The IoT Hacker's Handbook. A practical Guide to Hacking the Internet of Things. Apress, USA, s. 2-4.

Heinzman, Andrew 2019. Not All 5G Is Equal: Millimeter Wave, Low-Band, and Mid-Band Explained. Viitattu 30.3.2020, https://www.howtogeek.com/428337/not-all-5g-is-equal-millimeter-wave-low-band-and-mid-band-explained/

Hoffman, Chris 2020. Wi-Fi 6 Is Here: Should You Upgrade to Wi-Fi 6 in 2020? Viitattu 9.4.2020, https://www.howtogeek.com/525698/wi-fi-6-is-here-should-you-upgrade-to-wi-fi-6-in-2020/

Impreva 2020. Distributed Denial of Service (DDoS). Viitattu 20.4.2020, https://www.imperva.com/learn/application-security/denial-of-service/

Kaspersky 2018. New IoT-Malware Grew Three-Fold in H1 2018. Viitattu 22.4.2020, https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018

Kaspersky 2019. IoT Under Fire: Kaspersky Detects More Than 100 Million Attackers on Smart Devices in H1 2019. Viitattu 22.4.2020, https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019

Khvoynitskaya, Sandra. The history and future of the internet of things. Viitattu 24.3.2020, https://www.itransition.com/blog/iot-history

Knud, Lasse Lueth 2020. IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year. Viitattu 27.3.2020, https://iot-analytics.com/iot-2019-in-review/

Kreminchuker, Eli – Zavodchik, Maxim 2019. Echobot Malware Now up to 71 Exploits, Targeting SCADA. Viitattu 24.4.2020, https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

Lea, Perry 2018. Internet of Things for Architects. Packt, Englanti, s. 390-391.

Li, He – Ota, Kaoru – Dong Mianxiong 2018. Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing. IEEE, s. 1-3.

Lin, Huichen 2016. IoT Privacy and Security Challenges for Smart Home Environments.
Linthicum, David. Edge Computing vs. Fog Computing: Definitions and Enterprise Uses. Viitattu 2.4.2020, https://www.cisco.com/c/en/us/solutions/enterprise-networks/edge-computing.html

Lueth, Knud Lasse 2014. Why the Internet of Things is called Internet of Things: Definition, history, disambiguation. Viitattu 23.3.2020, https://iot-analytics.com/internet-of-things-definition/

Lyon, Chris – Taye, Hywote 2020. Secure the Refrigerator: Broad New California and Oregon IoT Security Laws Come Into Effect. Viitattu 17.4.2020, https://www.cpomagazine.com/data-protection/secure-the-refrigerator-broad-new-california-and-oregon-iot-security-laws-come-into-effect/

Mahmood, Zaigham 2019. Security, Privacy and Trust in the IoT Environment. Springer International Publishing, Switzerland, s. 98-99.

Mann, Adam 2020. Starlink: SpaceX's Satellite Internet Project. Viitattu 8.4.2020, https://www.space.com/spacex-starlink-satellites.html

McClelland, Calum 2020. What is IoT? – A Simple Explanation of the Internet of Things. Viitattu 22.3.2020, https://www.iotforall.com/what-is-iot-simple-explanation/

Moghaddam, Hooman Mohajeri ym. 2019. Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices. Princeton University and University of Chicago. Viitattu 27.4.2020, https://www.princeton.edu/~pmittal/publications/tv-tracking-ccs19.pdf

Mundle, Kent. Home Smart IoT Home: Domesticating the Internet of Things. Viitattu 23.3.2020, https://www.toptal.com/designers/interactive/smart-home-domestic-internet-of-things

Mundy, Jon – Thomas, Kevin 2019. What Is Massive MIMO Technology? Viitattu 30.3.2020, https://5g.co.uk/guides/what-is-massive-mimo-technology/

Narayanasamy, Aru – Ahmad, Yasser Asrul – Othman, M 2017. Nanosatellites Constellation as an IoT Communication Platform for Near Equatorial Countries. IOP Publishing, Englanti, s. 2. Viitattu 7.4.2020, https://iopscience.iop.org/article/10.1088/1757-899X/260/1/012028/pdf

Network World 2018. Why is OFDMA a Magical Feature in the 802.11ax Standard? Viitattu 9.4.2020, https://www.networkworld.com/article/3315056/why-is-ofdma-a-magical-feature-in-the-802-11ax-standard.html

Norton 2020. Internet of Things (IoT) security: 9 Ways You Can Help Protect Yourself. Viitattu 23.3.2020, https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html

Norton 2020. Smart Watches and Internet Security: Are My Wearables secure? Viitattu 29.4.2020, https://us.norton.com/internetsecurity-iot-how-to-protect-your-connected-wearables.html

O'Donnell, Lindsey 2020. Mandatory IoT Security in the Offing with U.K. Proposal. Viitattu 16.4.2020, https://threatpost.com/mandatory-iot-security-uk-proposal/152217/

O'Donnell, Lindsey 2020. More Than Half of IoT Devices Vulnerable to Severe Attacks. Viitattu 20.4, https://threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609/

Palmer, Danny 2019. AI, Quantum Computing and 5G Could Make Criminals More Dangerous Than Ever, Warn Police. Viitattu 4.5.2020, https://www.zdnet.com/article/ai-quantum-computing-and-5g-could-make-criminals-more-dangerous-than-ever-warn-police/

Palmer, Danny 2020. AI is Changing Everything about Cybersecurity, for Better and for Worse. Here's What You Need to Know. Viitattu 10.5.2020, https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/

Park, Youngseok ym. 2019. Security Analysis of Smart Speaker: Security Attacks and Mitigation. Tech Science Press. Viitattu 27.4.2020, http://www.techscience.com/cmc/v61n3/35289/pdf

Pathak, Nishith – Bhandari, Anurag 2018. IoT, AI, and Blockchain for .NET. Building a Next-Generation Application from the Ground Up. Apress, USA, s. 29-34.

Postscapes 2019. Internet of Things (IoT) History. Viitattu 24.3.2020, https://www.postscapes.com/iot-history/

Prabhu, Csr 2017. Overview – Fog Computing and Internet of Things (IoT). s. 9. Viitattu 2.4.2020, https://www.researchgate.net/publication/324021412_Overview_-_Fog_Computing_and_Internet-of-Things_IOT

Premsankar, Gobika – Di Francesco, Maria – Taleb, Tarik 2018. Edge Computing for the Internet of Things: A Case Study, IEEE. Viitattu 1.4.2020, https://users.aalto.fi/~premsag1/docs/premsankar2018edge.pdf

Proske, Sandra 2019. Securing the IoT 'Security Nightmare' is a Massive Opportunity for Service Providers. Viitattu 28.4.2020, https://blog.f-secure.com/service-providers-iot-security/

Ren, Jingjing ym. 2019. Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf

Reyna, Ana ym. 2018. On Blockchain and its Integration with IoT. Challenges and Opportunities. s. 174. Viitattu 30.4.2020, https://www.sciencedirect.com/science/article/pii/S0167739X17329205

Rishi, Rahul – Saluja, Rajeev 2019. Future of IoT. Viitattu 4.4.2020, http://ficci.in/spdocument/23092/Future-of-IoT.pdf

Robertson, Marta 2019. Why IoT Needs Machine Learning to Thrive. Viitattu 31.3.2020, https://www.iotforall.com/why-iot-needs-machine-learning/

Schatsky, David – Kumar, Navya – Bumb, Sourabh 2017. Intelligent IoT. Bringing the Power of AI to the Internet of Things. Viitattu 11.5.2020, https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/intelligent-iot-internet-of-things-artificial-intelligence.html

Seal, Alan 2020. Centralized vs Decentralized Network: Which One Do You Need? Viitattu 30.4.2020, https://www.vxchnge.com/blog/centralized-decentralized-network

Security Research Labs 2019. Smart Spies: Alexa and Google Home Expose Users to Vishing and Eavesdropping. Viitattu 29.4.2020, https://srlabs.de/bites/smart-spies/

Shah, Vaibhav 2019. 9 Main Security Challenges for the Future of the Internet of Things (IoT). Viitattu 26.4.2020, https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iot/

Sheetz, Michael – Petrova, Magdalena 2019. Why in the Next Decade Companies Will Launch Thousands More Satellites Than in All of History. Viitattu 8.4.2020, https://www.cnbc.com/2019/12/14/spacex-oneweb-and-amazon-to-launch-thousands-more-satellites-in-2020s.html

Simko, Christian 2016. Man-in-the-middle Attacks. Viitattu 24.4.2020, https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot

Storm, David 2017. IoT Security: 8 Lessons Learned From the Mirai Botnet. Viitattu 21.4.2020, https://www.hpe.com/us/en/insights/articles/iot-security-8-lessons-learned-from-the-mirai-botnet-1702.html

Tegio, Rose Ann 2019. Quantum Computing and the IoT. Viitattu 4.5.2020, https://www.azoquantum.com/Article.aspx?ArticleID=101

Vella, Heidi. 5G vs 4G: What is the Difference? Viitattu 30.3.2020, https://www.raconteur.net/technology/4g-vs-5g-mobile-technology

Viswanathan, Vibhuthi 2019. Eight Ways to Secure Your Data on IoT Devices. Viitattu 7.5.2020, https://www.itproportal.com/features/eight-ways-to-secure-your-data-on-iot-devices/

Wi-Fi Alliance 2019. Wi-Fi Certified 6. Viitattu 9.4.2020, https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6