Digitalisaation vaikutukset turvallisuusjärjestelmäympäristön hallintaan

Juha Viinikka

2022 Laurea

Laurea-ammattikorkeakoulu

Digitalisaation vaikutukset turvallisuusjärjestelmäympäristön hallintaan

Juha Viinikka

Liiketalouden ylempi AMK-tutkinto

Opinnäytetyö

Toukokuu, 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**

Liiketalouden ylempi AMK-tutkinto

Turvallisuusjohtaminen (YAMK)

Juha Viinikka

Digitalisaation vaikutukset turvallisuusjärjestelmäympäristön hallintaan

Vuosi 2022 Sivumäärä 63

Tämän opinnäytetyön tarkoituksena oli selvittää digitalisaation vaikutuksia rakennetun ympäristön turvallisuusjärjestelmien toteutusprosessiin osana kiinteistöjärjestelmäympäristöä. Kehittämistyön tavoitteena oli laatia suosituksia osaamisvaatimuksiksi turvallisuusjärjestelmien tuottajille. Digitalisaation vaikutukset alkoivat näkyä isommissa rakennushankkeissa. Näissä hankkeissa ja projekteissa tuli esiin tarve miettiä turvallisuusteknologiaa ja niihin liittyviä palveluja uudelleen. Hankkeissa tuli vastaan yhä enemmän kysymyksiä ja tarpeita mihin ei ollut vastauksia. Nämä kysymykset liittyivät yleensä järjestelmäympäristön kokonaisarkkitehtuuriin tai integraatioihin sekä tietoverkkoihin ja tietoliikenteeseen. Näissä kysymyksissä palveluntoimittajilla saattoi olla kokemattomuutta tai näkemyseroja erilaisissa myynti ja suunnittelutilanteissa.

Samaan aikaan kiinteistö- ja rakentamisenala (KIRA) kehittää voimakkaasti toimintatapojaan erilaisissa kasvu –ja koulutusohjelmissa. Näissä ohjelmissa turvallisuusratkaisut eivät olleet mukana tai niitä kehitettiin omissa ohjelmissaan. KIRA-alan kehitysohjelmat tulivat tutuiksi kehittämistyön aikana ja sieltä löytyikin turvallisuusratkaisuihin omaa kehitystä digiturvallisen rakentamisen varmistamiseksi. Turvallisuusjärjestelmäympäristön digitalisaation tuomia mahdollisuuksia ei vielä hyödynnetä ja turvallisuusalan kypsyystasoa tässä asiassa piti lähteä selvittämään.

Osaamisvaatimuksia selvitettiin kehittämistyön avulla. Kehittämistyön lähestymistapa on laadullinen toimintatutkimus ja tiedonkeruumenetelmät olivat osallistava havainnointi ja teemahaastattelu. Tässä kehittämistyössä selvitettiin yleisesti turvallisuusjärjestelmäympäristön tilaa ja toteutusprosessia Suomessa ja löytää suosituksia palveluntuottajien osaamisvaatimuksiksi digitalisoituvassa toimintaympäristöissä. Tulokset osoittivat, että digitalisaation myötä aihealueelle syntyy uusia vaatimuksia sekä palveluja ja se edellyttää uutta osaamista. Tässä opinnäytetyössä tunnistettiin selkeitä osaamiseen liittyviä suositeltavia toimenpiteitä. Näiden toimenpiteiden myötä toimialalla olisi parempi kyvykkyys vastata digitalisaation tuomiin haasteisiin sekä ulosmitata tällä hetkellä vielä hyödyntämätön potentiaali.

Kehittämistyölle toivotaan jatkoa esim. miten turvallisuusjärjestelmien data ja analytiikka voisi auttaa energiatehokkuuden parantamisessa.

Asiasanat: johtaminen, digitalisaatio, turvallisuusteknologia, Operational Technology

Laurea University of Applied Sciences **Abstract**

Degree Programme in Security Management

Master of Business Administration

Juha Viinikka

The Influence of Digitalization on the Management of the Security Systems Environment

Year 2022 Pages 63

The main purpose of this thesis was to find out the effects of digitalization on the implementation process of security systems in the built environment as part of the real estate system environment. The aim of this development work was to draw up recommendations on competence requirements for security system producers. The effects of digitalization began to show more and more often in large construction projects. These projects raised the need to rethink security technology and related services in a new way. There were more questions and needs in the projects with no answers. The questions were related to architecture, integrations, as well as IT-networks and telecommunnications connections. In those cases, service providers might had some lack of experience or differences of opinion.

At the same time, the real estate and construction industry (KIRA) is strongly developing their operating methods and practices in various growth and training programs. These programs do not include security solutions or security technology, because usually the security technology industry has its own development programs. These KIRA-industry development programs became familiar during the thessis and there was a development program related to security solutions to ensure digital security constructions. The potential of the digitalization of the security systems has not been exploited yet, and the level of security industry in this case had to be clarified.

Competence requirements were studied through the development project. The approach of this development project was qualitative action research and the data collection methods were participatory observation and thematic interview. This thesis attempts to clarify the status of the security systems environment and implementation process in general in Finland. Also attempt is clarify and found recommendations for the competence requirements of service providers in a digitized operating environment. The results showed that with digitalization, new demands and services are emerging in the subject area and it requires a lot of new skills and qualifications. Clear actions related to development of competences were identified by this study. The industry would have better resilience and capabilities to answer to needs and challenges as well as exploit untapped potential by taking these actions.

The thesis is expected to continue, for examble, how to security systems data and analytics could help to improve conditions and energy effiency in built environment.

Keywords: management, digitalization, security technology, operational technology

Sisällys

1 Johdanto

Laajojen kokonaisuuksien ja pitkien elinkaarten siilomaisissa toimintaympäristöissä tarvitaan uudenlaista johtamista. Kiinteistöjen ja toimitilojen toimintaympäristön monikäyttöisyys, teknologian kehitys sekä nopea digitalisoituminen haastaa uudella tavalla turvallisuuden ja riskienhallinnan menetelmiä turvallisuudenhallinnassa. Kiinteistöjä ohjaa teknologia ja prosessit, jotka ovat juuri tuon muutoksen vaikutuspiirissä. Kiinteistöjärjestelmäympäristö jakaantuu tällä hetkellä toiminnallisesti ainakin kolmen eri toimialan piiriin eli talotekniikka, turvallisuustekniikka ja ICT. Tuo edellä mainittu jako aiheuttaa koko kiinteistön operatiivisen ja teknisen toimintaympäristön pirstaloitumisen ja kokonaisuuden johtaminen on haastavaa. Tämä on tullut vastaan myös riskienarviointityössä, jossa tarkasteltavan aihealueen rajaaminen ja omistajuuksien löytäminen on vaikeaa ja välillä jopa mahdotonta. Aihealue on laaja ja koskettaa koko kiinteistöympäristön suunnittelun, hankinnan, toteuttamisen sekä ylläpidon prosesseja. Se miksi tämä on erittäin kiinnostavaa on se, että hyvin monella toimialalla itse kiinteistö on liiketoiminnan mahdollistaja ja usein kiinteistön häiriönsietokykyä ei oteta huomioon liiketoiminnan jatkuvuudenhallinnassa.

Rakennetun omaisuuden tilaa koskevan Rakennusinsinöörien liiton (RIL) julkaiseman Airaksinen M. johtaman ROTI-hankkeen raportin mukaan rakennusten ja kiinteistöjen arvo on tällä hetkellä n. 500 mrd €. Samaisen raportin mukaan kiinteistöihin kohdistuu n. 9,5 mrd:n korjausvelka vuosina 2016-2025. Seuraavan kymmenen vuoden aikana korjausvelan arvioidaan kasvavan n. 1,1, mrd €. Rakennettu ympäristö digitalisoituu kovaa vauhtia ja se tuo uusia vaatimuksia ja haasteita kiinteistön lukuisille järjestelmille ja niiden ympärille tarjottaville palveluille. (ROTI-2021, 5.) Rakennettu ympäristö saattaa pitää sisällään kymmeniä järjestelmiä ja tuhansia laitteita sekä sensoreita. Jokaisella järjestelmällä on oma tarkoituksensa ja oma tavoitteensa juuri siinä tietyssä käyttötapauksessa. Teknologia kehittyy ja siitä saadut hyödyt lisääntyvät samassa tahdissa. Digitalisaatio kannustaa ottamaan hyödyntämättömän potentiaalin käyttöön.

Kiinteistöjärjestelmäympäristöön eli kiinteistön OT-ympäristöön (OT=Operational Technology) liittyy paljon teknisiä ja toiminnallisia ICT:lle tyypillisiä prosesseja, jotka saattavat olla kriittisiä kiinteistön jatkuvuuden näkökulmasta. Tähän kehittyvään toimintaympäristöön liittyy paljon mahdollisuuksia, mutta myös joukko riskejä. Puhutaan kiinteistöjärjestelmien verkoista, integraatioista, riippuvuuksista ja tietoliikenneyhteyksistä, hankinnan malleista ja muutoshallinnasta. Rakennetussa ympäristössä on paljon erilaisia järjestelmiä, laitteita ja sensoreita, joita on hankittu kiinteistön pitkän elinkaaren aikana. Tässä työssä tätä

kiinteistöjärjestelmäympäristöä kutsutaan OT-ympäristöksi ja järjestelmiä OT-järjestelmiksi. Turvallisuusjärjestelmät ovat osa OT-järjestelmiä.

OT-järjestelmillä tarkoitetaan kaikkia niitä järjestelmiä, laitteita ja ratkaisuja sekä prosesseja ja palveluita, joilla ohjataan rakennettua ympäristöä toimimaan sen määritellyn käyttötarkoituksen mukaisesti. OT-ympäristöön kytketään tyypillisesti valtava määrä erilaisia IoT-laitteita. OT-järjestelmät pitävät prosessit käynnissä viikon jokaisena päivänä, mikäli niistä pidetään huolta tarpeenmukaisesti. Digitalisaatio koskettaa vahvasti myös tuvallisuuspalveluja ja -ratkaisuja. Turvallisuusjärjestelmien toimittajilta vaaditaan yhä laajempaa näkemystä ja osaamista käyttäjän tarpeista sekä syvää osaamista digitalisaation vaikutuksista ja riippuvuuksista turvallisuuden toimintakentässä. Prosesseissa ja palveluissa on paljon omistajuuksiin, vastuisiin ja arkkitehtuuriin liittyviä kysymyksiä, joihin tarvitaan vastauksia. Tärkeää on tuntea toimintaympäristöön vaikuttavat tekijät. Yksi tapa lähestyä asiaa on turvallisuusjohtamisen kautta, sillä kyse on riskienhallinasta. Airaksisen johtaman ROTI-hankkeen raportin mukaan Suomen kiinteistökanta on vanhaa ja siellä olevien järjestelmien ylläpito on puutteellista tai niitä korjataan vain vikaantuessa. (ROTI, 2021, 5.) Turvallisuusteknologian ja siihen liittyvien prosessien tarkoituksena on varmistaa liiketoiminnan jatkuvuutta ja turvata vakavien vahinkojen aiheuttamia liiketoiminnan menetyksiä sekä mahdollistaa turvallinen toimintaympäristö normaalissa arjessa.

Rakennettu ympäristö koostuu monista erilaisista laitteista, etäohjattavista järjestelmistä ja niihin liittyvistä tietoliikenneratkaisuista. Tämä kehittämistyö on rajattu työelämän kehittämishankkeeksi, jossa keskitytään rakennetun ympäristön turvallisuusteknologioihin ja niihin liittyviin palveluihin palveluntoimittajien osaamisvaatimusten näkökulmasta. Tiedolla johtamisen tavoitteet ja innovaatiot ovat tuoneet paljon kerroksia ja riippuvuuksia järjestelmien välille ja niiden sisään. Tämä lisää merkittävästi rakennetun teknisen toimintaympäristön kompleksisuutta. Suunnittelu, hankinta, toteutus sekä käytönaika tapahtuu voimakkaissa siiloissa ja niissä toimiminen on haastavaa. Systemaattista poikkitieteellistä yhtenäistä mallia ei ole koko OT-ympäristöön ole.

Teknologia kehittyy nopeasti ja niiden ympärillä olevat palvelut sekä prosessit myös. Kiinteistö- ja turvallisuusalalla ei ole käytössä digitalisaation näkökulmasta yhteisiä sellaisia standardeja tai vakioituja toimintamalleja, joiden varaan voisi digimurrosta rakentaa. Olen omassa työssäni päässyt tutustumaan monia vuosia järjestelmähankinnan toimitusketjuihin aina suunnittelusta käytönajan jatkuviin palveluihin asti.

Eräässä rakennushankkeessa jouduttiin miettimään asioita ihan uudella tavalla, koska palvelut ja ratkaisut olivat uusia ja niiden saatavuus oli vielä hyvin rajattua. Yhtenä merkittävänä havaintona hankkeissa nousi esiin hyvin vahvat siilot. Oli selkeästi nähtävillä hankkeen eri osa-alueille muodostuva osa-optimointi, jossa sinänsä ei ole mitään väärää. Jos osaoptimointi

johtaa siihen, että kokonaisuus kärsii, niin yhteinen tavoite saattaa kadota. Digitalisaatio tuo myös riskejä, mitkä liittyvät rajapintoihin, vastuusiirtoihin, omistajuuksiin ja muihin ratkaisuihin, mitkä taas vaikuttavat asioiden hallittavuuteen. Tämä oivallus kollegani kanssa sai aikaan tarpeen ryhtyä selvittämään asiaa tarkemmin. Asian tarkemman pohdinnan ja syvällisemmän sidosryhmäyhteistyön johdosta aihealueelta löytyi paljon mahdollisten riskien lisäksi myös hyödyntämätöntä potentiaalia, uusia liiketoimintamahdollisuuksia ja mahdollisia ansaintalogiikan muutospaineita.

1.1 Opinnäytetyön tavoite

Tämän opinnäytetyön tavoitteena on laatia suosituksia osaamisvaatimuksiksi turvallisuusjärjestelmien tuottajille. Tarkastelussa otetaan huomioon vastuulliset ja kustannustehokkaat toimintamallit järjestelmien elinkaaren aikana. Vaatimukset, lainsäädäntö ja valvonta oikeassa suhteessa on hyvä raami, jolla rakennetaan kivijalkaa tälle aihealueelle. Näkökulmana on tarkastella edellä olevia asioita erityisesti jatkuvuuden näkökulmasta. Työ pyrkii vastaamaan mm. seuraaviin tutkimuskysymyksiin. Miten digitalisaatio vaikuttaa turvallisuusjärjestelmäympäristöön tulevaisuudessa? Miten turvallisuusjärjestelmät ja niihin liittyvät palvelut tulevat kehittymään tulevaisuudessa? Minkälaisiin haasteisiin turvallisuusjärjestelmien tuottajien pitää osaamisessaan ja resursoinnissaan varautua kokonaisarkkitehtuurin näkökulmasta?

Tässä opinnäytetyössä keskitytään rakennetun ympäristön turvallisuusteknologiaan, niihin liittyviin palveluihin ja prosesseihin. Työ selvittää miten digitalisaatio vaikuttaa näiden asioiden kehitykseen ja toimintavarmuuteen sekä miten voidaan osaamisen kautta koko turvallisuusjärjestelmäympäristön hallintaa parantaa. On myös tunnistettu tarve kirkastaa näkemystä miten näihin haasteisiin voidaan vastata siten, että järjestelmien käytettävyys ja turvallisuus on varmistettu. Turvallisuusteknologia on liiketoiminnan jatkuvuuden näkökulmasta keskeinen osa OT-ympäristöä, niiden tekniset rajapinnat usein kohtaavat. Kiinteistö- ja rakentamisala (KIRA) on vahvasti pirstaloitunut ja hankintaa tehdään paljon siiloissa. Urakkamuodosta ja hankintavastuista riippuen, järjestelmiä hankitaan osakokonaisuuksina ja niiden välisistä integraatioista ja riippuvuuksista kokonaisuuden näkökulmasta ei välttämättä vastaa kukaan. Turvallisuusjärjestelmät ovat yleensä osana toimitilaturvallisuuden keinovalikoimaa ja riippuvuuksia tarkasteltaessa siinä harvoin ovat mukana muut kiinteistön järjestelmät.

Kehittämistyön tuotoksena syntyy käsitys siitä, miten rakennettu ympäristö järjestelmineen muuttuu digitalisaation myötä ja löytää suosituksia osaamisvaatimuksiksi turvallisuusjärjestelmiä tuottaville yrityksille.

1.2 Opinnäytetyön rakenne

Opinnäytetyön rakenne on jaettu kuuteen lukuun. Ensimmäinen luku on johdanto, jossa kuvataan aihealue lyhyesti ja työelämähankkeen taustat. Johdannossa kerrotaan mistä löytyi idea ja tarve tälle työlle sekä miten selvitystyö käynnistyi. Johdannossa perustellaan myös aihealueen laajuus, tarpeellisuus ja hyödynnettävyys sekä yrityksen näkökulmasta, että koko toimialalla.

Opinnäytetyön toisessa luvussa kerrotaan koko aihealueen toimintaympäristön kuvaus. Kuvataan toimintaympäristön rajaukseen liittyviä haasteita sekä millaisilla tutkimusmenetelmillä asiaa ratkaistiin ja ongelmaa selvitettiin. Tämä ei ollut tyypillinen tutkimus vaan työelämähanke, jossa isossa roolissa oli konkreettiset opit suoraan hankkeesta sekä sen johdosta käynnistetyistä toimenpiteistä eri verkostoissa. Toimenpiteet eri verkostoissa sisälsivät kolme eri kokonaisuutta, hankkeissa havainnointi, hankkeen analysointi ja kenttäkokemukset.

Kolmannessa luvussa käsitellään aihealueen teoreettista viitekehystä. Neljännessä luvussa kuvataan kehittämistyön eri vaiheet, tiedonkeruu- ja tutkimusmenetelmät perusteluineen. Viidennessä luvussa käsitellään kokonaiskuva tuloksista ja kuudennessa luvussa käydään läpi tulosten yhteenveto ja pohdinta.

1.3 Perustelut aihevalinnalle

Tässä kehittämistyössä yksi ohjaava tekijä oli se, että työ voidaan luokitella julkiseksi työksi ja sillä voi vaikuttaa positiivisesti kiinteistö-, rakentamisen- ja turvallisuusalan kehitykseen. Rajauksen pitää olla sellainen, että sitä ei tarvitse miltään osin salata. Se oli lähtökohta aiheen ja sisällön vaatimusten osalta. On myös merkityksellistä, että aihealueesta löytyisi jatkoa tutkimukselle aina väitöskirjaan saakka. Aihe ja sen vaikutuspiiri on niin laaja, että saattaa löytyä useitakin uusia opinnäytetyön aiheita. On myös hyvä tarkentaa, että tämä työ kirjoitetaan turvallisuusjärjestelmäympäristöä tunteville ja rakennetun ympäristön parissa työskenteleville asiantuntijoille.

Olen ollut tietoinen järjestelmien suunnitteluun ja hankintaan liittyvistä haasteista jo pitkään, mutta aihealueen laajuuden ja ongelmallisuuden oivalsin, kun pääsin osallistumaan erääseen isoon rakennushankkeeseen. Kyseisen rakennushankkeen tavoitteena oli rakentaa uusilla innovatiivisilla teknologioilla ja älykkäillä aikaa kestävillä ratkaisuilla moderni toimiva käyttäjille tarpeenmukainen kiinteistö. Siinä pääsin osallistumaan ja vastaamaan kohteen turvallisuusratkaisuista yhdessä poikkitieteellisen projektiryhmän kanssa. Tässä nopeasti digitalisoituvassa kiinteistöalan ja rakentamisen ympäristössä on haastavaa nähdä pitkälle kun teknologia kehittyy nopeasti.

Rakennetussa ympäristössä voi olla kymmeniä järjestelmiä, joiden suunnittelu, hankinta ja tapahtuu siiloissa. Järjestelmien elinkaaret ovat pitkiä, jopa 15 vuodesta 30 vuoteen, mutta esim. järjestelmien ohjelmistojen ylläpito vaatii jatkuvaa huolenpitoa. Kiinteistöjen tekninen infra mahdollistaa uusien digitaalisten palvelujen käytön tai pahimmillaan estää sen. Vanhaa kiinteistökantaa on Suomessa todella paljon ja niiden korjausvelka vastaamaan digitalisaation tuomiin vaatimuksiin on valtava. Teknologia on kehittynyt todella nopeasti viimeisten vuosien aikana ja palvelut sen mukana. Hyvä kysymys on, löytyykö palvelutarjonnassa oikeita palveluja ja onko osaaminen riittävää ja kohtaako tilaajan ja toimittajan tavoitteet.

1.4 Kehittämistyön taustaa

Olen seurannut oman pitkän turvallisuusalan työtyöhistoriani aikana turvallisuuspalveluiden ja -ratkaisujen myyntiin tai ostamiseen liittyvää kehitystä. Lähes aina mukana vastuukentässäni ovat olleet toimitila- ja kiinteistöturvallisuusasiat. Olen tarkastellut asiaa riskienhallinnan, turvallisuuden ja jatkuvuuden näkökulmasta. Kaikkiin edellä oleviin prosesseihin liittyy vahvasti johtamisen erilaiset mallit. Usein johtaminen joko mahdollistaa tai estää kehityksen. Näin olen päässyt seuraamaan myös laajemmin turvallisuusalan kehitystä kiinteistöympäristössä eri rooleissa ja pitkällä aikavälillä. Lisäksi olen toiminut 2000 luvun alusta lukien turvallisuusjärjestelmien suunnittelun ja hankinnan kanssa ja kokemukseni mukaan turvallisuussuunnittelu ja niihin liittyvät palvelut ovat olleet vahvasti erillishankintaa erillään muusta kiinteistötekniikasta ja rakentamisesta.

Turvallisuusratkaisut ja palvelut ovat näyttäytyneet tilaajalle aina 2000 luvun alusta asti erittäin konservatiivisesti ja teknologiakeskeisesti. Pitkän kokemukseni mukaan kaikki on lähtenyt siilomaisesta ajattelusta ihan suunnittelusta asti. Kiinteistöjärjestelmähankinnassa perinteisesti jokainen suunnitteluala on rajannut monestakin eri syystä oman suunnittelunsa tarkasti huomioimatta laajasti suunnittelualojen integraatioita ja riippuvuuksia. Tällaiseen toimintamalliin on ollut omat syynsä esim. kulloisenkin ajan tapa toimia tai budjetointimalli. Voidaan todeta, että jokaisella aikakaudella ovat olleet omat toimintamallinsa sen ajan parhaan tietämyksen mukaan, mutta viimeisten vuosien aikana teknologian kehitys on ollut todella nopeaa.

Kiinteistöjärjestelmäympäristöön liittyvät prosessit ovat syntyneet vuosien tai jopa vuosikymmenien aikana erilaisissa siiloissa vakiintuneilla rakentamisen, hankinnan ja ylläpidon toimintamalleilla. Tämä toimintaympäristö on ikään kuin varkain digitalisoitunut ja digitaalisten palveluiden nopea kehitys edellyttää poikkitieteellistä saumatonta yhteistyötä eri siilojen välillä. Kiinteistön järjestelmien välillä syntyy toiminnallisia integraatioita tai riippuvuuksia, joiden ymmärtäminen kokonaisuuden näkökulmasta on välttämätöntä. On tunnettava kokonaisuus, jotta ympäristön digitalisoitumisen tarjoamat edut suunnittelussa, hankinnassa, rakentamisessa ja ylläpidossa voidaan hyödyntää ja toisaalta toimintaympäristön riskit hallita.

Idea tähän opinnäytetyöhön syntyi käytännössä jo vuosia sitten, mutta nyt se konkretisoitui jo edellä mainitussa hankkeessa, jossa kiinteistön järjestelmiin liittyen tavoitteena oli löytää innovatiivisia, pitkäaikaisia ja kestäviä ratkaisuja. Kaiken keskiössä olivat ”älykkäät ratkaisut”. Uutta oli, että hankkeessa oli järjestelmäympäristön kokonaisarkkitehtuurista vastaava asiantuntija, joka auttoi ajattelemaan asiaa kokonaisuuden kannalta. Omalla vastuullani oli turvallisuusjärjestelmät ja -ratkaisut. Ryhdyimme yhdessä arkkitehtuurista vastaavan asiantuntijan kanssa pohtimaan asiaa laajemmalla kulmalla huomioiden koko rakennetun ympäristön ratkaisut ja palvelut. Muutaman kuukauden sisällä olimme vakuuttuneita siitä, että rakennetun ympäristön järjestelmiin liittyvät prosessit vaativat uudistamista ja koko ala vaikutti olevan jonkinasteisen rakenteellisen murroksen vaiheessa. Tunnistimme monta kehitettävää asiaa ja kokonaisuutta, joita lähdimme systemaattisesti edistämään eri sidostyhmien kanssa verkostoissa. Haasteen suuruus ja monikerroksisuus selvisi vähitellen ja sen johdosta aihealuetta ryhdyttiin systemaattisemmin tarkastelemaan. Aluksi tuntui olevan vaikeaa jäsentää toimintaympäristöä uudella tavalla eri verkostoille ymmärrettävästi. Oli myös vaikeaa löytää oikeaa osaamista hankkeen ja käytön aikana tunnistettuihin tarpeisiin. Toimiala ja toimijat näkivät asiat edelleen siilomaisesti ja muutosten läpivienti tai ylipäätään näkemys muutoksen tarpeellisuudesta aiheutti paljon kysymyksiä.

Muutama kuukausi, paljon palavereja, monia hankkeita, vahvaa verkostoitumista, jonka jälkeen ajatus vahvistui, että haasteet liittyvät koko toimialan tapaan tehdä asioita. Toimialalla tarkoitetaan tässä työssä rakennus-, kiinteistö- ja ylläpidon alaa, KIRA-alaa ml. turvallisuusjärjestelmäympäristö. KIRA-alan tapa toimia on ollut hyvin siilomainen ja perinteinen erityisesti suunnittelun ja hankinnan näkökulmasta. Hankinnan yhteydessä hyvin harvoin huomioidaan käytönajan tarpeet, joka vaikeuttaa järjestelmien kustannustehokasta potentiaalin ulosmittaamista kiinteistön omistajan tai käyttäjän tarpeisiin. Järjestelmien suunnittelu, hankinta ja käyttöönotto ovat pitkiä toimitusketjuja ja noista toimitusketjusta löytyi valtava kokonaisuus haltuun otettavaksi seuraavien vuosien ja jopa vuosikymmenten aikana.

KIRA-ala on jo tunnistanut aihealueeseen liittyviä kehitystarpeita ja ala on käynnistänyt kasvuohjelman kirittämään rakennusalaa rakentamaan vähäpäästöisesti ja kustannustehokkaasti. Vähähiilisyystavoitteiden lisäksi painopistealueena on työmaatehokkuuden parantaminen ja digitalisuuden hyödyntäminen saaden uusista teknologioista myös paras potentiaali irti. (Airaksinen, M. 2021.) Tämän opinnäytetyön aiheena olevat turvallisuusteknologiat ja niihin liittyvät prosessit sekä palvelut eivät ole sellaisenaan näissä kasvuohjelmissa mukana. On tärkeää, kiinteistöjärjestelmäympäristöä kehitetään kokonaisuutena, etenkin digitalisaation näkökulmasta.

Digitalisaatio, integraatiot ja riippuvuudet ovat olleet jo pitkään puheenaihe etenkin teollisuudessa. Nyt tässä ajassa tuo käsitteistö on vallannut palstatilaa myös rakentamisen ja kiinteistöjärjestelmien ympärillä. Paljon on puhetta ja kirjoituksia sellaisista käsitteistä kuin

tekoäly, Smart Building, analytiikka, kyberturvallisuus, käyttöturvallisuus, tiedolla johtaminen jne. Nämä kaikki edellä mainitut käsitteet ovat mukana digitalisaation ympärillä olevissa keskusteluissa. Digitalisaatio tuo esim. palveluita meille kaikille käyttöön laajemmin ja nopeammin. Vaikutukset ovat näkyneet talouden prosesseissa jo pitkään, mutta olemme kuitenkin digitalisaatiossa rakennetun ympäristön järjestelmissä vasta alkuvaiheessa. Huolimatta ajanjakson lyhyydestä, digitalisaatio on nopeasti johtanut syvälliseen murrokseen ja kehitys jatkuu edelleen voimakkaana. Digitalisaatio ja internet-talouden hyödyntäminen ovat keskeisiä tekijöitä palveluiden skaalautuvuuden ja vietävyyden sekä jalostusarvon ja tuottavuuden kasvattamisessa. (Työ – ja elinkeinoministeriön julkaisu 2021, 9, 21.) Digitalisaatio on mm. sitä, että tekoälyä hyödynnetään jo monissa laitteissa ja järjestelmissä ja järjestelmien dataa voidaan hyödyntää paremmin liiketoiminnassa eri käyttötarkoituksiin. Tekoälyjärjestelmät ja erilaiset muut digitaaliset järjestelmät ovat jo osa suurimmalle osalle meistä arkielämää. Digitaaliset järjestelmät tuovat arkeen hyviä asioita toimiessaan, mutta ne vaativat jatkuvaa huolenpitoa. Ne yleensä parantavat toimintojen turvallisuutta ja sitä kautta sujuvuutta ihmisten arkeen. On myös mahdollista, että ne saattavat synnyttää uudenlaisia riskejä, joihin joudumme varautumaan. Palveluntoimittajien on selvitettävä palveluidensa käyttäjille, mihin tehtäviin ja kuinka digitaalisuuteen perustuvia älykkäitä laitteita ja ohjelmistoja hyödynnetään. Yhteisenä toiveena ja tavoitteena on käyttää uutta teknologiaa parantamaan palveluita toiminnasta kerättävää dataa hyödyntämällä. (Hallamaa, Hakkarainen & Kalliokoski 2021, 11-12.)

Muutaman vuoden käytännön kokemuksen mukaan turvallisuusjärjestelmiin liittyvien investointien painotus on vahvasti siirtymässä järjestelmien omistamisesta elinkaaripalveluihin. Turvallisuusratkaisut ja niiden elinkaaripalvelut sisältävät yhä enemmän ohjelmistoja, analytiikkaa, tietoturvaa, pääkäyttöpalveluja sekä käyttäjäoikeuksien hallintaa. Niihin liittyvät elinkaaren prosessit ovat osittain uutta turvallisuusjärjestelmäympäristössä, mutta ICT-alalle tyypillisiä palveluja. Hankkeissa turvallisuusjärjestelmien suunnittelijoille ja tuottajille esitetyt kysymykset esim. tietoturvasta, elinkaaripalveluista, riippuvuuksista ja arkkitehtuurista ovat olleet usein vieraita tai niitä ei ole tuotteistettu. Esim. järjestelmien arkkitehtuurikuvaukset pääosin puuttuvat toteutuskuvista kokonaan. Juuri tästä syystä on tarpeellista lähteä selvittämään minkälaisia tarpeita käyttäjillä on ja minkälaisiin tarpeisin palveluntoimittajien tulisi vastata tässä digitalisaation murroksessa.

2 Toimintaympäristön kuvaus

Rakennetussa ympäristössä on ensisijaisesti varmistettava koko järjestelmäympäristön ja siellä työskentelevien turvallisuus. Pääsääntöisesti järjestelmätoimittajilla on tavoitteena löytää ja toteuttaa älykkäitä aikaa kestäviä ratkaisuja useiden vuosien ajalle. Yksittäisiä kohdekohtaisia älykkäitä kustannustehokkaita turvallisuusratkaisuja voidaan jo toteuttaa, mutta

kun ratkaisuiden ja niihin liittyvien palveluiden tulisi olla skaalautuvia ja hallittuja sekä vielä turvallisia, niin asioiden hallinta monimutkaistuu ja osaajien määrä vähenee.

Nopea rakennetun ympäristön digitalisoituminen on tuonut uudistamistavoitteisiin vauhtia. Viimeiset vuodet kiinteistöjen teknisten palveluiden digitalisoitumisen myötä, tarve parempaan järjestelmien elinkaarenhallintaan on kasvanut. On myös tunnistettu digitalisaation vaikutukset kustannuksiin ja riskeihin. Konkreettiset toimet vielä laajasti puuttuvat ja on tarpeen synnyttämisen vaihe. Turvallisuusjärjestelmät ovat hyvä esimerkki jo olemassa olevan potentiaalin hyödyntämättömyydestä. Turvallisuusteknologiaa pystyisi hyödyntämään olosuhdetiedon keräämisessä ja ylläpidon järjestelmien tukena ylläpidon ohjauksessa jo paljon laajemmin nykyiseen verrattuna. Kiinteistöissä on koko ajan enemmän erilaisia järjestelmiä ja laitteita, jotka ovat yhteydessä internettiin ja etävalvomoihin jonkun yhteyden avulla. Etäkäyttöä hyödynnetään kyllä, mutta esim. turvallisuusjärjestelmien osalta tarjonnan perusteella hyödynnetään pääosin perinteisessä turvallisuusvalvonnassa tila- ja valvontatietojen vastaanottamiseen sekä kuvavalvonnassa. Suomessa on erittäin vanhaa kiinteistökantaa teknisen infran näkökulmasta. Se luonnollisesti haittaa digitalisaation hyödyntämistä laajamittaisesti nopealla aikataululla. (ROTI 2021, 5.) Yksittäisiä kohdekohtaisia älykkäitä ratkaisuja kyllä on, mutta niillä on usein tapana jäädä paikallisiksi ja projekteiksi.

Kiinteistössä käytettäviä turvallisuusjärjestelmät luokitellaan SESKO ry:n mukaan sähköjärjestelmiksi. SESKO ry on Suomen sähköteknisen alan standardointijärjestö. SESKO osallistuu alansa kansainväliseen (IEC) ja eurooppalaiseen (CENELEC) yhteistyöhön Suomen edustajana ja saattaa tämän työn tuloksen kansallisiksi SFS-standardeiksi. (SESKO ry, 2022).

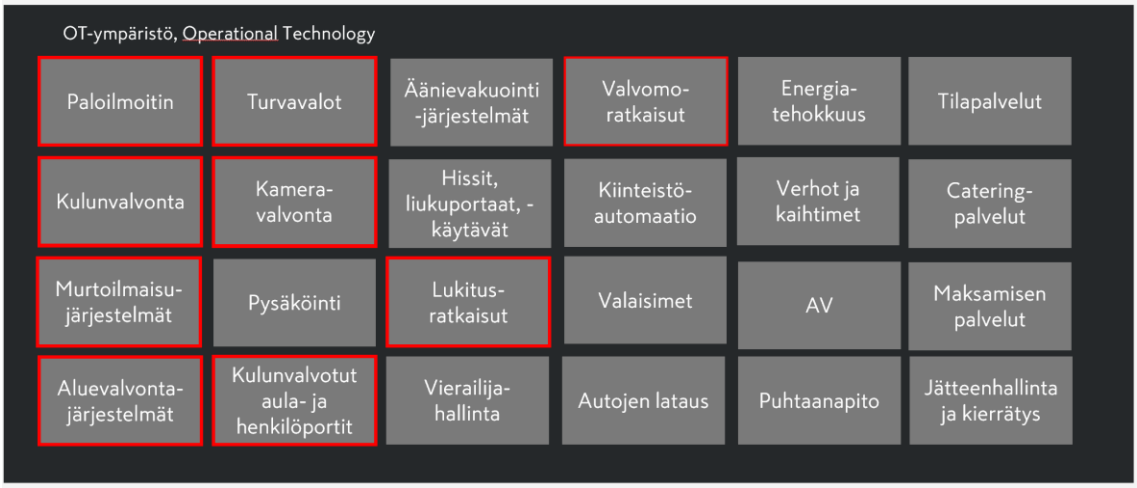
Toimitilaturvallisuus ja siihen liitetyt sähköiset turvallisuusjärjestelmät ovat oleellinen osa yrityksen kokonaisturvallisuutta. Turvallisuusteknologia on kehittynyt nopeasti viimeisten vuosien aikana ja yhdessä muun talotekniikan järjestelmien kanssa muodostavat kiinteistön älykkään ytimen. Turvallisuusteknologia liitetään usein mainospuheissa osaksi rakennetun ympäristön isoa teknistä kokonaisuutta vaikka, hyvin harvoin niitä suunnitellaan toimimaan saumattomasti keskenään huomioiden kaikkien suunnittelualojen tekniset ja toiminnalliset yhteiset tavoitteet.

Toimintaympäristön määrittäminen ja rajaaminen on ensiarvoisen tärkeää näin laajassa kokonaisuudessa, jota hallitsee vertikaaliset ja horisontaaliset prosessit sekä johtamismallit. Johtajan tehtäviin kuuluu näyttää yritykselle ja henkilöstölle suuntaa. Johtajien tärkeimpiin tehtäviin kuuluu arvioida yrityksen menestymisen mahdollisuuksia markkinoilla, jotka yleensä muuttuvat koko ajan. Toimintaympäristöä pitää säännöllisesti arvioida liiketoiminnan mahdollisuuksien näkökulmasta. Arviointiin voi käyttää monia hyödyllisiä työkaluja, kuten SWOT-analyysi, PESTE-analyysi sekä Porterin malli. Noista kolmesta parhaiten OT-toimintaympäristön analysointiin tuntuisi soveltuvan analysointimalli PESTE/-L, jonka nimilyhennekin viittaa

analysoinnin kohteisiin: poliittiseen (Political), taloudelliseen (Economical), sosiaaliseen (Social), tekniseen (Technical) ja juridiseen (Law). (Jylhä & Viitala, 2019, 75-77.)

Rakennetun ympäristöön järjestelmistä voidaan käyttää nimitystä OT-järjestelmät. Tässä yhteydessä OT-järjestelmistä puhuttaessa OT pitää sisällään myös palvelut ja prosessit. OT aihealueena on varsin uusi rakennetussa ympäristössä ja tutumpi teollisuudesta tuotannon turvaajana. Rakennetussa ympäristössä OT:lla tarkoitetaan kiinteistöä ylläpitäviä, tukevia ja ohjaavia järjestelmiä.

OT on kaikkia niitä järjestelmiä, laitteita ja ratkaisuja sekä prosesseja että palveluita, joilla ohjataan rakennettua ympäristöä toimimaan sen määritellyn käyttötarkoituksen mukaisesti. Amerikkalaisen rakennusalan ammattijärjestö ASCE:n julkaisun mukaan rakennusalan digitalisaatio ja digitaalinen muutos vaikuttaa tiedonvaihtoon ja saattaa jopa vaikeuttaa rakennustyömaiden toimintaa. OT-järjestelmien kautta ohjataan koneiden ja laitteiden toimintaa ja säädellään ohjelmistojen avulla joiden päivityksistä ja muutoshallinnasta täytyy huolehtia. (ASCE 2021.) Turvallisuusjärjestelmien potentiaali on vielä paljolti ulosmittaamatta ja ne osallistuvat koko ajan enemmän rakennetun ympäristön olosuhteiden valvontaan ja hallinnointiin. Se voi olla pääsynhallintaa, liiketoiminnan prosessien valvontaa, työturvallisuuden parantamiseen ja työvaiheiden kuvaamiseen tarkoitettua tehtävää jne. Turvallisuusteknologian mukanaolo jo hankkeen alkuvaiheessa ja pitkän elinkaaren aikana tuottaa käyttäjille ja ylläpitäjille tilannekuvaa ja tietoa osana johtamisen työvälineitä.

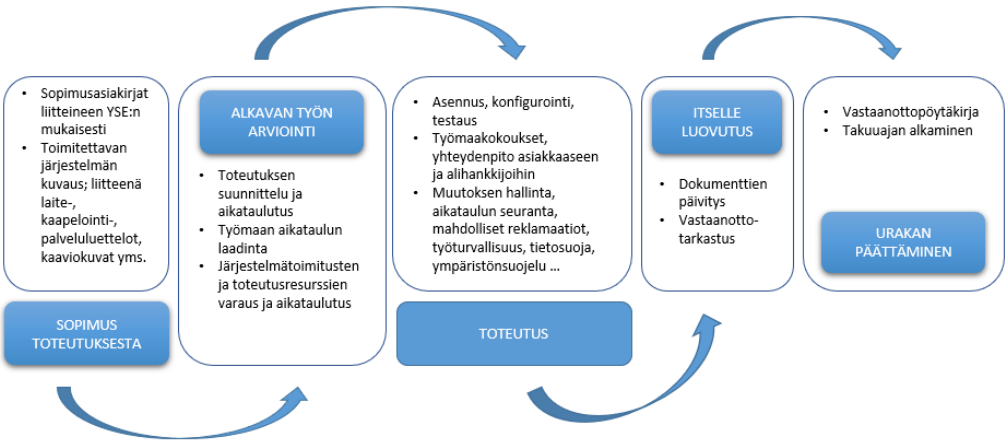


Kuvio 1: OT-ympäristön määritys

Kuvassa 1 on kuvattu tässä opinnäytetyössä rakennettuun ympäristöön kuuluvat OT-järjestelmät, palvelut, prosessit sekä niihin liittyvät rajaukset. Kuvassa punaisella kehyksellä korostetut turvallisuusjärjestelmät ovat osakokonaisuus koko kiinteistöjärjestelmäympäristössä. Kiinteistön luotettavan ja tarkoituksenmukaisen toiminnan kannalta on ensiarvoisen tärkeää ymmärtää järjestelmien ja prosessien väliset riippuvuudet. Kiinteistön järjestelmiä ml.

turvallisuusjärjestelmiä ohjaavat erilaiset ohjelmistot, sähkölaitteet ja herkkä elektroniikka, jonka johdosta pienelläkin häiriöllä saattaa olla laajoja vaikutuksia. Koko kiinteistöjärjestelmäympäristön arkkitehtuuri on kuvattava hyvin, jotta riippuvuudet ymmärretään. Arkkitehtuurin kuvaaminen tarkoittaa myös prosesseja ja palveluja. Tähän kokonaisuuteen sisältyy nyt ja tulevaisuudessa yhä enemmän samankaltaisia prosesseja, palveluita ja vaatimuksia mitä on ICT-järjestelmillä. Niitä ICT:lle tuttuja käytäntöjä ei vain ole otettu OT-ympäristössä käyttöön eikä vakiintuneita malleja ole. ICT-ala ratkoi näitä hankinnan ja elinkaaripalveluiden prosesseihin liittyviä haasteita vuosia sitten ja nyt digimurroksen aiheuttamat haasteet ovat ICT:n vastuulla olevissa palveluissa helpommin ratkaistavissa. Tunnusomaista ICT-alalla on se, että järjestelmiä hankitaan usein palveluna, mutta aktiivilaitteita hankitaan myös omaan taseeseen. ICT-palveluiden ja -laitteiden elinkaarenhallinnasta aina kuitenkin yleensä sovitaan kattavin sopimuksin ja ehdoin. Tämä käytäntö on ollut vieraampaa OT-järjestelmien osalta.

Turvallisuusjärjestelmien hankintamallit laajoissa koko rakennettua ympäristöä koskevissa hankkeissa ovat hyvin perinteisiä. Suunnittelu ja hankintavaiheisiin on julkaistu turvallisuusalan verkostoissa erilaisia oppaita ja ohjeita. Ohjeita on paljon ja toteutusprosessit aina suunnittelusta käytönaikaan on usein kuvattu. Ohjeita on saatavilla eri paikoissa ja kokemuksen mukaan niiden saatavuus ja käyttö arjessa vaihtelee. Jokaisella suunnittelualalla ovat omat ohjeensa ja toteutusprosessinsa ja silloin ne eivät tue koko ympäristöä käsittävää kokonaisuutta vastaamaan digitalisaation tuomiin haasteisiin. Henkilö- ja yritysturvallisuusarviointi SETI Oy:n on kuvannut esimerkillisesti turvallisuusjärjestelmien toteutusprosessin sekä TU-turvaurakoitsijasertifikaatin, jonka mukaan suositellaan toimivan. Mallin avulla pyritään varmistamaan onnistunut ja vaatimustenmukainen käyttöönotto. Malli löytyy Turva-alan Yrittäjät ry:n oppaasta. (Turvaa Oikein-opas 2019, 62.) Tämä ohje ei kuitenkaan ota kantaa riippuvuuksiin ja integraatioihin toimintaympäristön kokonaisarkkitehtuurin näkökulmasta. Näiden rooli korostuu yhä enemmän toimintaympäristön tullessa kompleksisemmaksi ja muutoshallinta sitä kautta vaikeutuu.



Kuvio 2: Turvallisuusjärjestelmien toteutusprosessi (mukaillen Turvaa oikein-opas 2019)

2.1 Määritelmät

2.1.1 Digitalisaatio

Digitalisaatiolle ei ole vain yhtä määritelmää. Eri lähteissä kuvataan asia eri tavalla. Yhteistä kuvauksille ja määritelmille on se, että kyseessä on iso systeeminen muutos kaikissa eri yhteiskunnan rakenteissa ja palveluissa mukaan lukien yritysmaailma. Digitalisaatio näkyy arjessa yhä useamman ja sen hallinnan merkitys kasvaa koko ajan.

Gartner (2016) kuvaa digitalisaatiota seuraavasti: “Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business” (Gartner 2016). Vapaasti käännettynä digitalisaatio on erilaisten digitaalisten teknologioiden käyttöä ja hyödyntämistä liiketoimintamalleissa ja sitä kautta mahdollistaa uusien liiketoimintamahdollisuuksien ja lisäarvon tuottamisen. Se on prosessi kohti digitaalista liiketoimintaa. (Gartner 2016.)

Vuonna 2015 Valtiovarainministeriölle suunnatussa avoimessa kirjeessä silloinen pääministeri Juha Sipilä ja kunta- ja uudistusministeri Anu Vehviläinen määrittelevät digitalisaatiota seuraavasti: “Digitalisaatio on toimintatapojen uudistamista ja sisäisten prosessien digitalisointia, ei vain palveluiden sähköistämistä” (Sipilä ym. 2015).

2.1.2 Turvallisuusjärjestelmät

Sähköiset turvallisuusjärjestelmät ovat oleellinen osa toimitilaturvallisuutta ja yrityksen kokonaisturvallisuutta. Turvallisuusjärjestelmien toteutus tulee nähdä laajemmin siten, että suunnittelussa huomioidaan rakennus ja rakennuksen ympäristö. Sähköisten turvallisuusjärjestelmien tavoitteena on estää tai ennaltaehkäistä rikoksia. Sähköisiä turvallisuusjärjestelmiä

suunnitellaan omana yleensä suunnittelualana tai osana sähkösuunnittelua. Turvallisuusjärjestelmiä kutsutaan myös tilaturvallisuusjärjestelmiksi. Tilaturvallisuusjärjestelmien tavoitteena on myös yrityksen toiminnan häiriöttömyys sekä yrityksen henkilöstön, omaisuuden, tietojen ja ympäristön omaisuuden suojaaminen onnettomuuksilta, vahingoilta, ilkivallalta ja erilaisilta rikoksilta. (Turvaa Oikein-opas 2019, 7-8.)

2.1.3 Operational Technology (OT)

”Operational Technology (OT) is hardware and software that detects or causes change, through the direct monitoring and/or control of industrial equipment, assets, processes and events” (Gartner 2021). Vapaasti käännettynä tähän kehittämishankkeeseen liittyen voidaan sanoa, että OT on rakennetussa ympäristössä kiinteistön toimintaa ohjaava ja tukeva teknologia.

3 Teoreettinen viitekehys

Tässä kappaleessa avataan tämän työn keskeisiä käsitteitä. Aikaisempaa tutkimustietoa haettiin hakusanoilla johtaminen, digitalisaatio, kiinteistöjärjestelmäympäristö, turvallisuusteknologia, turvallisuudenhallinta ja Operational Technology. Hakua kohdistettiin pääosin artikkeleihin, väitösjulkaisuihin ja aihealueen tieteellisiin julkaisuihin. Tutkimusaineistoa haettiin pääosin tieteellisistä maksuttomista julkaisuista viimeisen viiden vuoden ajalta tiedonhakupalvelu Finnasta sekä Google Scholarista. Erityisesti haettiin julkaisuja, missä olisi tutkittu yhdessä näitä osa-alueita, kuten digitalisaation vaikutuksia turvallisuusjärjestelmiin tai turvallisuusjärjestelmin osana koko kiinteistöjärjestelmäympäristöä. Haettiin myös aineistoa, joka ottaa kantaa koko kiinteistöjärjestelmäympäristön johtamisen haasteisiin tai ylipäätään johtamistapoihin. Lopputuloksena oli se, että tutkimusta digitalisaation vaikutuksista kiinteistöjärjestelmä- ja turvallisuusjärjestelmäympäristöön on hyvin vähän. Aika hyvin löytyi digitalisaatiosta ja kyberturvallisuudesta, joka liittyy digitalisaation ja turvallisuudenhallintaan. Niistä löytyi hyvin aineistoa viimeisten viiden vuoden ajalta. Näiden löytyneiden aineistojen kautta pääsee hyvin kiinni siihen minkälaisia tavoitteita digitalisaatiolta odotetaan ja miten toimintaympäristö tulee sen vaikutuksesta muuttumaan. Toimintaympäristöön kohdistuvat muutokset tulee ymmärtää, jotta turvallisuusjärjestelmien tuottajat pystyvät varautumaan oikean osaamisen kehittämiseen tulevien vuosien aikana.

3.1 Johtaminen ja digitalisaatio

”Johtaminen on perustunut aiemmin pitkälti mekanistiseen organisaatiokäsitykseen, mutta nyt organisaatiot on alettu hahmottaa yhteisöinä, joiden voima on ihmisen älyllisessä ja sosiaalisessa kyvykkyydessä”. (Viitala & Jylhä, 2019, 35). Nykyään johtaminen erityisesti asiantuntijaorganisaatioissa korostuu yrittäjämäinen malli ja johtamisopeissa korostetaankin

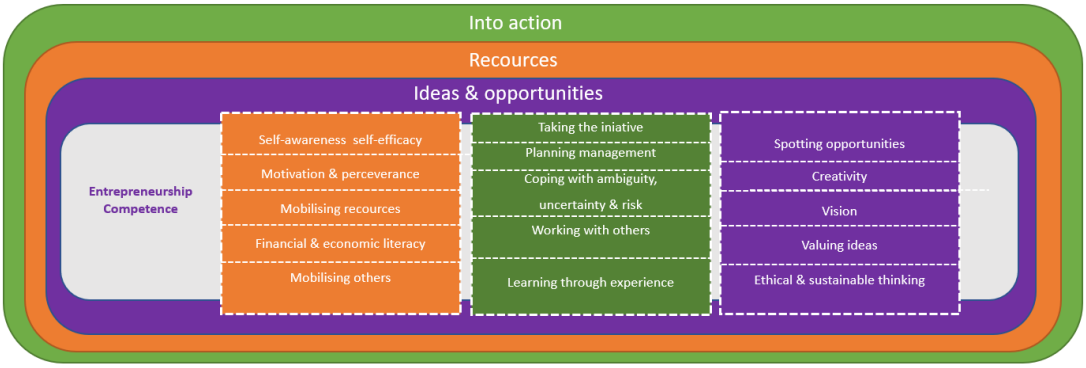
johdettavien itseohjautuvuuden vahvistamista. Yksiköiden ja tiimien jäsenet ottavat vastuuta omasta tekemisestään ja okaisesta organisaation jäsenestä toivotaan aktiivista, itseohjautuvaa toimijaa. (Viitala & Jylhä, 2019, 35.) Usein silloin, kun asia on uusi ja kompleksinen, johtamismallit eivät tue muutosta ja asioiden läpiviennin onnistuminen mitataan verkostoissa. Kehittymistä yleensä tapahtuu vasta, kun saadaan tiettyjä muutoksia aikaiseksi. Muutosjohtamisessa aihealueen pioneerit kohtaavat usein merkittäviä haasteita yrittäen viedä muutosta eteenpäin. Muutosjohtamisella tarkoitetaan systemaattista toimintaa, jolla pyritään toteuttamaan tavoiteltu muutos. Itse muutos ei muutosohjelmissa ole aina se varsinainen ongelma, vaan muutosvastarinta löytyy usein ihmisistä, vaikka juuri ihmiset ovat usein se muutoksen aikaansaava voima. Voidaan arvioida johtuuko asioiden läpivientiin liittyvät haasteet yksittäisistä ihmisistä, mutta Ihmiset eivät kuitenkaan useinkaan välttämättä vastusta itse muutosta, vaan sen vaikutuksia omaan työhön, olosuhteisiin ja yhteisöön. Hyvä johtaja huomioi työyhteisön kokonaisuutena ja ymmärtää, että jokaisella ihmisellä on muutoksessa jokin rooli ja viestii sen myös avoimesti. (Viitala & Jylhä, 2019, 281.)

Organisaatioiden ja prosessien johtamisen näkökulmasta muutoksen läpiviennissä, uusien toimintatapojen oivalluttamisessa, mallien käyttökelpoisuuden tunnustamisessa sekä käyttöönotossa on kyse jonkinlaisesta koulutus- ja oppimisprosessista. Laajan rakenteellisen pysyvän muutoksen synnyttäminen työelämässä on myös työlästä pioneerityötä ja etenkin kun, tavoite ja päämäärä koskettaa useita toimialoja tai organisaatioita. Voidaan puhua myös eräänlaisesta sisäisen yrittäjyyden mallista. Silloin kun tehdään laajoja rakenteellisia muutoksia, niin usein muutoksen läpivienti edellyttää vahvaa verkostoissa johtamista sekä yrityksen sisällä, että palveluorganisaatioissa. Euroopan komissio julkaisi raportin EntreComp-tutkimuksesta, jossa oli tutkittu mm. miten voidaan edistää sisäistä yrittäjyyttä organisaatioiden välisessä johtamisessa ja ylipäätään oppimisprosessissa. Tutkimuksen tavoitteena oli rakentaa yhteys työnteon ja koulutuksen välille sisäisen yrittäjyyden mallia hyödyntämällä kuvaamalla tekemiset kohteet osaamisen kautta. Tutkimus pohti yrittäjyyttä kompetenssien näkökulmasta. Tutkimuksen viitekehyksessä yrittäjyys kuvataan poikkitieteelliseksi osaamiseksi, jota voidaan soveltaa esim. olemassa olevien organisaatioiden ja sidosryhmien kanssa. Tavoitteena tutkimuksessa oli luoda yhteinen käsitteellinen malli, johon yrittäjyysmallissa voisi aina viitata. (Bacigalupo, M., Kampylis Yves Punie, P. & Van Den Brande, G. 2016, 6-7).

Kuvassa 3 löytyy osaamisen kompetenssialueet tässä EntreComp-käsitemallissa. Malli perustuu kolmeen osatekijään, joiden sisään on rakennettu osaamisen kompetenssit. Nuo kolme osatekijää ovat ideat ja mahdollisuudet, resurssit ja itse toiminalliset tekijät. EntreComp käsitemalli on laaja kattava työkalu, jossa on kolme osaamisaluetta, 15 osaamista, 15 kuvaajaa, 8 pätevyystasoa ja 442 oppimistulosta. Käsitemalli kuvaa yrittäjyyden osaamisalueiden moninaisuutta, joka koskettaa ihan jokapäiväisiä arjen asioita. Raportissa todetaan myös, että erilaiset instituutiot, toimijat ja muut tahot, jotka kehittävät uutta, voivat ottaa EntreComp-käsitemallin viitekehykseksi ja hyödyntää sitä omiin käyttötarkoituksiinsa. EntreComp-

käsitemallin prosessin etenemisen kuvaus käsittelee yrittäjyyttä osaamisena, jolla kehitetään yksilöiden ja kollektiivisten tahojen toimia arvon luomiseksi muille. (Bacigalupo ym. 2016, 14-15.)

Yrittäjyysoppimisen etenemismalli koostuu kahdesta näkökulmasta. Ensimmäinen näkökulma koostuu lisääntyvän autonomian ja vastuun kehittämisen ideoiden ja arvon luomismahdollisuuksien toteuttamisessa. Toinen näkökulma koostuu siitä, että kehitetään kykyä luoda arvoa yksinkertaisista ja ennustettavista yhteyksistä monimutkaisiin jatkuvasti muuttuviin ympäristöihin asti. (Bacigalupo ym. 2016, 14-15.)



Kuvio 3: EntreComp-käsitemallin osa-alueet ja osaamisen alueet (mukaillen Bacigalupo ym. 2016,14)

Digitalisaatio edellyttää kokonaisuuden hallintaa, joka laajoissa teknisissä toimintaympäristöissä edellyttää eri suunnittelusaloille yhtenäisiä toimintamalleja. Digitalisaatio mielletään usein sellaisiin asioihin kuten automaatio, tehostaminen ja liiketoiminnan kehitys. Digitalisaatio on myös tietotekniikan hyödyntämistä organisaation toiminnassa. Aina ei välttämättä ole kyse siitä, että digitalisaatio tukee liiketoimintaa. Usein on kyse siitä, että luodaan jotain uutta, mikä saattaa sisältää myös riskejä. Digitalisaatio mahdollistaa uusia toimintatapoja ja sen mahdollistaminen edellyttää osaamista ja näkemystä tietotekniikasta ja sen prosesseista. Digitalisaatio vaatii siis laaja-alaista ymmärrystä tietotekniikasta, organisaation toiminnasta sekä johtamiskäytännöistä ja organisaation tarvitsemasta tiedosta. Yhtäaikainen kehittäminen on saattaa olla hankalaa, koska yhteistä arkkitehtuuria ei ole ja lähestymistapa asioihin saattaa olla erilainen. Kokonaisarkkitehtuuri on kaiken perusta ja sen luomiseen tulee ottaa mukaan laaja-alainen joukko asiantuntijoita. Tärkeää on ottaa mukaan myös ei-ICT-taustaisia henkilöitä, jotta heidät saadaan ymmärtämään arkkitehtuurimallien tarpeellisuuden ja sitoutettua asioiden kehittämiseen uudella tavalla. Arkkitehtuurin kuvaamista voidaan pitää myös oppimisprosessina. Alkuvaiheessa organisaation kyvykkyys uusien työtapojen käyttöönottoon on heikko ja siihen pitää varata aikaa. Syynä hitaaseen kehitykseen saattaa olla ICT-

tyyppiset mallit, jotka on tehty ICT:n tarpeisin, eikä niitä ole mitenkään muokattu kiinteistö- ja turvallisuusjärjestelmäympäristön tarpeisiin. (Pekkola 2018, 1-2.)

Kypsyystason kasvaessa kokonaisuuden hallinta paranee ja kehittäminen siirtyy pois teknologioista. Tässä kohtaa pystytään keskittymään prosesseihin ja kokonaisarkkitehtuurin kehittäminen tulee osaksi normaalia toiminnan kehittämistä. On tärkeää, että näinkin vaikea laaja kokonaisuus, kuten digitalisaatio on, niin se on osa liiketoiminnan strategista kehitystä. Silloin kun johtamismallit johdetaan suoraan strategiasta, niin vastuut voidaan määritellä johdonmukaisesti eikä mandaattiongelmia vaikuttavuuden näkökulmasta tule. Tiivistettynä digitalisaatiossa on kyse siitä, se on osa normaalia liiketoiminnan kehitystä. Organisaatioiden kypsyystasot voivat olla hyvin eri tasoilla ja siksi monet yksittäiset digikehitysprojektit jäävät irrallisiksi yksittäisiksi projekteiksi ja ne eivät siksi skaalaudu. Syynä tähän voi olla riittämätön tietämys prosesseista, teknologioista ja ylipäätään aiheeseen liittyvistä muista tiedoista. Yhteisten tavoitteiden asettaminen ja saavuttaminen on mahdotonta sillä organisaation läpileikkaava kokonaisuudenhallinta puuttuu. Aihealue ja kehitysportaat on jaettava pieniin osakokonaisuuksiin, jotta kehitys on mahdollinen. (Pekkola 2018, 1-2.)

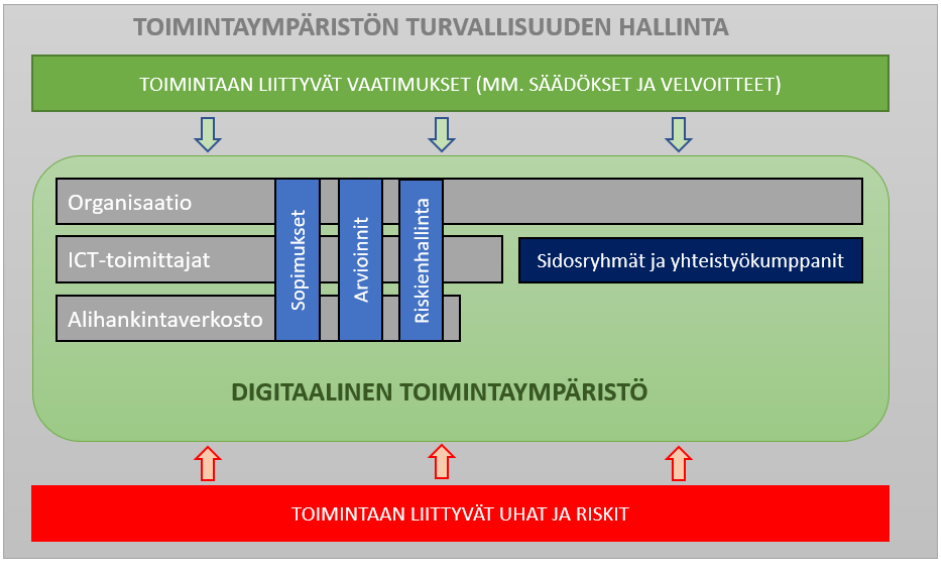
Digitaalinen transformaatio luo uusia mahdollisuuksia ekosysteemiseen toimintaan haastaen samalla perinteisiä liiketoimintamalleja. Kustannustehokkuus kulkee käsikädessä digitalisaation kanssa ja siksi lisääntyneet digitaalisen transformaation vaikutukset liiketoimintaympäristössä nostaa yrityksissä tarpeen perehtyä aihealueeseen tarkemmin. (Luttinen 2018, 7.) Makkosen (2019) mukaan kiinteistöihin kohdistuva disruptio on jo nähtävissä. Kiinteistöihin asennettavien laitteiden teknologia kehittyy ja kiinteistöjen teknologian kehittyminen nähdään erittäin kiinnostavana. Digitalisaatio kuitenkin kehittyy palveluiden näkökulmasta hitaasti, mutta elinkaaripalveluissa nähdään kuitenkin jo mahdollisuuksia ja disruptiota. Hitaaksi kehittymisen tekee osaksi se, että näihin mahdollisuuksiin ei tällä hetkellä löydy riittävästi kyvykkyyttä ja osaamista. (Makkonen 2019, 52.)

Toimintaympäristö on globaalisti muutoksessa. Yhtenä muutosajurina pidetään digitalisaatiota, joka näkyy jokapäiväisessä elämässä ja on päässyt jo jonkin aikaa kehittymään kaikissa yhteiskunnan rakenteissa. Digitalisuus on synnyttänyt tarpeen tuntea toimintaympäristö paremmin ja digitalisaatio tuo siihen uusia vaikutusalueita. Erityisesti rakennetussa ympäristössä, jossa on paljon teknologiaa ja vaativia prosesseja, syntyy uusia digitaalisia ratkaisuja ja palveluja. Uusien palveluiden ja prosessien aiheuttamat riippuvuudet tuovat uusia mahdollisuuksia, mutta myös uusia riskejä. (Heikkinen, 2020, 8.) ”Digitaalisessa yhteiskunnassa tiedon saatavuuden, liikkuvuuden ja yhteen toimivuuden merkitys on aina vain tärkeämpää”. (Valtionvarainministeriön julkaisu, 2019, 36). Yritykset ovat jo tällä hetkellä tuottaneet erilaisia palveluja verkkoon kovaa vauhtia ja niihin liittyvät palvelut ovat muokkaantuneet siinä samalla synnyttäen usein uusia riippuvuuksia palveluiden taakse. Onko tilaajilla ja toimittajilla kyvykkyyttä nähdä ja ennustaa kehitys palveluiden ketjuuntumisen osalta.

Toimintaympäristöissä syntyy uudenlaisesta teknologiaa missä on uusi digitaalinen kerros ja vanha palvelukerros, jotka ovat räätälöity toimimaan yhteen. Tällaisia vanhan ja uuden yhteensovittamisia tulee olemaan vielä vuosia tai vuosikymmeniä ja se saattaa vain lisätä haasteita järjestelmäympäristön hallinnan näkökulmasta. Näin syntyvät uudet teknologiat ja uusi toimintaympäristö luovat uusia uhkakuvia ja myös sitä kautta uusia riskejä liiketoiminnalle ja ylipäätään tiedon turvaamiselle. (Heikkinen 2020, 8-9.)

Toimintaympäristö digitalisoituu kovaa vauhtia ja kyberturvallisuuden strateginen johtamisen onnistuminen on kiinni siitä, että jokaisessa toimintaympäristössä löydetään oikeat rakenteet, missä kyberturvallisuuteen liittyviin uhkakuviin haetaan ratkaisua. Tekninen ympäristö on haastaa kyberturvallisuutta joka päivä ja digitalisaatio saattaa muokata teknistä toimintaympäristöä hyvinkin nopeasti. Myös kybertoimintaympäristölle ominaista on yhä kiihtyvä muutosnopeus. ”Yhteiskunnan haavoittuvuuden lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti”. (Lehto, M., Limnèll J., Pöyhönen, J. & Kokkomäki, T. 2018, 29-30).

IT-organisaatioille ja toiminnoille on tuttua toimintaympäristön kokonaisarkkitehtuuri ja siihen liittyvä huomiot. Valtiovarainministeriön julkaiseman julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman mukaan teknologian nopea kehittyminen 2010-luvulla on aiheuttanut mahdollisuuden kehittää toimintoja ja palveluja yhä nopeammin. Nämä mahdollisuuden koskevat erityisesti palvelujen tuotantomalleja, päätelaitteita sekä tietoliikenneyhteyksiä sekä kaikkia teknologioita, joiden toiminnan ylläpito edellyttää jatkuvaa säännöllistä huolenpitoa. Tulevaisuudessa on yhä helpompi erilaisten laitteiden avulla kerätä tietoa ja pyrkiä hyödyntämään sitä eri tavoitteiden saavuttamisessa eri liiketoiminnan osa-alueille tai ylipäätään toiminnan varmistamiseksi ja turvaamiseksi. Tulevaisuus näyttää siltä, että laitteita tullaan kytkemään internettiin ja tietoliikenneverkkoihin yhä kiihtyvällä vauhdilla ja silloin tietoliikenneverkon tietoturva nousee yhä merkityksellisemmäksi. Tietoliikenneverkko, jonka sisällä on useita keskenään integroituja järjestelmiä, toimintaympäristön riskienhallinta vaatii jatkuvaa seurantaa ja kehittämistä. (Rousku 2018, 16-19.)

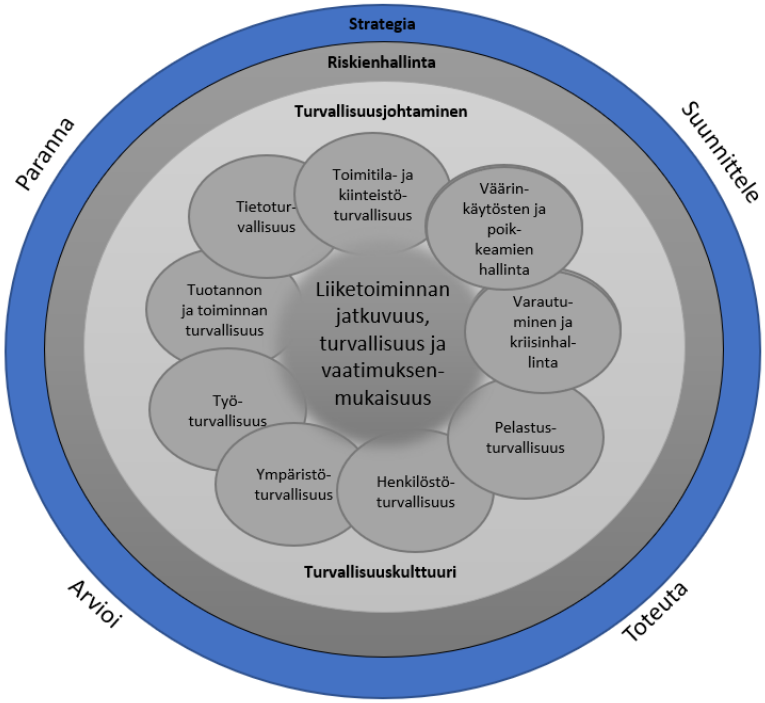


Kuvio 4: Digitaalisen toimintaympäristön turvallisuuden hallinta (mukaillen Rousku 2018,19)

3.2 Turvallisuusjohtaminen

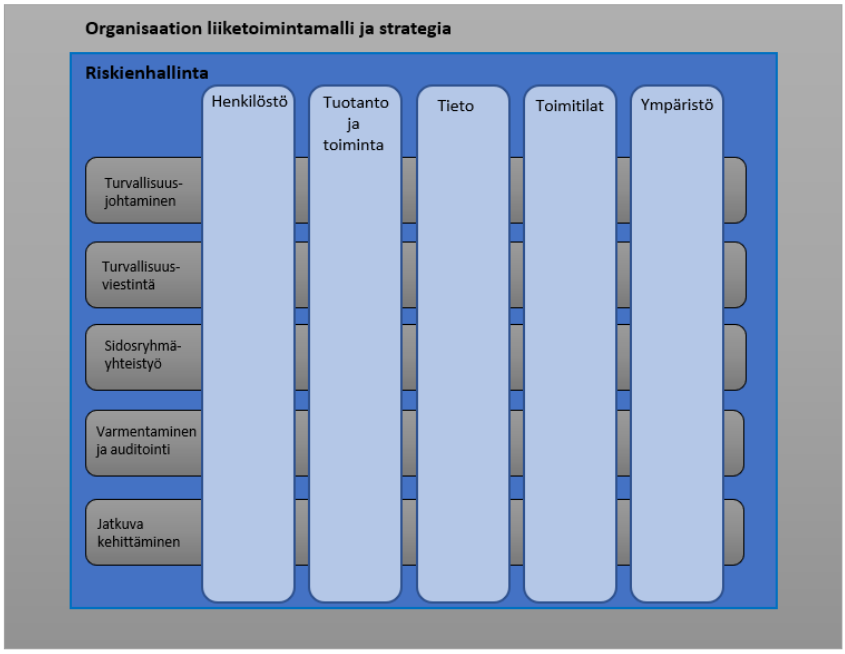
Kiinteistö- ja toimitilaturvallisuus on keskeinen osa yritysten turvallisuutta. Kiinteistöjen, laitosten ja toimitilojen yleiset rakenteelliset turvallisuusvaatimukset täyttyvät niissä osaksi sitä kautta, että rakennukset ja toimitilat rakennetaan noudattaen rakentamista koskevia yleisiä turvallisuusmääräyksiä. Koska määräykset ovat yleisluontoisia ja tulkinallisia, sekä ne koskevat myös muita suojautumiskeinoja, laitosten erityisiä riskejä ym., on kuitenkin välttämätöntä, että yrityksen johto itse määrittää ja hyväksyy kiinteistö- ja toimitilaturvallisuuden yleiset rakenteelliset ja toiminnalliset tasovaatimukset. (Kerko 2001, 277.) Turvallisuuteen liittyvät vastuut kiinteistöissä saattavat jakaantua useille eri tahoille ja silloin vastuu kokonaisuuden johtamisesta saattaa jäädä epäselväksi. Kiinteistöissä saattaa olla eri yhtiöitä ja silloin myös siellä työskentelee useiden yhtiöiden henkilökuntaa. Saattaa olla tilanne, jossa jokainen yritys hankkii omat palvelunsa eri toimijoilta. Eri yhtiöt ovat saattaneet myös monella tavalla verkottua ja keskittää palvelujen hankintaa, jolloin syntyy ns. yhteisen työpaikan piiriin kuuluvia vastuita ratkaistavaksi. Lisäksi yritykset ovat saattaneet ulkoistaa aputoimintojaan, jolloin vastuurajat jäävät epäselväksi ja kompleksisuus lisääntyy entisestään. (Kerko 2001, 278.)

Elinkeinoelämän Keskusliiton yritysturvallisuusmallin (2016) mukaan turvallisuusjohtaminen on normaalia yrityksen johtamista, joka on sisällytetty eri organisaatioiden ja yksiköiden johtamiskäytänteisiin. Tavoitteena ei siis ole yksittäinen erillinen turvallisuustoiminto vaan yrityksen eri toimintojen turvallisuuden ja vaatimuksenmukaisuuden varmistaminen kaikissa tilanteissa. Tällä tarkoitetaan myös kiinteistöympäristön erilaisia teknisiä ja operatiivisia toimintoja, prosesseja sekä palveluja. (Elinkeinoelämä keskusliitto, 2016, 4.)



Kuvio 5: Turvallisuusjohtamisen malli (mukaillen Elinkeinoelämän keskusliitto 2016)

Turvallisuusjohtamista Elinkeinoelämän yritysturvallisuusmallin (2016) mukaan voidaan ajatella myös matriisissa organisaation liiketoimintamalliin ja strategiaan pohjautuen. Turvallisuusjohtaminen eri siilot läpileikkaavat liiketoiminnan prosessit horisontaalisesti mm. henkilöstön, tuotannon, tiedon, toimitilat ja ympäristön osalta. Tätä ajattelumallia käytetään mm. teollisuudessa ja isoissa yrityksissä. (Elinkeinoelämän keskusliitto, 2016, 4-5.)



Kuvio 6: Riskienhallintamalli (mukaillen Elinkeinoelämän keskusliitto)

Laaja-alainen kompleksinen toimintaympäristön turvallisuuden hallinta tarvitsee myös toimivan operatiivisen riskienhallinnan työkalut ja toimintamallit. Hopkin (2012, 13-14) kannustaa lähestymään tarkastelun kohteena olevaa asiaa, toimintaympäristöä tai prosessia tunnistamalla riskit sen vakavimman menetyksen, onnettomuuden, loukkaantumisen tai muun vaikuttavan ei toivotun seurauksen kautta. Hopkin (2012, 13-14) korostaa myös, että riskien tunnistamisessa koskaan ei pidä tyytyä yhteen lähteeseen vaan käyttää monia lähteitä. Apuna voi käyttää tunnettuja viitekehyksiä, kuten esim. riskienhallinnan standardia ISO 31000. Hyvä systemaattinen riskien tunnistaminen, arviointi ja niiden vähentäminen osana normaalia johtamismallia on turvallisuusjohtamisen ja riskienhallinnan peruspilareita. (Hopkin, 2012, 13-14.)

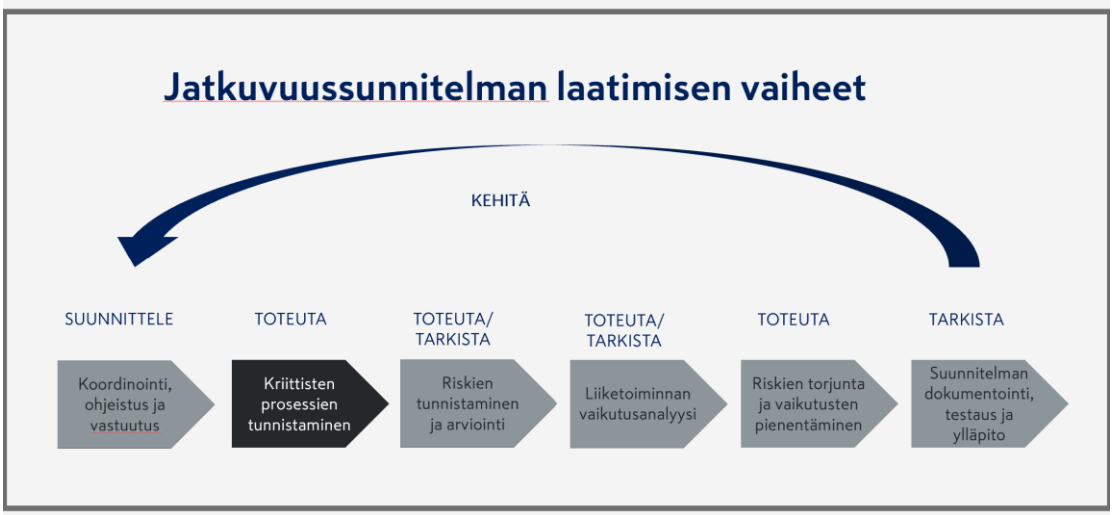
Yritysturvallisuustoiminnon ja siihen liittyvien prosessien on myös syytä uudistua säännöllisesti välttääkseen liiallisen eriytymisen organisaation muusta johtamisesta. Turvallisuusasiat ja siihen liittyvä perustekeminen tulee olla aina kuvattu selkeäsi toimenkuvissa ja toimintasuunnitelmissa integroituna yrityksen strategiaan. Linkitys strategiaan tuo syvyyttä ja vaikuttavuutta turvallisuustyöhön. Yritysturvallisuus on yleensä asiantuntijaorganisaatio, jonka työntekijät tuovat erityisosaamista yritykselle tukemaan kaikkien organisaatioiden toimintaa ja johtamiseen liiketoiminnan turvallisuuden ja jatkuvuuden varmistamiseksi. On tärkeää ja jopa välttämätöntä, että yrityksen johto ymmärtää ja sisäistää turvallisuuden merkityksen sillä yrityksen johto tekee päätökset ja ratkaisee sekä määrittelee viimekädessä yrityksen turvallisuustason. (Lanne, M. 2007, 85.)

3.3 Turvallisuusprosessien johtaminen ja jatkuvuudenhallinta

Toimivat järjestelmäympäristön häiriönhallinnan mallit on mahdollista tehdä vasta kun koko toimintaympäristön riippuvuudet ja prosessit on kuvattu sekä dokumentoitu. Jatkuvuudenhallinta on vaativaa yksityiskohtiin pureutuvaa työtä. Prosessien tarkka kuvaaminen on myös edellytys onnistuneelle jatkuvuussuunnittelulle ja häiriöistä toipumiselle. Ilman kattavaa kokonaiskuvaa yrityksen liiketoiminnasta, strategiasta ja tavoitteista, keskeiset prosessit saattavat jäädä epäselviksi ja varaudutaan vääriin asioihin. Jatkuvuudenhallinnan tavoite on kuitenkin tunnistaa ja varautua siihen mihin kaikkeen mahdollinen häiriö, poikkeustilanne tai muu skenaario voi vaikuttaa. (Iivari & Laaksonen 2009, 105.) Kiinteistöjärjestelmäympäristön osalta omistajuudet ovat usein jakaantuneet, eikä koko ympäristölle ole elinkaarelle käytössä samankaltaisia samaan tavoitteeseen tähtääviä jatkuvan palvelun prosesseja. Siksi juuri tämän tyyppinen prosessi- ja riippuvuustarkastelu on edellytys tässä kiinteistöjärjestelmäympäristössä, jossa toimintaympäristöä eli OT-ympäristöä ei ole toimialana virallisesti tunnustettu, kuten ICT-toimiala on. Turvallisuusjärjestelmiä tulee tarkastella osana koko kiinteistöjärjestelmäympäristöä.

Tässä kehittämistyössä yksi yhdistävä tekijä kaikissa turvallisuusjärjestelmäympäristöön toiminnoissa on riskienhallinta ja jatkuvuus, siksi sen esiin nostaminen tässä yhteydessä on välttämätöntä. Kriittisten prosessien ja riippuvuuksien tunnistaminen sekä niiden toiminnan ja sisällön tuntemus on jatkuvuussuunnittelun onnistumisen kannalta tärkeää. Liiketoiminnan jatkuvuussuunnittelun tavoitteena on turvata organisaation tunnistettujen erikseen määriteltyjen kriittisten prosessien toiminta erilaisissa häiriötilanteissa. Ilman kriittisten prosessien tunnistamista, analysointia ja priorisointia voidaan keskittyä turvaamaan vääriä asioita tai turvataan oikeita asioita väärällä tavalla. (Iivari & Laaksonen 2009, 104.)

On hyvä muistuttaa, että toimiva, tarpeenmukainen ja laadukas turvallisuusjärjestelmäympäristö on juuri niin toimiva, tarpeenmukainen ja laadukas miten osaavia sen suunnittelijat ja toteuttajat siinä kyseisessä hankkeessa ovat. Siksi on tärkeää ymmärtää suunnittelijoiden ja urakoitsijoiden osaamisen vaatimukset tulevaisuudessa. Osaamisen osalta tulee huolehtia kyky toimia kompleksisessa eri aikakauden järjestelmiä sisältävässä kiinteistöjärjestelmäympäristössä.



Kuvio 7: Jatkuvuussuunnitelman laatimisen vaiheet (mukaillen Iivari & Laaksonen 2009, 104)

4 Tiedonkeruu ja tutkimusmenetelmät

Työelämän kehittämistyö opinnäytetyön aiheena asettaa pohtimaan kysymystä onko kyseessä tutkimus vai kehittämistyö. Onko laadullinen tutkimus ylipäätään tutkimustyypiltään teoreettinen vai empiirinen tutkimus. Silloin kun opinnäytetyö on selkeästi työelämän kehittämistyö, niin tulosten kerääminen painottuu empiiriseen suuntaan. Laadulliseksi tutkimukseksi voi nimetä sellaisia tutkimuksia, missä numeroaineistoja ja tilastollisia menetelmiä ei käytetä. Työn tulee kuitenkin täyttää tietyt laadullisen tai määrällisen tutkimuksen reunaehdot, eikä voi olla kokonaan teoriatonta. (Tuomi & Sarajärvi 2012, 19.) Kehittämistyön kohteena olevaa ongelmaa ryhdyttiin ratkaisemaan mahdollisimman yksinkertaisten menetelmien avulla huomioimalla asian laaja-alaisuuden ja kompleksisuuden. Menetelmien tuli olla sellaisia, mikä antaa tilaa tutkia asioita, mitkä ovat uusia. Sopivimmalta tässä kehittämistyössä tiedonhankinnan menetelmän strategiaksi tuntui sopivan toimintatutkimus ja valittavana olevia aineistonkeruun perusmenetelmiä ovat kysely, haastattelu sekä havainnointi. Näiden osalta on vaihtoehtoina kyselystä, haastattelusta ja havainnoinnista on erilaisia variaatioita, joista tulee valita tähän työhön sopiva. (Hirsijärvi, S. 2013, 192.)

Toinen mahdollinen tapa tutkia aihetta oli tapaustutkimus. Tapaustutkimus eli case study voidaan määritellä empiiriseksi tutkimukseksi, joka monipuolisia ja monilla tavoilla hankittuja tietoja käyttäen tutkija tutkii jotain olemassa olevaa tapahtumaa tai ihmisen toimintaa tietyssä rajatussa ympäristössä. Tapahtuma voi olla oikeastaan mikä tahansa toiminto, prosessi tai projekti. Määrittelyn kannalta ongelmallista on se, että tapaus voi olla lähes mikä vain. (Metsämuuronen, 2001, 16-17.) ”Tutkittava tapaus voi olla yksilö, ryhmä, työpaikka, urheilutapahtuma, osasto jne. Tapaus on yleensä jossain suhteessa muista erottuva, se voi olla

poikkeava kielteisesti tai myönteisesti, mutta myös aivan tavallinen arkipäivän tapahtuma". (Syrjälä 1994, 11-12).

Tässä kehittämistyössä päätettiin soveltaa toimintatutkimuksen strategiaa, jossa laaja-alaisen ja syvällisen kuvan saamiseksi tutkittavasta kokonaisuudesta, tietoa kerättiin suorittamalla osallistavaa havainnointia, osallistumalla kiinteistö- ja rakennusalan kehityshankkeisin, tekemällä teemahaastatteluja sekä tutustumalla alan oppaisiin ja ohjeisiin. Toimintatutkimus on tutkimusta, jonka avulla pyritään löytämään erilaisia käytännön ongelmia tai haasteita erilaisissa sosiaalisissa ympäristöissä, työyhteisössä tai organisaatioissa. Toimintatutkimus soveltuu hyvin laaja-alaisen kompleksisen ympäristön tutkimiseen pyrkimällä vastaamaan käytännön toiminnassa havaittuun ongelmaan tai epäkohtaan ja kehittämään olemassa olevaan käytäntöä paremmaksi. (Metsämuuronen 2001, 28.) Opinnäytetyössä sovellettiin siis toimintatutkimuksen strategiaa ja aineistonkeruumenetelminä keskeisten aihealueiden osatekijöiden tiedon syventämiseen osallistuvaa havainnointia ja puolistrukturoitua teemahaastattelua.

Kehittämistyön kohteena tässä opinnäytetyössä oli turvallisuusjärjestelmäympäristön palveluntuottajien osaamisvaatimusten selvittäminen digitalisoituvassa kiinteistöjärjestelmäympäristössä. Tarkoituksena tunnistaa osaamisen osa-alueet ja tarvittavat palvelut, jotka parantavat koko toimintaympäristön turvallisuudenhallintaa. Tarkoituksena ei ole laatia tyhjentävää listaa asioista mitä turvallisuusjärjestelmätoimittajien tulee osata, vaan tunnistaa tehtäviä ja palveluita, joiden tarve on syntynyt rakennetun ympäristön nopean digitalisoitumisen myötä.

Kehittäminen lähtee liikkeelle ongelman tunnistamisesta. Tämän aihealueen ongelman ratkaisemiseen piti tehdä paljon taustatyötä. Hyvin nopeasti huomattiin, että kyse on ensisijaisesti johtamisesta eri verkostoissa. Huomattiin myös, että erilaisia asioita tavoitteen saavuttamiseksi jää pimentoon ja niille ns. katvealueille ei löydy selkeää omistajaa. Asiaa lähdettiin siis ratkaisemaan tunnistamalla aihealueen omistajat ja riippuvuudet. Työ lähti käyntiin kuvaamalla kaikki sidosryhmät, jotka asiaan liittyvät. Tässä oli tärkeää löytää sekä sisäiset, että ulkoiset sidosryhmät. Kehittämisen kohteena oli pureutua erilaisten kiinteistöympäristöön kohdistuviin uudistamis- tai peruskorjaushankkeisiin, missä turvallisuusjärjestelmäympäristöön tehtiin kokonaisuudistus tai rakennettiin kokonaan uutta.

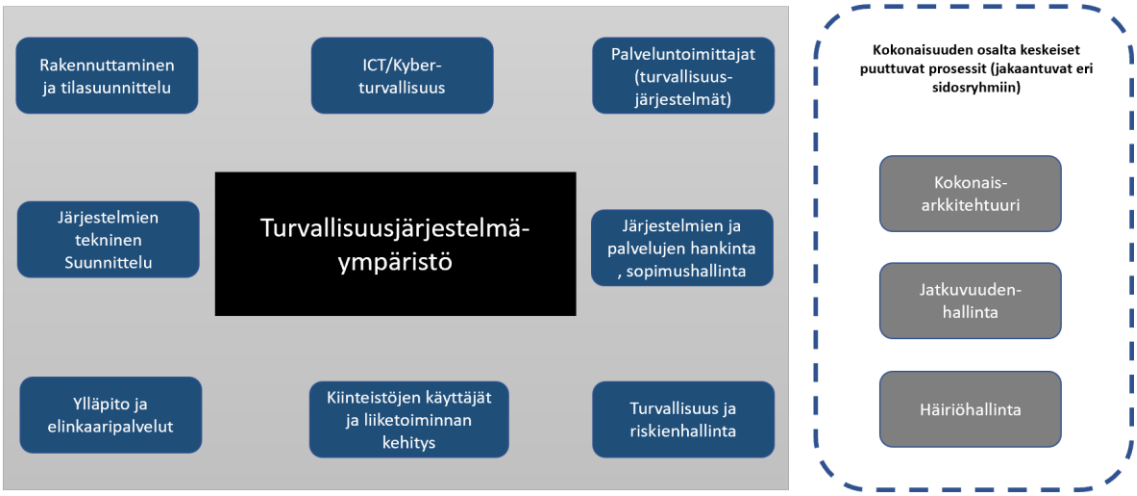
Tässä kehittämistyössä pyritään ratkaisemaan siis digitalisaation tuomia haasteita ja mahdollisuuksia turvallisuusjärjestelmäympäristössä palvelutoimittajien osaamisen näkökulmasta. Tutkimuksen kohteena oleva aihealue on uusi ja juuri siihen rajattuun spesifiin toimintaympäristöön löytyy vähän tutkimusta.

4.1 Havainnointi

Kyselyn ja haastattelun avulla saadaan selville mitä henkilöt ajattelevat ja tutkittavat kertovat mitä tutkittavassa toimintaympäristössä tapahtuu ja mitä he havaitsevat. Havainnoinnin

avulla saadaan selville mitä toimintaympäristössä *todella* tapahtuu ja miten *oikeasti* ihmiset siellä toimivat. Havainnoinnin suuri etu on myös se, että saadaan suoraa informaatiota organisaatioiden ja sidosryhmien toiminnasta. Havainnoinnin avulla päästään autenttisiin arjessa tapahtuviin asioihin ja ympäristöihin. Havainnointi on toki myös työläs menetelmä, varsinkin silloin kun itse tutkija osallistuu havainnointiin samalla kehittäen konkreettisesti tutkittavaa asiaa. Menetelmällä on kuitenkin pitkä historia etenkin kasvatus ja yhteiskuntatieteellisissä tutkimuksissa ja sitä kautta sen toimivuus on todettu hyväksi. Tässä työssä sovellettiin osallistuvaa havainnointia, joka muotoutuu vapaasti tilanteen mukaan ja havainnoija on ryhmän toimintaan osallistutuva tai jopa ryhmän toimintaa ohjaava henkilö. (Hirsijärvi, S. 2013, 212-214.) Tässä kehittämishankkeessa havainnointia tehtiin eri sidosryhmien kanssa erilaisissa hankkeissa, projekteissa, joissa pyrittiin ratkaisemaan ongelmia tai kehittämään toimintamallia ja prosessia paremmaksi.

Toimintaympäristöön rajatut turvallisuusjärjestelmät ja niihin liittyvät prosessit sekä palvelut ovat keskeinen osa kiinteistöjärjestelmäkokonaisuutta. Kehittämistyössä olleet keskeiset sidosryhmät on kuvattu alla olevassa kuvassa 8. Kuvassa on mainittu myös tälle aihealueelle tunnistetut keskeiset prosessit, joita kuvatuilta sidosryhmiltä ei löytynyt. Aineistonkeruu nykytilasta ja tarpeista toteutettiin eri sidosryhmien kanssa erilaisissa projekteissa ja palvelujen määrittelyyn liittyvissä tehtävissä. Eri sidosryhmien kanssa asioita kehitettiin yksittäisten vastuuhenkilöiden ja heidän tiimiensä kanssa ja sen lisäksi erikseen sisäisten ja ulkoisten sidosryhmien kanssa muodostetuissa ohjausryhmissä.



Kuvio 8: Kehittämistyön keskeiset sidosryhmät

4.2 Haastattelut

Haastattelu toteutettiin puolistrukturoituna teemahaastatteluna ja kysymykset oli jaettu viiteen eri kokonaisuuteen. Teemahaastattelussa haastateltiin seitsemää eri henkilöä, jotka olivat eri taustoista. Haastateltavat olivat tarkkaan valikoitu vastaamaan opinnäytetyön tutkimusongelmaan. Henkilöt edustivat tuvallisuusjärjestelmäympäristön osalta korkeaa osaamista omissa organisaatioissaan ja liiketoiminta-segmenteissään. Henkilöt edustivat elinkeinoelämää, energiateollisuutta, pankkisektoria, konepajateollisuutta, rakennetun ympäristön segmentissä toimivaa liikkeenjohdon konsulttitaloa sekä turvallisuusalalla toimivaa sijoitusneuvontaa. Haastateltavien erikoisosaamiset olivat teknologiakehitys, kokonaisarkkitehtuuri, korkean tason turvallisuusratkaisut, rahoitus ja kehitys sekä turvallisuusalaa koskeva sääntely.

Haastattelun viisi eri teemaa:

1. Turvallisuusjärjestelmien suunnittelu
2. Toimintaympäristö
3. Turvallisuusjärjestelmät
4. Datan hyödyntäminen
5. Riskienhallinta

Kuvio 9: Teemahaastattelun toteutuksen malli ja haastattelun aihealueet

Haastatteluissa kuvattiin tarkkaan toimintaympäristö ja haastateltavan rooli. Jokainen haastateltava pääsi kertomaan näkemyksensä ja kokemuksensa laajasti peilaten oman toimialansa, tehtävänsä ja erityisosaamisensa kautta kysymyksiin ja kulloisenkin aihealueen vaikutusalueisiin. Lähtökohtaisesti tuloksia peilattiin kokonaisuutena teemoittain tällä hetkellä olemassa oleviin vallitseviin käytänteisiin ja menettelyihin, mutta samalla kysyttiin mihin suuntaan asioita tulisi viedä, jos tilanne ei ollut optimaalinen haastateltavan mielestä.

4.3 Kehittämistyö

Kokonaisuus tiedonkeruun osalta koostuu monesta eri kokonaisuudesta. Tutustuminen aikaisempiin tutkimuksiin, kohdennettu teemahaastattelu valikoidulle joukolle ja empiiriset kokemukset työhön liittyvässä muutosohjelmassa sekä pitkä kokemus kiinteistöjen turvallisuusauditoinneista eri tulokulmista. Muutosohjelman tavoitteena oli turvallisuusratkaisuiden suunnittelun, hankinnan ja toteutuksen uudistaminen vastaamaan digitalisaation tuomiin haasteisiin ja mahdollisuuksiin huomioiden järjestelmien ja palveluiden tavoitteet sekä päätehtävät niiden elinkaari aikana.

Kehittämistyössä kiinteistö- ja rakentamisenalan eli KIRA-alan operatiivisten prosessien tuntemus oli oikeastaan välttämätöntä tämän työn syntymiseen. KIRA-alalla digitalisaation ympärillä on paljon erilaista keskustelua ja kehitystyö sekä tavoitteet on asetettu pitkälle tulevaisuuteen. KIRA-alan digikehitystä vie eteenpäin mm. KIRAHub-verkosto, joka edistää kyseisen toimialan digitalisaation murrosta. KIRAHub-verkoston yksi tavoitteista on saada kiinteistö- ja rakentamisen toimialalle selkeitä tavoitteellisia harkittuja prosesseja, joiden kestävyyttä ja yhteiskunnallista vaikuttavuutta voidaan mitata. Tätä tavoitetta edistetään KIRA-kasvuohjelman kautta. (KIRAHub 2020.) Näissä kasvuohjelman työpajoissa on tärkeää olla mukana, jotta tietää mihin kasvuohjelma ottaa kantaa ja mihin jää katvealueita sekä epäjatkuvuuskohtia turvallisen rakennetun ympäristön kehittämisessä. Nämä kasvuohjelmat eivät pureudu riittävästi kiinteistöjärjestelmäympäristöön. Erityisesti turvallisuusjärjestelmiä ja niiden kehitystä osana rakennettua ympäristöä ei käsitellä näissä kehitysohjelmissa.

Toinen keskeinen vaikuttaja rakennetussa ympäristössä on Rakennustieto. Rakennustiedon omistaa Rakennustietosäätiö RTS sr. Rakennustiedon tehtävänä on edistää hyvää rakennustapaa toimialalla kiinteistö- ja rakennusalan tiedon tuottajana ja välittäjänä suunnittelusta ylläpitoon. (Rakennustieto, 2022.) Kolmas ohjeita ja menettelyjä rakennettuun ympäristöön tuottaa Sähkö- ja teleurakoitsijaliitto STUL ry. STUL ry on talotekniikka-alan edistäjä, tiedon tuottaja ja jäsentensä edunvalvoja. Vuonna 2020 Rakennustieto julkaisi uudet RT-ohjekortit ja STUL ry julkaisi uudet ST-ohjekortit rakennusten digitaalisen turvallisuuden huomioimiseksi tilaajaorganisaatioissa, suunnittelussa sekä ylläpidossa. (Sähkö- ja teleurakoitsijaliitto, 2022.) Saatiin mahdollisuus osallistua kollegaryhmän kanssa Rakennustiedon digiturvallisen rakentamisen RT-ohjekortin valmisteluun ja ottamaan kantaa ohjeen käytettävyyteen konkreettisena työkaluna. Ohje julkaistiin marraskuussa 2020 ja tässä vaiheessa statuksella *suositus*. Turvallisuusalalla digitalisaatio systemaattisen pitkän tähtäimen kehittämisen näkökulmasta on vasta alussa ja siksi on tärkeää myös ymmärtää miten se otetaan huomioon erilaisissa rakentamisen ja kiinteistöalan kasvu- ja kehitysohjelmissa. RT-ohjekortti rakennusten digitaalisen turvallisuuden parantamiseksi on hyvä startti kehitykselle. Kyseisessä ohjeessa otetaan kantaa digitalisaatioon sekä kyberturvallisuuteen rakentamisen ja järjestelmähankinnan näkökulmasta. RT-

ohjekortit on tarkoitettu tilaajalle, suunnittelijalle ja ylläpidolle rakennusten digitaalisen turvallisuuden varmistamiseksi.

Yksi turvallisuusalan vaikuttamiskanava on järjestö Finnsecurity ry, joka toimii turvallisuusalan ammattilaisten yhdistyksenä ja sen päämääränä on turvallisempi yhteiskunta. (Finnsecurity ry, 2022). Muita merkittäviä turvallisuusalan vaikuttajafoorumeja on Turva-alan yrittäjät ry sekä Turvaurakoitsijat ry. Ala kehittyy laajalla rintamalla ja koulutuksen ja osaamisen varmistaminen on ensiarvoisen tärkeää. Juuri tälle aihealueelle ei systemaattista kokonaisvaltaista koulutusohjelmaa ole, vaan kouluttaminen on pirstaloitunut eri toimialojen koulutusohjelmiin. Turvallisuusjohtamisen ja erityisesti turvallisuusalan strategisen johtamisen koulutustaho on Aalto University Professional Development, Aalto Pro. ”Aalto Pron turvallisuusjohtamisen koulutusohjelmassa opitaan lakisääteisten ja omaehtoisten turvallisuuden johtaminen sekä asioiden, että ihmisten näkökulmasta”. (Aalto University 2022). Turvallisuusalan koulutuksen kehittämisen kautta saadaan myös aihealueella tarvittavaa osaamistarvetta syntymään, jossa Aalto Pro on edelläkävijä ja aktiivinen toimija. Edellä olevien toimijoiden kanssa on nostettu keskusteluun turvallisuusjärjestelmäympäristön digitalisaation tuomia haasteita ja mahdollista potentiaalia ja sitä kautta päästy mukaan myös kouluttamaan aihealueella.

Kehittämistyön tavoitteena oli tuoda esiin tulkintoja turvallisuusjärjestelmäympäristön digitalisoitumisesta ja sen vaikutusalueista sekä laatia suosituksia osaamisvaatimuksiksi turvallisuusjärjestelmien tuottajille työelämähankkeiden kehitysprojektien ja haastatteluiden avulla. Turvallisuusjärjestelmäympäristön prosesseineen ja palveluineen oli tarkastelun ja kehittämisen kohde kaikissa työelämän hankkeissa ja projekteissa 2019 alkaen. Pienetkin muutokset, tehostamiset ja kehittämisen kohteet edellyttivät horisontaalista johtamista verkostoissa ja sidosryhmissä. Tätä muutosta pyrittiin johtamaan poikkitieteellisen ohjausryhmän toimesta ja sen kautta oli mahdollisuus tunnistaa, kehittää ja testata asioita, joita projekteissa ja hankkeissa tuli esiin. Poikkitieteellinen ohjausryhmä koostui liiketoiminnan, hankinnan, riskienhallinnan, yritysturvallisuuden, talotekniikan ja IT:n asiantuntijoista ja päätöksentekijöistä. Tässä kehittämishankkeessa työelämän havaintoja hyödynnetään ja tuloksia analysoidaan tarkasteltaessa koko alaa koskevia käytänteitä ja toimintamalleja. Tämän työn tulokset ottavat siis kantaa turvallisuusjärjestelmien tuottajien toimintatapoihin ja toimintakulttuuriin rakennetussa ympäristössä. Tämän kehittämistyön työelämän empiirisen tiedonkeruun tavat on kuvattu kuvassa 10.

Kuvio 10: Työelämän kehittämistyön empiirisen tiedonkeruun tapoja

Tässä kehittämistyössä osana turvallisuusjärjestelmäympäristön kehittämistä ryhdyttiin valmistelemaan palveluntoimittajaverkostolle uusia osaamisvaatimuksia samanaikaisesti kun, valmisteltiin koko toimintaympäristön toimintamalleja ja käytänteitä. Kehittämishankkeen tiedonkeruu jäsenneltiin neljään eri osa-alueeseen, ongelman tunnistaminen, tiedon kerääminen, laatu ja turvallisuus sekä lopuksi tavoitteen mukaisesti uusien osaamisvaatimusten suositusten kuvaaminen. Kehittämistyön vaiheet on kuvattu alla olevassa kuvassa 11. Tässä kehittämistyössä nämä vaiheet toteutettiin osana normaalia työskentelyä erilaisissa hankkeissa, projekteissa ja työryhmissä. Prosessissa oli mukana tai tuotti kehittämistyöhön aineistoa kuvan 8 ja 10 kuvatut sidosryhmät ja erilaiset koulutustapahtumat ja kehitysohjelmat.

Kuvio 11: Kehittämistyön eri vaiheet ja osa-alueet (ote projektisuunnitelmasta 2019)

4.4 Menetelmän valinta ja toteutus

Laadullisen tutkimuksen metodeja aineiston hankinnassa ovat mm. teemahaastattelu ja osallistava havainnointi. Yksi mahdollisuus oli lähettää valitulle joukolle kysely, mutta aihealue on varsin uusi ja sen ymmärtäminen ennakkopohdinnan mukaan olisi ollut haastavaa. Todennäköisenä riskinä olisi ollut se, että vastattaisiin väärällä kulmalla tai väärään asiaan. Aihealue vaatii taustoittamista ja se onnistuu hyvin keskustelemalla, jossa haastateltavalla on mahdollisuus kysyä jos ei ymmärrä riittävän hyvin asiaa. Näin myös haastatteluissa useasti kävi. Työelämän kehittämishankkeessa keskeistä on oppia työssä tekemisen kautta ja hyödyntää opittua suoraan käytäntöön. Kyselyn tai haastattelun avulla saadaan selville, mitä ihmiset ajattelevat, tuntevat ja uskovat. Ne kertovat miten tutkittavat havaitsevat, mitä ympärillä oikeasti tapahtuu. (Hirsijärvi 2013, 164.)

Työn tavoitetta, rajausta ja kohderyhmää ajatellen puolistrukturoitu haastattelu sopii hyvin tähän työhön. Puolistrukturoitua haastattelua Metsämuuronen kutsuu myös teemahaastatteluksi. Etenkin silloin tämä tutkimusmuoto on hyvä, kun tarvitsee selvittää heikosti tiedostettuja asioita, arvostuksia, ihanteita ja perusteluja. Aihealue on myös uusi ja kysymyksiä joutuu todennäköisesti tarkentamaan ja avaamaan laajemmin. Ei strukturoitu eli avoin haastattelu on myös yksi vaihtoehto, jota voidaan nimittää myös vapaaksi, syväksi tai informaaliksi haastatteluksi. (Metsämuuronen 2001, 41-42.)

Teemahaastattelu sopii siis parhaiten tähän kehittämistyöhön, koska siinä on mahdollisuus keskustella valitun joukon kanssa. Teemahaastattelun toteutettiin puolistrukturoidun haastattelun muodossa. Laadin strukturoidut tarkat samanlaiset kysymykset kaikille vastaajille, mutta kuitenkin ne käytiin läpi vapaasti keskustellen varmistaen, että haastateltavat ymmärtävät rajauksen, teeman, näkökulman sekä sisällön. Teemahaastattelu on Hirsijärven (2013, 208) mukaan lomake- ja avoimen haastattelun välimuoto. ”Teemahaastattelussa on tyypillistä, että haastattelun aihepiirit eli teema-alueet ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuu. Teemahaastattelua käytetään paljon kasvatus- ja yhteiskuntatieteellisessä tutkimuksessa, koska se vastaa hyvin monia kvalitatiivisen tutkimuksen lähtökohtia”. (Hirsijärvi 2013, 208).

Tässä kehittämistyössä on myös pedagoginen kulma ja siksi valitsin teemahaastattelun. Aihealue vaatii taustoittamista ja tarkennuksia monessa osa-alueessa, että kaikkien haastateltavien kanssa ollaan samassa kontekstissa. Teemahaastattelussa on mahdollista kertoa oma tausta, ongelman löytymisen taustat ja ongelman laajuus. Vasta nuo edellä mainitut ymmärrettyään vastaaja pystyy antamaan puolueettoman ja asiantuntijuuteen perustuvan lausunnon tai näkemyksen aiheesta.

Haastattelun tulokset esitetään teemoittain teoreettisten viitekehyksessä esitettyjen näkökulmien valossa. Sen lisäksi kaikkien kysymysten vastaukset on analysoitu Likertin asteikolla

saaden selville aihealueen näkemysten painotukset. ”Likertin asteikko täyttää hyvin järjestysasteikon tunnusmerkit. Likertin asteikolla tehdään tilastollista analyysiä, mutta ilman mitään perusteluja toiminta voi tuntua ristiriitaiselta”. (Vehkalahti 2014, 34-35). Tässä Opinnäytetyössä käytetään tätä mittaustapaa lähinnä tekemään asennemittausta haastattelujen tulosten tukena.

Työelämän kehittämishankkeessa keskeistä on oppia työssä tekemisen kautta ja hyödyntää opittua suoraan käytäntöön. Kyselyn tai haastattelun avulla saadaan yleensä selville, mitä ihmiset ajattelevat, tuntevat ja uskovat. Ne kertovat miten tutkittavat oikeasti asioista ajattelevat ja mitä ympärillä tapahtuu varmistaen, että konteksti on oikea. (Hirsijärvi 2013, 208.)

Kehittämistyön työelämän prosessien tiedonkeruutavat on kuvattu luvussa 4.3 ja siinä on mainittu aikajanalla vaiheet ja asiakokonaisuudet missä aihealuetta käsiteltiin ja keskustelua käytiin. Tärkein oppimisen lähde oli hankkeet ja projektit, joissa turvallisuusteknologia ja siihen liitetyt palvelut koskettivat koko rakennettua toimintaympäristöä leikaten horisontaalisesti kaikki organisaation johtamisen siilot. Toimintaympäristön siilomaisuus aiheuttaa haasteita etenkin elinkaarenhallinnan ja muutoshallinnan osalta, sillä turvallisuusjärjestelmien hankintaan liittyvät toimitusketjut ovat pitkiä aina suunnittelusta käytönaikaan ja järjestelmän vaihtoon tai purkamiseen saakka. Vastuut ja rajapinnat menevät tässä toimitusketjussa monelle eri toiminnolle ja siksi sen johtaminen toimintaympäristön digitalisoituessa on entistä haastavampaa. Turvallisuusjärjestelmien toteutusprosessi on kuvattu aikaisemmin luvussa 2.

5 Kokonaiskuva tuloksista

Näitä eri järjestelmäkokonaisuuksia suunnitellaan, toteutetaan ja hankitaan siiloissa, turvallisuusjärjestelmät mukaan lukien. Kiinteistön käytönaikaa on kuitenkin mietittävä yhtenä kokonaisuutena ja pitkissä elinkaarissa se on haastavaa. Haastatteluissa ja palveluntoimittajien tarjonnassa tuli vahvasti esiin toimintaympäristön digitalisaatio, teknologian nopea kehittyminen sekä voimakas tahtotila hyödyntää avoimia rajapintoja järjestelmien välillä. On entistä tärkeämpää tunnistaa, kuvata, dokumentoida ja etenkin ymmärtää koko järjestelmäympäristön keskinäiset riippuvuudet, prosessit, palvelut ja sitä kautta häiriönsietokyky. Kenelle vastuu kokonaisuudesta kuuluu, niin on vielä osittain epäselvää. Kiinteistöjärjestelmäympäristön johtaminen jakaantuu moneen eri siiloon ja jo siitä syystä kokonaisuuden johtaminen on haastavaa. Haastetta lisää tuo rakennetun ympäristön digitalisoituminen ja sen tuomat vaatimukset kehittää osaamista ja prosesseja. Rakennusvaiheessa kiinteistöön asennetaan parhaimmillaan tuhansia erilaisia laitteita, sensoreita ja erilaisia muita laitteita, jotka on kytketty tai tulevaisuudessa kytketään internettiin. Kokonaisuuden hallinta on erittäin haastavaa järjestelmien riippuvuuksista ja integraatioista johtuen. Riippuvuuksien ymmärtäminen todettiin tärkeäksi myös siksi, että toimintaympäristössä on elinkaaren eri vaiheissa olevia järjestelmät ja

niiden kehityskaaret vaativat toisistaan eroavaa huolenpitoa. On tärkeää, että loppukäyttäjän tarve ja palveluntuottajien tarjonta kohtaavat oikealla tavalla ja oikeassa kohtaa.

Turvallisuussuunnittelu

Turvallisuussuunnittelun osalta näkemyksiin vaikutti toimiala ja kokemuksen määrä konkreettisista turvallisuusratkaisuiden hankinnasta. Haastatteluissa turvallisuussuunnittelun koettiin tulevan mukaan hankesuunnitteluun liian myöhään ja yhteiset tavoitteet muun kiinteistöjärjestelmäympäristön kanssa puuttuvat. Kiinteistö- ja rakennusalan kasvu- ja kehitysohjelmat tukevat tätä ajatusta. Kiinteistöjärjestelmäympäristöä ei nähty kokonaisuutena mikä osaltaan vaikutti myönteiseen näkemykseen siitä, että vaikutukset olisi arvioitu kokonaisvaltaisesti. Näkymää koko ympäristöön ei ole. Digitalisaatio mahdollistaa uusia toimintatapoja ja sen mahdollistaminen edellyttää osaamista ja näkemystä tietotekniikasta ja sen prosesseista. Haastattelujen tulosten ja työelämän havaintojen perusteella on olemassa paljon olettamuksia siitä, että turvallisuusjärjestelmäympäristön tietoliikenneverkkojen suunnittelu ja järjestelmäarkkitehtuurin kuvaaminen toteutuu suunnittelupöydällä ja toteutukseen löytyy vakiintuneita käytäntöjä. Syntyy vaikutelma, että ICT-organisaatioihin automaattisesti luotetaan, vaikka turvallisuusjärjestelmäympäristön palveluiden sisältöjä ei ole riittävällä tasolla kuvattu niiden elinkaarenhallinnan näkökulmasta. Kokonaisarkkitehtuurin luomiseen tulee ottaa mukaan myös ei-ICT-taustaisia henkilöitä, ainakin yksi kukin osa-alueen prosessin omistaja kyseessä olevasta liiketoiminta-alueesta tai hallinnon alasta. ICT ei yksin pysty ratkaisemaan suunnitteluun liittyviä kysymyksiä, mutta ei myöskään muut organisaatiot ilman ICT:tä. Tulosten perusteella ICT-organisaatioilla on aika itsenäinen tapa työskennellä ja muiden ulkopuolisten organisaatioiden sijoittaminen osaksi IT:n toimintamalleja on haastavaa. IT:llä toimintatavat, ammattikieli ja osaamisvaatimukset eroavat merkittävästi muiden organisaatioiden tavasta toimia. Nähtiin, että syntyy vahingossa tai jonkin prosessin osana ns. varjo-ICT. Varjo-ICT:llä tarkoitetaan tässä jonkinlaista mallia, prosessia tai työryhmää, joka ratkoo järjestelmäympäristössä ICT:lle tyyppisiä palvelutarpeita, ongelmia, vikoja tai muita toiminnan jatkuvuuden näkökulmasta välttämättömiä asioita.

Turvallisuusjärjestelmiä ei vielä nähdä luonnollisena osana OT-ympäristöä ja siksi suunnitteluvastuut operatiivisella tasolla jakaantuvat suunnittelupöydällä. Tulosten perusteella yhteisten tavoitteiden asettaminen ja saavuttaminen on vaikeaa ellei mahdotonta, koska organisaatioiden läpileikkaava kokonaisuudenhallinta puuttuu. Kyberturvallisuuteen liittyvät kysymyksiä ratkaistaan eri sidosryhmissä eri järjestelmän elinkaaren vaiheissa ja kokonaisvaltainen kattavuus kyberturvallisuuden osalta saattaa jäädä epäselväksi ja usein ohueksi ja tekniseksi. Se vaikeuttaa erityisesti käytönaikana turvallisuusjärjestelmäympäristön tietoturvaan ja tietoliikennepalveluiden hankintaan systemaattisen määrittelytyön puuttumisen takia.

Turvallisuusjärjestelmien omistajuus ajattelutapana oli uusi. Haastatteluissa asia nähtiin järjestelmien omistajuus itsestäänselvyytenä, mutta alan tapa toimia kertoo kuitenkin jotain muuta. Omistajuuksia turvallisuusjärjestelmiin ei määritetä koko järjestelmän elinkaaren näkökulmasta. Omistajuudet vaihtelevat kuitenkin toimialasta, prosessista ja organisaatiosta riippuen. Haastateltavien näkemyksiä peilattiin käytännön kokemuksiin ja nykyisiin tapoihin toimia. Turvallisuusjärjestelmien hankinta tai päivittäminen osana isoa kiinteistöjärjestelmäkokonaisuutta nähdään tulevaisuudessa hallinnan näkökulmasta kompleksisena ja myös osittain haavoittuvampana. Hankkeita toteutetaan suunnittelualakohtaisesti ja sovittaen ne hankkeen aikatauluun ja budjettiin. Sähkö-, ICT-, talotekniikka- ja turvallisuusjärjestelmät sekä erilaiset liiketoimintalähtöiset järjestelmät kuten esim. jäähdytys- ja energiajärjestelmät suunnitellaan erillisinä toiminnallisina kokonaisuuksina kokonaisarkkitehtuurin näkökulmasta. Yhteensovittaminen tapahtuu toteutusvaiheen loppupuolella tai käytönaikana. Tekninen ja fyysinen tietoturvallisuus koettiin turvallisuusjärjestelmien suunnittelussa tärkeänä ja itse järjestelmän ohjelmistojen kannalta kriittiseksikin. Näkemykset erosivat tässä kohtaa paljon ja yhtenä syynä oli haastateltavien näkemys siitä, kuinka laajana nähtiin turvallisuusjärjestelmäympäristön vaikutukset koko rakennetussa ympäristössä. Oli vahva olettamus siitä, että turvallisuusjärjestelmäympäristön tietoturvasta vastaa ICT-organisaatio kaikilta osin, vaikka käytäntö osoittaa muuta.

Toimintaympäristö

Turvallisuusjärjestelmien päätehtävät ja riippuvuudet tunnistettiin olevan hyvinkin merkityksellisiä palveluien tuottajien näkökulmasta. Järjestelmien tehtävät nähtiin jokseenkin selvänä perustuen niiden perinteiseen tarkastelukulmaan. Järjestelmätoimittajat ja maahantuojat ovat määritelleet omissa asennus- ja käyttötapaohjeissa järjestelmille kuvaukset niiden käyttötarkoituksesta. Turvallisuusjärjestelmät koettiin olevan riippumattomia muista järjestelmistä ja siten esim. kyberturvallisuus olisi mahdollista hallita paremmin. Nähtiin, että kyberturvallisuus nousee voimakkaammin esiin suunnittelupuolella erilaisten toimintaympäristöön liittyvien vaatimusten kautta. Kyberturvallisuuden osalta odotetaan selkeästi uutta velvoittavaa lainsäädäntöä ja etenkin IoT-laitteisiin kohdistuvaa sääntelyä. Turvallisuusjärjestelmäympäristön kokonaisarkkitehtuuri osana koko rakennetun ympäristön järjestelmiä koettiin uutena asiana ja alan tapa toimia tukee tuota käsitystä. Koettiin arkkitehtuurien kuvaamiset olevan enemmän ICT-organisaation vastuulla olevia prosesseja. Olettamus ICT-organisaatioiden vahvasta roolista koko rakennetun ympäristön järjestelmien verkkojen ja tietoliikenneratkaisuiden osalta tässäkin oli vahva. Käytäntö osoittaa, että näihin ei ole laajasti vakiintuneita käytäntöjä.

Digitaalisen toimintaympäristön turvallisuuden hallintaan liittyvät vaatimukset tuovat paljon poikkitieteellistä tarkastelun tarvetta ja erilaista riippuvuuksien ymmärtämistä.

Toimintaympäristöön liittyvät uhat pitää arvioida ja määritellä ICT:n rooli koko turvallisuusjärjestelmäympäristössä. ICT:n tärkeys on tunnistettu, mutta palveluntoimittajien tarjonnassa ja tuotteistuksissa tämä ei tule esiin. Kokonaisarkkitehtuuriajattelu ei kata vielä kaikkia suunnittelualoja siten, että olisi mahdollista saada vakioituja standardinomaisia yhteisiä malleja, mikä auttaa tunnistamaan paremmin esim. käytön ajan palveluiden tarpeet. Turvallisuusjärjestelmät koettiin erillisenä arkkitehtuurina, joka ei suoraan vaikuta koko rakennetun ympäristön toimintaan. Turvallisuusjärjestelmät ja talotekniikka nähtiin toisistaan hyvinkin erillisenä toimintona.

Turvallisuusjärjestelmät

Turvallisuusjärjestelmien teknologinen kehitys on nopeaa ja markkinoilla potentiaalista tarjontaa on paljon. Tilaajan näkökulmasta käyttötapausten määrittelytyö koettiin tarpeellisena, mutta samalla erittäin työläinä. Ilman määrittelyjä turvallisuusratkaisuiden tarjonta on hyvin pitkälti tuotelähtöistä. Koettiin myös, että suunnittelutyössä jo otetaan kantaa laitevalintoihin ja määritetään vaatimukset ja tarpeet, mutta erillään muusta kiinteistöjärjestelmäympäristöstä. Nähtiin myös, että suunnittelussa on tärkeää ottaa kantaa myös järjestelmien prosessien ja palveluiden tietoturvaan, niiltä osin mikä kuului haastateltavien vastuualueelle. Käytännön kokemukset alalta ja tietoturvapalveluja myyvien yhtiöiden palvelutarjonta kohdistuvat enemmän ICT-organisaatioiden vastuulla oleviin prosesseihin ja järjestelmiin. Palveluntoimittajien tuotteistuksessa myyntihetkellä järjestelmäympäristön elinkaaripalvelut näkyvät heikosti. Käytännön kokemus osoittaa, että järjestelmiä hankitaan pääsääntöisesti hankkeelle ja käytönajan suunnittelu jää suunniteltavaksi vasta kun järjestelmä on hankittu.

Järjestelmien väliset rajapinnat ja riippuvuudet nähtiin vieraana asiana. Järjestelmien välisistä rajapinnoista ei puhuta riittävästi eikä niiden tärkeyttä täysin ymmärretä. Järjestelmien väliset rajapinnat ovat ihan keskeisiä asioita digitalisaation näkökulmasta. Elinkaaripalvelut tulevat muuttumaan enemmän tarpeenmukaiseen suuntaan ja palveluja voidaan hankkia tietoon perustuen. Samalla nähtiin, että palveluntuottajien tuntemus ja näkemys digitalisaation tuomiin vaatimuksiin järjestelmien elinkaarella nähtiin vähäiseksi tai niihin ei kiinnitetä huomiota. Syitä voi olla monia, esim. että asiakkaat eivät maksa siitä osaamisesta toimittajille. Korostui, että yksittäisen hankinnan osalta turvallisuusjärjestelmien suunnittelu, urakointi ja ylläpito ovat usein eri toimittajien vastuulla ja hankittu eri osissa.

Turvallisuusjärjestelmien ja niihin liitettyjen palveluiden prosessit ovat muuttuneet ja se tuli esiin sekä haastatteluissa, että alan tavassa toimia konkreettisissa hankkeissa. Turvallisuusjärjestelmät ja niiden elinkaaripalvelut, joita kutsutaan myös ylläpitopalveluiksi sisältävät yhä enemmän ICT-tyyppisiä palveluja. Tulee tietää mm. tuotteiden ohjelmistoista ja niiden tietoturvasta, tunnistaa turvalliset käytettävät protokollat erilaisissa asennuksissa ja tietää

järjestelmäympäristön tietoverkoista ja arkkitehtuurista. Näitä käsitteitä viljellään erilaisissa yhteyksissä, mutta ne eivät vielä näy tuotteistettuina palveluina, eikä näiden asioiden kyvykkyydet nouse tarjonnassa esiin. Tulosten ja havaintojen perusteella osaamista on vaikeaa löytää koko hankittavalle toimitusketjulle suunnittelusta loppukäyttäjälle asti. Asioita ratkaistaan ongelmalähtöisesti ja systeeminen ajattelu aihealueen osalta puuttuu. Oheisessa kuvassa 12 nähdään kehittämistyön tuloksena syntyneet digitalisaation kannalta merkitykselliset turvallisuusjärjestelmäympäristön prosessit ja palvelut, jotka ovat keskeinen osa toimintaympäristön turvallisuuden hallintaa. Oheiset prosessit ja palvelut edellyttävät uutta osaamista turvallisuusjärjestelmien toimitusketjun eri osissa.

Kuvio 12: Turvallisuusjärjestelmiin liittyvät tunnistetut prosessit ja palvelut

Datan hyödyntäminen

Turvallisuusjärjestelmien datan hyödyntäminen koettiin aika ristiriitaisesti. Dataa kertyy paljon, mutta potentiaalia jää paljon hyödyntämättä. Erityisesti esiin nousi erilaisten hälytys- ja valvontatietojen hyödyntäminen, joka ovat turvallisuusjärjestelmien ydintehtäviä. Niiden osalta prosessien nähtiin toimivan hyvin, mutta kehitystä ei viimeisten vuosien aikana ole paljon tapahtunut. Selkeästi esiin nousi tiedon hyödyntämisen vähäisyys eri järjestelmien välillä. Koettiin, että yhteistä tavoitetta datan harmonisoinnille ei ole eri suunnittelualojen kesken ja samalla myös tarjonta erilaisille tiedon käsittelyn alustapalveluille on runsas. Aihealueella toimii paljon startup-yrityksiä ja muita pieniä toimijoita, joilla osaamista on ja jotka luovat

tarvetta alalle. Tilaajan näkökulmasta kokonaisuus näyttää edelleen pirstaleiselta ja tuotelähtöiseltä. Tuotelähtöisellä tarkoitetaan sitä, että tarjonta kattaa aina vain tiettyjä osia koko järjestelmäympäristöstä ja on sidottu tiettyihin palveluihin ja jopa tiettyyn palvelun-tuottajaan. Toisin sanoen rajapinnat ovat tuotteistettu vain tietyille tuotteille. Dataan liittyvä keskustelu oli paljolti erilaista pohdintaa siitä, mitä alalla tarvitaan, mutta koettiin, että konkretia ja standardit puuttuu. Rakennettu ympäristö näkee datan hyödyntämisen kehittämisen enemmän tällä hetkellä energia-asioissa ja turvallisuusteemat ovat jääneet taka-alalle. Turvallisuusjärjestelmien data on vielä jollain tavalla ”pyhää” ja sen laaja hyödyntäminen poikkitieteellisesti hakee vielä muotoaan. Turvallisuusala on itse osittain aiheuttanut alan hitaamman kehityksen järjestelmien yleisen kehityksen osalta. Turvallisuusjärjestelmät ovat teknisessä mielessä sähköjärjestelmiä, joten STUL ry ja SESKO ry tarvitaan mukaan kehitykseen. Asiasta vielä kompleksisemman tekee tietosuojalainsäädäntö, joka sääntelee paljon tiedon käyttöä turvallisuusjärjestelmien osalta ja työllistää etenkin prosessin omistajia.

Kustannustehokkuus nousi esiin datan hyödyntämisestä puhuttaessa. Tiedolla johtamisen mallit tukevat erilaisten etäkäyttöpalveluiden kasvua ja se tuo myös vaatimuksia järjestelmien tietoverkoille ja tietoliikenteelle. Tässä korostuu se, että suunnittelussa tulee huomioida lähes aina etäkäytön mahdollisuus. Tuo etäkäytön valmiuden määrittely perustuu itse järjestelmän teknisiin valmiuksiin, kuten esim. onko kyseisen järjestelmän keskuslaite kytkettävissä verkkoon tai mitä valvomo-ohjelmistoja kyseinen järjestelmä tukee. Tämä edellyttää myös laite- ja vastaanottopäässä tiettyjä digitaalisia valmiuksia ja määrittelyjä tietoturvalle. Koettiin, että turvallisuusjärjestelmiä tuottavien yrityksen kirjo on laaja, mutta hyvin vähän löytyy kypsyystasoltaan yrityksiä, joilla on osaamista pohtia turvallisuusjärjestelmäympäristöä täysin asiakkaan tarpeisiin.

Riskienhallinta

Turvallisuusjärjestelmäympäristö muodostaa rakennetussa ympäristössä riskienhallinnan näkökulmasta laajan aika usein muihin kiinteistöjärjestelmiin integroituneen kokonaisuuden. Näkemykset eri toimialojen edustajien osalta erottuivat selvästi koko toimintaympäristöä koskevan riskienarvioinnin osalta. Riskienarviointiprosessi nähtiin olevan jokseenkin liiketoiminnan operatiivisiin ja strategisiin riskeihin liittyvää tarkastelua. Turvallisuusjärjestelmien suunnittelua tehdään pääsoin erillisenä suunnittelualana ja niiden urakointi myös. Riskienarviointi nähdään liiketoimintalähtöiseksi tarkasteluksi tai järjestelmien suunnitteluun ja hankintaan liittyen hyvin tekniseksi tarkasteluksi. Nähtiin, että digitalisaatiosta puhutaan paljon ja siihen liittyvästä tietoturvahaasteista, mutta erityisesti digitalisaation vaikutusten arviointi turvallisuusjärjestelmien prosesseihin ja palveluihin osana OT-järjestelmäympäristöä on vähäistä. Näkemyseroja muodostui palveluiden kriittisyyksistä riippuen. Liiketoimintaprosessien kriittisyys siis vaikutti näkemykseen riskienarvioinnin tärkeydestä ja kattavuudesta, mutta yhteyttä

kiinteistöjärjestelmiin ei täysin nähty. Näin ollen kokonaisarkkitehtuurin ja riippuvuuksien näkökulmasta koko kiinteistöjärjestelmäympäristön riskienarviointitarkastelu prosessien näkökulmasta oli uutta.

Turvallisuusjärjestelmiin kohdistuvat elinkaarikustannukset koettiin olevan suhteellisen hyvin tiedossa, vaikka näkymä digitalisaation vaikutuksista järjestelmien elinkaareen onkin vielä hieman epäselvä. Yksi syy heikkoon näkymään nähtiin olevan koko kiinteistö- ja rakentamisen alaa koskeva voimakas murros ja toimintatapojen eriävä kehittyminen eri osa-alueilla. Nähtiin, että turvallisuusjärjestelmät eivät ole vielä niin paljon integroituneet muun kiinteistöteknologian kanssa, että niiden taloudellinen tarkastelu yhtenä kokonaisuutena olisi tullut tarpeelliseksi tai sen puute ylipäätään olisi ongelma. Tiivis yhteistyö organisaatioiden ylläpidon kanssa mahdollistaa paremman kustannusten seurannan, mutta kustannusten kohdistaminen esim. ongelmakohtiin datan puuttumisen osalta on haastavaa. Turvallisuusjärjestelmäympäristöön kohdistuvista häiriötilanteista saatiin paljon näkemyksiä. Osa kokee niiden olevan hyvin hallinnassa ja niillä on harvoin vaikutusta suoraan liiketoimintaan, eikä juurikaan kustannuksiin. Osa koki, että käytössä ei ole mitään erityisiä häiriöhallinnan malleja tai jatkuvuussuunnitelmia, vaan asioita ratkotaan erilaisilla huoltosopimuksilla, laitetesteillä tai muulla laadunvalvonnalla esim. hankkeissa ennen käyttöönottoa. ICT:n vastuulla olevissa palveluissa häiriönhallintamallit ja jatkuvuussuunnitelmat ovat tuttuja vakioituja toimintamalleja, mutta ne eivät sellaisenaan ulotu kiinteistö- ja turvallisuusjärjestelmäympäristöön asti kattavasti.

6 Yhteenveto ja pohdinta

Yleinen kuva toimintaympäristöstä on se, että yhteiset toimintamallit ja yhteisen tavoitteen puuttuminen kompleksisessa rakennetuissa ympäristöissä tekee asioista siilomaisia ja pirstaleisia sekä samalla pahimmillaan hyvin tehottomia. Kehittämishankkeessa nousi esiin, että tämän tyyppinen kokonaistarkastelu aihealueen ympärillä on täysin uutta koko alalle. Digitalisaatio tekee muutosnopeuden haastavaksi turvallisuudenhallinnan näkökulmasta. Toimintaympäristö, jota tässä tarkastellaan on kontekstina uusi kokonaisuus, jollaista ei tutkimusmielessä ole juurikaan tarkasteltu. Asiaa pitää tarkastella strategisen johtamisen tasolla ja kiinteänä osana liiketoimintaa. Strategiassa vastataan kysymykseen johtamisen näkökulmasta, miten aiotaan päästä päämäärään ja sen on tässä ihan keskeistä aihealueen pirstaloitumisen takia isoissa muutosta vaativissa kokonaisuuksissa. (Viitala 2019, 281.)

Digitaalisen turvallisuuden tilaa koskevan raportin mukaan julkisen puolen hallinnon sisäisten ja ulkopuolisten tuotantoketjuissa on digitalisaation myös tullut uusia haasteita. Riskitasot ovat muuttuneet ja tietoturvallisuus, osaaminen sekä tuotantokapasiteetti tuovat epävarmuutta turvallisuuden hallintaan. On todettu, että kunnissa ei ole riittävästi parannettu

digitaalisen turvallisuuden toimintamalleja, eikä otettu huomioon tätä muuttunutta tilannetta keskeisten ICT-toimijoiden kanssa. (Valtiovarainministeriö 2020, 23.) Sama tilanne näkyy hyvin yksityisellä puolella turvallisuusjärjestelmäympäristöä koskevissa prosesseissa ja toimintamalleissa, jossa nousee samankaltaisia haasteita tämän opinnäytetyön tulosten mukaan.

Jonkinlaisena riskinä nähdään tulosten suhteen aihealueen johtamiseen liittyvät siilot. Siilomainen johtamismalli voi aiheuttaa keskustelun puutteen siilojen välillä. Keskustelusta saattaa tehdä haastavan myös yhteisen kielen puuttuminen. Yhteisen kielen puuttuminen vaikeuttaa yhteisen tavoitteen löytämiseen digitalisaation transformaation osalta. Keskeistä on tunnistaa vaikutusalueet ja sitä kautta on mahdollisuus arvioida toimenpiteiden kriittisyyksiä. Poikkitieteellinen ajattelu vaatii laaja-alaista näkemystä, muutoksen läpivienti rohkeutta ja pitkäjänteisyyttä sekä verkostoissa vaadittavaa arvokasta pioneerityötä. Operatiivinen toiminta ja sieltä saadut kokemukset puhuvat poikkitieteellisen johtamisen puolesta tällä uudella aihealueella. Uudet monimutkaiset ja monikerroksiset osaamisalueet vaativat uudenlaista lähestymistapaa johtamiselle.

Euroopan Komission julkaisemassa raportissa yrittäjäkompetenssien viitekehyksestä. Siinä viitataan uuteen ns. yrittäjyysoppimismalliin, jonka oppeja voidaan hyödyntää organisaatioiden kehittämisessä ja osaamisen kasvattamisessa isoissa monia organisaatioita ja toimialoja koskevassa systeemisessä muutoksessa. (Bacigalupo ym. 2016, 14.) EntreComp-käsitemallia voitaisiin käyttää esim. osaamisvaatimusten suunnittelussa ja opetussuunnitelman laatimisessa uuden toimintaympäristön tuomiin haasteisiin. Johtamisen näkökulmasta on ensiarvoisen tärkeää saada ihmiset oivaltamaan mistä on kyse, mitä tavoitellaan ja mitä tavoitteeseen pääseminen edellyttää organisaatioilta. EntreComp-käsitemalli tuo viitekehyksen jäsentää erilaisia osaamisalueita ja miten ne saadaan käyttöön. (Bacigalupo ym. 2016, 14-16). Malli sopii hyvin isojen kokonaisuuksien systeemisen muutoksen edistämiseen, jossa voidaan hyödyntää yrittäjämäistä toimintamallia, ideoidaan, ollaan luovia, synnytetään tarvetta, tunnistetaan osaamisalueita ja tunnistetaan kohderyhmiä jne. Malli on hyvin samansuuntainen kun startup-yritysten maailmassa. Kehittämistyön alkuvaiheessa jo tunnistettiin, että digitalisaation vaikutukset koko rakennettuun ympäristöön ovat niin valtavat, että joitain uusia menetelmiä ja toimintatapoja aihealueen johtamiseen pitää löytää. Kehittämistyössä tapa toimia ja kehittää muistutti hyvin paljon startup yrityksen tapaa toimia. Toiminnan kehittäminen vaatii yrittäjämäistä otetta ja tekemistä, joka lähtee oivalluksista, intuitiosta ja vahvasta operatiivisesta käytännön kokemuksesta.

Kehittämistyön tulosten perusteella voi todeta, että turvallisuusteknologiaa suunnitellaan, hankitaan ja toteutetaan edelleen aika perinteisesti yhä nopeammin digitalisoituvassa rakennetussa ympäristössä. Haastatteluista ja vuosien käytännön kokemuksista hankkeissa käy ilmi, että yhä edelleen tarkastellaan turvallisuusjärjestelmiä hyvin pitkälti erillisenä kokonaisuutena irti muusta kiinteistöjärjestelmäympäristöstä. Tarkastelua tulee tehdä paljon laajemmin

koko rakennetun ympäristön turvallisuusjärjestelmin, -palveluihin ja -prosesseihin integraatioiden ja riippuvuuksien näkökulmasta. Digitalisaatio on tullut mukaan koko toimitusketjuun ja siksi asia koskettaa monen johdettavan toiminnon prosesseja. Toimintaympäristön turvallisuuden hallinnan kannalta tulee entistä paremmin tunnistaa prosessien vaikutusalueet ja arvioida niiden kriittisyyksiä.

Tämän kehittämistyön aihealueen kehittämiselle löytyy myös riskejä. Tässä lähestytään ongelmaa digitalisaation näkökulmasta ja sen vaikutukset läpileikkaavat kaikki siilot ja organisaatiotasot. Silloin toivottu muutos täytyy saada koko toimitusketjun läpi ja joissain tapauksissa jopa yhtäaikaisesti. Tulosten perusteella on todennäköistä, että yritysten eri organisaatioiden välillä saattaa olla ehkä liiaksi kunnioitusta toisiaan kohtaan uskaltaen haastaa nykyisten toimintamallien kehittämistarpeet asian ollessa myös toisen organisaation vastuulla. Se saattaa tuoda tilanteen, jossa kehittämistyötä on lähes mahdotonta aloittaa, kun ei ole olemassa poikkitieteellistä päätöksentekoprosessia. Eri organisaatioiden spesifit toimintamallit ja omat toimintasuunnitelmat ja kehityspolut saattavat aiheuttaa haasteita rakennetun ympäristön vaatimuksien määrittelyyn. Jos määrittelyt eivät ole johdonmukaisia toisiinsa nähden kaikissa rakennetun ympäristön järjestelmissä, niin järjestelmille tarjottavat palvelutkaan eivät ole toisiinsa nähden johdonmukaisia. Silloin syntyy pirstaleisia osakokonaisuuksia, jonka turvallisuuden hallinta saattaa olla vaikeaa ja osittain reaktiivista.

Turvallisuusjärjestelmien palveluntoimittajien Kypsyystasot osaamisen osalta vaihtelevat merkittävästi ja järjestelmähankinnan pitkän toimitusketjun eri vaiheissa syvää osaamista kyllä löytyy. Ongelmalliseksi tilanteen tekee se, että prosessit eivät ole vakioituja ja useissa tapauksissa syväosaaminen henkilöityy. Lopputuloksena saattaa syntyä hankekohtaisia ratkaisuja. Näin ollen kokonaisuuden osalta ei toivottua lopputulosta saada tai se on hyvin työlästä. Turvallisuusjärjestelmäympäristön käytönajan haasteet ja kustannukset jäävät käytönajalle ratkaistavaksi ja kannettavaksi, siksi ylläpidon ja käyttäjien mukaan ottaminen suunnitteluun on tärkeää. Turvallisuusjärjestelmiä tarjotaan yhä enemmän elinkaaripalveluna, mutta tarpeenmäärityksessä ja suunnittelussa käytönajan tarpeita hyvin harvoin tunnistetaan ja määrittelytyö elinkaaripalveluille alkaa vasta käytönaikana. On ihan kriittistä tunnistaa jo suunnitteluvaiheessa käytönajan tarpeet, sillä elinkaaripalvelu-mallissa parhaat hankinta ja toteutusehdot käytönajalle voidaan sopia ennen järjestelmien hankintaa, ei sen jälkeen. Tässä kehittämistyössä haastattelun tulokset ja empiiristen konkreettisten kenttäkokemusten avulla aihealueelta löytyi turvallisuusjärjestelmien toteutusprosessista selkeästi uusia tehtäviä ja prosesseja, jotka eivät ole tällä hetkellä palveluntuottajien tarjonnassa mukana. Uudet löydökset ovat kuitenkin sellaisia, jotka ovat keskeisiä turvallisuusjärjestelmäympäristön jatkuvuuden ja kyberturvallisuuden näkökulmasta tulevaisuudessa eli ovat osa koko rakennetun ympäristön turvallisuuden hallintaa.

Turvallisuusjärjestelmien tuottajat ovat uusien vaativien asioiden äärellä. Kyberturvallisuutta haastetaan joka päivä ja juuri tämä osa-alue ottaa kantaa turvallisuusjärjestelmien turvallisuudenhallintaan fyysisen ja teknisen kyberturvallisuuden osalta. Kokonaisuuksien hallinta vaatii vahvaa poikkitieteellistä osaamista. Jatkuvuuden ja riskienhallinnan näkökulmasta on välttämätöntä tunnistaa kaikki vaikutusalueet. Siellä korostuvat arkkitehtuuri, kokonaisuuden hallinta, elinkaari sekä jatkuvuuden operatiivinen hallinta. Tavoitteena tilaajalla on saada mahdollisimman häiriöttömiä palveluita ja ratkaisuja kustannustehokkaasti. Kuvassa 12 olevat prosessit ja palvelut ovat turvallisuusjärjestelmien toimittajille uusia tai niitä ei tuoda tarjonnassa ja suunnittelussa selkeästi esille.

Turvallisuusjärjestelmät ovat siinä määrin digitalisoituneet, että järjestelmissä on paljon IP-pohjaisia (IP=Internet Protocol) laitteita ja silloin ne vaativat tietoliikenneverkon. Tietoliikenneverkon turvalliseen ylläpitoon liittyy erilaisia niiden valvontaan ja tietoturvaan liittyviä vaatimuksia. Järjestelmät sisältävät ohjelmistoja ja lisenssejä, jotka edellyttävät säännöllistä huolenpitoa mm. ohjelmisto- ja tietoturvapäivityksiä. Tietoliikenneverkot sisältävät erilaisia kytkimiä, joiden turvallisuusvaatimukset edellyttävät käyttötapausten ja kriittisyyksien määrittelyä. Kaikki edellä mainitut luovat tarpeen synnyttää uusia palveluja, joita turvallisuuspalvelujen tuottajat eivät perinteisesti tarjoa. ICT-organisaatioilta löytyy kyvykkyyttä, mutta ICT-talot yleisesti ottaen eivät turvallisuusjärjestelmien toimittajiksi vielä laajasti ole ilmoittautuneet. ICT-taloja muistuttavat yritykset jo myyvät tai edustavat jo jonkin verran esim. IP-pohjaisia kameravalvontajärjestelmiä, joiden tallennus tapahtuu pilvipalvelussa. Näitä palveluja myydään vielä perinteisten turvallisuusjärjestelmiä myyvien yritysten kautta ja se edellyttää palveluja ostavien yritysten ICT-organisaatioita määrittämään näiden palveluiden tietoliikenneratkaisut. Analogisen maailman muuttamisen digitaaliseksi vaatii aina jonkinlaista digitaalista transformaatiota ja jos niitä halutaan systemaattisesti edistää niin se edellyttää yleensä strategiatason päätöksiä tilaajan yrityksissä. Digitaalisen turvallisuuden tilaa koskevassa raportissa todetaan, että ”nykyisellään IoT-laitteiden sisäänrakennettu turvallisuus on melko heikko johtuen kustannustehokkaista prosesseista tuotannossa”. (Valtiovarainministeriö 2020, 23).

Turvallisuusjärjestelmissä liikkuvan datan hyödyntäminen on vielä aivan alussa. Erilaisista analytiikkapalveluista on puhuttu melkein 15 vuotta, mutta Suomessa tällaiset palvelut eivät ole saaneet imua. Kyseisiä palveluja on yritetty myydä sinnikkäästi turvallisuusorganisaatioille, ICT-organisaatioille ja suoraan liiketoiminnalle, mutta lähes tuloksetta. Uusia hyviä innovaatiota turvallisuusteknologian segmentissä löytyy, mutta hankinnan mallit ja tilaajaorganisaatioiden kyvykkyydet vaativat vielä kehittymistä.

Yhteenvetona voidaan todeta, että turvallisuusjärjestelmiä tuottavien yrityksen on tunnistettava rakennetun ympäristön muutokset ja kehitys. Mitä vaikutuksia digitalisaatiolla on ja miten uudet teknologiat sekä niiden kehittyminen vaikuttaa palveluihin ja tuotteisiin. Tarvitaan

uutta osaamista aina suunnittelusta ja palveluiden myynnistä lähtien. Tekninen osaaminen ei enää riitä, vaan pitää ymmärtää laajasti koko kiinteistöjärjestelmäympäristön eli OT-ympäristön toimintaa, käyttäytymistä ja prosesseja. On tärkeää osata tunnistaa miten kehittyvässä digitalisoituvassa ympäristössä turvallisuuspalvelut suunnitellaan, rakennetaan ja integroidaan osaksi ekosysteemiä ja sen ekosysteemin muutoshallinta elinkaaren aikana. Sen lisäksi uutta osaamista edellytetään analytiikkapalveluissa ml. integraatiot ja rajapinnat eli APIt. ”API tarkoittaa ohjelmointirajapintaa ja se on lyhenne sanoista Application Programming Interface”. (Frisk, S. 2019, 6). Osaamisen ja palveluiden kehittäminen pitää tehdä laaja-alaisesti yhteistyössä tilaajien, palveluntoimittajien, alan verkostojen ja järjestöjen sekä oppilaitosten kanssa. Kaikki lähtee laaja-alaisesta laadukkaasta systemaattisesta toimintaympäristön riskien ja mahdollisuuksien kartoittamisesta. Sen pohjalta voidaan priorisoida asioita ja laatia kehityssuunnitelmia pitkälle aikavälille. Siilomaisessa suunnittelussa ja urakoinnissa koko turvallisuusjärjestelmäympäristön tarkastelu erilaisine vaikutusalueineen riskienarvioinnin näkökulmasta jää usein vaillinaiseksi tai sitä ei tehdä laajamittaisesti ollenkaan. Yhteisenä tavoitteena tulee olla toimiva turvallinen kiinteistö, joka mahdollistaa siellä harjoitettavan liiketoiminnan suunnitellusti ja strategian mukaisesti.

Lähteet

Painetut

Hirsijärvi, S., Remes, P. & Sajavaara, P. 2013. Tutki ja kirjoita. 15.-17. painos. Helsinki: Tammi.

Hopkin, P. 2012. Fundamentals of risk management. Understanding, evaluating and implementing effective risk management. Printed and bound by CPI Group (UK) Ltd, Croydon, CRO 4YY.

Jylhä, E., & Viitala, R. 2019. Johtaminen, keskeiset käsitteet, teoriat ja trendit. Helsinki: Edita.

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu. Tallinna: Painotalo Raamattutrukikoda.

Kerko, P. 2001. Turvallisuusjohtaminen. Porvoo: Bookwell Oy.

Metsämuuronen, J. 2001. Laadullisen tutkimuksen perusteet. Viro: International Methelp Ky.

Tuomi, J., & Sarajärvi, A. 2012. Laadullinen tutkimus ja sisällönanalyysi. Vantaa: Hansaprint Oy

Syrjälä, L. 1994. Tapaustutkimus opettajan ja tutkijan työvälineenä. Rauma: Kirjapaino Westpoint Oy, Kirjayhtymä Oy.

Sähköiset

Aalto University, Professional Development 2022. Viitattu 12.2.2022. https://www.aalto-pro.fi/ohjelmat/turvallisuusjohdon-koulutusohjelma-tjk

Airaksinen, M. (marraskuu 2021). KIRA-kasvuohjelma kirittää rakentamaan vähäpäästöisesti. Rakennustaito. 2021. Julkaistu 24.11.2021. Luettu 23.1.2022. https://rakennustaito.fi/kira-kasvuohjelma-kirittaa-rakentamaan-vahapaastoisesti/

Airaksinen, M. 2021. ROTI-hanke. Rakennetun omaisuuden tila 2021. Viitattu 16.5.2021. https://www.ril.fi/media/2021/vaikuttaminen/roti2021_low.pdf

Frisk, S. 2019. API RAJAPINTOJEN HALLINTA JA TIETOTURVA. Kandidaatin tutkielma. Jyväskylän yliopisto. Jyväskylä. Viitattu 12.3.2022. https://jyx.jyu.fi/bitstream/handle/123456789/64334/URN%3aNBN%3afi%3ajyu-201906042942.pdf?sequence=1&isAllowed=y

Gartner, Operational Technology, määritelmä. Viitattu 28.11.2021: https://www.gartner.com/en/information-technology/glossary/operational-technology-o

Hallamaa, J., Haikarainen, R. & Kalliokoski T. 2021. Tekoälyteknologiat ja turvallisuus. Tieteessä tapahtuu, julkaisu. Viitattu 21.1.2022. https://journal.fi/tt/article/view/111214

Henkilö- ja yritysarviointi SETI Oy. TU-turvasertifikaatti. Luettu 1.4.2022. https://www.seti.fi/tu-turvaurakoitsijasertifikaatti

Heikkinen, H. 2020. Digitaalisen turvallisuuden harjoitustoiminnan tila julkisessa hallinnossa. Maisterivaiheen työ. Informaatioteknologian tiedekunta. Jyväskylän Yliopisto. Viitattu 14.4.2022. https://jyx.jyu.fi/bitstream/handle/123456789/68760/URN%3aNBN%3afi%3ajyu-202004282963.pdf?sequence=1&isAllowed=y

KIRA-InnoHub ry. KIRA-alan digitalisaation tavoitteet. Viitattu 8.3.2022. https://kira-hub.org/on-aika-nostaa-kirahvi-poydalle-kira-alan-on-paatettava-mita-se-haluaa-digitalisaatiolta/

Lanne M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. Viitattu 12.11.2021. https://www.vttresearch.com/sites/default/files/pdf/publications/2007/P632.pdf

Lehto, M., Limnèll J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. Viitattu 15.3.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf?sequence=1&isAllowed=y

Luttinen, O. 2018. Digitaalinen transformaatio liiketoimintaekosysteemissä. Tietojärjestelmätiede, kandidaattitutkielma. Jyväskylän yliopisto. Viitattu 10.1.2022 http://www.urn.fi/URN:NBN:fi:jyu-201812205254

Makkonen, M. 2019. Kiinteistöpalvelujen digitalisaatio Suomessa. Informaatioteknologian tiedekunta. Maisterivaiheen työ. Jyväskylän Yliopisto. Viitattu 12.2.2022. http://www.urn.fi/URN:NBN:fi:jyu-201910184511

Tukiainen L. 2020. Organisaation pilvipalveluiden hallinta tietoturvan näkökulmasta. Informaatioteknologian tiedekunta. Maisterivaiheen työ. Jyväskylän Yliopisto. Viitattu 18.3.2022. http://www.urn.fi/URN:NBN:fi:jyu-202006043965

Pekkola, S. 2020. Digitalisaatio edellyttää kokonaisuuksien hallintaa. Tietojohtaminen, Artikkeli. Tampereen yliopisto. Tampere. Viitattu 17.23.2022. https://trepo.tuni.fi/bitstream/handle/10024/135776/Digitalisaatio_edellytt_kokonaisuuden_hallintaa.pdf?sequence=1&isAllowed=y

Rakennustieto Oy. Luettu 11.4.2022. https://www.rakennustieto.fi/yritys

Rousku, K. 2018. Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma. Valtiovarainministeriö. Viitattu 15.1.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161218/VM_32_2018_Julkisen_hallinnon_digitaalisen_turvallisuuden_kehittamisohjelma.pdf?sequence=1&isAllowed=y

Sonkor, M. & Garcia de Soto, B. 2021. ASCE Journal of Construction Engineering Management. Volume 147 issue 12. Joulukuu 2021. Luettu 1.2.2022. https://ascelibrary.org/doi/full/10.1061/%28ASCE%29CO.1943-7862.0002193

Sipilä, J. & Vehviläinen, A. 12.6.2015. Digitalisaatiolla tuottavuusloikka. Viitattu 17.3.2022. https://vm.fi/documents/10623/1464506/VM_1184_00-01-02-02_2015_avoin_kirje_digitalisaatiohaaste.pdf/bf2c3dda-13b7-4054-bf1f-b4803a7dd4a4

Sähkö- ja teleurakoitsijaliitto STUL ry. https://www.stul.fi/digiturvallinen-rakennus-18-5-2020-seminaari/ Luettu 1.3.2022.

Turva-alan Yrittäjät ry. Turvaa oikein-opas 2019. Viitattu 12.1.2022. https://www.turva-alanyrittajat.fi/doc/2019/Turvaa-oikein--opas_v2_0.pdf

Teknologiateollisuus ry. Digipooli. Rakennusten digitaalinen turvallisuus. Luettu 11.4.2022. https://www.digipooli.fi/fi/ajankohtaista/uutinen/rakennuksen-digitaalista-turvallisuutta-kasittelevat-ohjekortit-ovat

Turvaurakoitsijat ry. Luettu 18.3.2022. https://www.turvaurakoitsijat.fi/yhdistys/

Työ- ja elinkeinoministeriö 2015. Palvelutalouden murros ja digitalisaatio - Suomen kasvun mahdollisuudet. Elinkeino- ja innovaatio-osasto. Etlatieto Oy. Viitattu 1.2.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/74984/TEM-jul_12_2015_web_30032015.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö 2020. Julkisen hallinnon digitaalinen turvallisuus. Viitattu 1.4.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf?sequence=2&isAllowed=y

Valtioneuvoston julkaisuja 2019:31. (2019). Pääministeri Sanna Marinin hallituksen ohjelma 10.12.2019 Osallistava ja osaava Suomi. Viitattu 18.3.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161931/VN_2019_31.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö 2020. Julkisen hallinnon digitaalinen turvallisuus. Viitattu 1.4.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf?sequence=2&isAllowed=y

Valtiovarainministeriön julkaisu 32/2018. (2018). Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma. Viitattu 19.3.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf?sequence=2&isAllowed=y

Vehkalahti, K. 2014. Kyselytutkimuksen mittarit ja menetelmät. Finn Lectura: Helsinki. Painetun kirjan kanssa samansisältöinen on Helsingin yliopiston PDF-julkaisu 2019. https://helda.helsinki.fi/bitstream/handle/10138/305021/Kyselytutkimuksen-mittarit-ja-menetelmat-2019-Vehkalahti.pdf?sequence=1&isAllowed=y

YTNK 2016. Elinkeinoelämän yritysturvallisuusmalli. Elinkeinoelämän keskusliitto. Helsinki. Luettu 15.2.2022. https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf

Kuviot ja kaaviot

Liitteet

Liite 1: Teemahaastattelun kysymykset

1 Turvallisuusjärjestelmien suunnittelu

- Turvasuunnittelu liitetään osaksi hankkeiden muuta teknistä suunnittelua
- Turvallisuusjärjestelmien ja niihin liittyvien palveluiden omistajuudet tulee aina määritellä
- Turvallisuusjärjestelmien potentiaalia hyödyntämättä talotekniikan tukena olosuhdevalvonnassa
- Suunnittelussa huomioidaan fyysinen ja tekninen tietoturvallisuus (Physical and Technical Cyber Security)
- Muuta suunnittelussa huomioitavaa

2 Toimintaympäristö

- Turvallisuusjärjestelmien päätehtävät ja riippuvuudet tulee tunnistaa ja kuvata
- Kiinteistö – ja turvajärjestelmien arkkitehtuuri tulee kuvata ja arkkitehtuurista vastaava henkilö nimetä
- Järjestelmäympäristölle asetetaan yhteiset tekniset ja toiminnalliset tavoitteet koko rakennetussa ympäristössä (turvatekniikka ja talotekniikka)
- Järjestelmäympäristön tietoturvallisuusvaatimukset on asetettu koko rakennetun ympäristön järjestelmiin ja prosesseihin
- Muuta toimintaympäristössä huomioitavaa

3 Turvallisuusjärjestelmät

- Hankintaa/myyntiä ohjaa ajantasaiset suunnitteluohjeet ja vakioidut hankintamenettelyt
- Laitevalinnoissa/-tarjonnassa mahdollistetaan modulaariset skaalautuvat ratkaisut
- Hankinnan/myynnin ohjeissa huomioidaan etävalvonnan ratkaisut ja toteutustavat
- Suunnitteluohjeissa otetaan kantaa järjestelmien ja prosessien tietoturvaan
- Järjestelmien rajapinnat muihin järjestelmiin on tiedossa ja kuvattu
- Muuta turvallisuusjärjestelmissä huomioitavaa

4 Datan hyödyntäminen

- Turvajärjestelmiin liittyvät tekniset etävalvontapalvelut on käytössä/tarjonnassa
- Turvajärjestelmien dataa hyödynnetään jollain tavalla kiinteistön ylläpidossa tai turvallisuusvalvonnassa / palvelutarjonnassa
- Turvajärjestelmien dataa hyödynnetään ylläpidon tukena kiinteistön olosuhdevalvonnassa/ onko mukana tarjonnassa
- Datan omistajuudet, tietoturva ja tietosuojakäytännöt tunnistettava ennen hankintaa
- Muuta datan hyödyntämisessä huomioitava

5 Riskienhallinta

- Onko syytä tarkastella turvallisuusjärjestelmiä osana OT-järjestelmiä riskienarviointiprosessin näkökulmasta?
- Onko yrityksissä yleensä tai organisaatiossanne turvallisuusjärjestelmäympäristön kehittämisessä huomioitu koko OT-järjestelmäympäristön nopea digitalisoituminen?
- Onko yrityksissä yleensä tai organisaatiollanne kyvykkyys tunnistaa merkittävimmät kustannuksia aiheuttavat häiriötilanteet järjestelmäympäristössä?
- Onko yrityksissä yleensä tai organisaatioissanne riittävä näkyvyys OT-ympäristöön liittyviin kustannuksiin?
- Onko yrityksissä yleensä tai organisaatiossanne OT-järjestelmien häiriönhallintaprosessit kuvattu ja vastuutettu?

Asteikko:

täysin eri mieltä

jokseenkin eri mieltä

jokseenkin samaa mieltä

täysin samaa mieltä

Liite 2: Teemahaastattelun saateteksti

Hei,

olen tekemässä opinnäytetyötä Laurea YAMK:ssa. Minulla on työelämän kehittämishanke, jossa aineiston keruu tapahtuu haastatteluilla (N=7) sekä havainnoimalla.

ONT-aihe

- **Opinnäytetyön aihe käsittelee turvallisuusjärjestelmiä toimittavien yritysten kyvykkyysvaatimuksia vastaamaan rakennetun ympäristön nopean digitalisoitumisen tuomia mahdollisuuksia ja haasteita. Näkökulma on kehittyvät tietoturvalliset palvelut ja ratkaisut osana OT-järjestelmäkokonaisuutta. Teoreettinen viitekehys turvallisuusjohtaminen ja riskienhallinta. Kyse on uusien asiakokonaisuuksien johtamisesta.**

Opinnäytetyön otsikko: Digitalisaation vaikutukset turvallisuusjärjestelmäympäristön hallintaan.

Olen valinnut haastateltavien joukkoon turvallisuusjärjestelmien tilaajan edustajia ja aihealueen piirissä olevia asiantuntijoita eri kategorioista, jotka työnsä puolesta vastaavat joko palvelutoimittajien tuotteiden, palveluiden ja prosessien kehityksestä tai osallistuvat rakennetun ympäristön digitalisaation tuomien haasteiden ratkaisemiseen omalla tehtäväalueellaan.

Toivon siis, että ehdit antamaan n. tunnin mittaisen haastattelun ja laitan kysymykset ennakkoon, jotta pääsette tutustumaan aiheeseen. Haastattelut käydään Teamsillä.

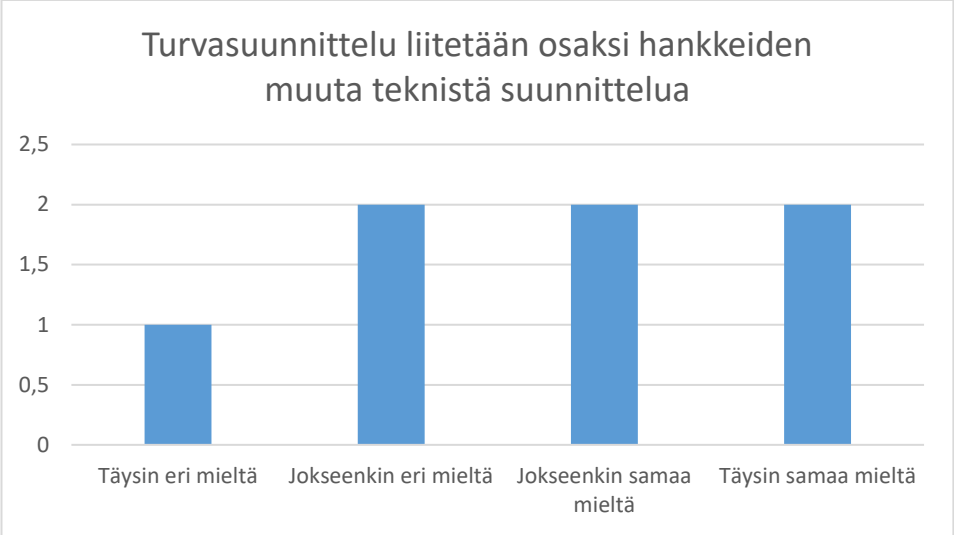
Jos haastattelu sopii teille, niin voitteko kuitata asian minulle niin olen teihin puhelimitse yhteydessä ja sovitaan haastatteluaika. Haastattelut pitää tehdä marraskuun 19. päivään mennessä. Mitä aikaisemmin niin sen parempi.

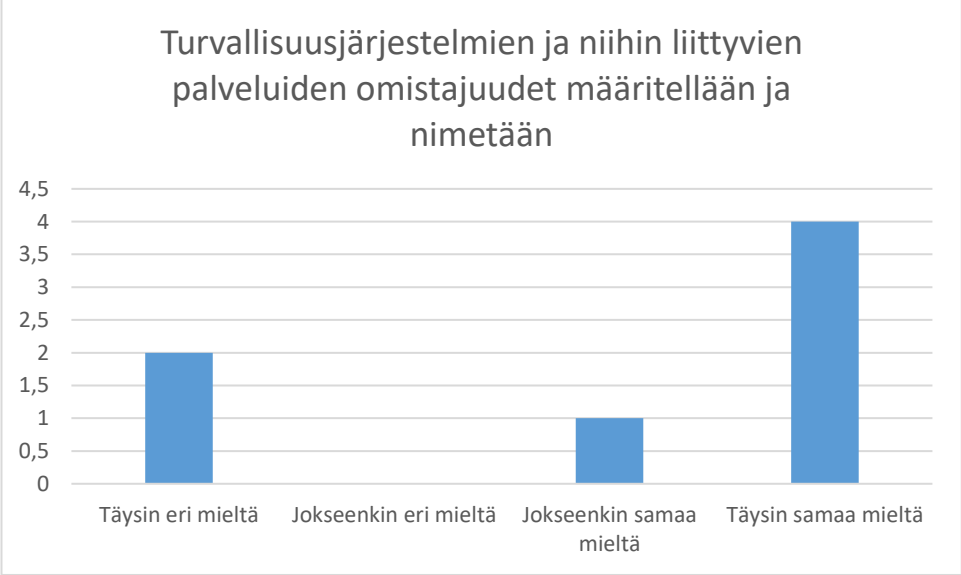
Mitä on OT:

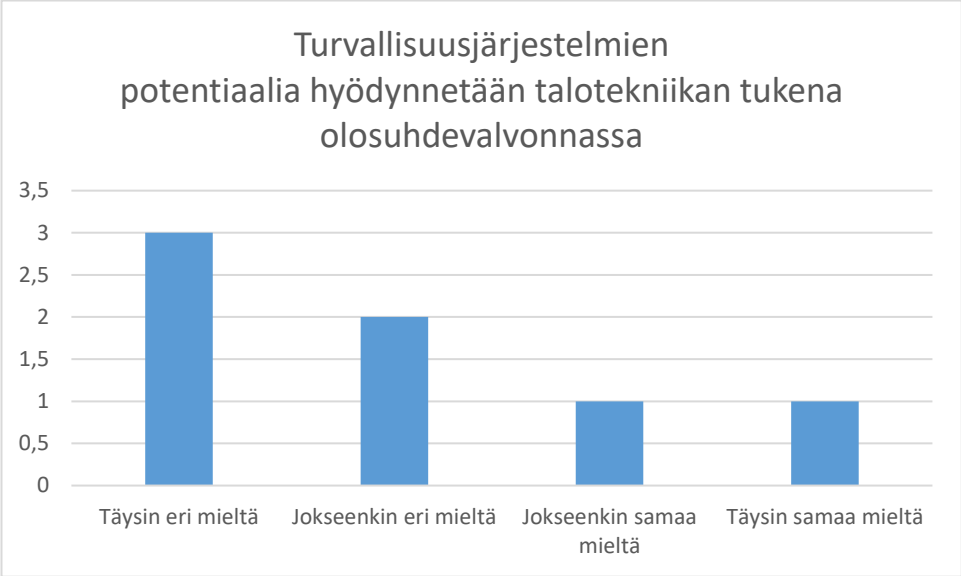
- *OT (Operational Technology) on järjestelmiä, laitteita ja ratkaisuja sekä prosesseja ja palveluita, joilla ohjataan rakennettua ympäristöä toimimaan sen määritellyn käyttötarkoituksen mukaisesti. OT toimii samoilla teknisillä alustoilla ja usein myös samanlaisissa verkoissa kuin IT-järjestelmät. OT-ympäristöön kytketään tyypillisesti useita erilaisia IoT-laitteita. OT-järjestelmät jäävät usein IT:n prosessien ulkopuolelle.*

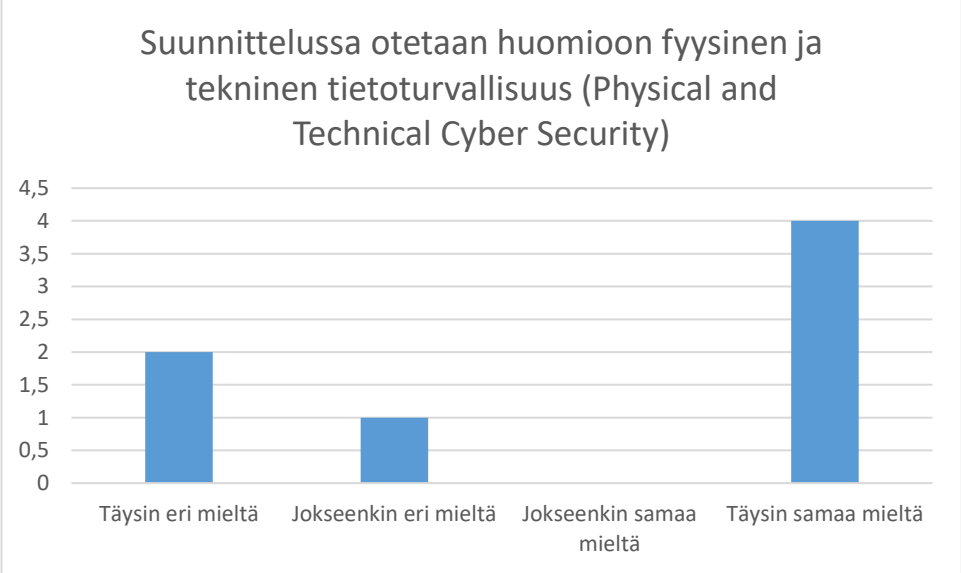
Liite 3: Haastatteluiden vastaukset graafeina

Turvasuunnittelu

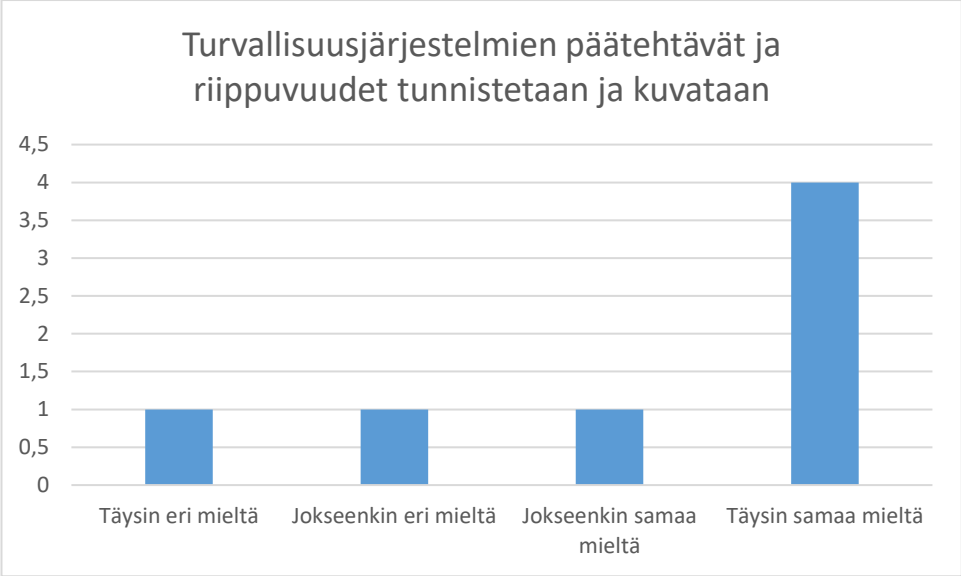


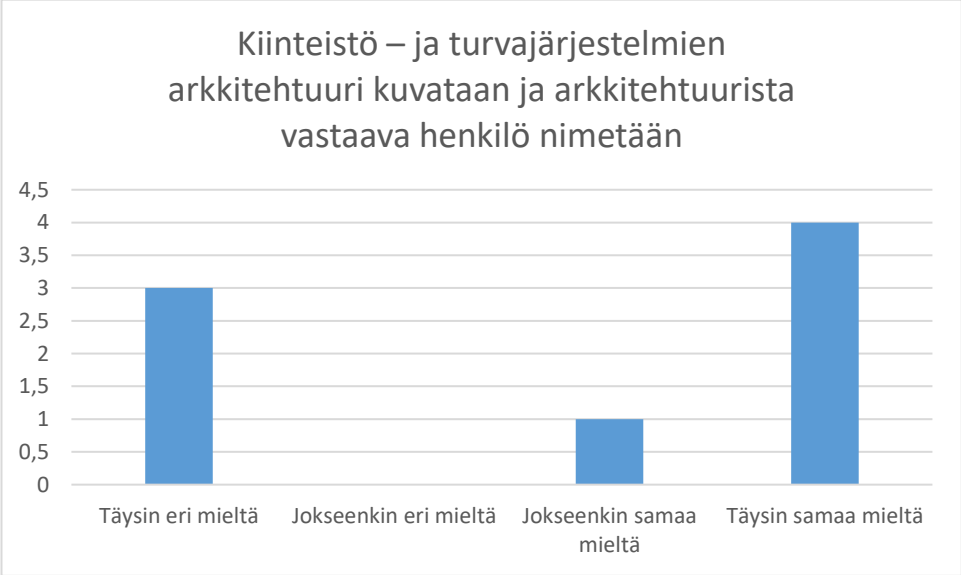



Turvallisuusjärjestelmien potentiaalia hyödynnetään talotekniikan tukena olosuhdevalvonnassa
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä

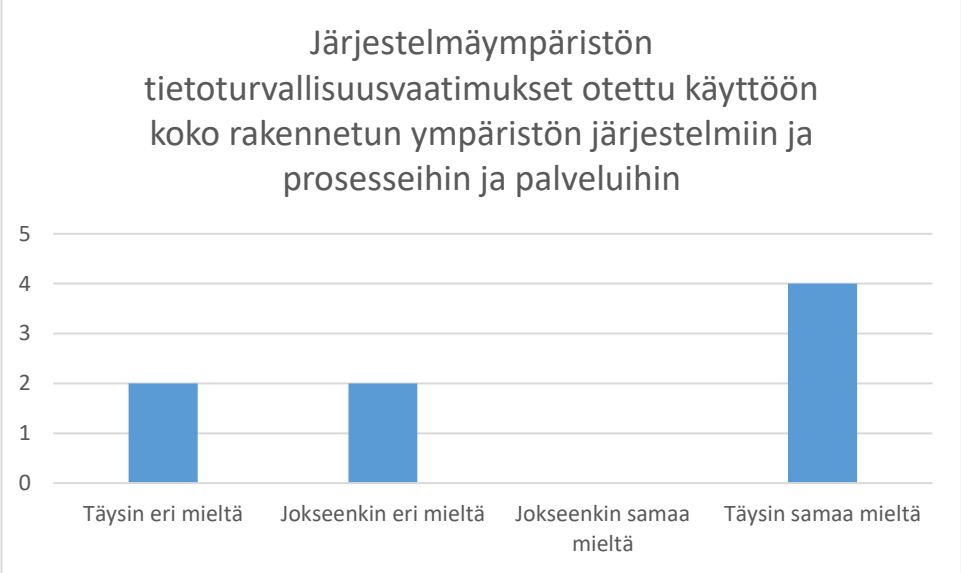

Suunnittelussa otetaan huomioon fyysinen ja tekninen tietoturvallisuus (Physical and Technical Cyber Security)
4,5
4
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä

Toimintaympäristö

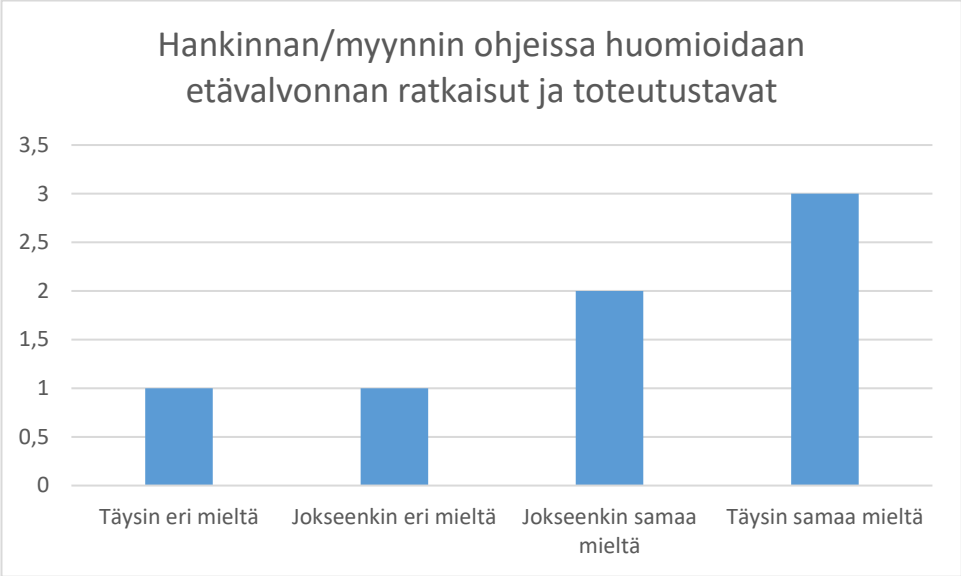




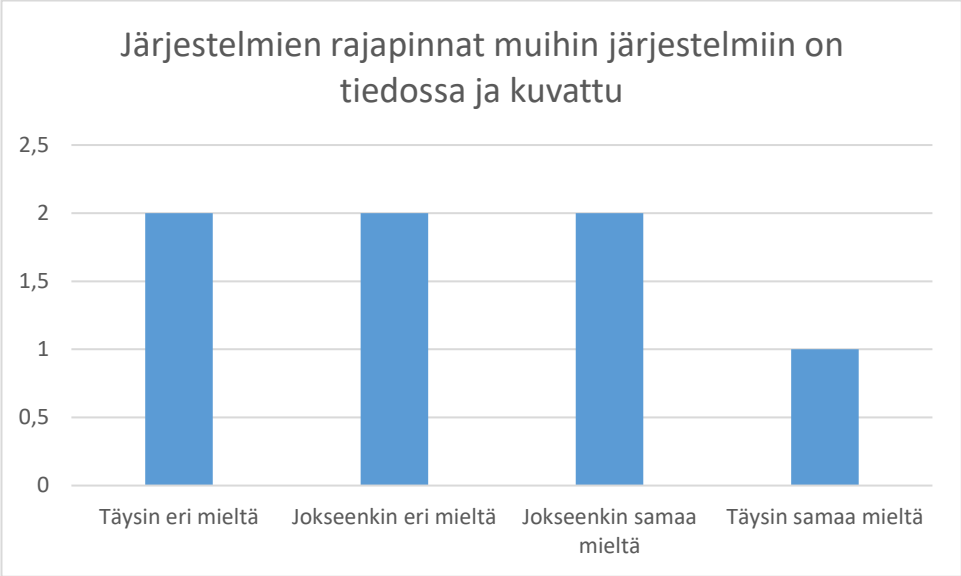

Järjestelmäympäristölle asetetaan yhteiset tekniset ja toiminnalliset tavoitteet koko rakennetussa ympäristössä (turvallisuustekniikka ja talotekniikka)
5
4
3
2
1
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä


Järjestelmäympäristön tietoturvallisuusvaatimukset otettu käyttöön koko rakennetun ympäristön järjestelmiin ja prosesseihin ja palveluihin
5
4
3
2
1
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä

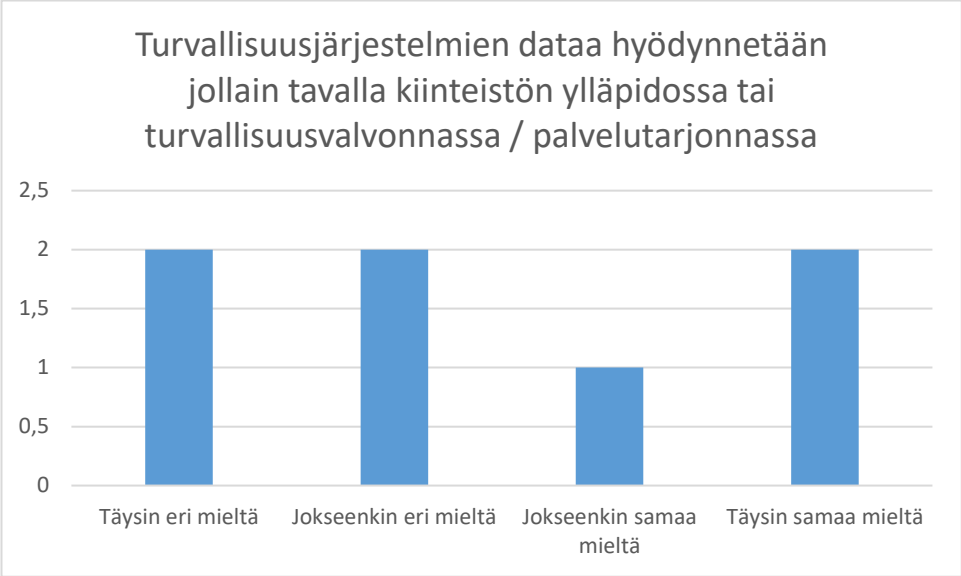
Turvallisuusjärjestelmät

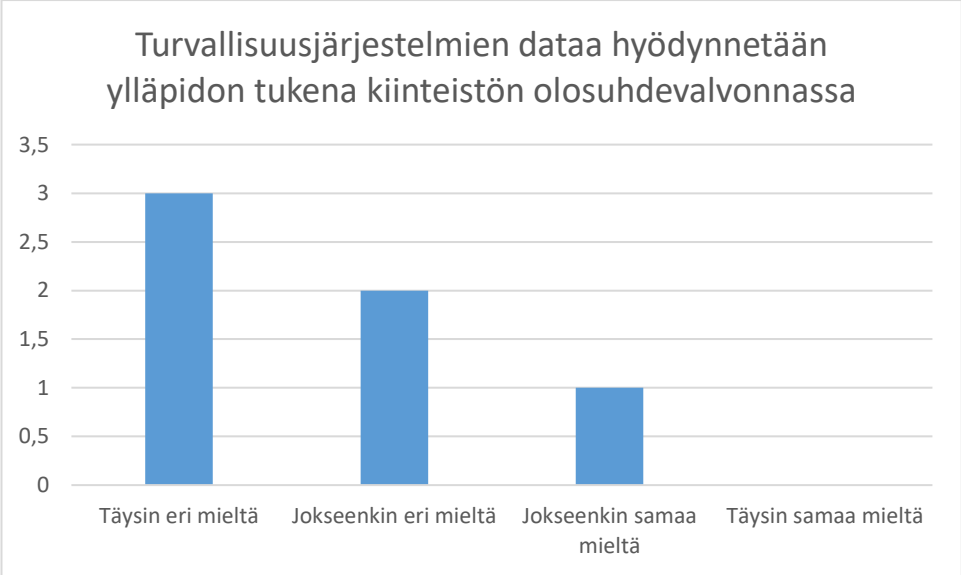

Hankinnan/myynnin ohjeissa huomioidaan etävalvonnan ratkaisut ja toteutustavat
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä

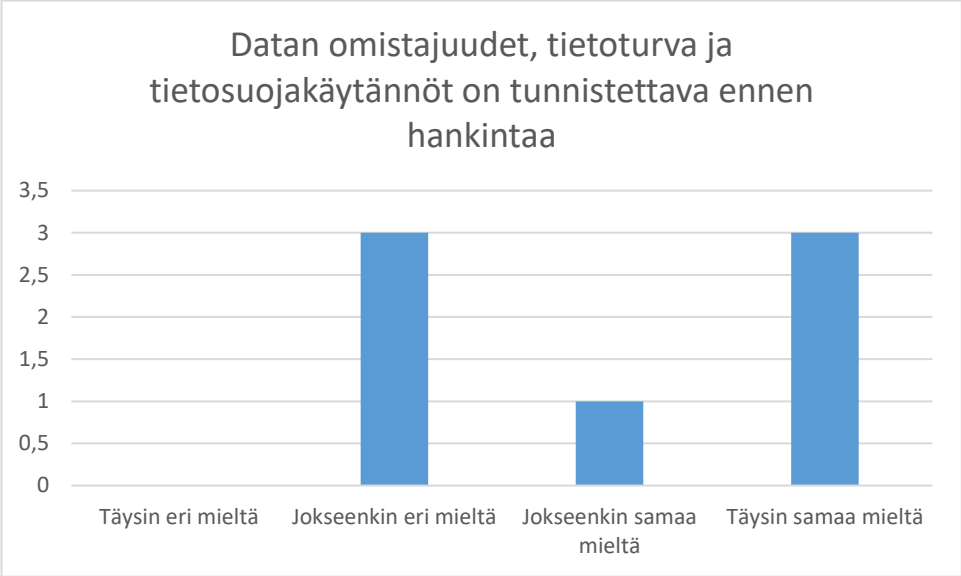

Suunnitteluohjeissa otetaan kantaa järjestelmien ja prosessien ja palveluiden tietoturvaan
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä



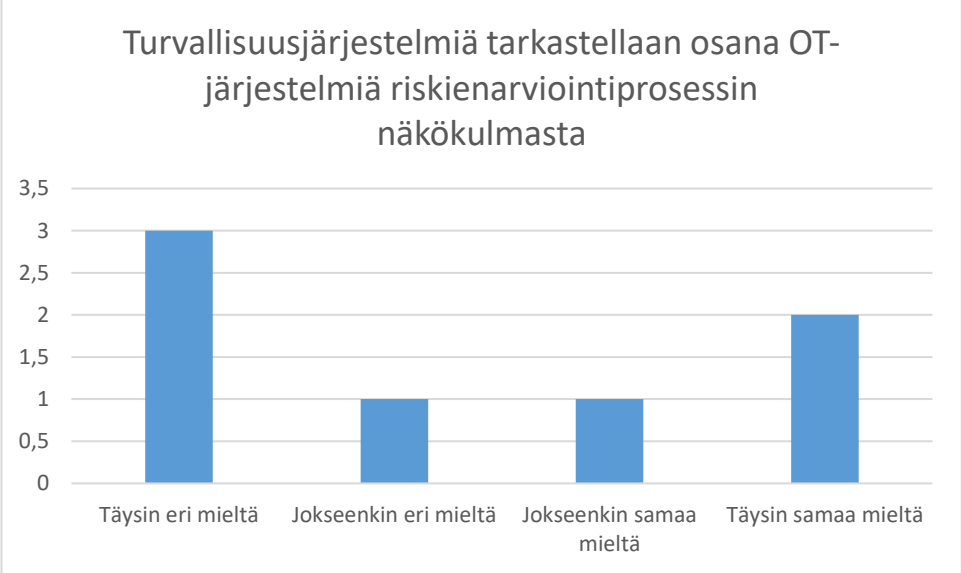
Datan hyödyntäminen

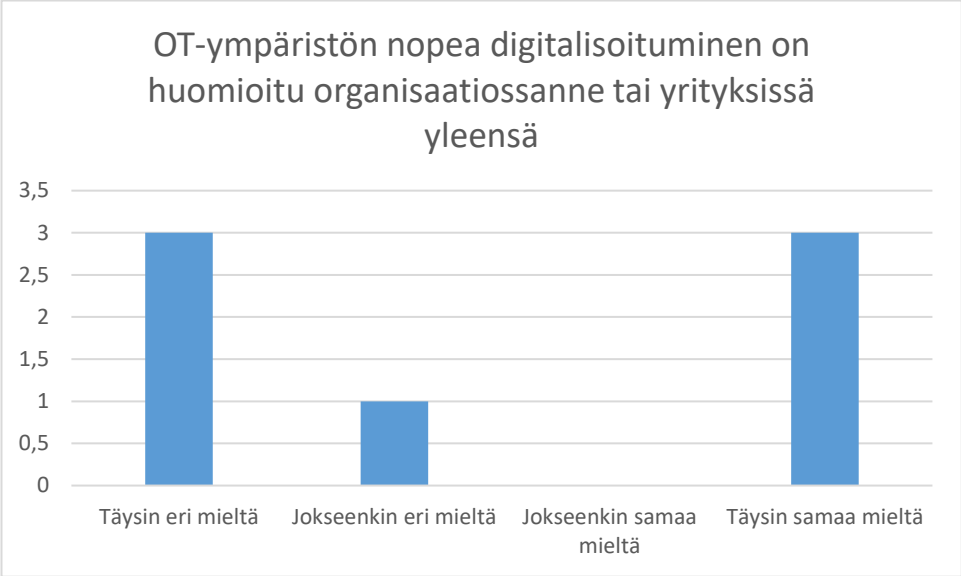

Turvallisuusjärjestelmien dataa hyödynnetään jollain tavalla kiinteistön ylläpidossa tai turvallisuusvalvonnassa / palvelutarjonnassa
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä


Turvallisuusjärjestelmien dataa hyödynnetään ylläpidon tukena kiinteistön olosuhdevalvonnassa
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä

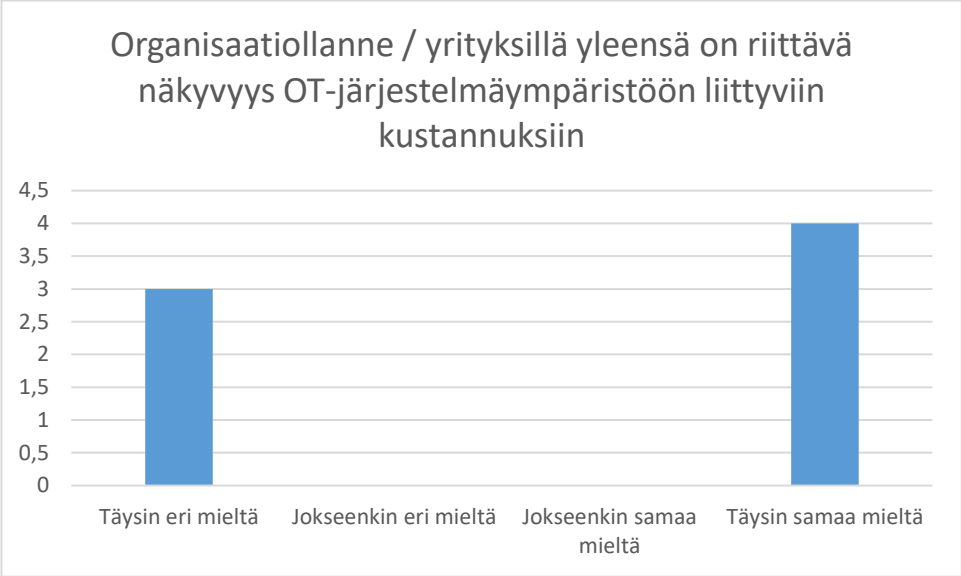


Riskienhallinta




OT-ympäristön nopea digitalisoituminen on huomioitu organisaatiossanne tai yrityksissä yleensä
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä


OT-järjestelmäympäristön merkittävimmät kustannuksia aiheuttavat häiriötilanteet on tunnistettu organisaatiossanne / yrityksissä yleensä
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä


Organisaatiollanne / yrityksillä yleensä on riittävä näkyvyys OT-järjestelmäympäristöön liittyviin kustannuksiin
4,5
4
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä


OT-järjestelmiin liittyvät häiriöhallintaprosessit on kuvattu ja vastuutettu organisaatiossanne / yrityksissä yleensä
3,5
3
2,5
2
1,5
1
0,5
0
Täysin eri mieltä
Jokseenkin eri mieltä
Jokseenkin samaa mieltä
Täysin samaa mieltä