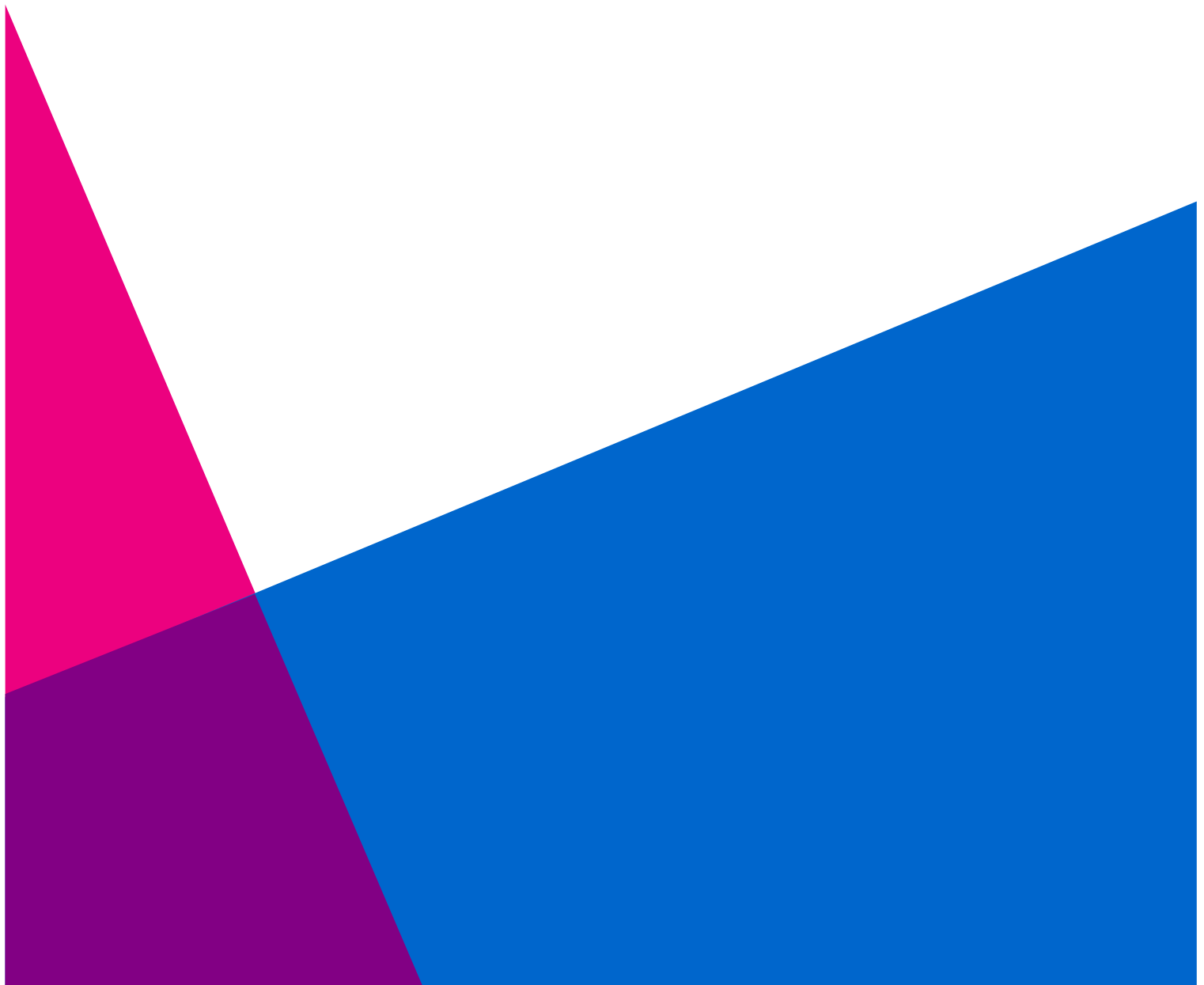


TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2019



Sisällysluettelo

1	Johdanto	2
2	Suojaamattomia automaatiolaitteita suomalaisissa verkoissa	2
3	Keskeisiä tuloksia ja havaintoja vuonna 2019	3
3.1	Teollisuuden hallintajärjestelmät.....	5
3.2	Teollisuusautomaatio.....	5
3.3	Rakennusautomaatio.....	5
3.3.1	Keinoja rakennusautomaatiolaitteiden tilanteen parantamiseksi?	6
4	Muita kartoituksessa tehtyjä havaintoja	6
5	Mahdollisia uhkia	7
6	Miksi hyvä salasana ja laitteen uusin ohjelmistoversio eivät riitä?	8
7	Uhat teollisuudessa	8
8	Vinkkejä teollisuuden tietoturvan parantamiseksi	8
9	Uhat rakennusautomaatiossa	9
10	Vinkkejä rakennusautomaation tietoturvan parantamiseksi	9
10.1	Onko kiinteistössäsi suojaamaton rakennusautomaatiolaitte?	9
11	Avoimesta laitteesta ilmoittaminen laitteiden ylläpitäjille	10
12	Miten toimia ylläpitäjänä?	10
13	Miten kartoittaa omia verkkoja?	12
14	Lähdeluettelo	15

1 Johdanto

Automaatiojärjestelmiä käytetään ohjaamaan ja monitoroimaan mitä erilaisimpia asioita. Käytön helpottamiseksi näihin järjestelmiin ja yksittäisiin laitteisiin saatetaan haluta päästä etänä mistä ja milloin tahansa. Valitettavasti toisinaan helppokäyttöisyys tarkoittaa myös sitä, että rikolliset pääsevät käsiksi laitteisiin mistä tahansa internetistä. Huonoissa tapauksissa rikollinen voi päästä ohjaamaan näiden murrettujen laitteiden kautta tärkeitä järjestelmiä tai murtautumaan muihin samassa verkossa oleviin tärkeämpiin järjestelmiin.

2 Suojaamattomia automaatiolaitteita suomalaisissa verkoissa

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus teki huhtikuussa 2019 vuotuisen kartoituksen, jonka tarkoituksena oli havaita suomalaisissa julkisissa verkoissa toimivat suojaamattomat automaatiolaitteet. Havainnoista on ilmoitettu laitteistojen ja järjestelmien omistajille ja ylläpitäjille.

Kyberturvallisuuskeskus lähetti viestin yhteistyökumppaneilleen ennen skannausten aloittamista. Viestissä kerrottiin skannauksissa käytettävät IP-osoitteet sekä skannausten ajankohta. Asiasta julkaistiin myös Tietoturva Nyt! -artikkeli [1].

Kartoituksen tarkoituksena on luoda tilannekuvaa suomalaisista suojaamattomista automaatiolaitteista, laitteiden määrän kehityksestä, tiedottaa laitteistojen omistajia ja ylläpitäjiä sekä opastaa omistajia laitteistojen suojaamiseksi.

Ennen vuotta 2019 Viestintäviraston Kyberturvallisuuskeskus on tehnyt vastaavia kartoituksia [2], [3], [4], [5], [6]. Näitä on tehty vuodesta 2015 lähtien. Liikenteen turvallisuusvirasto Trafi ja Viestintävirasto sekä Liikenneviraston tietyt toiminnot yhdistyivät Liikenne- ja viestintävirasto Traficomiksi 1.1.2019, ja näin ollen Traficomin Kyberturvallisuuskeskus tekee kartoitukset jatkossa.

Kartoituksessa kiinnitettiin erityistä huomiota kriittisen infrastruktuurin suojaamattomien laitteiden havaitsemiseen ja ilmoittamiseen. Havainnot suojaamattomista rakennusautomaation laitteistoista, joita perinteisesti esiintyy paljon, pyritään ilmoittamaan omistajille ja ylläpitäjille ensisijaisesti suurempina kokonaisuuksina esimerkiksi valmistajien tai maahantuojien kautta sekä tarvittaessa teleoperaattoreiden avulla.

Vuoden 2019 kartoitus tehtiin huhtikuussa, ja havainnoista ilmoitettiin laitteistojen ylläpitäjille kartoituksen tulosten valmistuttua toukokuusta lähtien. Näistä osa oli mahdollista tunnistaa ja ilmoittaa suoraan järjestelmien omistajille. Järjestelmät, joiden omistaja ei selvinnyt, ilmoitettiin teleoperaattoreiden kautta.

Automaatiolaitteet tulkitaan suojaamattomaksi, jos siihen tai sen kirjautumissivulle on pääsy internetistä. Automaatiolaitteita ei useinkaan ole suunniteltu liitettäväksi suoraan internetiin; esimerkiksi laitteeseen kirjautumisia ei kirjata lokiin.

Kartoitus toteutettiin skannaamalla Suomen IP-osoiteavaruuden tiettyjen yleiskäyttöisten ja yleisesti tunnettujen automaation käytössä olevien porttien osalta. Näin saadusta materiaalista on erikseen pyritty tunnistamaan automaatioon liittyviä laitteita esimerkiksi etsimällä viitteitä tuotenimiin tai käyttöpaikkoihin.

Kyberturvallisuuskeskuksen tekemän kartoituksen havaintoja on vertailtu verkon hakukoneiden¹ tuloksiin. Tulokset ovat olleet samansuuntaisia, pieniä eroja on näkynyt, mutta havaintojen suuruusluokat ovat olleet hyvin samankaltaisia.

¹ Mm. Shodan- ja Censys -palvelut.

Vastaavia kartoituksia olisi mahdollista tehdä myös käyttäen ulkopuolisia palveluita, mutta kuten Tiilikaisen lopputyössä [7] mainitaan, Suomen sisältä tehtävien skannausten tiedot jäävät Suomeen, eivätkä ulkopuoliset tahot pysty seuraamaan, mitä palveluita ja haavoittuvuuksia skannauksissa etsitään.

Automaatiojärjestelmien käyttämistä porteista löytyneet laitteet ovat suurella todennäköisyydellä automaatiolaitteita, ja tulosten koostaminen on siten nopeaa. Haasteen etsinnälle asettavat laitteet, joiden hallintaan käytetään yleisessä käytössä olevia portteja kuten esimerkiksi www-selailussa käytettävät portit TCP/80 ja TCP/443. Laitteiden sekä niiden omistajien tai käyttäjien tunnistaminen ei valitettavasti ole aina mahdollista esimerkiksi yksinkertaisella etusivujen tai web-palvelinten nimien skannauksella. Joissakin tapauksissa käyttöpaikan tiedot on voitu kertoa erillisissä kirjautumisikkunoissa tai portaalisivun takana olevilla sivuilla. Yksi esimerkki tällaisista on Siemens S7 -järjestelmän web-portaali. Portaalista on mahdollista päästä varsinaiselle kirjautumisivulle, jossa saatetaan kertoa tarkemmin tietoa laitteesta - kuten sen sijainnista.

Automaatioon liittyviä laitteita etsitään niiden vastauspaketeissa palauttamien tietojen perusteella. Eri laitteet palauttavat laitteisiin liittyvät tiedot hieman eri tavoin, joten laitteiden löytäminen vaatii useita eri tunnistustapoja. Erilaiset palautuneet tiedot johtavat siihen, että kartoituksessa pystytäänkin löytämään vain laitteita ja järjestelmiä, jotka tunnetaan ja joiden tunnistamismenetelmä on tiedossa. Siksi etenkin harvinaisempia järjestelmiä jää pakostakin havaitsematta.

3 Keskeisiä tuloksia ja havaintoja vuonna 2019

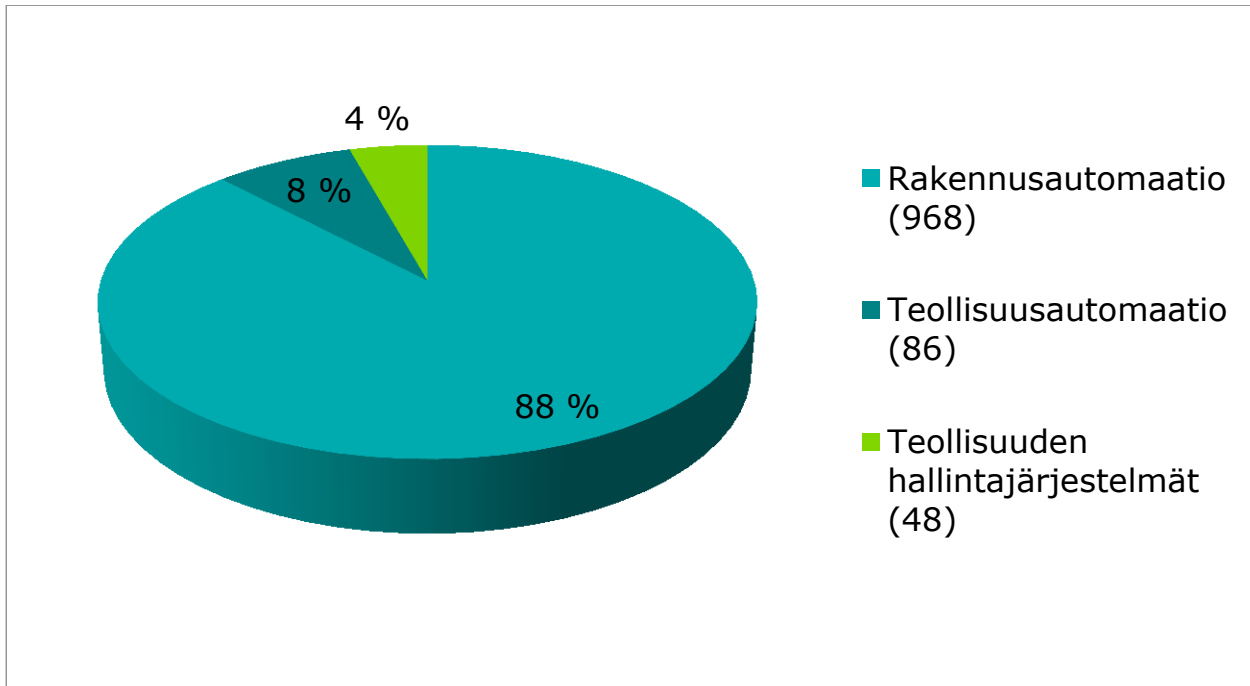
Vuoden 2019 kartoituksessa käytiin läpi reilut 1500 verkkoa ja 14 miljoonaa IP-osoitetta.

Kartoituksessa löytyneet laitteet on jaoteltu seuraaviin luokkiin:

- Kriittiseen teollisuusautomaatioon kuuluvat automaation hallintajärjestelmät (SCADA), näyttöpaneelit (HMI), logiikat (PLC).
- Teollisuusautomaatioon kuuluvat laitteet, joiden takana olevia yksittäisiä järjestelmiä ei pystytä selvittämään. Pääsääntöisesti kyseessä ovat erilaiset protokollamuuntimet.
- Rakennusautomaatioon kuuluvat kiinteistöjen ohjaukseen liittyvät laitteet ja järjestelmät, esimerkiksi hissien, ilmanvaihdon ja lämmityksen ohjaukset.

Muut kriittiseen infrastruktuuriin kuuluvien toimialojen laitteet ilmoitetaan harkinnan mukaan, vaikka ne eivät varsinaisia automaatiolaitteita olisikaan.

Vuoden 2019 kartoituksessa havaittiin eniten erilaisia rakennusautomaatiolaitteita, joita oli hieman alle tuhannessa IP-osoitteessa. Teollisuusautomaatioon kuuluvia järjestelmiä havaittiin hieman alle 90 ja kriittiseen teollisuusautomaatioon kuuluvia järjestelmiä alle 50.



Kuva 1. Havaittujen järjestelmien osuudet ja määrät vuonna 2019

Täsmällisten havaintomäärien sijaan on havainnollisempaa käyttää suuruusluokkia. Teollisuuteen liittyviä järjestelmiä on helpompi kartoittaa verkosta kuin esimerkiksi rakennusautomaatiolaitteita. Tämä johtuu siitä, että teollisuuden järjestelmät käyttävät usein omaan tarkoitukseen määriteltyä porttia, jonka avulla ne voi tunnistaa paremmin. Esimerkiksi rakennusautomaatiojärjestelmät käyttävät usein esimerkiksi porttia TCP/80, jonka avulla laitteen selainhallinta on mahdollista.

Kartoituksessa huomattiin joitakin tapauksia, joissa muutamat eri rakennusautomaatiolaitteet vastasivat yhden IP-osoitteen eri porteissa.

Automaatiolaitteet on mahdollista erottaa muista havainnoista, jos tiedetään, mitä tarkalleen ottaen ollaan etsimässä. Muutoin osa laitteista jää havaitsematta.

Kartoituksessa huomattiin, että osa aikaisemmin suoraan internetiin avoimena olleista rakennusautomaatiolaitteista oli laitettu erillisten keskitettyjen web-käyttöliittymien taakse tehokkaammille web-palvelimille. Tällöin suoria yhteyksiä laitteille ei enää ole, vaan käyttäjän pitää ensin kirjautua internetiin näkyvään keskitettyyn palveluun, josta muodostetaan yhteydet varsinaisten sulautettujen järjestelmien tai automaatiolaitteiden web-palvelimille.

Kartoituksessa havaittiin automaatiolaitteiden ulkonäköä ja ominaisuuksia matkivia hunajapurkkeja². Hunajapurkki on esimerkiksi tunkeilijasta tietoja keräävä järjestelmä, joka pyrkii herättämään hyökkääjän mielenkiinnon tekeytymällä huonosti suojatuksi [8]. Tällaisiin laitteisiin sovellettiin samaa ilmoitusprosessia kuin kaikkiin muihinkin laitteisiin. On todennäköistä, että hunajapurkilta näyttävät järjestelmät ovat hunajapurkkeja, mutta on toki mahdollista (mutta epätodennäköistä), että oikeat järjestelmät olisi asetettu näyttämään hunajapurkeilta [9].

² Yksi palvelu hunajapurkkien löytämiseen on Shodanin "Honeypot or not" -palvelu: <https://honeyscore.shodan.io/>

3.1 Teollisuuden hallintajärjestelmät

Teollisuusautomaation hallintajärjestelmiä havaittiin kartoituksessa lähes 50. Joukossa oli mm. PLC-logiikoita ja HMI-ohjauspaneeleita. Vuoden 2019 kartoituksessa löytyi esimerkiksi elintarviketeollisuuden yritykselle kuulunutta suojaamatonta PLC-logiikkaa.

Teollisuuden järjestelmistä ilmoitettaessa yritykset ottavat yleensä ilmoitukset vakavasti ja reagoivat niihin nopeasti. Pääosin kaikki edellisinä vuosina ilmoitetut järjestelmät on suojattu, eikä niitä ole havaittu enää seuraavina vuosina. Poikkeuksiakin toki on.

3.2 Teollisuusautomaatio

Teollisuuden yksittäisistä suojaamattomista laitteista tehtiin lähes 90 havaintoa. Teollisuuden yksittäiset laitteet ovat pääosin erilaisia protokollamuuntimia.

Modbus-protokolla on tarkoitettu käytettäväksi esimerkiksi ohjauksiin, eikä se sisällä menetelmiä viestinnän osapuolten tunnistamiseen tai sisällön suojaamiseen. Tällaisen portin ollessa auki internetiin siihen voidaan luvattomasti kohdistaa komentoja, jotka laite suorittaa.

Korostamme, että paikallisesti operoitavaksi tarkoitettua laitetta ei ole järkevää kytkeä suoraan ja suojaamatta internetiin. Osa Modbus-protokollalla liikennöivistä laitteista kuuluu rakennusautomaatioon.

3.3 Rakennusautomaatio

Rakennusautomaatioon liittyviä laitteita havaittiin noin 1000 kappaletta.

Rakennusautomaatiolaitteiden suojaukset kohdistetaan mitä luultavimmin uusiin käyttöönotettaviin järjestelmiin. Uudet kohteet on helppo suojata jo suunnitteluvaiheessa, mutta jälkeinpäin suojaukset jäävät usein tekemättä. Valmistajilla on tarjolla valmiita ratkaisuja juuri uusiin järjestelmiin, mutta vanhempien järjestelmien suojaus vaatii laitteiston omistajalta niin omaa aktiivisuutta kuin myös ymmärrystä suojausten tarpeellisuudesta.

Rakennusautomaatioon liittyvissä järjestelmissä havainnot liittyivät kiinteistön ohjauksiin, pääasiassa lämmityksen ja ilmastoinnin ohjausjärjestelmiin tai kiinteistöjen lukituksiin liittyviin aikaohjauksiin.

Edellisten vuosien tapaan kartoituksessa havaittiin useita laitteita, joita ei ollut suojattu edes salasanalla. Tällaisten laitteiden asetuksia on mahdollista helposti muuttaa selaimella ja aiheuttaa haittaa esimerkiksi rakennuksen lämmönsäätöjärjestelmille.

Olemme Kyberturvallisuuskeskuksessa ilahtuneet lukuisista rakennusautomaatioon liittyvien yritysten ja valmistajien yhteydenotoista. Alan toimijat näkevät tilanteen huolestuttavana ja haluavat parantaa järjestelmien suojausta. Saamamme palautteen mukaan laitteistot jäävät yhä valitettavan usein suojaamatta asiakkaan päätöksen vuoksi. Suojaaminen koetaan ehkä liian kalliiksi tai hankalaksi toimenpiteeksi ja suojaamattomuuteen liittyviä uhkia ei todennäköisesti täysin ymmärretä.

Suojaamattomia kauppojen elintarvikkeiden jäähdytysjärjestelmiä havaittiin yhä runsaasti, ja kohteita on ilmoitettu laitteistojen omistajille. Pelkästään hakukoneiden avulla tietyillä hakusanoilla suojaamattomia rakennusautomaatiolaitteita löytyy verkosta useita satoja.

3.3.1 Keinoja rakennusautomaatiolaitteiden tilanteen parantamiseksi?

Tiedotusta suojaamattomien järjestelmien uhkista pitää jatkaa isännöitsijöille ja kiinteistöjen ylläpidosta vastaaville yrityksille ja tätä kautta yrittää lähestyä esimerkiksi asunto-osaakeyhtiöiden hallituksia ja asukkaita. Isännöitsijät voisivat viedä tietoa asiasta taloyhtiöiden hallituksille.

Peräänkuulutamme yhä myös ylläpitopalveluita tarjoavien ja etähallintaa hyödyntävien yritysten, kuten myös tietoturvatuimittajien osallistumista ongelman ratkaisuun. Perinteisten lämmön- ja ilmastoinnin säädön lisäksi rakennusautomaatiolaitteisiin integroidaan yhä enemmän esimerkiksi lukituksia, mittarien etäluentaa ja valaistuksen ohjauksia. Näin myös häiriöt rakennusautomaatiossa vaikuttavat yhä enemmän kiinteistön toimivuuteen ja asumismukavuuteen. Esimerkiksi lämmityshäiriöt voivat aiheuttaa pakkaskaudella mittavia vahinkoja nopeasti.

Laitteistojen suojaaminen ei välttämättä aiheuta suuria kuluja. Joillakin valmistajilla suojatut etäyhteydet kuuluvat peruspalveluun, ja erillisiä suojauksia saa käyttöön jo muutaman sadan euron kertakorvauksella.

Vuosittaisen kartoituksen lisäksi Kyberturvallisuuskeskus kartoittaa Suomesta löytyviä haavoittuvia järjestelmiä, kun tieto niissä olevista haavoittuvuuksista ja/tai hyväksikäytöistä tulee. Näin tehtiin esimerkiksi maaliskuussa 2019 Fidelixin rakennusautomaatiojärjestelmistä löydettyjen haavoittuvuuksien [10], [11], [12] sekä kesäkuussa haavoittuvien Exim-sähköpostijärjestelmien ja cPanel-hallintapaneelien [13] tapauksissa. Tällöin Kyberturvallisuuskeskus lähetti tiedon asiasta laitteiden omistajille tai teleoperaattoreille, joiden verkoissa haavoittuvat laitteet olivat. Kyberturvallisuuskeskus skannaa tiettyjä haavoittuvuuksia toistuvasti useita kertoja vuodessa, ja vertailee miten niiden tulokset muuttuvat. Suomessa Kyberturvallisuuskeskuksen lisäksi myös muut tahot, kuten yritykset [14], [15] ja korkeakoulut [16], [7], [17] tekevät kartoituksia haavoittuvista laitteista ja ilmoittavat niistä niiden omistajille tai viranomaisille. On olemassa myös kaupallisia palveluita erilaisten skannausten tekemiseen. Kartoituksia ja niiden hintoja voi kysellä vaikkapa tietoturvayrityksiltä, operaattoreilta tai tutkimuslaitoksilta. Suomessa korkeakoulujen, tutkimuksen ja opetuksen käyttöön on olemassa Finnish University and Research Network (Funet)³ -tietoverkko, josta pystyy tekemään vastaavia skannauksia tutkimusta varten. Maailmalta löytyy esimerkkejä siitä, miten käyttää avoimista lähteistä saatavaa tietoa automaatiolaitteiden tutkimisessa⁴. Mikäli miettii onko skannauksia järkevää tehdä, voi ajatella, että joku tekee sitä joka tapauksessa [18].

4 Muita kartoituksessa tehtyjä havaintoja

Automaatiolaitteiden lisäksi kartoituksessa havaittiin jälleen suuri määrä verkkoon liitettyjä IoT-laitteita (Internet of Things, esineiden internet). Tällaisiksi tunnistettiin esimerkiksi kotireitittimet, laajakaistamodeemit, tulostimet ja verkkokamerat. Näitä laitteita verkoissa on paljon enemmän kuin esimerkiksi rakennusautomaatiolaitteita. Kannattaa huomioida, että kartoitusajankohta voi vaikuttaa havaintomäärään merkittävästi, koska joukossa on paljon laitteita, jotka eivät ole aina päällä tai verkkoon kytkettyinä. Esimerkkejä tällaisista laitteista ovat tulostimet. Muita syitä siihen, että laitteita voi näkyä huomattavasti enemmän eri ajankohtina, ovat esimerkiksi laitteiden edessä olevien palomuurien palomuurisäännöissä tapahtuneet virheet.

³ Funet-palvelut <https://www.csc.fi/fi/funet-kaikki-palvelut>. Funet Tutkain - haavoittuvuusskanneri <https://www.csc.fi/fi/funet-tutkain-haavoittuvuusskanneri>

⁴ Blogikirjoitus siitä mitä kaikkea automaatiolaitteista voi löytää avoimia lähteitä käyttäen <https://www.icscybersecurityconference.com/intelligence-gathering-on-u-s-critical-infrastructure/>

Erilaiset suojaamattomat laitteet tarjoavat hyökkäjille oikotien kiinteistössä toimivien asukkaiden tai yritysten tietoihin. Kotien lisäksi onkin tärkeää eriyttää rakennusautomaatio- ja IoT-laitteet omiin verkkoihinsa [18] erityisesti teollisuuden ja kaupan alan kiinteistöissä sekä toimistokiinteistöissä, sillä monien IoT-laitteiden suojauksissa on heikkouksia [19]. Älylaitteiden hankinta on ollut valtaosalla suomalaisista ajankohtaista viimeisen vuoden aikana. 49 prosenttia elokuussa 2019 nettitutkimukseen vastanneista ilmoitti olevansa huolissaan myytävien älylaitteiden tietoturvallisuudesta [20].

Etenkin yritysmaailmassa on myös tärkeää poistaa käytöstä kaikki käyttämättömät laitteen palvelut. Kuluttajalaitteista laitevalmistajien tulisi poistaa käytöstä tarpeettomat portit laitteistojen ohjelmistoista ja oletusasetuksista.

Traficom on perustanut tiedonjakoa ja yhteistyötä edistävän IoT-verkoston. Verkostossa mukana olevat eri alojen asiantuntijat voivat aktiivisesti vaikuttaa yhteisesti käsiteltäviin aiheisiin. Traficomın Kyberturvallisuuskeskus on luonut IoT-kuluttajalaitteille ja pilvipalveluille tietoturvaperiaatteita ja niiden täyttämistä kertovan tietoturvamerkkin [21], joka auttaa kuluttajia löytämään tietoturvalliset tuotteet. Tietoturvamerkki myönnetään vain tuotteille tai palveluille, jotka täyttävät Traficomın asettamat tietoturva-vaatimukset [22]. Lisäksi Traficom opastaa kansalaisia ja kuluttajia IoT-laitteiden ja pilvipalveluiden tietoturvalliseen hankintaan ja käyttöön. [23]

5 Mahdollisia uhkia

Suojaamattomana internetissä oleva laite on houkutteleva kohde murtautujille. Laitteen voi valjastaa esimerkiksi osallistumaan palvelunestohyökkäyksiin, tai laite voi tarjota helpon pääsyn yrityksen verkkoon.

Lisää tietoa haavoittuvuuksista voi lukea esimerkiksi CISA:n ICS-CERT:n julkaisemasta katsauksesta [24].

Automaatiolaitteet eivät useinkaan kirjaa lokiin kirjautumisyrityksiä tai laitteeseen kohdistuvaa liikennettä, ja näin murtautumiset tai niiden yritykset jäävät havaitsematta ja tapahtumien selvittäminen myöhemmin voi olla mahdotonta.

Vaikka haavoittuvuustietoja ei tietyille laitteelle löydy, se ei tarkoita, että laite ei olisi haavoittuva. Onko tiedossa, mitkä laitteen portit ovat avoinna ulospäin? Mitä palveluja porteista tarjotaan? Hallintaan käytetyn portin lisäksi laitteessa voi olla avoinna muita palveluita, esimerkiksi FTP ja SNMP. Ovatko näiden palveluiden parametrit muutettavissa (esim. oletussalasanat) ja voiko tarpeettomat palvelut poistaa käytöstä? Mitkä ovat näiden palvelimien versiot ja löytyykö niistä haavoittuvuuksia?

Suojaamattomien automaatiolaitteiden muille järjestelmille muodostama uhka vaihtelee laitteen käyttöympäristön mukaan. Yksittäinen laite asuinkiinteistössä aiheuttaa uhan kyseisen kiinteistön lisäksi usein myös kolmansille osapuolille, esimerkiksi osallistuessaan palvelunestohyökkäykseen. Vastaava laite teollisuudessa aiheuttaa uhan teollisuusprosessin toiminnalle ja muodostaa näin liiketoiminnallisia riskejä.

Teollisuudessa järjestelmien suojaamiseen on käytössä resursseja, jotta tuotannon jatkuminen voidaan varmistaa. Tuotantohäiriöille on helposti laskettavissa rahallinen kustannus, siksi niiden suojaamiseen ollaan valmiita panostamaan enemmän kuin esimerkiksi kiinteistöjen rakennusautomaatiojärjestelmiin.

Myös suojaamattomien rakennusautomaatiolaitteiden kautta on mahdollista aiheuttaa käyttöympäristölle merkittäviä kustannuksia häiritsemällä valaistusta kauppakeskuksissa tai hyväksikäyttämällä automaatiolaitteen mobiililiittymän maksullisia palveluita.

Jos laitteen havaitaan osallistuvan vaikkapa palvelunestohyökkäyksiin tai aiheuttavan tietoturvuhan, teleoperaattorin on mahdollista katkaista tietoliikenneyhteys tietoturvasyistä.

6 Miksi hyvä salasana ja laitteen uusin ohjelmistoversio eivät riitä?

Laadukas salasana ja uusin päivitys pienentävät hyväksikäyttömahdollisuuksia, mutta

eivät suojaa laitetta riittävästi. On täysin mahdollista, että tänään haavoittumaton järjestelmä on huomenna haavoittuva. Haavoittuvan ohjelmiston paikkaaminen valmistajalla ja sen toimittaminen ylläpitäjälle vie parhaimmillaankin paljon aikaa. Voi myös olla, että päivitystä ei koskaan tule saataville.

Hyökkääjät murtavat laitteita automatisoidusti. Kartoituksessa havaittiin, että tietyissä automaatiolaitteissa on käytössä samoja http-palvelinohjelmistoja kuin esimerkiksi laajakaistamodeemeissa. Vastaavissa tilanteissa laitemurron uhriksi voi päätyä myös vahingossa, vaikka varsinainen kohde on täysin toisen tyyppinen laitemalli.

7 Uhat teollisuudessa

Automaatiolaitteeseen kohdistuvalla tietomurrolla tai esimerkiksi palvelunestohyökkäyksellä halutaan vaikuttaa pääasiassa kohdeyritykseen tai sen tuotantoon.

Tuotantokatkoksilla on usein välittömiä vaikutuksia, jotka ovat helposti mitattavissa rahan tai maineen menetyksinä. Teollisuusyrityksen onkin tärkeä kiinnittää huomiota tapaan, jolla sen laitteet on kytketty internetiin ja siihen, miten laitteet tulee suojata.

Suojaamattomana internetiin kytketty laite on paljon helpompi reitti yrityksen verkkoon kuin päivitetty ja kirjautumisia sekä yhteydenottoja kirjaava palvelin. Tietomurron selvittäminen jälkikäteen käy työlääksi tai jopa mahdottomaksi, mikäli laite ei kerää tietoja kirjautumisista tai siihen kohdistuvasta liikennöinnistä. Vaikka big game hunting -tyylisissä [25] tapauksissa onkin toistaiseksi hyödynnetty lähinnä tietojenkalastelua, huonosti suojattuja työasemia ja niihin ujutettuja haittaohjelmia, on myös mahdollista, että rikollinen pääsisi suoraan sisään vanhojen ja huonosti suojattujen automaatiolaitteiden kautta [26].

8 Vinkkejä teollisuuden tietoturvan parantamiseksi

Teollisuuden tietoturvaa on mahdollista parantaa parilla perusasialla:

1. Tunne ympäristösi ja sen laitteet. Yritysten ja teollisuuden ulkorajapintoja on suositeltavaa kartoittaa säännöllisesti. Tällöin esimerkiksi vahingossa internetiin avoinna olevat palvelut huomataan ja järjestelmän turvallisuuden tilanne tulee kartoitettua. Jos kartoituksen tekee ulkopuolinen, näkökulma voi erota oman henkilökunnan näkökulmasta, ja siten on mahdollista saada entistä monipuolisempi näkemys tilanteesta. Huomioi, että automaatioympäristön käytön aikainen skannaaminen automaatioverkossa ei ole järkevää, vaan se on tehtävä suunnitelmallisesti huoltokatkosten yhteydessä.

2. Tutki tai tutkituta verkkosi säännöllisesti. Näin voidaan havaita, onko haavoittuvuuksien korjaaminen onnistunut, toimivatko päivitysprosessit ja onko verkko suunnitellun mukainen. Verkon tutkimisessa voi käyttää niin normaaleja hakukoneita [27] kuin skannaukseen tarkoitettuja palveluita [28].

9 Uhat rakennusautomaatiossa

Hyökkäys tai murto rakennusautomaatiolaitteeseen ei välttämättä näy selvästi tai nopeasti ylimääräisinä kustannuksina. Tosin poikkeuksiakin on. Vuonna 2016 uutisoidussa tapauksessa murtauduttiin suomalaisten jäähallien jäähdytyslaitteistoihin ja onnistuttiin aiheuttamaan jopa 10000 euron kustannukset lähettämällä tekstiviestejä kalliisiin ulkomaisiin numeroihin.

Hyökkääjä voi aiheuttaa kohteelleen myös mittavia seurannaisvahinkoja. Esimerkiksi kauppakeskuksen toimintoja ohjaavaan laitteeseen päässyt murtautuja voi tyhjentää kauppakeskuksen vain valaistusta ohjaamalla. Tällöin laitteen väärinkäytöllä voidaan aiheuttaa mittaviakin kustannuksia.

Yksittäisten rakennusautomaatiolaitteiden tietotekninen ylläpito on vielä suhteellisen harvinaista. Kiinteistön ylläpidon tehostamiseksi laitteita kytketään etäkäyttöön "tökkäämällä" laite internetiin ilman tietoturvan tai suojauksen pohtimista. Tämän jälkeen laite unohdetaan. Rakennusautomaation toteuttaminen tietoturvallisesti heti rakennusvaiheessa on kustannustehokkain malli pitkällä aikavälillä. Samalla turvataan laitteiden ylläpito, varmuuskopiointi, pääsynhallinta ja käyttäjien oikeuksien hallitut muutokset. Edellä mainittuja ominaisuuksia laitteet harvoin tukevat, mutta valmistajan tai kolmannen osapuolen tarjoamana keskitettynä pilvipalveluna on ne mahdollista toteuttaa vanhempiinkin laitteisiin. Esimerkiksi kiinteistön lämmityksen säädön parametrien menettäminen laiterikon tai murron vuoksi voi tulla hyvinkin kalliiksi huonontuneena energiatehokkuutena.

Myös muutokset kiinteistöhuollon ylläpito-organisaatiossa tai koko huoltoyhtiön pääsyoikeuksien vaihtaminen käy helposti keskitetyssä mallissa. Tämä voi nousta tavallista merkityksellisemmäksi seikaksi, esimerkiksi jos kiinteistön sähköistä lukitusta on mahdollista etäohjata.

10 Vinkkejä rakennusautomaation tietoturvan parantamiseksi

Seuraavat tietoturvavinkit ovat alan toimijoille huomion arvoisia:

1. Tietoturvallinen toteutus rakennusprojektin alussa tulee usein paljon edullisemmaksi kuin vastaavan tason saavuttaminen jälkikäteen.
2. Suosi keskitettyjä ratkaisuja. Pääsyyloilla voidaan pienentää tietomurron riskiä, mutta edut keskitetystä ratkaisusta menetetään.
3. Myös mobiililiittymillä yhdistetyt automaatiolaitteet on syytä suojata ja muun muassa poistaa liittymistä mahdollisuus käyttää maksullisia palveluja.

10.1 Onko kiinteistöissäni suojaamaton rakennusautomaatiolaitte?

Rakennusautomaatiolaitteen tunnistaminen suojatuksi tai suojaamattomaksi voi osoittautua vaikeaksi tehtäväksi. Seuraavista vinkeistä on apua tilanteen selvittämisessä:

1. Onko rakennusautomaatiolaitte kytketty verkkoon verkkokaapelilla tai langattomasti? Jos laite ei ole verkossa ja vain paikallisesti operoitavissa, sitä ei voi hyväksikäyttää muualta. Huolehdi kuitenkin laitteen fyysisestä suojaamisesta, muun muassa lukituksesta.

2. Jos laite on kytketty verkkoon, ota selvää esimerkiksi isännöitsijän kautta, kuka pääsee käyttämään laitetta ja miten verkkoyhteys on suojattu. Ota tarvittaessa yhteyttä valmistajaan tai laitteen myyjään, ja tiedustele sieltä erilaisia ratkaisuita laitteen suojaamiseksi.

11 Avoimesta laitteesta ilmoittaminen laitteiden ylläpitäjille

Kyberturvallisuuskeskus ilmoittaa havaituista avoimista järjestelmistä niiden ylläpitäjille. Tavoitettavuutta pyritään parantamaan ilmoittamalla suurempia kokonaisuuksia suoraan ylläpitäjille, jos se vain on mahdollista. Ilmoitustapa toimii esimerkiksi rakennusautomaatiolaitteiden ja kaupan järjestelmien kanssa. Kriittiseen infrastruktuuriin liittyvät havainnot ovat luonteeltaan yksittäisiä; tällöin yhteyttä on otettu suoraan yritykseen.

Suuri osa havaittujen järjestelmien ylläpitäjistä on kuitenkin saavutettavissa vain laitteen käyttämän IP-osoitteen perusteella. Tieto IP-osoitteen haltijasta on teleyrityksillä, joten näissä tapauksissa yhteys ylläpitäjiin tehdään teleyritysten kautta, teleyritysten välittämänä.

Jos Kyberturvallisuuskeskuksen tietoon tulee avoimena verkossa oleva kriittiseen infrastruktuuriin tai teollisuusautomaatioon liittyvä laite, periaatteena on ilmoittaa siitä välittömästi laitteen ylläpitäjälle. Tarvittaessa ilmoitus toistetaan. Kiinteistöautomaatioon liittyvistä yksittäisistä laitteista ilmoitetaan harvemmin, esimerkiksi kerran vuodessa.

12 Miten toimia ylläpitäjänä?

Onko käytössäsi automaatiolaitteita, joita pääset käyttämään etäyhteyden avulla? Jos pääsyä ei ole rajoitettu esimerkiksi VPN-tekniikalla tai pääsyylistalla, on syytä miettiä keinoja yhteyden suojaamiseksi.

- Poista käytöstä turvattomat palvelut, esimerkiksi telnet, jos mahdollista.

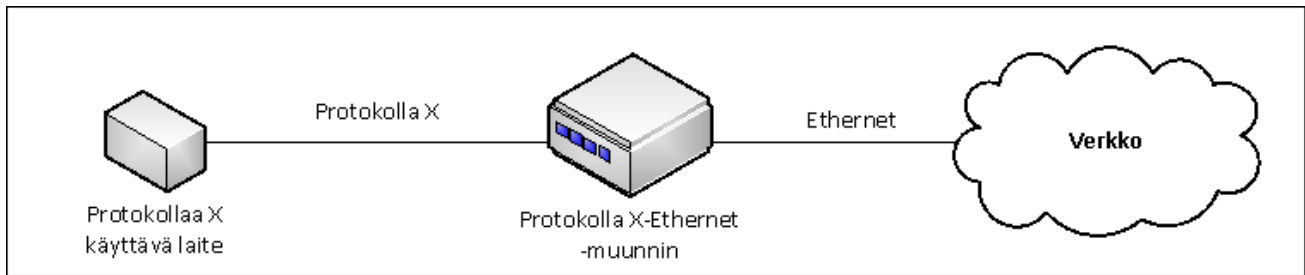
Yksittäisen laitteen suojaaminen palomuurilla voi olla ylläpidollisesti hankala toteuttaa.

- Kysy valmistajalta tai laitteen myyjältä, onko laitteelle olemassa keskitettyä ylläpito- ja pääsynhallintaratkaisua.
- Kysy myös palveluoperaattoriltasi, onko yksittäiseen laitteeseen pääsyä mahdollista rajoittaa operaattorin pääsyylistoilla. Muista, että tällöin menetät keskitetyn ratkaisun suomat edut.
- Skannaa säännöllisesti oman yrityksesi verkkoa. Oma verkko saa ja tulee tutkia säännöllisesti. Huomioi kuitenkin, että automaatioympäristön käytönaikainen skannaaminen automaatioverkossa ei ole järkevää, vaan se on tehtävä suunnitelmallisesti huoltokatkosten yhteydessä. Tällöin esimerkiksi laiteasetuksissa tehdyt inhimilliset virheet tulevat tietoon ylläpidolle, toivottavasti ennen ulkopuolisia.

Rikolliset etsivät verkosta pääsyä automaatiojärjestelmiin automaattisilla menetelmillä. He saattavat käyttää löytämiään järjestelmiä väärin joko itse tai myymällä tiedot eteenpäin. Murrettu laite voi toimia myös porttina yrityksen sisäverkkoon.

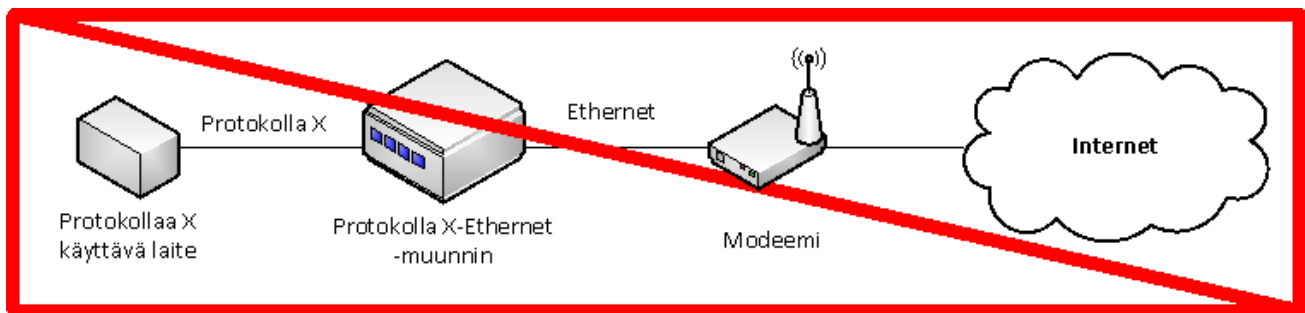
Jos sinulla on automaatiolaitteita kytkettynä suojaamattomana internetiin tai saat ilmoituksen sellaisesta, arvioi, mitkä ovat riittävät suojaustoimenpiteet laitteen turvallisen käytön mahdollistamiseksi. Lisätietoa laitteiden suojaamisesta saa valmistajalta tai laitetoimittajalta. Valitettavasti toisinaan esimerkiksi laitteiden manuaaleissa ei puhuta laitteiden turvaamisesta, vaan esimerkkikuvissa voi olla laitteen yhdistäminen verkkoon kertomatta tarkemmin, mitä verkko tarkoittaa.

Sen pitäisi tarkoittaa sisäverkkoa tai jotenkin muuten suojattua (palomuurilla, VPN-ratkaisuilla, tms.) ja/tai internetistä eristettyä verkkoa. Alla on esimerkkikuva, jollaisen voi nähdä tuotteiden manuaaleissa.



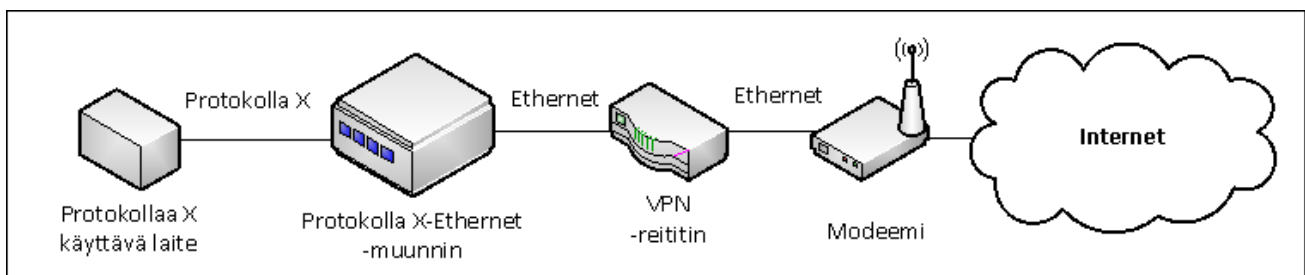
Kuva 2. Esimerkki miten automaatiolaitteen yhdistäminen esitetään toisinaan laitteiden manuaaleissa.

Tämä ei kuitenkaan tarkoita, että kuvan "Verkko" olisi internet tai että automaatiolaitteesta olisi suora yhteys internetiin. On mahdollista, että asia kuitenkin on ymmärretty näin, jolloin automaatiolaitteita on saatettu yhdistää suoraan Ethernet-verkkokaapelilla huoneiston DATA/ATK-pistorasiaan, modeemiin tai reitittimeen tai USB-yhteydellä langattomaan modeemiin (GPRS, 3G, 4G, 5G). Tämä on esitetty kuvassa 2., eikä näin pitäisi koskaan tehdä.



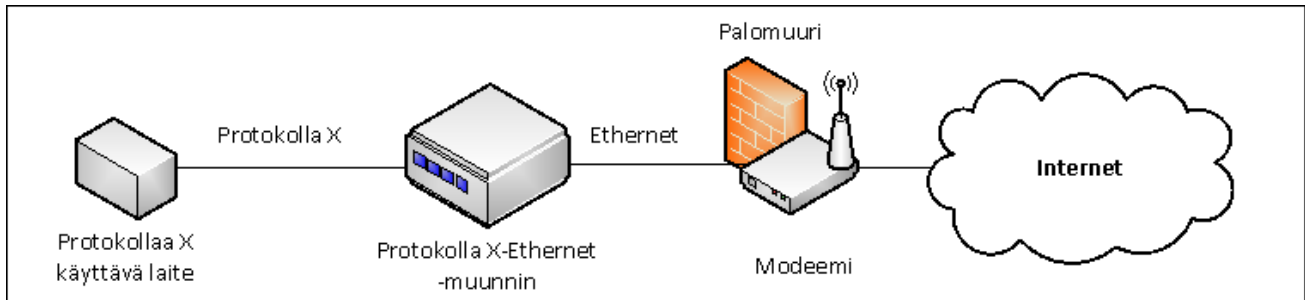
Kuva 3. Älä kytke automaatiolaitteita suoraan langattomiin tai langallisiin modeemeihin äläkä DATA/ATK-pistorasioihin.

Sen sijaan pääsyä voi rajoittaa esimerkiksi VPN-tekniikalla. Automaatiolaitteet voi eriyttää sisäverkkoon, johon pääsee ulkoa internetistä vain ottamalla ensin VPN-yhteyden verkon reunalla olevaan reitittimeen tai erilliseen VPN-laitteeseen.



Kuva 4. Rajoita pääsyä automaatiolaitteille esimerkiksi pelkästään VPN-yhteyksien kautta.

Toinen vaihtoehto rajoittaa pääsyä palomuurien avulla. Näillä voi sallia pääsyn automaatiolaitteille tai niiden käyttämään sisäverkkoon esimerkiksi pelkästään tietyistä IP-osoitteista.



Kuva 5. Rajoita pääsyä automaatiolaitteille esimerkiksi käyttämällä palomureja.

Jos et saa ilmoitusta suojaamattomasta laitteesta, älä silti tuudittaudu turvallisuudentunteeseen. Kyberturvallisuuskeskus ei ole ehkä havainnut käyttämäsi laitetta, tai ilmoitus ei ole saapunut oikeaan paikkaan. Mieti, mitä järjestelmiä sinulla on hallussasi ja miten ne on suojattu. Ota tarvittaessa yhteyttä laitteen valmistajaan tai myyjään tarkempien ohjeiden saamiseksi.

Automaatioon liittyviä uhkia on kuvattu aiemmin Kyberturvallisuuskeskuksen julkaisemissa Tietoturva nyt! -artikkeleissa sekä aiemmissa raporteissa. Nämä ovat yhä ajankohtaisia.

- Tietoturva nyt! Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille (04.03.2019) [29].
- Tietoturva nyt! Automaatiolaitteiden suojaaminen on tärkeää (08.11.2016) [30]
- Tietoturva nyt! Tuhansia automaatiolaitteita suojaamattomina suomalaisissa verkoissa (04.05.2018) [31]
- Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2018 (04.05.2018) [32]
- Tietoturva nyt! [Teema] Huonot etäyhteydet ovat myrkyä automaatiojärjestelmille (20.04.2015) [33]
- Tietoturva nyt! [Teema] Kodin ja teollisuuden älykkäät järjestelmät tulilinjalla (02.04.2015) [34]

13 Miten kartoittaa omia verkkoja?

On olemassa monia ilmaisia ja kaupallisia työkaluja sekä palveluita kartoitusten tekemiseen. Kartoituksia ja haavoittuvuuksien etsimistä voi ostaa myös muiden tekemänä palveluna. On tärkeää muistaa, että jo pelkkä muiden omistamien järjestelmien luvaton skannaus voi olla rikollista sekä aiheuttaa vahinkoa, ja etenkin kirjautuessa luvattomasti muiden omistamiin järjestelmiin voit syyllistyä tietoturtoon.



Varsinainen skannaus on mahdollista usein tehdä varsin nopeasti tai ainakin automatisoidusti, mutta skannaustulosten analysointiin ja raportointiin voi mennä suhteellisesti huomattavan paljon enemmän aikaa. Eri työkaluilla pystytään automatisoimaan monet eri vaiheet kartoituksissa, mutta usein epäselvissä tilanteissa asiantuntijat joutuvat tutkimaan laitteita manuaalisesti vieraillemalla niiden web-sivuilla, käymällä läpi eri portteihin tehtyjen skannausten vastauksia tai vertailemalla tuloksia muiden palveluiden skannaustuloksiin.

Monien automaatiolaitteiden web-palvelinten HTML-sivut tarjoavat toisinaan lisätietoa esimerkiksi siitä, missä laite sijaitsee fyysisesti. Skannaustyökalut käyvät usein läpi vain juuressa olevat sivut, jolloin saadaan selville palvelimen tiedot, mutta ei välttämättä juurikaan muuta. Esimerkiksi DELTA enteliTOUCH -palvelimen juurisivu voi vastata seuraavasti:

```
<html>
  <head>
    <title>Object Moved</title>
  </head>
  <body>
    <h1>Object Moved</h1>
    This object has moved to /deltaweb/hmi_login.asp
  </body>
</html>
```

Mikäli kyseisellä hmi_login.asp -sivulla käy vierailemassa, voi mahdollisesti nähdä tietoja laitteen omistajasta tai palvelun käyttäjästä.


← → ↻ ⓘ Not secure [redacted] /deltaweb/hmi_login.asp

 [redacted] **Sisäänkirjaus** 

Mustan palkin alla on lisätietoa laitteen mahdollisesta fyysisestä sijainnista tai tahosta, joka käyttää laitetta

Käyttäjä:

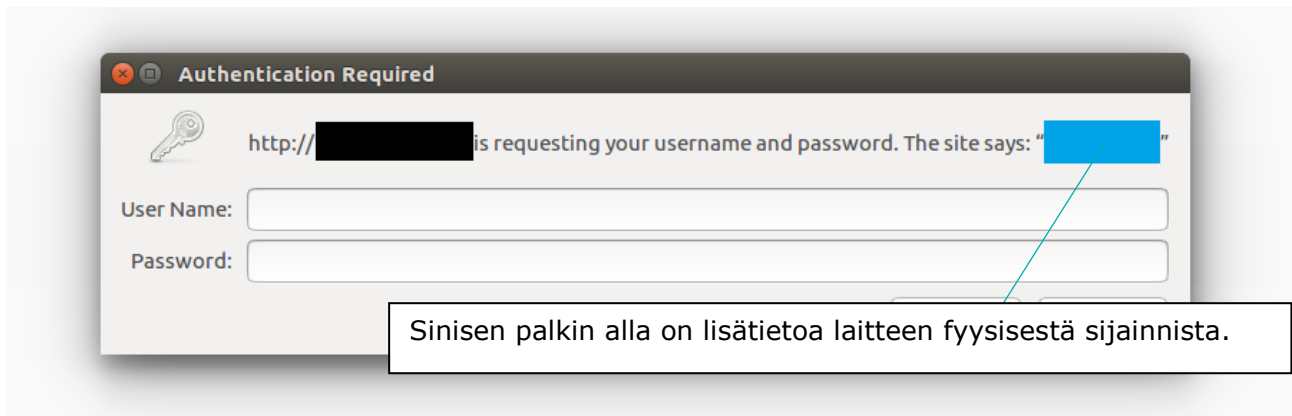
Salasana:


OK

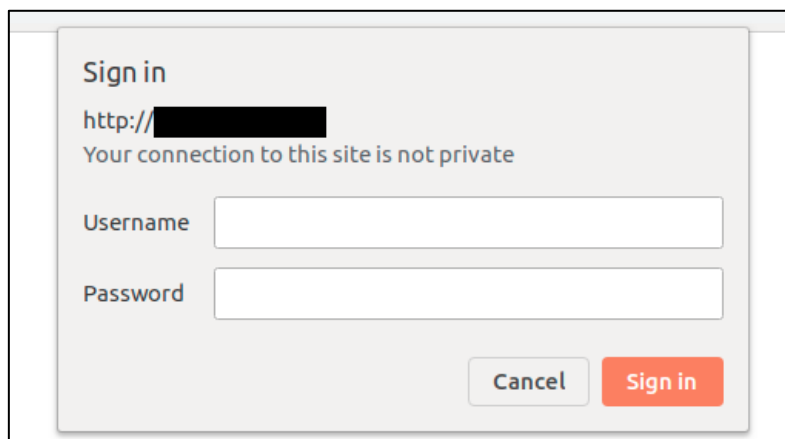
Kuva 6. DELTA enteliTOUCH -päänteen sisäänkirjautumisikkuna

Tämän takia skannauksia tehdessä voi olla järkevää seurata automaattisesti, minne joidenkin palvelimien etusivuilta pääsee. Mikäli tiettyjen automaatiolaitteiden tiedetään tarjoavan tietynlaisia sivuja tietyissä tunnetuissa tai tiettyä formaattia olevissa kansioissa, ne voi olla hyvä käydä myös läpi.

Osa web-sivuista näyttää erilaisista eri selaimia käyttäessä. Esimerkiksi tietyn Niagaran web-palvelimen tulokset Mozilla Firefox ja Chrome -selaimilla eroavat toisistaan. Tämän takia skannaukset voi olla järkevää tehdä yhtäaikaaisesti useita eri selaimia matkivilla skannaustyökaluilla.



Kuva 7. Mozilla Firefox -selaimelle näytetty Niagara-palvelimen kirjautumissivun ikkuna, joka näyttää enemmän tietoja kuin sama sivu Chrome -selaimella. Sinisen laatikon alla on kerrottu kyseessä olevan rakennuksen nimi, jonka avulla pystyi etsimään laitteen omistajan.



Kuva 8. Chrome -selaimelle näytetty saman Niagara-palvelimen kirjautumissivun ikkuna.

Kuten aiemmin mainittiin, kartoituksessa pystytään löytämään vain laitteita ja järjestelmiä, jotka tunnetaan ja joiden tunnistamismenetelmä on tiedossa. Siksi etenkin harvinaisempia järjestelmiä jää pakostakin havaitsematta, samoin kuin järjestelmiä, jotka näyttävät joltain muulta kuin automaatiolaitteilta. Esimerkkinä voi olla automaatiolaitte, jossa pyörii jokin yleisesti muuallakin käytetty web-palvelin. Tällöin kartoituksen tuloksia voi parantaa yhdistelemällä kaikkien porttien skannausten vastaukset yhteen, jolloin automaatiolaitte erikoisine portteineen erottuu usein varsin helposti normaalista web-palvelimesta.

Voit ottaa yhteyttä kartoitukseen liittyen osoitteeseen cert (at) traficom (piste) fi.

14 Lähdeluettelo

- [1] Kyberturvallisuuskeskus, "Tietoturva nyt! Liikenne- ja viestintävirasto Traficom kartoittaa suojaamattomia automaatiojärjestelmiä," 28 03 2019. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-trafficom-kartoittaa-suojaamattomia>.
- [2] Kyberturvallisuuskeskus, "Tietoturva nyt! Viestintävirasto jatkaa selvityksiä automaatiojärjestelmien suojaamattomista yhteyksistä," Viestintävirasto, 16 05 2016. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/05/ttn201605160958.html>.
- [3] Kyberturvallisuuskeskus, "Suojaamattomien automaatiolaitteiden kartoitus 2016," Viestintävirasto, 22 06 2016. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/06/ttn201606221034.html>.
- [4] Kyberturvallisuuskeskus, "Tietoturva nyt! Suojaamattomia automaatiolaitteita runsaasti kotimaisissa tietoverkoissa," Viestintävirasto, 18 05 2017. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/05/ttn201705181420.html>.
- [5] Kyberturvallisuuskeskus, "Tietoturva nyt! Viestintävirasto kartoittaa suojaamattomia automaatiojärjestelmiä ja haavoittuvia verkkopalvelimia," Viestintävirasto, 16 03 2017. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/03/ttn201703161053.html>.
- [6] Kyberturvallisuuskeskus, "Tietoturva nyt! Viestintävirasto kartoittaa suojaamattomia automaatiojärjestelmiä," Viestintävirasto, 29 01 2018. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801291036.html>.
- [7] S. Tiilikainen, Improving the National Cyber-security by Finding Vulnerable Industrial Control Systems from the Internet, Espoo: Aalto University, 2014, p. 7+65.
- [8] Valtiovarainministeriö, "Tietoturvapoikkeamatilanteiden hallinta," Valtiovarainministeriö, 2017.
- [9] VTT, "Webinar: Cyber deception - Defend your organisation from cyber attacks," VTT Technical Research Centre of Finland Ltd, 2018.
- [10] T. Keränen, "Yle testasi: Näin helposti hakkeri pystyy pistämään taloyhtiön lämmityksen ja ilmastoinnin sekaisin," YLE, 04 03 2019. [Online]. Available: <https://yle.fi/uutiset/3-10669307>.
- [11] Fidelix, "Fidelix mukana YLE:n "Team Whack: kaikki on hakkeroitavissa" -ohjelmasarjassa," Fidelix, 04 03 2019. [Online]. Available: <https://www.fidelix.fi/fidelix-mukana-ylen-team-whack-kaikki-on-hakkeroitavissa-ohjelmasarjassa/>.
- [12] YLE, "Docstop: Team Whack - kaikki on hakkeroitavissa - Jakso 1: Team Whack iskee taloyhtiöön," YLE, 04 03 2019. [Online]. Available: <https://arena.yle.fi/1-4664683>.
- [13] Kyberturvallisuuskeskus, "VAROITUS 1/2019: Exim-sähköpostipalvelimen haavoittuvuuden avulla tehdään tietomurtoja," Liikenne- ja viestintävirasto Traficom, 10 06 2019. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/fi/exim-sahkopostipalvelimen-haavoittuvuuden-avulla-tehdään-tietomurtoja>.
- [14] Nixu, "Internetin heikot kohdat Suomessa," 17 Lokakuu 2013. [Online]. Available: <https://www.nixu.com/fi/release/internetin-heikot-kohdat-suomessa>.
- [15] T. Suominen, "Help needed — who owns these building automation appliances?," Remod, 30 04 2019. [Online]. Available: <https://medium.com/remod/fidelix-fi-helping-those-exposed-e69654bdd7c6>.
- [16] S. Tiilikainen ja J. Manner, "Suomen automaatioverkkojen haavoittuvuus," Aalto-yliopisto, Espoo, 2013.

- [17] T. Järekallo, *Methods for Identification and Classification of Industrial Control Systems in IP Networks*, Espoo: Aalto University, 2016, p. 7+55.
- [18] FBI, "Tech Tuesday: Internet of Things (IoT)," 03 12 2019. [Online]. Available: <https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot>.
- [19] Viestintävirasto, "Tietoturva nyt! [Teema] Näistä aineksista syntyy toimivaa IoT:tä," 09 11 2017. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/11/ttn201711091326.html>.
- [20] Kyberturvallisuuskeskus, "Joka toinen suomalainen on huolissaan älylaitteiden tietoturvasta," 2019. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Joka%20toinen%20suomalainen%20on%20huolissaan%20%C3%A4lylaitteiden%20tietoturvasta.pdf>.
- [21] Kyberturvallisuuskeskus, "Tietoturva nyt! Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitteiden hankintoja," 26 11 2019. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomi-aloittaa-alylaitteiden-turvallisuuden-varmistamisen-ensimmaisena-euroopassa>.
- [22] Liikenne- ja viestintävirasto Traficom, "Tietoturvamerkki," [Online]. Available: <https://tietoturvamerkki.fi/>.
- [23] Traficom, "Traficom - Tulevaisuustyö," 2019. [Online]. Available: <https://www.traficom.fi/fi/traficom/tietoa-meista/tulevaisuustyo>.
- [24] CISA ICS-CERT, "Overview of Cyber Vulnerabilities," [Online]. Available: <https://www.us-cert.gov/ics/content/overview-cyber-vulnerabilities>. [Haettu 14 11 2019].
- [25] Kyberturvallisuuskeskus, "Tietoturva nyt! Edistyneet kiristysyökkäykset yleistyvät – Varo joutumasta saaliiksi!," 06 06 2019. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/edistyneet-kiristysyokkaykset-yleistyvat-varo-joutumasta-saaliiksi>.
- [26] T. Väisänen, L. Trinberg ja N. Pissanidis, "I accidentally malware - what should I do... is this dangerous? Overcoming inevitable risks of electronic communication," NATO CCD COE, Tallinn, 2016.
- [27] S. Noponen ja J. Pärssinen, "Hakukoneet ja tietoturva," VTT, 05 07 2017. [Online]. Available: <https://vttblog.com/2017/07/05/hakukoneet-ja-tietoturva/>.
- [28] S. Noponen ja J. Pärssinen, "Miten Shodania käytetään?," VTT, 05 07 2017. [Online]. Available: <https://vttblog.com/2017/07/05/miten-shodania-kaytetaan/>.
- [29] Kyberturvallisuuskeskus, "Tietoturva Nyt! Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille," 04 03 2019. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa>.
- [30] Kyberturvallisuuskeskus, "Tietoturva nyt! Automaatiolaitteiden suojaaminen on tärkeää," Viestintävirasto, 08 11 2016. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/11/ttn201611081338.html>.
- [31] Kyberturvallisuuskeskus, "Tietoturva nyt! Tuhansia automaatiolaitteita suojaamattomina suomalaisissa verkoissa," 04 05 2018. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/04/ttn201805041320.html>.
- [32] Kyberturvallisuuskeskus, "Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2018," Viestintävirasto, 2018.
- [33] Kyberturvallisuuskeskus, "Tietoturva nyt! [Teema] Huonot etäyhteydet ovat myrkyä automaatiojärjestelmille," Viestintävirasto, 20 04 2015. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/04/ttn201504201735.html>.

- [34] Kyberturvallisuuskeskus, "Tietoturva nyt! [Teema] Kodin ja teollisuuden älykkäät järjestelmät tulilinjalla," Viestintävirasto, 02 04 2015. [Online]. Available: <https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/03/ttn201504011647.html>.

**Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus**

PL 320, 00059 TRAFICOM
p. 029 534 5000

[kyberturvallisuuskeskus.fi](https://www.kyberturvallisuuskeskus.fi)

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus