Aalto-yliopisto
Sähkötekniikan korkeakoulu

Raportti
21.3.2013

Suomen automaatioverkkojen haavoittuvuus

- Raportti Internetissä julkisesti esillä olevista automaatiolaitteista

- Seppo Tiilikainen, Jukka Manner

Aalto-yliopisto
Sähkötekniikan korkeakoulu
Tieliikenne- ja tietoverkkotekniikan laitos

Postiosoite
PL 17800
00076 AALTO

Käyntiosoite
Lämpömiehenkuja 2
Espoo

Puhelin 09 47001
Faksi -
Y-tunnus 2228357-4

www.aalto.fi
etunimi.sukunimi@aalto.fi
VAT FI22283574 Kotipaikka Helsinki

1. Johdanto

Suomen infrastruktuurin haavoittuvuus Internetistä tulevia kyberhyökkäyksiä vastaan on noussut Stuxnetin ja Red Octoberin kaltaisten hyökkäysten myötä tärkeäksi kysymykseksi. Valoa asiaan saadaan kartoittamalla kuinka paljon kriittisiä SCADA-, kontrolli-, ja tehdasautomaatiojärjestelmiä Suomesta on löydettävissä yleisen Internetin kautta. Järjestelmien kartoitusta voidaan tehdä työkaluilla, kuten hakupalvelu Shodanilla[1], joka analysoi Internetissä kiinni olevia laitteita ja tallentaa näistä tietoja tietokantaansa. Tietokannasta oikeilla hakutermeillä ja rajauksilla on löydettävissä Internetissä kiinni olevia laitteita ja järjestelmiä, joihin rajoittamatonta pääsyä ei pitäisi olla, kuten monet automaatiojärjestelmät. Internetistä on helppoa etsiä tunnettuja haavoittuvuuksia löydetyille laitteille, joka entisestään vähentää väärinkäytöksiin tarvittavaa aikaa ja taitoa. Tammikuussa 2013 olemme tehneet Shodanilla laitekartoitusta Suomessa sijaitsevista tehdasautomaatiolaitteista. Löysimme yhteensä 2915 laitetta, jotka kuuluvat erilaisiin teollisuuden automaatiojärjestelmiin, rakennusautomaatioon, sähkönhallintaan ja järjestelmien etäkäyttöön. Shodanilla löytyi Suomesta yhteensä 185 000 HTTP-vastausta antavaa laitetta ja määrä on jatkuvassa tasaisessa kasvussa. Tämänhetkisen tilanteen ja tulosten kasvun perusteella voidaan arvioida, että Shodan ei ole vielä skannannut kaikkia suomalaisia IP-osoitteita, vaan Shodanin otos Suomen IP-avaruudesta on arviolta vasta muutaman kymmenen prosentin luokkaa. Tämän tutkimuksen puitteissa löydetyistä laitteista 60%:iin löytyi yleisesti tiedossa oleva haavoittuvuus julkisista haavoittuvuustietokannoista. Tämä raportti erittelee löydöt teollisuusautomaation ja teollisuuden ulkopuolella käytetyn automaation perusteella, ja antaa esimerkkejä löydetyistä laitteista sekä niiden käyttötarkoituksista. Tarkka laite- ja järjestelmäkohtainen analyysi laitteiden käyttökohteista vaatisi järjestelmiin tunkeutumista, jota emme ole voineet tehdä rikoslain 38. luvun nojalla (tietomurto). Lopuksi raportissa esitetään hälyttävimmät löydöt ja arvioidaan kokonaiskuvaa Suomen haavoittuvuudesta Shodan-tutkimuksen perusteella.

Tutkimuksestamme on kirjoitettu kaksi raporttia. Tämä raportti sisältää yleisellä tasolla kuvauksia haasteista ja löydöksistämme Suomesta. Täydellinen lista käytetyistä hakusanoista, löydetyistä kohteista ja laitteiden IP-osoitteista on annettu erikseen viranomaisille, mm. CERT-FI:lle.

[1] http://www.shodanhq.com

2. Tutkimuksessa käytetyt menetelmät

Tutkimuksessa saadut tulokset perustuvat Shodan-hakukoneen käyttöön. Shodanin tulokset perustuvat laajaan koko Internetiä koskevaan satunnaiseen porttiskannaukseen. Palvelu kerää tietoja useassa eri maassa sijaitsevien palvelimien avulla, jotka skannaavat satunnaisia IP-osoitteita ja tallentavat osoitteesta saadut vastausviestit tietokantaan arkistointia varten. Shodan skannaa useaa eri tietoliikenneporttia ja pystyy tällä tavalla havaitsemaan useita erilaisia avoinna olevia palveluita kohdeosoitteessa, kuten Telnet, FTP ja SNMP. Yleisimmät Shodanin skannaamat portit ovat 80 ja 22 (HTTP ja SSH, vastaavasti). Kaikki Shodanin löytämä tieto ei välttämättä ole ajantasaista, sillä arkistoituja tuloksia ei poisteta tietokannasta. Tällä hetkellä Shodanin tietokannasta löytyy yli 150 miljoonaa hakutulosta.

Shodanin löytämät laitteet ovat laitteita, joihin kuka tahansa voi ottaa yhteyden Internetin yli. Laitteeseen murtautumisen helppous riippuu täysin laitteen ja järjestelmän tieturvaratkaisuista, mutta Shodan helpottaa haavoittuvien sekä mielenkiintoisten kohteiden löytämistä. Riippuen laitteen Shodanille antaman vastausviestin tiedoista, toisinaan on mahdollista nähdä käytössä olevat ohjelmistoversiot, joka paljastaa onko jokin tietty haavoittuvuus hyödynnettävissä kohdelaitteessa. Toisinaan vastausviesti paljastaa myös sen, että yhteyden muodostamiseen ei tarvita autentikointia ollenkaan. Kuten johdannossa jo mainittiin, oletukset laitteista ja niiden käyttötarkoituksista perustuvat Shodanin arkistoimiin tietoihin, eikä ilman järjestelmään tunkeutumista voida varmuudella sanoa onko laite juuri se, mikä se sanoo olevansa, vai esimerkiksi hämäykseksi tarkoitettu hunajapurkki eli valelaite.

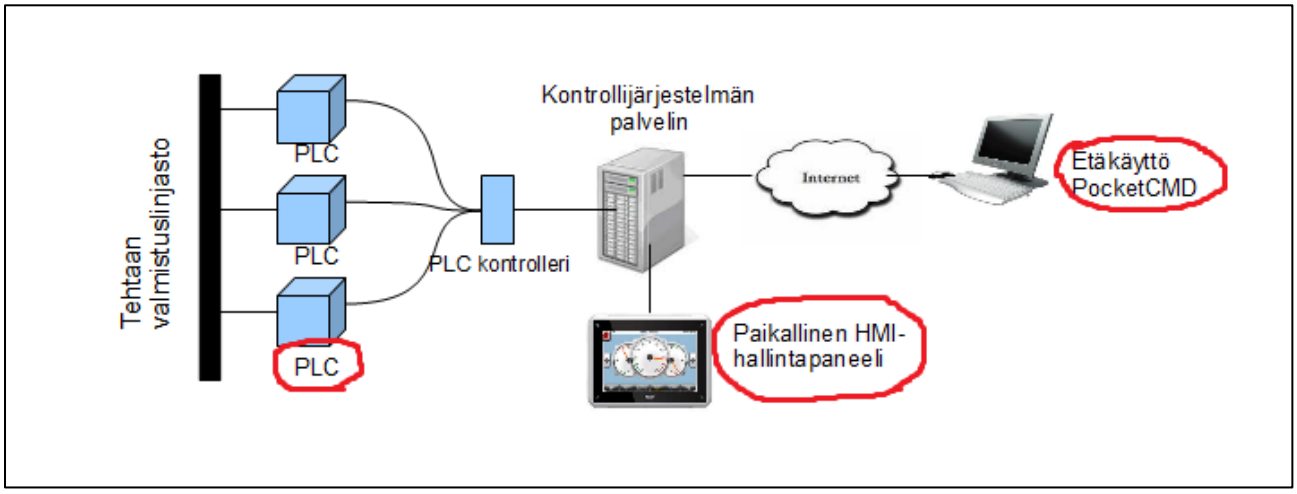
Tässä tutkimuksessa etsittiin automaatiolaitteita Shodanin avulla käyttämällä valikoituja hakusanoja, sekä maa- ja IP-osoiterajauksia. Hakusanoina käytettiin automaatiotuotteiden valmistajia, tuotenimikkeitä, sekä automaatioverkoissa käytettyjä protokollia ja palveluita, kuten Modbus. Maarajauksella saatiin kohdistettua tulokset vain Suomen sisäisiin IP-osoitteisiin. IP-osoitteen rajausta käytettiin, kun tuloksia haluttiin etsiä esimerkiksi tietylle yritykselle rekisteröidystä IP-osoitelohkosta. Tällä menetelmällä saatiin tietoa yrityksen Internetiin näkyvistä laitteista, ja samalla myös opittiin lisää hyödyllisiä hakutermejä, joita voitiin soveltaa hakuun koko Suomen IP-avaruudesta. IP-osoitteiden selvityksessä käytettiin RIPE:n tietokantaa[2]. Lista käytetyistä hakusanoista on annettu viranomaisille.

[2] http://www.ripe.net

3. Teollisuussautomaatio (sis. SCADA)

Rajaamalla löydöistä laitteet, joita hyvin suurella todennäköisyydellä käytetään pelkästään teollisuuden tärkeissä järjestelmissä (SCADA, kontrollijärjestelmät, hallintapaneelit, etäkäyttö) Suomesta löytyi 77 laitetta, joista suoraan SCADA-järjestelmiin viittaavia nimiä oli 33. Koska kartoitusta suoritettiin vain Shodanilla saatujen tietojen nojalla, tarkempi arvionti järjestelmistä ja niiden sijainnista on vaikeaa. Laitteiden nimen ja IP-osoitteen omistavan yrityksen perusteella voi kuitenkin tehdä arvauksia laitteen käyttötarkoituksesta. Nimen perusteella saadaan tieto siitä, minkälaiseen käyttöön laite soveltuu, ja yrityksen nimi voi paljastaa tarkemmin käyttökohteen- ja sijainnin. Usein kuitenkin yrityksen nimi jää pimentoon, koska IP-osoite voi olla rekisteröitynä yleiselle Internet-yhteyden palveluntarjoajalle, eikä laitteen omistavalle taholle. Alla muutama esimerkki löydetyistä laitteista ja niiden käyttötarkoituksista. Ensimmäisen esimerkin HMI (Human Machine Interface) tarkoittaa koneenhallintakäyttöliittymää, ja PLC (Programmable Logic Controller) tarkoittaa laitteita, jotka ohjaavat automaatiojärjestelmän komponenttien toimintaa.

- Siemens Simatic laitteita: S7, HMI, NET: PLC-laitteita, valvontajärjestelmiä, automaatiojärjestelmän osien ethernetintegraattori etävalvonnalla. Yhteensä: 8 kpl
- Schneider TSX: Automaatioverkkojen kommunikaatiomoduleita. Yhteensä: 12 kpl
- Schneider Modicon Quantum, web-käyttöliittymä: PLC-laitteiden kontrolleri raskaan tason vaativaan automaatiokäyttöön. Yhteensä: 6 kpl
- clearScada: Scheiderin SCADA-palvelinalusta web-etäkäyttöliittymällä. Yhteensä: 3 kpl
- Pocket CMD – Komentorivikäyttöliittymä telnet-yhteyden yli Windows CE käyttöjärjestelmälle. Käytetään mm. automaation hallinnassa. Yhteensä: 8 kpl



Kuva 1: Esimerkki muutamasta kontrollijärjestelmäkomponentista

Edellä mainitut laitteet mitä ilmeisimmin ovat käytössä automaation kontrollijärjestelmissä, kohdelaitoksina esimerkiksi tehtaiden valmistuslinjastot, voimalaitokset ja vedenkäsittelylaitokset. Siemens ja Schneider ovat suosittuja automaatiotuotteiden valmistajia ja ovat siksi myös suosittuja

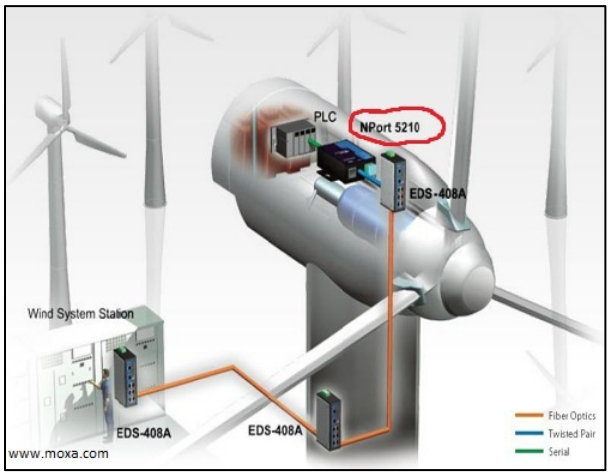
kohteita haavoittuvuuksien etsinnälle. Esimerkiksi Stuxnet-mato[3] hyökkäsi juuri Siemensin Simatic S7 PLC-laitteita vastaan Iranilaisessa ydinvoimalassa vuonna 2010 ja aiheutti tuhoa voimalan sentrifugeissa. Syksyllä 2012 julkaistiin myös vakava haavoittuvuus laajasti raskaassa automaatiokäytössä olevaan Schneider Modicon Quantum-laitteeseen[4]. Yllä oleva esimerkki Pocket CMD-käyttöliittymästä on hyvä näyte tietoturvan täydellisestä puuttumisesta. Shodanilla löytyi kahdeksan kyseistä käyttöliittymää, joihin yhteyden saa muodostettua ilman salasanaa, ja käyttäjä voi komentoriviltä vapaasti suorittaa komentoja kohdejärjestelmässä. Kolme löydetyistä käyttöliittymistä kuuluivat Simatic HMI (human-machine-interface) paneeleille, joita käytetään automaation hallinnassa. Asiattomien pääsy käsiksi teollisuusjärjestelmiin voi olla hyvinkin tuhoisaa ja vain kokeilumielessäkin tehty tunkeutuminen voi aiheuttaa vaurioita järjestelmässä ja myös sen hallitsemassa fyysisessä ympäristössä.

3.1 Teollisuusautomaatiolaitteiden muut käyttökohteet

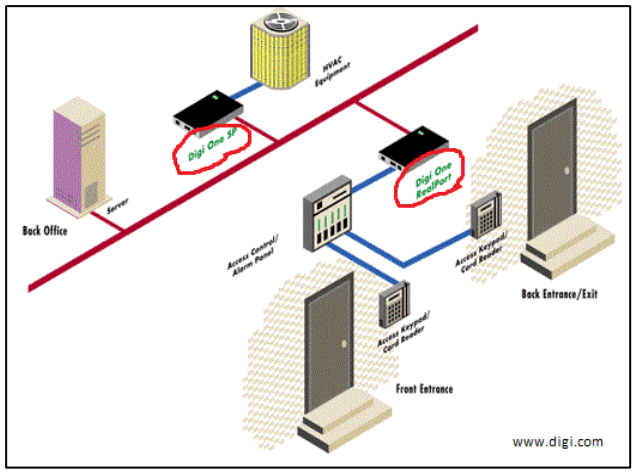
Laitteita, joita käytetään teollisuusautomaation lisäksi myös kaupan alalla ja kiinteistöjenhallinnassa, löytyi yhteensä 520. Nämä sisältävät edellä esiteltyjä hieman kevyemmän kaliiberin laitteita, joita kylläkin käytetään teollisuudessa, mutta myös muilla mainituilla aloilla. Näihin laitteisiin kuuluvat erilaiset automaatioverkkojen kommunikaatiomoduulit, joilla liitetään sarjaliitäntälaitteita (esim. RS-232/422/485-liitännöillä), kuten PLC, ethernet-verkkoon ja sitä kautta yrityksen verkkoon tai Internetin yli tapahtuvaan etäkäyttöön. Tällaisia sarjaliitäntälaitteita käytetään mm. tehtaiden kontrollijärjestelmissä, bensa-asemilla, kaupoissa ja rakennusautomaatiojärjestelmissä. Laitteita löytyi edellämainittujen kohteiden lisäksi muun muassa sähköntuotannon ja vedenjakelun yrityksiltä.

- **EDW-100**: sarjaliitäntälaitteet (esim. PLC) voivat kommunikoida keskenään ethernet-verkon välityksellä. Yht.: 206 kpl
- **Digi One SP ja Realport**: liittämään sarjaliitäntälaitteita ethernet-verkkoon. Yht.: 69 kpl
- **Moxa Nport 5210/5110**: sarjaliitäntälaitteiden etähallinta. Yht.: 34 kpl
- **xweb 500**: hallintapalvelin isolle joukolle sarjaliitäntälaitteita esim. kaupoissa ja bensa-asemilla. Sisältää web-pohjaisen etäkäyttöliittymän. Yht.: 62 kpl

[3] http://en.wikipedia.org/wiki/Stuxnet
[4] http://www.digitalbond.com/tools/basecamp/schneider-modicon-quantum/



Kuva 2: Moxa Nport 5210 tuulimyllyn etäkäytössä



Digi One SP/Realport yhdistämässä rakennuksen automaatiolaitteita

Ylläolevista kuvista vasemmanpuoleisessa esimerkissä Moxa Nport 5210 mahdollistaa tuulimyllyssä olevan PLC:n liitännän verkkoon ja sitä kautta myös mahdollisen etäkäytön. Oikeanpuoleisessa esimerkissä Digi One laitteita käytetään rakennusautomaatiojärjestelmässä LVI-laitteiden ja ovien lukitusten keskittämiseen ja ohjaamiseen. Tällaisten laitteiden näkyminen Internetissa mahdollistaa murtautumisen rakennusautomaatiojärjestelmään ja sitä kautta antaa myös fyysisen pääsyn rakennukseen etäohjaamalla ovien lukituksia.

4. Rakennusautomaatio ja sähkönhallinta

Teollisuuskäytön ulkopuolelta löydetyissä laitteissa oli suuri määrä erilaisia automaatio-komponentteja, joita käytetään muun muassa rakennusautomaatiojärjestelmissä ja sähkön-hallinnassa. Järjestelmästä riippuen rakennusautomaatiolla voidaan hoitaa ja valvoa rakennusten lämmitystä, ilmastointia, veden kulkua, ovien lukkoja, valaistusta ja hälytyksiä. Näitä järjestelmiä löytyi Shodanilla yhteensä 2229 kappaletta, joista suurin osa kuuluu kerrostaloille ja toimisto- ja kauppakiinteistöille. Löydetyissä on siis tavallisia asuinrakennuksia, pieniä kauppoja, tavarataloja, toimistoja ja myös hieman erikoisempia kohteita vähemmässä määrin, kuten jäähalli, vankila, sairaala sekä pankkikonttori. Viimeksimainituimmat ovat isoin huolenaihe, sillä esimerkiksi sairaaloiden lämmityksen ja ilmastoinnin tulee ollaa tarkkaan säädeltyä. On selvää, että yksittäisenä tapauksena tällaisen järjestelmän sabotointi ei välttämättä aiheuta paljoa harmia mutta, jos kyseessä on järjestelmällinen satojen kiinteistöjen sabotointi, seuraukset voivat olla myös yhteiskunnallisesti merkittäviä. Monet rakennusautomaatiojärjestelmät tulevat valmiina paketteina helpottaakseen asennusta ja käyttöönottoa. Tästä syystä erityisesti etähallinta-käyttöliittymät jäävät usein tietoturvamielessä heikoiksi sisältäen esimerkiksi yleisesti tunnettuja oletussalasanoja ja turhaan avoinna olevia tietoliikenneportteja. Tämän seurauksena etäkäyttö-liittymiä on paljon esillä Internetissä ja ne ovat siten helppo kohde hyökkäyksille. Tuore paljastus Niagara -nimisen valmistajan rakennusautomaatiojärjestelmän haavoittuvuudesta[5] on saanut USA:ssa paljon huomiota johtuen sen laajasta käytöstä muun muassa sairaaloissa, sekä hallituksen ja armeijan kiinteistöissä. FBI:n raportin mukaan haavoittuvuus on Niagaran etähallintaohjelmistosta löytyvä takaovi, jolla tunkeutuja pääsee järjestelmään käsiksi ilman tunnistautumista. Suomessa Niagaran rakennusautomaatiojärjestelmiä löytyi 252 kappaletta, joista ainakin 184 käyttää vanhaa Niagaran versiota, jota löydetty haavoittuvuus koskee.

Tila- ja rakennuskohtaisia sähkönhallintajärjestelmiä, sähkön jakelutyksiköitä ja UPS-hallintalaitteita löytyi yhteensä 73 kappaletta. Sähköhallinta liittyy rakennusautomaatioon, mutta pidetään usein erillisenä järjestelmänä. Sähkön jakeluyksikköjä käytetään muun muassa tietokonesaleissa. Löydetyissä kohteet olivat pääasiassa hotelleja ja web-ja hosting-palveluiden tarjoajia.

4.1 Hälyttäviä löytöjä

Tutkimuksessa löytyi paljon erilaisia laitteita, joiden ei kuuluisi olla näkyvillä julkisessa Internetissä. Yleisestä huolimattomuudesta kertoo se, että löysimme useita laitteita, joihin tarvittavat käyttäjätunnukset ja salasanat olivat tallennettuina web-käyttöliittymään, valmiina päästämään

[5] http://arstechnica.com/security/2012/07/ics-security-light-years-behind-itunes/

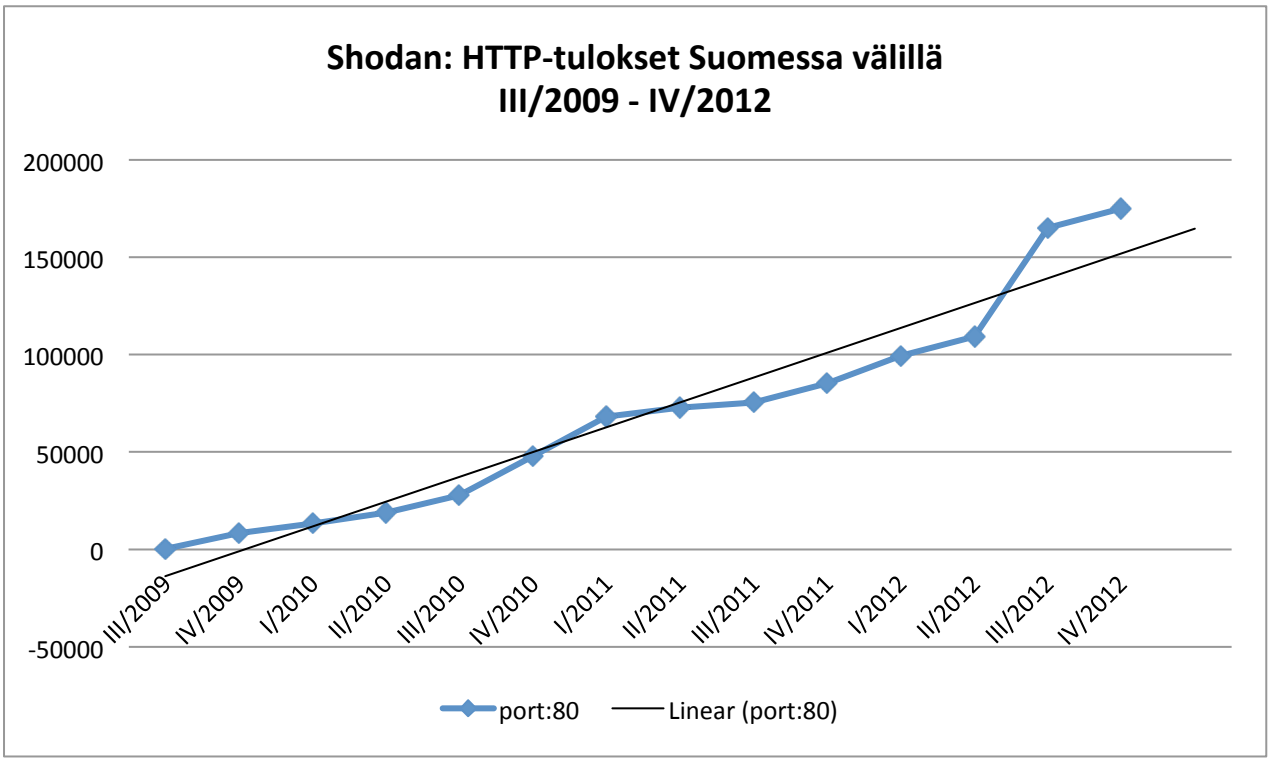
kenet tahansa järjestelmään sisälle. Alla on listattu muutamia hälyttävimpiä löytöjä laitteista, joita raportissa ei ole vielä käsitelty.

- Avoin telnet-portti kahden eri voimalaitoksen laitteessa, ilmeisesti ADSL-reitittimessä
- Avoin telnet-portti tuulimyllyyn liitetyssä laitteessa
- Lämpövoimalan laite, joka vastaa ulkoisiin netBIOS kutsuihin. Voi mahdollistaa sisäverkossa olevien IP- ja MAC-osoitteiden, sekä käyttäjätunnusten vakoilun.
- Vedenkäsittelylaitos: reititin ja palomuuri, avoin telnet-portti
- Vedenhuoltoyrityksen palomuuri/reititin: salasana tallennettuna web-käyttöliittymään
- Vankila: rakennusautomaation hallintajärjestelmä, sekä avoin telnet-portti.
- Liikenteenohjausjärjestelmä

Yllä on listattu avoimia telnet-portteja, koska telnet on vanhentunut ja haavoittuva palvelu, jonka SSH on nykypäivänä korvannut. Telnetin yli kaikki tieto kulkee selvätekstinä ilman salauksia, mikä mahdollistaa esimerkiksi salasanojen kaappaamisen.

5. Arvioita kokonaistilanteesta

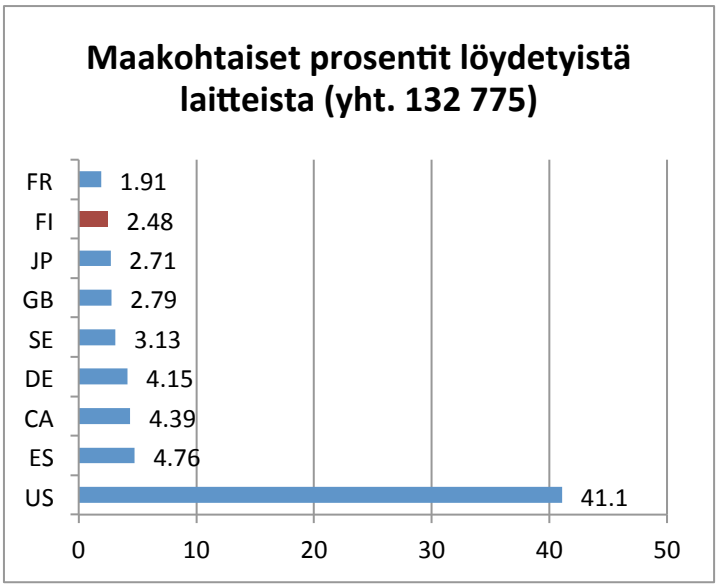
Shodanin löytämien tulosten määrä on jatkuvassa, melko lineaarisessa, kasvussa. Suomen tilannetta tarkasteltaessa kahden viimevuoden aikainen vuosikasvu on ollut lähes 200% per vuosi. Tämän perusteella voidaan olettaa, että Shodan ei ole vielä skannannut kaikkia suomalaisia IP-osoitteita. Skannauksen määrästä on vaikea tehdä arvioita, mutta Shodanin antamat 185 000 HTTP-vastausta kielivät siitä, että Shodan on luultavimmin indeksoinut vasta muutaman kymmenen prosenttia Suomen IP-avaruudesta. HTTP-vastauksia antavien laitteiden kokonais-määrä Suomessa ei ole tiedossa, mutta niiden lukumäärä voi hyvinkin lähennellä miljoona kappaletta. Shodanin Myös löydettyjen automaatiolaitteiden määrän tasainen kasvuu kertoo siitä, että tämä tutkimus on suuntaa antava, eikä paljasta kaikkia Internetissä esillä olevia laitteita.



Kuva 3: Shodanin Suomesta löytämien HTTP-vastausten määrä mitattuna vuosineljänneksittäin vuosien 2009 ja 2012 välillä.

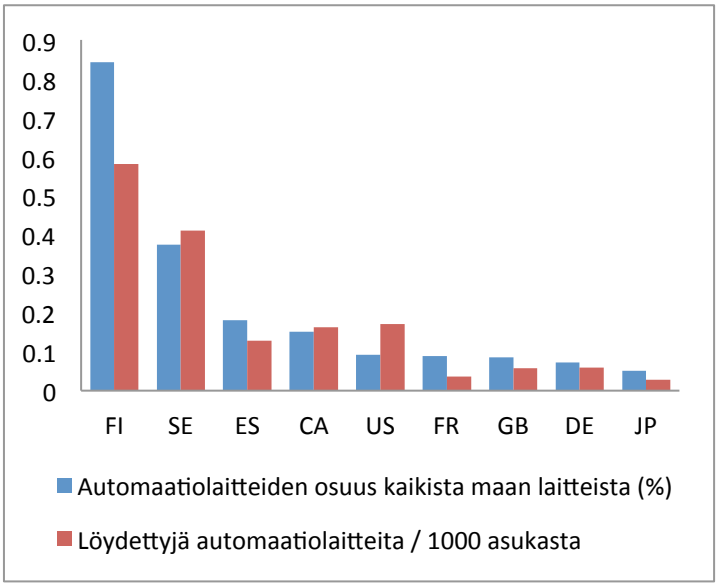
Energiantuotannon, sähkönjakelun ja vedenhuollon aloilta Shodanilla löytyi laitteita yhteensä 35:ltä yritykseltä. Tähän on laskettu mukaan laitteet, jotka ovat mahdollisia hyökkäysrajapintoja yrityksen laitteisiin tai verkkoihin, kuten etäkäyttöliittymät, palomuurit ja reitittimet, VPN:t, automaatiolaitteet, tai haavoittuvat protokollat, kuten telnet, RDP ja netBIOS. Löytöjen vakavuutta on vaikea arvioida ilman järjestelmiin tunkeutumista tai sen yrittämistä. Paljon riippuu myös mahdollisen hyökkääjän taidoista ja motiiveista. Monien Shodanin löytämien laitteiden kohdalla ongelma on siinä, että turvallisuudesta vastaavat tahot eivät oletettavasti tiedä heidän järjestelmien olevan näkyvillä yleisessä Internetissä, eivätkä siksi ole voineet puuttua asiaan. On myös mahdollista, että käytännön asennuksista vastaavat työntekijät eivät ole noudattaneet riittävän tarkasti annettuja

tietoturvaohjeistuksia, ja laitteet ovat jääneet näkyville Internetiin vastoin johdon määräyksiä. Tästä syystä erityisesti yritysten, joiden verkoissa on paljon komponentteja ja muutoksia, tulisi aktiivisesti testata tietoturvan tasoa mahdollisten heikkojen kohtien löytämiseksi.



5.1 Vertailua Suomen ja muiden maiden välillä

Käyttäen 53:n hakusanatermin listaa, teimme vertailua Shodanilla löytyvistä automaatiolaitteista Suomen ja muiden maiden välillä. Vertailumaiksi valittiin Ruotsin lisäksi useampi maa euroopasta, sekä USA, Kanada ja Japani vertailukohdiksi muista maanosista. Hakusanoilla löytyi yhteensä 132775 laitetta, joista iso osa (41%) sijaitsi USA:ssa. Suomi on vertailussa toiseksi viimeisenä 2,5%:n osuudella mutta on yllättävän tasoissa isojen teollisuusmaiden, kuten Japanin ja Iso-Britannian, kanssa. Ensimmäisessä kuvaajassa oikealla on esitetty maiden prosentuaalinen osuus kaikista Shodanilla maailmanlaajuisesti löydetyistä automaatiolaitteista.



Toisessa kuvaajassa havaitaan hieman huolestuttava asia: Suomesta löytyi eniten laitteita suhteutettuna sekä väkilukuun, että löydettyjen laitteiden osuuteen kaikkiin maasta löytyviin Internetissä kiinni oleviin laitteisiin. Esimerkiksi väkilukuun suhteutettuna Ruotsi on ainoa, jonka osuus pääsee lähelle Suomea, ja kokonaismäärässä hallitseva USA on tässä vertailussa keskikastissa. Suomen ja Ruotsin tulos saattaa olla hieman biasoitunut ylöspäin johtuen hakusanalistan pohjautumisesta tutkimukseen Suomesta löytyvistä laitteista, mutta hakusanoina käytettiin myös kahtakymmentä muista lähteistä olevaa termiä, joten pelkästään käytetty lista ei näin suuria eroja selitä. Myöskään rakennusautomaation suuri määrä, noin 75% Suomesta löydetyistä laitteista, ei selitä eroja. Jos rakennusautomaation hakutermit jätetään pois hakutuloksista, Suomi ja Ruotsi ovat väkilukuun suhteutettuna lähes tasoissa mutta yli

kaksikertaisella osuudella verrattuna lähimmäksi pääseviin USA:han ja Kanadaan. Syystä tai toisesta Suomessa on suhteellisesti hyvin paljon automaatilaitteita esillä Internetissä muihin maihin verrattuna. Maidenvälisessä vertailussa käytetty automaatiolaitteiden hakusanalista on annettu viranomaisille.

6. Tulosten jälkitarkastelu

Shodanin tietokannasta löydettyjä tuloksia voidaan pitää suuntaa antavina. Kaikki Shodanin tietokannassa olevat laitteet ovat joskus olleet avoinna yhteyksille Internetistä mutta kaikki eivät sitä välttämättä enää ole. Vaikka jokin laite poistuu Internetistä, eikä ole enää saavutettavissa, Shodanin tietokannasta ei poistu mitään tietoa. Tästä johtuen osa tässäkin tutkimuksessa käytetystä tiedosta on todennäköisesti vanhentunutta – toisaalta jos laite on joskus ollut verkossa, se on voitu silloin kaapata ja järjestelmään murtautua. Ainoa keino tutkia tietyn laitteen tämänhetkinen tila on ottaa yhteys kyseiseen laitteeseen. Saadaksemme raportin tulokset luotettavammalle tasolle, otimme yhteyttä Shodanin löytämiin laitteisiin ja selvitimme kuinka iso osa on edelleen näkyvillä yleisessä Internetissä.

Yhteyksiä laitteisiin otimme Shodanin antamien IP-osoitteiden ja porttien perusteella. Selvitystä nopeutettiin ensin karsimalla IP-osoitteiden listasta pois alhaalla olevat laitteet Nmap-verkkoskannausohjelman avulla. Shodanilla löydetyistä 2915:sta IP-osoitteesta ylhäällä oli Nmap-skannauksen mukaan 1969 laitetta. Nmap tunnistaa laitteen ylhäällä olevaksi mikäli jokin annetuista porteista vastaa yhteyspyyntöihin, joko kieltävästi tai myöntävästi. Tapauksissa, joissa esimerkiksi palomuuria käytetään porttien filtteröintiin, Nmap ei välttämättä tunnista laitetta ylhäällä olevaksi vaikka se sitä todellisuudessa olisi. Selvittääksemme onko tietyssä osoitteessa edelleen sama laite, jonka Shodan paljasti, ylhäällä oleviin laitteisiin otettiin yhteys ja saatuja vastausviestejä verrattiin automaatiolaitteiden avainhakusanalistaan. Lopulliseksi tulokseksi saatiin 1170 IP-osoitetta, jotka edelleen vastaavat yhteyskutsuihin ja joissa ajetaan tässä tutkimuksessa tutkittuja automaatioverkkoihin liittyviä laitteita.

Tulos laitteiden määrästä on suuntaa antava ja oikea määrä on todellisuudessa suurempi. Saatu tulos kertoo tässä tapauksessa alarajan, kuinka monta laitetta tällä hetkellä vähintään on Suomesta löydettävissä. Tunnistusprosessista johtuen osa kiinnostuksen kohteina olevista laitteista jäi varmastikin löytämättä. On myös hyvä muistaa, että Shodanin tietokanta ei sisällä vielä täyttä otosta Suomen IP-avaruudesta, mistä johtuen tulokset eivät voi olla tarkkoja mutta antavat hyvän arvion Suomen tilanteesta automaatiolaitteiden osalta.

Tutkimuksemme osoittaa, että kotimaisilla toimijoilla on paljon haasteita edessään. Osa tuloksista on täysin normaalia toimintaa ja järjestelmien pitääkin olla esillä, mutta on vaikea uskoa, että kaikki löydetyt kohteet ovat tarkoituksella esillä, ja vielä koko Internetin laajuisesti. Mahdollisia ongelmia voi ja pitääkin hallita eri menetelmillä. Kaikki lähtee luonnollisesti kohdejärjestelmän omasta suojasta, mutta tämän päälle voidaan palomuureilla hallita tehokkaasti järjestelmiin pääsyä ja

murtautumisenestolaitteilla (Intrusion Prevention System, IPS) puolestaan valvoa läpipäästettyjä yhteyksiä.

Osa näistä tuloksista saattaa johtua esimerkiksi konfigurointivirheistä, joita valitettavasti tulee, kun on kyse inhimillisestä toiminnasta. Näitä virheitä ja muita ongelmia voi etsiä jatkuvalla järjestelmien skannaamisella. Suomessa on vain muutamia miljoonia IP-osoitteita, jonka päälle tulee virtualisoidut palvelimet – ei siis ihan mahdoton urakka valvoa 24/7.