Elmeri Saukonoja

Rakennuksen digitaalisen turvallisuuden selvitys RT-korttien pohjalta

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

06.05.2024

Tiivistelmä

Tekijä:	Elmeri Saukonoja
Otsikko:	Rakennuksen digitaalisen turvallisuuden selvitys RT-korttien pohjalta
Sivumäärä:	32 sivua + 1 liite
Aika:	06.05.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine:	Automaatiotekniikka
Ohjaajat:	Osastonjohtaja Jukka Karhu Lehtori Jukka Karppinen

Opinnäytetyössä käsiteltiin rakennusten digitaalista turvallisuutta sekä teoreettisesti että tietoturva-auditoinnin näkökulmasta. Työ toteutettiin Granlund Oy:lle, joka on suomalainen rakennus- ja kiinteistöalan asiantuntijakonserni. Opinnäytetyön tavoitteena oli luoda malli tietoturva-auditoinnin toteuttamiseksi, mikä sisältää auditointiin liittyvän tarkastusprosessin ja tukiaineiston.

Opinnäytetyön aluksi käsiteltiin digitaalista turvallisuutta, kyberuhkia ja taloteknisiä järjestelmiä sekä niiden riskejä ja riskienhallintakeinoja. Teoriaosuuden jälkeen alkoi opinnäytetyön käytännön osuuden eli tietoturva-auditoinnin käsittely. Teorian tavoitteena oli perehdyttää lukija aiheeseen ja siten helpottaa tietoturva-auditoinnin merkityksen ymmärtämistä.

Tietoturva-auditointi tehtiin Granlundin asiakkaan kiinteistöön. Auditointi suoritettiin haastattelemalla kohteen kiinteistöpäällikköä ja digitaalisesta turvallisuudesta vastaavaa henkilöä. Auditoinnin tulokset käsiteltiin ja raportoitiin. Tulosten käsittelyn jälkeen pohdittiin auditoinnissa käytettyjen rakennusten digitaalisen turvallisuuden RT-korttien hyödynnettävyyttä tietoturva-auditoinnin tekemisessä.

Opinnäytetyön lopputuloksena syntyi malli rakennuksen digitaalisen turvallisuuden tason selvittämiseksi tietoturva-auditoinnin avulla. Luodun mallin avulla Granlund voi jatkossa tarjota asiakkailleen tietoturva-auditointia.

Avainsanat: digitaalinen turvallisuus, kyberuhka, talotekniikka, riski, tietoturva-auditointi

Abstract

Author:	Elmeri Saukonoja
Title:	Survey of a Building's Digital Security based on RT-Cards
Number of Pages:	32 pages + 1 appendix
Date:	6 May 2024
Degree:	Bachelor of Engineering
Degree Programme:	Electrical and Automation Engineering
Professional Major:	Automation Engineering
Supervisors:	Jukka Karhu, Head of department
	Jukka Karppinen, Senior Lecturer

The thesis work dealt with the digital security of buildings both theoretically and from the perspective of information security auditing. The project was carried out for a Finnish company called Granlund Oy. The company operates in the construction and real estate industry. The aim of the thesis work was to create a model for implementing information security auditing. The model includes the audit process and supporting materials.

The thesis begins with a theoretical section discussing digital security, cyber threats, building technology systems, and their risks and risk management measures. After this, the practical part handles information security auditing. The purpose of the theoretical section is to introduce the reader to the topic and thus facilitate understanding of the importance of information security auditing.

The information security audit was conducted on a property owned by one of Granlund's clients. The audit was conducted by interviewing the property manager and the person responsible for the digital security of the property. The results of the audit were analyzed and reported. After processing the results, the potential utilization of the RT-cards used in the audit for assessing the digital security of buildings in information security auditing was considered and this is discussed in the thesis.

As a result of the project, a model was developed for determining the level of digital security of a building with the help of information security auditing. Granlund can offer information security auditing to its clients in the future with the developed model.

Keywords: digital security, cyber threat, building automation, risk, information security audit

Sisällys

Lyhenteet

BGP: *Border Gateway Protocol*. Ulkoinen reititysprotokolla, joka vaihtaa internetin saavutettavuus- ja reititystietoja autonomisten järjestelmien välillä.

DVV: Digi- ja väestötietovirasto.

GDPR: *General Data Protection Regulation*. Euroopan unionin yleinen tietosuoja-asetus.

IoT: *Internet of Things*. Suomeksi esineiden internet. Tarkoittaa laitteita, jotka käyttävät internettiä tiedonvälityskeinonaan.

LVI: Lämmitys, vesi ja ilmastointi.

RT-kortisto: Rakennustietokortisto eli RT-kortisto on Rakennustieto Oy:n omistama tietopalvelu rakentamisen tueksi.

ST-kortisto: Sähkötietokortisto eli ST-kortisto on Sähkötieto ry:n julkaisema tietopalvelu sähköisten järjestelmien suunnitteluun, toteutukseen ja ylläpitoon.

TATE: Talotekniikka.

VAK: Rakennusautomaation valvonta-alakeskus.

VPN: *Virtual Private Network*. VPN-verkko suojaa toiminnan ja yhteyden julkista verkkoa käytettäessä.

Wi-Fi: *Wireless Fidelity*. Langaton verkkoyhteys.

1 Johdanto

Yhteiskunnan digitalisaation kasvun ja kehityksen myötä myös digitaalisen turvallisuuden uhat ovat kasvaneet ja kehittyneet. Digitaalisia verkkoja ja alustoja hyödynnetään viestintään ja tietojen tallentamiseen jatkuvasti. Yksittäisistä ihmisistä kertyy tietoja julkisen hallinnon ja yritysten sähköisiin palveluihin. Jotta digitaaliset toimintaympäristöt toimivat, on siellä operoivien tahojen tiedostettava riskit ja varauduttava erilaisiin uhkiin. Digi- ja väestötietoviraston (DVV) mukaan digitaalinen toimintaympäristö tarkoittaa kaikkia niitä tietojärjestelmiä, joissa tietoa käsitellään eri tavoin ohjelmistoilla, laitteilla tai verkoissa. DVV:n esimerkkejä digitaalisista toimintaympäristöistä ovat pikaviestipalvelut, pankki- ja maksupalvelut, verkko-oppimisympäristöt, sosiaalisen median alustat ja tuotannonohjausjärjestelmät. [1.]

Opinnäytetyön tarkoituksena on perehtyä rakennusten digitaaliseen turvallisuuteen tekemällä tietoturva-auditointi käytännön kohteeseen. Työn tavoitteena on luoda Granlundille malli tietoturva-auditointia varten. Granlund Oy on vuonna 1960 perustettu kiinteistö- ja rakennusalan yhtiö, jonka palveluksessa työskentelee yli 1400 asiantuntijaa pääosin Suomessa, mutta toimipisteitä on myös Ruotsissa ja Isossa-Britanniassa [2]. Tietoturva-auditointi tehtiin Granlundin asiakkaalle, jota käsitellään opinnäytetyössä sopimuksen mukaisesti anonyymisti turvallisuussyistä.

Luodun ja jatkokehitettävän mallin avulla Granlund voi jatkossa tarjota asiakkailleen uutena palvelunaan myös tietoturva-auditointia. Ennen käytännön osuuden käsittelyä aihetta pohjustetaan teoriaosuudella, jossa käydään läpi yleisesti digitaalista turvallisuutta, kyberuhkia ja taloteknisiä järjestelmiä. Teoriaosuudessa käytettiin lähteinä verkkoaineistoja, raporttia ja rakentamisalan ohjekortteja.

2 Digitaalinen turvallisuus

Digitaalinen turvallisuus tarkoittaa tilaa, jossa digitaalisen toimintaympäristön toiminta on valvottua, turvallista ja hallittua, myös häiriötilanteissa [3]. Kuvassa 1 esitellään digiturvallisuuden keskeiset toteutusalueet.

Kuva 1. Digiturvallisuuden keskeiset toteutusalueet [1].

Riskienhallinta eli riskeihin varautuminen ja toiminnan jatkuvuuden hallinta ovat osa digiturvallisuutta. Riskienhallinnan tarkoituksena on ennakoida ja varautua mahdollisiin ongelmatilanteisiin [3, s. 53]. Riskienhallintaa varten luodaan toimenpiteet ja riskien arviointiprosessi [1].

Jatkuvuudenhallinta tarkoittaa organisaation toimintakyvyn varmistamista häiriötilanteissa. Tämä onnistuu, kun häiriötilanteita ennaltaehkäistään ja niihin varaudutaan. Häiriötilanteista tulee myös opetella palautumaan ja niitä tulee opetella hallitsemaan. [1.] Jos toimintakyky menetetään ja digiturvallisuus vaarantuu, on tärkeää tietää, kuinka kyseisessä tilanteessa pitää toimia, jotta vahinko ei pääse leviämään hallitsemattomasti ja aiheuta liian suurta tuhoa. Oikealla etukäteen opitulla toimintatavalla vahingon laajuus saadaan minimoitua.

Kyberturvallisuus on digiturvallisuuden osa-alue, millä pyritään digitaalisesti verkostoituneen yhteiskunnan turvallisuuteen [4]. Sen avulla pyritään turvaamaan yhteiskunnan elintärkeät ja kriittiset toiminnot mahdollisten vaikuttamisyritysten, häiriöiden tai hyökkäysten varalta [1].

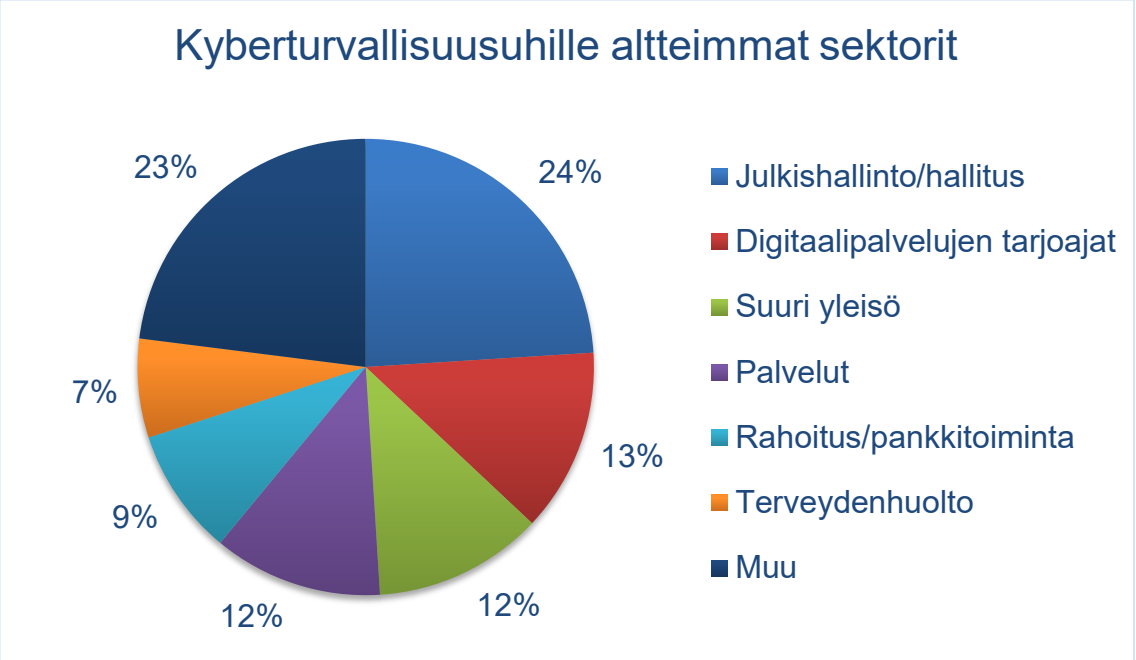
Tietosuoja tarkoittaa ihmisten yksityisyyden suojaa, eli henkilötietojen oikeanlaista säilytystä ja käsittelyä, etteivät ne joudu vääriin käsiin. Organisaation näkökulmasta tämä tarkoittaa esimerkiksi potilastietojen huolellista käsittelyä. Yksilön näkökulmasta tämä puolestaan tarkoittaa tarkkaa harkintaa henkilötietojen syöttämisessä digitaalisiin palveluihin. [1.] Tietoturvallisuus eli tietoturva tarkoittaa toimia, joilla pyritään varmistamaan ja suojaamaan organisaation tietoja. Tietoturvan avulla pyritään myös turvaamaan organisaation tietoja sisältävien palveluiden, järjestelmien, tietoliikenteen tai tietovarastojen luottamuksellisuus, eheys ja saatavuus [4]. Tietoturvallisuus- ja tietosuoja-termin ero on se, että tietosuojan tavoitteena on yksittäisen henkilön tietojen luottamuksellinen ja suojattu käsittely. Tietoturva kattaa puolestaan kaikki organisaation toiminnan kannalta tärkeiden tietojen suojan. [5.]

3 Kyberuhat

Kyberturvallisuusuhat ovat kasvaneet digitalisaation kasvun myötä. Uhkia ovat esimerkiksi:

- haittaohjelmat
- kiristysohjelmat
- käyttäjän manipulointi
- dataan kohdistuvat uhat
- palvelunestohyökkäykset
- internetin saatavuuteen kohdistuvat uhat
- disinformaatio ja misinformaatio
- toimitusketjuhyökkäykset [6.]
- ohjelmistojen/järjestelmien päivittämättömyys [7]
- julkiset Wi-Fi-verkot [8].

Kuvassa 2 on esitetty ympyräkaavion avulla kyberuhille altteimmat sektorit heinäkuun 2021 ja kesäkuun 2022 välisenä aikana.



Kuva 2. Kyberturvallisuusuhille altteimmat sektorit (heinäkuu 2021 – kesäkuu 2022) [6].

Haittaohjelmat

Haittaohjelmat ovat haitallisia sovelluksia tai koodeja, mitkä häiritsevät ja vahingoittavat verkkojärjestelmään yhdistettyjen fyysisten laitteiden normaalia toimintaa. Haittaohjelman tartuttaman laitteen tietoja voidaan käyttää luvattomasti ja lukita laitteen käyttäjä ulos laitteesta, kunnes vaatimuksiin on vastattu. Kyberrikolliset levittävät laitteisiin haittaohjelmia ja kiristävät niiden käyttäjiltä lunnasrahaa esimerkiksi pankkitietojen tai myyntikelpoisten henkilötietojen avulla. [9.]

Kiristysohjelmat

Kiristysohjelma on haittaohjelmatyyppi, minkä tarkoitus on salata käyttäjän tiedostoja ja estää tätä käyttämästä tietokonettaan. Tiedostojen lukituksen poistamiseksi on yleensä maksettava lunnaat. Kiristysohjelma voi levitä myös muihin

samassa verkossa oleviin laitteisiin. Kiristysohjelma voi päästä tietokoneelle, jos käyttäjä vierailee suojaamattomilla, epäilyttävillä tai väärennetyillä verkkosivustoilla. Myös avaamalla odottamattoman tuntemattomalta lähettäjältä saadun liitteen tai haitallisen linkin esimerkiksi sähköpostista tai tekstiviestistä käyttäjä saattaa päästää kiristysohjelman tietokoneelleen. [10.] Vuonna 2022 kiristysohjelmahyökkäykset olivat yksi suurimmista kyberuhista, ja ne ovat muuttumassa yhä monimutkaisemmiksi [6].

Käyttäjän manipulointi

Käyttäjän manipulointi (engl. social engineering) tarkoittaa tekniikoita, joilla uhria huijataan paljastamaan ja luovuttamaan arkaluonteisia tietoja tai toimimaan hyökkääjän tahdon mukaan. Arkaluonteisia tietoja ovat esimerkiksi käyttäjätunnukset ja pankkitiedot. Tekniikka perustuu ihmisten hyväntahtoisuuden tai inhimillisen virheen hyödyntämiseen. Suurten yritysten työntekijät ovat yleinen kohde, koska heiltä voidaan saada pääsy yrityksen tietoihin, tietokonejärjestelmiin tai muuhun omaisuuteen. Huijarit esiintyvät yleensä luotettavana tahona, kuten esihenkilönä, virkamiehenä tai muuna kohteen tuttuna henkilönä. Huijarit vetoavat kiireeseen, jotta kohde ei ehdi ajattelemaan tekojensa seurauksia. [11.]

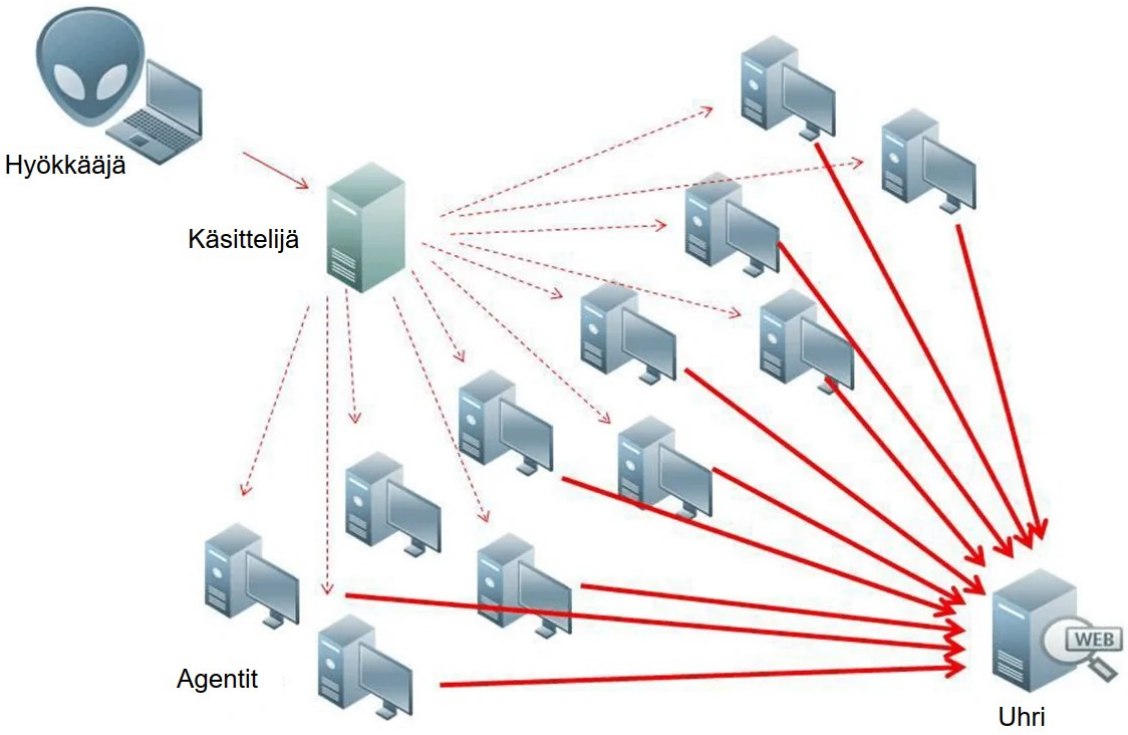
Dataan kohdistuvat uhat

Datalähteisiin kohdistuvien hyökkäysten tavoitteena on tietojen luvaton käyttö ja paljastaminen [6]. Rikolliset haluavat häiritä organisaation toimintaa tai hyötyä datasta rahallisesti [12]. Yleisimmin rikollisten motivaationa on raha, mutta noin kymmenessä prosentissa tapauksista motiivina on vakoilu. [6.]

Palvelunestohyökkäykset

Palvelunestohyökkäyksen pyrkimyksenä on estää verkkosivuston tai palvelun käyttö häiritsemällä sen toimintaa kuormittamalla kohdepalvelu tai verkkoliikenne ylimääräisellä liikenteellä ja hyödyntämällä haavoittuvuutta. Hajautetussa palvelunestohyökkäyksessä hyökkääjä on kaapannut useita internetiin

yhdistettyjä laitteita hyökkäyskäyttöön laitteiden omistajien tietämättä ja lähettää liikennettä kohteeseen useista eri lähteistä samanaikaisesti (kuva 3). Nykyään suurin osa on juuri tällaisia hyökkäyksiä. Liikenteen suuri määrä ei kuitenkaan ole ainoa vaihtoehto, vaan hyökkäyksen voi myös toteuttaa lähettämällä sellaista liikennettä, joka saa kohdelaitteen käyttämään normaalia enemmän muisti- ja laskentaresursseja. [13.]



Kuva 3. Hajautettu palvelunestohyökkäys [14].

Internetin saatavuuteen kohdistuvat uhat

Internetin käyttö ja tiedon vapaa liikkuminen vaikuttavat monien elämään. Monille ihmisistä internetiin pääsy on muodostunut perustarpeeksi töissä, opiskelussa, mielenilmaisussa, poliittisessa vapaudessa tai sosiaalisessa vuorovaikutuksessa. Siksi internetin häiriöt vaikuttavat lähes jokaisen elämään jollain tavalla. Internetin saatavuutta voidaan häiritä esimerkiksi internetinfrastruktuurin fyysisellä haltuunotolla ja tuhoamisella tai BGP (Border Gateway Protocol) -kaappauksella eli reitittämällä verkkoliikenne uudelleen haitallista reittiä

pitkin. Kaappaus voi johtaa virheelliseen reititykseen, tietojen seurantaan tai uudelleenohjaukseen toiselle verkkosivustolle. [15, s. 78–79.]

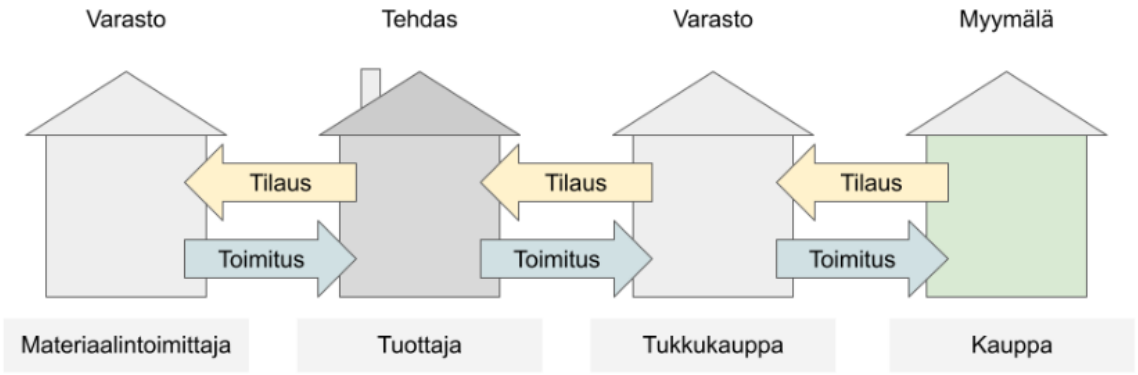
Disinformaatio ja misinformaatio

Disinformaatio on valheellisen ja harhaanjohtava tiedon levittämistä, minkä tarkoitus on vaikuttaa ihmisiin sekä heidän ajatteluunsa. Disinformaation levittämiselle on monia syitä, kuten esimerkiksi taloudellinen hyöty, poliittiset motiivit, trollaus ja epäluulon kylväminen. [16.]

Misinformaatio on myös väärää tietoa, mutta sen tarkoituksena ei ole johtaa lukijaa tai kuulijaa harhaan. Esimerkiksi jakamalla vahingossa sosiaalisessa mediassa virheellistä tietoa sisältävän uutisen syyllistyy misinformaation levittämiseen. [16.]

Toimitusketjuhyökkäykset

Toimitusketjulla tarkoitetaan eri organisaatioiden välisiä materiaali- tai palveluvirtoja sekä niihin liittyviä raha- ja tietovirtoja. Tavaralogistiikan tilaus-toimitusketjun organisaatiot ovat materiaalintoimittaja, tuottaja, tukkukauppa ja kauppa/myymälä (kuva 4). [17.]



Kuva 4. Tavaralogistiikan tilaus-toimitusketju [17].

Toimitusketjuhyökkäyksen tarkoituksena on päästä käsiksi organisaation tietojärjestelmiin käyttämällä hyväksi organisaation käyttämiä verkostoja, palveluita, tuotteita tai avoimen lähdekoodin projekteja. Tämä tapahtuu hyödyntämällä organisaatioiden luottamusta toimittajiinsa. Hyökkäyksessä polkuna voivat toimia yhteistyökumppanit, palveluntarjoajat, ohjelmistot tai laitteet. Tunkeuduttuaan toimittajan järjestelmiin hyökkääjä tartuttaa osan toimitusketjusta omalla haittakoodillaan. Tämän jälkeen haittakoodi leviää tuotteen jakelukanavaa pitkin yhteistyö- ja asiakasorganisaatioihin. [18.]

Ohjelmistojen ja järjestelmien päivittämättömyys

Haittaohjelmat ja virukset tarttuvat helposti tietokoneisiin, joiden käyttöjärjestelmiä tai viruksentorjuntaohjelmistoja ei ole päivitetty. Useimmat verkkorikollisten laatimista haittaohjelmista ja viruksista on kehitetty juuri näiden päivittämättömien ohjelmistotyyppien murtamiseen. Murtamista edesauttaa se, että uusien ohjelmistopäivitysten yhteydessä luetellaan ne vanhan ohjelmistoversion tietoturva-aukot, jotka on uusimmassa versiossa korjattu. Näin ollen on tärkeää huolehtia laitteiden ohjelmistojen ja käyttöjärjestelmien päivittämisestä. Laitekäyttäjän ei tarvitse manuaalisesti tarkistaa ja päivittää ohjelmistoja, mikäli automaattiset ohjelmistopäivitykset ovat päällä. [7.]

Julkiset Wi-Fi-verkot

Julkisissa Wi-Fi-verkoissa eli langattomissa verkoissa asiointi ei ole tietoturvallista. Julkisen verkon omistaja tai jopa saman verkon käyttäjä voivat saada tietoonsa käyttäjän laitteen ja sen tietoliikenteen. Samassa julkisessa langattomassa verkossa olevat käyttäjät voivat nähdä toistensa käyttämät verkkosivustot ja salaamattomana lähettämät tiedot. Salasanalla varustetut julkiset verkot ovat harvemmin yhtään salaamatonta verkkoa turvallisempia, koska salasana on yleensä saatavilla sitä kysyttäessä. [8.] Uutisten lukeminen tai muu vastaava verkossa surffaaminen ei ole vaarallista, mutta esimerkiksi verkkopankin käyttäminen, henkilötietojen käsittely, verkossa maksaminen tai työn tekeminen ei ole järkevää. Julkista Wi-Fi-verkkoa voi käyttää turvallisesti VPN (Virtual Private

Network) -yhteyden, eli virtuaalisen erillisyhteyden avulla, koska silloin tietoliikenne on täysin salattua [8].

4 Talotekniset järjestelmät

LVI-, sähkö- ja rakennusautomaatiojärjestelmät ovat taloteknisiä järjestelmiä, jotka huolehtivat rakennuksen toimivuudesta ja turvallisuudesta. Ne varmistavat, että rakennuksen sisäolosuhteet ovat miellyttävät ja terveelliset. [19.] LVI-järjestelmät huolehtivat lämmityksestä, jäähdytyksestä, vedestä ja viemäröinnistä sekä ilmastoinnista. Rakennusautomaatiojärjestelmä kuitenkin valvoo, ohjaa ja säätää kaikkia muita taloteknisiä järjestelmiä. Rakennusautomaatiojärjestelmä on täten merkittävässä roolissa rakennusten energiankulutuksen säännöstelyssä. LVI- ja sähköjärjestelmien lisäksi rakennusautomaatiojärjestelmään voi lisätä esimerkiksi palo-, turva- ja mittausjärjestelmiä. [20.] Kuvasta 5 voidaan nähdä, kuinka paljon talotekniikkaa rakennuksessa voi olla.

Kuva 5. Esimerkki rakennuksesta löytyvästä talotekniikasta [21].

4.1 Riskit

Nykyään monet taloteknisistä järjestelmistä ovat digitaalisessa ympäristössä ja etähallittavissa verkon välityksellä. Järjestelmiin kohdistuu useita riskejä, jotka toteutuessaan voivat vaarantaa ihmisten terveyttä ja turvallisuutta sekä aiheuttaa taloudellisia menetyksiä [4, s. 5]. Rakennusten digitaalisessa turvallisuudessa riskit vaihtelevat rakennuksen koon, käyttötarkoituksen ja teknologian mukaan.

Rakennuksista ja niiden ympäristöstä kerätään erilaisia tietoja, kuten olosuhdetietoja. Kulun- ja kameravalvontajärjestelmät sisältävät henkilötietoja, koska niistä voi seurata henkilöiden liikkeitä tiettyinä ajankohtina. Kameravalvontajärjestelmä saattaa sisältää myös mikrofoneja, jotka tallentavat ihmisten välisiä keskusteluja. Näiden tietojen keräämisen ja käsittelyn on oltava perusteltua ja luvallista. Lupien rikkominen voi johtaa rikosoikeudellisiin seurauksiin. [4, s. 5–6.]

IoT (Internet of Things) -laitteet eli langattomaan verkkoon yhdistetyt laitteet, kuten monitoimitulostimet ja anturit ovat turvallisuusriski, jos niiden suojauksesta ei ole huolehdittu ja ne ovat osa liiketoimintaa palvelevaa verkkoa. Niiden turvallisuuspuutteiden takia voidaan päästä käsiksi rakennuksen langattomaan verkkoon ja tietojärjestelmiin ja sitä kautta jopa asiakastietorekisteriin. Siksi yritysten on kannattavaa lisäinvestoida taloteknillisten järjestelmien ja liiketoimintaa palvelevien verkkojen fyysiseen erottamiseen pienentääkseen riskejä. [4, s. 6.]

Kybervaikutusta kohdistamalla voidaan pyrkiä vaikuttamaan rakennuksen tiettyihin toimintoihin. Esimerkiksi energiankulutukseen kohdistetulla hyökkäyksellä voidaan vaikuttaa rakennuksen kustannuksiin. Tilan lämmityksen ja jäähdytyksen ohjaaminen päälle samanaikaisesti vaikuttaa sekä olosuhteisiin että suoraan kustannusten nousuun. Kustannusten nousuun voidaan pyrkiä kybervaikuttamaan myös välillisesti esimerkiksi häiritsemällä ovien automaatiota. Tällöin kulunvalvonta tarvitsee lisätyövoimaa, mikä aiheuttaa samalla kustannusten kasvua. [4, s. 6.]

4.2 Riskien hallintakeinot

Rakennusten digitaaliseen turvallisuuteen liittyvien riskien hallintakeinot ovat jaettavissa seuraavasti:

- hallinnolliset keinot
- henkilöstöturvallisuus
- fyysinen turvallisuus
- digitaalinen turvallisuus
- poikkeustilanteiden hallinta
- jatkuvuuden hallinta
- ylläpito. [22, s. 8.]

Hallinnolliset keinot

Digitaalisen turvallisuuden hallinnollisia keinoja ovat esimerkiksi ajantasaiset turvallisuussuunnitelmat ja -menettelyt, vastuuhenkilöiden nimeämiset ja pääsyoikeuksien hallinta [22, s. 8]. Turvallisuussuunnitelmat ja -menettelyt on syytä käydä läpi säännöllisesti, jotta niihin voidaan tarvittaessa tehdä muutoksia eivätkä ne pääse unohtumaan. Vastuuhenkilöt ja heidän vastuualueensa kannattaa nimetä, jotta ei synny epäselvyyksiä asioiden hoidossa. Pääsyoikeuksista on hyvä pitää kirjaa ja ne on tarkistettava kokonaisuudessaan aina, kun niihin tulee muutoksia esimerkiksi oikeuksia lisätessä tai poistaessa. Käyttötapahtumista, kuten kulunvalvonnan käytöstä ja järjestelmiin kirjautumisesta, on jäätävä merkintä lokiin. [22, s. 14–15.]

Henkilöstöturvallisuus

Henkilöstön on tiedettävä digitaaliseen turvallisuuteen liittyvät riskit ja turvallisuuskäytännöt niiden hallintaan. Henkilöstöturvallisuuteen kuuluu henkilöstöön kohdistuvat uhat ja riskit. Ilmoitusprotokolla tietokalasteluun liittyen on oltava henkilöstön tiedossa ja käytössä. [22, s. 9.] Henkilöstöturvallisuuteen voidaan vaikuttaa jo työhönottovaiheessa. Vaikutuskeinoina voidaan käyttää

turvallisuusosuuden lisäämistä työsopimukseen sekä turvallisuuskäytänteiden ja -tentin lisäämistä perehdytykseen. [22, s. 15.]

Fyysinen turvallisuus

Digitaalinen turvallisuus vaatii järjestelmien ja laitteiden fyysisiä suojauskeinoja. Näitä ovat tilojen sekä laitekaappien ja -koteloiden lukitukset ja verkkojen liityntäpisteiden suojaus. Suojauskeinoja ovat myös arkaluontoista tietoa sisältävien dokumenttien fyysinen suojaus, kulunvalvonta, murtohälytykset sekä kaapelointiin kytkeytymisen ilmaisevat järjestelyt [22, s. 9]. Valaistus on myös tärkeässä roolissa fyysisessä turvallisuudessa, jotta mahdolliset vaaratilanteet ja epäilyttävät tilanteet voidaan havaita kameravalvonnan avulla.

Digitaalinen turvallisuus

Niin langallisten kuin langattomienkin verkkojen tiedonsiirtoprotokollat ja salaukset on suunniteltava turvallisuusvaatimusten mukaisesti sallien vain luvallisen tiedonsiirron eri osapuolten välillä. Järjestelmien etäkäyttöratkaisut on suunniteltava huolellisesti ja huoltojen sekä päivitysten on oltava osana käytönaikaista kiinteistön ylläpitoa. Lokitiedot eli aikajärjestyksessä tallennetut tiedot tapahtumista ja niiden aiheuttajista sekä varmuuskopiot säilötään ja käytetään suunnitellusti. [22, s. 9; 22, s. 19.]

Poikkeustilanteiden hallinta

Järjestelmät eivät juurikaan tarvitse hallintatoimenpiteitä, jos ne toimivat suunnitellusti. Tahallinen kybervaikuttaminen, laitevika ja tiedonsiirron tai sähkönsyötön katkos voivat kuitenkin aiheuttaa poikkeustilanteeseen siirtymisen ja senaikaisten menettelyiden ja toimintojen käyttöönoton. Mahdollisimman nopea paluu takaisin normaalitilaan edellyttää suunnitelmallista ja harjoiteltua toimintaa poikkeustilanteessa. Asuinkiinteistössä asukkaita voidaan harjoituttaa poikkeustoimiin, koska ylläpitohenkilöstön resurssit eivät välttämättä riitä laajan kybervaikutuksen aikana. Sähkönjakelun häiriötilanteita varten suunnitellaan katkoton jännitesyöttö kiinteistöä suojaavien toimintojen turvaamiseksi. Erityyppisten

poikkeustilanteiden varalle laaditaan toiminta- ja tiedotusohjeet sekä harjoitusohjelmat. [22, s. 10.]

Jatkuvuuden hallinta

Jatkuvuuden hallintaa on poikkeustilanteesta normaaliin käyttötilanteeseen pääseminen minimoimalla tarvittavat resurssit ja aika. Jatkuvuuden hallinta on tärkeää etenkin vakavammissa poikkeustilanteissa. Näitä tilanteita voivat olla esimerkiksi tahaton häiriö, laitevika, kybervaikuttaminen tai automaation toiminnan estäminen. Osa järjestelmien ohjelmistoista voidaan joutua asentamaan ja käyttöönottamaan uudelleen. Poikkeustilanteita varten on hyvä laatia jatkuvuuden hallintasuunnitelmia ja harjoitella niitä. [22, s. 10.]

Ylläpito

Ylläpito tarkoittaa laitteiden, järjestelmien ja palveluiden toiminnan varmistamista niiden koko elinkaaren ajan. Rakennusten digitaalisen turvallisuuden kohdalla tämä tarkoittaa laitteiden ja järjestelmien toiminnan tarkastamista ja huoltoa säännöllisesti sekä dokumentaation ja pääsyoikeuksien asianmukaista hallintaa ja kirjaamista. Ylläpitoon kuuluvat myös poikkeustilanteiden ja jatkuvuuden hallinnan ohjeistusten tarkastukset sekä toimintamallien harjoittelu. [22, s. 10.]

5 Ohjeet ja standardit

5.1 Rakennustietokortisto

Rakennustietokortisto eli RT-kortisto on suomalaisen Rakennustieto Oy:n omistama tietopalvelu rakentamisen tueksi. Kortisto sisältää ohje-, säännös- ja tuotetietoja suunnitteluun, toteutukseen sekä kunnossapitoon. Koska tiedot ovat kortistoissa luotettavia ja helposti löydettävissä, kuluu tiedon etsintään vähemmän aikaa, ja rakentamisen laatu paranee. Ohjeet on luotu alan suunnittelun ja rakentamisen asiantuntijoiden kanssa. Kortiston käyttö vaatii maksullisen lisenssin. [23.]

RT-kortiston tiedonhakuun on vuoden 2023 lokakuun lopusta lähtien voinut käyttää ChatGPT-tekoälyassistenttia. Rakennustiedon verkkosivuilla [24] kerrotaan, kuinka kortiston käyttäjien haastatteluissa on korostunut kortiston normaalin haun hitaus. Normaalisti tietosisältöä on haettava samanaikaisesti useasta eri tietokortista. ChatGPT-tekoälyassistentti ohjaa käyttäjän oikean RT-ohjekortin luokse assistentille syötetyn tekstin perusteella. Tämä tekee tiedonhausta kustannustehokkaampaa. [24.]

Tässä opinnäytetyössä käytettiin rakennusten digitaalista turvallisuutta käsitteleviä RT-kortteja 103206–103208. Kyseisissä RT-korteissa on käsitelty talotekniikan tieto- ja kyberturvallisuuteen sekä tietosuojaan liittyviä tekijöitä tilaajan, suunnittelijan ja kiinteistön ylläpidon näkökulmasta.

5.2 ST-kortisto ja standardisarja ISO/IEC 27000

Vaikka opinnäytetyö painottuu RT-kortteihin, on olemassa myös muita rakennusten digitaalista turvallisuutta käsitteleviä ohjeita ja standardeja. Standardeissa on yhteisesti sovittuja vaatimuksia, suosituksia tai ominaisuuksia tuotteille ja niiden valmistukselle tai testaukselle sekä järjestelmille tai palveluille [25].

ST-kortisto on Sähkötieto ry:n julkaisema tietolähde sähköisten järjestelmien suunnitteluun, toteutukseen ja ylläpitoon. Kortisto on tarkoitettu sähköisen talotekniikan ammattilaisten käyttöön. Kortisto on kattava ja sisältää ohjeita seuraavista aihealueista:

- järjestelmäteoria
- suunnitteluohjeet
- dokumentointiohjeet
- asennusohjeet
- tarkastus-, testaus- ja käyttöönotto-ohjeet
- järjestelmien käyttö- ja kunnossapito-ohjeet
- järjestelmien kuntoarvio ja -tutkimusohjeet. [26.]

ST-kortti 710.02 käsittelee sähkö- ja taloteknisten järjestelmien tietoturvaa. Kortissa on asiaa esimerkiksi tietoturvasta järjestelmien elinkaaren aikana, tietoturvan vastuista ja sopimuksista ja eri järjestelmien erityispiirteistä tietoturvan kannalta. Kortti sisältää myös sanastoa ja määritelmiä.

Tietoturvallisuudesta on myös standardisarja ISO/IEC 27000, joka tarjoaa organisaatioille apua tietoturvallisuuden riskienhallintaan. Organisaatioilla on omat tietoturvallisuuden hallintajärjestelmänsä, jotka koostuvat erilaisista menettelytavoista, toimintaperiaatteista ja ohjeista. Organisaation tieto-omaisuus voi sisältää esimerkiksi taloudellista tietoa, henkilöstön tietoja tai asiakkaiden tietoja. [27.]

Standardisarja ISO/IEC 27000 sisältää noin viisikymmentä eri standardia. Koko sarjan pohjana toimii kuitenkin sen ensimmäinen standardi ISO/IEC 27001. Tämä päästandardi käsittelee tieto- ja kyberturvallisuutta sekä tietosuojaa. Standardissa esitetään vaatimukset koskien tietoturvan hallintajärjestelmän luomista, ylläpitämistä ja parantamista. Sisältöön kuuluu myös tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset, jotka mukautuvat organisaatioiden tarpeisiin. Vaatimukset ovat luonteeltaan yleisiä ja sopivat siksi kaikentyyppisille organisaatioille. [27.]

6 Tietoturva-auditointi

6.1 Tausta

Opinnäytetyön yritysohjaajan kokemuksen mukaan rakennushankkeissa ei paneuduta tarpeeksi rakennusten digitaaliseen turvallisuuteen. Aiheesta on laadittu RT-kortit, joita hyödynnetään hyvin harvoin rakennushankkeissa. Tämän takia Granlundilla haluttiin lähteä selvittämään, miten rakennusten digitaalisesta turvallisuudesta on huolehdittu asiakkaan kohdekiinteistössä.

Opinnäytetyön yritysohjaajan mukaan Granlundin tavoitteena on toimia johtavana toimijana älykkäiden digitaalisten kiinteistöjen suunnittelijana sekä

palveluntuottajana kiinteistöjen tuottaman datan perusteella. Tietoturva-auditointi toimisi jatkossa osana kyseisiä palveluja. Granlundilla ja heidän asiakkaallaan oli ollut jo aiemmin puhetta asiakkaan kiinteistöjen digitaalisen turvallisuuden hallinnasta. Tämän takia Granlund tarjosi heille sähköisten taloteknisten järjestelmien tietoturva-auditointia asiakkaan nimeämään kohteeseen opinnäytetyönä. Työn tarjouksessa kerrotaan, että auditointi suoritetaan aihetta käsittelevien RT-korttien pohjalta.

Granlundin hyöty työstä on se, että se saa uuden asiakkailleen tarjottavan palvelun itselleen. Opinnäytetyön perusteella ei ole vielä tehty täysin valmista palvelua, mutta työ luo pohjaa tietoturva-auditoinnin mallin luomiselle sekä toimii referenssinä jatkoa ajatellen. Asiakkaan hyöty on se, että se saa referenssikohteen perusteella käsityksen siitä, miten hyvin tietoturvasta on huolehdittu ja missä asioissa tarvitaan toimenpiteitä heidän olemassa olevien ja uusien kiinteistöjen osalta.

6.2 Toteutus

Opinnäytetyön käytännön osuutena toteutettiin tietoturva-auditointi Granlundin asiakasyritykselle. Auditoinnissa selvitettiin kohdekiinteistön digitaalisen turvallisuuden taso aihetta käsittelevien RT-korttien avulla luotua tarkastuspohjaa käyttäen. Auditoinnissa arvioidaan organisaation toimintaa, dokumentaatiota, prosesseja ja järjestelmiä vertaamalla niitä erilaisiin vaatimuksiin eli auditointikriteereihin. Auditointi on riippumaton ja järjestelmällinen prosessi organisaation toiminnan vahvuuksien, poikkeamien sekä parannusmahdollisuuksien tunnistamiseen. [28.]

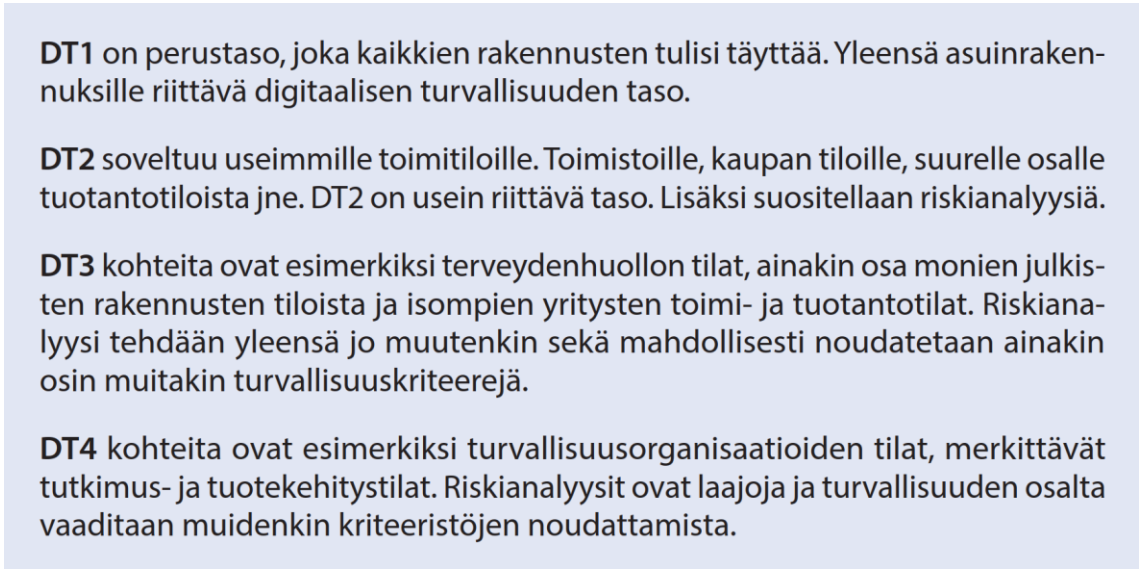
Tutkimuksen lähtöajatuksena oli se, että auditointi suoritettaisiin tekemällä kierros kohdekiinteistöön sen tuntevien henkilöiden avulla. Kierros olisi pitänyt sisällään kiinteistöstä löytyvään dokumentaatioon sekä taloteknisiin tiloihin tutustumista. Tällaista kohdekierrosta oli kuitenkin vaikea saada järjestymään aikatauluhaasteiden vuoksi. Sopivia tahoja lähestyttiin sähköpostitse ja puhelimitse,

mutta lopulta aikataululliset syyt johtivat kohdekierroksen tekemättä jättämiseen.

Muita vaihtoehtoja pohdittaessa tultiin siihen tulokseen, että auditointi toteutetaan haastattelemalla etäyhteyksin kohteen kiinteistöpäällikköä ja digitaalisesta turvallisuudesta vastaavaa henkilöä. Heille molemmille lähetettiin etukäteen auditointia varten luotu tarkastuspohja, jonka mukaan kiinteistön digitaalisen turvallisuuden taso selvitetään osa-alueittain. Heitä pyydettiin myös vastaamaan tarkastuspohjan kohtiin ja perustelemaan omat vastauksensa. Näin tarkastuspohjaa yhdessä läpikäydessä heillä oli jo valmiiksi käsitys siitä, mitä etäpalaveri pitää sisällään. Tutkimuksessa varauduttiin etäpalaverissa käymättä jääneiden tarkastuspohjan kohtien selvittämiseen käymällä kohteessa. Kaikki tarkastuspohjaan kuuluvat kohdat onnistuttiin käymään läpi kokonaisuudessaan, joten tämä osoittautui tarpeettomaksi.

Palaverissa oli läsnä opinnäytetyön tekijä, yritysohjaaja, kohteen kiinteistöpäällikkö ja kohteen digitaalisesta turvallisuudesta vastaava henkilö. Digitaalisesta turvallisuudesta vastaavan henkilön kanssa käytiin läpi vain digitaalista turvallisuutta koskevat asiat, koska sen osa-alueen hän tunsi parhaiten. Kiinteistöpäällikön kanssa käytiin läpi muut tietoturva-auditoinnin osa-alueet. Näitä osa-alueita olivat hallinnolliset keinot, henkilöturvallisuus, fyysinen turvallisuus, poikkeustilanteiden hallinta, jatkuvuuden hallinta ja ylläpito.

Tarkastuspohjassa sekä rakennusten digitaalisen turvallisuuden RT-korteissa rakennuksen digitaalisen turvallisuuden taso on jaettu neljään suojaustasoon (DT1...DT4) (kuva 6). Asiakkaan kohdekiinteistö kuuluu lähtökohtaisesti tasolle kaksi, mutta myös ylemmän kolmannen tason kriteerit kiinteistön osalta käytiin läpi, koska on hyvä pyrkiä vähimmäistasoa parempaan.



Kuva 6. RT-kortin kuva suojaustasoista [4, s. 5].

Liitteen 1 taulukossa on kuvattu digitaalisen turvallisuuden osa-alueittain, miten jokin rakennuksen digitaaliseen turvallisuuteen vaikuttava kriteeri tulisi olla huomioituna digitaalisen turvallisuuden eri tasolla (DT1...DT4). Tulosten käsittelyssä mainituilla kriteereillä tarkoitetaan liitteen 1 mukaisia kriteereitä. Liitteessä 1 on esimerkkinä vain hallinnollisten keinojen kriteerit.

6.3 Tulokset

Palaveri tallennettiin tulosten raportointia varten. Palaverin osallistujat hyväksyivät palaverin tallennuksen, joten sen aikana ei tarvinnut tehdä muistiinpanoja. Tallennusta oli mahdollista tauottaa ja kuunnella sitä useamman kerran, mikä helpotti raportointia ja tulosten käsittelyä. Digitaalista turvallisuutta käsittelevä kappale on ainoa, jonka tiedot eivät ole peräisin kohdekiinteistön kiinteistöpäälliköltä. Kyseisen kappaleen tiedot ovat peräisin kiinteistön digitaalisesta turvallisuudesta vastaavalta henkilöltä.

6.3.1 Hallinnolliset keinot

Hallinnollisten keinojen kriteereistä vain noin puolet toteutuivat. Puutteet koskivat pääosin dokumentaatiota koskevia kriteereitä. Kohteesta on tehty turvallisuussuunnitelma, mutta se ei ota kantaa digitaaliseen turvallisuuteen. Kiinteistöpäällikön mukaan hän luottaa siihen, että palveluntuottajien henkilökunnat ovat tietoisia digitaalisesta turvallisuudesta kiinteistön ylläpidossa. Myöskään digitaalista turvallisuutta koskevia kirjallisia ja hyväksyttyjä turvallisuusmenettelyjä ei ole dokumentoitu.

Asiakkaan kohdekiinteistössä hankkeisiin liittyville asiakirjoille ei tehdä luottamuksellisuusluokittelua. Talotekniikan turvallisuutta ei kohdekiinteistössä tarkasteta tai auditoida siihen vaikuttaneen rakennus- tai muutostyön jälkeen. Kiinteistöpäällikön mukaan käyttäjät ja hankkeiden tekijät ovat samoja vakiintuneita henkilöitä, jotka tietävät ja tuntevat toimintatavat. Taloteknisten muutosten suunnittelussa on viime vuosien aikana ollut sama suunnitteluryhmä, joka on hoitanut hankkeiden suunnittelun, toteutuksen ja loppudokumentaation. Muutostöiden vaikutusta digitaaliseen turvallisuuteen ei ole kuitenkaan arvioitu.

Hankkeiden dokumentaatiot on tallennettu projektipankkiin, jonka käyttöoikeuksista on huolehdittu riittävällä tasolla. Kohteen digitaalisesta turvallisuudesta vastaava henkilö ylläpitää ja valvoo käyttöoikeuksia.

Yhteistyö talotekniikan eri sidosryhmien kanssa on säännöllistä. Huollosta ja ylläpidosta vastaa sama toimija. Kerran kuukaudessa kiinteistöpäälliköllä on paikallisen palvelupäällikön kanssa palaveri, jossa käydään läpi automatiikan toiminta ja etähallintaraportti. Kolmen kuukauden välein tehdään auditointi talotekniikan toimivuudesta huoltoliikkeen kanssa tehdyn sopimuksen mukaisesti.

Kiinteistöpäällikön mukaan kiinteistön vuokralaiset ottavat talotekniikkaan liittyvät riskit omalla tavallaan huomioon. Kiinteistö ei erikseen edellytä riskien huomiointia eikä erillistä riskianalyysiä tuoteta. Vuokralaisten tarpeet kuunnellaan talotekniikkaan vaikuttavien tilamuutosten yhteydessä.

Kiinteistön ylläpidon data säilytetään EU:n (Euroopan unioni) alueella. Datan käsittelyssä noudatetaan tietosuojasta annettuja lakeja ja asetuksia esimerkiksi GDPR:ää (General Data Protection Regulation) eli EU:n yleistä tietosuoja-asetusta. EU:n verkkosivujen mukaan yleisessä tietosuoja-asetuksessa yrityksille ja organisaatioille asetetaan tarkat vaatimukset, jotka koskevat henkilötietojen keräämistä, säilytystä ja hallinnointia [29]. Kiinteistössä yleistä tietosuoja-asetusta on käyty läpi muun muassa kameravalvonnan tuottaman datankin osalta.

Myös seuraavat kriteerit toteutuvat kiinteistöpäällikön mukaan. Talotekniikan riskit, haavoittuvuudet ja suojausratkaisut ovat jatkuvan kehitystarkastelun kohteena. Energiatehokkuutta tarkastellaan ja parannetaan säännöllisesti. Tähän syynä on kiinteistön tavoittelema hiilineutraaliustavoite vuoteen 2030 mennessä. Myös yhteydenpito turvallisuusviranomaisiin on säännöllistä. Pelastustoimeen liittyvät talotekniset järjestelmät käydään vuosittain läpi yleisen palotarkastuksen yhteydessä.

6.3.2 Henkilöturvallisuus

Henkilöturvallisuuden kriteereistä kaikki toteutuivat, mutta eivät täydellisesti. Ensimmäinen puute oli, että tietokalastelun tai muuhun henkilövaikutukseen pyrkivän toiminnan epäilylle tai todistamiselle ei ole tiettyä ilmoituskanavaa ja reagointimenettelyä. Edellä mainitut asiat tulevat huomioon palveluntuottajilta. Kaikki turvallisuuspoikkeamat ja kirjautumisyritykset raportoidaan ja tutkitaan, mutta tiettyä toimintamallia niiden hoitamiseen ei ole kirjattuna. Toinen puute oli, että huoltohenkilöstön turvallisuusselvitysten toteutumisesta jo työhönottovaiheessa ei ole näyttöä. Turvallisuusselvitykset toteutuvat vartiointiliikkeen kanssa, mutta eivät huoltoliikkeen kanssa.

Uuden työntekijän perehdyttämisessä otetaan huomioon turvallisuusasiat. Perehdytykseen on olemassa turvallisuussuunnitelma ja -menettelyt. Turvallisuuskäytännöt ja -menettelyt oikeuksineen ja velvollisuuksineen ovat myös osana työsopimusta. Huoltoliikkeellä on oma prosessinsa asian hoitamiseksi.

Pääsy talotekniikan järjestelmiin ja tiloihin on valvottua. Käyttöoikeuksien hallinta ja valvonta on kunnossa. Käyttö-/pääsyoikeudet saa vain perustellusta syystä ylemmältä taholta. Kiinteistöllä on ohjeet vartiointiliikkeelle fyysisestä pääsynhallinnasta. Jokainen työntekijä hoitaa omat kulkuoikeutensa henkilökohtaisesti kiinteistön kanssa. Kulkuoikeudet voi saada vasta silloin, kun työntekijä on suorittanut turvallisuuspassin hyväksytysti verkossa. Turvallisuuspassi on uusittava kerran vuodessa.

Järjestelmien käyttöä ja tiloissa kulkemista voidaan seurata kirjautumisista ja kulkutunnisteen käytöstä. Järjestelmien etäkäyttöoikeudet rajataan ajallisesti ja niitä valvotaan säännöllisesti. Kameravalvontaa on vain vartiointiliikkeen turvavalvomossa. Muissa teknisissä tiloissa sitä ei ole.

Kiinteistö luottaa siihen, että huoltoliike huolehtii henkilöstönsä aseman ja pääsyoikeuksien tarkistuksista säännöllisesti ja tehtävien vaihtuessa sekä haastatteluista tehtävän päättyessä. Tämä perustuu siis vain luottamukseen, koska kirjallista sopimusta tai dokumenttia asiasta ei ole.

6.3.3 Fyysinen turvallisuus

Fyysisen turvallisuuden osalta kahden ensimmäisen digitaalisen turvallisuuden tason kriteerit toteutuivat yhtä lukuun ottamatta. Kriteerinä oli, että talotekniikan tilat ovat kulunvalvottuja. Kiinteistöpäällikön mukaan noin kymmenen prosenttia ei ole. Esimerkiksi ilmanvaihtokonehuoneet eivät ole kulunvalvottuja, vaan fyysisen lukituksen takana. Myös jotkin parkkihallin tekniset tilat ovat fyysisen lukituksen takana.

Talotekniikan verkkojen fyysisessä suojauksessa on noudatettu rakennusten sisäverkkoja koskevia määräyksiä muun muassa lukituksen osalta. Talotekniikan verkko on oma kiinteistön yleiskaapeloinnista erotettu verkko. Talotekniikan verkkoon pääsy julkisista tiloista on estetty. Siihen pääsee vain lukituista liityntäpisteistä tai langattomasti vain ennalta määritettyjen liityntäpisteiden kautta. Liityntäpisteet ja -kotelot, taloteknisten järjestelmien automaation päätelaitteet

sekä verkkolaitteet sijaitsevat lukituissa ja kulunvalvotuissa tiloissa, joihin on pääsy vain asianomaisilla.

Kolmannella digitaalisen turvallisuuden tasolla kriteereistä osa toteutui osittain ja loput eivät ollenkaan. Talotekniikan fyysisiä haavoittuvuuksia ei ole kohteesta dokumentoitu, eikä mahdollisia haavoittuvuuskohtia ole analysoitu. Sähkökatkokset on kuitenkin huomioitu ja kriittiset laitteet ovat varavirran tai akustojen takana.

Koko kiinteistön kattava murtohälytysjärjestelmä on yöaikaan päällä. Taloteknisten laitteiden, kojeiden ja järjestelmien verkkolaitteet ja keskukset eivät kuitenkaan ole sijoitettu kriteerin mukaisesti murtohälytysjärjestelmään kytketyillä liiketunnistimilla valvottuihin tiloihin.

Automaatiotason kaapelit on suojattu fyysiseltä vaikuttamiselta. Julkisissa tiloissa kaapelit kulkevat alakattojen päällä tai muussa vastaavassa paikassa poissa näkyvistä. Osa kaapeleista on näkyvissä, mutta ne ovat joko korkealla käden ulottumattomissa tai tiloissa, joihin asiattomat eivät pääse sisään.

6.3.4 Digitaalinen turvallisuus

Digitaalisen turvallisuuden puutteet koskivat dokumentaatiota. Digitaalista turvallisuutta, sen hallintaa, ylläpitoa ja varmistusta käsittelevää dokumentaatiota ei ole. Järjestelmäntoimittajien kanssa ei ole tehty sopimusta tietoturvaan liittyvien asioiden dokumentoimisesta. Dokumentteja talotekniikan toteutuksesta, sijaintipiirroksista, laiteluetteloista ja verkkotopologioista ei ole. Verkkotopologialla tarkoitetaan tietokoneverkon rakennetta eli miten verkon laitteet ovat liitoksissa toisiinsa [30]. Muuten digitaalinen turvallisuus oli kunnossa.

Kiinteistön palomuuri suodattaa sisään tulevan liikenteen eli vain tietyillä tunnistettavilla IP-osoitteilla pääsee kirjautumaan sisään kiinteistön verkkoon. Verkkoon pääsee kirjautumaan suojatun VPN-yhteyden avulla eli käyttäjän ja verkon

välinen yhteys on suojattu ja yksityinen. Kiinteistön ja talotekniikan verkoissa käytetään ajantasaisia ja osapuolet autentikoivia protokollia.

Työasemien ja palvelimien virus- ja haittaohjelmatorjunta on määritelty ja dokumentoitu. Uusien tietokoneiden ohjelmistot on päivitetty ja niiden virustorjunta ja lisenssit uusitaan vuosittain. Laitteiden oletussalasanat ja -käyttäjätunnukset on poistettu käytöstä, jolloin niihin murtautuminen vaikeutuu huomattavasti.

Virustorjunnan päivityksen voi hoitaa myös etänä. Etäkäyttäjien (henkilö/yritys) kanssa on erilliset sopimukset, kuinka järjestelmiä kuuluu käyttää. Langattomien verkkojen, niiden päätelaitteiden ja käyttäjien turvallisuusvaatimukset ja -ohjeistukset ovat asianmukaiset. Langattomat verkot ovat toimijakohtaisia virtuaaliverkkoja, joiden keskinäinen liikenne ei ole sallittua. Taloteknisten verkkojen fyysiseen erotukseen ei ole tarvetta, koska looginen erotus on toteutettu virtuaaliverkkojen avulla ja se on kustannustehokkaampaa kuin fyysinen erotus.

Uusia laitteita ja järjestelmiä hankittaessa käytetään luotettavia valmistajia, joiden tietoturvallisuudesta on dokumentoitua näyttöä. Näin toimitaan myös pilvipohjaisten valvomoratkaisujen kanssa. Laitteiden ja järjestelmien valmistajien ohjeita ja suosituksia noudatetaan. Noudattamatta jättäminen umpeuttaisi takuun. Vanhoja laitteita käytettäessä, joiden turvallisuustaso ei vastaa nykypäivää, kiinnitetään erityistä huomiota muun muassa verkon suojaamiseen. Niitä pyritään myös uusimaan mahdollisuuksien mukaan.

Rakennus-, huolto- ja korjausprojektien aikaiset väliaikaisratkaisut digitaalisen turvallisuuden osalta on sovittu etukäteen yhdessä tilaajan ja toimittajan kesken. Projektien dokumentoinnista, aikataulusta ja vastuullisesta henkilöstä on sovittu. Projektien vastaanottotarkastusten yhteydessä suoritetaan toimintakokeet ja tietoturvavaatimusten toteutumisen tarkastukset.

Ajantasaisten konfiguraatiotietojen ja varmuuskopioiden fyysisiä dokumentteja säilytetään turvallisesti muualla kuin kiinteistössä. Jos palomuurin asetuksiin on tehty muutoksia, ne varmuuskopioidaan seuraavana yönä ulkoiseen palveluun.

6.3.5 Poikkeustilanteiden hallinta

Poikkeustilanteiden hallinta on hyvin hoidossa, koska vain kahdessa kriteerissä on puutteita. Talotekniikan hallinta- ja ylläpitohenkilöstöllä ei ole erillistä sovellusta tai ohjelmaa, jonka avulla olisi mahdollista kerrata ja harjoitella poikkeustilanteita varten. He ovat kuitenkin koulutettuja poikkeustilanteisiin, joten he tietävät, kuinka niissä pitää toimia. Ainoa kertaus tapahtuu vuosittain aiemmin luvussa 5.3.2 mainitun verkossa suoritettavan turvallisuuspassin avulla.

Talotekniikan järjestelmistä akustojen takana on vain turvavalaistus ja savunpoisto. Näin ollen koko talotekniikan häiriötön toiminta ei ole varmennettua sähkönjakelun häiriötilanteissa. Menettelyt toiminnan jatkamiseen on kuitenkin määritelty muun muassa sähkökatkon aikana. Sähköjen katkaisu häiriötilanteessa toimimisen varalta on vaikea toteuttaa, koska siitä voi tulla isot tappiot kiinteistön vuokralaisille, kun heidän järjestelmänsä ei ole toiminnassa. Yöllä sähköjen katkaisun voisi toteuttaa, mutta silloin tilanne ei ole sama kuin päiväsaikaan tilojen ollessa käytössä, joten sekään ei ole kannattavaa.

Mahdollisista tietoturvapoikkeamista raportoidaan ohjeiden mukaisesti. Joskus ongelmien etsinnässä tarvitaan ulkopuolista apua, jolloin ulkopuoliselle taholle voidaan antaa oikeuksia määräajaksi. Laajennetut oikeudet kuitenkin palautetaan oikealle tasolle tarpeen päätyttyä.

Poikkeustilanteissa toiminta ja tiedottaminen on suunniteltua ja vastuut on jaettu. Esimerkiksi tulipalon syttyessä kiinteistössä, turvallisuusohjeistuksen mukaan vuokralaistilojen henkilökunta ohjaa asiakkaat ulos kiinteistöstä kokoontumispaikalle. Kiinteistön johdon vastuulla on tiedottaminen.

Ulkoisen palveluntuottajan kautta hoidetaan talotekniikan järjestelmiin liittyvät ongelmat, jotka vaikuttavat kiinteistön normaaliin käyttöön. Talotekniikka on myös osana poikkeustilanteiden hallinnan koulutusta. Huolto- ja vartiointiliikkeen roolit on käyty läpi yhdessä heidän kanssaan.

Poikkeustilanteiden hallintasuunnitelmia harjoitellaan ja muokataan säännöllisten fyysisten harjoitusten perusteella. Kerran vuodessa harjoitellaan kiinteistön evakuointia. Talotekniikan osalta ei harjoitella järjestelmien alasajoja ja uudelleen käyttöönottoja. Kolmen vuoden välein kiinteistössä tehdään muuntamohuollot, jotka aiheuttavat koko kiinteistön kaikkien sähköisten järjestelmien sammumisen samanaikaisesti.

6.3.6 Jatkuvuuden hallinta

Talotekniikasta ja sen päivityksistä sekä lisensointimalleista ei ole jatkuvuuden hallintasuunnitelmaa. Henkilöstölle ei ole erillistä sovellusta tai ohjelmaa, joilla jatkuvuuden hallintaa voisi kerrata ja harjoitella. Varmuuskopioiden ja ajantasaisten konfiguraatiotietojen fyysisen dokumentaation luontia ja palautusta ei testata säännöllisesti. Näitä kriteereitä kiinteistö ei täyttänyt jatkuvuuden hallinnan osalta.

Yksittäisten laitteiden tai osa- ja alijärjestelmien manuaalikäyttö onnistuu huoltotilanteessa. Esimerkiksi rakennusautomaation valvonta-alakeskuksen omalta kosketusnäytöltä voi tehdä ohjauksia ja muutoksia. Alakeskuksen näytöltä voi seurata reaaliaikaisesti järjestelmien toimintaa ja hallinnoida niitä. Rakennuksen digitaalisesta turvallisuudesta vastaavan tahon kanssa on sopimus, jonka mukaan ulkoisten palveluiden saatavuus, jatkuvuus sekä oikeanlainen käyttäjienhallintaprosessi on varmistettu.

Jatkuvuuden hallinnan kannalta kiinteistön dokumentaatio on digitaalisen turvallisuuden kaikilla osa-alueilla hankkeen ja elinkaaren eri vaiheissa laajuudeltaan sekä sisällöltään sopimuksien mukaista ja ajantasaista. Kiinteistön dokumentaatiota päivitetään hankkeen yhteydessä, oli kyseessä sitten talotekniikkaan tai digitaaliseen turvallisuuteen liittyvä hanke.

6.3.7 Ylläpito

Ylläpidon osalta puutteena oli vain fyysisten ja ohjelmallisten komponenttien puolivuosittain tehtävä korvaussuunnitelman ylläpito. Muilta osin ylläpidon kriteerit toteutuivat.

Kunnollisten salasanojen ja henkilökohtaisten käyttäjätunnusten merkitys erityisesti internetpohjaisissa järjestelmissä tai valvomopalveluissa on ymmärretty. Myös tietoturvaohjeistus valvomotietokoneen ja työasemien yleisestä käytöstä on ymmärretty.

Talotekniikkajärjestelmien suunnitelmallinen huolto, esimerkiksi ohjelmien päivitykset, tapahtuvat luotettavan kunnossapitäjän toimesta. Ylläpidossa ulkoisten palvelujen käyttöön tarvittavien pääte- ja tietoliikenneyhteyksien avaaminen ja sulkeminen tapahtuu sovitusti pääkäyttäjän toimesta. Pääkäyttäjänä toimii digitaalisesta turvallisuudesta vastaava ulkopuolinen henkilö.

Taloteknisten laitteiden materiaalivalvonta ja -hallinta on toteutettu. Kiinteistöön hankitaan luotettavia ja järjestelmiin yhteensopivia taloteknisiä laitteita tuttua hankintakanavaa pitkin. Laitteiden käyttöikä on se, mitä elinkaarelle luvataan. Kiinteistössä suositaan laadukkaampaa ja pitkäikäisempää vaihtoehtoa edullisemman ja käyttöiältään lyhyemmän laitteen sijaan.

Kaikki laite- ja ohjelmistopäivitykset perustuvat esimerkiksi teknisen isännöitsijän antamaan valtuutukseen, ja ne dokumentoidaan asianmukaisesti. Kriittisimpien tietoliikennelaitteiden ohjelmistopäivitykset ovat automatisoituja valmistajan suositusten mukaisesti. Kaikki laite- ja ohjelmistopäivitykset sekä konfiguraatiomuutokset ovat jäljitettävissä.

Poikkeustilanteiden sekä jatkuvuuden hallinnan ohjeiden ja menettelyjen (muun muassa tiedottamisen ja harjoittelun) osalta toimitaan niistä tehtyjen sopimusten mukaisesti. Kiinteistöllä on sopimukset palveluntuottajien kanssa. Vartioinnin ja huollon kanssa harjoittelu ja tiedottaminen tapahtuu etukäteen kokeiltuja kanavia pitkin.

Kiinteistön dokumentaatio on digitaalisen turvallisuuden osalta hankkeen ja elinkaaren eri vaiheissa laajuudeltaan ja sisällöltään ylläpidon kannalta sopimuksien mukaista ja ajantasaista. Hankintavaiheessa on sovittu takuuasiat ja ylläpitosopimuksissa on sovittu, miten laitteita ja järjestelmiä huolletaan. Ylläpitosopimusta myös päivitetään laitehankintojen/-vaihtojen ja järjestelmäpäivitysten yhteydessä.

Ylläpitohenkilöstön perehdytykseen sisältyy dokumentoitu tietoturvallisuuden osio. Ylläpitohenkilöstön kanssa on sovittu vasteajat häiriö- ja vikatilanteisiin reagoimiseen ja niiden korjaamiseen. Huollon kanssa on sovittu, että saapuminen kiinteistölle on tapahduttava alle tunnissa, myös kiinteistön ollessa kiinni.

6.4 RT-kortiston hyödynnettävyys tietoturva-auditoinnissa

RT-kortistoa voi hyvin hyödyntää tietoturva-auditoinnin tekemisessä. Kortistossa on selkeästi kerrottu yleistietoa rakennusten digitaalisesta turvallisuudesta, käsitteistä, digitaalisen turvallisuuden riskien hallinnasta ja tietosuojasta. Näiden tietojen avulla saa hyvän yleiskäsityksen aiheesta. Lisäksi kortiston lopussa olevan taulukon avulla voi tehdä tietoturva-auditoinnin.

Vaikka rakennusten digitaalisen turvallisuuden RT-kortistossa on paljon hyvää, siitä on myös negatiivista sanottavaa. Tietoturva-auditointia tehdessä huomasimme kiinteistöpäällikön ja yritysohjaajan kanssa, että koska emme ole alan asiantuntijoita, emme ymmärrä kaikkia tarkastuspohjan kohtia. Kohteen tietoturvallisuudesta vastaava henkilö alan asiantuntijana puolestaan tiesi, mitä tarkastuspohjan kohdat tarkoittavat. Ilman asiantuntijuutta tietoturva-auditointia on vaikea tehdä RT-kortiston avulla.

Mikäli yritys haluaisi tarjota asiakkailleen tietoturva-auditointia, olisi tehtävään hyvä palkata ulkopuolinen asiantuntija tai kouluttaa omasta henkilökunnastaan henkilö rakennusten digitaalisen turvallisuuden asiantuntijaksi. Opinnäytetyössä tehdyn tietoturva-auditoinnin perusteella on tultu siihen tulokseen, että tietoturvatarkastuspohjaa tulisi kehittää auditointia varten sopivammaksi. Hyvän pohjan

saa RT-kortiston avulla, mutta vaikeat kohdat pitäisi tarkentaa ja selittää laajemmin, jotta asiaan perehtymätön ymmärtäisi, mistä on kyse.

7 Yhteenveto

Tämän opinnäytetyön tarkoituksena oli perehtyä rakennusten digitaaliseen turvallisuuteen tekemällä tietoturva-auditointi Granlundin asiakkaan kiinteistöön. Tavoitteena oli luoda Granlundille malli tietoturva-auditointia varten. Työssä käsiteltiin ensin rakennusten digitaalista turvallisuutta teorian avulla ja aiheeseen liittyviä ohjeita ja standardeja. Tämän jälkeen käsiteltiin työssä tehdyn tietoturva-auditoinnin tulokset. Lopuksi pohdittiin rakennusten digitaalista turvallisuutta käsittelevien RT-korttien hyödynnettävyyttä tietoturva-auditoinnin tekemisessä.

Työn haasteena oli saada auditointi järjestymään ensimmäisen suunnitelman mukaisesti eli kohdekierroksen merkeissä. Syynä olivat aikataulutushaasteet. Lopulta auditointi suoritettiin haastattelemalla etäyhteyden välityksellä kohteen kiinteistöpäällikköä ja digitaalisesta turvallisuudesta vastaavaa henkilöä.

Haasteena oli myös RT-korttien pohjalta luodun tarkastuspohjan ymmärtäminen. Osa tarkastuspohjan kriteereistä jäi osittain ymmärtämättä, koska auditointiin osallistuneet henkilöt eivät olleet alan asiantuntijoita. Jatkoa varten tarkastuspohjan hankalasti tulkittavia kriteereitä on selvennettävä ja tarkennettava.

Opinnäytetyöstä opittiin, että tietoturva-auditointipalveluiden tekijöiksi soveltuu paremmin sellaiset henkilöt, joilla on kokemusta rakennusten digitaalisesta turvallisuudesta. Auditoinnin haasteellisuuden vuoksi auditointi tulee tehdä asiantuntijoiden tai asiaan riittävällä tasolla perehtyneiden henkilöiden toimesta.

Tehdyn auditoinnin avulla saatiin luotua kehityskelpoinen ja jalostettavissa oleva palvelumalli Granlundille, joten tavoitteeseen päästiin osittain. Malli ei ole täysin valmis, mutta yhden referenssiauditoinnin perusteella sen kehittämiseen on kerätty tietoa ja kokemusta. Jatkokehitettävää on tarkastuspohjan selkeyden ja ymmärrettävyyden parantamisessa. Myös raportointimallin tekeminen on vielä vaiheessa. Tavoitteena on saada malli lopullisesti valmiiksi ja käyttöön tulevaisuudessa.

Lähteet

1 Mitä on digiturva? Verkkoaineisto. Digi- ja väestötietovirasto. <https://dvv.fi/mita-on-digiturva> Luettu 27.7.2023.

2 Meistä – Granlund. Verkkoaineisto. Granlund Oy. <https://www.granlund.fi/meista/> Luettu 30.3.2024.

3 VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään. 15.11.2022. Verkkoaineisto. Digi- ja väestötietovirasto. <https://dvv.fi/documents/16079645/110183105/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaympäristöön.pdf> Luettu 27.7.2023.

4 RT 103206, Rakennusten digitaalinen turvallisuus, Tilaajan ohje. 25.6.2020. Rakennustieto.

5 Mikä on tietosuojan ja tietoturvan ero? Verkkoaineisto. D-Fence Oy. <https://www.d-fence.fi/tietosuojaa-vai-turvaa/> Luettu 27.7.2023.

6 Kyberturvallisuus: nykyiset ja tulevat uhat. 20.4.2023. Verkkoaineisto. Euroopan parlamentti. <https://www.europarl.europa.eu/news/fi/headlines/society/20220120STO21428/kyberturvallisuus-nykyiset-ja-tulevat-uhat> Luettu 4.8.2023.

7 5 syytä, miksi sinun pitäisi aina päivittää ohjelmistot! Verkkoaineisto. SoftwareLicense4U. <https://softwarelicense4u.com/fi/5-reasons-why-you-should-always-update-software/?wmc-currency=EUR> Luettu 10.8.2023.

8 Onko julkinen Wi-Fi turvallinen? Verkkoaineisto. F-Secure. <https://www.f-secure.com/fi/articles/is-public-wi-fi-safe> Luettu 10.8.2023.

9 Mitä ovat haittaohjelmat? Verkkoaineisto. Microsoft. <https://www.microsoft.com/fi-fi/security/business/security-101/what-is-malware> Luettu 4.8.2023.

10 Tietokoneen suojaaminen kiristysohjelmilta. Verkkoaineisto. Microsoft. <https://support.microsoft.com/fi-fi/windows/tietokoneen-suojaaminen-kiristysohjelmilta-08ed68a7-939f-726c-7e84-a72ba92c01c3> Luettu 4.8.2023.

11 Mitä on käyttäjän manipulointi? Verkkoaineisto. F-Secure. <https://www.f-secure.com/fi/articles/what-is-social-engineering> Luettu 4.8.2023.

12 Salmela, Teemu. 3.10.2022. Datan tietoturvaa – Tunnista haasteet ja riskit. Verkkoaineisto. <https://digia.com/blogi/datan-tietoturvaa-tunnista-haasteet-ja-riskit> Luettu 4.8.2023.

13 Toimintaohje – Palvelunestohyökkäys. Verkkoaineisto. Traficom. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf> Luettu 4.8.2023.

14 Porter, Evan. 2023. Mikä on palvelunestohyökkäys ja miten estät sen vuonna 2023. Verkkoaineisto. SafetyDetectives. <https://fi.safetydetectives.com/blog/mika-on-palvelunestohyokkays/> Luettu 10.8.2023.

15 Enisa threat landscape 2022. October 2022. The European Union Agency for Cybersecurity (ENISA).

16 Mitä on disinformaatio ja misinformaatio? Verkkoaineisto. F-Secure. <https://www.f-secure.com/fi/articles/what-is-disinformation> Luettu 7.8.2023.

17 Logistiikka ja toimitusketju. Verkkoaineisto. Logistiikan maailma. <https://www.logistiikanmaailma.fi/logistiikka/logistiikka-ja-toimitusketju/> Luettu 7.8.2023.

18 Toimintaohje – Toimitusketjuhyökkäys. Verkkoaineisto. Traficom. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toimitusketjuhy%C3%B6kk%C3%A4ysToimintaohje.pdf> Luettu 7.8.2023.

19 Talotekniikkasuunnittelu. Verkkoaineisto. Granlund Oy. <https://www.granlund.fi/palvelut/talotekniikkasuunnittelu/> Luettu 28.7.2023.

20 Teeri, Sauli. 13.3.2019. LVIA-järjestelmät, toimintakokeet ja luovutusvaiheen tarkastukset asuinkerrostaloissa. Theseus-tietokanta.

21 Opinto-ohjaajat. Verkkoaineisto. Lvi-ala tutuksi. <https://lvi-ala.fi/opinto-ohjaajat/> Luettu 3.8.2023.

22 RT 103207, Rakennusten digitaalinen turvallisuus, Suunnittelijan ohje. 25.6.2020. Rakennustieto.

23 RT-kortisto – monipuolisin tietopalvelu rakentamisen tueksi. Verkkoaineisto. Rakennustieto Oy. <https://www.rakennustieto.fi/palvelut/tietoa-rakentamiseen/kortistot/rt-kortisto> Luettu 1.8.2023.

24 Tekoäly uudistaa rakentamisen ammattilaisten keskeisen tietolähteen RT-kortiston käyttöä. 31.10.2023. Verkkoaineisto. Rakennustieto Oy. <https://uutiset.rakennustieto.fi/kortistot/tekoaly-uudistaa-rakentamisen-ammattilaisten-keskeisen-tietolahteen-rt-kortiston-kayttoa/?_gl=1*ykvxqp*_ga*MTUzNjAyNTM3OS4xNzEzMzcyNTEy> Luettu 17.4.2024.

25 Mitä standardi tarkoittaa? Verkkoaineisto. SFS Suomen Standardit ry. < https://sfs.fi/standardeista/mika-on-standardi/> Luettu 29.4.2024.

26 ST-julkaisut. Verkkoaineisto. Sähkötieto ry. < https://www.sahkotieto.fi/st-julkaisut> Luettu 29.4.2024.

27 ISO/IEC 27000 Tietoturvallisuuden standardisarja. Verkkoaineisto. SFS Suomen Standardit ry. < https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/> Luettu 29.4.2024.

28 Mitä on auditointi? 15.9.2023. Verkkoaineisto. Excellence Finland. <https://www.excellencefinland.fi/mita-on-auditointi/> Luettu 6.5.2024.

29 Yleinen tietosuoja-asetus. Verkkoaineisto. Euroopan unioni. <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm> Tarkistettu 6.7.2022. Luettu 6.4.2024.

30 TEPA-termipankki. Verkkoaineisto. Sanastokeskus ry. <https://termipankki.fi/tepa/fi/ryhm%C3%A4/3/haku/verkon%20topologia> Luettu 7.4.2024

RT-ohjekortin taulukko suositelluista toimenpiteistä eri DT-tasoilla

OHJEITA TAULUKON KÄYTTÖÖN
Taulukossa kuvataan digitaalisen turvallisuuden osa-alueittain miten jokin rakennuksen digitaaliseen turvallisuuteen vaikuttava tekijä tulisi olla huomioituna digitaalisen turvallisuuden eri tasolla (DT1...DT4). Jotkin toimista voivat olla epäloogisessa kohdassa, mutta useimmiten tähän on syynsä, esimerkiksi toiston välttäminen toimenpiteen vaikuttaessa useammalla osa-alueella. Kaikkiin kohtiin on otettava kantaa, vaikka ko. tapauksessa ei toimenpiteitä tarvittaisi. Päätös tehdä tai olla tekemättä on siis tehtävä perustellusti. Myös hyväksyttävä toimenpiteen laajuus vaihtelee etenkin DT1-tasolla, koska esimerkiksi pientalossa, rivitalossa ja asuinkerrostalossa tilanteet ovat erilaisia. xlsx -muotoista taulukkoa voi muokata käyttötarkoitukseensa soveltuvaksi lisäämällä tarkennuksia, muistiinpanoja yms. varten soluja ja rivejä sekä ryhmitellä niitä tarpeen mukaan.Useisiin taulukossa esiintyviin suosituksiin löytää tarkempia perusteita tai määrittelyjä itse ohjeesta tai Tilaajan ohjeen liitteestä 2 sekä Suunnittelijan ohjeen liitteestä 2. Suosituksissa on useita kohtia, joissa viitataan suunnitelmiin tms., mutta ei määritetä sen tarkemmin standardia tai muuta esimerkkiä, minkä mukaisesti pitäisi toimia. Tämä on tietoinen päätös ohjetyön tässä vaiheessa. Lähivuosien aikana hyvät käytänteet ja tarkemmat rakennusalan toimintaa ohjaavat ohjeet, kuten useat RYL:it, tehtäväluettelot yms., tulevat määrittämään vaatimukset täyttävät menettelyt. Taulukossa on periaatteena se, että kyseessä olevan asian kohdalla on aina vaatimusten noustessa täytettävä myös alemmat vaatimustasot. Talotekniikalla, talotekn.isillä laitteilla ja järjestelmillä tarkoitetaan kaikkia Talotekniikka-RYL:ssä (TateRYL 2002) ja Sähkönimikkeistössä (S2010) mainittuja laitteita, kojeita ja järjestelmiä ohjelmistoineen.

DT1 Lakien ja määräysten vaatimien lisäksi:	DT1-huomiota	DT2 DT1 lisäksi:	DT2-huomiota	DT3 DT1 ja DT2 lisäksi:	DT3-huomiota	DT4 DT1, DT2 ja DT3 lisäksi:	DT4-huomiota
Käytä salausta.		Käytä xx-salausta.		Käytä zz-yhteyksillä yy-salausta.		Käytä ww- ja zz-yhteyksillä A-luokan salainta.	
HALLINNOLLISET KEINOT							
Kirjallinen ja hyväksytty turvallisuussuunnitelma kattaa myös digitaalisen turvallisuuden.		Hankeasiakirjoille tehdään luottamuksellisuusluokittelu.		Talotekniikka on sisällytetty erikseen mainiten turvallisuuspolitiikkaan ja -käytänteisiin ja se tarkastetaan tai auditoidaan säännöllisesti.		Talotekniikan hallinta on toteutettu turvallisuusvyöhykkeittäin.	
Kirjalliset ja hyväksytyt turvallisuusmenettelyt kattavat myös digitaalisen turvallisuuden.		Kirjallinen ja hyväksytty turvallisuusvyöhykkeisiin perustuva turvallisuussuunnitelmien ohjausdokumentaatio tilaja digitaaliselle turvallisuudelle.		Talotekniikan riskit, haavoittuvuudet ja suojausratkaisut ovat jatkuvan kehitystarkastelun kohteena ja yhteydenpito turvallisuusviranomaisiin ja -teollisuuteen on aktiivista.		Omien laitteiden, siirrettävien muistilaitteiden tai muistia sisältävien siirrettävien laitteiden käyttö on rajoitettu turvallisuusvyöhykkeittäin.	
Talotekniselle järjestelmille on nimetty elinkaaren eri vaiheissa vastuuhenkilö.		Fyysiset pääsyoikeudet eri turvallisuusvyöhykkeille perustuvat rooleihin ja yksilöityyn hyväksyntään.		Talotekn.isten järjestelmien digitaalinen turvallisuus tarkastetaan tai auditoidaan säännöllisesti.		Talotekniikan laitteiden fyysiset suojaukset ja niiden sinetöinnit tarkistetaan säännönmukaisesti, mutta satunnaisina ajankohtina.	
Säännöllinen yhteistyö talotekniikan eri sidosryhmien kanssa.		Talotekniikan digitaalisesta turvallisuudesta vastaava on nimetty.		Suunnitellut muutokset talotekniikaan katselmoidaan arviointiryhmässä ennen toteutusta ja kokouksetdokumentoidaan.			

DT1 Lakien ja määräysten vaatimien lisäksi:	DT1-huomiota	**DT2** DT1 lisäksi:	DT2-huomiota	**DT3** DT1 ja DT2 lisäksi:	DT3-huomiota	**DT4** DT1, DT2 ja DT3 lisäksi:	DT4-huomiota
HALLINNOLLISET KEINOT							
Talotekniikan riskit huomioidaan myös käyttäjien liiketoiminnassa.		Talotekniikan turvallisuus tarkastetaan tai auditoidaan siihen vaikuttaneen rakennus- tai muutostyön jälkeen.					
Talotekniikan riskienhallinnassa huomioidaan myös käyttäjien liiketoiminta.							
Kiinteistönpidon data säilytetään EU:n alueella ja sen käsittelyssä noudatetaan tietosuojasta annettuja lakeja ja asetuksia.							