jamk.fi

Rakennusautomaation kyberturvallisuuskartoitus

Kartoituksen laadinta ja testaus

Lauri Kimari

Opinnäytetyö
Toukokuu 2020
Tekniikan ala
Insinööri (AMK), sähkö- ja automaatiotekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Kimari, Lauri	Opinnäytetyö, AMK	Toukokuu 2020
	Sivumäärä 47	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Rakennusautomaation kyberturvallisuuskartoitus

Kartoituksen laadinta ja testaus

Tutkinto-ohjelma

Insinööri (AMK), sähkö- ja automaatiotekniikka

Työn ohjaaja(t)

Teppo Flyktman, Vesa Hytönen

Toimeksiantaja(t)

Planetcon Oy

Tiivistelmä

Opinnäytetyön tarkoituksena oli tuottaa toimeksiantajalle osaamista rakennusautomaation ja talotekniikan kyberturvallisuuteen liittyen. Aihe rajattiin kyberturvallisuuskartoituksen laadintaan ja sen testaamiseen pilottikohteella. Tavoitteena oli laatia kyberturvallisuuskartoitus, nostaa esiin käytännön haasteita sen toteuttamisessa sekä selvittää yleiskuva pilottikohteen rakennusautomaation kyberturvallisuuden tilasta.

Työn teoriaosuudessa käsitellään rakennusautomaation ja talotekniikan kyberturvallisuuteen vaikuttavia käsitteitä sekä esitetään valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän julkaisema tietoturvallisuuden arviointiohjeen perusteella laadittu rakennusautomaation kyberturvallisuuskartoitus. Kyberturvallisuuskartoituksen sisältö on koostettu alan keskeisimmistä julkaisuista.

Kartoitusta testattiin pilottikohteessa. Tavoitteena oli saada selkeä yleiskuva pilottikohteen rakennusautomaation kyberturvallisuuden tilasta. Kartoitusta päästiin testaamaan osittain, tulokset näiltä osin olivat kuitenkin hyviä.

Lisäksi tarkoituksena oli tuoda ilmi haasteita, jotka nousevat esiin kartoitusta toteuttaessa. Keskeisimpiä esiin nousseita haasteita olivat tehokkaan viestinnän merkitys kartoitusta suunniteltaessa, tiedonkulun aiheuttamat haasteet, henkilöstön vastuualueet sekä alalle vakiintuneet käytänteet.

Työn johtopäätöksenä todetaan, että rakennusautomaation kyberturvallisuuskartoituksen laatiminen onnistui. Kartoituksella pystyttiin muodostamaan käsitys pilottikohteen nykytilasta ja kartoituksen haasteita saatiin nostettua esiin.

Avainsanat (asiasanat)

Kyberturvallisuus, rakennusautomaatiojärjestelmä, kiinteistöautomaatiojärjestelmä, kyberturvallisuuskartoitus

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Kimari, Lauri	Bachelor's thesis	May 2020
		Language of publication: Finnish
	Number of pages: 47	Permission for web publication: x

Title of publication

Building automation cybersecurity mapping

Creation and testing of the mapping

Degree programme

Bachelor's degree programme in Electrical and Automation Engineering

Supervisor(s)

Teppo Flyktman, Vesa Hytönen

Assigned by

Planetcon Oy

Abstract

The purpose of the thesis was to produce competencies for the client in cybersecurity of building automation and building services. The topic was narrowed down to the creation of cybersecurity mapping and its testing. The aim of the thesis was to create the mapping, highlighting its practical challenges in its implementation, and coming up with an overview about the state of cybersecurity in the building automation at the pilot building.

In the theoretical part of the thesis, concepts affecting the cybersecurity of building automation and building services were described and the basis for the mapping was presented. The mapping was based on the information security assessment guideline published by the State Administration's Information and Cybersecurity Management Group. The contents of the cybersecurity mapping were derived from the most important publications in the field.

The mapping was tested at a pilot building. The aim was to come up with a clear overview of the state of cybersecurity in the building automation at the pilot building. The mapping was partially tested. The results in the tested areas were good.

The testing of the mapping was also intended to highlight practical challenges in the implementation. The main challenges that emerged were the importance of effective communication when planning the survey, the general challenges in communications, the responsibility areas of the personnel and the established practices in the field.

The conclusion of the work was that the creation of the cybersecurity mapping of building automation was successful. The mapping was able to obtain results from the current state of the pilot building and the challenges in its implementation were highlighted.

Keywords/tags (subjects)

Cybersecurity, building automation system, cybersecurity mapping, building services

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

Perinteisesti rakennusautomaatiojärjestelmät on suunniteltu palvelemaan rakennuksen ohjaamisen tarpeita, mutta etäohjaustarpeita ei suunnittelussa kuitenkaan ole huomioitu. Digitalisaation tuomien etujen myötä järjestelmiä on kuitenkin alettu liittää erilaisten yhteyksien avulla verkkoon. Tämä yhdistäminen altistaa järjestelmät samoille uhille, joille tietokoneet ja muut perinteisemmin verkkoon kytkeytyneet laitteet ovat altistuneet jo pitkän aikaa. Nyt rakennusautomaatiojärjestelmiä kytketään verkkoon ajattelematta sen tarkemmin kyberturvallisuutta ja sen tuomia riskejä. (Antonini, Barenghi & Pelosi 2014, 1.)

Kyberturvallisuus sekoitetaan helposti tietoturvallisuuteen. Tietoturvallisuus käsittää nimensä mukaan itse tiedon (datan) turvaa. Rousku (2014) jakaa tietoturvallisuuden tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen. Tiedon luottamuksellinen käsittely tarkoittaa sitä, että on määritelty, kenellä on pääsy tietoon. Eheydellä tarkoitetaan sitä, että tieto ei saa päästä muuttumaan. Saatavuus taas kuvaa tiedon saatavuutta sitä tarvitseville tahoille. (Rousku 2014, 47-51.) Kyberturvallisuus taas on laaja käsite, joka kattaa kaikki tietoteknisiin laitteisiin liittyvät vaikuttamisen keinot (Rousku 2014, 54-57). Sainio (2019) on kuvannut kyberturvallisuuden hienosti näin:

> *Kyse on perinteisen tietoturvallisuuden laajentamisesta käsittämään myös ympäristöt, joissa ei ole suojattavaa tieto-omaisuutta, kuten esimerkiksi varasto- tai kiinteistöautomaatiojärjestelmät. Kyberturvallisuuden piiriin kuuluvat myös rajapinnat, joita käyttämällä alihankkijat ja yhteystyökumppanit pääsevät yrityksen verkkoon kiinni. (Sainio 2019, 16.)*

Kyberturvallisuuden riskejä ei välttämättä koeta rakennusautomaatiossa realistisina uhkina, mutta myös Suomesta on esimerkkejä kyberhyökkäyksistä. Vuonna 2016 ulkomaalaiset rikolliset häiritsivät Lappeenrannassa taloautomaatiojärjestelmää saaden aikaan mm. lämmönsyötön häiriön ruuhkauttamalla järjestelmää ohjaavan tietokoneen (Koponen 2016). Lahdessa verkkohyökkäys kaupungin tekniikkaa vastaan vuonna 2019 aiheutti haittaa toiminnalle. Haittaohjelma pääsi leviämään kaupungin laitteissa ja muun muassa tietoyhteydet terveydenhuoltopalveluihin

jouduttiin sulkemaan. (Ahjopalo 2019.) Hyökkäyksen aiheuttamat kustannukset nousivatkin yli puoleen miljoonaan euroon, kun asiaa jälkikäteen selviteltiin ja turvallisuutta lisättiin (Ojanperä 2019). Kyberturvallisuuden uhat ovatkin monipuolisia erilaisista luonnonilmiöistä aina inhimillisiin virheisiin, eikä niitä tulisi vähätellä.

Tämän opinnäytetyön lähtökohtana toimi toimeksiantajan kiinnostus rakennusten kyberturvallisuuteen etenkin talotekniikan näkökulmasta. Opinnäytetyön tavoite oli tuottaa toimeksiantajalle yleistä osaamista aiheeseen sekä mahdollisesti luoda yritykselle tuotteistettava palvelu aiheeseen liittyen. Tämän perusteella työn aiheeksi rajattiin kyberturvallisuuskartoituksen laadinta. Tarkoituksena oli pyrkiä luomaan prosessi, jonka avulla voidaan saada kiinteistön kyberturvallisuuden tasosta parempi yleiskäsitys. Tämän pohjalta kiinteistön haltijalle voidaan esittää parannusehdotuksia kyberturvallisuuden tilaan.

2 Tutkimusasetelma

2.1 Tavoite ja tutkimuskysymykset

Työn tavoitteen määrittely oli haastavaa. Toimeksiantaja toivoi yleisesti osaamista aiheeseen liittyen. Kiinnostuksen herättäjänä toimi keväällä 2020 julkaistava RTS 19.50 Rakennustietosäätiön julkaisema ohjekortti, joka käsittelee rakennusten digitaalista turvallisuutta. Opinnäytetyötä tehtäessä tuota korttia ei ollut vielä julkaistu virallisesti, joten siihen ei tässä työssä viitata. Näiden lähtökohtien pohjalta tehtiin kirjallisuuskatsaus aiheeseen sekä neuvolteltiin toimeksiantajan kanssa, mitä työltä lähdettäisiin konkreettisesti hakemaan. Nopeasti tuli selväksi, että rakennusten digitaalisen turvallisuuden kartoittaminen vanhemmissa rakennuksissa olisi mielenkiintoinen ja tutkittava aihe. Näin aiheeksi rajattiin kyberturvallisuuskartoituksen laatiminen. Kartoitus oli tarkoitus koostaa aiheesta julkaistujen ST-korttien pohjalta.

Rakennusten digitaalinen turvallisuus on aiheena hyvin laaja ja aihetta rajattiin edelleen rakennusautomaatiojärjestelmien kyberturvallisuuteen keskittyen etenkin taloteknisiin järjestelmiin. Teoriaosassa luodaan katsaus aiheeseen liittyvään tutkimukseen sekä tämänkaltaisen kartoituksen toteuttamiseen. Työhön liittyi myös käytännön osuus, jossa testattiin kyberturvallisuuskartoitusta pilottikohteella. Käytännön osuuden tavoitteena oli tuoda esiin haasteita, jotka ilmenevät kartoitusta tehdessä. Näitä ovat mm. erilaiset ennakkoluulot aihetta kohtaan, tiedonkulun haasteet, organisationaaliset haasteet sekä yleinen tietämättömyys aiheesta. Alkuperäisenä oletuksena oli, että aihe on melko vieras myös kiinteistön haltijoille.

Tämän pohdinnan perusteella muodostettiin seuraavat tutkimuskysymykset:

- Miten kyberturvallisuuskartoitus käytännössä toteutetaan?
- Mikä on taloteknisen rakennusautomaation kyberturvallisuuden nykytila pilottikohteessa?
- Mitkä ovat keskeisimmät haasteet kartoitusta tehtäessä?

2.2 Tutkimusmenetelmä

Hakala (2004) erittelee ammattikorkeakoulujen opinnäytetyöt karkeasti tutkimustyyppisiin sekä kehittämistöihin. Ammattikorkeakouluissa työt ovat monesti käytännönläheisempiä verrattuna yliopiston lopputöihin. (Hakala 2004, 21.) Käytäntöä ja teoriaa yhdistävä työ on kehittämistutkimus. Kehittämistutkimuksiin kuuluu aina käytännön osuus sekä teoriaosuus. Teoriaosuus pohjustaa käytäntöä ja selittää erilaisia huomattuja ilmiöitä. Teorian on tarkoitus luoda tekijälle, eli oppijalle, osaamista, ja tätä opittua apuna käyttäen tulisi muodostaa ratkaisu ongelmaan. (Kananen 2007, 12-16). Tämän työn tavoitteena oli tuottaa toimeksiantajalle konkreettinen lopputuote, ja siksi kehittämistutkimus on perusteltu valinta työlle.

Seuraavaksi tuli pohtia, mikä olisi sopiva tutkimusote eli miten lähteä lähestymään työtä. Tieteellisten tekstien tärkein asia on niiden luotettavuus ja toistettavuus. Tästä syystä tulee lähestymistapa määritellä tutkimuskohteen mukaan oikein. Työn kulku tulisi dokumentoida siten, että lukijan on helppo arvioida työn luotettavuus. Erilaisia lähestymistapoja ovat mm. laadullinen ja määrällinen tutkimus sekä moniotteiset

tutkimukset, kuten case-tutkimus, kehittämistutkimus ja toimintatutkimus. (Kananen 2007, 25-44.) Tämän opinnäytetyön lähestymistavaksi valikoitui kehittämistutkimus, sillä työllä on konkreettinen tavoite kehittää prosessi.

Kehittämistutkimuksessa on tärkeää kerätä tarkka dokumentaatio tutkimuksen kulusta, myös kentällä. Kehittämistyön rakenteen tulisi olla karkeasti sellainen, että alussa tarkastellaan nykytila, tutkitaan ja ehdotetaan keino parantaa sitä, testataan käytännössä, arvioidaan onnistuminen ja lopulta seurataan lopputulosta. (Kananen 2007, 48-52.) Kartoituksen laadintaan käytetty tutkimusaineisto kerättiin alan keskeisimmistä julkaisuista. Kartoituksen testauksessa käytetty tutkimusaineisto tuotettiin työssä laaditun kartoituksen avulla. Näiden lisäksi haastateltiin laitteisto- ja järjestelmätoimittajaa.

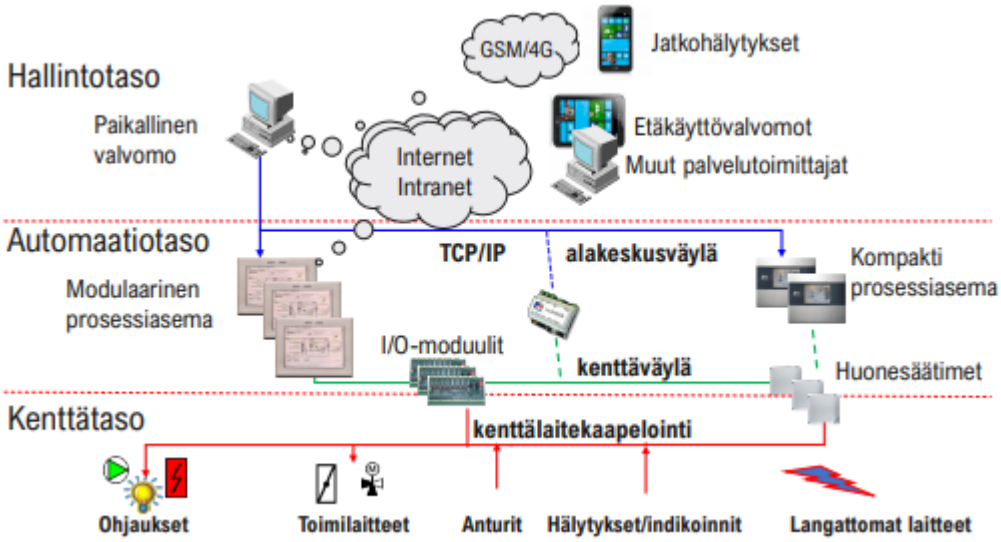
3 Kyberturvallisuus taloteknisessä rakennusautomaatiossa

Tässä luvussa käsitellään ensin rakennusautomaatiota ja talotekniikkaa yleisesti, minkä jälkeen esitellään erilaisia riskejä näihin liittyen. Riskit on jaettu teknisiin, henkilöstöllisiin sekä fyysisiin riskeihin. Näiden jälkeen on esitetty samalla kaavalla erilaisia hallintakeinoja näille riskeille. Hallintakeinot on jaettu teknisiin ja hallinnollisiin keinoihin.

3.1 Rakennusautomaatio ja talotekniikka

Rakennusautomaatiojärjestelmä (Building automation system, BAS) tai kiinteistönhallintajärjestelmä (Building management system, BMS) on järjestelmä, joka koostuu laitteista ja järjestelmistä. Sen tehtävä on ohjata rakennusten talotekniikkaa ja muita teknisiä järjestelmiä. Niihin kuuluvat nykypäivänä mm. kulunvalvonta, lämmitys, ilmastointi, paloilmaisimet, valvontakamerat, murtoilmaisimet, sähköjärjestelmät ja valaistus. (ST-710.02, 2019, 29.)

Rakennusautomaatiojärjestelmä voidaan jakaa kolmeen tasoon, kenttätasoon, automaatiotasoon ja hallintotasoon. Näitä havainnollistaa kuvio 1. Kenttätasolla on erilaiset kenttälaitteet eli fyysiseen ohjaukseen ja mittaukseen osallistuvat laitteet. Ne välittävät tietoa järjestelmälle ja toteuttavat järjestelmän toiveita fyysisesti. Kenttälaitteet kytketään automaatiotasolla erilaisten muuntimien ja prosessointilaitteiden kautta automaatiojärjestelmään, joka toteuttaa ohjausta. Automaatiotaso voi yhdistyä esimerkiksi internetin yhteydellä hallintotasolle. Hallintotasolla voi olla erilaisia valvomoita, etäyhteyksiä ja hälytysjärjestelmiä. Tähän tiedonsiirtoon voidaan käyttää kiinteitä, mutta myös langattomia yhteyksiä. (Liedes & Härkönen 2018, 59 - 61.)



Kuvio 1. Rakennusautomaatiojärjestelmän rakenne (Liedes & Härkönen 2018, 60)

Taloteknisen rakennusautomaatiojärjestelmän tehtävä on toteuttaa rakennuksen erilaisten prosessien säädöt ja ohjaukset, taloteknisten toimintojen mittaukset ja hälytykset, tuottaa mittausdatan avulla tietoa rakennuksen ylläpidon tueksi sekä tarjota selkeä ja helposti käytettävä käyttöliittymä näiden hallintaan. Järjestelmän tarjoaman tiedon avulla tulisi rakennusta pystyä ohjaamaan järkevästi ja näin

saavuttaa merkittäviä taloudellisia etuja mm. energiatehokkuuden parantuessa. (Liedes & Härkönen 2018, 22.) Erilaisilla älykkäillä ohjaustavoilla saadaan lisättyä energiatehokkuutta sekä -säästöjä ja siksi järjestelmien ohjaaminen ja datan kerääminen on perusteltua (Kamali, Khakzar & Abdali Hajiabadi 2014, 335). Myös kiertotalous korostuu jatkuvasti enemmän ja enemmän, globaalisti on hyvin tärkeää pyrkiä hyödyntämään resursseja mahdollisimman tehokkaasti. Erilaiset älykkäät ratkaisut tehojärjestelmissä eli tehoa kuluttavissa kokonaisuuksissa, esim. lämmitys, ilmastointi ja sähköjärjestelmät, säätävät energiankulutuksessa merkittävästi. (Goebel, Jacobsen, Razo, Doblander, Rivera, Ilg, Flath, Schmeck, Weinhardt, Pathmaperuma, Apperath, Sonnenscheln, Lehnloff, Kramer, Staake, Fleisch, Neumann, Strüker, Erek, Zarnerkow, Zlekow & Lässig 2013, 26-27.)

Erilaiset palveluliiketoimintamallit lisäävät verkottumista kiihtyvällä tahdilla. Yhä useammalla alalla, esimerkiksi rakennusautomaatiossa, audiovisuaalisessa viestinnässä ja turvallisuuspalveluissa, toiminta siirtyy yksittäisten kohteiden palvelemisesta suurempien kokonaisuuksien keskitettyyn palvelemiseen. Käytännössä tämä tarkoittaa sitä, että dataa on kerättävä monien eri palveluiden hyödynnettäväksi. Kun tietoa pystytään keräämään enemmän, voidaan sen avulla erilaisia palveluita tarjota suuremmalle joukolle. Esimerkkinä on pyrkimys liittää rakennusautomaatiosta saatu mittausdata energiankulutuksen optimointiin ja seurantaan sekä kiinteistön suunnitteluun. Myös eri alojen palveluiden yhdistämisellä on mahdollista saavuttaa suuriakin taloudellisia säästöjä sekä lisätä kiinteistöjen käyttöarvoa. (Ollenberg 2015, 8-9.)

Kun näistä syistä kiinteistöautomaatiojärjestelmiä liitetään verkkoon yhä enemmän, lisääntyvät myös erilaiset digitaalisen vaikuttamisen keinot kiinteistöautomaation ja taloteknisten laitteiden kohdalla. (Nana 2016, 1.) Kun rakennuksessa samaan verkkoon yhdistetään tietokoneiden lisäksi kiinteistöautomaation erilaiset järjestelmät, kuten esimerkiksi valaistus ja kulunvalvonta, voidaan näitä häiritsemällä vaikuttaa merkittävästi rakennuksen käyttäjiin. Esimerkiksi jos yrityksen työntekijöiltä estetään pääsy työpaikalle, vaikuttaa se merkittävästi yrityksen toimintaan. (Kelly n.d., 3.) Samoin jos valaistus kytkeytyisi yllättäen pois, se häiritsisi useiden alojen toimintaa merkittävästi. Etenkin meillä pohjoisessa vaikutukset olisivat ilmeiset.

Motiiveja hyökkäyksille voi olla monia. Kelly (n.d.) jakaa mahdolliset hyökkääjät aktivisteihin, terroristeihin, valtioihin, yrityksiin, vanhoihin työntekijöihin ja kiusantekijöihin tai tylsistyneisiin teineihin. Aktivistien tarkoituksena on ajaa omia etujaan, terroristit pyrkivät horjuttamaan valtioiden toimintaa, valtiot pyrkivät häiritsemään niiden turvallisuutta uhkaavia tekijöitä, yritykset voivat sabotoida kilpailijoitaan ja kiusantekijät testailevat omia taitojaan. (Kelly n.d., 3.) Eli motiivi hyökkäykselle voi siis olla taloudellinen, poliittinen tai sotilaallinen hyöty, sosiaalinen arvostus tai terroriteko (Mundt & Wickboldt 2016, 6).

3.2 Turvallisuusriskit

Kyberturvallisuuden riskejä on lukemattomia ja tässä luvussa niistä tarkastellaan keskeisimpiä ja mielenkiintoisimpia. Ollenberg (2015) sekä Järvinen (2018) ovat kuvanneet mahdollisia riskejä monipuolisemmin.

3.2.1 Tekniset haavoittuvuudet

Särelän, Tiilikaisen ja Kiravuon (2013) tekemän tutkimuksen mukaan Suomessa on merkittävä määrä julkiseen verkkoon näkyviä automaatiolaitteita. Heidän tutkimuksessaan verkkoon näkyviä automaatiolaitteita oli kokonaisuudessa 3700 kappaletta. Näistä n. 76 % oli kiinteistöautomaatiolaitteita. Yli puoleen näistä laitteista oli olemassa tunnettu haavoittuvuus. (Särelä, Tiilikainen & Kiravuo 2013, 4.) Tilanne on tietoisuuden lisääntymisen ja mm. kyberturvallisuuskeskuksen tekemien kartoitusten ja toimenpiteiden takia parantunut. Kyberturvallisuuskeskuksen vuonna 2019 teettämässä tutkimuksessa havaittuja laitteita löytyi enää n. 1100. Kyberturvallisuuskeskuksen tekemässä tutkimuksessa (2019) rakennusautomaatiolaitteiden osuus on kuitenkin 88 % löydetyistä laitteista. Rakennusautomaatiojärjestelmien löydökset liittyivät erilaisiin kiinteistöjen ohjausjärjestelmiin, kuten esimerkiksi lämmityksen, ilmastoinnin ja kiinteistön lukitusten ohjauksiin. Osaa verkkoon näkyvistä laitteista ei ollut suojattu edes salasanalla. Alan yritykset tiedostavat nykytilan ja pyrkivät tuottamaan laitteita, joiden suojaus olisi paremmalla tasolla. Uudet laitteet onkin yleensä suojattu tehokkaammin, ja siksi suurempi ongelma onkin vanhempien laitteistojen suojauksen

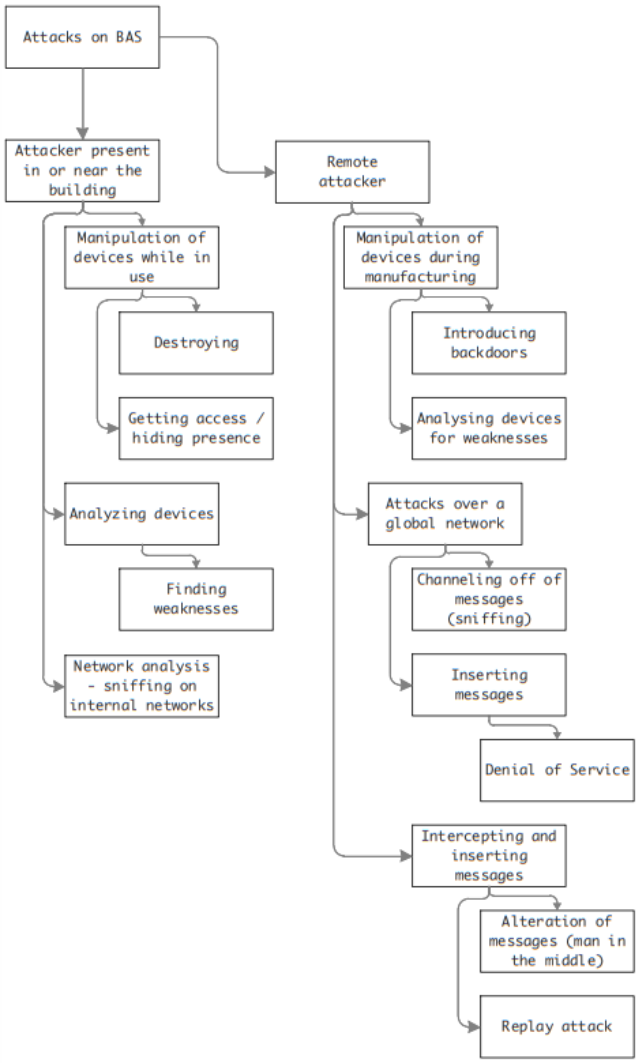
toteuttaminen. (Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2019, 4-5.)

Kiinassa eräs hotelli oli toteuttanut asiakkailleen digitaalisen hovimestarin luksushotellissaan tarjoamalla jokaiselle asiakkaalle iPadin, jolla ohjata huoneensa rakennusautomaatiota. Toteutukseen oli käytetty KNX-protokollaa, jossa liikennettä ei ollut salattu. Langattomat viestit liikkuivat siis hotellin sisällä suojaamatta. Eräs hotellivieras oli huomannut tämän ja pystynyt vaivattomasti ohjaamaan kaikkien hotellihuoneiden automaatiota. (Zetter 2014.) KNX-protokollaa on sittemmin kehitetty tietoturvallisempaan suuntaan (KNX Esineiden internet N.d.). Tämä esimerkki on kuitenkin osoitus huolettomien toimien ja vanhentuneiden teknologioiden vaaroista.

Mikäli laitteistoja päästään ohjaamaan verkon yli, on mahdollista aiheuttaa suurtakin taloudellista haittaa. Rakennuksia voidaan saattaa käyttökelvottomiksi tai laitteita voidaan rikkoa. Lämmityksen ja ilmastoinnin häirinnällä voidaan vaikuttaa olosuhteisiin rakennuksessa. Jos rakennuksen lukitusten tai kulunvalvonnan ohjaus joutuu vääriin käsiin, voi se taas altistaa rakennuksen esimerkiksi ryöstölle. Suurten kuormien toistuva ohjaaminen päälle ja pois voi puolestaan aiheuttaa normaalia suurempia kuormituksia sähköverkon muuntajille. Pienetkin kuormat voivat suurina joukkoina aiheuttaa suurta haittaa. Esimerkiksi, jos valaisimien ohjauksia kaapataan suuri määrä, voi niiden toistuvalla kytkemisellä olla merkittävät vaikutukset. Toistuva kytkeminen myös ikäännyttää valaisimia nopeammin kuin normaali käyttö. Näiden konkreettisten uhkien lisäksi voidaan automaatiojärjestelmistä varastaa myös tietoa. Tiedolla voidaan seurata tilan käyttäjiä ja heidän käytöstään sekä rakennuksen käyttöä ylipäätään. (Mundt & Wickboldt 2016, 4.)

Erilaisia hyökkäyskeinoja kiinteistöautomaatiojärjestelmään on esiteltynä kuviossa 2. Hyökkääjät on jaettu paikallisiin sekä verkon yli toimiviin hyökkääjiin. Erilaisia hyökkäystapoja on useita. Paikallisesti hyökättäessä käytössä oleviin laitteisiin voidaan vaikuttaa, niitä voidaan analysoida heikkouksien löytämiseksi tai verkkoa ja sen liikennettä voidaan seurata. Verkon yli toimiva hyökkääjä voi esimerkiksi pyrkiä vaikuttamaan laitteisiin jo valmistusvaiheessa kehittelemällä näihin haavoittuvuuksia

tai toisaalta etsimään niitä. Verkkoon kytkettyihin laitteisiin hyökkäyksiä voidaan kohdistaa periaatteessa mistä vaan maailmasta. Verkon yli voidaan pyrkiä sotkemaan järjestelmien sisäistä viestintää ja niihin voidaan pyrkiä ujuttamaan virheellisiä viestejä. (Mundt & Wickboldt 2016, 5.) Lappeenrannassa tapahtuneessa hyökkäyksessä rakennusautomaatiojärjestelmään kohdistettiin palvelunestohyökkäyksen tyylinen hyökkäys (Koponen 2016). Palvelunestohyökkäys on verkkohyökkäys, joka pyrkii lamaannuttamaan palvelun esimerkiksi estämällä laitteen kommunikoinnin (Deskmukh & Devadkar 2015, 1-4).



Kuvio 2. Erilaisia hyökkäystapoja rakennusautomaatiojärjestelmään (Mundt & Wickboldt 2016, 5).

Mikäli hyökkääjällä on pääsy rakennusautomaatioverkkoon, on hänen mahdollista aiheuttaa sen kautta huomattavaa vahinkoa. Tenkanen (2016) listaa omassa lopputyössään erilaisia uhkakuvia ja hyökkäysmalleja, mikäli näin pääsee käymään. Pienitehoiset rakennusautomaatioverkon muuntimet eivät pysty käsittelemään suuria määriä dataa, jolloin esimerkiksi lähettämällä dataa verkkoon (palvelunestohyökkäys), voidaan sen toimintaa häiritä merkittävästi tai jopa lamauttaa kokonaan. Yleensä verkkoon pääsy vaatii kuitenkin fyysisen liityntäpisteen järjestelmään. (Tenkanen 2016, 48-49.)

Yksittäisten laitteiden ja järjestelmien turvallisuus vaikuttaa huomattavasti kokonaisturvallisuuteen, etenkin kun niitä on yhdistelty kiinteistössä. Valmistajat ovat pitkälti vastuussa näiden turvallisuuden toteuttamisesta sekä ylläpidosta. Laitteiden ja järjestelmien kyberturvallisuus voi olla myös hankala testata ja todentaa sillä tekninen tarkastelu vaatii tietoturva osaamista. (ST-710.02 2019, 11.) Monesti automaatiossa yhdistyy useat eri järjestelmät, mikä lisää tilanteen haastavuutta entisestään, sillä silloin joudutaan tekemään erilaisia käyttöoikeus määrittelyjä, jotta eri järjestelmät saadaan kommunikoimaan keskenään. Myös verkon yli tehtäviä yhteyksiä määritellessä tulee varmistua, että erilaiset käyttäjien todentamiset ja sallitun tietoliikenteen määrittelyt ovat kunnossa. (ST-710.02 2019, 23.)

3.2.2 Henkilöstö

Rakennusautomaatiojärjestelmien kyberturvallisuutta on helppo lisätä merkittävästi toteuttamalla perusasiat oikein. Silti yksi suurimpia turvallisuusriskejä on henkilöstön puutteellinen tiedotus, uhkien vähättely tai jopa henkilöstön välinpitämättömyys. Joskus kyberturvallisuutta ajatellaan pelkästään IT-osaston vastuuna yrityksessä, yleensä talotekniset järjestelmät eivät kuitenkaan ole heidän vastuualuettaan. (Cyber-threat and the FM solution 2017, 9-10.) Käytännössä voi muodostua tilanne, jossa rakennusautomaatiojärjestelmien kyberturvallisuudesta ei oteta tai haluta ottaa vastuuta henkilöstön toimesta. Olisikin tärkeää, että tähän kiinnitettäisiin huomiota ja mietittäisiin tarkasti, kuka olisi oikea taho vastaamaan taloteknisten järjestelmien turvallisuuden ylläpidosta (Cyber-threat and the FM solution 2017, 10). Taloteknisiä järjestelmiä ei osata mieltää mahdollisina kyberturvariskeinä. Käyttäessä

näitä järjestelmiä ei siksi ymmärretä pitää mielessä edes sellaisia turvallisuustoimia, jotka muiden IT-laitteiden kanssa ovat itsestään selviä. (Kelly N.d., 4)

3.2.3 Fyysiset riskit

Laitteiden fyysinen sijoittelu on myös merkittävä osa kyberturvallista ympäristöä. Kuten aiemmin mainittiin, mikäli hyökkääjällä on pääsy järjestelmään fyysisen liityntäpisteen kautta, se altistaa järjestelmän vakavalle haitalle. Palvelintilat sekä esimerkiksi laitteiden liitäntäpisteet ovat paikkoja, joista verkkoon voidaan kytkeytyä. (Ollenberg 2015, 25.)

3.3 Turvallisuuden hallintakeinot

Kuten kyber- ja tietoturvallisuuden riskit, niin myös niiden hallintakeinot ovat moninaiset. Tässä luvussa esitetään aiheesta vain perusteet. Ne on pyritty valitsemaan toimeksiantajan asiakkaiden taloteknisen turvallisuuden nykytila mielessä pitäen. Hallintakeinot voidaan jakaa karkeasti teknisiin ja hallinnollisiin keinoihin (Ollenberg 2015, 23). Kyberturvallisuus on monimutkainen kokonaisuus ja on tärkeää, että sen hallintaa suunniteltaessa ymmärretään verkottunut talotekniikka kokonaisuutena. Kokonaisuuteen kuuluu kaikki käyttötavoista, ylläpitoon ja käyttäjien koulutukseen. (Ollenberg 2015, 9-11.)

3.3.1 Riskinarviointi

Edellytyksenä oikeiden hallintakeinojen valintaan tulee riskit ensin määritellä. Kun riskit pystytään määrittelemään, on niitä mahdollista myös vertailla. Vertailemalla riskejä on mahdollista asettaa ne tärkeysjärjestykseen, jolloin esimerkiksi korjausinvestointien kannattavuutta voidaan perustella järkevästi.
Riski voidaan määritellä, kun arvioidaan tapahtuman, eli riskin, todennäköisyys ja siitä toteutuessaan aiheutuvat seuraukset. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 25-26.) Tästä voidaan muodostaa lauseke: riski = todennäköisyys x vaikutus (ST-710.02 2019, 4). Siis mitä todennäköisempi riski on ja mitä suurempi sen vaikutus, sitä vakavammasta riskistä on kyse. Riskejä voi silti olla hankala arvioida ja niitä voikin olla helpompi hahmottaa sijoittamalla ne riskinarviointimatriisiin (ks.

taulukko 1). Kun riskit on saatu määriteltyä ja niitä voidaan vertailla, voidaan hallintakeinot suhteuttaa niihin. (Korpisaari ym. 2018, 27.)

Taulukko 1. Riskinarviointimatriisi (ST-710.02 2019, 4)

Riskin todennäköisyys	Riskin vaikutukset toteutuessaan		
	Vähäinen (1)	Merkittävä (2)	Vakava (3)
Alhainen (1)	Merkityksetön (1)	Vähäinen (2)	Kohtalainen (3)
Keskitasoinen (2)	Vähäinen (2)	Kohtalainen (4)	Merkittävä (6)
Korkea (3)	Kohtalainen (3)	Merkittävä (6)	Sietämätön (9)

3.3.2 Tekniset keinot

Verkkoon kytkettyjä palveluita tulee suojata vähintään tunnuksella ja salasanalla. Tämän lisäksi tulee varmistua, että seuraavat seikat ovat kunnossa: käyttäjällä on pääsyoikeus voimassa, tunnusten käyttö tai sen yritys tulee aina kirjata ylös, yhteys on palomuurisuojattu ja että työasemien käyttöjärjestelmät sekä haittaohjelmien torjuntaohjelmistot ovat ajan tasalla. (ST-721.01 2016, 9.) Suojatun internet yhteyden käyttö talotekniikan yhdistämisessä etäohjaukseen nähdään erittäin merkittävänä turvallisuustekijänä. Tämä voidaan toteuttaa esimerkiksi VPN-ohjelmistojen avulla. (ST-721.01 2016, 9; ST-710.02 2019, 6.) Mikäli näitä yhteyksiä ei suojata, näkyvät talotekniset järjestelmät mahdollisesti internetissä, jolloin kuka tahansa maailmassa voi niihin yrittää tunkeutua. Verkkoa voidaan verkon määrittelyillä jakaa osiin ja olisikin suositeltavaa, että näitä ns. aliverkkoja luotaisiin jokaiselle järjestelmälle. Näin voitaisiin eristää yhden järjestelmän kyberturvariskit vaikuttamasta muiden järjestelmien toimintaan. (ST-710.02 2019, 10.)

Valmistajia valittaessa tulisi varmistua valmistajan kyvystä tuottaa kokonaisvaltaisesti kyberturvallisia tuotteita ja palveluita. Tätä voi kuitenkin olla hankala todeta ja siksi valmistajaa valittaessa olisi hyvä pitää mielessä muutamia perusasioita. Esimerkiksi kotimaiset viranomaiset tekevät kartoituksia tuotteille ja palveluille, halutessaan

näitä käyttämällä voi varmistua siitä, että ne ovat hyväksyttyjä tai auditoituja. Tämän lisäksi olisi hyvä varmistaa, että valmistaja tarjoaa tuotteelle tai palvelulle ohjeistuksen turvalliseen käyttöönottoon ja ylläpitoon. Ylläpitoon kuuluu mm. päivitysten saatavuus ja se, kuinka nopeasti havaitut haavoittuvuudet korjataan. (ST-710.02 2019, 11.)

Fyysisen pääsyn estäminen järjestelmiin on tärkeää (Tenkanen 2016, 48-49). Siksi erilaiseen kulunvalvontaan ja tilojen pääsyoikeuksiin pitää kiinnittää erityistä huomiota. Jo suunnitteluvaiheessa olisi hyvä miettiä laitteistojen sijoittelua, ja näiden tilojen kulunvalvontaa sekä lukituksia. Myös laitteiden, etenkin liitäntärasioiden, sijoittelu tulee miettiä siten, että niihin ei ulkopuolisilla ole pääsyä. Tämä voidaan ratkaista esimerkiksi sijoittelemalla liitäntärasiat alas lasketun katon yläpuolelle. Näiden seikkojen lisäksi laitevalinnassa tulisi suosia laitteita, joiden kautta verkkoon on vaikea tunkeutua. (ST-710.02 2019, 7.)

3.3.3 Hallinnolliset keinot

Erilaiset hallinnolliset ratkaisut ovat merkittävä osa kyberturvallisuutta. Näitä ovat esimerkiksi järjestelmien ylläpidon toteuttaminen, pääsyoikeuksien hallinta, järjestelmien tarkoituksen mukaisen käytön määrittely sekä henkilöstön käytönopastus. Kuten jo aiemmin on mainittu, kyberturvallisuus on jatkuva prosessi. On hyvin tärkeää, että toimijoilla on määriteltynä selkeät toimintatavat kyberturvallisen tilan ylläpitämiseksi. Kun järjestelmät asennetaan, ne voivat asennushetkellä olla kyberturvallisia, mutta tietoteknisistä laitteista ja järjestelmistä paljastuu lähes aina erilaisia haavoittuvuuksia ajan kuluessa. Myös esimerkiksi uudet päivitykset voivat altistaa ne haavoittuvuuksille. Päivitykset toisaalta tuovat myös korjaukset näihin haavoittuvuuksiin. (Ollenberg 2015, 23.)

Traficomin liikenne- ja viestintäviraston kyberturvallisuuskeskus (2019) suosittelee tutkimuksessaan suojautumiskeinoiksi tiedotuksen lisäämistä asianosaisille, kuten isännöitsijöille ja muille kiinteistöjen ylläpidosta vastaaville tahoille. Ylläpitopalveluita tuottavat sekä muuten etähallintaa hyödyntävät yritykset tulisi ottaa mukaan kehittämistoimintaan sekä näiden haasteiden ratkaisemiseen. Tutkimuksessa myös

korostetaan, että laitteistojen suojaus voi olla hyvinkin edullisesti toteutettavissa. (Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2019, 6.)

Kun tehdään hankintoja ja asennetaan uusia järjestelmiä, tulisi kyberturvallisuus huomioida suunnittelussa, yksittäisten laitteiden, dokumentaation, asennuksen, käyttöönoton, käytön sekä ylläpidon kohdalla. Näissä projekteissa on tärkeää varmistua, että kaikille osapuolille viestitään tehokkaasti laadituista kyberturvallisuusmäärittelyistä, jotka kaikkien osapuolten tulee täyttää. On valvottava myös, että näitä noudatetaan. Käyttöoikeuksista tulee pitää kirjaa ja niitä tulee päivittää sitä mukaan, kun henkilöstö tai toimijat muuttuvat. Käyttäjätunnuksien tulisi olla henkilökohtaisia ja salasanoja tulisi päivittää määritellyin aikavälein. (ST-710.02 2019, 11-25.)

4 Laitteisto- ja järjestelmätoimittajan haastattelu

Laitteisto- ja järjestelmätoimittajien osuus kyberturvallisuudessa on merkittävä. Opinnäytetyön tiimoilta otettiin yhteyttä erääseen laitetoimittajaan, ja pyrittiin kartoittamaan kuinka rakennusautomaation kyberturvallisuuden vastuut ja toimenpiteet jakautuvat toimittajan, tilaajan ja suunnittelijan kesken. Tarkoituksena oli parantaa käsitystä eri osapuolten vastuista kyberturvallisuudessa kokonaisuutena: Mitä eri tehtäviä osapuolille kuuluu? Kuinka ylläpito hoidetaan? Mitä tilaajana tulisi osata vaatia? Mitä palveluita toimittajilla jo on? Näihin kysymyksiin pyrittiin saamaan vastaukset teemahaastattelua soveltaen.

4.1 Haastattelun tausta

Teemahaastattelu on keino, jolla pyritään määrittelemään ongelmaa tarkemmin. Teemahaastattelun tarkoituksena on keskustelun kautta tuottaa tietoa halutusta teemasta. Keskustelun teema tai teemat tulee määritellä siten, että ongelmasta saadaan mahdollisimman kattavasti tietoa. Haastattelijan tehtävänä on määrätietoisesti johtaa keskustelua syventymään näihin teemoihin. Tätä voidaan

käytännössä toteuttaa esimerkiksi toistuvilla miksi -kysymyksillä. Toistuvien kysymyksien kautta päästään syventymään teemaan ja tätä kautta saadaan haastateltavalta mahdollisimman paljon tietoa ja näkemystä aiheeseen. (Kananen 2012, 99-109.)

Teemahaastatteluun valitut teemat tässä työssä olivat: rakennusautomaation kyberturvallisuus laitetoimittajan näkökulmasta, rakennusautomaation ylläpidon järjestäminen kyberturvallisesti, tilaajan ja toimittajan vastuiden jakautuminen tilattaessa rakennusautomaatiojärjestelmää sekä se, mitä tilaajan tulisi osata vaatia laitteistotoimittajalta ja suunnittelijoilta.

4.2 Tulokset

Haastatteluun valikoitui suuren kansainvälisen rakennusautomaatioratkaisuja tarjoavan yrityksen Suomen turvallisuuspäällikkö. Haastattelu toteutettiin etähaastatteluna ja se taltioitiin videolle. Kyseinen toimittaja on tarjonnut kiinteistöautomaation etähallintajärjestelmää jo vuodesta 2005 alkaen. Nykyään yrityksen etähallintajärjestelmä täyttää standardin ISO 27001 määritelmän ja on myös ulkoisesti auditoitu. Toimittaja valmistaa myös kiinteistöautomaation laitteita.

Keskeisin ongelma, joka haastattelussa tuli ilmi, oli etäyhteyden ja -ohjauksen toteuttaminen turvallisesti. Perinteisesti kiinteistöautomaatiota on ohjattu paikallisella ohjaustietokoneella, joka on täytynyt liittää verkkoon. Tietokone on perinteisesti ollut tilaajan omaisuutta ja näin myös vastuu koneen päivittämisestä ja muusta ylläpidosta on ollut tilaajalla, eli kiinteistöstä vastaavalla taholla. Toimittaja on pyrkinyt poistamaan tämän ohjaustietokoneen yhdistämällä kiinteistöautomaatiojärjestelmän suoraan suojatulla yhteydellä verkossa sijaitsevaan valvomoonsa. Näin ohjaus on voitu helposti keskittää yhteen turvattavaan kohteeseen. Kun ohjaus on toteutettu yhdestä paikasta, voidaan päivitykset ja muu ylläpito myös toteuttaa helposti. Kun toimittaja myös huolehtii valvomosta ja pääsyoikeuksista, pystytään helpommin kontrolloimaan ja ohjeistamaan käyttäjienhallintaa sekä pääsyoikeuksia.

Toinen esiin noussut haaste on järjestelmien pääsyoikeuksien hallinta. Pääsyoikeuksia ei voida aina rajoittaa niin pitkälle, kuin turvallisuuden puolesta voisi olla perusteltua. Kun kiinteistönhuollossa on totuttu siihen, että esimerkiksi yhdellä tunnuksella on voitu kirjautua kaikkiin järjestelmiin, ei uusia toimintatapoja, kuten vaikka säännöllisesti päivittyviä henkilökohtaisia tunnuksia, ole välttämättä helppo jalkauttaa käyttöön. Keskitetty pääsyoikeuksien hallinta on kuitenkin helpompaa, kun niiden hallintaan on toimittajalla määritellyt käytännöt. Esimerkiksi rakennuksen käyttöönottovaiheessa on hyvin tärkeä, että järjestelmistä voidaan rajata pääsy rakentamisen aikaisilta tunnuksilta. Näin myös varmistutaan, että käyttäjätunnukset eivät jää oletustunnuksiin.

Toimittaja pyrkii omassa toiminnassaan aina varmistamaan, että kohteen ja etäohjauksen välinen yhteys on suojattu. Rakennusautomaatiojärjestelmiä ei siis haluta suoraan verkkoon näkyviksi. Käytännössä tämä tarkoittaa, että ei käytetä ns. ”julkisia IP-osoitteita”, vaan rakennusautomaatiojärjestelmä suojataan siten, että sitä ei kuka tahansa verkossa näe. Tämä voidaan tehdä esimerkiksi seuraavasti:

- Langattomissa laitteissa suojattu yhteys voidaan muodostaa mobiilioperaattoreiden tarjoamilla valmiilla ratkaisulla, joissa liikenne sallitaan vain tiettyjen pisteiden välillä.
- Kiinteissä yhteyksissä voidaan VPN tunnelin avulla muodostaa suojattu yhteys järjestelmästä valvomoon, muuta liikennettä ei sallita.
- Kiinteissä yhteyksissä liikenne voidaan myös rajoittaa palomuurin määrittelyillä siten, että vain haluttu liikenne sallitaan. Tämä voi olla hyvä tapa, mikäli ohjattavia kohteita on paljon.

Näiden lisäksi rakennusautomaatiojärjestelmien tiedonsiirto olisi hyvä salata. Tällä tuodaan lisäturvaa, mikäli ulkopuolinen pääsisi datavirtaa tarkastelemaan.

Hieman valitettava asia, joka haastattelussa nousi esiin, on fyysisten laitteiden suojaus. Haastateltava mainitsi, ettei laitteille ole määritelty samanlaisia täytettäviä vaatimuksia kuin järjestelmille. Tämän takia laitteiden suojausta ei ole toteutettu esimerkiksi jonkin standardin mukaan yhtenäisesti. Kuitenkin esimerkiksi

haastatellun yrityksen tuotteiden koko suunnitteluprosessissa kyberturvallisuus on otettu huomioon. Laitteiden ylläpidon vastuu saattaa myös jäädä tilaajalle, sillä kun laitteet hankitaan, tulee niistä tilaajan omaisuutta.

Haastateltava on kokenut, että tilaajien puolelta kyberturvallisuuden uhkia ei nähdä realisoitumassa. Tämän takia kyberturvallisuutta ei esimerkiksi tarjouspyynnöissä yleensä huomioida. Tarjouspyynnöissä keskitytään enemmän toiminnallisiin seikkoihin. Kuitenkin prosessin edetessä tilaajalla on yleensä toive pystyä ohjaamaan järjestelmiä etänä ja tässä vaiheessa voi myös olla kysymyksiä ja vaatimuksia kyberturvallisuudelle. Haastateltava kehottaa, että tilaajan olisi hyvä esittää laite- tai järjestelmätoimittajalle kyberturvallisuuteen liittyviä kysymyksiä. Vastauksia arvioimalla saa käsityksen laitteisto- tai järjestelmätoimittajan suhtautumisesta kyberturvallisuuteen. Jos toimittaja osaa perustella tilaajalle omat ratkaisunsa sekä miksi nämä on toteutettu niin, että tilaaja myös ymmärtää mistä on kyse, on tilanne varmasti parempi kuin jos kyberturvallisuutta ei käsiteltäisi kummankaan tahon puolesta lainkaan. Kysyä voi esimerkiksi: miten laitteet on suojattu, miten käytettävä etäyhteys on suojattu, onko tiedonsiirto salattua, miten käyttöliittymää hallitaan, kuinka käyttöliittymän pääsynhallinta on toteutettu ja miten järjestelmien käyttöönotto toteutetaan kyberturvallisesti. Mikäli toimittaja osaa vastata näihin kysymyksiin niin, että tilaaja ymmärtää, että asiat on hoidettu tavalla tai toisella, on tilanne huomattavasti parempi kuin jos vastauksia ei kysymyksiin löydy.

5 Kyberturvallisuuskartoitus prosessina

Edellä on esitelty taloteknisiä kyberturvallisuusriskejä sekä niiltä suojautumisen keinoja. Tässä luvussa pohjustetaan työn käytännön osa, eli turvallisuuskartoituksen tekeminen. Toimeksiantajan toiveena oli pystyä tulevaisuudessa tarjoamaan asiantuntijapalveluita rakennusautomaation kyberturvaan liittyen osana tuoteportfoliotaan. Toimeksiantaja tarjoaa asiantuntijapalveluita laajalle asiakaspohjalle. Heidän toimintansa kannaltaan ei ole perusteltua lähteä kartoittamaan yksittäisten teknisten järjestelmien haavoittuvuuksia, sillä jokaisella asiakkaalla on todennäköisesti erilaiset järjestelmät. Tämän takia kartoituksen tulisi

tarjota yleiskuva tilanteesta ja pyrkiä tarjoamaan toistettavat käytännöt siten, että niiden pohjalta kartoitus olisi mahdollista toistaa luotettavasti ja järkevästi erilaisiin kohteisiin.

5.1 Kartoituksen viitekehys

Kyberturvallisuuden tilan määrittely ja arviointi on tärkeä lähtökohta kyberturvallisuuden johtamiseen ja kehittämiseen. Kartoituksen perusteella saadaan selkeämpi käsitys kyberturvallisuuden tilasta. Kun kartoituksen avulla heikkoudet ja vahvuudet korostuvat, on tarvittaviin muutoksiin helpompi ryhtyä. Kyberturvallisuus on jatkuva prosessi ja kartoitus voidaankin toistaa aikavälein. Tulosten perusteella voidaan arvioida jo toteutettujen muutosten onnistumista. Turvallisuuden takaamiseksi on hyvä käyttää esimerkiksi jatkuvan parantamisen periaatetta: suunnittele – tee – arvioi/mittaa – paranna (PDCA) ks. kuvio 3. (Tietoturvallisuuden arviointiohje 2014, 14.)

Kuvio 3. Jatkuvan parantamisen malli (Tietoturvallisuuden arviointiohje 2014, 15)

Itse kartoitusta tulisi lähestyä jonkin viitekehyksen kautta. VAHTI-ohjeessa (2014) listattuja esimerkkejä näistä ovat sopimus, tietoturvastandardi tai valtiohallinnon viitekehys (esimerkiksi tietoturvatasot). Viitekehyksellä parannetaan katsauksen luotettavuutta ja näin sitä voidaan myös verrata teoriaan. Viitekehyksen valinta pitää päättää kohteen mukaan. Erilaisille kyberturvallisuuden sekä tietoturvan, eli datan turvan, osa-alueille on tehty omia viitekehyksiä ja arviointimenetelmiä. (Tietoturvallisuuden arviointiohje 2014, 16.) Myös rakennusautomaatioon on kehitetty viitekehyksiä, kuten esimerkiksi ST-kortti 730.05. ST-730.05 ei kuitenkaan käsittele koko kokonaisuutta, vaan keskittyy etupäässä erilaisiin etäyhteyksiin rakennusautomaatiossa. (ST-730.05 2018.)

Viitekehyksen valinta oli työssä melko haastavaa. Toimeksiantajalle olisi hyödyllisintä tuottaa mahdollisimman laaja ja hallinnollinen kartoitus. Lisäksi tarkoituksena olisi myös samalla kartoitusta tehdessä pyrkiä tuottamaan käytännön osaamista ja ymmärrystä aiheeseen. Mikä käytännössä tarkoittaa erilaisten kartoituksessa huomattujen puutteiden, haasteiden sekä käytäntöjen esiintuomista. Näistä syistä työhön ei ole valikoitu pelkästään yhtä viitekehystä, vaan kartoituksessa tullaan yhdistelemään useamman ST-kortin, sekä ST-ohjeiston tietoja. Rungon kartoitukselle tarjoaa Vahti 2/2014 ohjeistus tietoturvallisuuden arviointiin. Kyberturvallisuuskartoituksen teknisiä kysymyksiä ja teemoja koostetaan ST-kortista 710.02, ST-ohjeistosta 22 ja näiden lisäksi ST-kortista 730.05, jonka avulla kartoitetaan erilaisten etäyhteyksien turvallisuutta järjestelmissä.

5.2 Turvallisuuskartoitusprosessi

Turvallisuuskartoitus tullaan toteuttamaan mukaillen VAHTI 2/2014 ohjetta (VAHTI-ohjeessa käytetty termi, tietoturvallisuuden arviointi). Ohjeessa kartoitus jaetaan vaiheisiin ja näille vaiheille on määritelty suositellut sisällöt. Ohje on tehty tietoturva-arvion toteuttamiseen, mutta sitä sovelletaan tässä työssä pohjana kyberturvakartoitukselle. Kuviossa 4. on esiteltynä VAHTI-ohjeen vaiheet turvallisuuskartoitukseen prosessina.

Kuvio 4. Turvallisuuskartoituksen vaiheet (Tietoturvallisuuden arviointiohje 2014, 44)

Suunnittelun tulisi alkaa työryhmän perustamisella. Kyberturvallisuus, kuten aiemminkin mainittu, on laaja kokonaisuus ja siksi tulisi varmistua, että kartoitusta tekevällä ryhmällä on pääsy ja tarvittava osaaminen laadukkaan kartoituksen suorittamiseen. Työryhmälle tulee määritellä vetäjä, joka vastaa työn etenemisestä. Suunnitteluvaiheeseen kuuluu kaikki ennen itse varsinaista kartoitusta. Käytännössä tämä pitää sisällään kaikki yhteydenotot ja esiselvitykset järjestelmistä sekä mahdollisista järjestelmädokumentaatioista. Ennen kartoituksen suorittamista tulisi laatia kartoitussuunnitelma, jossa määritellään mm. kartoitettava kohde, mahdolliset rajaukset, tavoitteet, aikataulu sekä raportointimenettelyt. (Tietoturvallisuuden arviointiohje 2014, 44-45.)

Itse kartoitus olisi hyvä aloittaa kokouksella, missä määritellään yleiset asiat ja varmistetaan yleisesti kartoituksen sujuva läpivienti. Kartoituksen päätarkoituksena on saada tietoa erilaisista järjestelmistä ja käytännöistä. Myös tämän tiedon keräysmenetelmät tulisi miettiä valmiiksi jo suunnitteluvaiheessa. Menetelmiä voivat olla esimerkiksi haastattelut, dokumentaation katselmointi sekä havainnointi kohteella. Tiedonkeruun tavoitteet pitää olla selvillä. Haastatteluissa tulee kysymykset asetella siten, että vastaukset ovat monipuolisia, eivätkä vain kyllä tai ei vastauksia. (Tietoturvallisuuden arviointiohje 2014, 45-46.) Kartoituksessa selvitettävät asiat määritellään teknisten ohjeistusten avulla, joista lisää seuraavassa luvussa.

Kartoituksen tulokset raportoidaan tilaajalle. Raportissa tulisi kuvata turvallisuuskartoitus prosessina, sen tulokset sekä suositukset erilaisten havaintojen korjaamiseksi. Havaitut puutteet tulisi luokitella, niiden merkitys toiminnalle tulisi

kuvata sekä suositella toimenpiteet niiden korjaamiseksi. Raporttiin voidaan luontevasti liittää myös suositellut jatkotoimenpiteet ja ylläpito. Kun tarjotaan korjausehdotuksia ja parannusehdotuksia, on näiden toteutumisella suuri merkitys. Siksi onkin tärkeää, että kohteelle määritellään vastuuhenkilöt, ylläpitosuunnitelmat ja seuranta, jotta puutteet todella tulee korjatuksi. Luotettavan turvallisuuden takaamiseksi olisi hyvä määritellä kartoitukselle kohteesta riippuva sopiva aikaväli. Näin voidaan varmistua kyberturvallisesta tilasta myös tulevaisuudessa. (Tietoturvallisuuden arviointiohje 2014, 46-49.)

5.3 Tekniset ohjeistukset

Rakennusautomaation kyberturvallisuuteen on julkaistu Suomessa eri viranomaisten toimesta ohjeistuksia. Tässä luvussa on esiteltynä näitä julkaisuja sekä kuvaus, miten niitä on hyödynnetty kartoituksessa.

ST-98.17 Rakennusautomaatiojärjestelmän kuntotutkimusohje

ST-98.17 on yleinen kuntotutkimusohje. Siinä käsitellään koko kuntotutkimus prosessina ja ohjeistetaan läpikäytävät asiat. Korttia päivitettiin vuoden 2018 alussa ja siihen lisättiin tuolloin tietoturvallisuuteen liittyviä seikkoja. Ohje keskittyy yleisesti kuntotutkimukseen eikä siinä korosteta kyberturvallisuutta. Ohjeessa suositellaan kuntotutkimuksessa käytettäväksi myös ST-730.05, josta on oma osio tässä luvussa. (ST-98.17 2018.) Tätä ohjetta ei suoraan tässä työssä hyödynnetä. Ohje on kuitenkin hyvä mainita, sillä yleinen kuntotutkimus on hyvin samankaltainen kyberturvallisuuteen keskittyvän kartoituksen kanssa.

ST-710.02 Sähkö- ja tietoteknisten järjestelmien tietoturva

Nimestään huolimatta ST-kortti keskittyy laajemmin rakennusautomaatiojärjestelmien kyberturvallisuuteen sekä näihin liittyvien tietoteknisten järjestelmien turvallisuuteen. Kortissa käsitellään monipuolisesti kyberturvallisuuteen liittyvät keskeiset aiheet. Kyberturvallisuuden kokonaisuus on jaettu prosessin eri vaiheiden mukaan. Kokonaisuus kattaa suunnittelun, tilauksen, hankkeen aloituksen, asennuksen, käyttöönoton ja luovutuksen sekä käytön, ylläpidon ja järjestelmien laajentamisen ja integroimisen. Jokaiselle osa-alueelle on

määritelty perustason suositukset sekä lisäsuositukset. Ohjeessa olevat suositukset ja lisäsuositukset ovat hyvin konkreettisia ja käytännössä toteutettavia. (ST-710.02 2019, 3-25.)

Kartoitukseen on poimittu tästä ST-kortista erilaisia suosituksia, joita peilataan nykytilanteeseen. Esimerkki suosituksista:

> *Perustason suositukset:*
> *- Laitteita ei tule kytkeä rajoituksitta suoraan internetistä käytettäväksi missään tilanteessa.*
>
> *Lisäsuositukset:*
> *Vaihtoehtoiset ratkaisut:*
> *- VPN-pohjaiset yhteydet, joilla voidaan sekä salata liikenne että rajoittaa tarkalleen se, kuka tai mitkä tahot voivat muodostaa yhteyden laitteisiin.*
> *- Sellaisten tekniikoiden käyttäminen, joissa laite avaa yhteyden ns. ”ulospäin”, jolloin itse laite ei ole käytettävissä internetistä päin. (ST-710.02 2019, 6-7.)*

Näiden suositusten pohjalta kartoitukseen johdetaan kysymyksiä kuten, mitä laitteita asiakkaalla näkyy suoraan verkkoon, miten näiden laitteiden käyttörajoitukset on määritelty, miten pääsyä internetistä on muuten kontrolloitu? Näin voidaan keskustelun kautta selvittää nykytilannetta kohteella. ST-kortista on poimittu erilaisten hallinnollisten aiheiden suosituksia, ja kysymykset on painotettu nykytilanteen kartoitukseen. Siksi esimerkiksi suunnittelun tai järjestelmien laajentamisen suosituksia ei ole kartoitukseen sisällytetty.

Kartoituksessa huomioidut teemat ovat laitteiden fyysinen suojaus, sisäverkon kokoonpano, tietoturvallisuus ohjelmistojen ajantasaisuus, verkkotopologiat ja valmistajien antamat suositukset. ST-kortti tarjoaa myös huomioitavia erityispiirteitä erilaisiin järjestelmiin. Nämä on jaettu S2010-sähkönimikkeiden mukaisesti. Kuvattuna ovat kulunvalvonta, murtoilmaisu-, kameravalvonta-, paloilmoitin- ja rakennusautomaatiojärjestelmät. (Mts. 27-30.)

ST-730.05 Sähkö- ja tietoteknisten järjestelmien tietoturvan tarkastuspöytäkirja

ST-730.05 on tarkastuspöytäkirja, joka keskittyy etäyhteyden ja -ohjauksen toteuttamiseen. ST-Kortti 730.05 tarjoaa hyvän viitekehyksen taloteknisten etäyhteyksien kyberturvallisuuden tarkasteluun. Kortissa on eri kiinteistöautomaatiojärjestelmien etäyhteyden kyberturvallisuuteen liittyviä kysymyksiä, joiden avulla saadaan käsitys kyberturvallisuuden nykytilasta. Kiinteistöautomaatiojärjestelmät on luokiteltu S2010-sähkönimikkeistön mukaan ja jokaisen järjestelmän kohdalla on samat kysymykset liittyen etäyhteyden toteutukseen. Näillä peruskysymyksissä kartoitetaan etäyhteyden ja valvomon toteutustapaa, käyttöoikeuksien määrittelyä ja hallintaa sekä varmuuskopioinnin suoritustapaa. Pöytäkirjassa on myös muutama tyhjä sivu, joille voi itse määritellä tarkasteltavan järjestelmän. Tarkastuspöytäkirjaa hyödynnetään kartoituksessa jokaisen etäohjatun järjestelmän kohdalla. (ST-730.05 2018.)

ST-ohjeisto 22 Verkottuneen talotekniikan tietoturva

ST-Ohjeisto 22 on yleinen ohjeistus talotekniseen tietoturvallisuuteen. Ohjeessa käydään läpi aiheen perusteet sekä erilaiset riskienhallinta keinot. Siinä pyritään kuvaamaan eri toimijoiden ja osapuolien vaikutuksia tietoturvallisuuteen. Ohje tarjoaa myös kattavasti erilaisia keinoja hallita tietoturvariskejä. (Ollenberg 2018, 7.) Tässä työssä ohjeesta on hyödynnetty siinä esitettyä verkottuneen talotekniikan tietoturvan muistilistaa. Kun näitä kehotuksia verrataan kohteen nykytilaan, saadaan luotua käsitys nykytilasta ja tarvittavista muutoksista. Mikäli suosituksessa kehotetaan esimerkiksi asentamaan haittaohjelmien torjunta ja järjestelmien hallintaohjelmistot, voidaan pohtia, onko näin toimittu. Vastauksesta saadaan suoraan muodostettua parannusehdotus nykytilanteeseen. (Mts. 23)

RT-ohjekortti rakennusten digitaalinen turvallisuus

Tilaajan olisi hyvä miettiä myös oma kyberturvallisuuden tavoitetaso. Tässä apuna voisi käyttää esimerkiksi pian julkaistavaa RT-ohjekorttia, joka tarjoaa mallin digitaalisen turvallisuuden tasomäärittelyyn. Tämän pohjalta voi olla helpompi määritellä selkeä tavoitetaso. Tällä tavalla voidaan tarkentaa kartoitus järkevälle tasolle sekä välttyä turhilta kustannuksilta.

5.4 Kartoituksen toteuttaminen

Käytännössä kartoitus tulisi toteuttaa noudattaen edellä esitettyä VAHTI-ohjeessa määriteltyä prosessia (ks. kuvio 4). Tämän työn kartoitus on toimeksiantajalle ensimmäinen laatuaan, joten pilottikohteen avulla kartoitusprosessia pyritään kehittämään. Tämän takia aiempaa ohjeistusta tai materiaalia ei kartoituksen tekoon ole, jolloin tässä työssä merkittävässä osassa on kartoituksen suunnittelu ja toteuttaminen.

Kartoitus suunniteltiin aiemmin esiteltyjen teknisten ohjeistuksien perusteella. Siihen koostettiin kyberturvallisuutta koskeva kysymyslista näistä ohjeista. ST-ohjeistosta kysymykset kohdistettiin siitä löytyvään muistilistaan. ST-kortista 710.02, kysymykset johdettiin perussuosituksista sekä lisäsuosituksista. Kartoituksessa etsitään vastaukset näihin kysymyksiin sekä täytetään ST-kortin 730.05 tarkastuspöytäkirja soveltuvin osin. Näistä materiaaleista koostettiin asiakirja, jonka tarkoituksena on toimia kartoituksen kysymysrunkona. Laadittu asiakirja löytyy liitteestä 1.

Tiedonhaku pyritään toteuttamaan mahdollisimman monipuolisesti. Tilaajan kanssa on toimittava tiiviissä yhteistyössä ja esimerkiksi dokumentaatiot olisi hyvä jakaa molempien osapuolien kesken. Eri rakennuksista vastaavat tahot tulisi saada mukaan kartoitukseen tai heiltä tulisi ainakin pystyä tiedustelemaan erilaisia käytäntöjä ja asioita kohteesta. Kun kartoitukseen on saatu sopivat henkilöt, toteutetaan kartoitus pitkälti kysymysten avulla. Haastattelun lisäksi voidaan kohteella tehdä erilaisia teknisiä kartoituksia ja havainnointikierroksia.

Kartoituksen laadukkaan tuloksen varmistamiseksi on tärkeää, että tilaajan puolelta saadaan kartoitukseen osallistumaan oikeat henkilöt. Jotta tämä olisi mahdollista, tulee kartoituksen tekijällä olla selvää, mitä kartoituksessa on tarkoitus käsitellä. Kysymykset ja läpikäytävät asiat tulisi ymmärtää niin, että niitä voi selventää tilaajalle, jolle nämä asiat eivät ole tuttuja. Kun tilaaja ei tiedä mistä kyberturvallisuudesta talotekniikassa on kyse, on hyvin tärkeää viestiä tehokkaasti, mitä kartoituksessa on tarkoitus saavuttaa sekä mitä kysymyksiä kartoituksessa on tarkoitus käydä läpi. Näin tilaaja toivottavasti pystyy tarjoamaan kartoitukseen

henkilöitä, jotka pystyvät vastaamaan kysymyksiin. Tämä on myös lopputuloksen kannalta hyvin merkittävä tekijä. Myös kartoituksen onnistumista tulee arvioida, etenkin kun kartoitusta tehdään ensimmäistä kertaa. Tulokset sekä kaikki sitä tehdessä havaitut ongelmat ja puutteet tulee kirjata tarkoin ylös tulevien kartoitusten kehittämistä varten. Erityisesti käytännön ongelmia tulee korostaa.

6 Kyberturvallisuuskartoituksen testaaminen pilottikohteella

Työn käytännön osuutena oli kyberturvallisuuskartoituksen testaaminen. Tämän toteuttamiseen toimeksiantaja tarjosi omista asiakkaistaan pilottikohteen, johon kartoitus pyrittiin tekemään. Tämän testauksen avulla oli tarkoitus selvittää mitä käytännön haasteita ilmenee kyberturvallisuuden nykytilaa määriteltäessä.

6.1 Pilottikohde

Pilottikohde valikoitui toimeksiantajan asiakkaista, joka pidetään tässä työssä anonyyminä turvallisuuden vuoksi. Kohde on julkisessa omistuksessa ja käytössä. Kohteella järjestetään yleisötapahtumia, joissa voi olla useita satoja henkilöitä. Rakennus on valmistunut 1980-luvulla, joten rakennuksen tekniikka on osittain vanhentunutta, ja siksi hyvin kiinnostava pilottikohde. Toimeksiantajalta tilataan palveluita julkisiin kohteisiin, joten tämänkin puolesta kyseisen kohteen arviointi palvelee toimeksiantajaa hyvin.

Kyseessä on toimeksiantajan toteuttama kehitystyö, joten tässä työssä käytetty pilottikohde ei ole esittänyt toiveita kartoitukselle, eikä heillä ole havaittu ongelmia kyberturvallisuuden kanssa. Heidän kohteensa toimii siis vain esimerkkikohteena tässä työssä. Kun kohteen haltija ei näe tarvetta kartoitukselle, eikä koe rakennusautomaation kyberturvallisuutta huolen aiheena, aiheuttaa se omat haasteensa kartoituksen tekoon. Tämä vaikuttaisi kuitenkin olevan melko yleinen tilanne vastaavissa kiinteistöissä ja siksi valikoitunut pilottikohde palvelee hyvin tätä kartoitusta.

6.2 Toteutus

Aihe esiteltiin kiinteistön ylläpidosta vastaavalle taholle. Heidän kanssaan pyrittiin päättämään kartoitukseen osallistuvat tahot, joilla olisi mahdollisimman laaja tuntemus kartoituksessa käsiteltävistä aiheista. He kehottivat olemaan yhteydessä kiinteistön käytöstä vastaavaan henkilöön, sillä hänellä arveltiin olevan eniten tietoa kiinteistön tekniikasta ja sen käytöstä sekä siten myös rakennusautomaation ja talotekniikan turvallisuudesta. Tämän perusteella kiinteistön käyttäjän kanssa järjestettiin haastattelu. Käyttäjää edusti kartoituksessa kiinteistön käyttöpäällikkö. Käyttäjän haastattelun avulla pystyttiin muodostamaan hyvä käsitys erilaisista käyttäjään liittyvistä käytänteistä, joiden avulla saatiin parempi käsitys kokonaisuudesta. Kuitenkin teknisemmät kysymykset etenkin verkkoyhteyksiä ja etäohjattuja järjestelmiä kohtaan jäivät vajavaisiksi. Nämä eivät myöskään ole käyttäjän vastuualueita kiinteistössä. Tästä syystä kartoituksen testaukseen pyrittiin löytämään myös kiinteistön verkkotekniikkaa ymmärtävä haastateltava. Henkilöksi valikoitui kiinteistöjen tietotekniikka-asiantuntija. Hänen kanssaan käytiin läpi verkkoyhteyksiin liittyviä kysymyksiä, erilaisten etäyhteyksien toteutustapoja sekä vastuiden jakautumisesta eri toimijoille. Haastattelujen tulokset on esitelty tässä luvussa. Myös itse kartoitus jouduttiin kevään 2020 vallitsevan tilanteen takia toteuttamaan puhelinhaastatteluina.

Aihe oli ainakin tässä tapauksessa haastateltaville täysin vieras. Perinteisten työasemien tietoturvasta ymmärretään enemmän, mutta tietämys taloteknisistä järjestelmistä on vähäisempää. Haastateltavia pyrittiin informoimaan kartoituksesta etukäteen mahdollisimman kattavasti puhelinkeskustelun sekä sähköpostin avulla. Haastateltaville perusteltiin, miksi nykyään myös taloteknisiä laitteita liitetään verkkoon ja mistä näiden riskit voivat koostua. Tämä auttoi tilanteessa hyvin eteenpäin sekä vähensi ennakkoluuloja. Sähköpostitse heille toimitettiin etukäteen myös liitteen 1. asiakirja sekä ST-730.05 pöytäkirja.

6.3 Käyttäjän haastattelu

Käyttäjän edustajana toimi kiinteistön käyttöpäällikkö. Kartoitusta suunniteltaessa hänellä arveltiin olevan eniten tietoa kiinteistön asioista sekä järjestelmien käytöstä. Hänelle kuvattiin aihetta puhelimitse sekä sähköpostilla ennen haastattelun toteuttamista. Hänen haastattelunsa toimi kartoituksen ensimmäisenä käytännön testinä. Haastattelussa saatiinkin hyvin käsiteltyä fyysinen suojaus, kulun- ja murtovalvonnan toteutukset, käytönopastus, riskienmäärittely sekä tietenkin käyttäjän näkemys taloteknisestä kyberturvallisuudesta yleisesti. Teknisiä kysymyksiä, kuten esimerkiksi talotekniikan etäyhteyksiä sekä verkkotopologioita käsiteltäessä, tuli kuitenkin selväksi, että kiinteistön käyttäjä ei ole oikea taho vastaamaan näihin kysymyksiin.

Fyysinen suojaus oli käyttäjän kanssa helppo käydä läpi. Käyttäjälle oli selvää, missä laitteistot sijaitsevat ja kuinka tilojen kulku on valvottu ja järjestetty. Palvelimet, muut verkkolaitteet sekä työasemat, joilta on pääsy järjestelmään, on kaikki sijoitettu lukittuihin tiloihin. Käyttöpäällikön vastuulla on myös kulunvalvontajärjestelmän käyttö sekä kulkuoikeuksien hallinta. Tähän on käytössä etäohjattu järjestelmä, johon on yhdistetty myös murtoilmaisin sekä kamerajärjestelmät. Järjestelmään kirjaudutaan etänä työasemalta henkilökohtaisilla tunnuksilla. Käyttöliittymästä on mahdollista tarkastella hälytyksiä sekä kulkua. Kameravalvontaan on oma käyttöliittymänsä, ja tähän on erilliset tunnukset. Tallenteiden katseluoikeus on määritelty vain tietyille henkilöille. Järjestelmä on kuitenkin toteutettu palveluna ja sen ylläpito on hoidettu toimittajan puolesta. Käyttäjällä ei ole tarkemmin tietoa, kuinka ylläpito toteutetaan, vaan tämä on toimittajan vastuulla.

Etäohjattujen sekä -käytettävien järjestelmien kohdalla pyrimme käyttäjän kanssa täyttämään ST-730.05 tarkistuspöytäkirjan. Käyttäjän tiedot järjestelmistä eivät kuitenkaan olleet riittävät pöytäkirjan täyttöä varten. Pöytäkirjan kysymykset ovatkin luonteeltaan sellaisia, että järjestelmätoimittaja vaikuttaa ainoalta taholta, kuka niihin pystyy luotettavasti vastaamaan. Kartoituksen toteutuksessa voisi hyvä olla osana myös järjestelmätoimittajan haastattelu, ainakin tärkeimpien

rakennusautomaatiojärjestelmien kohdalla. Tämä pöytäkirja olisi hyvä laatia uusia järjestelmiä hankittaessa ja tiedot olisi hyvä säilyttää järjestelmän käyttäjällä.

Käytönopastusta pohtiessa esiin nousi selkeänä erona perinteiset IT-järjestelmät ja niiden kyberturvallisen käytön opastaminen verrattuna taloteknisten järjestelmien vastaavaan. Käyttäjä on saanut ohjeistuksen työasemien ja sen ohjelmien kyberturvalliseen käyttöön, mutta rakennusautomaatiojärjestelmien käyttöön ei ole sisältynyt käyttöliittymien tai muun osalta kyberturva-asioiden ohjeistusta. Perinteisten ohjelmistojen ja työasemien salasanoille on määritelty päivitysaikaväli, kun taas rakennusautomaatiojärjestelmien kohdalla näin ei ole.

Kiinteistön käyttäjän on suoritettava riskienmäärittely. Ainoastaan he tuntevat omat toimintansa ja sen haavoittuvuudet. Heidän tulee arvioida omaa toimintaansa sekä erilaisten riskien vaikutuksia siihen. Haastattelussa nousikin esiin, että riskienkartoitus on laadittu, ja sitä pyritään päivittämään aikavälein. Riskikartoituksessa ei kuitenkaan ole käyttäjän tietojen perusteella huomioitu mahdollisia rakennusautomaatiojärjestelmien kyberturvallisuusriskejä. Rakennusautomaation kyberturvallisuuden aiheuttamat riskit voivatkin olla vaikeita hahmottaa, eikä niistä välttämättä ole selkeää hyväksyttyä ohjeistusta. Tästä syystä riskienmäärittelyssä käyttäjää tulisi avustaa ja mahdollisia riskejä sekä niiden seurauksia tulisi kuvata käyttäjälle.

Rakennusautomaation kyberturvallisuus nähdään tärkeänä asiana, johon ei ole luotu valmiita toimintatapoja ja hallintakeinoja. Rakennusautomaation kyberuhkia ei nähdä myöskään realisoitumassa. Haastateltava ei koe, että heidän toimintaansa häiritsemällä kukaan voisi saavuttaa mitään. Suurta taloudellista vahinkoa ei heidän toimintaansa häiritsemällä voi saavuttaa, vaan mahdolliset hyökkäykset olisivat enemmän kiusantekoa ja häirintää. Kyberriskien vaikutuksia voi kuitenkin olla etukäteen hankala arvioida, joten riskienmäärittelyn kautta tulisi asiantuntija kanssa pohtia, kuinka merkittäviksi nämä vahingot oikeasti voivat nousta.

Haastattelussa nousi ylläpidon toteutus siinä esiin, että käyttäjällä on melko vähän tietoa järjestelmien päivityksestä ja ylläpidosta. Tästä syystä järjestelmiä hankittaessa

ja niistä sopimuksia laadittaessa on hyvin tärkeää, että ylläpito määritellään sopimuksiin selkeästi ja niin, että käyttäjälläkin on selvää, kuinka se on toteutettu. Tämä korostaa myös järjestelmätoimittajien vastuuta.

Yleisesti haastattelu meni hyvin, ja kartoitukseen onnistuttiin saamaan vastauksia. Vastausten perusteella saatiin muodostettua selkeä kuva näiden osa-alueiden kyberturvallisuuden tilasta. Alkuperäisen suunnitelman ja aiheen esittelyn jälkeen ajatuksena oli, että käyttäjä tuntisi kohteen parhaiten ja pystyisi näin vastaamaan valtaosaan kartoituksen kysymyksistä. Kuitenkin tätä haastattelua tehtäessä kävi hyvin ilmi se, miksi on hyvin tärkeää saada kartoitukseen osallistumaan kiinteistön teknisistä toteutuksista tietävä henkilö. Vaikka laitteiden ja järjestelmien huolto ja sitä kautta ylläpito kuuluu käyttäjän vastuisiin, käytännössä käyttäjä kuitenkin vain tilaa huoltohenkilön kohteelle ja järjestelmätoimittajat hoitavat omat laitteensa sekä niiden ylläpidon tilauksesta.

6.4 Verkkoyhteyksistä vastaavan henkilön haastattelu

Toinen kartoituksen testaamiseen osallistunut haastateltava oli kiinteistön tietotekniikka-asiantuntija. Hänelle pyrittiin esittämään teknisempiä kysymyksiä, etenkin verkkoliikenteestä ja eri toimijoiden käyttämistä tietoliikenne yhteyksistä ja näiden toteutustavoista. Haastateltavan työtehtäviin kuuluu mm. yhteyksien luominen uusille laite- ja järjestelmätoimittajille.

Haastattelussa nousi esiin, että etäyhteyksien, valvonnan ja ohjaamisen tarve kasvaa. Erilaisia palveluita yhdistetään jatkuvasti kiinteistöihin. Yhteyksiä luotaessa kiinteistön verkkoyhteyksistä vastaavalla taholla on omat määrityksensä yhteyden luomiseen. Verkkoyhteydestä vastaava taho, eli tässä tapauksessa haastateltava, ei kuitenkaan ota kantaa esimerkiksi järjestelmän sisäiseen verkkoliikenteeseen tai sen suojaamiseen, vaan nämä seikat jäävät laite- tai järjestelmätoimittajan vastuulle. Tässä tilanteessa kiinteistön haltija hoitaa liikenteen turvaamisen kiinteistön verkkoon ja sieltä toimittajan verkkoon. Tässä he suosittelevat käytettäväksi toimittajan omaa verkkoliittymää. Näin yhteys saadaan määriteltyä siten, että vain toimittajalta sallitaan liikenne tiettyyn osoitteeseen. Isommat toimijat, jotka ohjaavat

suurta määrää laitteistoja, ovat perinteisesti voineet saada käyttöönsä julkisesti näkyviä (suoraan verkkoon näkyviä) IP-osoitteita, joiden kautta he voivat helpommin ohjata suuria määriä järjestelmiä. Näille toimijoille on palomuurein määritelty yhteys kiinteistön verkkoon.

Kiinteistön verkkoyhteyksien hallintaa on siis selvästi mietitty. Kaikki yhteydet ulkomaailmaan tulee suojata, ja näitä suojattuja yhteyksiä pidetään ajan tasalla. Liittymiä seurataan ja mikäli liikennettä ei ole, järjestelmä ehdottaa automaattisesti näiden yhteysmäärittelyjen poistamista. Haastattelun tuloksista korostuu, kuinka tärkeä vastuu laite- ja järjestelmätoimittajilla on kyberturvallisuuden kokonaisuudessa. Vaikka verkkoyhteys kiinteistöön toteutetaan suojatusti, jää toimittajalle vastuu siitä, että kyberturvallisuustekijät ovat kunnossa. Kuten siis ST-710.02 (2019) kortissakin suositellaan, olisi tästäkin syystä tärkeää käyttää luotettavia järjestelmätoimittajia, joilla on myös esittää dokumentaatio laitteidensa kyberturvallisuudesta. (ST-710.02 2019, 12). Mikäli näin ei toimita, voidaan toimittajan järjestelmien kautta mahdollisesti häiritä kiinteistöä.

Haastattelussa nousi esiin yksi mahdollinen kehityskohta. Kiinteistöön yhdistetyt järjestelmät toimivat kiinteistössä samassa virtuaaliverkossa (VLAN), eli laitteet ja järjestelmät näkevät toisensa samassa verkossa. Näiden järjestelmien jakaminen omille verkkoalueille verkkolaitteilla lisäisi kyberturvallisuutta. Nykytilanteessa esimerkiksi yhden järjestelmän haavoittuvuuden avulla voisi olla mahdollista häiritä myös muita talotekniikan järjestelmiä. Tässä esimerkki yksinkertaisesta toimenpiteestä, jolla olisi mahdollista lisätä kyberturvallisuutta.

Tämänkin haastattelun aikana korostui organisaatiorakenteiden vaikutus kokonaisuuteen. Kun yksittäisille, tässäkin esimerkissä toisistaan erillään toimiville osastoille, on määritelty tehtävät, on näiden osastojen hyvin vaikea hahmottaa talotekniikan kyberturvallisuus kokonaisuutena. Keskittyminen kohdistuu helposti vain omaan vastuualueeseen. Tämän lisäksi palveluiden ulkoistaminen vaikeuttaa myös kokonaisuuden hahmottamiseen.

6.5 Käytännön haasteet

Työn yksi tavoite oli nostaa esiin konkreettisia haasteita kartoitusta tehdessä. Kartoitusta testatessa näitä haasteita saatiinkin hyvin nousemaan esiin. Kun tarkoituksena on kehittää prosessia, on haasteet tärkeää taltioida. Haasteiden taltiointi on myös tärkeä osa kehittämistutkimusta (Kananen 2012, 48-49). Keskeisimpiä esiin nousseita haasteita olivat tehokkaan viestinnän merkitys kartoitusta suunniteltaessa, tiedonkulun aiheuttamat haasteet, henkilöstön vastuualueet sekä alalle vakiintuneet käytänteet.

Tehokas viestintä on onnistumisen kannalta tärkeä asia. Työssä laadittu kartoitus koostuu lähes pelkästään henkilöstölle esitettävistä kysymyksistä. Onkin siis hyvin tärkeää, että kartoitukseen saadaan osallistumaan oikeat henkilöt niin, että jokaisen osa-alueen asiantuntija saadaan osallistumaan kartoitukseen. Tässä työssä kiinteistön ylläpidosta vastaavalle taholle ei heti alusta asti saatu viestittyä selkeästi mistä kartoituksessa on kyse ja minkälainen henkilöstö olisi kartoitukseen hyvä saada mukaan. Kartoituksen laatijan vastuulla on varmistua siitä, että jokaisen osa-alueen asiantuntija on läsnä kartoituksessa. Tämä voi kuitenkin osoittautua hankalaksi, mikäli osapuolia on paljon. Kartoituksen laatijan on viestittävä käsiteltävät aiheet niin selkeästi kartoitusta suunniteltaessa, että kartoitettavan osapuolen yhteyshenkilö ymmärtää kartoituksen laajuuden ja osaa tarjota sellaisen henkilöstön, joiden avulla kaikki osa-alueet saadaan käsiteltyä. Tämän takia onkin erittäin tärkeää, että viestintä on heti alusta alkaen mahdollisimman tarkasti ja monipuolisesti kartoitusta kuvaavaa. Molemmilla osapuolilla tulee olla selvää, mitä kartoituksella halutaan saavuttaa.

Toinen haaste sekä kartoituksen toteuttamiselle että kyberturvallisuuden tilalle on puutteellinen tiedonkulku isoissa organisaatioissa. Kun toimikentässä on useita osapuolia, kuten esimerkiksi kiinteistöstä ja sen käytöstä, verkkoyhteyksistä ja tietotekniikasta, ylläpidosta, järjestelmistä ja turvallisuudesta vastaavat tahot, on tiedonkulun merkitys laajassa ketjussa erittäin tärkeä. Osa näistä osapuolista saattaa lisäksi olla ulkoistettuja palveluntarjoajia. Vastauksista nousee esiin myös, että kyberturva-asioita on selkeästi joskus pohdittu, mutta kaikille ei ole selvää mistä

nämä määritykset tulevat. Laajassa toimikentässä ei kuitenkaan käytännössä aina ole mahdollista tiedottaa kaikkia osapuolia. Tämän takia kyberturvallisuus pitää nähdä kokonaisuutena ja sitä pitää myös johtaa järkevästi.

Kolmas esiin noussut haaste on henkilöstön vastuualueet. Eri toimijat ja osapuolet keskittyvät hoitamaan omat vastuunsa, jotka on tarkasti määritelty sopimuksissa. Vaikka omasta vastuualueesta opitaan huolehtimaan, saattaa silti jatkuvasti muuttuvassa ympäristössä syntyä katvealueita. Usein on epäselvää, kenen vastuulla nämä katvealueet ovat. Kartoitusta tehdessä nämä katvealueet saattavat nousta esiin, mikäli kartoitukseen valitut henkilöt eivät osaakaan vastata heille esitettyihin kysymyksiin. Tällöin on epäselvää, kenen vastuualueista on kyse. Kartoittajan tärkeä tehtävä onkin yhdistellä eri toimijoilta saatua tietoa ja pyrkiä siten välttämään näitä katvealueita. Tämä saattaa olla haastavaa, mutta se olisi hyvä tiedostaa ja pitää mielessä kartoitusta suunnitellessa ja tehdessä.

Neljänneksi esiin nousseeksi haasteeksi muodostuu alalle vakiintuneet käytännöt. Kuten Antonini ja muut (2014, 1) myös nostavat esiin, taloteknisiä järjestelmiä ei osata nähdä samalla tavalla kyberturvallisuusriskinä, kuten perinteiset tietotekniset laitteet nähdään. Tämä korostuu, kun pyritään selvittämään kyberturvallisuutta juuri taloteknisissä järjestelmissä. Kyberturva nähdään helposti IT-osaston vastuuna, ja IT-osasto taas näkee talotekniset järjestelmät talotekniikasta vastaavien vastuulla. Tämän lisäksi kyberturvallisuus on uusi aihe myös talotekniikan sekä rakennusautomaation kanssa toimiville osapuolille. Keskustelua aiheesta pitääkin lisätä ja se tulee sisällyttää suunnitteluun sekä alan asiantuntijoiden täytyy ottaa siitä vastuu.

7 Johtopäätökset

Tämän opinnäytetyön tavoitteena oli laatia rakennusautomaation kyberturvallisuuskartoitus ja testata sitä käytännössä. Tavoitteena oli muodostaa laaditun kartoituksen pohjalta yleiskuva rakennusautomaation kyberturvallisuuden

tilasta pilottikohteella. Näiden lisäksi tämän kehittämistyön tarkoituksena oli nostaa esiin erilaisia käytännön haasteita kartoitusta suorittaessa.

Työssä onnistuttiin laatimaan kartoitus, joka käsittää monipuolisesti rakennusautomaation kyberturvallisuuteen vaikuttavat osa-alueet sekä kartoitusprosessin kulun. Kartoituksen tekninen sisältö koostettiin alan ST-korteista ja ohjeistosta. Näiden pohjalta muodostettiin eri osa-alueita käsittelevät kysymykset. Kartoitusprosessin rungon tulisi koostua hyvin toteutetusta suunnittelusta, itse kartoituksen suorittamisesta, tulosten raportoinnista sekä ylläpidon seurannasta. Kartoitus tulee esitellä kartoitettavalle taholle ja heidän kanssaan tulee muodostaa monipuolinen asiantuntijaryhmä. Ryhmän tietotaidon avulla on tarkoitus pystyä muodostamaan vastaukset eri osa-alueiden kysymyksiin. Kartoittavan henkilön tulee ohjata keskustelua vastausten löytämiseksi ja hänen tulee ymmärtää aihe niin, että hänen on mahdollista yhdistellä eri asiantuntijoiden tarjoamat tiedot. Näin pystytään muodostamaan käsitys rakennusautomaation kyberturvallisuuden nykytilasta.

Työssä laadittua kartoitusta testattiin pilottikohteella, kuitenkin vain osittain. Testauksen perusteella saatiin hyvä käsitys kartoituksen toimivuudesta ja sen toteuttamisesta. Kartoituksen perusteella oli mahdollista muodostaa selkeä kuva pilottikohteen kyberturvallisuudesta, niiltä osin kuin kartoitus toteutettiin. Erilaisia puutteita, esimerkiksi verkkotopologioissa ja käytänteissä, saatiin nostettua esiin. Myös hyvin hoidetut osa-alueet korostuivat kartoituksen tuloksissa. Näiden huomioiden avulla on mahdollista määritellä selkeät toimenpiteet kyberturvallisuuden tilan parantamiseksi.

Kolmas opinnäytetyön tutkimuskysymys liittyi kartoitusprosessissa esiin nouseviin haasteisiin. Kun pyritään laatimaan uudenlainen tuote, on selvää, ettei sitä ensimmäisellä kerralla saada lopulliseen muotoon. Näitä esiin nousseita haasteita kartoitusta tehtäessä olivat tehokkaan viestinnän merkitys kartoitusta suunniteltaessa, tiedonkulun aiheuttamat haasteet, henkilöstön vastuualueet sekä alalle vakiintuneet käytänteet. Näiden tulosten pohjalta voidaan kartoitusta tulevaisuudessa kehittää, jolloin näihin haasteisiin osataan varautua.

8 Pohdinta

Automaatiojärjestelmät ohjaavat maailmaamme ja vaikuttavat erittäin konkreettisesti jokapäiväiseen arkeemme. Siksi näiden järjestelmien oikea toiminta on tärkeää kaikissa tilanteissa. Automaatiojärjestelmien koskemattomuudesta ja turvallisuudesta ei täten voi tinkiä. Kyberturvallisuuden ja tietoturvan toteuttaminen käy yhä haastavammaksi toteuttaa itse, sillä kenttä laajenee ja muuttuu jatkuvasti. Kyberturvallisuus on tästäkin syystä hyvin perusteltua ulkoistaa siihen erikoistuneelle toimijalle. Jatkuvasti laajeneva ala tarjoaa myös useita uusia liiketoimintamahdollisuuksia. Esimerkiksi tämän työn oli tarkoitus keskittyä rakennusautomaation kyberturvallisuuteen ja sen tilan kartoittamiseen.

Kun rakennusautomaation kyberturvallisuuden tilaa halutaan lähteä parantamaan, on ensimmäisenä tärkeä pystyä muodostamaan käsitys vallitsevasta kyberturvallisuuden tilasta. Kyberturvallisuuden hallinnan pitää lähteä nykytilan ymmärtämisestä. Seuraavaksi tulee miettiä tavoitetaso mikä halutaan saavuttaa ja tämän jälkeen tulee miettiä miten tuohon tilaan päästään. Tämän pohdinnan perusteella opinnäytetyön aihe rajattiin rakennusautomaation kyberturvallisuuskartoituksen laatimiseen sekä sen testaamiseen käytännössä. Nämä muut vaiheet voivat kuitenkin tarjota tuleville kehittämistöille aiheita.

Kyberturvallisuuskartoitus onnistuttiin laatimaan ja se kattaa monipuolisesti rakennusautomaation kyberturvallisuuden osa-alueet. Kartoitusta päästiin myös testaamaan käytännössä. Valitettavaa on, että testauksen tulokset jäivät vajavaisiksi. Kuitenkin testaamisen pohjalta saatiin nostettua esiin useita haasteita, joita kartoitusta tehtäessä voi kohdata. Kartoituksen tulosten perusteella oli mahdollista määritellä selkeästi, mitkä asiat on hoidettu hyvin ja mihin tulee kiinnittää huomiota. Tässäkin mielessä kartoitus onnistuu toteuttamaan sille määriteltyä tehtävää. Opinnäytetyössä laadittua kartoitusta voidaan hyödyntää kyberturvallisuuden tilan määrittämisessä tulevaisuudessa.

Perinteisesti talotekniikasta ovat vastanneet talotekniikan tai rakennusautomaation asiantuntijat, ja heillä ei aina välttämättä ole tarvittavaa osaamista tietoteknisten

haavoittuvuuksien analysointiin. Kuitenkin merkittävän osan kyberturvallista ympäristöä muodostavat myös inhimilliset tekijät, salasanapolitiikat, järjestelmämäärittelyt ja palomuurien asettelut. Näihin seikkoihin on hallinnollisilla toimilla mahdollista vaikuttaa huomattavasti. Tästä syystä kartoituksen kysymykset käsittelevät pitkälti toimintatapoja ja käyttötottumuksia taloteknisten järjestelmien osalta. Mikäli halutaan toteuttaa kyberturvallisuuden teknisten haavoittuvuuksien tarkka selvitys järjestelmätasolla, tulisi siinä hyödyntää kyberturvallisuuden asiantuntijoiden teknistä osaamista. Työssä laadittuun kartoitukseen voisikin sisällyttää myös järjestelmätason haavoittuvuuksien tarkemman määrittelyn. Se tarjoaisi kokonaisvaltaisemman kuvan kyberturvallisuuden tilasta, mutta vaatisi myös aikaa vievän analyysin järjestelmistä ja laitteistoista kyberturvallisuuden asiantuntijan toimesta. Tulevaisuudessa rakennusautomaation ja talotekniikan asiantuntijoiden täytyykin toimia enemmän yhdessä tietotekniikan asiantuntijoiden kanssa, jotta palvelut voidaan toteuttaa myös kyberturvallisesti.

Kyberturvallisuus tulisi pitää uusia järjestelmiä hankittaessa suunnittelussa mukana heti alusta asti. Suunnittelijoille tulisi olla heti selvää, mitä järjestelmiltä vaaditaan kyberturvallisuuden tiimoilta. Näin voidaan heti alusta asti tehdä järjestelmätoimittajille määrittelyt siten, että kyberturvallinen tila saavutetaan. Näin ei pääse syntymään esimerkiksi tilannetta, jossa toimittajat on jo valittu toiminnallisten ominaisuuksien pohjalta ja kun kyberturvallisuus nousee myöhemmin suunnittelussa esiin, voi kynnys enää lähteä vaihtamaan toimittajia olla jo suuri. Laitteiden ja järjestelmien valmistajalla on myös suuri vastuu rautatason turvallisuudesta. Tämän takia on tärkeää, että valmistajille osataan määritellä tarpeeksi kattavasti turvallisuuteen liittyvät toiveet. Kun uusia järjestelmiä hankitaan, olisi näistä hyvä tuottaa kiinteistön haltijalle ymmärrys myös kyberturvallisuudesta, esimerkiksi täyttämällä ST-730.05 pöytäkirja.

Laadittua kartoitusta testattiin opinnäytetyössä vain yhdessä pilottikohteessa ja siinäkin vain osittain, eli kartoituksen toimivuutta muilla kohteilla ei voi taata. Kartoituksen laatijalle jää myös huomattava vastuu kartoituksen onnistumisesta. Kartoittajan tulee olla hyvin perillä rakennusautomaatiojärjestelmien kyberturvallisuudesta. On myös hyvin tärkeää, että kartoittajalle on selvää, mitä

kysymyksillä pyritään saavuttamaan, sillä haastateltavat eivät välttämättä ymmärrä mistä kysymyksissä on kyse. Kartoittajan tulee ohjata keskustelua ja varmistua omalla asiantuntijuudellaan vastausten luotettavuudesta.

Turvallisuutta vähätellään niin pitkään, kunnes jotain sattuu. Nykypäivänä monella alalla on sattunut lukuisia kertoja, ja siksi turvallisuus on jo viety pitkälle. Turvallisuus yleisesti kuitenkin nähdään tärkeänä asiana ja on selvää, että sen kohdalla toiminnan tulee olla proaktiivista. Talotekniikan kyberturvallisuus on tällä hetkellä siinä tilassa, että uhkia ei nähdä konkretisoitumassa ja siksi suhtautuminen on vähättelevää. Kuten tässäkin työssä on esitetty, ovat kyberturvallisuuden riskit kuitenkin oikeita ja niihin tulisi suhtautua vakavasti. Kyberturvallisuuden tilaa parantaa tietoisuuden lisääminen riskeistä sekä keinoista suojautua niiltä. Tämä työ lisää keskustelua sekä tietoisuutta aiheesta, mikä toivottavasti parantaa rakennusautomaation kyberturvallisuuden tilaa tulevaisuudessa.

Lähteet

Ahjopalo, J. 2019. Lahden kyberhyökkäystutkinta: livahtiko haittaohjelma tuhanteen tietokoneeseen yksittäisen käyttäjän toiminnan vuoksi?. Uutinen Ylen verkkosivuilla. Viitattu 26.3.2020. https://yle.fi/uutiset/3-10832288.

Antonini, A., Barenghi, A., Pelosi, G. & Zonouz, S. 2014. Security challenges in building automation and SCADA. 2014 International Carnahan Conference on Security Technology (ICCST). Viitattu 12.4.2020. janet.finna.fi, IEEE/IET Electronic Library (IEL).

Cyber-threat and the FM solution. 2017. Urgent Technologyn julkaisema artikkeli. Viitattu 26.2.2020. https://it.ifma.org/.

Deshmukh, R. V. & Devadkar, K. K. 2015. Understanding DDoS Attack & its Effect in Cloud Environment. Procedia Computer Science, 49,202-210. Viitattu 6.3.2020. janet.finna.fi, Science Direct.

Goebel, C., Jacobsen, H., Razo, V., Doblander, C., Rivera, J., Ilg, J., Flath, C., Schmeck, H., Weinhardt, C., Pathmaperuma, D., Apperath, H., Sonnenscheln, M., Lehnloff, S., Kramer, O., Staake, T., Fleisch, E., Neumann, D., Strüker, J., Erek, K., Zarnerkow, R., Zlekow, H. & Lässig, J. 2014. Energy Informatics; Current and Future Research Directions. (Report). Business & Information Systems Engineering, 6, 1, 25-31. Viitattu 3.2.2020. janet.finna.fi, ProQuest Central.

Hakala, J. T. 2004. Opinnäyteopas ammattikorkeakouluille. Helsinki: Gaudeamus.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2010. Tutki ja kirjoita. 15.-16. p. Helsinki: Tammi.

Järvinen, A. 2018. Talotekniikan kyberturvallisuus. Opinnäytetyö, AMK. Tampereen ammattikorkeakoulu, Talotekniikan koulutus. Viitattu 28.4.2020. http://urn.fi/URN:NBN:fi:amk-201805168357

Kamali, S., Khakzar, G. & Abdali Hajiabadi, S. 2014. Effect of Building Management System on Energy Saving. Advanced Materials Research, 856, 333-337. Viitattu 13.2.2020. janet.finna.fi, IEEE Xplore Digital Library.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kelly, A. N.d.. Building Management Systems: the cyber security blind spot. QineticQ:n julkaisema artikkeli. Viitattu 16.2.2020. https://www.computerweekly.com/ehandbook/Building-Management-Systems-The-cyber-security-blind-spot.

KNX Esineiden Internet. N.d. Tuote-esite KNX Finland Ry:n verkkosivulla. Viitattu 9.3.2020. http://www.knx.fi/doc/esitteet/KNX_esineiden_internetissa.pdf.

Koponen, J. 2016. Viestintävirasto: Taloautomaatiojärjestelmiä kaataneen verkkohyökkäyksen takana oli rikollisia. Uutinen Ylen verkkosivuilla. Viitattu 26.3.2020. https://yle.fi/uutiset/3-9278497.

Korpisaari, P.,Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.

Liedes, R. & Härkönen, P. 2018. Rakennusautomaatiojärjestelmät. 6., uudistettu painos. Espoo: Sähköinfo Oy.

Mundt, T. & Wickboldt, P. 2016. Security in building automation systems – A first analysis. 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security). Viitattu 9.3.2020. janet.finna.fi, IEEE/IET Electronic Library (IEL).

Nana, N. 2016. FM professionals must study cyber security threats. Constructionweekonline.com artikkeli. Viitattu 13.2.2020. janet.finna.fi, ProQuest Central.

Ojanperä, S. 2019. Kyberhyökkäys on maksanut Lahden kaupungille lähes 690 000 euroa. Uutinen Ylen verkkosivuilla. Viitattu 26.3.2020. https://yle.fi/uutiset/3-10914550.

Ollenberg, J. 2018. Verkottuneen talotekniikan tietoturva, ST-ohjeisto 22. Sähkötieto ry. Espoo: Sähkötieto. Viitattu 16.3.2020. https://severi.sahkoinfo.fi/item/5730?search=st%20ohjeisto%2022.

Rousku, K. 2014. Kyberturvaopas: Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Sainio, M. 2019. Investoi ajoissa kyberturvallisuuteen. Automaatioväylä, 35, 1, 16-17.

ST-710.02. 2019. Sähkö- ja tietoteknisten järjestelmien tietoturva. Sähkötieto. Espoo: Sähköinfo. https://severi.sahkoinfo.fi/item/6606?search=ST%20710.02.

ST-721.01. 2016. Talotekniikan tietojärjestelmien käyttöliittymät. Sähkötieto. Espoo: Sähköinfo. https://severi.sahkoinfo.fi/item/384?search=ST%20721.01.

ST-730.05. 2018. Sähkö- ja tietoteknisten järjestelmien tietoturvan tarkastuspöytäkirja. Sähkötieto. Espoo: Sähköinfo. https://severi.sahkoinfo.fi/item/6597?search=ST%20730.05.

ST-98.17. 2018. Rakennusautomaatiojärjestelmän kuntotutkimusohje. Sähkötieto. Espoo: Sähköinfo. https://severi.sahkoinfo.fi/item/3978?search=ST%2098.17.

Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2019. 2019. Traficom. Liikenne- ja viestintävirasto kyberturvallisuuskeskus. Viitattu 3.3.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Suojaamattomia_automaatioj%C3%A4rjestelmi%C3%A4_suomalaisissa_verkoissa_2019.pdf.

Särelä, M., Tiilikainen, S. & Kiravuo, T. 2013. Kyberuhat tavoittavat automaation. Aalto-yliopiston verkkojulkaisu tutkimustuloksista. Viitattu 24.3.2020. .https://www.automaatioseura.fi/site/assets/files/1431/kiravuo_timo_srel_mikko_tiilikainen_seppo_automaation_kyberuhat_aalto_yliopisto_sas_asaf_16_10_2013.pdf.

Tenkanen, T. 2016. Kiinteistöautomaatiojärjestelmän tietoturvakatsaus. Pro gradu -tutkielma. Jyväskylän yliopisto, tietotekniikka. Viitattu 13.4.2020. http://urn.fi/URN:NBN:fi:jyu-201608193825

Tietoturvallisuuden arviointiohje. 2014. Vahti 2/2014. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän julkaisema ohje. Viitattu 23.3.2020. vahtiohje.fi.

Zetter, K. 2014. Hacking hotel room controls. Uutinen Wired.com verkkosivulla. Viitattu 9.3.2020. https://www.wired.com/2014/07/hacking-hotel-room-controls/.

Liitteet

Liite 1 . Kyberturvallisuuskartoitus

Kyberturvallisuuskartoitus

Ensimmäisenä teidän olisi hyvä miettiä mille riskeille talotekniset järjestelmät teidät altistaa. Mitkä ovat kriittisimpiä järjestelmiä toimintanne kannalta? Mitä aiheutuisi, mikäli kyseinen järjestelmä lakkaisi toimimasta tai toimisi virheellisesti? Näin kartoitusta voidaan myös kohdentaa teille merkittäviin seikkoihin ja turhia asioita voidaan pyrkiä karsimaan.

Lista erilaisista kiinteistöautomaatiojärjestelmistä, joiden toimintaa ainakin olisi hyvä kartoituksessa miettiä:

Kulunvalvonta
Murtoilmaisujärjestelmä
Kameravalvontajärjestelmä
Paloilmoitinjärjestelmä
Rakennusautomaatiojärjestelmä (Ilmastointi, lämmitys, valaistus, muut ohjaukset)

ST-730.05 tarkastuspöytäkirja etäohjattuihin järjestelmiin

Pyritään näiden kysymysten lisäksi täyttämään ainakin osittain etäohjattuihin järjestelmiin luotu tarkastuspöytäkirja, joka toimitetaan tämän asiakirjan liitteenä.

Mitä järjestelmiä teillä ohjataan verkon yli, tai kerätäänkö esimerkiksi mittausdataa verkkopalveluun?

Eli onko esim. lämmitykseen tai ilmastointii kytketty keskitettyä tai jonkinlaista älykästä ohjausta? Ohjataanko kulunvalvontaa verkosta? Tekevätkö paloilmoittimet suoran hälytyksen palolaitokselle? Nämä ovat merkkejä verkon yli ohjatuista järjestelmistä.

Kysymykset

Hallinnolliset kysymykset

Onko riskinmäärityksiä tehty jo ennen tätä kartoitusta? Onko teillä laadittuna varautumis- ja toipumissuunnitelma?

Onko teillä määriteltynä selkeät vastuut laitteistoista ja järjestelmistä eri osapuolten kesken?

Onko järjestelmien tarkoituksenmukainen käyttö määritelty ja turhat ominaisuudet karsittu pois?

Onko koko käyttöympäristön dokumentaatio ajan tasalla ja päivitettynä? Miten sitä ylläpidetään?

Onko laitteiden ja järjestelmien käytettävyys varmistettu sopimuksin? Suoritetaanko sille auditointeja?

Miten tilannekuvaa arvioidaan, päivitättekö riskiluetteloita?

Miten järjestelmien käytön valvonta on toteutettu?

Verkkoon kytkeminen

Onko teillä suoraan verkkoon kytkettyjä laitteita?

Miten näitä on suojattu?

Fyysinen sijoittelu

Miten kriittiset osat kuten valvomot, aktiivilaitteet ja järjestelmien käyttöpäätteet on sijoiteltu? Ovatko ne lukituissa tiloissa?

Onko talotekniikkaverkkoon pääsy julkisista tiloista estetty?

Miten kulku kiinteistön tele- ja teknisiin tiloihin on järjestetty? Onko muilla kuin huoltohenkilökunnalla pääsyä tiloihin?

Onko tiloissa kulunvalvontaa?

Sisäverkon kokoonpano

Onko sisäverkon työasemien ja palvelimien kokoonpano selvillä?

Ovatko virus- ja haittaohjelmienpoistotyökalut asennettuna?

Talotekniikan verkkotopologia suunnittelu

Miten verkon topologia on suunniteltu? IP-tason määrittelyt, pääsyn hallinta sisään ja ulos sekä yhteydet muihin verkkoihin? Eli miten verkon rakenne on muodostettu, onko tästä mahdollisesti esimerkiksi dokumentaatiota?

Onko talotekniikkaverkko eristetty ns. toimisto- tai business- verkosta?

Onko dokumentaatio ajan tasalla?

Onko talotekniikkaverkkoa jaettu osiin eri alijärjestelmiä varten, kuten esimerkiksi rakennusautomaatio, mittarointi, kulunvalvonta ja kameravalvonta?

Onko verkkoliikenteelle tehty rajoituksia tai laitetason varmistuksia (MAC- varmennuksia tms.)?

Onko järjestelmien verkkoliikennettä salattu?

Käytönopastus

Onko teillä käytössä henkilökohtaiset tunnukset ja salasanat taloteknisten järjestelmien käyttöön?

Onko henkilöstöllä selvää, miten toimia, mikäli havaitaan tietoturvapoikkeama?

Miten käyttäjät ohjeistetaan toimimaan oikein ja tietoturvallisesti?

Salasanojen hallinta

Onko laitteistojen oletussalasanat vaihdettu?

Onko teillä tiedossa verkkoon kytkettyjen laitteiden tunnukset ja salasanat, esimerkiksi listalla?

Käyttöoikeuksien hallinta

Onko salasanapolitiikkoja määritelty?

Onko teillä määriteltynä henkilö, joka on vastuussa käyttöoikeuksien myöntämisestä ja hylkäämisestä?

Kartoitetaanko järjestelmän käyttäjätunnuksia tietyin aikavälein ja poistetaanko tarpeettomat käyttöoikeudet?

Ylläpito

Onko teille tehty jatkuvuussuunnitelma?

Päivitykset

Kuinka teillä järjestelmät pidetään päivitettynä?

Laitteiden ja järjestelmien elinkaaren hallinta

Onko teillä varmistettu järjestelmien ja laitteiden saatavuus tulevaisuudessa, entä niiden tuki?

Onko teillä tietoturvallisuutta huomioitu pitkän tähtäimen suunnitelmissa?

Saman verkon hyödyntäminen useiden järjestelmien kommunikointiin

Käytetäänkö teillä samaa verkkoa useiden järjestelmien kommunikointiin?

Onko järjestelmiä yhteen liittäessä huomioitu tietoturvakriteereitä?

Integroidut järjestelmät

Onko teillä integroituja, eli yhdistettyjä järjestelmiä käytössä?

Onko näitä luotaessa huomioitu tietoturvanäkökohdat?

Liitteet

ST-kortti 730.05