Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2018

4.5.2018

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Suojaamattomia automaatiolaitteita suomalaisissa verkoissa 3

1 Keskeisiä tuloksia ja havaintoja vuonna 2018 5

1.1 Teollisuuden hallintajärjestelmät 6

1.2 Teollisuuden yksittäiset laitteet 6

1.3 Rakennusautomaatio 6

1.3.1 Keinoja rakennusautomaatiolaitteiden tilanteen parantamiseksi? 8

2 Muita kartoituksessa tehtyjä havaintoja 9

3 Mahdollisia uhkia 9

4 Miksi hyvä salasana ja laitteen uusin ohjelmistoversio eivät riitä? 10

5 Uhat teollisuudessa 10

6 Vinkkejä teollisuuden tietoturvan parantamiseksi 11

7 Uhat rakennusautomaatiossa 11

8 Vinkkejä rakennusautomaation tietoturvan parantamiseksi 12

8.1 Onko kiinteistössäni suojaamaton rakennusautomaatiolaite? 12

9 Avoimesta laitteesta ilmoittaminen laitteiden ylläpitäjille 12

10 Miten toimia ylläpitäjänä? 13

Suojaamattomia automaatiolaitteita suomalaisissa verkoissa

Viestintävirasto teki helmi-maaliskuussa 2018 vuotuisen kartoituksen, jonka tarkoituksena oli havaita suomalaisissa verkkoalueissa toimivat suojaamattomat automaatiolaitteet. Havainnoista on ilmoitettu laitteistojen ja järjestelmien omistajille ja ylläpitäjille.

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

Viestintävirasto on tehnyt vastaavan kartoituksen vuodesta 2015 lähtien. Kartoitusmenetelmät on pyritty pitämään vakioituina, jotta eri vuosien tulosten vertaaminen keskenään on mahdollista.

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 2018 kartoitus tehtiin helmikuussa ja havainnoista ilmoitettiin laitteistojen ylläpitäjille kartoituksen tulosten valmistuttua helmi-maaliskuussa. Teollisuuden ja kriittiseen infrastruktuuriin järjestelmiin liittyviin havaintoilmoituksiin reagoitiin hyvin nopeasti. Rakennusautomaatiojärjestelmien tilanne ei valitettavasti ole yhtä hyvä, vaan suojaamattomien laitteistojen määrä on pysynyt samana viime vuosien aikana.

Vuoden 2018 kartoituksen havainnot vastasivat suurusluokiltaan edellisten vuosien tuloksia. Muutoksia havaintomäärissä ei juurikaan ollut. Rakennusautomaatioon liittyviä suojaamattomia laitteita havaitaan yhä selvästi eniten. Teollisuuden hallintajärjestelmiä havaittiin hieman aiempia vuosia vähemmän, eli alle kaksikymmentä. Näistä osa oli mahdollista tunnistaa ja ilmoittaa suoraan järjestelmien omistajille. Järjestelmät, joiden omistaja ei selvinnyt, ilmoitettiin teleoperaattoreiden kautta. Edellisen kartoituksen aikana ilmoitetut teollisuuden järjestelmät ovat havaintojemme mukaan pääsääntöisesti suojattu.

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

Suojaamattomien laitteiden kartoituksessa Suomen tiettyjen porttien osoiteavaruus on käyty läpi ja näin saadusta materiaalista on pyritty löytämään automaatioon liittyvät laitteet.

Kartoitus toteutettiin skannaamalla Suomen IP-osoiteavaruusden tietyt 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.

Oman kartoituksen havaintoja on myös vertailtu verkon hakukoneiden tuloksiin, kuten esimerkiksi Shodan-hakukoneeseen. Tulokset ovat olleet samansuuntaisia, pieniä eroja on näkynyt, mutta havaintojen suuruusluokat ovat olleet hyvin samankaltaisia.

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

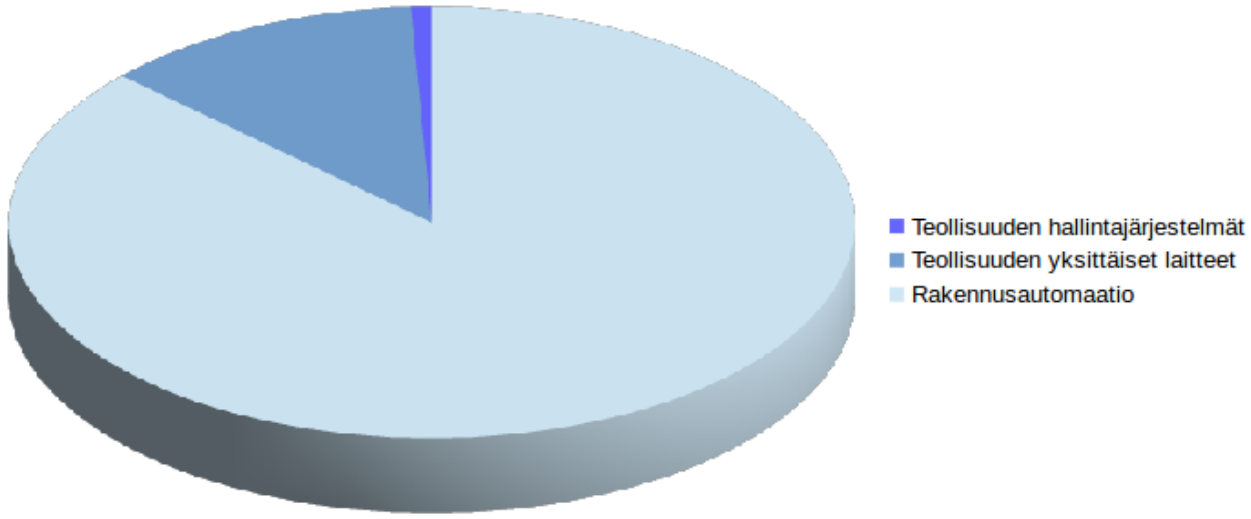
Automaatioon liittyviä laitteita etsitään niiden vastauspaketeissa palauttamien tietojen perusteella. Eri laitteet palauttavat laitteisiin liittyvät tiedot hieman eri tavoin, joten laitteiden löytäminen vaatii useita eri tunnistustapoja. Erilaiset palautuneet tiedot johtavat siihen, että kartoituksessa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

1 Keskeisiä tuloksia ja havaintoja vuonna 2018

Kartoituksessa löytyneet laitteet on jaoteltu edellisten vuosien tapaan 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 ilmanvaihdon ja lämmityksen ohjaukset.
- Kriittiseen infrastruktuuriin kuuluvien toimialojen laitteet ilmoitetaan harkinnan mukaan, vaikka ne eivät automaatiolaitteita olisikaan.

Vuoden 2018 kartoituksessa havaittiin alle 20 teollisuusautomaatioon kuuluvaa järjestelmää, teollisuuden yksittäisiä laitteita noin 300 ja rakennusautomaatioon liittyviä laitteita noin 2000. Havaitut järjestelmät ja laitemäärät vastasivat edellisvuosien havaintomääriä. Edellisiin vuosiin verrattuna suojaamattomien hallintajärjestelmien määrä oli hienoisesti pienentynyt. Yksittäisten automaatiolaitteiden ja rakennusautomaatioon liittyvien laitteiden määrät pysyivät samoina kuin vuonna 2017.



Kuva 1: Havaittujen järjestelmien osuudet vuonna 2018

Täsmällisten havaintomäärien sijaan on havainnollisempaa käyttää suuruusluokkia. Teollisuuteen liittyviä järjestelmiä on helpompi kartoittaa verkosta ja 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.

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

1.1 Teollisuuden hallintajärjestelmät

Teollisuusautomaation hallintajärjestelmiä havaittiin kartoituksessa lähes kaksikymmentä. Joukossa oli PLC-logiikoita ja HMI-ohjauspaneeleita. Vuoden 2018 kartoituksen kriittisimmäksi havainnoksi osoittautui elintarviketeollisuuden yritykselle kuulunut suojaamaton PLC-logiikka. Ilmoituksen jälkeen laite suojattiin nopeasti.

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

1.2 Teollisuuden yksittäiset laitteet

Teollisuuden yksittäisistä suojaamattomista laitteista tehtiin lähes kolmesataa havaintoa. Teollisuuden yksittäiset laitteet ovat pääosin Modbus-protokollalla tunnistettuja laitteita sekä 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 laitetta joka on tarkoitettu pelkästään paikallisesti operoitavaksi, ei ole järkevää kytkeä suoraan ja suojaamatta internetiin. Osa Modbus-protokollalla liikennöivistä laitteista kuuluu rakennusautomaatioon.

1.3 Rakennusautomaatio

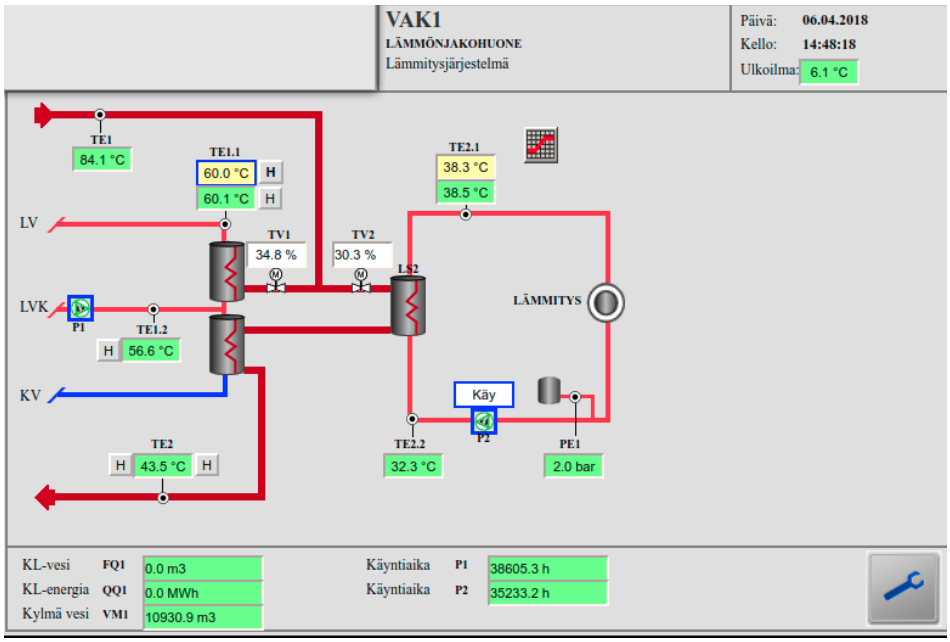
Rakennusautomaatioon liittyviä laitteita havaittiin sama määrä kuin vuoden 2017 kartoituksessa, eli noin 2000 laitetta.

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 omaa aktiivisuutta kuin myös ymmärrystä suojausten tarpeellisuudesta.

Rakennusautomaatioon liittyvissä järjestelmissä havainnot liittyivät kiinteistön ohjauksiin, pääasiassa lämmityksen ja ilmastoinnin ohjausjärjestelmiin. Vuonna 2017 tehtiin noin 20 havaintoa erään laitevalmistajan laitteista, joiden kautta oli nähtävissä muun muassa kiinteistöjen lukituksiin liittyviä aika-ohjauksia. Vuoden 2018 kartoituksessa näitä laitteita havaittiin vain yksi.

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

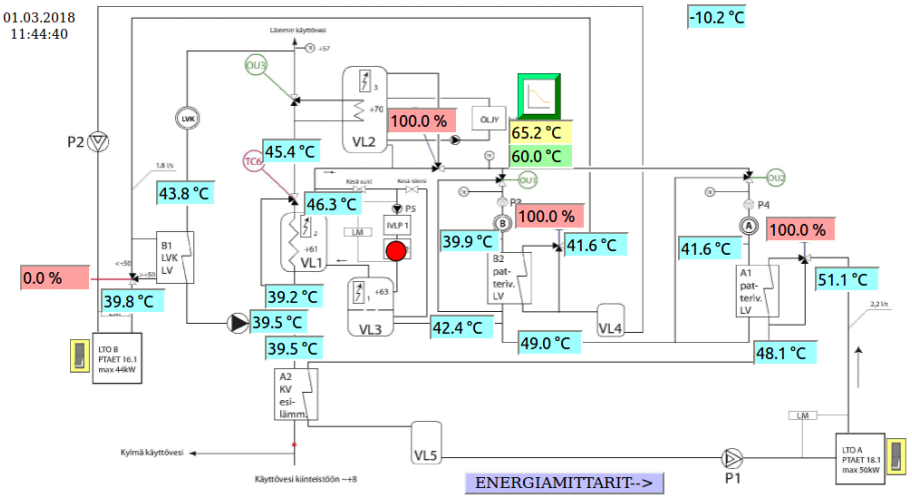
Kuvissa 2 ja 3 on esimerkit kartoituksessa havaituista rakennusautomaatiolaitteista, jotka eivät kysyneet edes salasanaa vaan käyttäjälle tarjottiin heti näkymää asetusten muuttamiseen.



Kuva 2: Kartoituksessa havaittu täysin suojaamaton lämmönsäätöjärjestelmä.

Olemme Viestintävirastossa ilahtuneet lukuisista rakennusautomaatioon liittyvien yritysten ja valmistajien yhteydenotoista. Alan toimijat näkevät tilanteen huolestuttavana ja haluavat on 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.

Mielenkiintoisia ovat kiinteistöjen aika-ohjattuja lukituksia koskevat havainnot. Laitteista, jotka lämmityksen ohella ohjaavat kiinteistön lukituksia, on suojattu vuoden 2017 ilmoitusten jälkeen lähes kaikki. Sitä vastoin laitteistoista, jotka ohjaavat "vain" lämmitystä, ei havaintoja suojaamisesta ole juuri lainkaan, vaikka lämmönohjauksella voisi vahingoittaa kiinteistöä mahdollisesti paljon pahemmin kuin aika-ohjatuilla lukituksilla. Onko lukituksiin kohdistuva uhka helpommin ymmärrettävissä kuin laitteistoon tai kiinteistön ulkopuoliseen kohteeseen kohdistuva uhka, joka muodostuu esimerkiksi kun laitteiden resursseja hyödynnetään palvelunestohyökkäyksiin?



Kuva 3: Kartoituksessa havaittu täysin suojaamaton lämmönsäätöjärjestelmä.

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

1.3.1 Keinoja rakennusautomaatiolaitteiden tilanteen parantamiseksi?

Tietoisuuden lisääntymisestä ja julkisuudessa olleista ikävistä esimerkeistä huolimatta rakennusautomaation suojaamattomien järjestelmien määrä ei näytä pienenevän.

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

Peräänkuulutamme yhä myös ylläpitopalveluita tarjoavien ja etähallintaa hyödyntävien yritysten 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 jo peruspalveluun, ja erillisiä suojauksia saa käyttöön jo muutaman sadan euron kertakorvauksella.

2 Muita kartoituksessa tehtyjä havaintoja

Automaatiolaitteiden lisäksi kartoituksessa havaittiin jälleen suuri määrä verkkoon liitettyjä IoT-laitteita (Internet of Things). Tällaisiksi tunnistettiin esimerkiksi kotireitittimet, laajakaistamodeemit, tulostimet ja verkkokamerat. Näitä laitteita verkoissa on paljon enemmän kuin esimerkiksi rakennusautomaatiolaitteita. Vuonna 2018 laitteiden hallintaan tarkoitetun (SNMP-) protokollan avulla havaittiin lähes 4000 laitetta, mikä on noin 2000 laitetta vähemmän kuin vuonna 2017. Tosin kartoitusajankohta voi vaikuttaa havaintomäärään merkittävästi, koska joukossa on paljon laitteita jotka eivät ole aina päällä tai verkkoon kytkettyinä. Esimerkiksi tulostimet.

Erilaiset suojaamattomat laitteet tarjoavat hyökkääjille oikotien kiinteistössä toimivien asukkaiden tai yritysten tietoihin. Kotien lisäksi onkin tärkeää eriyttää rakennusautomaatio- ja Iot-laitteet omiin verkkoihinsa erityisesti teollisuuden ja kaupanalan kiinteistöissä sekä toimistokiinteistöissä.

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

3 Mahdollisia uhkia

Suojaamattomana internetissä oleva laite on houkutteleva kohde murtautujille. Laitteen voi valjastaa esimerkiksi osallistumaan palvelunestohyökkäyksiin tai laite voi tarjota helpon pääsyn yrityksen verkkoon. Uusimpana uhkana on havaittu murrettujen laitteiden valjastaminen virtuaalivaluutan louhimiseen. Esimerkiksi Saksassa vesilaitoksen järjestelmään päässyt haittaohjelma hidasti prosessin toimintoja, kun järjestelmän resurssit kuluivat virtuaalivaluutan louhimiseen. (Uutinen: http://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack)

Pohjoisamerikkalaisen kasinon tietoihin päästiin puolestaan käsiksi kasinolla sijainneen akvaarion lämpötilan mittauksen kautta. Lämpötilan mittauslaitteeseen murtautumalla rikollisille avautui pääsy yrityksen muihin järjestelmiin. (uutinen: http://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4)

Itävaltalaisen laskettelukeskuksen hissi jouduttiin ottamaan pois käytöstä, kun sen hallintapaneeliin havaittiin olevan pääsy internetistä. (Uutinen: https://www.bleepingcomputer.com/news/security/ski-lift-in-austria-left-control-panel-open-on-the-internet/)

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 niihin mahdollisesti 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 palvelunesto-hyökkäykseen. 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 esimerkiksi häiritsemällä valaistusta kauppakeskuksissa tai hyväksikäyttämällä automaatiolaitteen mobiililiittymän maksullisia palveluita.

Jos laitteen havaitaan osallistuvan esimerkiksi palvelunestohyökkäyksiin tai aiheuttavan tietoturvauhan, teleoperaattorin on mahdollista katkaista tietoliikenneyhteys tietoturvasyistä.

Kartoituksessa havaittiin myös vuonna 2018 runsaasti laitteita, joissa on käytössä SSL-protokollan versio 3. Vanhentunut salausprotokolla vaarantaa laitteen, mutta aiheuttaa merkittävän uhan myös ylläpitäjille. Koska nykyaikaiset selaimet eivät enää tue SSL:n versiota 3, ylläpitäjien on käytettävä vanhentunutta selainta laitteisiin päästäkseen. Automaattisten päivitysten vuoksi ylläpitäjän käyttöjärjestelmäpäivitykset on ehkä estetty, jotta selain ei päivity. Ylläpitoyhteydet laitteeseen muodostetaan tällöin haavoittuvalla käyttöjärjestelmällä internetin kautta ja ylläpitäjän oma tietoturva vaarantuu.

4 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.

5 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 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, jos laite ei kerää tietoja kirjautumisista tai siihen kohdistuvasta liikennöinnistä.

6 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 on tehtävä suunnitelmallisesti huoltokatkosten yhteydessä.

2. **Tutki verkkosi säännöllisesti.** Näin voidaan havaita, onko haavoittuvuuksien korjaaminen onnistunut, toimivatko päivitysprosessit ja onko verkko suunnitellun mukainen.

7 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 10 000 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 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.

8 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, 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.

8.1 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.

9 Avoimesta laitteesta ilmoittaminen laitteiden ylläpitäjille

Viestintävirasto ilmoittaa havaituista järjestelmistä niiden ylläpitäjille. Tavoitettavuutta pyritään parantamaan ilmoittamalla suurempia kokonaisuuksia suoraan ylläpitäjille, jos se vain on mahdollista. Ilmoitustapa toimii esimerkiksi rakennusautomaatiolaitteiden ja kaupan järjestelmien kanssa. Kriittisen 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 Viestintäviraston 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.

10 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 on tehtävä suunnitelmallisesti huoltokatkosten yhteydessä. Tällöin esimerkiksi laiteasetuksissa tehdyt virheet tulevat 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 ilmo ituksen sellaisesta, arvioi mitkä ovat riittävät suojaustoimenpiteet laitteen turvallisen käytön mahdollistamiseksi. Lisätietoa laitteiden suojaamisesta saa valmistajalta tai laitetoimittajalta.

Jos et saa ilmoitusta suojaamattomasta laitteesta, älä silti tuudittaudu turvallisuudentunteeseen. Viestintävirasto ei ole ehkä havainnut 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 myös Viestintäviraston julkaisemissa Tietoturva nyt! -artikkeleissa vuonna 2015. Artikkelit ovat yhä ajankohtaisia.

- Kodin ja teollisuuden älykkäät järjestelmät tulilinjalla (2.4.2015) https://www.viestintavirasto.fi/2015/03/ttn201504011647
- Huonot etäyhteydet ovat myrkkyä automaatiojärjestelmille (20.4.2015) https://www.viestintavirasto.fi/2015/04/ttn201504201735

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi