IOT - HAAVOITTUVUUDET JA TIETOTURVA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Hämeenlinna, syksy 2017

Tero Jänisvaara

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittely
Visamäki

Tekijä Tero Jänisvaara **Vuosi** 2017

Työn nimi IoT - haavoittuvuudet ja tietoturva

Työn ohjaaja/t Lasse Seppänen

TIIVISTELMÄ

Tämän opinnäytetyön tilaaja oli Hämeen Ammattikorkeakoulun (HAMK) Älykkäät palvelut -tutkimusyksikkö. Opinnäytetyön päätarkoituksena on ollut HAMK:n Internet of Things (IoT) -aihealueeseen liittyvän tiedon ja osaamisen kerryttäminen keskittyen laitteiden ja järjestelmien tietoturvallisuuteen. Yksi tavoitteista oli myös opinnäytetyön tekijän oman IoT-tietämyksen kartuttaminen.

Opinnäytetyössä käydään läpi tällä hetkellä (2017) tunnettuja IoT-tietoturvauhkia, kuten haittaohjelmia ja laitteiden haavoittuvuuksia. Tämän lisäksi käydään läpi sitä, mitä mahdollisuuksia on olemassa IoT-laitteiden turvallisuusuhkien löytämiseen. Näiden lisäksi esitellään erilaisia IoT-tietoturvalaitteita-, sekä ohjelmistoja, joilla usein turvattomien IoT-laitteiden tietoturvaa voi parantaa kotona ja yrityksissä. Opinnäytetyössä esitellään myös parhaita käytäntöjä siitä, mitä tulisi ottaa huomioon, jotta IoT-laite olisi turvassa mahdollisilta hyökkäyksiltä ja haittaohjelmilta. Lopuksi käydään läpi Thingworx IoT-alustan turvallisuusasetukset.

Tällä hetkellä näyttää siltä, että IoT-laitteita kohtaan tapahtuvat hyökkäykset ovat ainakin hetkellisesti vähentyneet, eikä vuoden 2016 syksyllä tapahtuneiden usean bottiverkon jälkeen suurempia massauhkia ole esiintynyt. Tämä voi olla seurausta siitä, että käyttäjät ja valmistajat ovat tulleet tietoisemmiksi laitteiden haavoittuvuuksista. Luultavasti kuitenkin tulevaisuudessa hyökkäykset IoT-laitteita kohtaan tulevat entistä vaarallisemmiksi, viime vuosina on ollut kyse lähinnä avoimiin portteihin kohdistuneista hyökkäyksistä.

Avainsanat IoT, tietoturva, haittaohjelma**,** haavoittuvuudet

Sivut 48 sivua, joista liitteitä - sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Visamäki

Author Tero Jänisvaara **Year** 2017

Subject Internet of Things - Vulnerabilities and Security Overview

Supervisor Lasse Seppänen

ABSTRACT

This thesis is made for Häme University of Applied Sciences - HAMK's, Smart Services Research Unit. The main purpose of this thesis was to gather more information and knowledge about IoT for HAMK, concentrating on the information security of devices and systems. One of the goals has also been to gather more knowledge about IoT myself.

In this thesis I discuss some currently known IoT security threats, such as malware and device vulnerabilities. I also describe, what kind of possibilities there are to find vulnerabilities of IoT devices. And on top of this I've also tried to find devices and software that can help to prevent IoT threats at home and at the office. In the latter part of the thesis you will also find "golden rules" on what to do and what not to do, to make sure, that your IoT device is safe. In the last chapter, I present Thingworx IoT platform's security settings.

At the moment it seems, as if the (major) attacks on IoT devices have at least temporarily been decreased. There has not been any news about major botnets since autumn 2016. This may be due to consumers and manufacturers becoming more aware of the device and software vulnerabilities. But most likely the attacks on IoT devices will become more dangerous in the future, lately there have been attacks on device's open ports. It remains to be seen, how the situation will develop.

Keywords IoT, information security, malware, vulnerabilities

Pages 48 pages including appendices - pages

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on tuottaa Hämeen Ammattikorkeakoululle (HAMK) lisää tietoa IoT:stä (Internet of Things), tarkemmin sen haavoittuvuuksista ja tietoturvasta. Tarkoituksena on myös luoda ohjeistus, miten ThingWorx IoT-alustan tietoturva-asetukset tehdään. Mutta tietysti tavoitteena on osittain myös se, että pystyn luomaan itselleni syvällisemmän käsityksen IoT:stä.

Tässä opinnäytetyössä käsitellään IoT-asioita lähinnä kuluttajalle suunnattujen ratkaisujen näkökulmasta. Aloitetaan perusasioista, käydään ensin läpi erilaisia käsitteitä, jotka liittyvät tähän aiheeseen.

Huhtikuussa 2017 hakusana IoT tuottaa Google-haussa noin 82 100 000 tulosta. Kyseessä on varsin ajankohtainen ja paljon keskustelua, sekä kirjallista materiaalia tuottava aihe. Alan kaikki suurimmat toimijat, kuten esimerkiksi Cisco, SAP, Microsoft, Amazon, GE, Google, Intel, IBM, Oracle jne. ovat luonnollisesti mukana kehittämässä esineiden internetiä. Mutta mukana on myös runsaasti pienempiä toimijoita.

Toistaiseksi IoT on monimutkainen kokonaisuus sisältäen erilaisia protokollia ja sovelluksia, sekä laitteita. Vielä ei tiedetä, tulevatko kaikki niistä selviytymään, vai nouseeko esimerkiksi joku tietty, tai tietyt protokollat voittajiksi. Yrityksillä ei ole tällä hetkellä muuta vaihtoehtoa, kuin veikata parasta protokollavaihtoehtoa ja toivoa, että se menestyy tulevaisuudessakin.

Edellä mainittujen lisäksi täytyy yrityksen miettiä myös, haluaako se käyttää avoimen lähdekoodin ohjelmistoja, joita se pystyy tarvittaessa itsekin muokkaamaan haluttuun suuntaan, vai suljetun mallin ohjelmistoja, jotka taas pakottavat käyttämään samaa ohjelmistoa siten -kuin valmistaja on sen halunnut, ilman mahdollisuuksia suuren luokan yrityskohtaiseen räätälöintiin.

Tässä opinnäytetyössä etsitään vastausta seuraaviin kysymyksiin:
Millaisia tietoturvalaitteita on tarjolla kuluttajille tai yrityksille? Millaisia IoT-haittaohjelmia on olemassa? Miten IoT:n mahdollisia haavoittuvuuksia voidaan tutkia? Mitkä ovat parhaat käytännöt IoT-laitteiden suojaamiseen? Miten Thingworx IoT -alustan suojaus rakentuu?

2 IOT - INTERNET OF THINGS

IoT - Internet of Things on yleisnimitys kaikille älykkäille verkkolaitteille. IoT:n avulla voidaan käytännössä verkottaa fyysiset laitteet, esimerkiksi teollisuuden tuotantolaitteet. IoT jaetaan yleensä karkeasti kahteen ryhmään, on IoT (Internet of Things) eli Esineiden Internet ja IIoT (Industrial Internet of Things), eli Teollinen Internet. (Collin J., Saarelainen A. 2016, 30.)

IoT:n avulla esimerkiksi teollisuusyritykset voivat automatisoida tuotantoa huomattavassa määrin. Laitteilta voidaan myös kerätä dataa verkon yli, säätää niitä tai tutkia niiden tilaa verkon välityksellä. Siten pystytään tekemään ennakoivaa huoltoa, sekä pystytään paremmin ennakoimaan laitteiden rikkoutuminen ja odotettavissa oleva elinikä. Näiden ominaisuuksien lisäksi työvoiman tarve vähenee, koska parhaimmillaan voidaan hallita jopa tuhansia laitteita yhden ohjelmiston kautta, tarvitsematta mennä paikan päälle. Lisäksi tuotantoa voidaan ohjata vaikka tuhansien kilometrien päästä, verkon yli. Tulevaisuuden tavoitteena on kokonaan älykkäiden laitteiden pyörittämä tehdas, jossa laitteet kontrolloivat toisiaan, ihmistyövoimaa ei juuri tarvita. (Collin J., Saarelainen A. 2016, 120)

IoT:n helppoudella on kuitenkin myös varjopuolensa, koska mikä tahansa verkossa oleva laite on altis hyökkäyksille. Uutisissa on ajoittain mainintoja erilaisista roskapostia lähettävistä kodinkoneista ja verkkohyökkäyksistä. Oikein tehtynä IoT-laite voi olla tietoturvallinen. Tietoturvan toteuttamista tosin haittaa tällä hetkellä olemassa olevien IoT-ohjelmistojen ja laitteiden kirjavuus, sekä yhtenäisten toimintatapojen puute. Ei ole olemassa yhtä ainoaa tapaa toteuttaa IoT-laite tai ohjelmisto, vaan erilaisia alustoja on olemassa useita ja moneen eri käyttötarkoitukseen. Eräs näistä IoT-alustoista on tässä opinnäytetyössä käsiteltävä PTC:n Thingworx.

Hyvää IoT-tietoa voi löytää esimerkiksi Joni Anttilan HAMKissa aiemmin tänä vuonna tekemästä opinnäytetyöstä ”Eri palveluntarjoajien IoT-alustojen vertailu: IBM Watson IoT & Bluemix, Microsoft Azure IoT Hub ja PTC Thingworx” (Anttila J. 2017). Hyvänä johdatuksena IoT-maailmaan toimii myös kirja ”Teollinen Internet” (Collin J., Saarelainen A. 2016.)

IoT:n haavoittuvuuksista löytyy tietoa esimerkiksi eri tietoturvayhtiöiden sivustoilta (kuten McAfee, Symantec, F-Secure, Kaspersky jne.). Viestintäviraston sivuilta voi myös saada hyviä tietoturvavinkkejä. Kannattaa myös seurata varoituksia haittaohjelmista. Erilaiset haittaohjelmien seurantasivut, kuten Intelin MalwareTech botnet tracker antavat hyvän kuvan haittaohjelmien levinneisyydestä tällä hetkellä.

3 IOT-TIETOTURVA

IoT-laitteissa tietoturvan tulisi olla ensimmäinen ja tärkein asia. Mikäli laitteessa tai ohjelmistossa itsessään ei ole sisäänrakennettua tietoturvaa, on se altis erilaisille hyökkäyksille. Monesti IoT-laitteiden tietoturva on toteutettu huonosti, tai siitä huolehtiminen on jätetty käyttäjän vastuulle. Voidaan ehkä puhua paremminkin tietoturvattomuudesta, kuin tietoturvasta. Pahimmillaan laitetta voidaan käyttää välineenä erilaisissa DDoS (Distributed Denial of Service) -hyökkäyksissä kaatamaan erilaisia palveluita tai sivustoja. Tietoturvan testaamiseen on kuitenkin olemassa monia erilaisia työkaluja. Tämän lisäksi IoT-laitteiden tietoturvaa voi pyrkiä parantamaan erilaisilla tietoturvalaitteilla ja ohjelmistoilla, joita käydään tuonnempana opinnäytetyössä läpi.

3.1 Tietoturvan testaus

IoT:n tietoturvaa voidaan testata monin eri tavoin. Laitteisiin voidaan esimerkiksi yrittää erilaisten verkkotyökalujen avulla hyökätä ulkoapäin käsin. Tällaiset keinovalikoimat ovat yleensä käytössä lähinnä IT-ammattilaisilla. On kuitenkin olemassa myös kenen tahansa käytettävissä olevia erilaisia hakukoneita, joiden avulla pystytään kartoittamaan internetiin päin avoinna olevia laitteita. Lisäksi kuka tahansa voi testata itse oman verkon laitteiden avoimia portteja käyttäen pitkälti samoja työkaluja, joita käytetään yleisesti tietotekniikan parissa, kuten Wireshark, joka seuraa verkkoliikennettä, tai ShieldsUP, jonka avulla pystyy etsimään laitteista avoimia portteja.

Usein juuri IoT-laitteissa portit saattavat olla avoinna internetiin päin, jolloin mahdollinen hyökkääjä pääsee liiankin helposti laitteelle ja mahdollisesti sitä kautta verkon muihin laitteisiin käsiksi. Mutta testaamalla ja sulkemalla mahdolliset avoimet portit pystytään väärinkäyttö estämään.

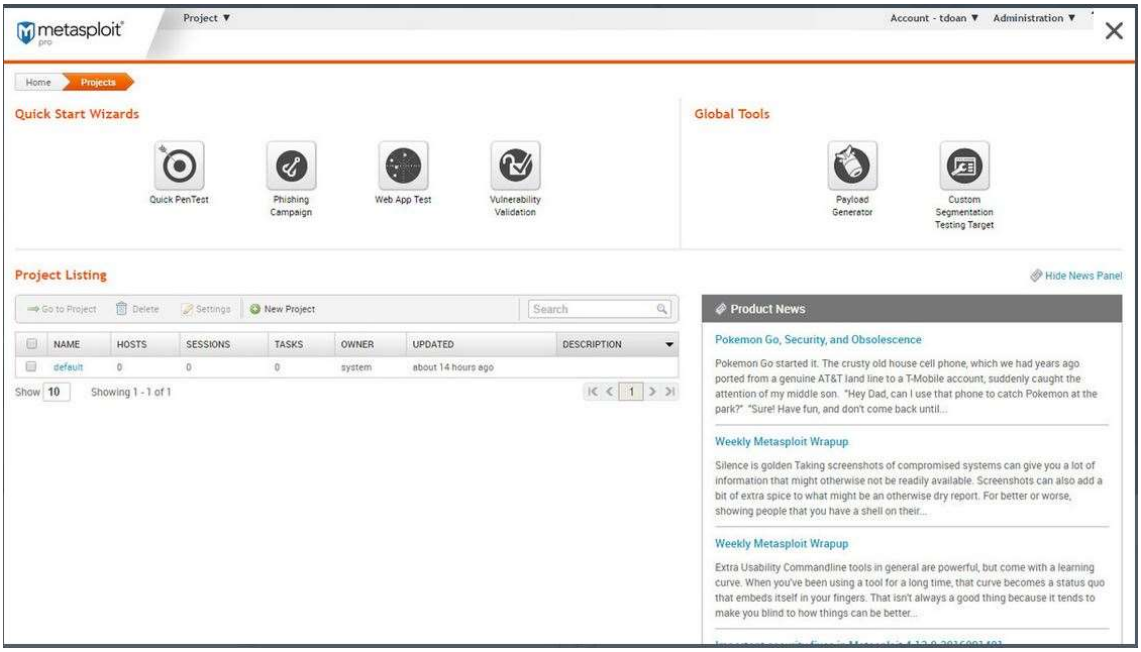
3.1.1 Metasploit

Metasploit on valmistajansa (Rapid7) mukaan maailman yleisin penetraatiotestaukseen (Penetration testing) käytetty ohjelmisto. Sen avulla voidaan simuloida verkkohyökkäyksiä ja sen tulosten perusteella voidaan vahvistaa verkon suojausta. (Rapid7 n.d.)

Käytännön tasolla Metasploit-ohjelmisto asennetaan tietokoneeseen, tätä varten tulee poistaa käytöstä koneen virustorjunta-ohjelmisto ja palomuuri. Toinen, ehkä turvallisempi vaihtoehto on asentaa Metasploit virtuaalikoneelle (Windows- tai Linux-pohjaiselle).

Mikäli Metasploit:ia halutaan testata ennen oikean järjestelmän testausta, voidaan luoda tarkoituksellisesti tietoturvaltaan haavoittuva virtuaalikone (Metasploitable - Ubuntu 8.04 serveri) VMwaren virtuaalialustalle. Tähän alustaan ja sen ohjelmistoihin kohdistetaan verkkohyökkäyksiä. Näistä verkkohyökkäyksistä saatujen tietojen perusteella kerätään tietoa sen heikkouksista. Tämän perusteella voidaan tehdä vastaavia testejä oikeassa (tuotanto-) järjestelmässä. (Metasploitable n.d.)

Kaikkiaan Metasploit:sta on olemassa 4 eri versiota. Pro-versio laajimmilla ominaisuuksilla on tarkoitettu lähinnä yritysten IT-osastoille. Express - maksullinen, hieman rajoitetumpi versio on suunnattu yleisesti IT-henkilöille. Ilmainen Community on tarkoitettu opiskelijoille ja pienyrityksille. Näiden lisäksi ilmainen Framework-versio on tarkoitettu kehittäjille ja tietoturvatutkijoille. Näistä vain Pro, Express ja Community sisältävät helppokäyttöisen Web-käyttöliittymän. Kuvassa 1 näkymä Metasploit Pro-versiosta. (Metasploit - Editions n.d.)



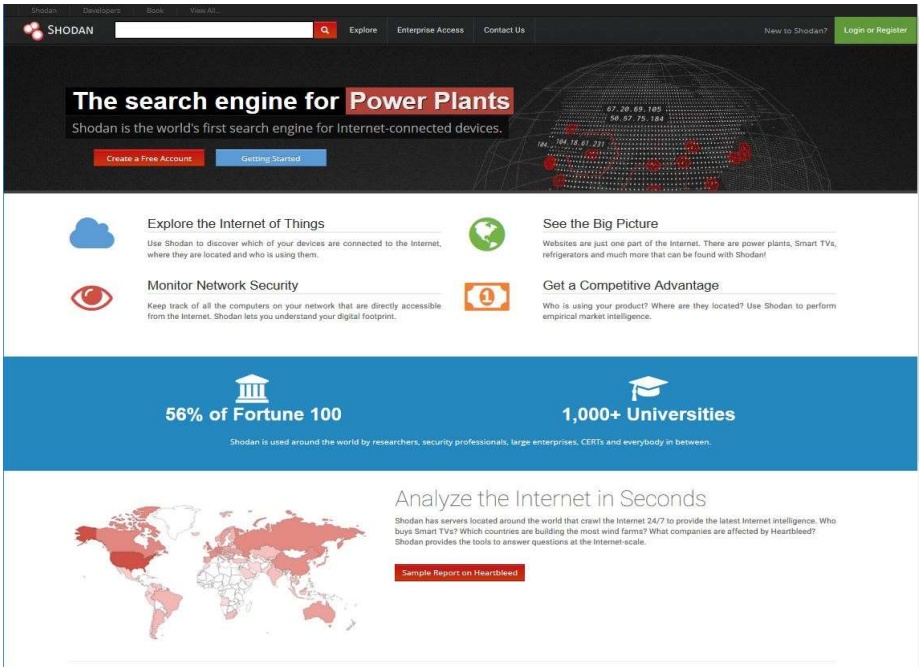
Kuva 1. Metasploit Pro -näkymä (Rapid7 2017)

Helmikuussa 2017 Rapid7 esitteli Metasploitin uuden ominaisuuden, jonka avulla voidaan testata sekä IoT-laitteita -että ohjelmistoja. Tämä voidaan tehdä joko rakentamalla laiteohjelmisto Metasploit-yhteensopivaksi, tai Rest API-rajapinnan avulla. (Rapid7 2017.)

3.1.2 Shodan

Vuonna 2013 perustettu hakukone Shodan (shodan.io) auttaa löytämään avoimeksi jätettyjä IoT-laitteita ja muita verkkoon kytkettyjä laitteita, kuten servereitä, web-kameroita ym. ympäri maailman. (Osborne C. 26.1.2016.)

Kuvassa 2 näkymä Shodan-hakukoneen etusivusta.



Kuva 2. Shodan-hakukone -etusivu (Shodan 2017.)

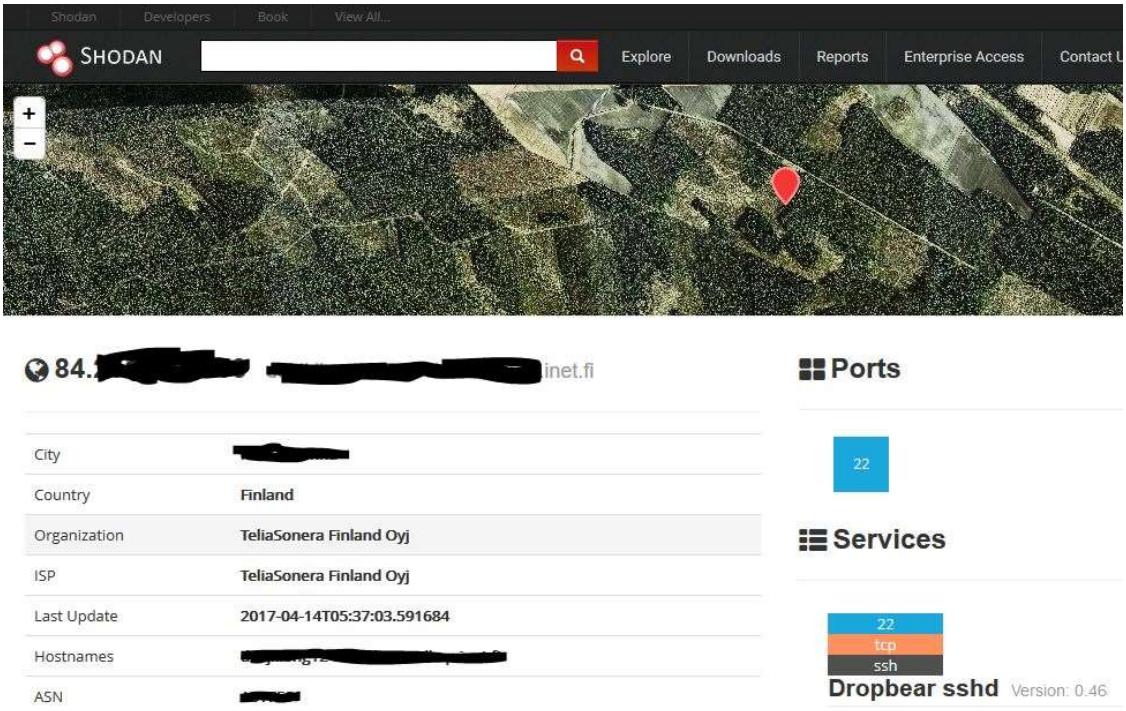
Usein laitteiden omistajat ovat tietämättömiä laitteidensa tietoturvattomuudesta, eivätkä ole esimerkiksi vaihtaneet laitteen valmistajan asettamaa oletussalasanaa. Tietoturvaan paremmin tutustuneet voivat kuitenkin testata omien laitteidensa tietoturvan Shodanin avulla. Shodania on myös kutsuttu “maailman vaarallisimmaksi hakukoneeksi”, koska se löytää avoimeksi jätetyt laitteet. Esimerkiksi löytäessään avoimeksi jätetyn webkameran -se ottaa kuvankaappauksen kameran näkymästä, ja niitä voi selata Shodanin sivuilta. Tämä on pelottavin puoli, tuskin kukaan haluaa web-kameransa tai valvontakameransa kuvaa julkiseen levitykseen, tai Shodanin sivustolle.

IoT-laitteiden käyttäjillä pitäisi olla vähintään kohtalaiset IT-taidot. Vaihtoehtoisesti valmistajan pitäisi luoda niin hyvä ohjeistus laitteille, ettei tietoturvavuotoja pääsisi tapahtumaan. Pahimmassa tapauksessa voi olla jopa niin, että laitteen valmistaja ei edes ole antanut käyttäjälle mahdollisuutta vaihtaa oletussalasanaa.

Shodanin avulla pystyttiin äskettäin paljastamaan ABB:n valmistamien teollisuusrobottien (IRB 140) haavoittuvuuksia. Kävi ilmi, että teoriassa hakkerit voisivat saada teollisuusrobotin hallintaansa ja saada sen tekemään toimenpiteitä, joiden seurauksena olisi viallisia tuotteita. Tämä testi tehtiin tietoturvatutkijoiden, eikä hakkereiden toimesta. Vaikka testi tehtiinkin suojaamattomassa verkkoyhteydessä, on ABB korjannut haavoittuvuudet testatussa mallissa. Valitettavasti tämän lisäksi Shodan löytää tutkijoiden mukaan edelleen yli 80 000 internetiin päin avoinna olevaa teollisuusrobottia, joten uhka on todellinen.

Pahin mahdollinen uhka lienee auton tai esimerkiksi lentokoneen osia valmistavien robottien hakkerointi. Tällöin saattaisi olla jo kyse ihmishengistä. Tästä syystä tietoturvan täytyy olla tärkeimpiä asioita, kun suunnitellaan teollisuusrobotteja. (Franceschi-Bicchierai L. 3.5.2017.)

Väärissä käsissä Shodan on vaarallinen työkalu. Se näyttää tarkkoja tietoja kohteesta ja tämän lisäksi myös sijainnin kartalla. Kuvassa 3 on esimerkki eräästä hausta, joka on tehty Shodanin avulla:



Kuva 3. Shodan-haku (Shodan 2017.)

Shodanissa haut tehdään esimerkiksi muodossa country:"FI" city:"Helsinki". Tällä haulla saadaan näkyviin kotimaassa Helsingin alueella sijaitsevat avoimet web-laitteet. Shodan tarjoaa myös mahdollisuutta käyttää muiden käyttäjien tekemiä hakuja pohjana, jolloin hakukoneen toimintoja pystyy oppimaan helpolla tavalla.

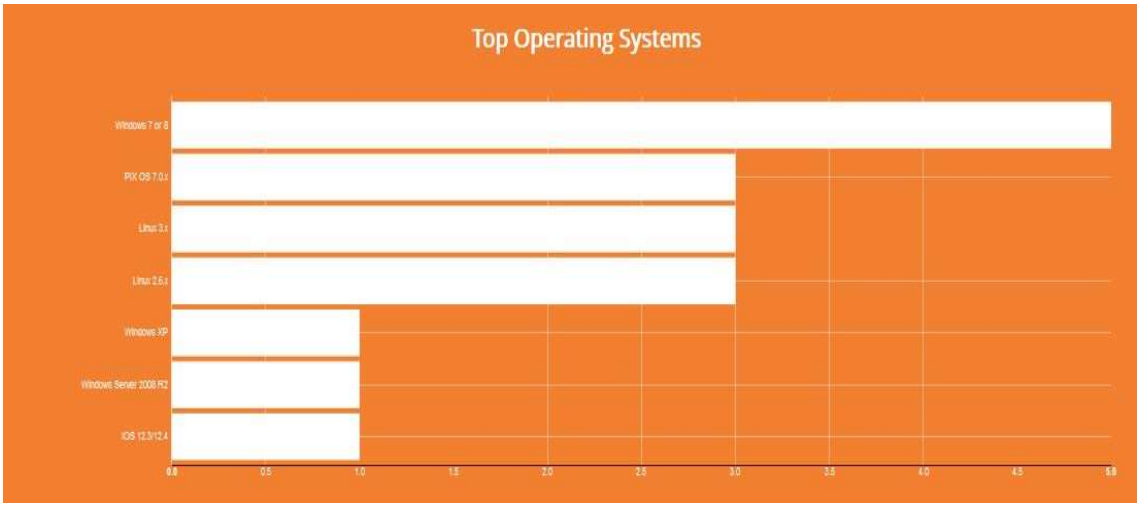
Kuvassa 4 on tehty haku, jossa pyritään löytämään Helsingin alueella olevat avoimet web-laitteet, joita hakuhetkellä on löytynyt kaikkiaan 97916 kpl:

Kuva 4. Shodan-haku -Helsinki (Shodan 2017.)

Mikäli halutaan hakea reitittimiä, joissa on edelleen oletuskäyttäjätunnus ja salasana, se tapahtuu hakuehdolla admin+1234, kuten kuvassa 5.

Kuva 5. Shodan haku - oletuskäyttäjätunnus ja salasana (Shodan 2017.)

Rekisteröitymällä käyttäjäksi Shodanissa pystyy myös luomaan näyttäviä raportteja havainnoista. Kuvassa 6 on pieni osa luodusta raportista.

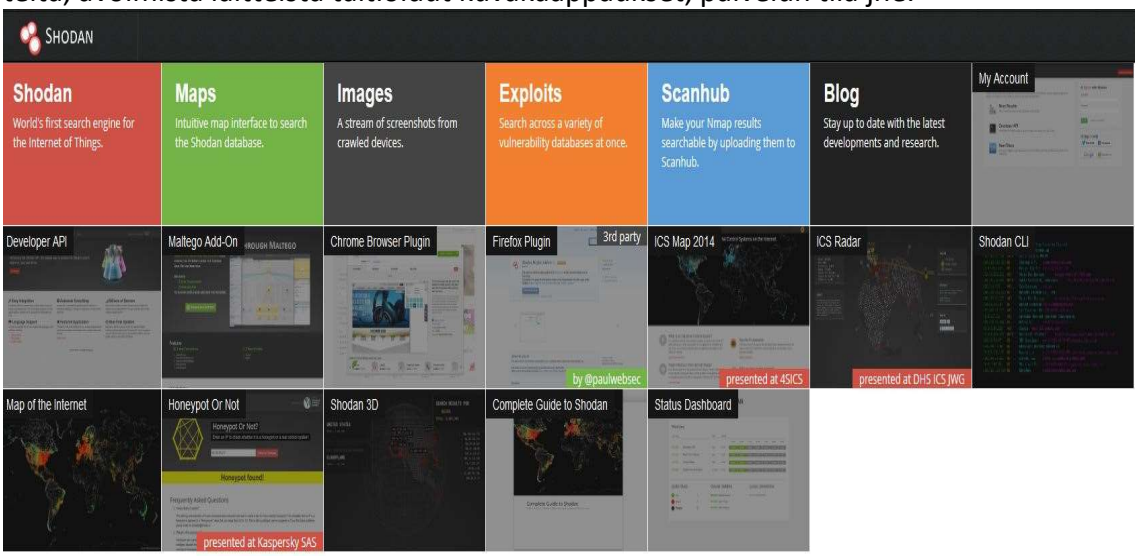


Kuva 6. Shodan-raportti 1 – suosituimmat käyttöjärjestelmät (Shodan 2017.)

Kuvassa 7 nähdään osa raportista, jossa haun kohteena ovat olleet D-Link -merkkiset Web-kamerat, jotka vastaavat http-kutsuun (200 OK).

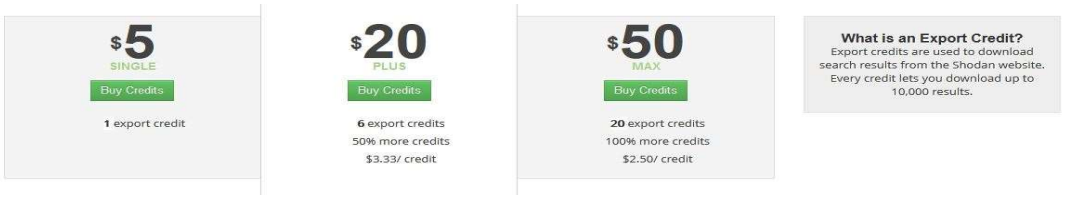
Kuva 7. Shodan-raportti 2 (Shodan 2017.)

Kuvassa 8 on esitettynä kaikki palvelut, joita Shodan tarjoaa. Näitä ovat esimerkiksi Shodan-hakukone, kartat -joiden avulla voi etsiä avoimia laitteita, avoimista laitteista taltioidut kuvakaappaukset, palvelun tila jne.



Kuva 8. Shodan – palvelut (Shodan 2017.)

Shodanissa luodut raportit saa myös ladattua omalle koneelleen CSV-, JSON- tai XML-muodossa. Tämä ei kuitenkaan ole ilmaista, vaan hinnat alkavat 5$:sta per raportti, kuten kuvassa 9 esitetään.



Kuva 9. Shodan -raporttien hinnoittelu (Shodan 2017.)

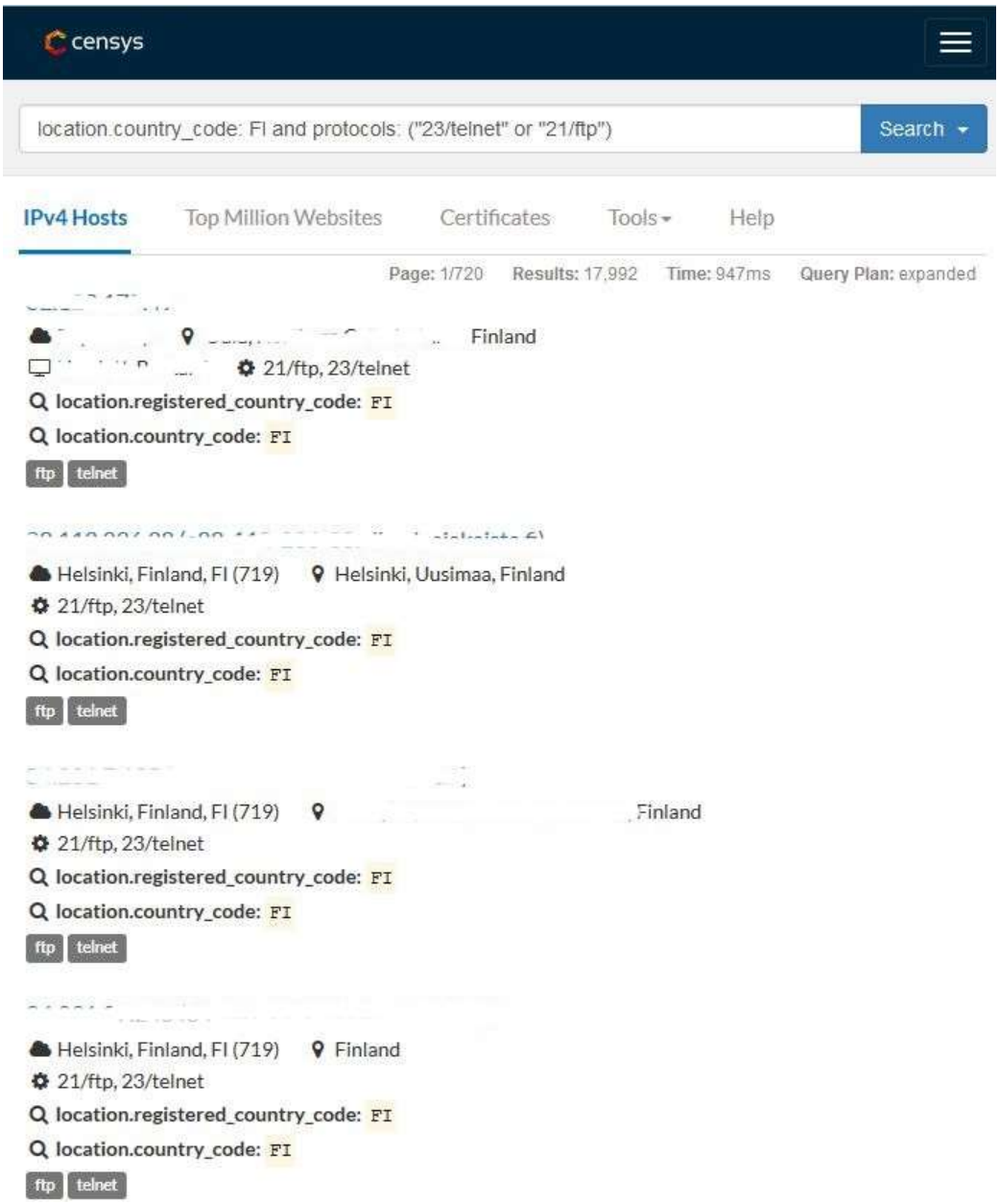
3.1.3 Censys

Censys (censys.io) on Michiganin yliopiston tutkijoiden kehittämä hakukone, joka ylläpitää tietokantaa kaikista internetiin avoimeksi jätetyistä laitteista. Haku tapahtuu ZMap-ohjelmiston avulla, joka myöskin on Michiganin Yliopiston tutkijoiden kehittämä. Censys:n tietokanta päivittyy joka päivä. ZMap käy läpi miljoonia IP-osoitteita päivässä, vastauksena saadaan tietoa esimerkiksi siitä, mikä laite kyseisessä IP-osoitteessa on, millaista ohjelmistoa se käyttää, onko laite salattu, sekä millainen laitteen kokoonpano on. Kuvassa 10 näkymä Censys-hakukoneen etusivusta. (Kumar M. 11.12.2015)

Kuva 10. Censys-hakukone - etusivu (Censys 2017.)

Censys:n tavoitteena on tehdä internetistä turvallisempi. Ensisijaisena kohderyhmänä ovat tietoturvayritykset. Mutta yhtä hyvin myös rikolliset tahot voivat käyttää hakukonetta avoimeksi jätettyjen laitteiden etsimiseen, ja sen seurauksena tietoja voidaan käyttää verkkohyökkäyksiin. Censys on ehkä jossain määrin haastavampi käyttää kuin Shodan, koska hakuehdon täytyy olla täsmälleen oikeassa muodossa, jotta tulokset ovat oikeanlaiset. Censys tarjoaa kuitenkin myös esimerkkihakuja ja opastaa tarvittaessa käyttäjää hakemaan oikein.

Kuvassa 11 on esimerkki Censys-hausta, jossa etsitään telnet- tai ftp-protokollaa käyttäviä isäntälaitteita Suomesta - portti 23 tai 21 avoinna. Käyttämällä hakuehtoa location.country_code: FI and protocols: ("23/telnet" or "21/ftp") saadaan kuvan 11 mukainen hakutulos.

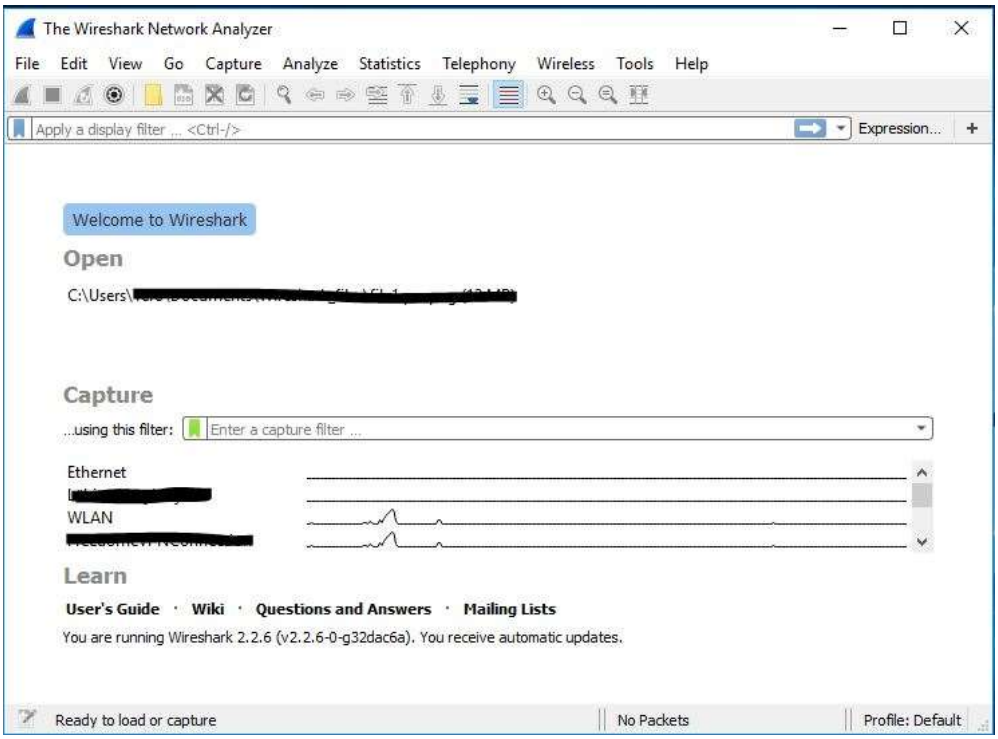


Kuva 11. Censys - hakutulokset (Censys 2017.)

3.1.4 Wireshark

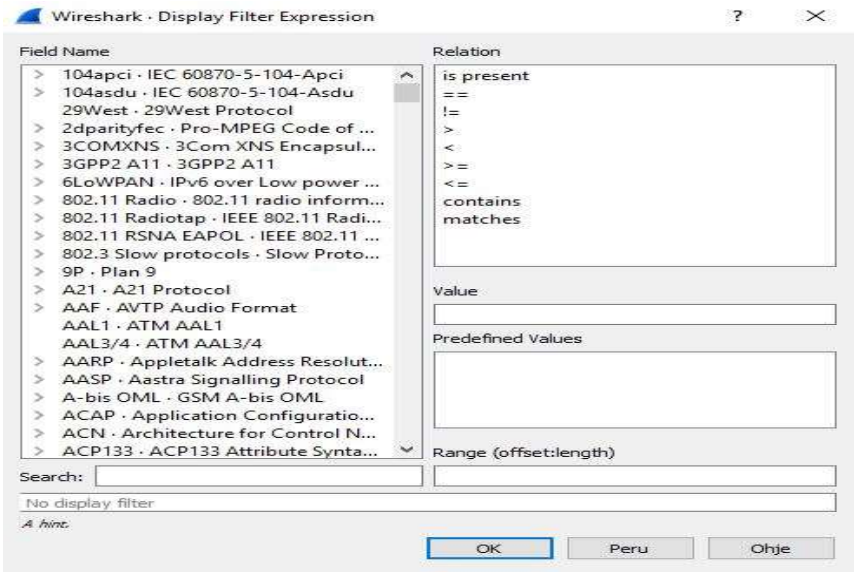
Wireshark on ensisijaisesti verkkoprotokollien analysointiin tarkoitettu avoimen lähdekoodin ohjelmisto. Sen avulla voidaan analysoida IoT-laitteiden verkkoyhteyksiä, sekä suorittaa vianetsintää. Käytännössä Wireshark seuraa esimerkiksi tietyn portin tai protokollan verkkoliikennettä.

Tätä liikennettä analysoimalla pystytään sitten tekemään johtopäätöksiä verkon toiminnasta. Kuvassa 12 näkymä Wiresharkin pääsivusta.



Kuva 12. Wireshark – pääsivu (Wireshark 2017.)

Wireshark-ohjelmisto tukee satoja eri verkkoprotokollia, myös IoT-maailmassa yleisesti käytettyjä, kuten ZigBee, 6LoWPAN, MQTT, BLE, IEEE 802.15.4 jne. Kuvassa 13 pieni osa tuetuista verkkoprotokollista.



Kuva 13. Wireshark - tuettuja verkkoprotokollia (Wireshark 2017.)

3.1.5 ShieldsUP

ShieldsUp on työkalu, jolla on mahdollista etsiä internetiin päin avoinna olevia portteja verkossa. IoT-laitteissa erityisesti BrickerBot ja Hajime -haittaohjelmat etsivät laitteista avoimia portteja (portti 22/23 jne). Kuvassa 14 on näkymä ShieldsUPin etusivulta.

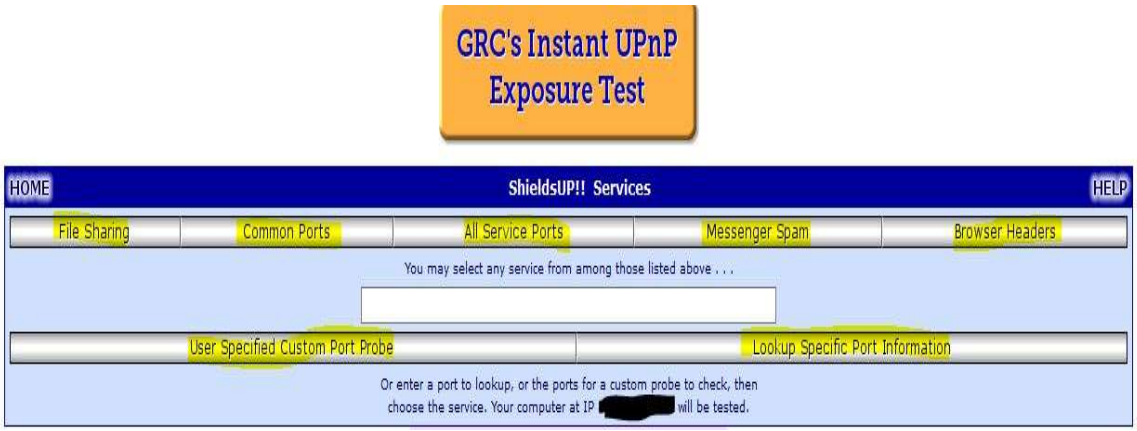
Kuva 14. ShieldsUP -etusivu (Gibson Research Corporation 2017.)

Kuvassa 15 on tehty porttiskannaus 11 eri portin osalta. Mikäli tulos näyttää tältä, olet turvassa ainakin avoimien porttien osalta.

Port	Service	Status	
0	<nil>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
21	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
22	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
119	NNTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
135	RPC	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

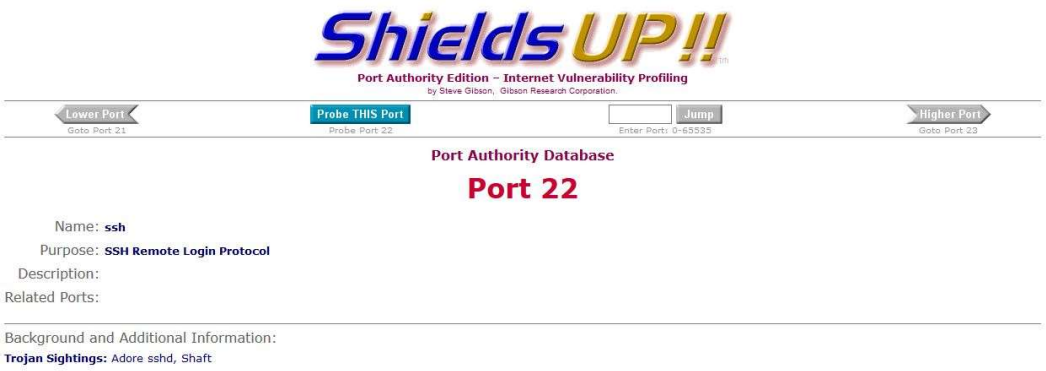
Kuva 15. ShieldsUP -porttiskannauksen tulos (Gibson Research Corporation 2017.)

ShieldsUp:n avulla verkkoja voidaan testata monien eri haavoittuvuuksien varalta. Kuvassa 16 ovat näkyvissä ShieldsUPin eri skannausvaihtoehdot, joita voidaan verkkosivulla suorittaa.



Kuva 16. ShieldsUP - skannausvaihtoehdot (Gibson Research Corporation 2017.)

Palvelua voi käyttää myös siten, että skannattavan portin numero annetaan suoraan osoiterivillä: http://www.grc.com/port_**port**.htm
Portti 22 muodossa http://www.grc.com/port_22.htm. Kuvassa 17 esimerkki hausta, jossa on skannattu portti 22.



Kuva 17. ShieldsUP – porttiskannaus – portti 22 (Gibson Research Corporation 2017.)

Valitsemalla sivun yläosasta toiminnon ”Probe this Port” saa tietää, onko portti auki internetiin päin.

3.2 IoT-tietoturvalaitteita kuluttajille tai pienyrityksille

Tällä hetkellä kuluttajille on tarjolla monenlaisia IoT-laitteiden tietoturvaa parantavia laitteita. Yhteistä näille tuntuu kuitenkin olevan se, että toimitusaikataulut venyvät. Monet laitteista on esitelty jo muutama vuosi sitten, mutta toimitukset eivät ole vieläkään alkaneet. Monet tietoturvayritykset ovat lähteneet mukaan IoT-tietoturvan parantamiseen. On olemassa kodin reitittimeen kytkettäviä tietoturvalaitteita, kodin reitittimenä toimivia tietoturvalaitteita, tietoturvayhtiöiden ohjelmistoilla lisättyjä tietoturvalaitteita. Eli laitteiden ja ohjelmistojen kirjo on suuri. Opinnäytetyön tässä luvussa käydään läpi tulossa olevia ja myynnissä olevia tietoturvalaitteita.

3.2.1 Bitdefender Box

Yksi vaihtoehto kodin IoT-laitteiden (sekä myös muiden laitteiden) suojaamiseen on tietoturvayritys Bitdefenderin tuote Bitdefender Box, kuten kuvassa 18. Sen kerrotaan suojaavan kaikki kodin internetiin liitetyt laitteet käyttöjärjestelmästä riippumatta, myös kodin ulkopuolella. Laite liitetään kodin reitittimeen, jossa se ikään kuin luo uuden, ylimääräisen turvatason kodin laitteille.

Kuva 18. Bitdefender Box (Tom’s Guide)

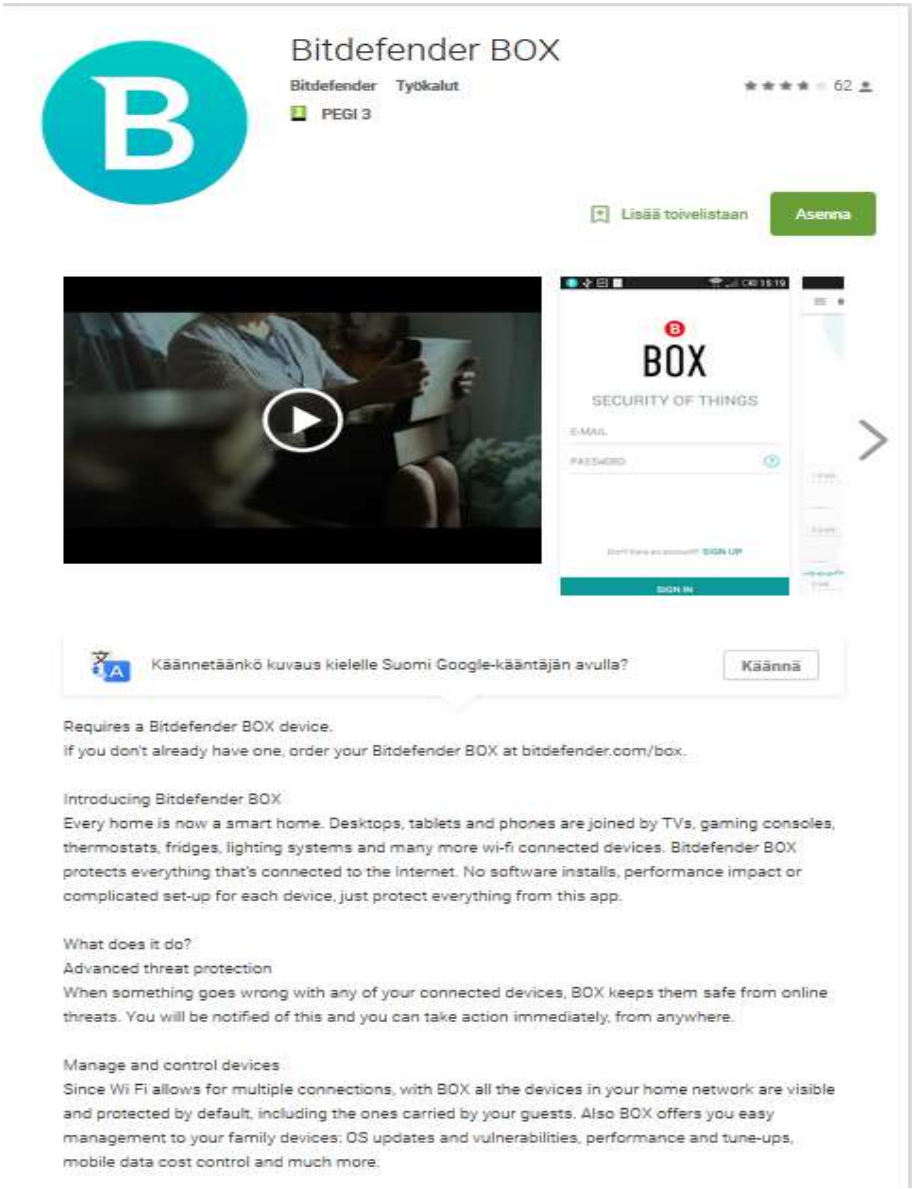
Bitdefender Box suojaa verkon käyttäjää neljällä tavalla suodattamalla epäilyttävät URL-osoitteet perustuen valmistajan tietokantaan. Se myös tutkii kodin kaikkien verkkoon liitettyjen laitteiden mahdolliset haavoittuvuudet joka 3:n päivän välein. Samalla se tarkistaa salasanojen vahvuudet, laiteohjelmiston ajantasaisuuden, sekä mahdolliset muut heikkoudet. Laitteen mukana tulee käyttöoikeus Bitdefender Total Security -turvaohjelmistoon, sekä Private Line VPN -palveluun, jolla käyttäjät voivat muodostaa luotetun yhteyden myös kodin ulkopuolella. (Nadel B. 2016).

Bitdefender Box -laitteella on hintaa noin 199$, ja laitteella saa suojattua rajattoman määrän laitteita kodissa. Kannattaa ottaa huomioon muuta-

mia laitteen rajoittavia ominaisuuksia, esimerkiksi se, että Box ei ole yhteensopiva kaikkien reitittimien kanssa. Laitetta käytettäessä verkon nopeus on enintään 100Mbps. Mukana tulevaa Total Security -turvaohjelmistoa ei voi asentaa Applen puhelimiin tai tabletteihin. Box ei myöskään turvaa reitittimen vierasverkkoja. (Nadel B. 2016).

Laite on myynnissä toistaiseksi vain USA:ssa. Laite on tulossa myyntiin muuallakin - aikataulu on vielä auki. Laite toimii vuosiveloituksella (99$ - jolla voidaan turvata rajaton määrä laitteita, eikä tämän lisäksi tarvita muita palomuuri- tai virustorjuntaohjelmistoja). Laite ei itsessään toimi WiFi-reitittimenä, vaan sen lisänä. (Nadel B. 2016).

Kuvassa 19 Bitdefender Boxin puhelimeen tai tablettiin ladattava ohjelmisto Google Play -kaupassa.



Kuva 19. Bitdefender Box Android-ohjelmiston lataussivu (Google Play 2017.)

3.2.2 F-Secure Sense

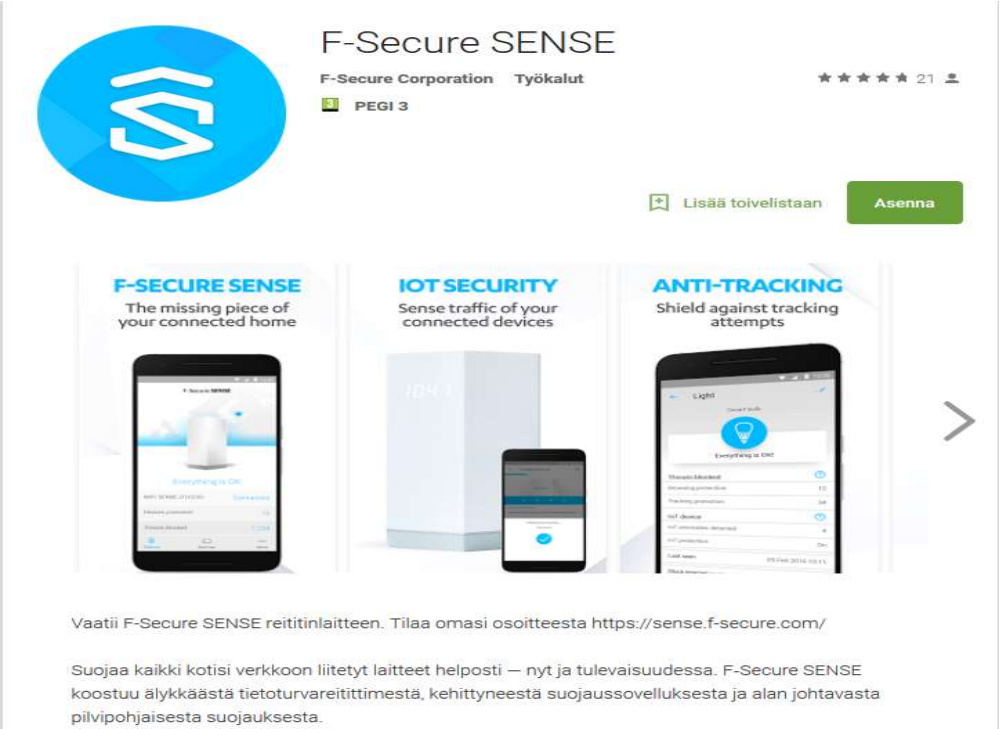
Kotimaisen F-Securen vastaus kodin tietoturvakisaan on Sense. Laite on alun perin julkistettu jo vuonna 2015, mutta se on tullut vastikään (06/2017) myyntiin. Valmistajan mukaan laite toimii reitittimenä ja se turvaa kodin kaikkien laitteiden yhteydet kodissa ja kodin ulkopuolella, myös IoT-laitteet. Laite tunnistaa verkkoon liitetyt laitteet verkkokäyttäytymisen perusteella ja estää haitalliset yhteydet laitteisiin -tai laitteista. Laite tarjoaa kolmitasoista suojaa. Ensinnä se on älykäs reititin, joka turvaa kodin laitteet verkkouhkien varalta. Toiseksi laitteen sovellus hallinnoi kotiverkkoa ja suojaa laitteet. Kolmanneksi laitteessa on vielä pilvipohjainen suojaus, joka suojaa kotiverkon reaaliaikaisesti uusien uhkien uhatessa. Kuvassa 20 F-Secure Sense-laite.

Kuva 20. F-Secure Sense (F-Secure)

Suomessa laitetta pystyy ostamaan joko suoraan F-Securen verkkokaupasta, tai Elisalta. Hinnaltaan se on samaa luokkaa -kuin muut vastaavat tuotteet, 199 € sisältäen itse laitteen ja tietoturvapalvelut ensimmäisen vuoden ajaksi. Ensimmäisen vuoden jälkeen tietoturvapalveluiden veloitus on 9,90 €/kk. Laitetta voi kuitenkin myös käyttää tavallisena reitittimenä, ilman erillisiä tietoturvapalveluita. Sense tukee IEEE 802.11a/b/g/n/ac 2.4GHz ja 5GHz, AC 1750 -WLAN-verkkoja. (F-Secure - Sense n.d.)

Laitteen ohjaamiseen tarvittavaa F-Secure Sense-sovellusta pystyy käyttämään iOS- tai Android-käyttöjärjestelmän omaavalla puhelimella tai tabletilla.

Kuvassa 21 Google-kaupan näkymä F-Secure Sensen Android-ohjelmiston lataussivusta.



Kuva 21. F-Secure Sense Android-ohjelmiston lataussivu (Google Play 2017.)

3.2.3 Norton Core

Hieman tavallisuudesta poikkeavasti muotoiltu Norton Core turvaa kaikki kodin internetiin kytketyt laitteet (kuten edelliset, myös IoT-laitteet). Core tutkii verkon IoT-laitteet ja tunnistaa niiden mahdolliset haavoittuvuudet, sekä suojaa ne uhkia vastaan. Kuvassa 22 Norton Core -laite.

Kuva 22. Norton Core (Symantec Corporation)

Corea voidaan käyttää myös pelkkänä WiFi-reitittimenä ilman erillisiä tietoturvaominaisuuksia. Hintaa laitteella on arviolta 279,90 $ sisältäen tietoturvaohjelmiston vuodeksi enintään 20:lle Windows, Mac OS, Android, iOS - tai rajattomalle määrälle IoT-laitteita. Ensimmäisen vuoden jälkeen palvelun kuukausiveloitus on 9,99 $. Core on ennakkotilattavissa USA:ssa (tulossa myös muualle - aikataulu vielä auki).

Core-laite on reitittin lisättynä Nortonin tietoturvaohjelmistoilla. (Symantec Corporation - Norton Core features n.d.).

3.2.4 Cujo

Sympaattisen näköinen Cujo -älykäs palomuurilaite suojaa valmistajan mukaan kodin kaikki internetiin kytketyt laitteet (myös IoT-laitteet). Kuvassa 23 esimerkki Cujo-laitteen muotoilusta.

Kuva 23. Cujo

Cujo kytketään reitittimeen, se ei toimi itsenäisesti reitittimenä. Se seuraa kodin verkkoliikennettä reaaliajassa ja lähettää tilastotiedot pilvipalveluun tutkittavaksi mahdollisten uhkien varalta (anonyymisti).

Kuvassa 24 Cujon Android-sovellus Google Play-kaupassa.

Kuva 24. Cujo Android-sovelluksen lataussivu (Google Play 2017.)

Cujo-laitteen hinta on 99$. Jotta palveluita voidaan käyttää, on laitteen hinnan lisäksi maksettava joko kk-veloitus 8,99$, vuosiveloitus 59$ tai 150$ kertaveloitus. Tuote on myynnissä - toimitukset maailmanlaajuisesti (Cujo n.d.)

3.2.5 Keezel

Hollantilaisen yrityksen tuote Keezel, joka tarjoaa sananmukaisesti verkon tietoturvaa kaikille, on käytännössä langaton VPN-laite. Sen avulla voidaan muodostaa salattu VPN (Virtual Private Network) -yhteys kotona, hotellissa, tai missä tahansa, missä verkkoyhteys on käytettävissä. Keezel kytkeytyy saatavilla olevaan WiFi-verkkoon, jonka jälkeen liikenne kulkee sen VPN-yhteyden läpi, salattuna. Kahden Keezel-laitteen avulla voidaan muodostaa salattu yhteys verkon yli. Laitteen avulla kodin IoT-laitteet voidaan eristää muusta verkosta, ja näin voidaan estää mahdollisia hyökkääjiä pääsemästä käsiksi kodin muihin laitteisiin. (Sayer P. 2016).

Kuvassa 25 Keezel VPN-laite.

Kuva 25. Keezel (Keezel 2017.)

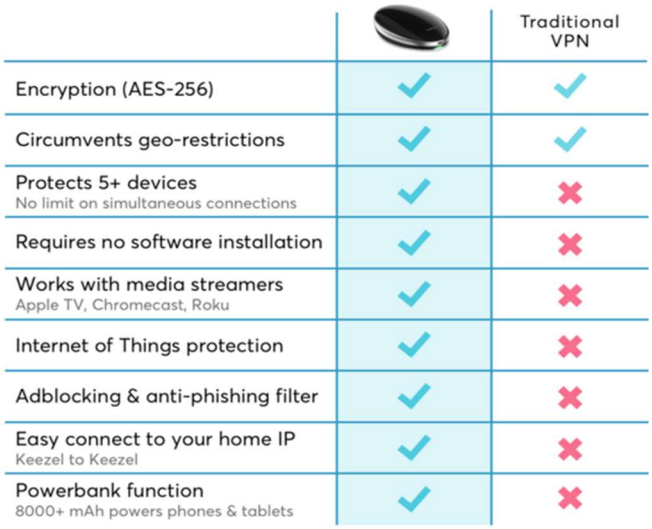
Keezelin hinnat alkaen -versio maksaa 144$, tällä hinnalla mukaan tulee yksi Keezel-laite. Perusversion hinnalla laite toimii vain 500 kbps -nopeudella, eli se ei sovellu esimerkiksi HD-videoiden katseluun, sen sijaan sähköpostin lukemiseen ja kevyeen nettiselailuun versio sopii. Myös VPN-palveluntarjoaja tulee asiakkaan itse löytää ja määrittää. Laite on päivitettävissä ohjelmallisesti parempaan ohjelmistopakettiin - ilman koko laitteen vaihtoa.

Hieman kalliimmassa versiossa (229$) mukaan tulee yksi Keezel-laite, sekä Premium-palvelu (käytettävissä 3 eri VPN-palveluntarjoajaa) kahdeksi vuodeksi. Tässä versiossa itse laitteen nopeutta ei ole rajoitettu, tosin se riippuu käytettävän WiFi-verkon nopeudesta. Kahden vuoden jälkeen Premium-palveluiden käyttöä voi jatkaa hintaan 5$/kk.

Kalleimmalla versiolla (05/2017 hinta 479 $) Keezel sisältää samat ominaisuudet, kuin edellinen versio, mutta Premium-palvelut ovat käytettävissä laitteen elinkaaren loppuun asti ilman lisäveloitusta.

Keezel on tällä hetkellä ennakkotilattavissa, toimitukset alkavat valmistajan ilmoituksen mukaan syyskuussa 2017. (Keezel n.d.).

Kuvassa 26 Keezelin vertailua tavanomaiseen VPN-palveluun.



Kuva 26. Keezel vs tavallinen VPN (Keezel 2017.)

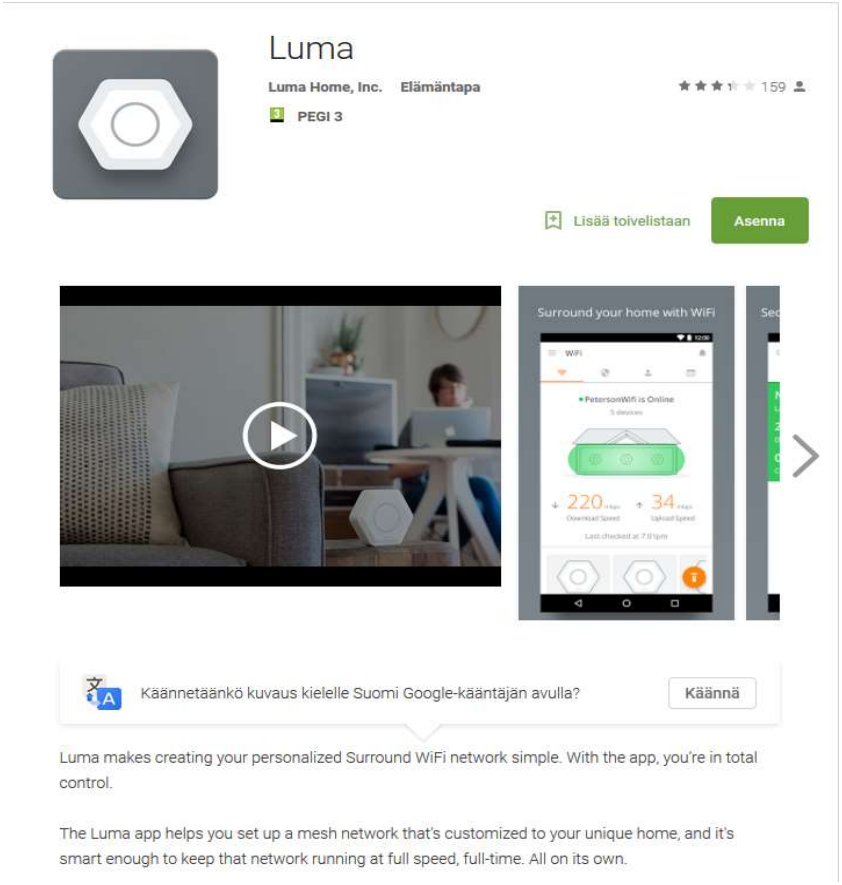
3.2.6 Luma

Luma on älykäs WiFi-reititin, joka tarjoaa yritystason tietoturvaa kotiin ja luo niin sanotun Mesh-verkon (reitittävä langaton verkko). Järjestelmään kuuluu 3 langatonta reititintä, jotka toimivat yhdessä/yhtenä. Ne muodostavat yhdessä kodin langattoman verkon, jonka yhteys ei katkea tai heikenny missään kohdassa. Luman mobiilisovellus jopa auttaa käyttäjää sijoittamaan reitittimet parhaaseen mahdolliseen paikkaan. Kuvassa 27 Luma -laite.

Kuva 27. Luma (Luma Home Inc. 2017.)

Luma suojaa myös IoT-laitteet. Mikäli IoT-laite joutuu haittaohjelman saastuttamaksi, täytyy sen kuitenkin olla yhteydessä saastuneeseen serveriin tai ohjausjärjestelmään, jotta verkkorikollinen voi toteuttaa palvelunestohyökkäyksiä tai muita ikäviä toimenpiteitä. Luma havaitsee väärinkäytöksen ja estää kyseisen laitteen verkkoliikenteen. Luma tarkkailee jatkuvasti verkon tilannetta mahdollisten turvallisuusriskien varalta, sekä etsii laitteita, joiden oletussalasana on jätetty vaihtamatta, tai jotka on muuten konfiguroitu väärin. (Dickson B. 2016).
Tällä hetkellä (05/2017) 2 kpl Luma-laitteita sisältävä paketti on hinnaltaan 249$, 3:n laitteen paketti taas 349$. (Luma Home Inc. n.d.).

Kuvassa 28 Luma-sovellus Android-laitteille Google Play-kaupassa.

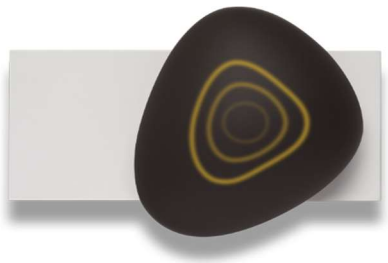


Kuva 28. Luma Android-sovelluksen lataussivu (Google Play 2017)

3.2.7 Dojo

Dojo on Israelilaislähtöisen Dojo Labs:n (joka on nykyään brittiläisen BullGuard internet-turvayhtiön omistama) kehittämä kodin reitittimeen kytkettävä palomuurilaite. Kun laite on kytketty reitittimeen, kaikki liikenne kulkee Dojon kautta ja se tarkkailee kaikkea verkon liikennettä ja laitteita. Tämän perusteella laite analysoi mahdolliset uhat ja lisäksi lähettää metadatan analysoitavaksi pilvipalveluun.

Näiden tulosten perusteella laite hälyttää sekä varoitusvaloilla (laitteen valo muuttuu verkon turvatilanteen mukaan vihreäksi, oranssiksi tai punaiseksi), että myös mobiilisovelluksessa. Kuvassa 29 Dojo-laite.



Kuva 29. Dojo (Dojo Labs)

Dojo hyödyntää koneoppimista, käytännössä mitä enemmän verkkodataa pilvipalveluun saadaan, sitä paremmin laitteet pystyvät ennakoimaan uhkia. IoT-laitteilla on yleensä yksi hyvin yksinkertainen toimintatapa, tai tehtävä. Yksinkertaistettuna Dojo luo tämän perusteella oletusarvon siitä, mitä kyseinen laite tekee ja miten. Jos laitteen käytöskuvio muuttuu, paljastuu mahdollinen haittaohjelma helposti. Laite on tällä hetkellä (05/2017) ennakkotilattavissa. (Lomas N. 2015).

3.3 IoT-tietoturvalaitteita yrityksille

3.3.1 Tosibox Lock 200

Tosibox on kotimainen VPN (Virtual Private Network) -yhteyksiin tarkoitettujen laitteiden ja ohjelmistojen valmistaja. Tosibox Lock 200 on valmistajan mukaan helppokäyttöinen palomuurilaite. Se on täysin yhteensopiva muiden Tosibox-laitteiden kanssa. Kaikkiin siihen kytkettyihin laitteisiin voidaan muodostaa suojattu VPN-yhteys internetin yli Tosibox Key 100/200-laitteilla. Näin pystyt esimerkiksi muodostamaan suojatun yhteyden IoT-laitteeseen internetin yli. Kuvassa 30 Tosibox Lock 200 -laite.

Kuva 30. Tosibox Lock 200 (Tosibox Oy 2017.)

Laitteen ominaisuuksia ovat mm. VPN-yhteys enintään 15 Mb/s -nopeudella, sisäänrakennettu palomuuri, se tukee enintään 50 samanaikaista

VPN-yhteyttä. Laite tukee myös mobiiliyhteyksiä 3G/4G-modeemin välityksellä, joko Tosibox:n omien ja eräiden muiden valmistajien tuotteiden. (Tosibox Lock 200 n.d.)

Kuvassa 31 on näkymä siitä, miten Tosibox Lock ja Tosibox Key -laitteilla voidaan muodostaa VPN-yhteys internetin yli.

Kuva 31. Tosibox Lock 200 - kuvaus (Tosibox Oy 2017.)

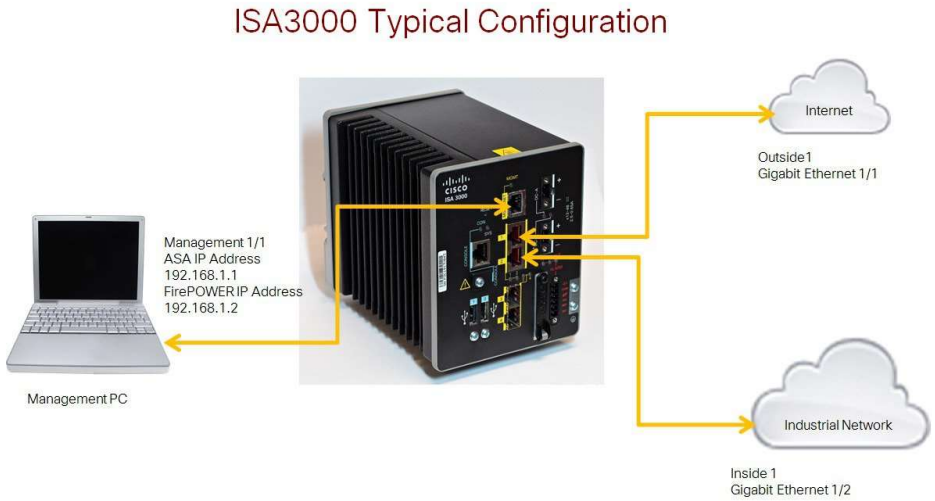
3.3.2 Cisco 3000 Series Industrial Security Appliances (ISA)

Cisco 3000 Series Industrial Security Appliances (ISA) on palomuurilaite järeään teollisuuskäyttöön. Oikein asennettuna se täyttää mm. seuraavien teollisten standardien määritykset: NERC-CIP, ISA 99, ISA 62443, CFATS, ANSI/AWWA G430. Yhdellä ohjelmistolla pystytään hallitsemaan satoja yhteyksiä. (Cisco Systems Inc. n.d.)

Kuvassa 32 esimerkki Cisco 3000-sarjan ISA-laitteesta.

Kuva 32. Cisco 3000 Series Industrial Security Appliances (Cisco Systems Inc. 2017.)

Kuvassa 33 tyypillinen Cisco 3000-sarjan ISA-laitteen kokoonpano.



Kuva 33. Cisco 3000 ISA tyypillinen kokoonpano (Cisco Systems Inc. 2017.)

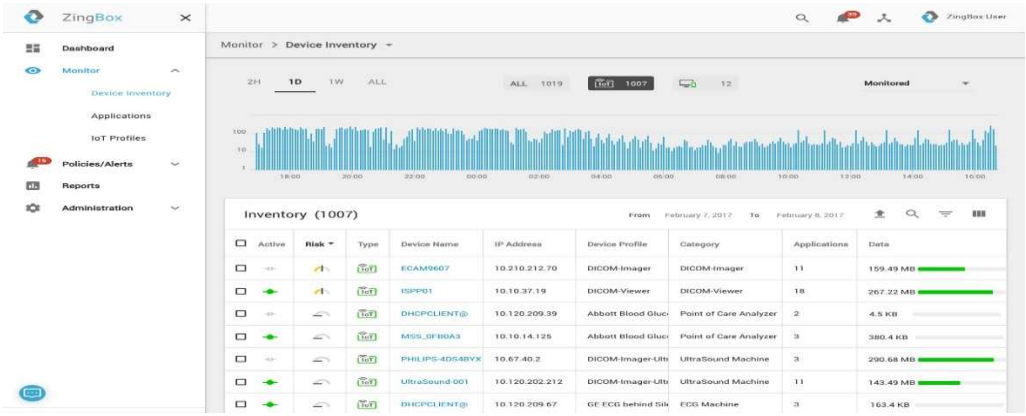
3.4 IoT-tietoturvaohjelmistoja yrityksille

Erilaisten tietoturvaohjelmistojen avulla yritys pystyy suojaamaan IoT-laitteensa ja niiden käyttämät yhteydet. Ohjelmistojen etuna on se, että ne eivät ole laite- eivätkä paikkasidonnaisia, toisin sanoen ohjelmiston avulla pystytään valvomaan suurempaa määrää erilaisia laitteita ilman, että ne on fyysisesti kytketty yhteen tiettyyn (esimerkiksi VPN-, tai palo-muurilaitteeseen).

3.4.1 ZingBox IoT Guardian

ZingBox IoT Guardian suojaa yritysverkon IoT-laitteita seuraamalla niiden käytöstä ja analysoimalla sitä erilaisten algoritmien avulla.

Kuvassa 34 näkymä ZingBox IoT Guardianin hallintaruudusta.

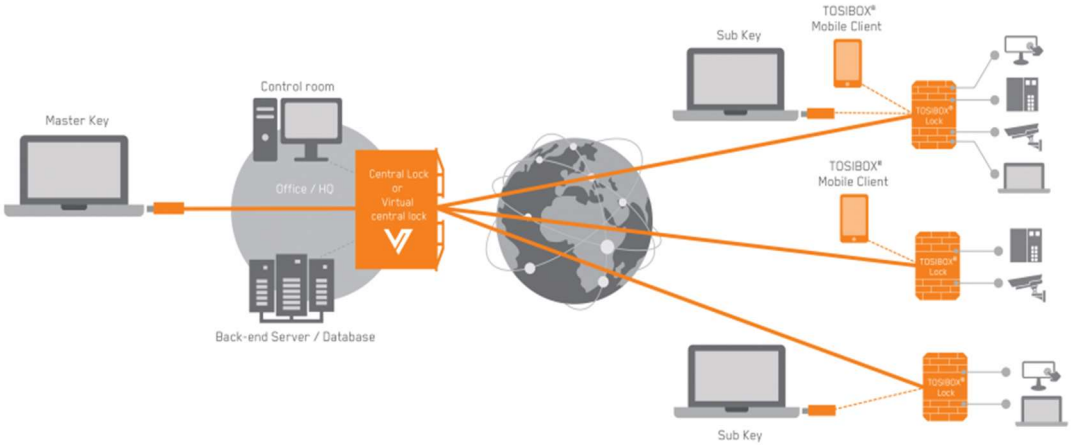


Kuva 34. Zingbox IoT Guardian - näkymä (Zingbox Inc. 2017.)

ZingBox IoT Guardian varoittaa heti, mikäli jokin laite ei toimi odotetulla tavalla ja suosittelee toimintatapoja vääränlaisen toiminnan korjaamiseksi. (ZingBox Inc. n.d.)

3.4.2 Tosibox Virtual Central Lock (VCL)

Avoimet yhteydet ovat IoT-maailmassa aina suuri riski. Tosibox VCL on tietoturvallinen etäyhteysratkaisu, joka toimii yhdessä muiden Tosibox:n tuotteiden kanssa. Sen avulla voidaan muodostaa VPN-yhteyksiä yksittäisistä satoihin tai jopa tuhansiin. Kuvassa 35 esimerkki Tosibox VCL-laitteen toimintaperiaatteesta.



Kuva 35. Tosibox Virtual Central Lock (Tosibox Oy 2017)

Tosibox VCL voidaan asentaa joko VMWare ESXi, Microsoft Hyper-V, tai Linux KVM (Kernel based Virtual Machine) -alustoille. Virtuaalisuutensa ansiosta se voidaan asentaa esimerkiksi toimistoverkkoon tai pilvipalveluun. Ominaisuuksiin kuuluu myös mahdollisuus tarkkailla VPN-yhteyksiä. (Tosibox VCL n.d.)

3.4.3 Cisco IoT Threat Defense

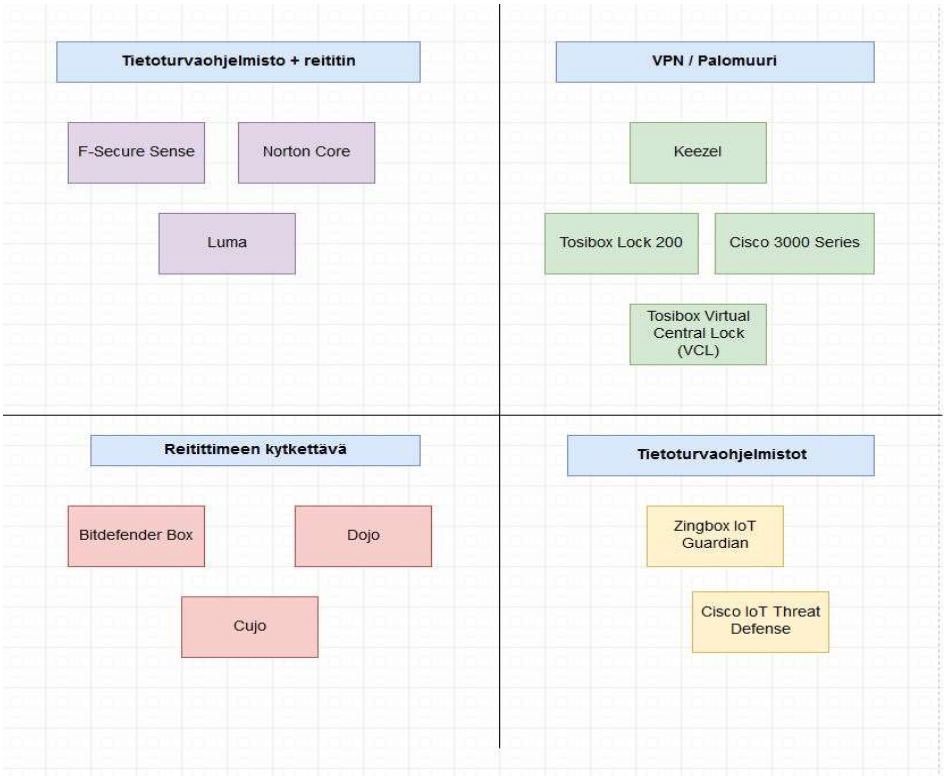
Verkkolaitevalmistaja Ciscon vastaus IoT:n tietoturvaan on Cisco IoT Threat Defense. Valmistajan mukaan IoT-laitteiden suoja on olematon, tai valmistajat ovat vasta suunnittelemassa suojausta laitteisiin. Tämän vuoksi on siis tällä hetkellä käytettävä ulkoisia ohjelmia IoT-laitteiden suojaukseen, jonka lisäksi ne on suojattava ja eristettävä muusta verkosta muutenkin, kuin vain VLAN:n (Virtual LAN) avulla.

IoT Threat Defense sisältää laitteiden turvaksi monia eri turvakerroksia, kuten kuvassa 36 on esitelty.

Kuva 36. Cisco IoT Threat Defense (Cisco Systems Inc. 2017.)

Ciscon tuotteen paketissa mukana ovat Cisco Identity Services Engine käyttäjien ja laitteiden hallintaan, Cisco Stealthwatch verkon valvontaan ja turvaamiseen, Cisco Umbrella pilvipalvelu verkon turvaksi ja Cisco AnyConnect turvallisten VPN-yhteyksien muodostamiseen. Näiden lisäksi paketissa tulevat Ciscon seuraavan sukupolven (Firepower-sarja) palomuurilaitteet. (Cisco IoT Threat Defense n.d.)

Kuvassa 37 vielä yhteenveto eri IoT-tietoturvalaitteiden- ja ohjelmistojen ominaisuuksista.



Kuva 37. Yhteenveto IoT-tietoturvalaitteiden ominaisuuksista

4 IOT-HAITAKKEET/HAAVOITTUVUUDET

Varmasti lähes kaikki ovat lukeneet kauhuesimerkkejä siitä, miten ei tulisi määritellä IoT-laitteen tietoturvaa. Tästä on olemassa lukuisia esimerkkejä, kuten esimerkiksi roskapostia lähettävä jääkaappi… Tulevaisuuden, tai ehkä jo nykyisyyden kauhuskenaarioita on monenlaisia. Esimerkkinä vaikka internetiin kytketty kahvinkeitin, jonka toimintaa verkkomurtautuja voisi muuttaa esimerkiksi siten, että se on jatkuvasti päällä ja pahimmassa tapauksessa aiheuttaa tulipalon. Haitakkeet voivat myös aiheuttaa DDoS-hyökkäyksen muodossa tiettyjen palveluiden tai sivuston toimimattomuuden, aiheuttaen suurta taloudellista haittaa. IoT-laitteiden ja järjestelmien riittävä suojaus on siis erittäin tärkeää.

Erityisesti kuluttajille suunnattujen IoT-laitteiden valmistaja on yleensä jokin kodinkonevalmistaja, tai sopimusvalmistaja, jolla ei välttämättä ole käsitystä siitä, miten laitteen tietoturva tulisi suunnitella. Tällöin laite on alttiina erilaisille hyökkäyksille verkon suunnasta. Seuraavassa muutamia viime vuosien tunnetuimpia IoT-haitakkeita.

4.1.1 BrickerBot

Tuorein (03/2017) IoT-laitteiden uhka on Radware-yhtiön löytämä haitta-ohjelma nimeltään Brickerbot. Kyseinen haitake toimii siten, että se rampauttaa kohdelaitteen DDoS:n (Distributed Denial of Service) sijaan aiheuttamalla niin sanotun ”Pysyvän palvelunestohyökkäyksen - Permanent Denial-of-Service (PDoS)”. Haitake on suunnattu erityisesti BusyBox-pohjaisella Linux-käyttöjärjestelmällä toteutettuihin IoT-laitteisiin. Yhteinen nimittäjä hyökkäyksen kohteena oleville laitteille oli, että portti 22 (SSH-portti) oli auki internetiin päin, jonka lisäksi laitteella pyöri vanhentunut versio SSH-serveristä (Dropbear). Tämä edellyttää kuitenkin myös sitä, että laitteen salasanaa ei ole muutettu.

Tartuttuaan laitteeseen Brickerbot suorittaa joukon Linux-komentoja, joilla se tuhoaa verkkoliitettävyyden, tiedostojärjestelmän sekä tämän päälle vielä pyyhkii kaikki tiedostot kohdelaitteesta. Kuvassa 38 esimerkki siitä, mitä komentoja kyseinen haitake suorittaa kohdelaitteessa.

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Kuva 38. BrickerBot -komennot (Radware Ltd)

Hyökkäyksen jälkeen laite lakkaa toimimasta, eli muuttuu kuten haittaohjelman nimikin kertoo, ”tiiliskiveksi”, eli pahimmassa tapauksessa täysin käyttökelvottomaksi. Lievemmissä tapauksissa laite voidaan vielä saada toimintaan asentamalla käyttöjärjestelmä uudelleen. Tämä kuitenkin aiheuttaa ylläpitäjille turhaa työkuormaa.

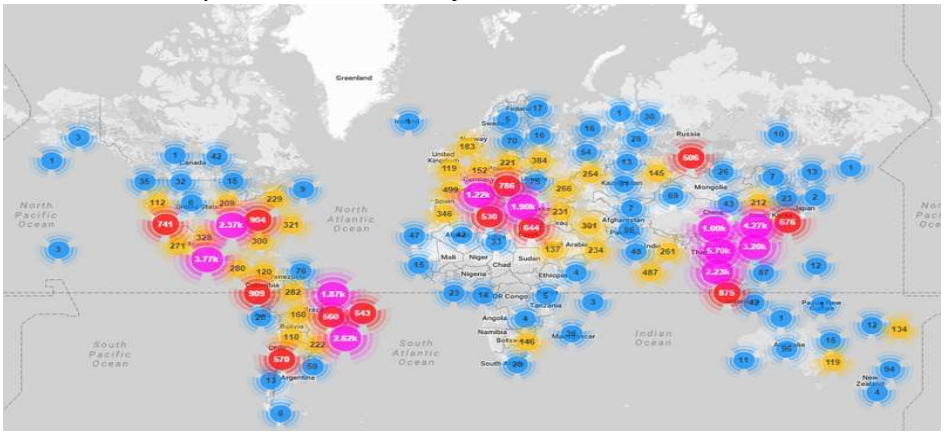
Tällä hetkellä Brickerbot-haitakkeesta tunnetaan jo versiot 1 ja 2. (Radware Ltd. 2017)

4.1.2 Mirai

Mirai-bottiverkkoa tiedetään käytetyn ensimmäisen kerran journalisti Brian Krebs:n sivuston kaatamisessa 20. syyskuuta 2016. Tämän jälkeen suuremmassa mittakaavassa esimerkiksi DDoS (Distributed Denial-of-Service attack) -palvelunestohyökkäyksessä DNS-palveluntarjoaja Dyn:iä vastaan 21. lokakuuta 2016. Tästä seurasi pitkiäkin katkoksia suurten toimijoiden, kuten esimerkiksi Netflix, PayPal, Spotify, Twitter, Starbucks, CNN jne. -sivustoilla, erityisesti Yhdysvalloissa.
Krebs B. (2016).

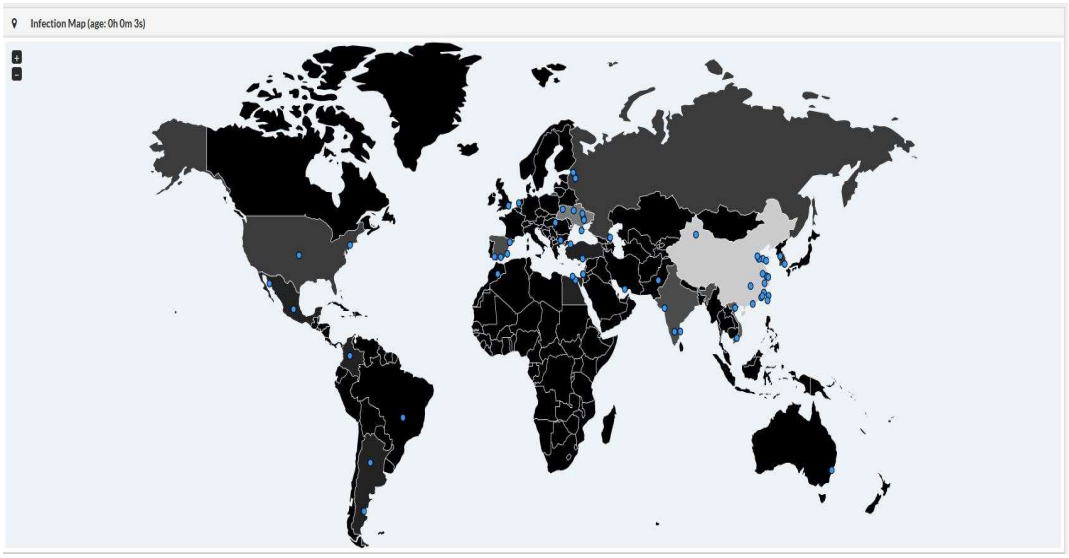
Miten Mirai-bottiverkko toimii tai muodostuu? Mirai käyttää muiden haitakkeiden tavoin kohteenaan IoT-laitteita, joiden käyttäjätunnusta tai oletussalasanaa ei ole muutettu. Mirai hyökkää ensisijaisesti reitittimiin, digibokseihin, valvontakameroihin, sekä muihin internetiin kytkettyihin laitteisiin. Mirai pyrkii niin sanotun Brute force-hyökkäyksen avulla arvaamaan salasanoja ja käyttäjätunnuksia (niin sanottu sanakirjahyökkäys - Dictionary attack). Tällaisessa hyökkäyksessä ohjelma yrittää arvata yksinkertaisia käyttäjätunnuksia (kuten admin, root jne.) ja salasanoja (kuten admin, 123456, default jne). Saatuaan tarpeeksi suuren määrän kohdelaitteita haltuunsa, Mirai käynnistää palvelunestohyökkäyksen tiettyä sivustoa tai toimijaa vastaan. (Herzberg B., Bekerman D., Zeifman I 2016).

Kuvassa 39 näkymä siitä, miten laajalti Mirai levisi alkuvaiheessa:



Kuva 39. Mirai – levinneisyys (Imperva Inc.)

Kuten kuvassa 40 voidaan nähdä, huhti-toukokuun 2017 aikana Mirai:n levinneisyys oli huomattavasti aiempaa vähäisempää.



Kuva 40. Mirai levinneisyys 17.05.2017 viime 30pv (Intel MalwareTech)

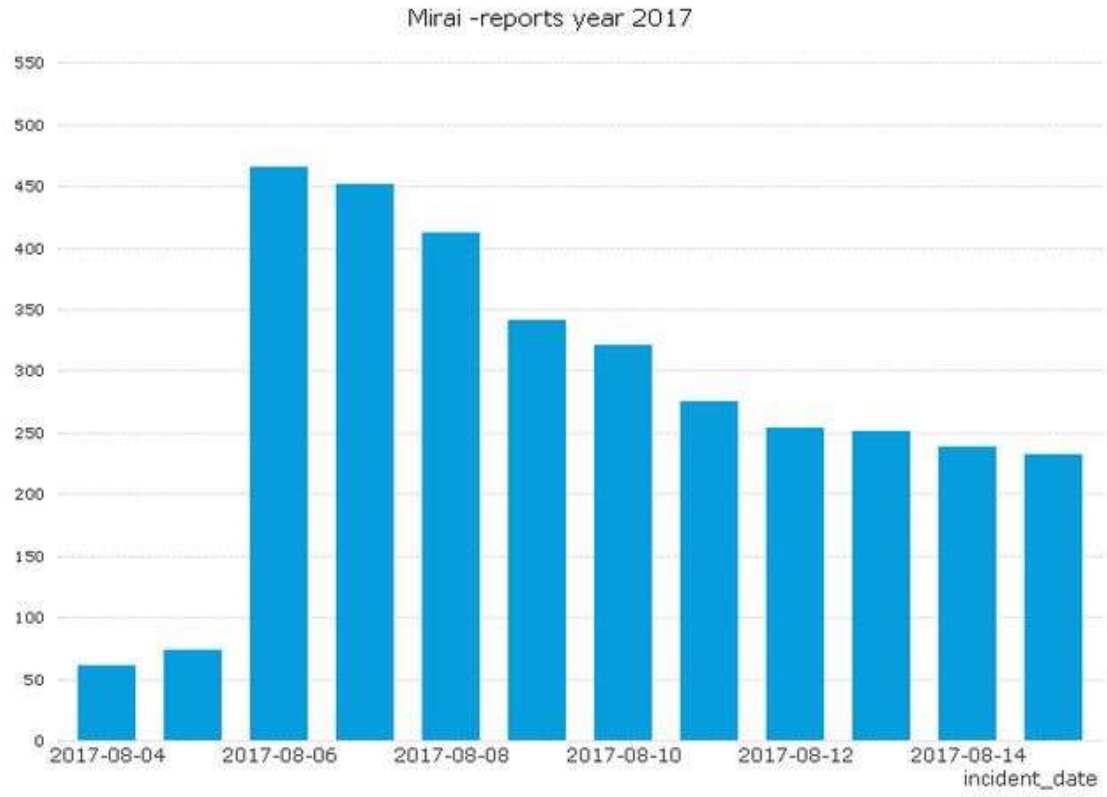
Kuvassa 41 esimerkkejä siitä, millaisia käyttäjätunnus/salasanayhdistelmiä Mirai etsii.

```
root      xc3511
root      vizxv
root      admin
admin     admin
root      888888
root      xmhdipc
root      default
root      juantech
root      123456
root      54321
```

Kuva 41. Mirai - käyttäjätunnus/salasanayhdistelmät (Imperva, Inc.)

Haittaohjelma etsii toisaalta valmistajan määrittämiä, muuttamatta jääneitä käyttäjätunnus/salasana -yhdistelmiä, sekä erittäin yksinkertaisia salasanoja. Käyttäjän kannattaa siis ehdottomasti nähdä hieman vaivaa IoT-laitteen käyttäjätunnuksen ja salasanan vaihdossa ja luomisessa, sekä myös muistaa määrittää tarpeeksi vaikeasti arvattava käyttäjätunnus/salasana-yhdistelmä. Mirai-haittaohjelman pystyy poistamaan laitteelta yksinkertaisesti käynnistämällä sen uudestaan. Mutta se tarttuu nopealla aikataululla uudestaan, mikäli oletuskäyttäjätunnusta ja salasanaa ei vaihdeta.

Mirai ei kaikesta huolimatta kuitenkaan ole katoamassa mihinkään. Viestintäviraston viimeisimmän tiedotteen mukaan kyseisen haittaohjelman tartunnat ovat elokuun 2017 aikana olleet taas noususuhdanteessa, kuten kuvasta 42 ilmenee. Kannattaa siis edelleen pitää huolta siitä, että verkkoon kytkettyjen laitteiden salasanat eivät ole valmistajan määrittämät. (Viestintävirasto 2017).



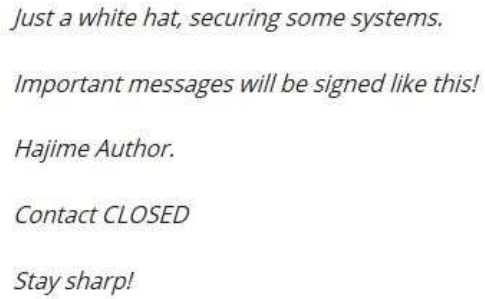
Kuva 42. Mirai – levinneisyys 08/2017 (Viestintävirasto 2017.)

4.1.3 Hajime

Hajime on haittaohjelma, jota on ensimmäisen kerran tavattu lokakuussa 2016. Kyseessä on huomattavasti Miraita vaikeammin löydettävä haitake. Hajimen kommunikointi tapahtuu hajautetussa P2P (Peer-to-Peer) -vertaisverkossa. Myös se hyökkää IoT-laitteisiin, jotka on varustettu BusyBox-Linuxilla. Edellytyksenä hyökkäykselle on se, että Telnet-portti (portti 23) on avoinna ja käyttäjätunnus ja salasana ovat alkuperäiset, valmistajan määrittämät.

On myös esitetty arvailuja, että Hajime voisikin olla vastaisku Mirai-bottiverkkoa vastaan, koska se tavallaan parantaa hyökkäyksen kohteena olevan IoT-laitteen suojausta. Tästä ei kuitenkaan ole olemassa täyttä varmuutta. Tartuttuaan Hajime estää pääsyn portteihin 23 (Telnet), 5358 (WSDAPI), 5555 (Oracle WebCenter Content), 7547 (CWMP), joihin taas Mirai-haittaohjelma yleisimmin hyökkää.

Hajime-haittaohjelmalla ei myöskään tällä hetkellä tiedetä olevan mitään DDoS (Distributed Denial of Service) -ominaisuuksia. Haitake näyttää kuvassa 43 näkyvän viestin pääteohjelmassa noin 10 minuutin välein. (Grange, W 2017)



Kuva 43. Hajime - ilmoitus käyttäjälle (Symantec Corporation)

5 IOT-LAITTEIDEN SUOJAUS (PARHAAT KÄYTÄNNÖT)

Tutustu IoT-laitteen kaikkiin ominaisuuksiin ja erityisesti turvaominaisuuksiin ennen ostamista.

Muuta käyttöönoton yhteydessä kaikkien IoT-laitteiden oletussalasanat ja/tai käyttäjätunnukset.

Muuta IoT-laitteiden salasanat säännöllisin väliajoin.

Käytä tarpeeksi vahvoja salasanoja (tulisi sisältää ainakin isoja ja pieniä kirjaimia, numeroita, erikoismerkkejä).

Tarkista erityisesti, että IoT-laitteen portit 22 (SSH), 23 (Telnet) ja 80/443 (HTTP/HTTPS) eivät ole auki internetiin päin.

Tarkista IoT-laitteen laiteohjelmiston (firmware) mahdolliset päivitykset valmistajan sivuilta säännöllisin väliajoin.

Poista käytöstä kaikki palvelut ja ominaisuudet, joita et tarvitse.

Milloin mahdollista, suosi langallista yhteyttä langattoman sijaan.

Estä IoT-laitteen etäkäyttömahdollisuus.

Poista laitteelta kaikki tarpeettomat käyttäjätunnukset.

Testaa verkkosi mahdollisten haavoittuvuuksien ja avointen porttien varalta (ShieldsUP, Shodan, Wireshark jne. avulla).

Käytä VPN-yhteyksiä, älä koskaan liitä IoT-laitetta suojaamattomana internetiin.

Tunne ja tunnista kaikki verkkosi IoT-laitteet.

Poista käytöstä reitittimen Universal Plug and Play (UPnP) -ominaisuus.

Eristä IoT-laitteet muusta (kodin) verkosta omaan suojattuun verkkoonsa.

Estä ulkopuolisten fyysinen pääsy IoT-laitteelle.

Sammuta laitteet ajoittain (päästäksesi eroon laitteen muistissa mahdollisesti olevista haittaohjelmista).

Seuraa tietoturvayritysten (McAfee, F-Secure, Kaspersky Lab, Symantec ym.) ja Viestintäviraston viimeisimpiä tietoja haittaohjelmista.
(McAfee Labs 2017)

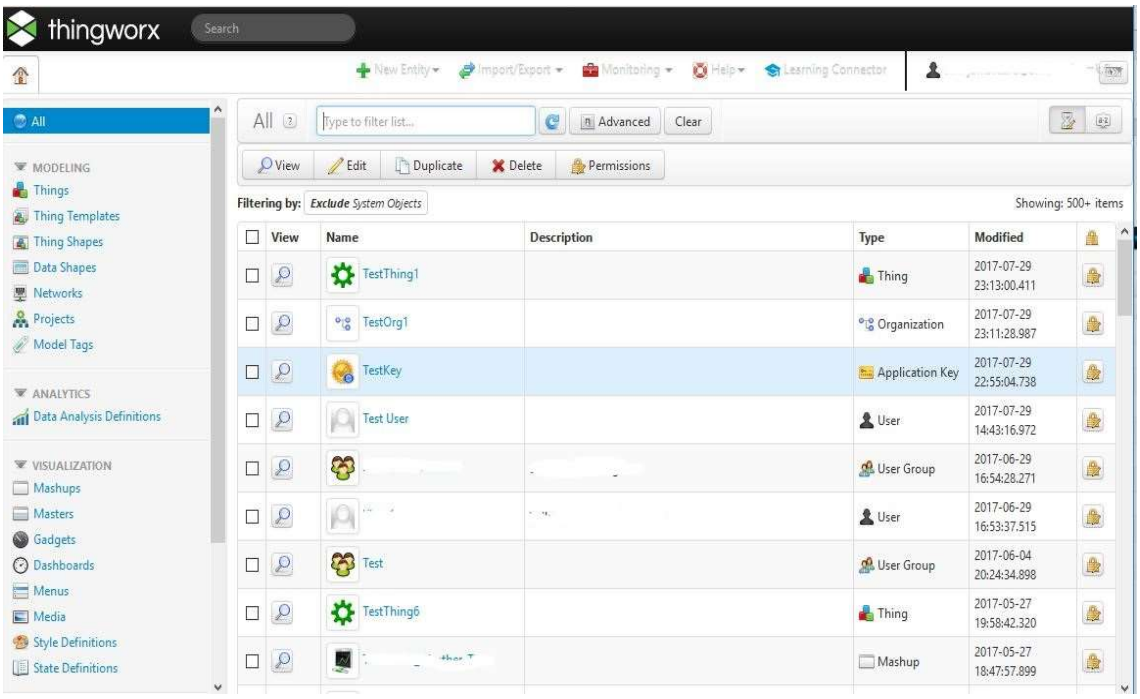
6 PTC THINGWORX IOT-ALUSTA

6.1 Thingworx-yleistä

PTC:n Thingworx IoT-alustaa yrityskäyttöön tarjoaa suomessa teleoperaattori Elisa. Se on alusta, johon voi tuoda sisältöä lähes mistä tahansa IoT-laitteesta tai pilvialustasta, kuten esimerkiksi Amazonin (AWS IoT Service), Microsoftin (Azure IoT Hub), tai Salesforcen (Salesforce IoT Cloud) pilvialustoista.

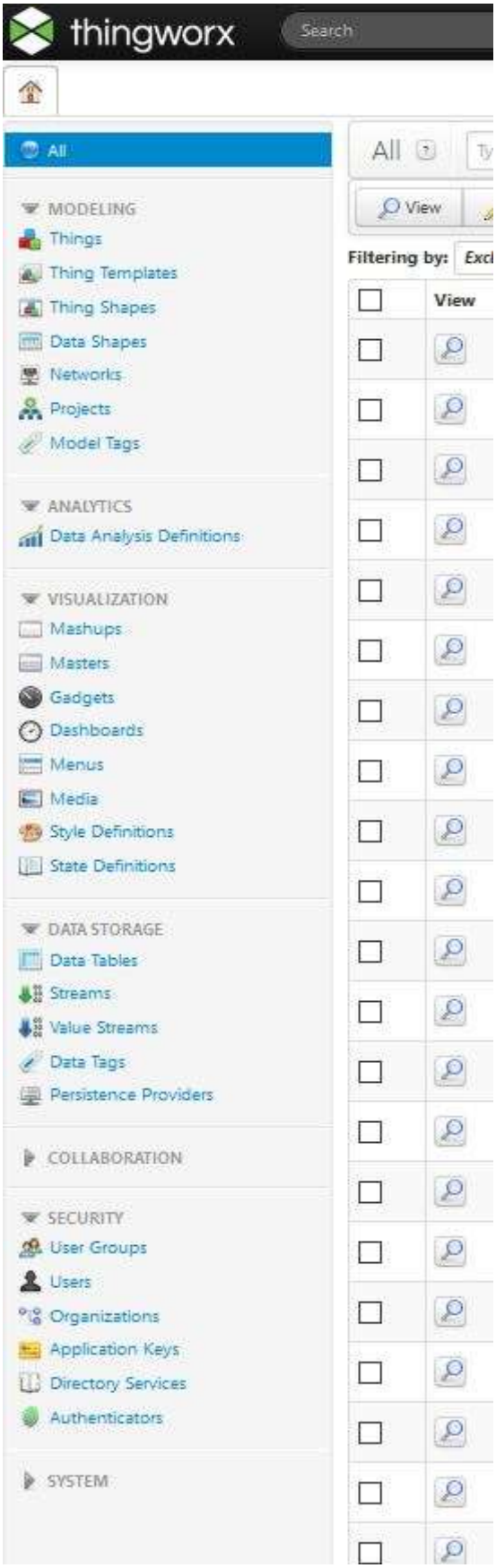
Thingworx:n käyttöliittymä toimii selaimessa. Sen perusnäkymän vasemmasta reunasta löytyy valikko, jonka avulla toimintoja hallitaan. Thing, eli suomeksi Esine on alku/peruste kaikelle, sitä voidaan käyttää esimerkiksi mallintamaan olemassa olevaa tuotantolaitetta.

Kuvassa 44 näkymä Thingworx:n käyttöliittymästä, jossa on näkyvissä kaikki mahdolliset objektit. Näytön oikeassa laidassa näkyvät All-perusnäkymässä kaikki järjestelmään luodut sisällöt (käyttäjät, käyttäjäryhmät, esineet ym.). Näytettäviä tietoja pystyy helposti suodattamaan, jotta oikea tieto löytyy.



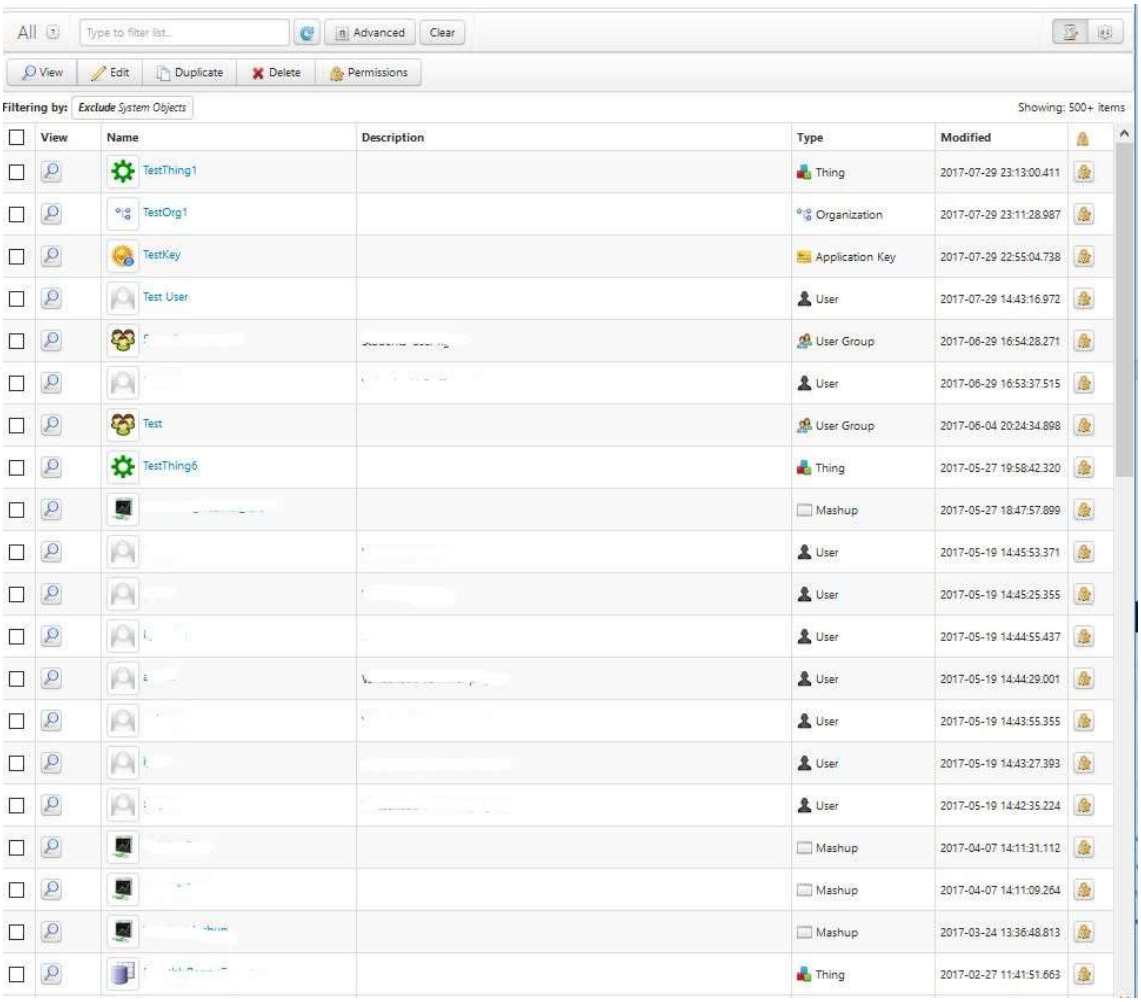
Kuva 44. Thingworx - käyttöliittymä

Kuvassa 45 vielä tarkempi näkymä vasemman reunan valikkoon.



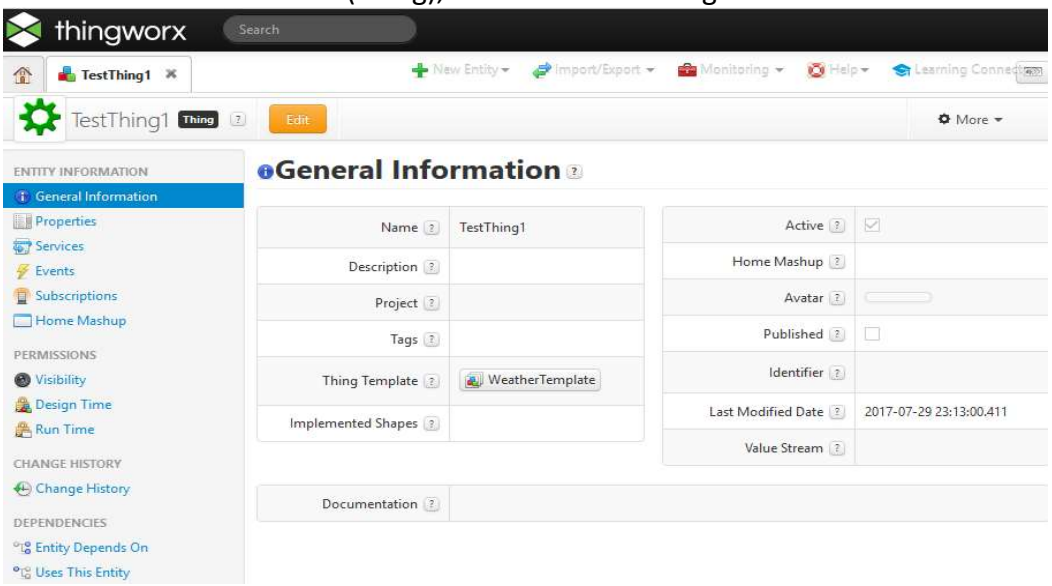
Kuva 45. Thingworx - valikko vasen

Kuvassa 46 tarkempi katsaus perusnäkymän oikeasta puolesta.



Kuva 46. Thingworx - valikko oikea

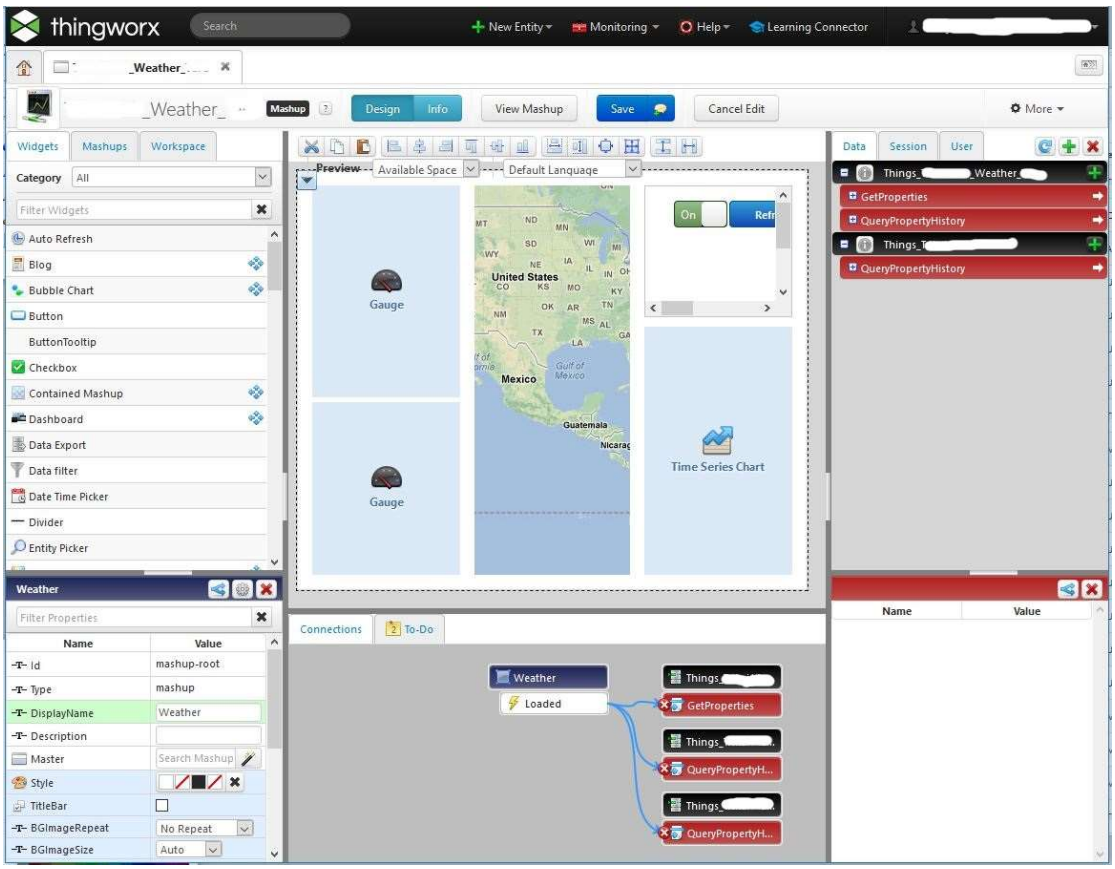
Kuvassa 47 on luotu esine (Thing), nimeltään TestThing1:



Kuva 47. Thing - TestThing1

TestThing1 pohjautuu (template) WeatherTemplate-esineeseen, joka hakee säätilatietoa Ilmatieteen laitoksen Avoin data-palvelusta.

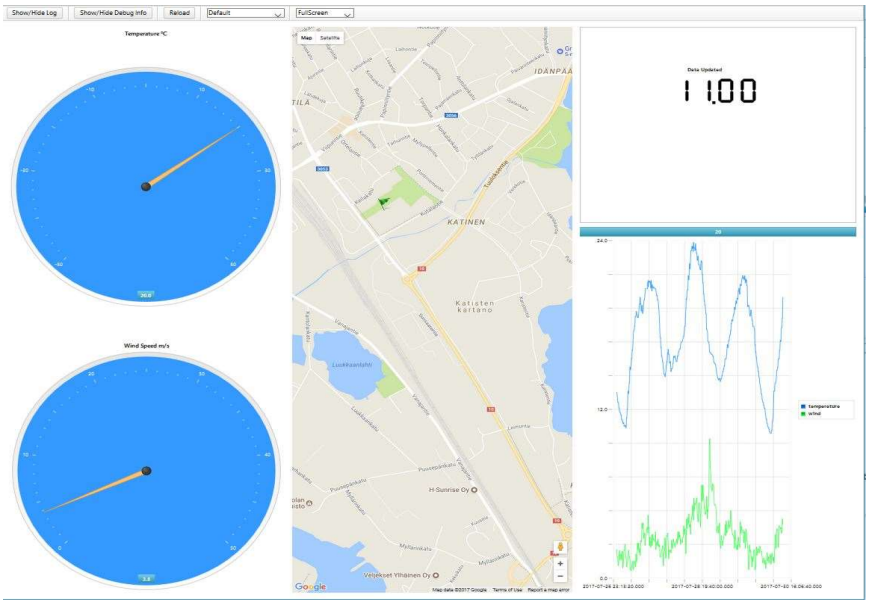
Mashup:n avulla Thingworx:ssä pystytään luomaan näyttäviä ”kojelautoja” (dashboard), joilla voidaan seurata eri lähteistä tulevaa tietoa. Kuvassa 48 esimerkki kojelaudasta, jonka avulla voidaan seurata säätietoja Hämeenlinnan Hätilän mittauspisteessä. Tiedot haetaan Ilmatieteen Laitoksen Avoin data-palvelusta Rest API-rajapinnan kautta.



Kuva 48. Thingworx Weather Thing - näkymä Thingworx:ssä

Thingworx hakee tiedot taustalla Ilmatieteen laitoksen palvelusta. Valitsemalla toiminto ”View Mashup” ruudun yläosassa keskellä, voidaan tietoja katsella selaimessa.

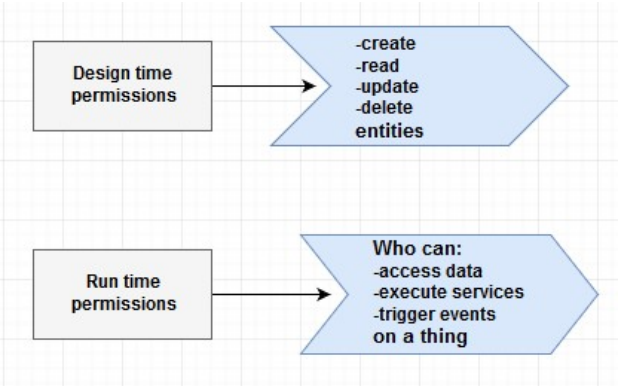
Kuvan 49 kaltaisessa yksinkertaisessa kojelautanäkymässä voidaan tarkastella lämpötilaa ja tuulen nopeutta mittarinäkymässä, sekä historiatietoa piirtyvänä graafisena kuviona.



Kuva 49. Weather Thing - näkymä selaimessa

6.2 Thingworx - tietoturvamääritykset

Miten ThingWorx IoT-alusta suojaa käyttäjän tietoja ja miten tietoturvamääritykset tehdään kyseisellä alustalla? Thingworx:n tietoturva jaetaan karkeasti kahteen eri luokkaan, suunnittelunaikaiseen (Design time) ja käytönaikaiseen (Run time). Kuvassa 50 yhteenveto Thingworx:n käyttöoikeuksista ja mitä ne mahdollistavat.



Kuva 50. Thingworx - käyttöoikeudet

Suunnitteluvaiheen oikeudet määrittävät sen, kuka on oikeutettu muuttamaan mallia - template (luo-, lue-, päivitä-, tai poista). Käytönaikaiset oikeudet taas määrittävät, kuka voi päästä käsiksi tietoon, suorittaa palveluita ja käynnistää esineen palveluita (tämä taas käsittää tietokantataulut, jonot ja käyttäjät).

Jokaisen käyttöoikeuden suhteen voidaan valtuuttaa käyttäjä tai ryhmä tekemään jokin tietty toimenpide (esimerkiksi muuttamaan esinettä - "Thing"), tai toisaalta on mahdollista myös estää käyttäjäryhmältä toimenpiteen (kuten esimerkiksi käyttäjäryhmältä voi estää esineen "Thing" muokkaamisen). Käyttöoikeuksien kielto "ajaa yli" mahdollisesti jo annetuista käyttöoikeuksista. Thingworx:ssä turvatoimintona mihinkään operaatioon ei anneta oletuksena oikeuksia.

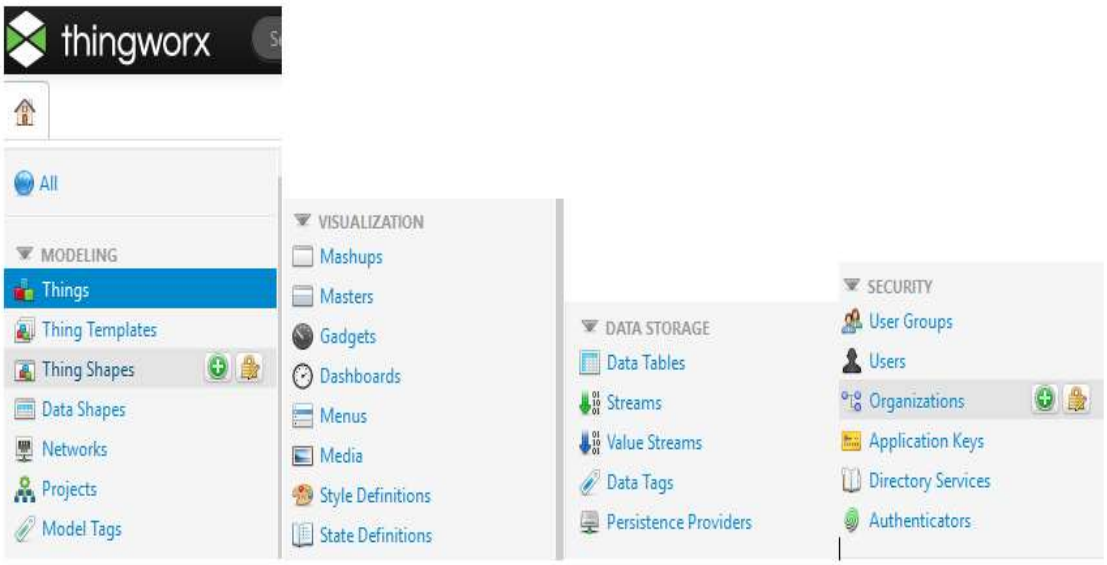
Suunnittelunaikaisilla käyttäjäoikeuksilla voidaan suorittaa luo-, lue-, päivitä-, poista / eng. Create-, Read-, Update-, Delete -toimenpiteitä.

Käytönaikaiset oikeudet sisältävät ominaisuuden luku-, kirjoitus-, tapahtuman suorittamisen ja palvelun suorittamisen. Nämä voidaan tehdä joko kaikkien ominaisuuksien tai kaikkien palveluiden tasolla esineelle (Thing).

Esineelle (Thing) on mahdollista määrittää käytönaikaiset oikeudet, joko esineen mallille (Thing template), tai kokoelmatasolla. Kokoelma on esimerkiksi esineiden tai esineiden mallien kokoelma. Kokoelmassa kaikki esineet perivät samat oikeudet. Kuitenkin kaikki perityt käyttöoikeudet voidaan ohittaa yksittäisen esineen tasolla. (PTC Thingworx Security n.d.)

ThingWorx Composerissa pääsyoikeuksia hallitaan vasemman reunan Security-valikossa.

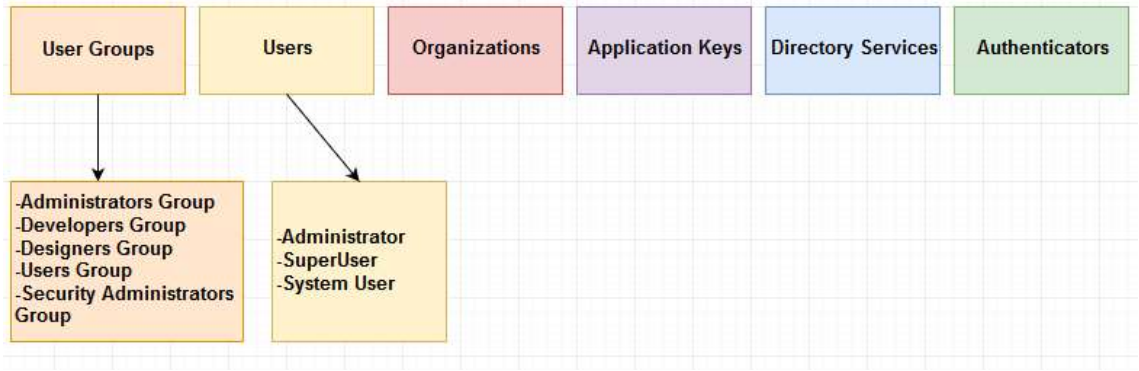
Kuvassa 51 näkymä Thingworx:n tärkeimmistä valikoista, joista tässä opinnäytetyössä keskitymme viimeiseen, eli **Security**-valikkoon:



Kuva 51. Thingworx – valikot

Kuvassa 52 on lueteltu mitä vaihtoehtoja Thingworxin Security-valikosta voi valita.

Security-valikosta löytyvät seuraavat vaihtoehdot:

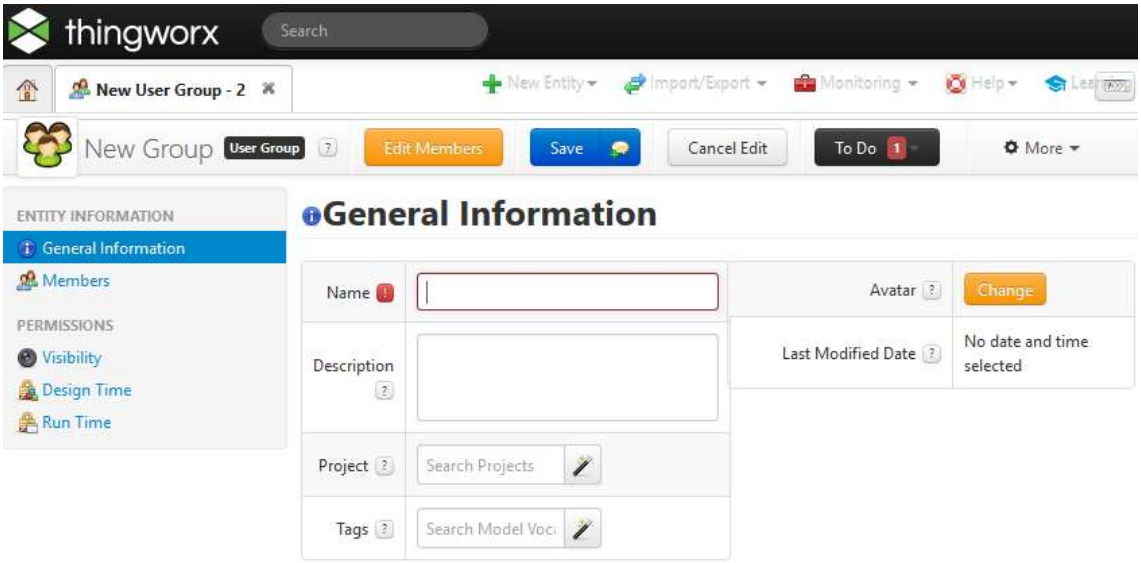


Kuva 52. Thingworx - Security-valikko

6.2.1 User Groups

Käyttäjäryhmillä (User Groups) voidaan määritellä, mitä toimintoja kukin käyttäjä voi Thingworx:ssä suorittaa, samalla tavoin, kuin esimerkiksi Windows-käyttöjärjestelmässä. Erilaisia käyttäjäryhmiä löytyy Thingworx:stä kaikkiaan 5 kappaletta; Administrators Group, Developers Group, Designers Group, Users Group ja Security Administrators Group. (PTC Thingworx Security n.d.)

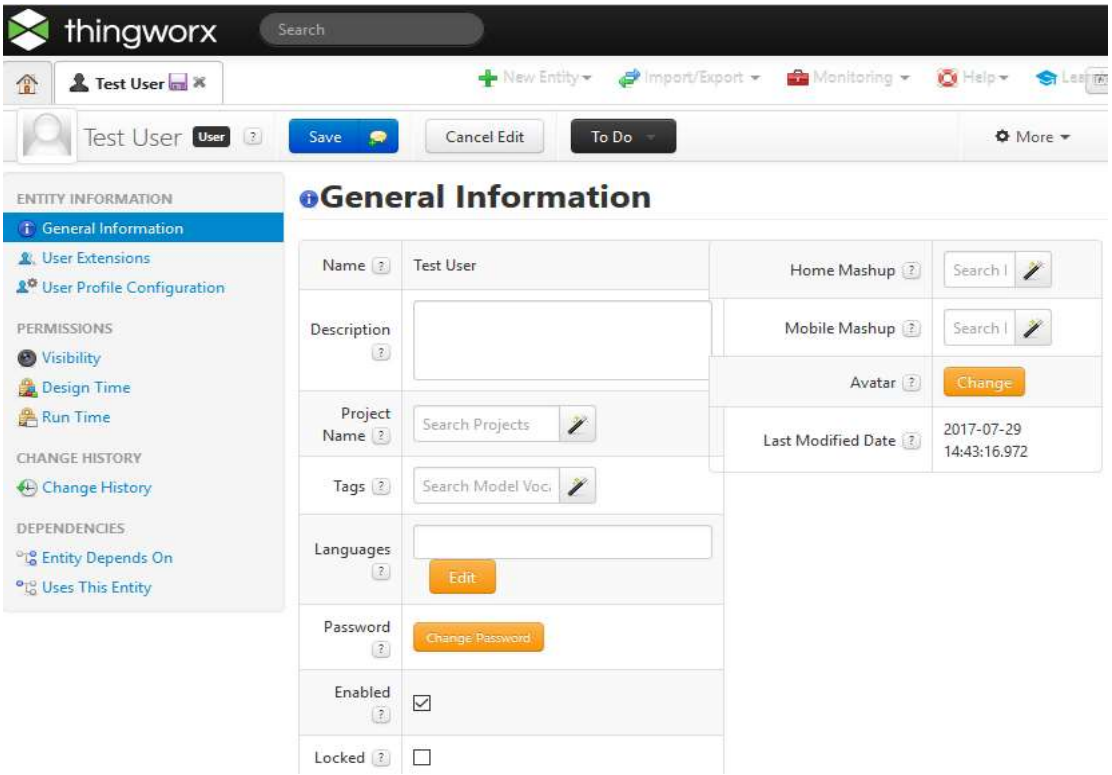
Kuvassa 53 näkymä uuden käyttäjäryhmän luomisesta.



Kuva 53. Thingworx – uuden käyttäjäryhmän luominen

6.2.2 Users

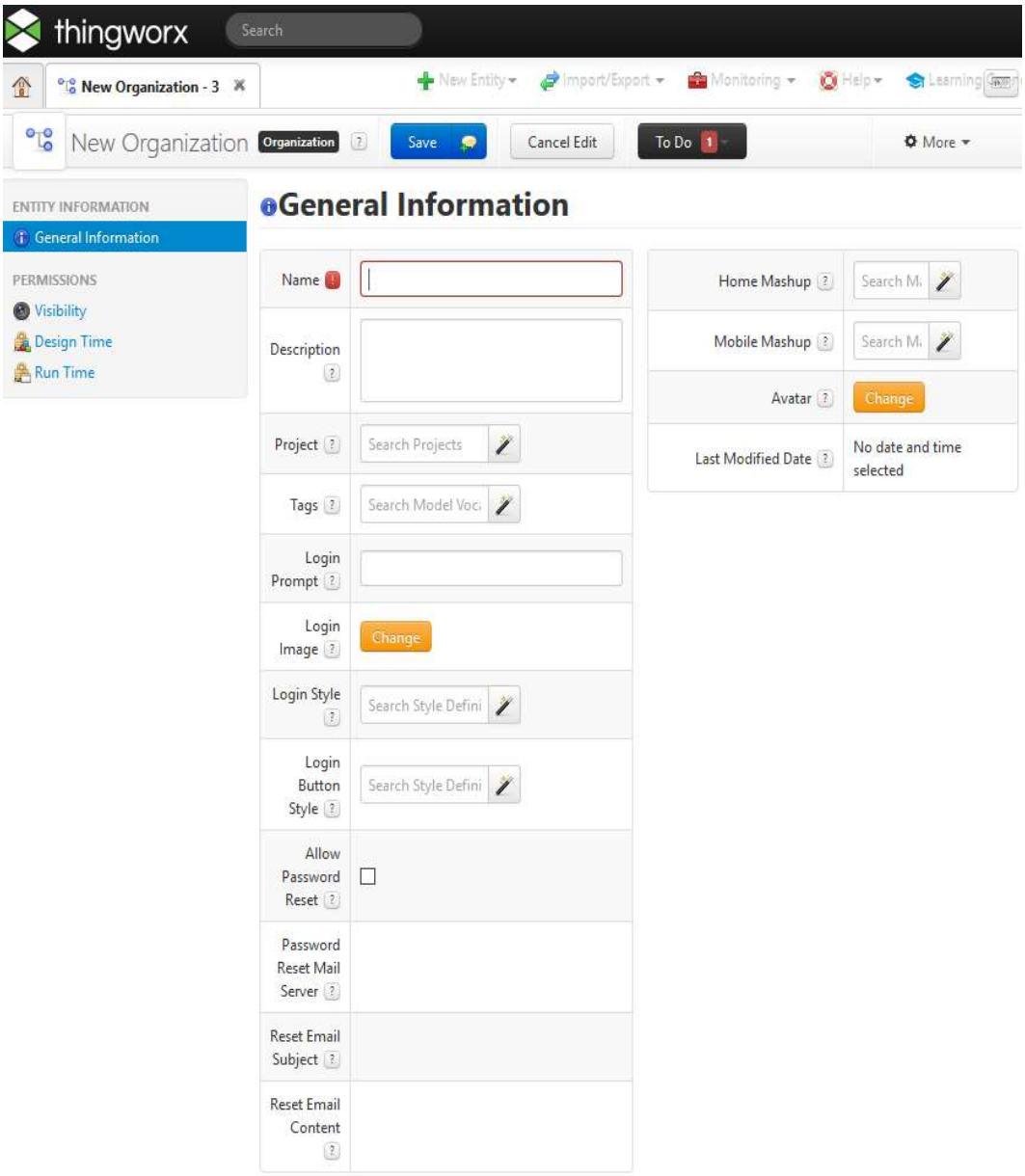
Käyttäjät (Users) - jokaisella Thingworx:n käyttäjällä tulee olla olemassa käyttäjätunnus. Käyttäjän profiilissa (User Profile Configuration) voidaan määritellä tarkalleen, mitä yksittäinen käyttäjä näkee Thingworks:ssä. Kuvassa 54 luodaan uusi Thingworx-käyttäjä.



Kuva 54. Thingworx – uuden käyttäjän luominen

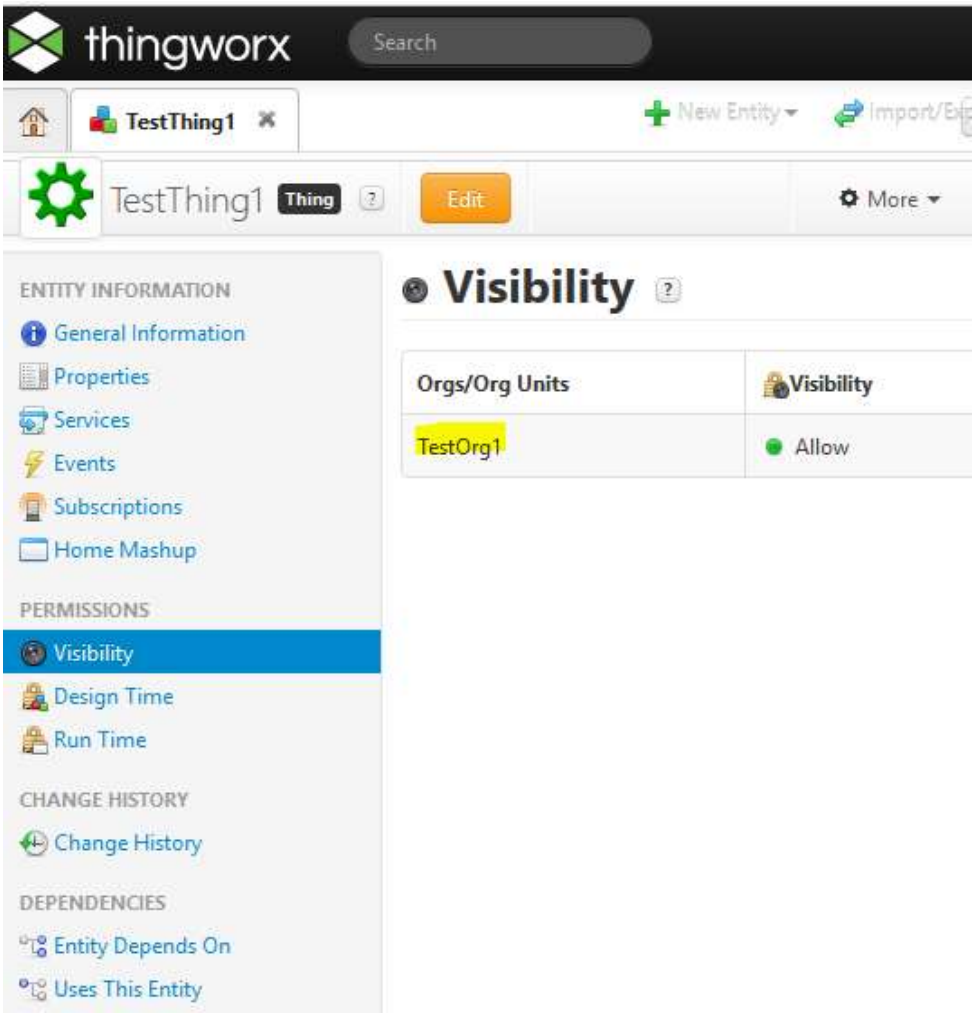
6.2.3 Organizations

Thingworx:n organisaatioiden (Organizations) avulla voidaan kontrolloida sitä, mitä käyttäjä näkee Thingworx:ssä. Edellytyksenä on, että käyttäjät ja käyttäjäryhmät ovat jo olemassa. Organisaatioilla voi olla myös aliorganisaatioita, joten näkyvyyttä pystyy kontrolloimaan hyvinkin tarkasti. Kuvassa 55 luodaan uusi organisaatio.



Kuva 55. Thingworx – uuden organisaation luominen

Kuvassa 56 luodaan TestThing1:lle näkyvyyssääntö, eli määritellään mitkä organisaatiot voivat nähdä kyseisen esineen.



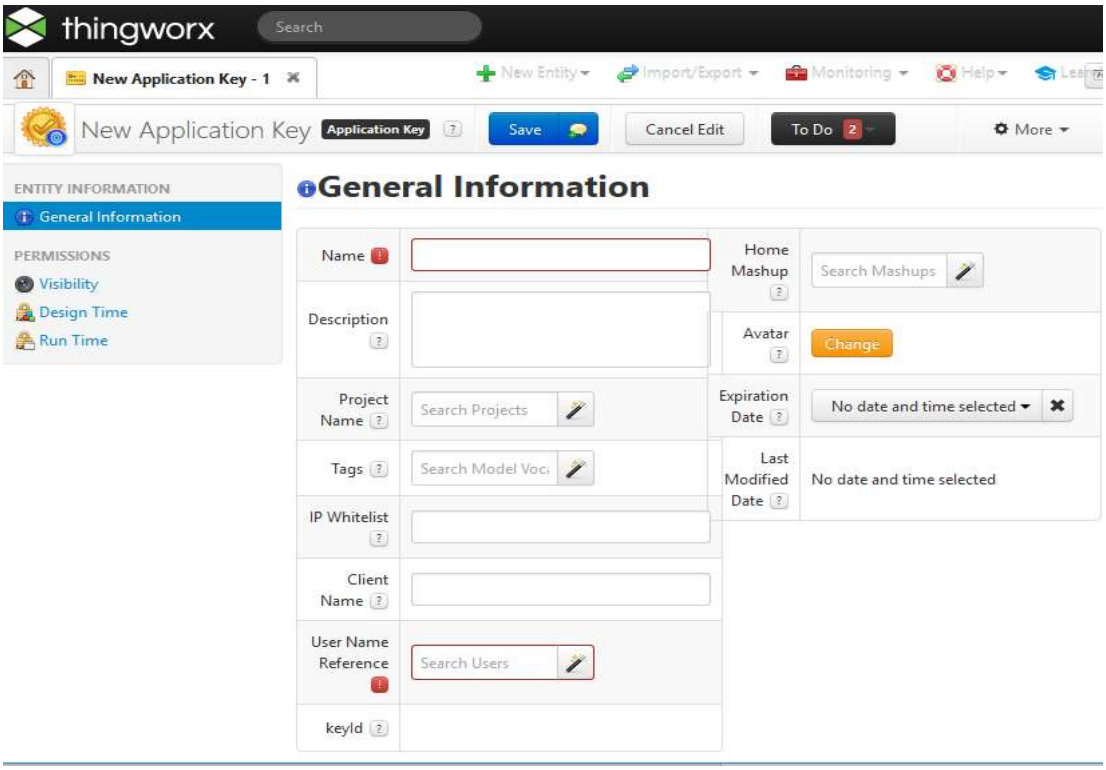
Kuva 56. Test Thing1 – näkyvyys

Kuvassa 56 on luotu TestThing1-esineelle sääntö, jonka mukaan se näkyy vain TestOrg1-organisaatiolle. Näin pystytään siis yksinkertaisesti sallimaan tai estämään näkyvyys tietyltä organisaatiolta.

6.2.4 Application Keys

Sovellusavaimella (Application Key) voidaan antaa pääsy Thingworx:iin ilman käyttäjätunnuksen ja salasanan antamista. Tällöin siis järjestelmän luoma yksilöllinen Application Key (32-merkkinen API-avain) syötetään suoraan Web-osoittessa muodossa https://sitename/folder/ ?appKey= aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee.

Luotuasi uuden Application Keyn, järjestelmän luoma avain tulee näkyviin kohtaan keyID, kuvassa 57. (PTC Thingworx Security n.d.)



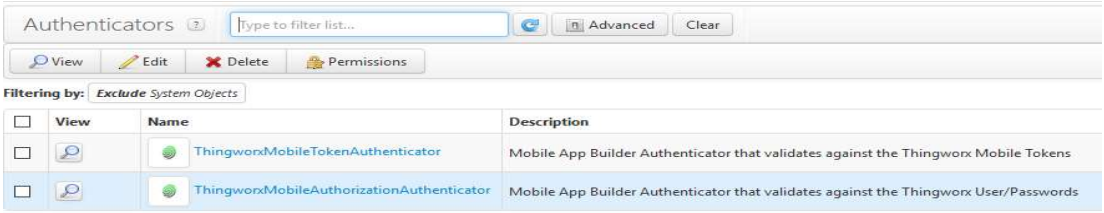
Kuva 57. Thingworx - Application Key

6.2.5 Directory Services

Käyttäjäoikeudet voidaan Thingworx:ssä todentaa myös erilaisten LDAP (Lightweight Directory Access Protocol) -järjestelmien, esimerkiksi Microsoftin Active Directory:n -avulla. Mikäli käyttäjien tunnukset ovat jo olemassa MS AD:ssä, käyttäjäryhmät voidaan viedä suoraan myös Thingworx:iin. (PTC Thingworx Security n.d.)

6.2.6 Authenticators

Authenticators -valikon alta löytyy vaihtoehdot ThingworxMobileTokenAuthenticator ja ThingworxMobileAuthorizationAuthenticator, joita käytetään tunnistautumiseen mobiililaitteella. Kuvassa 58 Authenticators-näkymä.



Kuva 58. Thingworx - Authenticators

7 YHTEENVETO

Tämän opinnäytetyön tarkoituksena oli kerätä IoT-tietoa ja lisätä IoT-tietoutta niin Hämeen Ammattikorkeakoulun Älykkäät palvelut-tutkimusyksikölle. Mielestäni tämä tavoite on saavutettu hyvin. Opinnäytetyössäni olen esitellyt monipuolisesti IoT:n eri alueita, kuten tietoturvan testausta, erilaisia IoT-tietoturvalaitteita ja ohjelmistoja, sekä erilaisia IoT-haitakkeita, ja viimeisenä myös Thingworx IoT-alustaa ja sen tietoturva-asetuksia.

Itselläni ei ennen tämän opinnäytetyön tekemistä ollut juuri kokemusta tai sen suurempaa tietämystä IoT:stä. Olin toki aiemmin lukenut erilaisia uutisia roskapostia lähettävistä jääkaapeista jne. Omasta mielestäni olen oppinut IoT-alueen asioista hyvinkin paljon. Jos nyt esimerkiksi olisin ostamassa IoT-laitetta, tietäisin varsin hyvin, mitä pitää ottaa huomioon tietoturvan näkökulmasta. Ymmärrän nyt myös huomattavasti paremmin erilaisten IoT-tietoturvalaitteiden ja ohjelmistojen toimintaperiaatteet. Näiden toiminta perustuu yleensä siihen, että ne seuraavat IoT-laitteita ja niiden toimintaa. Jos ja kun laite toimii jotenkin poikkeavalla tavalla, ohjelmisto tai laite tunnistaa sen ja sulkee ko. laitteen verkosta.

Aion myös tulevaisuudessa seurata IoT:n tietoturvan kehitystä ja myös haittaohjelmien levinneisyyttä. Nyt tiedän paljon paremmin tällä hetkellä IoT-laitteisiin iskevien haittaohjelmien toimintaperiaatteet. Mikäli olisin lähitulevaisuudessa ostamassa IoT-laitetta, tietäisin heti, mitä tulee tehdä ennen laitteen käyttöönottoa. Eli ainakin tässä mielessä opinnäytetyössäni olen onnistunut hyvin, tietoisuuteni IoT:stä on lisääntynyt huomattavasti.

LÄHTEET

Cisco 3000 Series Industrial Security Appliances (ISA). (n.d.) Viitattu 11.5.2017. https://www.cisco.com/c/en/us/products/security/industrial-security-appliance-isa/index.html

Cisco IoT Threat Defense. (n.d.) Viitattu 19.8.2017. https://www.cisco.com/c/en/us/solutions/security/iot-threat-defense/index.html?stickynav=1

Collin J., Saarelainen A. (2016). Teollinen internet. Talentum Pro.

Cujo LLC (n.d.). Viitattu 11.5.2017 https://www.getcujo.com/

Franceschi-Bicchierai L. (2017). Hackers Are Remotely Controlling Industrial Robots Now. Viitattu 15.5.2017 https://motherboard.vice.com/en_us/article/hackers-are-remotely-controlling-industrial-robots-now

F-Secure Sense (n.d.). Viitattu 11.5.2017 https://www.f-secure.com/en/web/home_global/sense

Grange, W (2017). Hajime worm battles Mirai for control of the Internet of Things. Viitattu 17.5.2017. https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things

Herzberg B., Bekerman D., Zeifman I. (2016). Breaking Down Mirai: An IoT DDoS Botnet Analysis. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Keezel (n.d.). Viitattu 11.5.2017. https://shop.keezel.co/

Dickson B. (2016). 4 devices that can help secure your home's IoT. Viitattu 17.5.2017. https://thenextweb.com/insider/2016/01/04/4-devices-that-can-help-secure-your-homes-iot/#.tnw_umzXHcc9

Krebs B. (2016). Hacked Cameras, DVRs Powered Today's Massive Internet Outage. Viitattu 17.5.2017 https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

Kumar M. (2015). Hacker-Friendly Search Engine that Lists Every Internet-Connected Device. Viitattu 11.5.2017. https://thehackernews.com/2015/12/internet-of-things-search-engine.html

Luma Home Inc. (n.d.). Viitattu 17.5.2017. https://lumahome.com/

Lomas N. (2015). Viitattu 11.5.2017. Dojo Is Designed To Protect Your Smart Home From Itself. https://techcrunch.com/2015/11/19/dojo-labs/

McAfee Labs Threats Report (2017). Viitattu 19.5.2017 https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

Nadel B. (2016). Bitdefender Box Review. Viitattu 11.5.2017. http://www.tomsguide.com/us/bitdefender-box,review-3766.html

Osborne C. (2016). Shodan: The IoT search engine for watching sleeping kids and bedroom antics. Viitattu 11.5.2017. http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/

PTC Thingworx Security. (n.d.). Viitattu 20.8.2017 http://support.ptc.com/help/thingworx_hc/thingworx_7_hc/#page/ThingWorx_Core_Help_Center%2FThingWorxHelpCenterDITAFiles%2FSecurity%2FSecurity.html%23

Radware (2017). BrickerBot" Results In PDoS Attack. Viitattu 11.5.2017 https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

Rapid7 (n.d.). Metasploit. Viitattu 11.5.2017. https://www.rapid7.com/products/metasploit/

Rapid7 (n.d.). Metasploit - Editions. Viitattu 11.5.2017 https://www.rapid7.com/products/metasploit/download/editions/

Rapid7 (n.d.). Metasploitable - Setting Up a Practice Target Machine. Viitattu 11.5.2017 https://community.rapid7.com/servlet/JiveServlet/downloadBody/1814-102-7-2720/Metasploitable_SetUpGuide.pdf

Rapid7 (2017). Exiting the Matrix: Introducing Metasploit's Hardware Bridge. Viitattu 11.5.2017 https://community.rapid7.com/community/transpo-security/blog/2017/02/02/exiting-the-matrix

Sayer P. (2016). Keezel's wireless device protects hotel Wi-Fi, home IoT connections. Viitattu 11.5.2016. http://www.pcworld.com/article/3115107/security/keezels-wireless-device-protects-hotel-wi-fi-home-iot-connections.html

Symantec Corporation (n.d.). Norton Core Features. Viitattu 11.5.2017 https://us.norton.com/core-secure-router-features

Tosibox Lock 200 (n.d.) TOSIBOX Lock 200. Viitattu 18.5.2017. https://www.tosibox.com/product/lock-200/

Tosibox VCL (n.d.) TOSIBOX Virtual Central Lock. Viitattu 18.5.2017. https://www.tosibox.com/product/virtual-central-lock/

Viestintävirasto (2017) Mirai voi hyvin - sinun modeemissasi! Viitattu 20.8.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturva-nyt/2017/08/ttn201708181500.html

Zingbox IoT Guardian. (n.d.) Viitattu 11.5.2017. https://www.zingbox.com/iot-guardian/