TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2020

Traficomin julkaisuja

5/2021

Sisällysluettelo

1 Johdanto

Automaatiojärjestelmiä käytetään ohjaamaan ja monitoroimaan monenlaisia kokonaisuuksia. Käytön helpottamiseksi näihin järjestelmiin ja yksittäisiin laitteisiin saatetaan haluta päästä etänä mistä ja milloin tahansa.

Toisinaan helppokäyttöisyys tarkoittaa sitä, että myös rikolliset pääsevät käsiksi laitteisiin mistä tahansa internetistä. Murrettujen laitteiden kautta rikollinen voi päästä ohjaamaan tärkeitä järjestelmiä tai murtautumaan muihin samassa verkossa oleviin tärkeämpiin järjestelmiin.

Kartoitimme suomalaisten verkkojen turvallisuutta etsimällä verkosta suojaamattomia automaatiolaitteita. Vuonna 2020 havaitsimme niitä noin tuhat. Määrä ei juuri poikkea edellisvuoden tuloksista.

2 Kartoitus suojaamattomista automaatiolaitteista suomalaisissa verkoissa

Automaatiojärjestelmillä tarkoitetaan laitteita, joilla tai joiden avulla pystytään esimerkiksi säätämään digitaalisesti etäyhteyksien avulla erilaisia fyysisiä muuttujia kuten huoneen tai pakastimen lämpötilaa. Näitä ovat esimerkiksi hallintajärjestelmät, erilaiset näyttöpaneelit, protokollamuuntimet ja kiinteistöjen lukituksen, hissien, ilmanvaihdon, lämmityksen tai jäähdytyksen ohjaamiseen käytetyt järjestelmät.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksessa tehtiin toukokuussa 2020 vuotuinen kartoitus, jonka tarkoituksena oli havaita suomalaisissa julkisissa verkoissa toimivat suojaamattomat automaatiolaitteet. Havainnoista ilmoitimme laitteistojen ja järjestelmien omistajille ja ylläpitäjille.

Lähetimme viestin yhteistyökumppaneillemme ennen skannauksien aloittamista. Viestissä kerroimme skannauksissa käytettävät IP-osoitteet ja skannauksien ajankohdan. Julkaisimme aiheesta huhtikuussa 2020 Tietoturva Nyt! -artikkelin [1].

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

Vuosina 2015-2019 Viestintäviraston Kyberturvallisuuskeskus teki vastaavia kartoituksia. Liikenteen turvallisuusvirasto Trafi ja Viestintävirasto sekä Liikenneviraston tietyt toiminnot yhdistyivät Liikenne- ja viestintävirasto Traficomiksi 1.1.2019, ja siitä lähtien Traficomin Kyberturvallisuuskeskus on tehnyt kartoitukset [2].

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

Vuoden 2020 kartoituksen teimme toukokuussa. Ilmoitimme havainnoistamme 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.

Automaatiolaite tulkitaan suojaamattomaksi, jos siihen tai sen kirjautumissivulle on pääsy internetistä. Automaatiolaitteita ei useinkaan ole suunniteltu liitettäväksi

suoraan internetiin; esimerkiksi laitteeseen kirjautumisia ei välttämättä kirjata lokeihin.

Toteutimme kartoituksen skannaamalla Suomen IP-osoiteavaruuden tietyt yleiskäyttöiset ja yleisesti tunnetut automaation käytössä olevat portit. Näin saadusta materiaalista pyrimme erikseen tunnistamaan automaatioon liittyviä laitteita esimerkiksi etsimällä viitteitä tuotenimiin tai käyttöpaikkoihin.

Olemme vertailleet kartoituksemme havaintoja verkon hakukoneiden[1] tuloksiin. Tulokset ovat olleet samansuuntaisia, erojakin havaitsimme, mutta havaintojen suuruusluokat ovat olleet samankaltaisia.

Vastaavia kartoituksia olisi mahdollista tehdä myös käyttäen ulkopuolisia palveluita, mutta kuten Tiilikaisen lopputyössä [3] mainitaan, Suomen sisältä tehtävien skannauksien tiedot jäävät Suomeen, eivätkä ulkopuoliset pysty seuraamaan, mitä kaikkia palveluita ja haavoittuvuuksia skannauksissa etsitään.

Automaatiojärjestelmien käyttämistä porteista löytyneet laitteet ovat suurella todennäköisyydellä automaatiolaitteita, ja tulosten koostaminen on siten nopeaa. Haasteellisia ovat laitteet, joiden hallintaan käytetään yleisessä käytössä olevia portteja kuten esimerkiksi www-selailussa käytettävät portit TCP/80 ja TCP/443. Laitteiden ja 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 kirjautumissivulle, 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 2020

Vuoden 2020 kartoituksessa käytiin läpi reilut 1280 verkkoa ja noin 12,8 miljoonaa IP-osoitetta.

Kartoituksessa löytyneet laitteet on jaoteltu seuraaviin luokkiin:

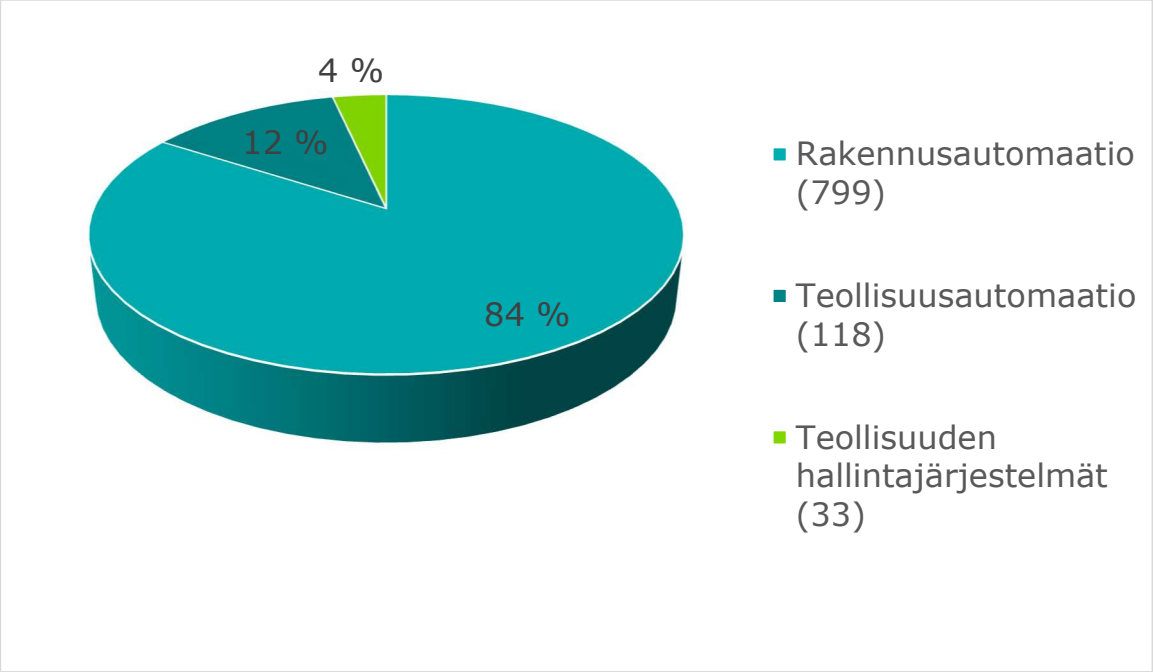
- Kriittiseen teollisuusautomaatioon kuuluvat automaation hallintajärjestelmät (SCADA), näyttöpaneelit (HMI), logiikat (PLC).
- Teollisuusautomaatioon kuuluvat laitteet, joiden takana olevia yksittäisiä järjestelmiä ei pystytä selvittämään. Pääsääntöisesti kyseessä ovat erilaiset protokollamuuntimet.
- 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. Esimerkiksi IoT-laitteista (kuten turhan avoimista CoAP ja MQTT-protokollia käyttävistä järjestelmistä) tehtiin lukuisia havaintoja ja joitakin ilmoituksia).

Vuoden 2020 kartoituksessa havaitsimme eniten erilaisia rakennusautomaatiolaitteita, joita oli noin 800 eri IP-osoitteessa.

[1] Mm. Shodan- ja Censys -palvelut.

Teollisuusautomaatioon kuuluvia järjestelmiä havaittiin noin 120 ja kriittiseen teollisuusautomaatioon kuuluvia järjestelmiä noin 30 eri IP-osoitteessa.



Kuva 1. Havaittujen järjestelmien osuudet ja määrät vuonna 2020

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 huomasimme 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.

Huomasimme, 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.

Havaitsimme joitakin automaatiolaitteiden ulkonäköä ja ominaisuuksia matkivia hunajapurkkeja[2]. Hunajapurkki on esimerkiksi tunkeilijasta tietoja keräävä järjestelmä, joka pyrkii herättämään hyökkääjän mielenkiinnon tekeytymällä huonosti suojatuksi [4]. Tällaisiin laitteisiin sovellettiin samaa ilmoitusprosessia kuin kaikkiin muihinkin laitteisiin. On todennäköistä, että hunajapurkilta näyttävät järjestelmät ovat hunajapurkkeja, mutta on toki mahdollista (tosin epätodennäköistä), että oikeat järjestelmät olisi asetettu näyttämään hunajapurkeilta.

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

3.1 Teollisuuden hallintajärjestelmät

Teollisuusautomaation hallintajärjestelmiä havaittiin kartoituksessa noin 30. Tähän kategoriaan lasketaan muun muassa PLC-logiikat ja HMI-ohjauspaneelit.

Jos teollisuuden järjestelmien omistajat löytyvät ja saadaan kiinni, vastaanottajat ottavat ilmoitukset yleensä vakavasti ja reagoivat niihin nopeasti. Pääosin kaikki edellisinä vuosina ilmoittamamme järjestelmät on suojattu, eikä niitä ole havaittu enää seuraavina vuosina. Poikkeuksiakin toki on.

3.2 Teollisuusautomaatio

Teollisuuden yksittäisistä suojaamattomista laitteista teimme noin 120 havaintoa. Teollisuuden yksittäiset laitteet ovat pääosin erilaisia protokollamuuntimia. Mukana oli myös esimerkiksi KVM-over-IP-etäyhteysratkaisuja.

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 havaitsimme noin 800 kappaletta.

Rakennusautomaatiolaitteiden suojaukset kohdistetaan mitä luultavimmin uusiin käyttöönotettaviin järjestelmiin. Uudet kohteet on helppo suojata jo suunnitteluvaiheessa, mutta jälkeenpäin 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 havaitsimme yhä runsaasti ja ilmoitimme niistä laitteistojen omistajille. Pelkästään hakukoneiden avuilla 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 yrittää lähestyä esimerkiksi asunto-osakeyhtiöiden hallituksia ja asukkaita. Isännöitsijät voisivat viedä tietoa asiasta taloyhtiöiden hallituksille.

Peräänkuulutamme yhä myös ylläpitopalveluita tarjoavien ja etähallintaa hyödyntävien yritysten sekä tietoturvatoimittajien 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.

4 Muita kartoituksessa tehtyjä havaintoja

Vuosittaisen kartoituksen lisäksi kartoitamme Suomesta löytyviä haavoittuvia järjestelmiä, kun saamme tietoa niissä olevista haavoittuvuuksista/hyväksikäytöistä. Näin tehtiin esimerkiksi maaliskuussa, kun kartoitimme muun muassa avointen etätyöpöytäyhteyksien ja tiedostonjakopalveluiden (esim. RDP, VNC ja SMB) määriä [5]. Laaja siirtymä etätyöhön näkyi maaliskuussa suojattomien laitteiden määrän selvänä kasvuna Suomen verkoissa. Suomessa sellaisten laitteiden, joissa tämänkaltaisia etäyhteyspalveluita on avoinna julkiseen internetiin, määrä kasvoi melkein neljänneksellä verrattuna tammi-helmikuuhun. Kehityssuunta oli huolestuttava, koska internetiin näkyvät etäyhteyspalvelut altistavat laitteen ja sen käyttäjät mahdollisten haavoittuvuuksien hyödyntämiselle ja luvattomille kirjautumisyrityksille. Rikolliset etsivät murrettavia palveluita verkosta automatisoidusti ja yrittävät tunkeutua niihin. Etätyöpöytäratkaisuja on käytössä myös joissakin automaatiojärjestelmissä. Maailmalla raportoitiin, että myös suojaamattomien automaatiolaitteiden määrä kasvoi mahdollisesti etätöiden lisääntymisen takia [6].

Kartoituksen jälkeen lähetimme tiedon asiasta laitteiden omistajille tai teleoperaattoreille, joiden verkoissa löydetyt turhan avoimet laitteet olivat. Kyberturvallisuuskeskuksessa skannataan tiettyjä haavoittuvuuksia toistuvasti useita kertoja vuodessa ja verrataan, miten niiden tulokset muuttuvat. Suomessa Kyberturvallisuuskeskuksen lisäksi myös esimerkiksi yritykset [7], [8] ja korkeakoulut [9], [3], [10] tekevät kartoituksia haavoittuvista laitteista ja ilmoittavat niistä niiden omistajille ja/tai viranomaisille. On olemassa myös kaupallisia palveluita erilaisten skannauksien tekemiseen. Kartoituksia ja niiden hintoja voi kysellä tietoturvayrityksiltä, operaattoreilta ja 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

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

automaatiolaitteiden tutkimisessa[4]. Jos joku miettii onko skannauksia järkevää tehdä, niin voi ajatella, että joku tekee sitä maailmalla joka tapauksessa [11].

Automaatiolaitteiden lisäksi kartoituksessa havaittiin verkkoon liitettyjä IoT-laitteita (Internet of Things, esineiden internet). Tällaisiksi tunnistettiin esimerkiksi kotireitittimet, laajakaistamodeemit, tulostimet ja verkkokamerat. Näitä laitteita verkoissa on enemmän kuin esimerkiksi rakennusautomaatiolaitteita. Kannattaa huomioida, että kartoitusajankohta voi vaikuttaa havaintomäärään merkittävästi, koska joukossa on aina laitteita, jotka eivät ole koko ajan 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.

Esimerkiksi MQTT-protokollaa käyttäviä turhan avoimesti internetiin palvelujaan tarjoavia todennäköisiä IoT-laitteita nähtiin noin 140:ssä eri IP-osoitteessa. Vertailun vuoksi: VarIoT -projektissa havaittiin Suomessa 12.3.2020 noin 140 [12], 30.3.2020 noin 130 [13] ja 30.4.2020 noin 210 [13] turhan avointa MQTT-viestien välittäjää (broker), joiden tietoja pääsi lukemaan anonyymisti. Mikäli MQTT-viestien välittäjien ei tarvitse näkyä julkiverkoissa kaikille, yhteyttä ottavat MQTT asiakasohjelmat (client) on hyvä todentaa ja pääsyä niihin rajoittaa palomuurien avulla.

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 [14].

Yhdysvaltojen viranomaiset NSA ja CISA julkaisivat heinäkuussa 2020 varoituksen [15] kuinka eri toimijat ovat kiinnostuneita hyökkäämään kriittistä infrastruktuuria vastaan hyödyntämällä Internetiin yhteydessä olevien automaatiolaitteiden haavoittuvuuksia. Samassa varoituksessa on kuvattu myös neuvoja laitteiden suojaamiseen.

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 tietylle 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

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

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 tietoturvauhan, 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 toinen 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 helpompi reitti yrityksen verkkoon kuin päivitetty ja kirjautumisia sekä yhteydenottoja kirjaava palvelin. Tietomurron selvittäminen jälkikäteen käy työlääksi tai jopa mahdottomaksi, jos laite ei kerää tietoja kirjautumisista tai siihen kohdistuvasta liikennöinnistä. Vaikka big game hunting -tyylisissä [16] 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 [17]. Maailmalla esimerkiksi uutisoitiin, kuinka Israelin vesihuoltosektorin ohjausjärjestelmiä pyrittiin manipuloimaan luvattomasti [18].

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 [19] kuin skannaukseen tarkoitettuja palveluita [20]. Verkkojen eristämisen ja eriyttämisen toimivuus on myös hyvä tarkastaa säännöllisesti verkkojen sisältä, esimerkiksi kun verkon palomuurien tai muiden verkon reunalla olevien laitteiden sääntöihin tehdään muutoksia.

9 Uhat rakennusautomaatiossa

Hyökkäys tai murto rakennusautomaatiolaitteeseen ei välttämättä näy selvästi tai nopeasti ylimääräisinä kustannuksina. Tosin poikkeuksiakin on. Esimerkiksi 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 suuriakin 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 usein 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 ne on mahdollista saada myös vanhempiinkin laitteisiin. Esimerkiksi kiinteistön lämmityksen säädön parametrien menettäminen laiterikon tai murron vuoksi voi tulla hyvinkin kalliiksi huonontuneena energiatehokkuutena.

Myös muutokset kiinteistönhuollon 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 edullisemmaksi kuin vastaavan tason saavuttaminen jälkikäteen.
2. Suosi keskitettyjä ratkaisuja. Pääsylistoilla 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 kiinteistössäni suojaamaton rakennusautomaatiolaite?

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

1. Onko rakennusautomaatiolaite 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 välittäminä.

Jos tietoomme tulee avoimena verkossa oleva kriittiseen infrastruktuuriin tai teollisuusautomaatioon liittyvä laite, periaatteenamme on ilmoittaa siitä välittömästi laitteen ylläpitäjälle. Tarvittaessa toistamme ilmoituksen. Kiinteistöautomaatioon liittyvistä yksittäisistä laitteista ilmoitamme harvemmin, esimerkiksi kerran vuodessa.

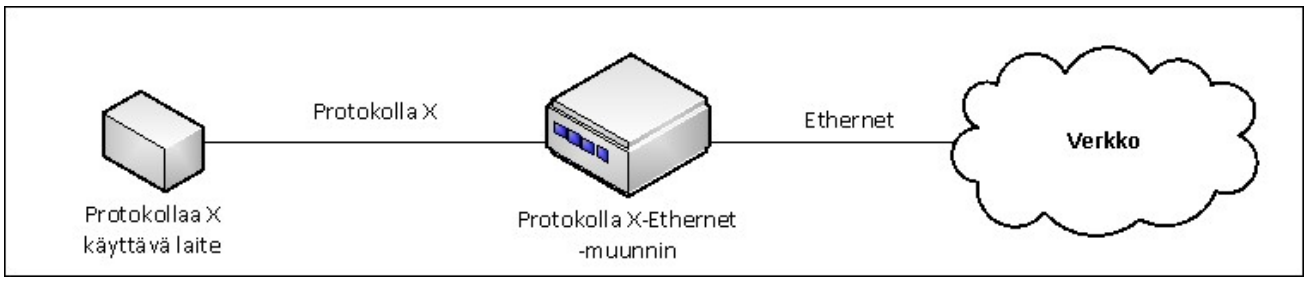
12 Miten toimia ylläpitäjänä?

Onko käytössäsi automaatiolaitteita, joita pääset käyttämään etäyhteyden avulla? Jos pääsyä ei ole rajoitettu esimerkiksi VPN-tekniikalla tai pääsylistalla, 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 pääsylistoilla. Muista, että tällöin menetät keskitetyn ratkaisun suomat edut.
- Skannaa säännöllisesti oman yrityksesi verkkoa. Omaa verkkoa 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.

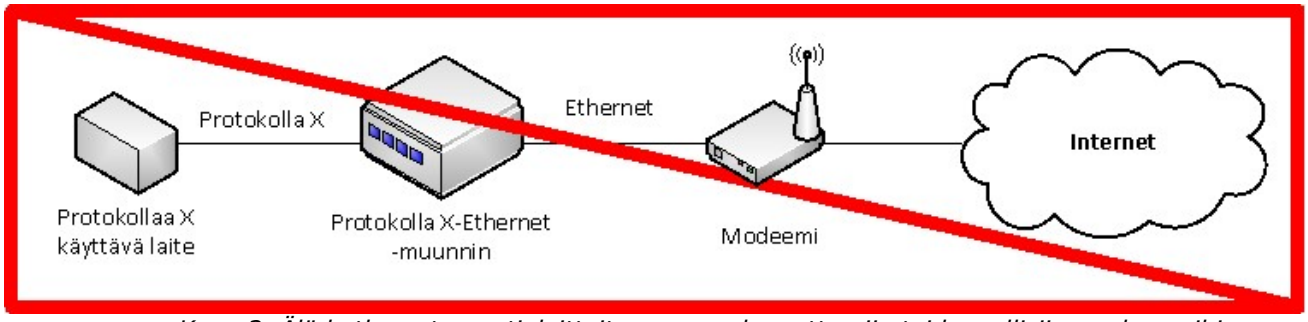
Rikolliset etsivät verkosta pääsyä automaatiojärjestelmiin automaattisilla menetelmillä. He saattavat käyttää löytämiään järjestelmiä väärin joko itse tai myymällä tiedot eteenpäin. Murrettu laite voi toimia myös porttina yrityksen sisäverkkoon.

Jos sinulla on automaatiolaite 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 voidaan kertoa laitteen yhdistämisestä verkkoon selventämättä, 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.



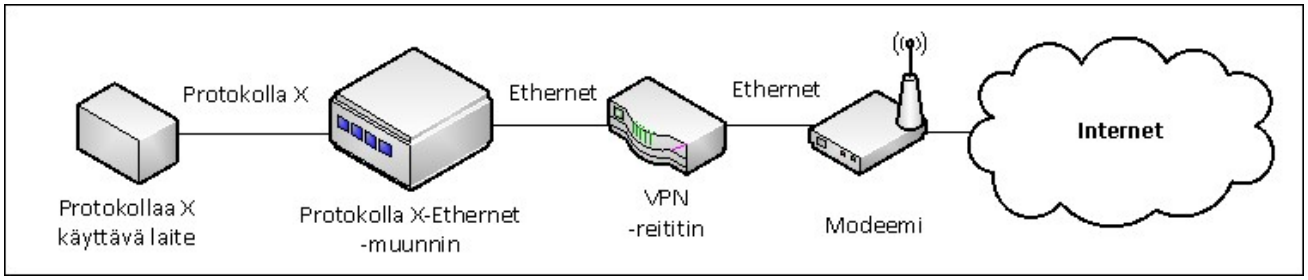
Kuva 2. Esimerkki miten automaatiolaitteen yhdistäminen esitetään toisinaan laitteiden manuaaleissa.

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 automaatiolaite 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.



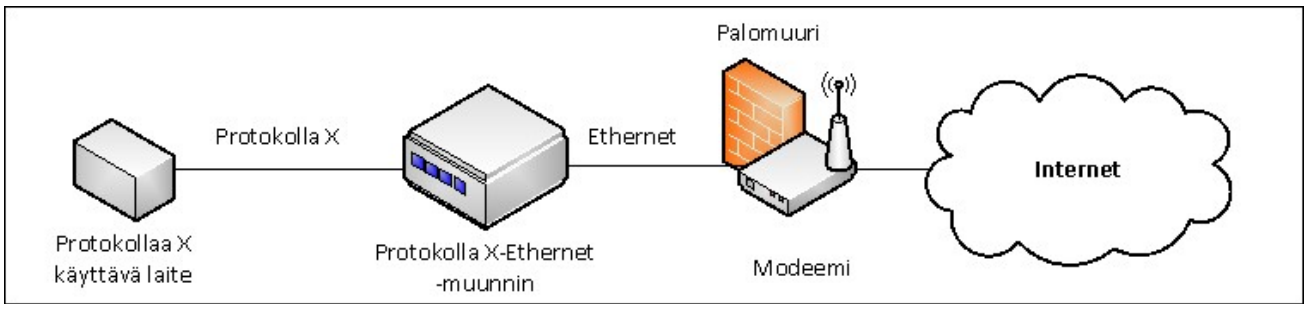
Kuva 3. Älä kytke automaatiolaitteita suoraan langattomiin tai langallisiin modeemeihin äläkä DATA/ATK-pistorasioihin.

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 palomuureja.

Jos et saa ilmoitusta suojaamattomasta laitteesta, älä tuudittaudu turvallisuudentunteeseen. Emme ehkä ole havainneet käyttämääsi 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 julkaisemissamme Tietoturva nyt! -artikkeleissa sekä aiemmissa raporteissa. Nämä ovat yhä ajankohtaisia.

- Tietoturva nyt! Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille (04.03.2019) [21].
- Tietoturva nyt! Tuhansia automaatiolaitteita suojaamattomina suomalaisissa verkoissa (04.05.2018)
- Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2018 (04.05.2018)

13 Miten kartoittaa omia verkkoja?

On olemassa monia ilmaisia ja kaupallisia työkaluja sekä palveluita kartoituksien 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 tietomurtoon.

Varsinainen skannaus on mahdollista usein tehdä varsin nopeasti tai ainakin automatisoidusti, mutta skannaustulosten analysointiin ja raportointiin voi mennä suhteellisesti enemmän aikaa. Eri työkaluilla pystytään automatisoimaan monet eri vaiheet kartoituksissa, mutta usein epäselvissä tilanteissa asiantuntijat joutuvat tutkimaan laitteita manuaalisesti vierailemalla niiden web-sivuilla, käymällä läpi eri portteihin tehtyjen skannauksien 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.

Skannauksia tehdessä voi olla järkevää seurata automaattisesti, minne joidenkin palvelimien etusivuilta pääsee. Jos tiettyjen automaatiolaitteiden tiedetään tarjoavan tietynlaisia sivuja tietyissä tunnetuissa tai tiettyä formaattia olevissa kansioissa, ne kannattaa käydä 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 yhtäaikaisesti useita eri selaimia matkivilla skannaustyökaluilla.

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

Jos haluat lisätietoja kartoituksesta, lähetä sähköpostia osoitteeseen kyberturvallisuuskeskus@traficom.fi.

Yhteystietomme saat osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot.

14 Lainatut lähteet

[1] Kyberturvallisuuskeskus, ”Tietoturva nyt! Kyberturvallisuuskeskus kartoittaa suojaamattomia automaatiojärjestelmiä,” 27 04 2020. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskus-kartoittaa-suojaamattomia-automaatiojarjestelmia.

[2] Kyberturvallisuuskeskus, ”Tietoturva nyt! Hieman yli tuhat automaatiolaitetta suojaamattomana suomalaisissa verkoissa,” 20 12 2019. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hieman-yli-tuhat-automaatiolaitetta-suojaamattomana-suomalaisissa-verkoissa.

[3] S. Tiilikainen, Improving the National Cyber-security by Finding Vulnerable Industrial Control Systems from the Internet, Espoo: Aalto University, 2014, p. 7+65.

[4] Valtiovarainministeriö, ”Tietoturvapoikkeamatilanteiden hallinta,” Valtiovarainministeriö, 2017.

[5] Kyberturvallisuuskeskus, ”Tietoturva nyt! Suojattomien etätyöpöytä- ja verkkoyhteyspalveluiden määrä kasvoi maaliskuussa selvästi,” 06 04 2020. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suojattomien-etatyopoyta-ja-verkkoyhteyspalveluiden-maara-kasvoi-maaliskuussa.

[6] J. Matherly, ”Trends in Internet Exposure,” Shodan, 29 03 2020. [Online]. Available: https://blog.shodan.io/trends-in-internet-exposure/.

[7] Nixu, ”Internetin heikot kohdat Suomessa,” 17 Lokakuu 2013. [Online]. Available: https://www.nixu.com/fi/release/internetin-heikot-kohdat-suomessa.

[8] 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.

[9] S. Tiilikainen ja J. Manner, ”Suomen automaatioverkkojen haavoittuvuus,” Aalto-yliopisto, Espoo, 2013.

[10] T. Järekallio, Methods for Identification and Classification of Industrial Control Systems in IP Networks, Espoo: Aalto University, 2016, p. 7+55.

[11] B. Krebs, ”Who’s Scanning Your Network? (A: Everyone),” 10 05 2015. [Online]. Available: https://krebsonsecurity.com/2015/05/whos-scanning-your-network-a-everyone/.

[12] ShadowServer, ”Open MQTT Report – Expanding the Hunt for Vulnerable IoT devices,” 15 03 2020. [Online]. Available: https://www.shadowserver.org/news/open-mqtt-report-expanding-the-hunt-for-vulnerable-iot-devices/.

[13] VARIoT, ”An Internet-wide (IPv4) scan of externally accessible MQTT services,” 05 05 2020. [Online]. Available: https://www.variot.eu/2020/05/05/312/.

[14] CISA ICS-CERT, ”Overview of Cyber Vulnerabilities,” [Online]. Available: https://www.us-cert.gov/ics/content/overview-cyber-vulnerabilities.

[15] CISA, ”Alert (AA20-205A) - NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems,” 23 07 2020. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-205a. [Haettu 10 12 2020].

[16] Kyberturvallisuuskeskus, ”Tietoturva nyt! Edistyneet kiristyshyökkäykset yleistyvät – Varo joutumasta saaliiksi!,” 06 06 2019. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/edistyneet-kiristyshyokkaykset-yleistyvat-varo-joutumasta-saaliiksi.

[17] 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.

[18] C. Cimpanu, ”Two more cyber-attacks hit Israel's water system,” ZDNet, 20 07 2020. [Online]. Available: https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/. [Haettu 10 12 2020].

[19] S. Noponen ja J. Pärssinen, ”Hakukoneet ja tietoturva,” VTT, 05 07 2017. [Online]. Available: https://vttblog.com/2017/07/05/hakukoneet-ja-tietoturva/.

[20] S. Noponen ja J. Pärssinen, ”Miten Shodania käytetään?,” VTT, 05 07 2017. [Online]. Available: https://vttblog.com/2017/07/05/miten-shodania-kaytetaan/.

[21] 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.

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-734-1
ISSN 2669-8757 (verkkojulkaisu)

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus