

Janne Ollenberg

Verkottuneen talotekniikan tietoturva

Metropolia Ammattikorkeakoulu

Rakennustekniikka, YAMK

Talotekniikka

Korjausrakentaminen

Opinnäytetyö

15.5.2015

Tekijä Otsikko	Janne Ollenberg Verkottuneen talotekniikan tietoturva
Sivumäärä Aika	53 sivua + 1 liite 15.5.2015
Tutkinto	Insinööri, (ylempi AMK)
Koulutusohjelma	Rakennustekniikka
Suuntautumisvaihtoehto	Talotekniikka, Korjausrakentaminen
Ohjaajat	Lehtori Veijo Piikkilä Johtaja Timo Rasimus
<p>Rakennustekniikan alan YAMK-opinnäytetyössä selvitettiin verkottuneen talotekniikan toimijoiden odotukset ja vaatimukset tietoturvan perustason toteuttamiselle.</p> <p>Opinnäytetyön osana laadittiin yhteenveto, josta Sähkö- ja teleurakointiliitto (STUL) toimitti Sähköinfo Oyn toimesta ST-ohjeistuksen. Ohjeistus on yleinen menettelyohje, joka on saatavana Sähköinfo Oy:n kautta julkaisuna. Työhön sitotui laaja asiantuntijaryhmä, joka edusti 18:aa alan toimijaa tai kiinteistön omistajaa. Välillisesti työn tulokset tulevat näin vaikuttamaan kaikkiin kiinteistöihin pidemmällä aikavälillä.</p> <p>Työn toteuttamista varten STUL perusti tietoturvaryhmän, joka valmisteli ohjeistusryhmän työtä, asetti työlle ohjausryhmän ja kokoontui lopuksi arvioimaan tuloksia. Ohjausryhmän myötävaikutuksella järjestettiin toimialakohtaisia haastatteluja ja yritysvierailuita, joiden perusteella aineiston sisältö ja painotus arvioitiin. Opinnäytetyön osana tuotettiin aineisto, jonka pohjalta toimitettiin lopullinen ST-ohjeistus. Tuotettu ST-ohjeistus muodostunee alan viiteaineistoksi tietoturvallisuuden toimintaohjeena. Vastuunjakotaulukoita ja urakkamalleja tarkistettaneen ohjeen myötä vastaamaan uusia suosituksia. Hankintoihin ja kilpailutuksiin saadaan ohjeistuksesta viiteaineisto, joka hyödyttää sekä kilpailuttajia että urakoitsijoita, kun toteutukset nojautuvat yhteiseen määritelmään.</p> <p>Tietoturvallisuuden kehittäminen on jatkuvaa työtä, jossa tulee aktiivisesti pitää ajantasainen kuva vallitsevista riskeistä, torjuntamenetelmistä ja muusta tilannekuvasta sekä päivittää olevaa ohjeistusta tarpeen mukaan. Liitteenä oleva ohje on alku tietoturvallisuuden systemaattiselle toteuttamiselle verkottuneen talotekniikan alalla.</p>	
Avainsanat	Verkottunut talotekniikka, IoT, M2M, konsultointi, toiminnan muutos, teknologiavallankumous, tietoturvallisuus, energiatehokkuus, älykaupungit

Author Title Number of Pages Date	Janne Ollenberg Cyber Security of Networked Building Services 52 pages 15 May 2015
Degree	Master of Engineering
Degree Programme	Civil Engineering
Specialisation option	Civil Engineering and Building Services
Instructors	Veijo Piikkilä, Principal Lecturers Timo Rasimus, Director
<p>The Master's thesis studied what expectations and requirements the operators in networked building technology had for basic level information security.</p> <p>A broad expert group was nominated to work with this project. Therefore, the results of the project introduced in the thesis will affect all properties, at least indirectly, in the long term. In addition, an information security group was set up for the implementation of the results. For the thesis, a series of industry-specific interviews and company visits were arranged.</p> <p>The guidelines given in the thesis were approved in January 2015. Based on the guidelines, an ST instruction manual was published in April 2015. The ST instruction manual is expected to become an industry reference in the field of information security. The thesis can be used to adjust the liability distribution tables and contracts to reflect the new recommendations. Furthermore, the guidance gives mutually beneficial reference for both parties in procurement and tendering processes.</p> <p>Developing information security is a continuous effort, in which current risks, methods of control and circumstances as well as the information security guidelines are actively kept up-to-date. The guidelines presented in the thesis are the first systematic implementation of information security in a networked building technology.</p>	
Keywords	Building Construction technology, Internet Of Things; IoT, Machine to Machine, M2M, Networked Building Services, Change management, Revolution of technology, Cyber and data security, Smart cities

Sisällys

1	Johdanto	1
2	Tietoturvan kehitys	1
2.1	Hallinnollinen tietoturva	3
2.1.1	Tekninen tietoturva	4
2.2	Kyberturvallisuus	5
2.3	Tietosuoja	6
3	Verkottuneen talotekniikan tekninen kehitys	7
3.1	Väylätekniikat	8
3.2	Verkottuminen	9
3.3	Esineiden internet ja big data	10
3.4	Verkottuneen talotekniikan palveluliiketoiminta	12
4	Toimintamallien muuttuminen	14
4.1	Ympäristöarvot ja energiatehokkuuden toteuttaminen	15
4.2	Sähköverkon ohjaus	18
4.3	Tietoturvan hallintamenetelmät	21
5	Verkottuneen talotekniikan toimintaympäristö	23
5.1	Lainsäädännön ja käytäntöjen muuttuminen	23
6	Tietoturvallisuuden taustoja	24
6.1	Alan standardit ja viitekehykset	25
6.2	Verkottuneiden talotekniikkajärjestelmien ominaispiirteitä	25
1.1	Tietoturvan hallinnan periaatteet	27
1.2	Tietosuojan hallinta	28
7	Muutoksen johtaminen	29
7.1	Teollinen (teknologinen) vallankumous	31
8	Työskentelymenetelmät	32
8.1	Ohjausryhmätyöskentely	32
8.1.1	Ohjausryhmän kokoonpano	33
8.2	Kirjallisuustutkimus	33

8.3	Haastattelut	34
8.4	Ohjeistuksen koostaminen	34
8.5	Lausunnot ja arvioinnit	35
9	Ohjeistuksen toteutus	35
9.1	Arviointi ja lausuntomenetelmät	36
10	Tulokset	36
10.1	Hallinnollinen kattavuus	38
10.2	Tekninen kattavuus	38
10.3	Työn julkisuusarvo ja tiedottaminen	39
11	Yhteenveto	39
	Lähteet	41
	Liitteet	
	Liite 1. ST ohje 22, Verkottuneen talotekniikan tietoturva, sisällysluettelo	

1 Johdanto

Opinnäytetyö kuvasi ja tuotti ohjeistuksen verkottuneen talotekniikan tietoturvan perustason toteuttamiseksi. Työn tilaaja, Sähkö- ja Teleurakointiliitto ry toimii jäsenistönsä edunvalvojana ja ammatillisen osaamisen edistäjänä. STUL:n jäsenistöön kuuluu yli 3000 urakoitsijaa, jäsenyhdistystä ja alan oppilaitosta. STUL julkaisee omistamansa kustantajan, Sähköinfo Oy:n kautta mm. ST-kortistoa. ST-kortistoa käytetään työtapaohjeena ja viiteaineistona käytännössä kaikessa suomalaisten standardien mukaan toteutettavassa sähkö- ja telealan toiminnassa. Tietoturvaohjeistukselle on ollut tarvetta erityisesti verkottuneen talotekniikan alueella. Toimialalle ei ole aiemmin Suomessa luotu kattavaa ja yhtenäistä perustason ohjeistusta tietoturvakäytännöistä.

Opinnäytetyö on koostunut taustaselvityksistä, haastatteluista, ohjausryhmätyöstä ja vertaisarvioinneista. Haastatteluiden havaintoja on lainattu tekstiin taustoittamaan tehtyjä valintoja. Viitteettömät lainaukset ovat ohjeistustyön haastattelumateriaalin aineistosta poimittuja.

2 Tietoturvan kehitys

Haittaohjelmien teoria on kirjoitettu vuonna 1966 Neumanin tieteellisessä artikkelissa (Neuman, 1966). Ensimmäiset tietokonevirukset luotiin epäonnistuneen demonstraation seurauksena, kun silloisessa Arpanet-verkossa levinnyt virus aiheutti verkon kaatumisen 1970-luvun alussa (Dalakov). Tietokonevirusten kehittäminen lisääntyi PC-tietokoneiden saapuessa markkinoille ja 90-luvulla niitä tuotettiin jopa tuhannen tapauksen kuukausivauhdilla. Virusajan valtakauden tekijäprofiili kuvattiin CNN:n haastatteleman torjuntayhtiön johtajan mukaan seuraavasti: ”Lähes kaikissa tapauksissa tekijä on tietokoneorientoitunut 14–34-vuotias mies, jolla on krooninen epäonni tyttöystävien suhteen ja ystäväpiiri koostuu muista virusten tekijöistä. Virus on kuin digitaalinen graffiti heille” (Virus writers, 2003).

Ensimmäisiä laajasti fyysiseen maailmaan kohdistuneita ulkoisen toiminnan aiheuttamia haittoja Suomessa oli junaliikenteen pysäyttänyt paperiliitin VR:n ohjausjärjestelmässä (Klemmari pysäytti junaliikenteen, 1997).

Torjunta- ja valvontamenetelmien kehitystä ja käyttöönottoa edistävät useimmiten vasta toteutuneet ja julkisuutta saaneet tapahtumat. Vuosien saatossa näitä on sattunut mm. pankkiverkoston sulkenut epidemia (Tietokonevirus sulki Nordean konttoreita Suomessa, 2003), laajaan liikenteenrajaukseen johtanut SQL-injektio (CERT-fi varoitus 1, 2013), teollisuuden automaatiolaitteisiin kohdistunut Stuxnet (Ståhlberg, 2010) ja valtiollisten toimijoiden vakoiluverkot (Wikileaks - informaatiotosodan alku, 2011), (Echelon raportti, 1999).

Historiaa peilaten tietoturvan menetelmäkehitykseen ovat aina kulkeneet katastrofin kautta, ennen kuin on löydetty riittävät resurssit riskien haltuunottoon ja toimintatapojen muutokseen. Perinteisesti tietoturvaan kiinnitetään huomiota vasta, kun toimialalla on jo tapahtunut merkittäviä tietoturvaloukkauksia ja -puutteita. Esimerkiksi pankkialan menetelmät saivat PCI-auditointivaatimuksensa sen jälkeen, kun oli jo menetetty miljoonia luottokorttitietoja tietomurtojen yhteydessä eri puolilla maailmaa (TJX:ltä 45 M luottokorttitietoa, 2007). Samoin monien toimialojen riskitietoisuus on kasvanut vasta julkistettujen ja toteutuneiden tietoriskien kautta. Stuxnet (Ståhlberg, 2010) muutti tapaa suhtautua automaatioalan tietoturvauhkisiin. Suhtautuminen luottamukselliseen viestintään on muuttunut sen jälkeen, kun kansalliset tietovuodot ja tiedustelupalveluiden toimintavat (Wikileaks - informaatiotosodan alku, 2011) paljastuivat luottamuksellista asemaa käyttäneiden henkilöiden vuodettua tietonsa Wikileaks-sivuston kautta yleiseen tietoisuuteen. Laaja julkisuus korottaa tietoisuutta tietoturvan merkityksestä toiminnan jatkuvuuden suhteen ja näin parantaa lopulta kohdealueidensa tietoturvaa. Tietoturvan tason parantamiseksi on useimmiten tarvittu ja saatu laskettavissa oleva uhkaskenaario, ennen kuin on tehty investointeja uhkien torjuntaan.

Vuosien saatossa tapahtunut tietoisuuden kehittyminen tietoturvauhkien olemassaolosta on johtanut siihen, että toimintaympäristöissä varaudutaan aiempaa tarkemmin tietoturvallisuuden poikkeamiin. Järjestelmällisen menettelyn tueksi on laadittu erinäisiä standardeja ja suosituksia, joiden pohjalta voidaan olettaa organisaation tai yksittäisen asiantuntijan ymmärtävän toimialan viitekehykset ja toimivan hyvien käytäntöjen mukaisesti. Samoin toimialan kypsyystasosta riippuen osapuolet osaavat vaatia toisiltaan tietoturvaan liittyviä sopimusvelvoitteita. Erityisesti tietotekniikkaan painottuvissa hankinnoissa vaatimusmäärittelyt ovat usein arkipäivää, mutta siirryttäessä laajempiin kokonaisuuksiin, kuten rakennuttamisessa ja

kiinteistöhallinnassa usein käy, jää tietoturvan huomiointi usein pienemmälle painotukselle.

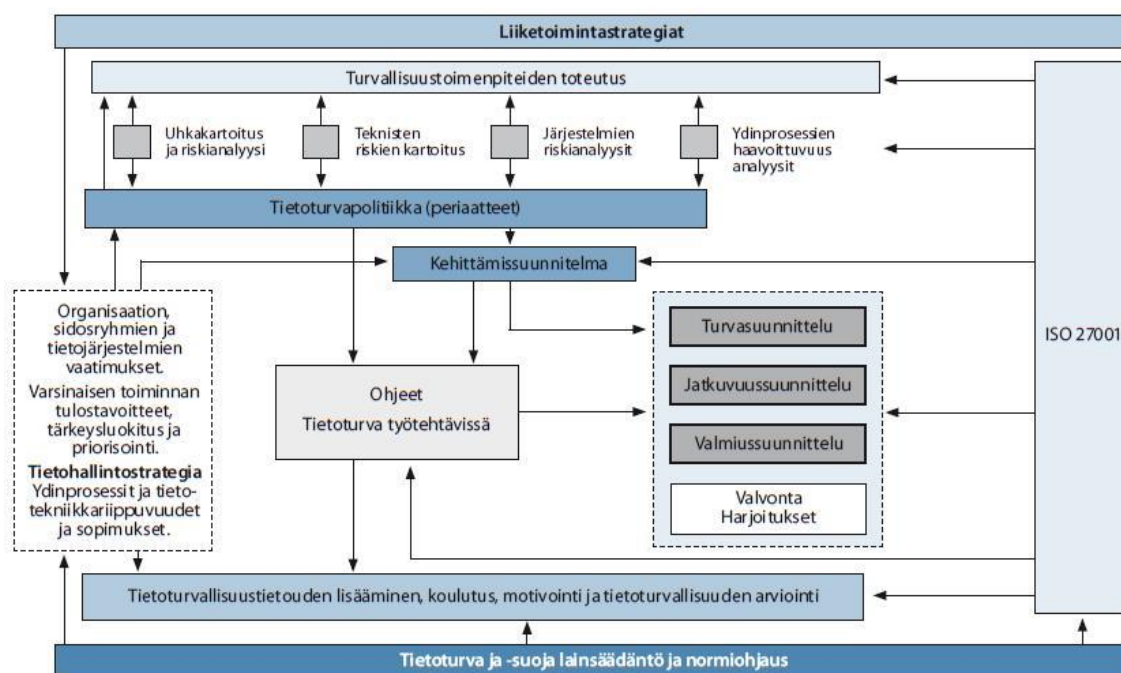
2.1 Hallinnollinen tietoturva

Yhteisön hallinnollista tietoturvaa on ryhdytty kehittämään useimmiten vasta siinä vaiheessa, kun on havaittu tietoturvauhan tai toteutuneen riskin olevan toiminnan jatkuvuuden kannalta kriittisellä tasolla. Hallinnollinen tietoturva tulisi ottaa kuitenkin strategiseksi menestymisen välineeksi ja yhteisöjen johtoryhmätasolle jo ennen kuin havaitaan ulkoisia uhkia. Teemahaastattelussa todettiin yleisen tietoturvan toteuttamiseen liittyvästä turvallisuusajattelusta, että "pitää erikseen korostaa, että turvallisuusdokumentit eivät saa kiertää yleisessä projektidokumentaatiossa".

Edelläkävijät saavuttavat tällöin helpommin markkinoiden luottamuksen ja kasvattavat markkinaosuuttaan. Ramboll on tehnyt Espoon kaupungin ja Uudenmaan ELY-keskuksen toimeksiannosta tietoturvallisuuden osaamisen kysyntään liittyvän kyselyhaastattelun (Tietotekniikka-alan osaamistarpeet, 2013). Tämän perusteella kysyntä korreloi tietoisuuden kanssa voimakkaasti ja erityisesti pitää huomioida havainto: "Osaamis- ja palvelutarpeet voivat muuttua verraten nopeastikin, esim. regulaation myötä tulevien mahdollisten uusien velvoitteiden kautta" (Tietotekniikka-alan osaamistarpeet, 2013).

Viime vuosina on muuttuvan lainsäädännön myötä kasvaneen tietoisuuden myötä alettu kiinnittää aiempaa enemmän huomiota esimerkiksi tietosuojan toteutumiseen ja yksityisyyden suojaan. Erityisesti valmisteilla oleva Tietosuoja-asetus (Tietosuoja-asetus pakottaa julkisyhteisöt muuttamaan toimintamallejaan, 2014) tulee todennäköisesti edistämään tietoisuutta organisaation vastuista hyvien hallintomenetelmien suhteen ja lisäämään alan parhaiden osaajien kysyntää.

Hallinnollisten menettelyiden tarkoituksena on tuottaa raamit yhteisön toiminnalle ja ohjata kehitystä kohti tavoitteena olevaa tasapainoa taloudellisten, tuotannollisten ja yhteiskunnan vaatimusten suhteen. Kuvassa 1 on esitetty vahtiohjeiston näkemys hallinnollisten menettelyjen ja lainsäädännön suhteesta varsinaiseen liiketoimintaan.

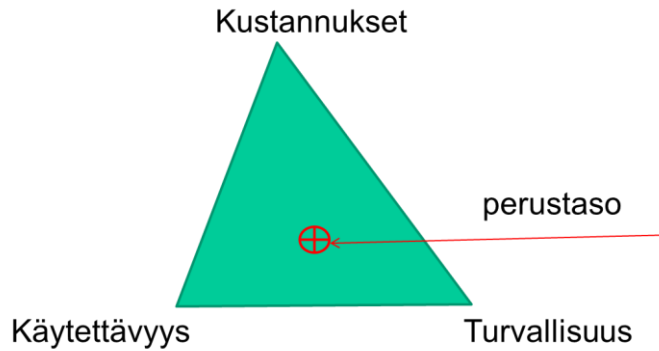


Kuva 1 Hallintomalli, (Vahti ohje; tietoturvallisuuden hallinnointimenetelmät, 2009)

Hallinnollisen tietoturvan menetelmiä ovat tietoturvastrategian, -politiikan ja -ohjeistuksen laatiminen ja riittävien resurssien hankkiminen tietoturvatyöhön. Hallinnollinen tietoturva kiinnittää tietoturvan osaksi yhteisön liiketoimintaa ja organisaatiota.

2.1.1 Tekninen tietoturva

Tekninen tietoturva tuottaa kohdejärjestelmälleen toiminnan kannalta riittävän käytettävyyden, luottamuksellisuuden, saatavuuden ja eheyden. Teknisen tietoturvan toteuttamista rajoittavat erityisesti käytettävyyksvaatimukset ja kustannukset. Tietoturvan optimaalista tasoa kuvataan usein kolmiolla, jonka kärjissä ovat tietoturvan taso, kustannukset ja käytettävyys. Pyrittäessä täydelliseen tietoturvaan, romahtaa käytettävyys, ellei samalla investoida. Opinnäytetyön osana toimitetussa ohjeistuksessa (ST ohje 2015) määritellään tietoturvan perustaso, joka antaa riittävän suojan kohtuullisella kustannustasolla.

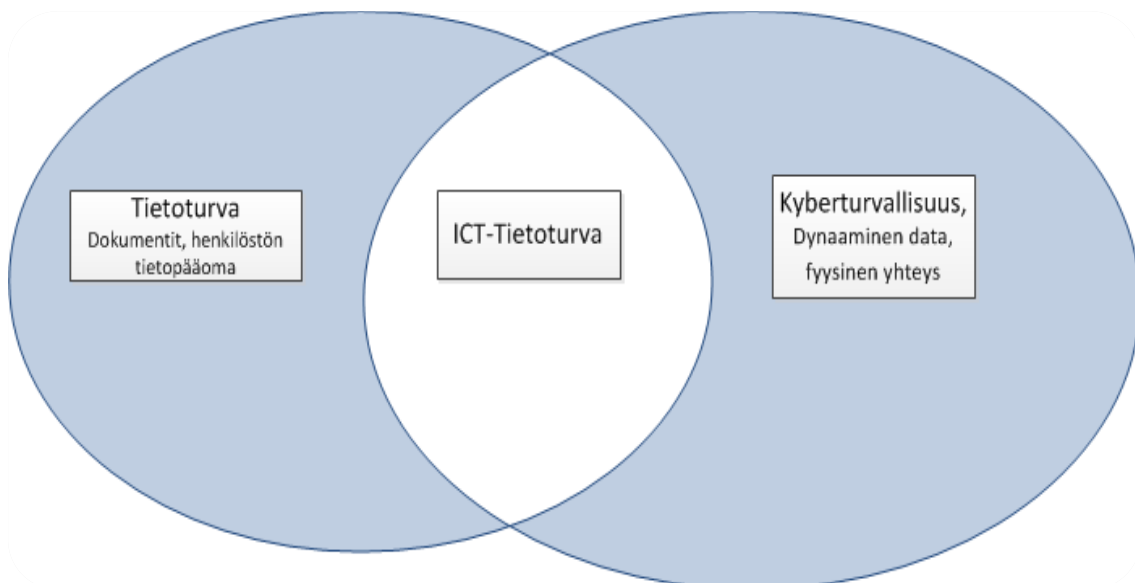


Kuva 2, turvallisuuden suhde käytettävyyteen ja kustannuksiin

2.2 Kyberturvallisuus

Digitalisaatio ja liitynnät fyysiseen maailmaan ovat laajentaneet tietoturvan kuvaamistarpeita perinteisistä malleista, ja tämän alueen termiksi on vakiintunut kyberturvallisuus (Cyber Security). Kyberturvallisuuden voi määritellä mm. seuraavasti: ”Kyberturvallisuuden lähtökohtana on yksilön tai yhteisön käyttämä digitaalinen maailma, jossa kukin toimija määrittää riskitasonsa ja riskinsietokykynsä sekä aktiivisesti seuraa ympäristön tilaa kehittäen toimintaansa muuttuvan todellisuuden mukaisesti.”

Kyberturvallisuuden suhdetta tietoturvaan voidaan vertailla kuvan 3 mukaisesti. Tietoturva-alueen muodostavat staattinen tietopääoma ja toisaalta tietojärjestelmät. Kyberturvallisuudella on myös yhteys ICT-tietoturvaan, minkä lisäksi sillä on oma reaaliaikainen maailmansa, jossa liikutellaan aktiivista dataa.



Kuva 3 Tietoturvan ja kyberturvan ryhmittely

Verkottuneeseen talotekniikkaan kyberturvallisuus kytkeytyy esimerkiksi yksittäisen anturitiedon kautta. Anturitietoa voidaan käyttää esimerkiksi huoneiston lämpötilan säätöön ja mittaukseen, jolloin anturitieto viedään osaksi laajempaa säätö- ja tilastointijärjestelmää. Tällöin mittaustieto rikastuu kohdetiedolla, joka on vaikkapa asunnon numero. Mittaustiedon kyberturvallisuus takaa anturitiedon muuttumattomuuden sekä saatavuuden varmistamisen, ja tietoturva takaa esimerkiksi luottamuksellisen henkilötiedon suojan. Mittaustiedosta muodostuu henkilökisteri, kun huoneiston numero on esimerkiksi osoitetiedon kautta yhdistetävissä yksittäiseen henkilöön. Teemahaastattelun yhteydessä kyberturvallisuuden haasteet kävivät ilmi mm. seuraavasta toteamuksesta: "Jokaisessa kenttälaitteessa voi olla oma siru, joka voi kommunikoida eri kohteiden kanssa, (laitteiden välistä) hallintaa ei ole toistaiseksi yleisesti määritetty." Lisäksi todettiin, että teknologiamuutokset edellyttävät laajaa ymmärrystä tietojen käytön hyödyntämisestä. "Uusi ja halpeneva teknologia mahdollistaa huoneistokohtaisen lämpötila- ja säätömittauksen, tällaisia asuntoja on jo otettu asiakkaille käyttöön."

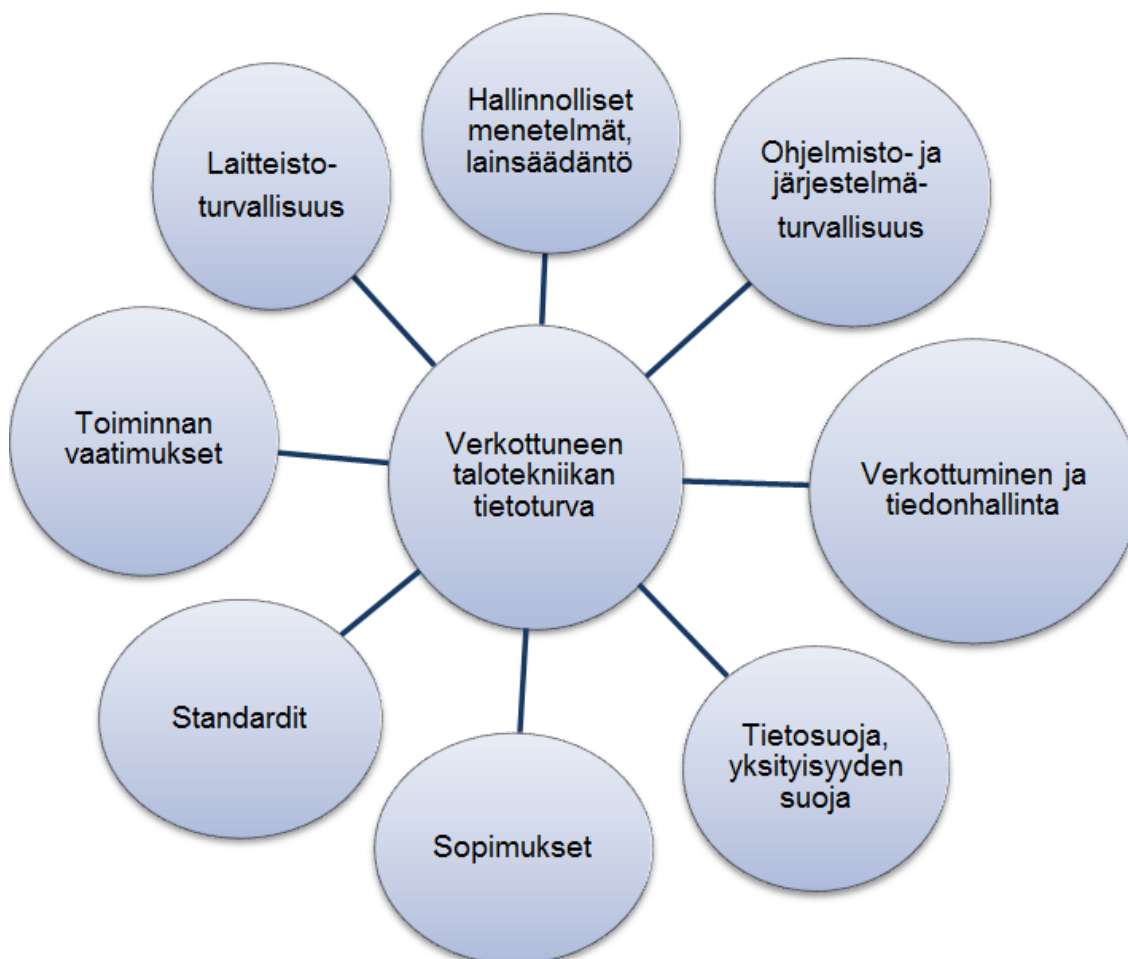
2.3 Tietosuoja

Tietosuoja on käsitteenä kehittynyt tietoturvan rinnalla. Tietosuoja (Työelämän tietosuoja, 2009) kohdistuu laadullisesti tunnistettavissa ja erotettavissa olevaan tietoon, joka kokonaisuudessaan muodostaa luottamuksellisen aineiston.

Tietosuojan piiriin katsotaan useimmiten kuuluviksi esimerkiksi yksityisyydensuojaan liittyvät rekisterit ja tiedot. Yleisellä tasolla tietosuojan haasteita ei ole aina ymmärretty, kun halutaan soveltaa uutta teknologiaa käyttöön. "Toimitilapuolella toivotaan jopa työpistekohtaista seuranta, joka menee helposti yksityisyydensuojan puolelle – kaikkea ei voida toteuttaa", todettiin teemahaastattelussa.

Tietosuojaan liittyvä lainsäädäntö on kehittynyt vuosien saatossa. Rikoslaisissa määrittellen yksityisyydensuojaan liittyvät salakatselu ja salakuuntelu. Lisäksi on useita huomioitavia lakeja ja asetuksia silloin, kun tarkastellaan henkilöön tai viestintään liittyvän tiedon luottamuksellisuutta ja käsittelyä. Eduskunta on valmistelemassa erillistä tietosuoja-asetusta, jonka valmistelevissa versioissa on esitetty varsin ankaria vastuuta yhteisöjen tietojenkäsittelylle tietosuojan näkökulmasta. Teemahaastattelussa todettiin, että verkottuneen talotekniikan tietoturvaohjeistus pitää jakaa useampaan päätasoon. "Tää pitäis osata jakaa eri kokonaisuuksiin ja palastella fyysiseen turvallisuuteen, hallinnolliseen turvallisuuteen ja ohjelmistoturvallisuuteen."

Kuvassa 4 on esitetty riippuvuuksia ja huomioitavia elementtejä, joiden avulla voidaan toteuttaa hallinnollisen ja teknisen tietoturvallisuuden vaatimukset, jotka ovat edellytyksiä tietosuojan toteutumiselle.



Kuva 4 verkottuneen talotekniikan tietoturvan elementtejä

3 Verkottuneen talotekniikan tekninen kehitys

Verkottuneen talotekniikan käyttöönotto on jatkumoa keskitettyjen analogisten ratkaisujen käytölle. Väyläpohjaiset järjestelmät ovat analogisia joustavampia ja mahdollistavat tilojen muutokset ja laajennukset (Paiho;ym., 2007). Analogisen kauden tuotteet olivat useimmiten kiinteästi johdotettuja valmistajakohtaisia ja suljettuja toteutuksia, joissa säätö tehtiin paikallisesti. Analoginen ympäristö on muuntojoustavuuden kannalta usein heikko. Monasti esimerkiksi tilamuutosten yhteydessä joudutaan kaapelointi uusimaan käytännössä kokonaan, jolloin työkustannukset nousevat merkittävästi.

Muuntojoustavuuden mahdollistamiseksi on luotu erilaisia väylätekniikoita, joissa kenttälaitteiden sijainti ja tehtävä väylän sisällä voidaan helposti muuttaa toiseksi. Tällöin useimmiten esimerkiksi kenttälaitteen jännitesyöttö ja ohjaussignaali erotetaan vähintään loogisesti toisistaan erillisiksi kokonaisuuksiksi. Väyläpohjaisessa toteutuksessa voidaan kohteen tilamuutosten yhteydessä tehdä ohjausmuutokset ilman uudelleenkaapeloinnin tarvetta. Voidaan siis esimerkiksi asettaa valaistuksen kytkimien toiminnalle uuden seinäjärjestelyn mukaiset valaistusalueet ohjattavaksi ja tämä sujuu usein ilman tarvetta uusia kaapelointeja. (Piikkilä, 2006)

Laajemmassa mittakaavassa väylätekniikalla mahdollistetaan eri toimintojen yhteisvaikutusten seuranta ja ohjaus. Kokonaisuuden hallinnan avulla rakennusta tai kiinteistökokonaisuutta voidaan hallinnoida yhtenäisesti. Tällöin voidaan hyödyntää kiinteistön ohjauksessa reaaliaikaisen mittaustiedon lisäksi ennusteita tai tilastollisia ohjausmalleja. Ennusteita hyödyntämällä voidaan tehokkaasti huomioida esimerkiksi rakennuksen käyttöennusteet, sääennusteet ja rakennusfysikaalisten ominaisuuksien vaikutukset, kuten massan hitaus lämmityksen ja jäähdytyksen suhteen.

Väyläpohjaisuus tuo mukaan useita etuja mm. järjestelmien etäkäytön ja maantieteellisen laajentamisen mahdollistajana. Toisaalta heikosti hallittu tietoturva voi estää etäkäytön kokonaan. Kehitys onkin muuttamassa kiinteistöt tietoteknisiksi kokonaisuuksiksi, joita on hallittava kuten tietojärjestelmää. Nykyiset käytännöt ohjelmistopäivitysten toteutusten suhteen vaihtelevat voimakkaasti asiakkaan lähtötasosta ja toimintaympäristöstä riippuen. Konsernitason toimijat hallitsevat ylläpitokäytännöt pieniä toimijoita paremmin. Ylläpitoa ja huoltoa ei välttämättä hankita kustannusten pelossa. "Laitepäivitykset automaatiojärjestelmissä saattaa olla heikosti hoidettu, voi olla kymmenen vuotta sitten asennettu käyttis, jota ei ole koskaan päivitetty."

3.1 Väylätekniikat

Väylätekniikoita on ollut ja tulee olemaan useita erilaisia. Osa tekniikoista on suljettuja ja valmistajakohkaisia. Joissakin tekniikoissa yhteysetäisyydet tai laajennettavuus on rajoittunut järjestelmän sisäisten ominaisuuksien vuoksi. Suljettujen ja rajoitettujen väyliä avuksi on tullut kattava joukko erilaisia mediamuuntimia, jotka voivat siirtää väylän signaalin esim. IP-verkon avulla seuraavaan kohteeseen.

Väylätekniikoiden yleinen rakenne koostuu

1. kenttälaitteista, jotka ohjaavat tai seuraavat varsinaista kohdetta
2. väylästä, jolla kenttälaitteet ja kontrollerit on kytketty toisiinsa
3. kontrollereista, joilla hallitaan kenttälaitteita
4. mahdollisista taustaväylistä, keskittimistä, reitittimistä ja mediamuuntimista.

Väylän tekninen rakenne ominaisuuksineen ja puutteineen pitää hallita silloin kun halutaan toteuttaa tietoturvallisuutta kokonaisuutena.

3.2 Verkottuminen

Osa väylätekniikoista tukee natiivisti tai laajennuksen kautta normaaleja TCP/IP-verkkoteknologioita ja yleisiä verkkoprotokollia. Useimpia yleiskäyttöisiä langattomia tiedonsiirtotapoja tuetaan myös. Mediamuunninten kautta on käytännössä aina mahdollistaa muuntaa liikenne kulkemaan normaalin tietoverkon kautta.

Ilmateitse siirtyvien signaalien puutteisiin havahdutaan usein vasta ongelmien tultua esiin. "Langattomien kenttälaitteiden käytöstä on luovuttu, kun on havaittu signaalin kulkevan rakennuksen ulkopuolelle." Signaalin kaappaamisen ja häirinnän lisäksi on mahdollista, että tiedon eheys menetetään, eli tietoa muutetaan siirtotiellä. Tämä saattaa keskeyttää tai haitata merkittävästi prosessin toimintaa. "Pitäisi puhua myös signaalin kaappaamisesta väylästä ja signaalin muuttamisesta."

Kuvassa 5 on esitetty tyypillisiä KNX-väylätekniikan alueellisia laajennuksia IP-verkon avulla. Kuvausten mukaisissa ratkaisuissa väylää voidaan laajentaa rakennusten välillä, internetin yli, väylästä etähallintapisteeseen tai KNX-väylän oman radiotaajuisen väylän avulla.

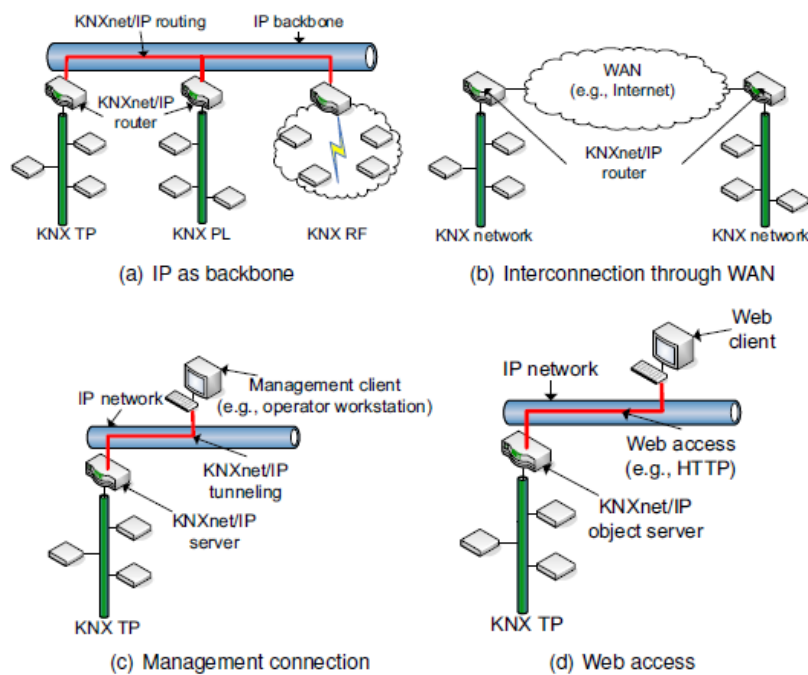


Figure 2: Using IP networks in KNX installations

Kuva 5, KNX-verkon rakenteita (Kastner s 4.)

3.3 Esineiden internet ja big data

Aalto-yliopisto on vuonna 2013 julkaissut raportin (Tiilikainen ym. 2013), jonka mukaan n. 185 000 tunnistettua automaatiolaitetta on avoimena verkossa. Näistä laitteista n. 3000 sisälsi tunnettuja tietoturvariskejä ja n. 1800 laitteistoa oli kokonaan suojaamatta julkaistua haavoittuvuutta vastaan tai muutoin käytettävissä etähallinnan kautta.

Laitteiden käyttökohteina oli mm. energiantuotantolaitos, vankilan rakennusautomaatiojärjestelmä, vedenkäsittelylaitos ja liikenteenvalvontajärjestelmä. Liikenne- ja viestintäministeriön julkaiseman Älykäs kaupunki palveluna -tutkimuksen (Majaniemi 2014) mukaan lähivuosina älykaupunkihankkeiden määrä tulee moninkertaistumaan nykyisestä tasostaan ja tätä myötä integraatioaste tulee kasvamaan verkottuneen talotekniikan sovelmissa. Tällöin on todennäköistä, että tietoisuus palveluiden tietoturvariskeistä kasvaa ja samalla kysyntä kohdistuu turvalliseksi koettuihin tuotteisiin.

Verkottuneen taloteknisen järjestelmän toteuttamisessa hyvän ennakkosuunnittelun merkitys korostuu. "Pitäisi saada tieto tilaajille ja suunnittelijoille, jotta nämä

osaisivat määritellä vaatimukset papereissaan." Lisäksi usein tilanne on se että tilaaja on eri organisaatiossa kuin yrityksen IT, jolloin voi tulla sekaannuksia ja tiedonkulun puutteita, kun verkottuneen taloteknisen järjestelmän tarpeita ei huomioida riittävästi ennakkoon muun infrastruktuurin suhteen. "IT tulee vasta mukaan kun talo- ja automaatioverkot on otettu käyttöön."

Vakiintuneiden toimintatapojen ja yhteisten toimintamallien puute vaivaa yleisesti toteutuksissa. Tietoturvan perusmääreet voivat olla olemassa yksittäisen valmistajan suosituksina tai suunnittelijan toimintatapana, mutta tieto ei välttämättä kulje tahojen välillä ja kilpailutuksissa ei osata vaatia alan parhaiden käytäntöjen toteuttamista. "Ei ole mitään yhtenäistä tapaa määritellä automaation tietoturvaa, jokainen toteutus on yksilö, myös saman tilaajan sisällä." Järjestelmien monimutkaisuus ja vaihteleva termistö asettaa myös haasteensa, viestinnässä osapuolten kesken on ajoin vaikeuksia. "On myös niin päin ongelma, että toimittajat eivät osaa kertoa asiakkaalle mitä tarvitaan." Alan yhteisestä tietoturvan perustason määrittelystä toivotaan ratkaisua, jolla saadaan vakioitua toimintamallit osapuolten välille. "Yhteinen toimintamalli tavoitettavissa oleva asia."

Monet laitevalmistajat ja johtavat ohjelmistotuottajat ennustavat esineiden internetin (Internet of Things, IoT) jakelun laajenevan 2020-luvulla koskemaan käytännössä kaikkia sähkötekniisiä laitteita. Samsung on ilmoittanut varustavansa kaikki myymänsä laitteet internet-yhteydellä vuoteen 2020 mennessä. Verkkolaittevalmistaja Cisco on arvioinut internet-liittymien määräksi 5×10^{12} vuonna 2020, mikä tarkoittaisi n. 150 internetiin kytkettyä anturia jokaista internetiin liittynyttä henkilöä kohden. Ohjelmisto- ja konsultointiyhtiö IBM on esittänyt Cison kanssa yhteneviä lukuja.

Verkottunut talotekniikka koetaan raporteissa erääksi keskeiseksi integraatiopisteeksi esineiden internetissä. Laitteet voivat olla yhteydessä toisiinsa ja kerätä toteutumien kautta ennustedatata, jolla on merkitystä esimerkiksi kohteiden energiatalouteen. Tiedon kerääminen ja hallinnointi tulee olemaan merkittävässä asemassa tulevaisuuden väyläjärjestelmiä suunniteltaessa (Zikopoulos 2015). Laaja-alaisen tietojen hyödyntäminen edellyttää avoimuutta ja tietojen vaihtoa eri tuottajien välillä, jotta uuden teknologian mahdollisuudet voitaisiin hyödyntää laajasti. "Suljetut järjestelmät hidastavat kehitystä."

Tietojen käsittely, yhdistäminen ja kokonaisuuden hallinta koetaan merkittävimmäksi osaamiskapeikoksi digitalisaation kehittämisessä Suomessa. Esimerkiksi ICT 2015 -työryhmä toteaa tiedon määrän kasvavan valtavaksi ja tiedon analysoinnin ja jäsentämisen taidon nousevan merkittäväksi kilpailueduksi lähivuosina. Työryhmän mukaan tietoturvasta tulee huolehtia tietojenkäsittelyn kaikilla tasoilla aiempaakin tarkemmin ja järjestelmä- ja ohjelmisto-osaaminen nousee kansalliseksi menestystekijäksi (Neittaanmäki ym. 2014).

3.4 Verkottuneen talotekniikan palveluliiketoiminta

Verkotetun talotekniikan mahdollistamat palvelumarkkinat tulevat kasvamaan merkittävästi lähivuosina (Majaniemi 2014). Tällöin palvelutuotannon edellytyksenä tulee olemaan nykyistä laajempi integraatioaste eri tuottajien käyttöympäristöjen välillä, jolloin tultaneen yleisesti edellyttämään vähintään verkottuneen talotekniikan perustason tietoturva-vaatimuksia. Verkottuneiden järjestelmien toiminnan edellytyksenä on riittävä ja aktiivinen ylläpito. Alan urakoitsijoiden ja palveluntuottajien tulee huolehtia siitä, että kuluttajilla on käytettävissään riittävät palvelut ja tiedot laitteiden ylläpitoon. "Käyttäjä ei osaa välttämättä kysyä tai kyseenalaistaa toimintoja. Ongelmaan havahdutaan vasta kun laite ei enää toimi ollenkaan." Yritystason toimijoidenkin tulee varmistua riittävän ammattitaidon saatavuudesta järjestelmän huoltoon ja ylläpitoon. Sopimusten lisäksi kriittisten järjestelmien osalta tulisi ajoittain testata jatkuvuuteen liittyvien palveluiden ja varaosien saatavuus. "Ammattitaitoinen päivystys ja vasteajat ovat haasteellisia jopa pääkaupunkiseudulla." Järjestelmien ostajilla ja myyjillä tulisi olla riittävä ymmärrys kokonaisuuksien toiminnasta, jotta voidaan arvioida järjestelmien käyttöönoton mielekkyys kohteen elinkaari ja järjestelmän käyttöikä huomioiden. "Vaatusmallien puuttuessa saatetaan hankkia vanhentuvaa tekniikkaa. Saattaa olla viisi vuotta vanha talo, jonka järjestelmiin ei saa enää laajennuksia." Verkottuneiden taloteknisten järjestelmien käyttöönotossa tulee korostumaan laaja-alainen ymmärrys kokonaisuuden soveltuvuudesta käyttötarkoitukseensa, ja riippumattomien konsulttien palveluille tulee olemaan kysyntää asiakkaiden ja urakoitsijoiden edunvalvojina.

Verkottuneen talotekniikan järjestelmät tulevat olemaan keskeisessä roolissa IoT-viitekehityksessä, jonka piirissä arvioidaan olevan maailmanlaajuisesti lähteistä riippuen 15-26 miljardia laitetta vuonna 2020 (Garthner 2015). Perinteisten järjestelmien rinnalle tai yhteyteen tullaan liittämään sensoreita ja antureita, jotka keräävät ja hyödyntävät

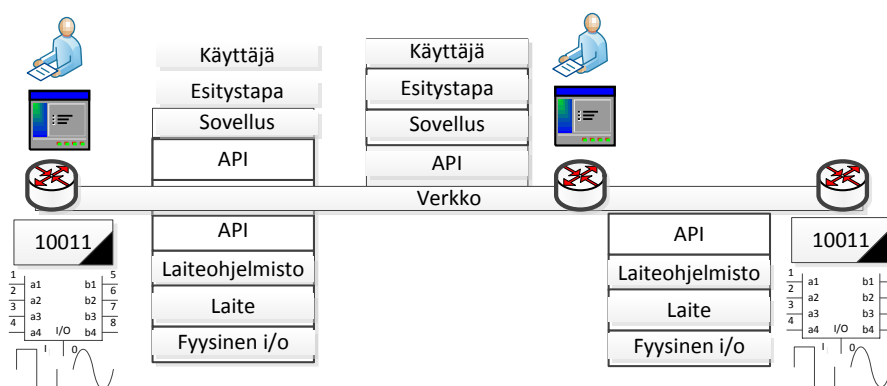
muiden laitteiden tietoja. Esineiden internetin arvo Suomessa vuonna 2020 on n. 1,4 miljardia euroa ja suurin kasvu syntyy analytiikasta, sovelluksista ja palveluista (Neittaanmäki ym. 2014, s 12).

Palveluliiketoiminta tulee kehittymään monin tavoin IoT-järjestelmien käyttöönoton myötä. Esineiden internet mahdollistaa esimerkiksi ennakoivan säädön ja huollon monille perinteisille verkottuneen talotekniikan osa-alueille. 2020-luvulle tullessa laitteiden väliset M2M (Machine to Machine, laitteelta-laitteelle) -yhteydet tulevat lisääntymään IoT-laitteiden tapaan eksponentiaalisesti. Laitteiden välinen telemetria tapahtuu useimmiten seuraavien tapahtumien kautta:

1. tiedon kerääminen
2. suodatetun tiedon lähettäminen verkon yli
3. tiedon analysoiminen
4. toiminta analysoidun tiedon pohjalta

Telemetria tulee avoimien rajapintojen kautta yleistymään ja arkipäiväistymään etenkin kuluttajatuotteissa. Rakenteellisesti kokonaisuuden hallinnan kannalta tulee olemaan merkityksellistä, käytetäänkö laitteiden välisessä liikenteessä kerrostamista. Mikäli kerrostamista käytetään, voidaan laitteet segmentoida ja suorittaa vuon valvontaa ja segmentointia eri laitteiden välisessä liikenteessä.

Kuvassa 6 on esitetty periaatteellinen toteutus laitteiden välisestä kommunikoinnista. Hyvin tehdyssä ympäristössä kommunikointi tapahtuu laitetason yläpuolisissa kerroksissa välttämällä laitteiden välistä suoraa kommunikointia, jolloin liikennettä on mahdollista valvoa verkkokerroksessa.



Kuva 6, Verkottuneen talotekniikan kerroksia

Verkottuneen talotekniikan toimintaympäristössä erotellaan nykyisellään useimmiten kiinteistö-, rakennus- ja taloautomaatio sekä kotiautomaatio. Lisäksi erotellaan turva- ja av-verkot. Esineiden internet ja digitalisaation kehitys tulee kuitenkin hämärtämään raja-aitoja nopeasti nykyisten toimintamallien väliltä. Eri laitteet liittyvät verkottuneissa ympäristöissä toisiinsa vähintään tietojen hyödyntämisen avulla sovelluskerroksen kautta, ja monissa tapauksissa pyritään käyttämään myös jaettuja laitteita, kuten yhteisiä liiketunnistimia. Kotiautomaation kehittyminen tulee myös näyttämään merkittävää osaa verkottuneen talotekniikan palvelutuotannon kehitymisessä, kun kotiautomaation kenttälaitteiden tietoja voidaan hyödyntää ja jopa ohjata verkottuneen taloteknisten järjestelmien avulla. Ensimmäisiä verkottuneen talotekniikan ja kotiautomaation välisiä yhteyksiä nähtäneen sähkön kysyntäjoustoon liittyvissä sovelluksissa, kun ohjataan kulutuselektroniikkaa optimaaliseen käyttöön energian hinnan ja kohteen käyttöhistorian suhteen.

Uudis- ja korjausrakentamisen trendejä ovat laajempien ja valmiimpien kokonaisuuksien hankkiminen ja laatuvaatimusten korostaminen hinnan sijaan. Myös korjausrakentamiseen on tulossa palvelumalleja (Pirainen ym. 2015). Alianssimalleille on kysyntää sekä uudisrakentamisessa että korjaushankkeissa. Näin tilaaja pystyy helpommin edellyttämään laatutekijöiden huomiointia koko rakennushankkeelta. Alianssimallissa osapuolet sitoutuvat yhteisiin tavoitteisiin aikataulun ja laadun suhteen ja jakavat yhteisesti sanktiot ja bonukset, jolloin yhteistoiminta rakentamisen eri osapuolten kesken on sekä luontevaa että palkitsevaa. Toiminnan jatkuvuuden kannalta pitää kaikkien sopimusmallien suhteen arvioida, ovatko huolto- ja ylläpitojärjestelyt riittäviä siirtotien kerrosten komponenttien ja kokonaishallinnan osalta, kun huomioidaan kohteen käyttövaatimukset (tilakeskus, 2005).

4 Toimintamallien muuttuminen

Verkottuneen talotekniikan monet toimitusympäristöt ovat kehittymässä perinteisestä rakennuttaja-urakoitsija-mallista erityyppisiä palveluliiketoiminnan muotoja kohden. Pohjoismaissa on meneillään useampia isoja elinkaarihankkeita, kuten Karoliininen sairaala Ruotsissa. Näissä hankkeissa rakennuttaja vastaa kohteen ylläpidosta kymmeniä vuosia ja tällöin käyttökustannusten ennakointi ja taloudellinen hallinta muodostuvat kannattavuuden suhteen merkittäviksi kokonaisuuksiksi. Elinkaarihankkeissa onkin nähty toteutuksia, joissa on yhdistetty sekä rakentamisen

tietomallinnusta (Building Information Modeling, BIM), että verkottunutta talotekniikkaa rakennusten säädön ja huollon optimoimiseksi.

Sopimusmallit hakevat muotoaan ja monasti käy niin, että laajassa rakennuttamishankkeessa noudatetaan yleisiä urakoinnin ja konsultoinnin sopimusehtoja, vaikka verkottuneen talotekniikan osalta olisi luontevampaa käyttää IT-sopimus pohjia. "Pelkkä rakennusurakkasopimus ei ota kantaa miten toimitaan urakan päättymisen jälkeen." IT-sopimusmalleja käytetään nykyisellään silloin, kun urakan tai toimituksen kohteena on selkeästi pääosin verkottuneeseen talotekniikkaan liittyvä järjestelmä. "Tietotekniikkapuolen sopimusmallit ovat parempia, kun kyseessä on puhtaat järjestelmätoteutukset."

"Alakohtaisia sopimusmalleja ei ole, lähinnä kattojärjestöt suosittelevat menetelmiä."

Sopimusmalleihin kaivataan selkeyttä alan tunnettavuutta ja yhteisiä menetelmiä kehittämällä. "Yhteistoiminnan ja pelisääntöjen sopiminen helpottaisi yhteistyötä yritysten tietohallintojen kanssa – yhteinen ohjeistus vähentäisi päällekkäisten järjestelmien tarvetta ja nopeuttaisi käyttöönottoja." Yhteisen toimintamallin luonti esimerkiksi tarkistuslistojen ja auditointimenetelmien muodossa edistäisi haastatteluun osallistuneiden mukaan tietoturvan huomiointia. "Pitäisi löytää yhteinen alusta toteuttaa ratkaisuita ja yhteiset pelisäännöt toteuttaa ratkaisuita." Samoin vakiintuneet käytännöt palvelisivat yleisesti markkinoita, kun ymmärrys tavoitetilasta olisi konkreettisempi esimerkiksi kilpailutuksissa. Nykyisellään vaatimustasot vaihtelevat paljon. "Ei ole yhtenäistä vaatimustasoa, teollisuudessa ja yrityksillä selkeämpi tahtotila kuin asuntorakentajilla ja käyttäjillä, vaatimustasot vaihtelevat hurjasti."

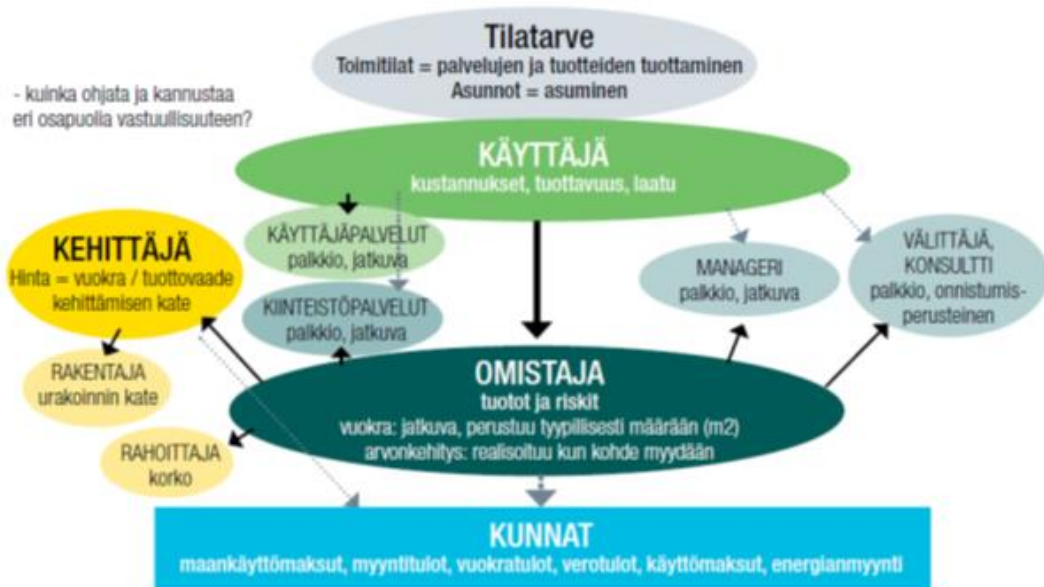
Sopimusriskien osalta tulee huolehtia siitä, että hallinnointikumppani sitoutuu luottamuksellisuuteen ja riittävään taustaselvitykseen henkilöstönsä osalta sekä käyttää hyväksyttäviä työskentelymenetelmiä. Erikseen tulee määritellä avustusvastuut ja velvoitteet tietojen siirrossa sopimuskauden päättyessä.

4.1 Ympäristöarvot ja energiatehokkuuden toteuttaminen

Ympäristölainsäädännön kehittyminen, kasvavat energiansäästövaatimukset ja yhteisöjen tavoittelemat vihreät arvot tuovat tarpeita energiatehokkuuden lisäämiselle ja kestävän kehityksen suosimiselle. Rakennusmääräysten johdosta kasvatetut

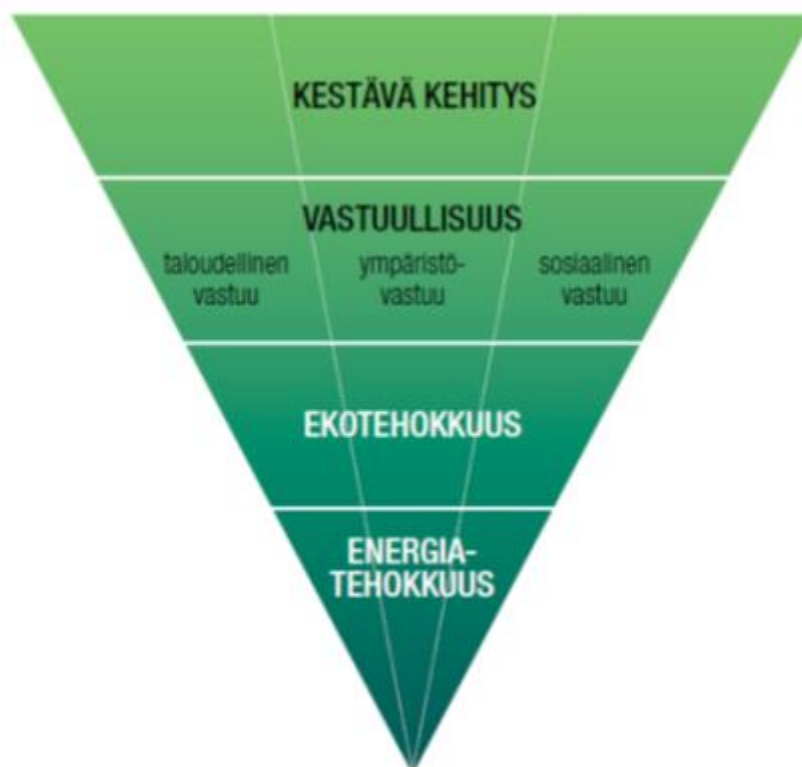
eristepaksuudet ovat jo käytännössä saavuttaneet taloudellisen huippunsa ja lisäsäästöjä on taloudellisessa mielessä järkevällä tavalla merkittävästi saavutettavissa rakennusten toiminnan suunnitteluun ja käytön aikaiseen säätöön panostamalla.

Rakennetun ympäristön vaikutus kansantaloudelle on merkittävä: 20 % kansantuotteesta ja 25 % työllisyydestä muodostuu rakennettuun ympäristöön liittyvän liiketoiminnan kautta. Suomen tuottamista päästöistä noin 35 % ja energiankulutuksesta noin 40 % tulee rakennetusta ympäristöstä. Kuvassa 7 on esitetty Kiinteistöliiton näkemys alan palveluketjuista ja toimijoista. Kiinteistöjen teknistyminen ja lupaprosessien monipuolistuminen lisää palveluiden ja konsultoinnin merkitystä kiinteistöalan toiminnassa. Verkottuneen talotekniikan mahdollisuudet tuottavat alalle myös uusia toimintamalleja, kun vaikkapa rakennusautomaatiojärjestelmä toimitetaan tulevien säästöjen jako-osuutta vastaan.



Kuva 7 Kiinteistöalan palvelurakenne (Kiinteistöliitto 2014)

Vanhojen rakennusten osalta on laskettu, että energiatehokkuutta voidaan parantaa jopa 40 % nykytilanteeseen verrattuna verkottuneen talotekniikan avulla. Tällöin ohjataan keskitetysti ja ennusteisiin perustuen kiinteistöjen ilmastointia, lämmitystä, aurinkosuojausta ja valaistusta (Ahiola ym. 2010), (Kämppi, 2011 s 48).



Kuva 8 Kiinteistöalaa ohjaavat vaikutteet (Kiinteistöliitto 2014)

Ympäristöohjelmien toteuttamisen ja tavoitteiden saavuttamisen osoittaminen edellyttää usein monipuolisia liityntöjä eri palveluntuottajien ja yhteistyökumppaneiden kanssa, jotta tuloksia voidaan vertailukelpoisesti laskea ja toisaalta optimoida käyttöä toteutumien perusteella. Kokonaisuuden ymmärtäminen on tärkeää, jotteivät tietosuoja ja henkilötiedot vaarannu raportoinnissa. Lisäksi tulee huomioida optimoinnin ja säätöjen vaikutukset tuotantoon, jos ulkoista laskentaa aletaan runsaasti hyödyntämään yksilöllisessä kohteessa.

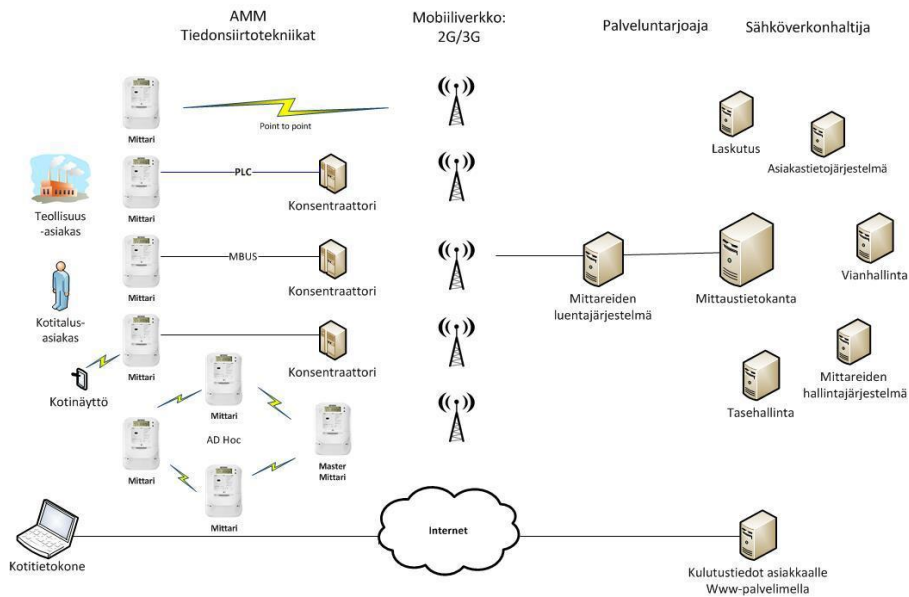
Tampereen teknillisen yliopiston rakennusfysiikan professori Juha Vinhan mukaan rakennuksen ulkovaipan ja ilmanvaihdon välinen toiminta nousee merkittävään asemaan energiatehokkaassa rakentamisessa. Rakennuksen vaipan ilmatiiviyden voimakas paraneminen edellyttää ilmanvaihdon huolellista suunnittelua, säätöä ja mittaamista, jotteivät paine-erot vaipan yli kasvaisi liikaa. Säättäminen on osoittautunut haasteelliseksi etenkin vuorokäyttöisissä kohteissa, kuten kouluissa ja toimistoissa, joissa ilmanvaihto voidaan ajastaa suljettavaksi öisin ja viikonloppuisin. Paine-erojen muutokset voivat tällöin johtaa mikrobien kulkeutumiseen huoneilmaan rakenteista, hormistoista ja viemäreistä. Lisäksi on huomioitava, että korjausrakentamisen yhteydessä joudutaan usein asentamaan lisäeristys rakennetun vaipan sisäpuolelle,

jolloin koko vaipan kosteustekninen toiminta muuttuu ratkaisevasti, ja kastepiste saattaa siirtyä rakenteiden sisään (Vinha 2015).

Kuten Vinhan tekstistä käy ilmi, voidaan energiansäästöä tavoiteltaessa tehdä paljon vahinkoa rakennukselle ja rakennuksen käyttäjille. Rakennusfysiikan toiminnan tarkastelu tulisikin ottaa osaksi sallittujen säätöalueiden asettamista, sekä tarkkailla toiminnan aikana, ettei rakennusten säätöä ohjata kielletylle alueelle kokonaisuuden toiminnan kannalta. Energiateknisen toiminnan optimointi edellyttää uudenlaisia yhteistyömuotoja eri toimijoiden kesken, sekä jatkuvaa tasapainon valvontaa. Rakennusten toiminnan kannalta on tärkeää, että esimerkiksi ulkoisten ennusteiden ei anneta viedä rakennuksen lämpötasapainoa kriittiselle alueelle vallitsevan kosteuskuormituksen suhteen, vaan painotetaan säätö- ja mittaustiedoissa rakennusten ja ihmisten terveyttä. Mittausantureiden ja mittausdatan saatavuuteen ja tiedon eheyteen pitää myös paneutua huolella. Mikäli tiedon eheys menetetään, saattaa se johtaa virheelliseen säätöön tai hälytystiedon puuttumiseen, jolloin voi koitua merkittäviä ongelmia rakennusterveyden ja pidemmälle vietyä ihmisten hyvinvoinnin ja terveyden suhteen. Rakennuksen lisäksi ongelmat voivat kohdata erilaisia ainevarastoja ja valmistusprosesseja, jos tavarat pääsevät väärän ohjauksen johdosta sulamaan tai jäätymään. Mittaustietojen fyysinen kahdentaminen ja eriyttäminen ohjelmallisesti toistaan saattaa olla tavoiteltavaa etenkin kriittisemmissä kohteissa. Ohjelmallisella eriyttämisellä tarkoitetaan sitä, että esimerkiksi lämpötilan säätö ja hälytysrajat tarkistetaan eri rutiineilla ja mielellään useammasta lähteestä, jolloin yhden pisteen ohjelmallinen tai fyysinen vahingoittuminen ei johda koko prosessin vioittumiseen.

4.2 Sähköverkon ohjaus

Energiankulutuksen ohjaukseen liittyvä data tulee olemaan lähitulevaisuudessa merkittävä osa verkotetun talotekniikan kokonaisuutta. Tähän ohjaa regulointi ja alan standardointityö. Lähitulevaisuudessa kiinteistöjen 0-energiatavoitteiden saavuttaminen tulee ohjaamaan entistä tehokkaammin oman tai paikallisen energiatuotannon hyödyntämiseen. Energiankulutuksen ohjauksessa tultaneen hyödyntämään laajasti kysyntäjouston tarjoamaa edullista energiaa ja hyödyntämään kulutuskäyttäytymisen perustella muodostuvaa historiatietoa ja sääennusteita energialähteen optimoinnissa.



Kuva 9 Etäluennan koko kuva, esimerkki kodin sähköverkon luennan kokoamisesta ja välittämisestä asiakkaalle etäluettavasta mittausjärjestelmästä (Savolainen ym. 2013)

Paikallisia energialähteitä tullaan kytkemään jakeluverkkoon, mikä mahdollistaa kuormitushuippujen tehokkaamman hallinnan. VTT on tehnyt tietoturvaselvityksen sähkönkulutuksen etäluentaan liittyen (Savolainen ym. 2013). Raportissa on tarkasteltu laajasti jakeluverkon ohjauksen ja mittauksen kautta mahdollistuvia uhkakuvia ja analysoitu näiden hallintamekanismeja. Monet raportin uhkakuvat ja torjuntamenetelmät ovat sovellettavissa suoraan verkotettuun talotekniikkaan.

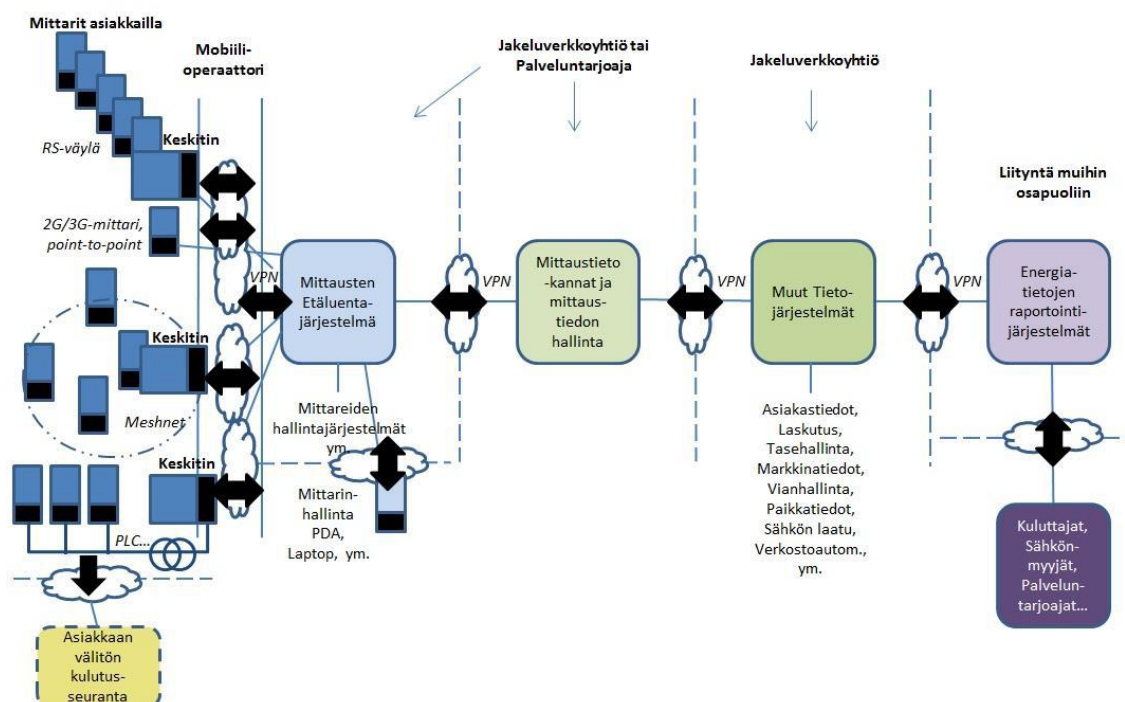
Raportissa tunnistettuja uhkia olivat

- suunnitteluvirheet rajapinnoissa ja ohjelmistomoduleissa, ei suojata eri tason toteutuksia tai ylipäättään järjestelmäkomentoja käyttäjätunnistein
- toteutusvirheet, esimerkiksi puskurin ylivuoto
- hälytyslokien seuranta ja sen puuttuminen
- laite- ja ohjelmistokirjo sekä etäluenta. Tuetaan useita alustoja, jotka keskitetään samaan etäkäyttöön, etäkäyttörutiinien kautta mahdollisuus murtautua järjestelmiin.
- pitkät alihankintaketjut, kokonaisuuden hahmottaminen vaikeaa, uhkien hallinta perustuu luottamukseen ja sopimuksiin, ei testata ja tiedetä todellista tilannetta

- laitevalmistajien tarjoaman teknisen tiedon ja dokumentoinnin taso vaihtelee voimakkaasti
- salauksen toteutuksen laatu
- autentikoinnin heikkoudet
- inhimilliset käytönaikaiset virheet
- raportointitietoja käyttäjille tuottavat palvelimet
- asiakastiedot, luottamuksellinen kulutusdata, josta voidaan päätellä esim. asiakaskannattavuus
- yksityisyydensuoja, kulutustiedot muodostavat henkilörekisterin
- fyysinen pääsy toimilaitteille (mittareille)
- datan kuuntelu ja häirintä, kohteesta riippuen tietoja voidaan saada optisesti, radioteitse tai tietoverkon avulla. Lisäksi on mahdollista häiritä etäluettavien mittareiden siirtoteitä ja vääristää mittaustuloksia.
- etähallinnan kautta ajettavat massamuutokset, käytetään usein heikkoja tai yhteisiä varmistuksia kaikille kohteen asiakkaille

Tutkimuksen kuluessa oli riskien todennäköisyyksiä ja vaikutuksia testattu arvottamalla riskit erilaajuisten tapahtumaskenaaridoiden kautta. Tällöin oli tuotettu eri tapahtumien riskiluvut, joiden kautta löydettiin merkittävimmät suojauksen kohteet. Verkottuneen talotekniikan hankkeissa tulee vastaavaan tapaan selvittää kokonaisuuden toiminta ja suhteuttaa vallitsevat riskit ja niiden vaikutus toiminnan laatuun. Riskiluettelo ja riskien vaikutusten arviointi on jatkuvaa seurantaa vaativa prosessi. Kokonaisuudessa tulee huomioida lisäksi energian käyttökohteet ja niistä kerättävä data ja mahdollinen oma energiantuotanto. Vaikka julkinen jakeluverkko syöttäisi luotettavaa dataa, voidaan kuluttajalaitteen tai oman energiantuotannon säätöarvoja muuttaa tahallisesti tai tuottamuksellisesti. Väärän datan perusteella tehdään väärä päätös taloudellisemmasta energialähteestä ja hyödyntämishetkestä. Verkottuneen

talotekniikan käyttämien tietovarantojen ja datan käyttötapaukset sekä asetusarvojen suojaus tuleekin täten suunnitella huolellisesti, jotta voidaan varmistua tietojen eheydestä koko siirtotien ja järjestelmän suhteen.



Kuva 10 Kuvassa energiateollisuuden näkemys tietoturvan viitekehyksestä (Savolainen ym. 2013)

4.3 Tietoturvan hallintamenetelmät

Hallintamenetelmät voidaan jakaa teknisiin ja hallinnollisiin hallintamenettelyihin. Hallintamenettelyjen avulla määritellään organisaation vastuuketjut ja vuosikello jatkuvien ylläpito- ja seurantamenetelmien toteuttamiseksi. Yleisellä tasolla yhteisö määrittää toimintaansa liittyvät riskit ja suhteuttaa käytettävät suojausmenettelyt ja toimintamallit ajantasaiseen riskiluetteloon.

Yhteisö laatii ja hyväksyy ohjeistuksen noudatettavasta tietoturvastrategiasta ja tietoturvapoliitikasta sekä sitouttaa kumppaniverkostonsa noudattamaan ohjeistusta. Yhteisö nimeää keskuudestaan ohjeistuksen ajantasaisuudesta vastaavan henkilön. Riskien toteutumista seurataan ja riskiluetteloa päivitetään tilanteiden muuttuessa. Yhteisö järjestää riittävät resurssit jotta toimintaa voidaan hallita teknisesti.

Tekniseen hallintamenettelyyn liittyy dokumentoinnin ylläpito, tekninen seuranta, tarkastus ja auditointimenettelyt. Järjestelmän käyttöönoton yhteydessä määritellään dokumentoinnin ylläpitovastuut eri osapuolten kesken, ja dokumentin ajantasaisuus tarkastetaan säännöllisesti vastuumatriisissa sovitun mukaisesti. Teknisen seurannan osalta liikenteen määrää ja laatua seurataan tarkoituksenmukaisilla välineillä.

Verkottuneen talotekniikan liiketoimintamalleissa on havaittavissa keskittämisen ja etähallinnan korostumista teknisen hallinnoinnin keinoina. Tällöin kootaan useiden rakennusten ja kiinteistöjen valvontatietoja etähallinnan keinoin yhteen, jolloin yksi asiantuntija voi valvoa keskitetysti usean kohteen toimintoja ja hälytystietoja (Hyypä ym. 2012).

Erilaiset etäpalvelut kotitalouksille ovat myös lisääntyneet. Kotitalous saattaa saada esimerkiksi asunnon tai ilmalämpöpumpun hankinnan yhteydessä tablet-laitteen, jonka avulla voi seurata ja säätää lämpötiloja ja tarkkailla asunnon tilatietoja. Lisäksi asuntojen etävalvonta- ja hälytyspalveluita myyvät vartiointiliikkeet ja teleoperaattorit. Etähallinnan käyttöönottoon liittyy useita toiminnallisia ja teknisiä riskejä, jotka yhteisön tulee puntaroida ennen kuin ryhtyy siirtymään etähallinnan pariin.

Teknisinä ja taloudellisina riskeinä voidaan mainita mm.

- yhteyden eheys, saatavuus ja luottamuksellisuus
- toiminnan jatkuvuus ja sopimusriskit

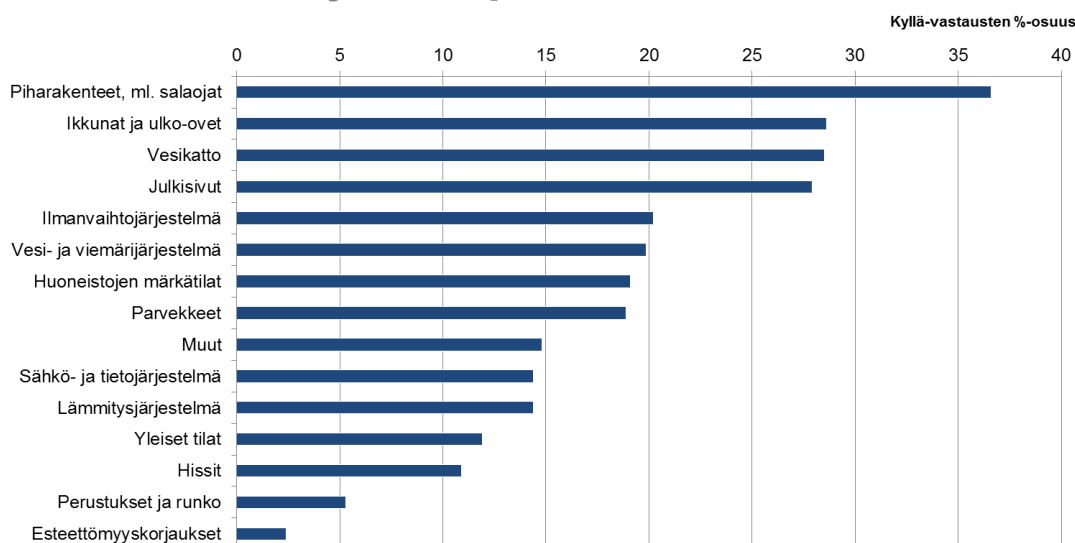
Siirrettäessä verkottunut talotekninen järjestelmä etähallinnan piiriin, tulee ottaa riittävästi selvää kohteen hallinnasta kokonaisuuden kannalta. Merkittäviä kokonaisuuksia muodostavat etäyhteyden tunnelointi ja käyttäjähallinta, mediamuunnosten toteutus ja eri kerroksissa toteutettavien salausten menetelmien vahvuus ja hallinta. Etähallinnan suhteen pitää varmistaa, että säätötiedot ovat kiinteistön omistajan tai käyttäjän käytettävissä myös sopimuskauden jälkeen, ja että palvelun tuottaja sitoutuu avustamaan sopimuksen siirtotilanteessa palvelun vastaanottavaa sopimuskumppania.

5 Verkottuneen talotekniikan toimintaympäristö

Verkottuneen talotekniikan järjestelmiä käytetään lähes poikkeuksetta uudistuotannossa ja valtaosassa suurempia korjausrakentamisen hankkeita, kuten kouluissa ja kerrostaloissa. Korjausrakentaminen ohitti liikevaihdoltaan uudistuotannon vuonna 2013 ja tilanteen on arvioitu olevan pysyvä.

Kiinteistöliitto arvioi vuoden 2015 korjausbarometrin perusteella korjausrakentamisen olevan suhdanteista huolimatta vilkasta. Erityisesti pääkaupunkiseudulla ja kasvukeskuksissa investoidaan esimerkiksi linjasaneerausten yhteydessä asumisviihtyvyyttä ja kiinteistön arvoa kohottaviin kohteisiin kuten verkottuneeseen talotekniikkaan. VTT arvioi vuoteen 2030 ulottuvassa ennusteessaan korjausrakentamisen arvon jatkavan kasvuaan ja uudisrakentamisen taantuvan voimakkaasti etenkin jakson loppupuolella (Laitinen 2011). Kiinteistöliiton korjausbarometrissa vuodelta 2014 havaitaan, että moniin verkottuneen talotekniikan järjestelmiin kohdistuu korjaustarpeita tarkastelujaksolla.

Korjaustarpeet 2014 - 2018



Kuva 11 Kiinteistöliitto, korjausbarometri 2014 (Kiinteistöliitto, 2014)

5.1 Lainsäädännön ja käytäntöjen muuttuminen

Suurimmat kaupungit ovat jo asettaneet rakennusjärjestyksessään ehdon talotekniikasta vastaavan suunnittelijan nimeämiselle, kun rakennushankkeen arvo tai talotekniikan osuus ylittävät määritellyt kynnsarvot. Määräyksellä pyritään parantamaan integraatioiden ja kokonaisuuden yhteentoimivuuden laatua.

Tulevaisuudessa vastaavat työnjohtajat osaltaan ohjaavat myös verkottuneen talotekniikan tietoturvan toteuttamista. Tietosuoja-asetuksen valmistelussa on määritelty tiettyjä vastuurajoja rekisterinpidolle toiminnan vaikutusalueen mukaan. Tällöin esimerkiksi henkilörekistereille on määriteltävä tietosuojavastaava. Teknisesti pitää huolehtia myös siitä, että yksilöllä on oikeus vaatia tietojensa poistamista, eli ”tulla unohdetuksi” (Lexia 2014). Verkottuneen talotekniikan järjestelmäsuunnittelussa tulee huomioida mahdollisuus yksilöivän datan käytön kieltämisestä tai estämisestä.

6 Tietoturvallisuuden taustoja

Tietoturvan hallinnasta on tullut arkipäivää kaikille digitalisoituvassa maailmassa liikkuville toimijoille. Yhteiskunnan ja yksilöiden päivittäinen toimintakyky on pitkälti riippuvainen verkottuneiden järjestelmien toimintakyvystä, ja perus-ICT-järjestelmiä on jo kohtuudella opittu suojaamaan haittaohjelmilta ja verkkorikollisuudelta.

Tietoturvan hallinta ei kuitenkaan ole staattista ja kertaluonteista tekemistä, vaan edellyttää aktiivista otetta ja muuttuvan ympäristön sekä uhkakuvien huomiointia, jotta toiminta olisi tehokasta. "Alkuvaiheessa määritellään tarkasti oikeudet ja kuka saa tilata, mutta seuranta usein unohtuu, esimerkiksi poistuneiden tunnuksia ei ole poistettu järjestelmistä." Käyttäjien hallinta korostuu erityisesti ympäristöissä, jotka ovat hallittavissa etäyhteydellä tai pilvestä. Tällöin sekä asiakkaiden että palveluntuottajien tulee aktiivisesti ylläpitää käyttäjätietoja, jottei järjestelmän tai tietojen asiaton käyttö ole mahdollista esimerkiksi palvelusopimuksen tai työsuhteen päättymisen jälkeen. "Käyttäjän tunnistaminen korostuu eri yhteyksissä koko ajan enemmän."

Yhteiskunnan toiminta on menossa suuntaan, jossa tietoteknisten järjestelmien toimintakyky on välttämätön osa toimintaprosesseja. Välttämättä ei aina ole olemassa korvaavia järjestelyitä tilanteelle, jossa menetetään tietotekniikan tuottama osaprosessi. Meneillään olevan kehityksen johdosta on tärkeää, että panostetaan riskien hallintaan ja ylläpidetään tilannekartan lisäksi aktiivisesti tietojärjestelmiä ja tietovarantoja.

Tuotettavan tiedon määrä on moninkertaistunut vuosien saatossa, ja käsiteltävän tiedon analysointitavat ovat kehittyneet valtavasti. Tietovarannot muodostavat

haltijoilleen kilpailuedun ja toisaalta tuottavat riskin liiketoiminnan kilpailuedun tai yksityisyydensuojan menettämisestä joutuessaan väärin käsiin.

Verkottuneen talotekniikan tietoturvan perustason määritelmässä pyritään löytämään se perustaso, johon sitoutumalla toimijat voivat kohtuudella turvata toimintansa jatkuvuuden ja luottamuksellisuuden verkottuvassa maailmassa. Peruseriaatteina käytetään tietoteknisissä järjestelmissä omaksuttuja parhaita käytäntöjä soveltaen niitä verkottuneen talotekniikan erityispiirteisiin ja liiketoimintamalleihin.

6.1 Alan standardit ja viitekehykset

Tietoturvallisuudesta on yleisesti olemassa kansainvälisiä ja kansallisia viitekehyksiä ja suosituksia. Lisäksi on olemassa valmistajakohtaisia menetelmiä tietoturvan toteuttamiseen ja todentamiseen. Ohjeistuksessa käytettiin viiteaineistona yleisimpiä vakiintuneita standardeja, ja ohjeistuksesta tehtiin yhtenäinen Vahti-ohjeistuksen kanssa.

6.2 Verkottuneiden talotekniikkajärjestelmien ominaispiirteitä

Verkottuneiden talotekniikkajärjestelmien käyttöliittymät ovat moninaisia ja vakiintumattomia. Käyttöliittymänä saattaa toimia esimerkiksi numeronäytön ja näppäimistön yhdistelmä ("hissin käyttöliittymä"), tai toisena ääripäänä liittymänä saattaa olla tavanomainen sovellusnäkyvä.

Verkottuneet talotekniset järjestelmät saattavat olla pitkälle räätälöityjä toteutuksia, jotka käyttävät rajattua verkkoprotokollaa. Protokollia on useita käyttötarkoituksien tai lisenssinhaltijoiden kaupallisten lähtökohtien toteuttamiseksi. Yleisimmille protokollille on saatavissa ohjelmalliset tai laitepohjaiset mediamuuntimet, joiden avulla voidaan esimerkiksi käyttää normaalia TCP/IP-verkkoa siirtotienä.

Merkittävin ero verkottuneen talotekniikan järjestelmien ja tietojärjestelmien välillä on verkotettujen taloteknisten järjestelmien tuottama fyysinen I/O-tieto, ohjaus ja havainnointi, jotka varsinaiselta tietojärjestelmältä puuttuvat. Ympäristöön liittyvä mekaniikka ja fyysiset liittymät tuottavat yhden huomioitavan ja suojattavan lisätason järjestelmiin.

Tilaturvallisuudessa pitää kiinnittää huomiota laitteiden fyysiseen koskemattomuuteen asetusmuutosten varalta. Pitää huolehtia esimerkiksi siitä, että laitteistot ja kenttälaitteet on kiinnitetty niin, ettei niiden sijaintia pysty muuttamaan vahingossa tai vähäisellä vaivalla. Verkottuneen talotekniikan tietoverkkojen siirtokerrokset ovat useimmiten suoraan tai mediamuuntimen kautta yhteensopivia internetin TCP/IP-protokollan kanssa, jolloin peruskäyttö onnistuu liittymällä tavanomaisella päätelaitteella sellaiseen verkkoon, josta on yhteys haluttuun palveluun.

Ohjausominaisuuksiensa osalta kiinteistöautomaation piiriin kuuluvat järjestelmät eivät juuri poikkea toisistaan. Suuntaus on jo pitkään ollut siirtyminen avoimiin käyttöympäristöihin ja yleisesti saatavilla oleviin varusohjelmistoihin automaatiojärjestelmien peruspalveluiden tuotannossa. Useimmiten myös automaatioverkot toteutetaan normaaleina IP-verkkoina, jolloin väylää ajetaan IP-verkon päällä. Jos päivityspolut on suunniteltu hyvin, voidaan ympäristöä uudistaa tietojärjestelmätoimittajien päivityssuositusten mukaisesti.

Suurimmat haasteet aiheutuvat toimittajakohtaisista toteutuksista, joiden on mukauduttava yleisiin päivitysaikatauluihin. Esimerkkinä tämänkaltaisesta toteutuksesta on vaikkapa automaatioprotokollan mediamuunnin, joka kapseloi automaatioverkon liikenteen normaalin IP-verkon kautta siirrettäväksi. Käytön estävä ominaisuus saattaa tulla vastaan esimerkiksi IPv6-reititystä tai NAT-muunnosta tehtäessä, kun automaatioverkkoa liitetään osaksi laajempaa kokonaisuutta. Mikäli mediamuunnin ei hallitse kaikkia ympäristössä käytettäviä reititys- ja osoitteenmuunnosmenettelyjä, ei verkkoyhteyttä voida muodostaa suunnitellusti automaatioverkkoon. Käyttöympäristön vaatimusmäärittelyihin ja riittäviin ylläpito- ja huoltosopimuksiin tulee laitteiston käytön jatkuvuuden kannalta paneutua huolellisesti, jotta käytönaikaisilta yllätyksiltä vältytään.

Verkottuneen talotekniikan järjestelmiä suunniteltaessa kohdataan usein hallinnollisia tai aikataulullisia ongelmia asiakasyritysten sisäisten verkkojen käytössä. Tämä saattaa johtua esimerkiksi tiedonkulun puutteesta tilaajan ja muun asiakasorganisaation välillä. Pitkät palveluketjut tuovat myös oman lisänsä aikatauluihin ja ennakkosuunnittelu ja aikataulutus korostuu hankkeissa. "Pieni ymmärtämysongelma on myös toimittajilla, ajatellaan että isolla yrityksellä on helposti muokattava verkko."

1.1 Tietoturvan hallinnan periaatteet

Tietoturvan hallinnan tulee kattaa menetelmät järjestelmien suunnittelusta, laitteiden käyttöönotosta ja ylläpidosta aina käyttäjien koulutukseen asti. Tietoturva tulee huomioida kokonaisuutena, jossa hahmotetaan verkottuneiden taloteknisten järjestelmien käyttötarkoitus, käyttöympäristö ja tuetut käyttötapaukset. Kokonaisuutta ohjaa loppukäyttäjien toiminnan tietoturvastrategia, -politiikka ja -ohjeistus. Tietoturvastrategia ja -politiikka voidaan laatia esimerkiksi siten, että yhteisö määrittää yleisellä tasolla toimintansa tavoitteet lyhyellä ja pitkällä tähtäimellä sekä tavoitteita uhkaavat riskit ja näitä vastaan tehtävät varautumiset. Ohjeistuksella määritellään menettelyt, joilla on mahdollista hallita riskejä tietoturvapoliitiikan asettamissa rajoissa. Mikäli yhteisöllä ei ole olemassa olevaa tietoturvastrategiaa, tulee tällainen aluksi luoda käyttäen viiteaineistona esimerkiksi VAHTI-aineistoa (Vahti ohje 2009).

Tietoturvastrategia tai -tavoitetila voi taloyhtiöllä ja muulla pienimuotoisella yhteisöllä olla melko yksinkertainen, yhtiökokouksen tai hallituksen hyväksymä periaatekuvaus, jonka pohjalta kaikki taloon tulevat verkottuneet talotekniset järjestelmät otetaan käyttöön ja hallinnoidaan sekä ylläpidetään. Kansainvälistä toimintaa harjoittavalla yhteisöllä tietoturvastrategia tulee olla laajempi, ottaen huomioon monipuolisemman toiminnan tuottamat riskit.

Tietoturvapoliitiikka tai -toimintamalli kuvaa toimintaa lyhyemmällä tähtäimellä ja ottaa jo kantaa käytännön tekemiseen. Ohjeistus puolestaan konkretisoi yksittäisen ihmisen tekemisen huomioiden strategian ja politiikan vaatimukset.

Verkottuneen taloteknisen laitteen ja järjestelmän käyttöönotossa voidaan hyödyntää laitteen valmistajan tuottamia yleisohjeita. Yleisohjeet eivät kuitenkaan koskaan yksin ratkaise tietosuojan toteutumista tai järjestelmän sovittamista yhteisön strategiseen toimintaan, jolloin soveltamisohjeet tulee laatia kunkin järjestelmän osalta erikseen. On myös huomioitava, että mikäli verkottunut talotekninen järjestelmä hyödyntää tai tuottaa yksilöitävää henkilörekisteriä toimituksessaan, on tästä mainittava rekisteriselosteessa (Tietosuoja 2009).

Valmistajien, urakoitsijoiden ja palveluntuottajien tulee luonnollisesti huolehtia prosessin vaiheista oman ympäristönsä osalta niin, että suositusten mukaan asennetun ympäristön voidaan yksiselitteisesti todeta toteuttavan sovitun tietoturvatason.

Palveluiden tilaajien ja loppukäyttäjien puolestaan tulee käyttää ja hallita järjestelmää ohjeiden ja ylläpidon edellyttämien toimien mukaisesti tai hankkia tarvittava osaaminen kolmannelta osapuolelta.

1.2 Tietosuojaan hallinta

Monet verkottuneen talotekniikan järjestelmät muodostavat yksin tai yhdessä muiden järjestelmien kanssa henkilörekisterin tai yhteisön toiminnan kannalta kriittisen tietovarannon. Valmisteilla olevan tietosuoja-asetuksen perusteella tietosuojaan alaisen materiaalin käsittelyn luottamuksellisuudelle annetaan ankara vastuu tiedon omistajalle. Asetuksen vastuut kohdistuvat valmisteluvaiheessa tahoihin, jotka käsittelevät yli 5000 tapahtumaa vuosittain. Valmistelussa olevan tietosuoja-asetuksen vastuut tarkoittavat sitä, että erityisesti asiakas- ja henkilötietojen käsittelyssä tulee olla erityisen huolellinen ja perusteellinen. Henkilörekistereitä käytetään monissa verkottuneen talotekniikan järjestelmissä, ja lisäksi järjestelmät muodostavat henkilörekisterin alaista dataa itsenäisesti.

On huomioitava, että jo yksilöitävissä oleva osoitetieto voi muodostaa henkilörekisterin, vaikka samassa yhteydessä ei suoraan säilytetä kohdehuoneiston asukastietoja. Tällöin esimerkiksi huoneiston säätötiedot voivat olla tietosuojaan tarkoittamia henkilörekisteritietoja, joiden käyttöä pitää rajoittaa ja seurata niin, että tietosuoja säilyy. Esimerkiksi rikoslain 24§ määrittelee salakatselun ja -kuuntelun sekä näiden valmistelun teknisellä laitteella rangaistavaksi. Tämän johdosta tulee kiinnittää huomiota riittäviin ohjeistuksiin ja määrittelyihin otettaessa käyttöön verkottunutta talotekniikkaa.

Tietovarannot saattavat muodostaa myös henkilörekisterin, jos tietojen avulla on yhdisteltävissä muiden järjestelmien avulla kokonaisuuksia, jotka johtavat yksittäisen henkilön tietoihin. Jos esimerkiksi kootaan huoneistokohtaista seurantadataa, muodostaa se osoitetietojen kautta henkilörekisterin. Tällöin tietojen käsittelyssä ja säilyttämisessä tulee noudattaa menetelmiä, jotka on säädetty henkilötietojen käsittelylle.

Kameravalvonnalle asetetaan julkisissa ja yksityisissä tiloissa rajoituksia kuvan ja tallenteiden käytön sekä varastoinnin suhteen. Verkotettu sähköinen talotekniikka saattaa tuottaa kuvan kaltaista tietoa järjestelmiä yhdistettäessä. Verkotettujen

taloteknisten järjestelmien käyttöönoton yhteydessä on syytä suorittaa rekisterikatselmus, mikäli rakennus on julkisessa käytössä tai palvelee sisäisesti yli 1000 henkilöä.

Tietosuojaan osalta pitää lakien ja asetusten lisäksi pitää mielessä kilpailuedun ja kaupallisen arvon säilyttäminen tiedonkäsittelyn eri vaiheissa. Esimerkiksi tieto yrityksen aktiviteeteista eri toimipisteissä tai hallinnollisissa osissa saattaa indikoida aktiivisuutta julkaisemattoman kaupallisen toimen suhteen ja viedä kilpailuedun. Kiinteistötoiminnassa puolestaan kerättävä ja säilytettävä data saattaa paljastaa toimijan taloudellisen aseman ja menetelmät vuokralaiselle toteutuneiden kulutus- ja huoltotoimien kautta ja huonontaa toimijan asemaa neuvotteluissa.

7 Muutoksen johtaminen

Verkottuneen talotekniikan parissa ollaan merkittävässä muutostilanteessa, kun suljetuista toteutuksista ollaan vauhdilla tulossa kohti avointa ja verkottunutta maailmaa. Jaetut ympäristöt edellyttävät yhteisiä toimintatapoja. Hallittu muutos edellyttää hyvien toimintatapojen ja johtamismallien soveltamista, jotta toimintatavat saadaan muutettua uutta tilannetta vastaavaksi. Pääosin muutos tulee olemaan osapuolten asenteiden ja toimintatapojen muokkaamista, tekniset järjestelmät saadaan ihmisiä helpommin toteuttamaan uuden toimintamallin edellytykset.

Sunzi (770–476 eaa.) kirjoittaa kirjassaan Sodankäynnin taito: ”ettei meidän tulisi liiaksi pohtia vihollisen hyökkäyksen todennäköisyyttä vaan sitä mikä on oma valmiutemme kohdata vihollisen hyökkäykset”. Lisäksi hän toteaa, että ”ne jotka hallitsevat perusasiat, voittavat”. Sunzin kirjaa on käytetty satoja vuosia johtamisstrategioiden perusteoksena ja sen opit toimivat myös verkottuneen talotekniikan tietoturvallisuuden johtamisen oppeina. Pitää tuntea toimintaympäristö, seurata muutoksia ja osata toimia oman järjestelmänsä ja palvelunsa kanssa oikein muuttuvissa tilanteissa.

Yhtenä haasteena on perinteisen toimintamallin uudistuminen nopeasti urakoitsija-rakennuttaja/tilaaja-mallista palvelumalliin. Perinteisessä tuotantomallissa osapuolilla on ollut selkeät vastuurajat, ja rakennuksen tai toimintokokonaisuuden luovutuksen jälkeen on siirrytty uuden urakan pariin. Verkottuneen talotekniikan järjestelmät kuitenkin edellyttävät jatkuvaa huolto- ja ylläpitotyötä toimiakseen, ja tämä tuottaa uutta

liiketoimintaa ja toimintatapoja osapuolille. Uusien roolien omaksumisessa pitää panostaa tiedottamiseen ja koulutukseen, jotta saadaan selätettyä muutosvastarinta ja edistettyä parhaiden toimintatapojen käyttöönottoa.

Åbergin mukaan ilman viestintää ei voi johtaa. (Åberg 2000) Muutostilanteessa johtamisen ja viestinnän kytkös on vielä voimakkaampi. Tämä asettaa viestinnän ja tiedottamisen suunnittelun keskeiseen asemaan onnistuneen muutoksen toteuttamisessa.

Ohjeistuksen valmistelun kuluessa viestintää on toteutettu yleisöluentojen, lehtiartikkeleiden ja jäsentiedotteiden muodossa. Ohjeistuksen julkaisun yhteydessä on tarkoitus hyödyntää ohjausryhmän kokoonpanon sidosryhmiä viestinnässä ja tiedottamisessa, jotta tieto uudesta toimintamallista saadaan kentälle mahdollisimman nopeasti ja yhtenäisesti.

Hyvä muutosjohtaminen on kitetyttävissä seuraaviin kokonaisuuksiin: hyvä suunnittelu, joustava ja olosuhteet huomioiva toteutusprosessi, muutoksen jatkuva hallinta ja motivointi sekä innostaminen muutoksen toteutukseen (Stenvall ym. 2007).

Tiekartta konkretisoi toimintaskenaarion ja toimii helposti omaksuttavana välineenä laadintaprosessissa (Santalainen 2009). Toimintaskenaarion kuuden tarkastelukohdan etenemismallissa korostetaan toimintakentän muutosten ennakointia, käyttäytymisen ennakointia ja kumppanuuden sekä ekosysteemin merkitystä muutoksen johtamisessa ja hallinnassa.

Verkottuneen talotekniikan tietoturvatyössä on pyritty huomioimaan strategisen ajattelun opit tuottamalla mahdollisuus vaiheittaiseen, tavoitteelliseen ja jatkuvaan etenemiseen tietoturvallisuuden polulla jo ennen kuin on pakko sopeutua muuttuneeseen toimintaympäristöön. Santalainen toteaaakin (Santalainen 2009) että strateginen näkemys on teoria tulevasta menestysmallista, ja että menestyvillä organisaatioilla voi olla useita päällekkäisiä strategioita. Tietoturva-alan toimintamalleihin tämänkaltainen ajattelu heijastuu siten, että muutosta ja toimintaa sekä teknologiakyvykkyyksiä ja uhkakuvia tulee seurata aktiivisesti ja rakentaa toimintamallit muuttuvan maailmankuvan mukaan.

Alan toimijoiden kannattaa pyrkiä vakioituja toimintamalleja edistävään yhteistyöhön ja keskittää voimavaroja yhteisten pelisääntöjen laadintaan, jolloin terävimmän kärjen hiontaan jää enemmän vapaita resursseja. Suomessa on perinteisesti ollut paljon toimialojen sisäistä yhteistyötä edunvalvonnan merkeissä ja tätä voimavaraa kannattaa hyödyntää myös tietoturvatyössä. Esimerkiksi Viestintäviraston kyberturvallisuuskeskus on tukenut useiden huoltovarmuuskriittisten toimialojen neuvottelukuntia, ja myös verkottuneen talotekniikan toimijoiden kannattaa vastaavaan tapaan verkostoitua.

Verkostoitumisessa voidaan Santalaisen mukaan puhua synergiaeduista, jossa useat toimijat lähtevät kohti yhdessä sovittua tavoitetta. Tällöin saavutetaan parempi osaamispääoma ja neuvotteluvoima, jolloin muutosten läpivienti ja markkinoiden muuttaminen on yksittäistä toimijaa nopeampaa ja varmempaa (Santalainen 2009).

7.1 Teollinen (teknologinen) vallankumous

Teollinen vallankumous ja teknologinen vallankumous ovat vakiintuneita termejä jo 1800-luvulta lähtien. Termi ”teollinen vallankumous” tuli tietoisuuteen Arnold Toynbeen käytettyä sitä otsikkonaan kirjassaan *The Industrial Revolution in England* (1884).

Käsite oli esiintynyt kuitenkin jo aiemmin kirjallisuudessa esimerkiksi 1800-luvun alussa ranskalaisen taloustieteilijän Jérôme-Adolphe Blanquin toimesta, joka käytti sitä vuonna 1837 teoksessaan *Histoire de l'économie politique en Europe depuis les Anciens jusqu'à nos jours* (1837-1842) 5 vol., (Helsingin yliopisto 2011) ja englantilaisen taloustieteilijän Friedrich Engelsin toimesta, joka käytti sitä vuonna 1844 julkaisussaan *Työväenluokan asema Englannissa* (Helsingin yliopisto 2011). Tunnettuja teollisen vallankumouksen tutkijoita ovat esimerkiksi T. S. Ashton, Paul Mantoux, Phyllis Deane, Peter Mathias, Nicholas Crafts, Pat Hudson ja David Landes (Helsingin yliopisto, 2011).

1800-luvun loppupuolelta alkaen termi ”teknologinen vallankumous” on vakiintunut tarkoittamaan yleisesti merkittävää toimintamallien muutosta, joka on tapahtunut uuden teknologisen tuotteen markkinoilletulon myötä.

Merkittävästi ihmisen toimintaan liittyneitä teknologiaratkaisuja ovat energiamuotojen, liikkumisen ja viestinnän muutokset, jotka ovat yleistyttyään nopeasti muuttaneet vanhoja toimintatapoja merkittävästi ja pysyvästi. Esimerkkeinä ovat siis höyryvoiman, sähköön, auton ja erilaisten viestintätekniikoiden tuomat muutokset sähköttämisestä

puhelimien kautta internetiin. Useimmiten uusien teknologiaratkaisujen tullessa markkinoille niiden merkitystä lähitulevaisuudessa liioitellaan ja toisaalta niiden vaikutuksia pidemmällä tähtäimellä vähätellään (Wiio 1970-2009). Teknologiamuutokset tapahtuvat useimmiten varhaisten edelläkävijöiden toimesta, jolloin uusi tekniikka otetaan kokeilunhaluisten henkilöiden tai yhteisöjen toimesta käyttöön suurten massojen seurattessa myöhemmin uuden alueen liiketoiminnan kehittyessä ja kypsyessä.

Teknologista vallankumousta kuvataan oppimisprosessina. Uuden oppiminen on teknologiavallankumousten historiassa ollut tehokkainta siten, että on voitu tuoda uusi toimintamalli vanhan rinnalle ja siirtyä joustavasti uuteen toimintamalliin. Tällöin vanhan menetelmän osaajille jää mahdollisuus omaksua muutos ja yhdistää uusi malli aiempaan osaamiseen (Leppämäki 1998).

Verkottuneen talotekniikan alalla ollaan murrosvaiheessa, jossa tulee huomioida uudet liiketoimintamahdollisuudet tietojen yhdistämisessä ja laajassa hyödyntämisessä ja toisaalta muuttuvan ympäristön aiheuttamat toiminnalliset ja tuotannolliset riskit. Kokonaisuuden hallinta edellyttää monipuolista osaamista ja päättelyketjuja, kun rakennetaan verkottunutta talotekniikkaa avoimen tiedon maailmaan.

8 Työskentelymenetelmät

Ohjemateriaalin teossa noudatettiin konsultatiivisen työskentelymenetelmän pääperiaatteita. Ohjeistusta laatimaan asetettiin ohjausryhmä, joka ohjasi työn suorittamista. Varsinainen materiaali kerättiin työpajojen ja kirjallisuustutkimuksen avulla.

8.1 Ohjausryhmätyöskentely

Ohjausryhmätyöskentelyn tarkoituksena on valvoa työn tarkoituksenmukaista etenemistä, antaa suuntaviivoja ja hyväksyä työn tulokset. Ohjausryhmätyöskentely toimii tekijää ja organisaatiota yhdistävänä siteenä (Tokola 2004).

Opinnäytetyön ohjausmenettelyissä noudatettiin STUL:n yleisiä toimintatapoja, jotka ovat käytössä vastaavien ohjemateriaalien laadinnassa. Työtä ohjasi 18 alan yhteisöä edustajiansa kautta. Ohjausryhmä kokoontui yhteensä kuusi kertaa.

8.1.1 Ohjausryhmän kokoonpano

Ohjausryhmän kokoonpano koostui seuraavista henkilöistä ja yhteisöistä:

Timo Rasimus, Sähköinfo Oy/STUL (puheenjohtaja)
 Olli Mäkinen, Audico Systems Oy/Avita ry (varapuheenjohtaja)
 Kimmo Arenius, Sähkötieto ry (sihteeri)
 Timo Hiekkänen, Akukon Oy/Avita ry
 Tauno Hovatta, Henkilö- ja yritysarviointi SETI Oy
 Kenneth Hänninen, Energiateollisuus ry
 Juho Jakka, Core Factory Oy/Avita ry
 Sami Johansson, Flexim Security Oy/Turva-alan yrittäjät ry
 Veijo Kauppi, Sähköinfo Oy
 Antti Koskinen, Fidelix Oy/STUL:n AU-ryhmä
 Petri Käyhkö, Kesko Oyj
 Tuomas Lehmusmetsä, Senaatti-kiinteistöt
 Pasi Lehtinen, Neste Oil Oyj/Suomen Automaatioseura
 Markku Leskinen, Granlund Oy/Turva-alan yrittäjät ry
 Riikka Liedes, Sähköinfo Oy
 Kalle Luukkainen, Nixu Oy
 Veijo Piikkilä, Metropolia-ammattikorkeakoulu
 Janne Rasi, Fatman Oy/Avoin Automaatio ry
 Timo Tuominen, Avita ry
 Jari Virta, Kiinteistöliitto
 Aki Väänänen, Granlund Oy/Turva-alan yrittäjät ry

Ohjausryhmän kokoonpano edusti laajasti verkottuneen talotekniikan tuottajia ja käyttäjiä. Ohjausryhmä järjesti mahdollisuuden haastatella ohjausryhmän toimialoihin liittyviä yhteisöjä ja asiantuntijoita.

8.2 Kirjallisuustutkimus

Kirjallisuustutkimuksen avulla selvitettiin teemahaastattelun taustoitusta ja kyselyrunko. Kirjallisuutta ja artikkeleita tutkittiin kolmesta eri näkökulmasta: verkottuneen tietotekniikan, talotekniikan ja tietoturvan kannalta. Keskeisiksi lähdeaineistoiksi valikoitui Suomen Automaatioseuran laatima Teollisuusautomaation tietoturvaohje (Suomen automaatioseura 2010) sekä Aalto-yliopiston laatima tutkimusraportti automaatiolaitteiden haavoittuvuuksista (Seppo Tiilikainen 2013).

Automaatioseuran laatiman tietoturvaohjeen sisällysluetteloä käytettiin haastattelututkimuksen runkona, ja sen perusteella etsittiin osapuolten tarkemmat painotukset. Haastattelujen ja ohjausryhmän valintojen perusteella kokonaisuus rakentui lopulliseen muotoonsa.

8.3 Haastattelut

Haastatteluita tehtiin ohjeistustyön eri vaiheissa sekä toimialakohtaisina että yritysakohtaisina toteutuksina. Ohjausryhmän kontaktien avulla järjestyi viisi haastattelutilaisuutta sekä kolme yhteisövierailua. Haastattelumateriaalia kertyi yhteensä 15 tuntia ja haastatteluihin osallistui yhteensä kolmekymmentä henkilöä. Haastatellut henkiöt edustivat laajasti verkottuneen talotekniikan sidosryhmiä ja kiinteistönomistajia. Haastattelujen lopputuloksista purettiin yhteenveto ohjausryhmän seurantakokoukseen, joka valitsi painopistealueet havaintojen pohjalta.

Toimialakohtaisissa teemahaastatteluissa käytettiin viitteenä automaatiojärjestelmien tietoturvallisuusohjeistuksen sisällysluetteloä, jonka pohjalta keskusteltiin toimialueiden vakiintuneista käytännöistä ja odotuksista tietoturvallisuuden toteutuksen tasolle. Yhteisökohtaisissa haastatteluissa käytiin vapaamuotoisempia keskusteluita ja tarkasteltiin jo valmistunutta ohjeistusmateriaalia.

8.4 Ohjeistuksen koostaminen

Ohjeistuksen koostaminen oli iterointiprosessi, jossa sovitettiin tunnettuja tietoturvakäytäntöjä toimialan vaatimuksiin. Painotukset ja rajaukset rajattiin ohjausryhmän ja lausuntojen mukaisesti huomioiden jalostettavuuden säilyminen ja alkuperäinen tarkoitus tuottaa yhtenäinen perustason ohjeistus.

Toimialojen asiakaskunnassa, toimintavolyymeissa ja kertatoimituksissa sekä palvelumalleissa oli runsaasti eroja ja näin jouduttiin tekemään tiettyjä yleistyksiä. Esimerkiksi tietoliikenteen aktiivinen valvonta esitettiin edelläkävijöiden toimesta perustason vaatimukseksi, mutta lopulta todettiin, että alkuvaiheessa liian tiukaksi viritetty normisto saattaa johtaa siihen, että toteutukselle ei saada yleistä hyväksyntää. Ohjeistuksessa esitettiin muutamia hahmotelmia korotetun tason järjestelmille ja kattava ehdotus raci-matriisiksi. Korotetun tason täsmällisempi ohjeistaminen on jatkokehityksiasia, kun perustason ohjeistu on ensin tehty tunnetuksi.

8.5 Lausunnot ja arvioinnit

Ohjeistusta ovat pyynnöstä arvioineet muutamat tietoturvan ja verkkotekniikan asiantuntijat ja arviointien avulla on täydennetty ja tarkennettu ohjeistusta.

Ohjeistusta ovat eri vaiheissa arvioineet mm. seuraavat asiantuntijat:

Kari Saarelainen, KPMG

Antti Pirinen, KPMG

Pyry Heikkinen, Tulli

Jarkko Saarimäki, Viestintävirasto

Tommi Roto, Telia Sonera Finland

9 Ohjeistuksen toteutus

Ohjeistuksen laadinnassa painottuivat erityisesti kohtuullinen kustannus- ja osaamistaso tietoturvan perustason tuottamiseksi. Tällä haluttiin varmistaa matala käyttöönoton kynnys, jotta tietoturvan perustason käsite saisi nopeasti yleisen hyväksynnän ja riittävän käyttäjämässän. Asiakkaat eivät useinkaan ilman ulkoista ohjausta ole valmiita panostamaan ylimääräistä. "Mitä pienempi asiakas, sen vähemmän kiinnostusta panostaa tietoturvaan." Asiakkaat luottavat myös markkinointimielikuviin ja ajattelevat asioiden olevan ja pysyvän kunnossa ilman omaa panostusta. Rakennuttamisen perinteiset toimintamallit eivät välttämättä edistä parhaimpien ratkaisujen käyttöönottoa. "AS Oy:n asukkailla ja loppukäyttäjillä ei ole ollut perinteisesti edellytyksiä toteuttaa tietoturva-asioita, rakennukset rakennetaan alkuperäisen rahoitussuunnitelman ja teknisten reunaehtojen mukaan, jolloin päätökset on lyöty lukkoon etukäteen." Haluttiin, että ohjeistuksen avulla voidaan edistää parhaiden käytäntöjen tunnettavuutta, ja saada kilpailuetua toimijoille, jotka noudattavat verkottuneen talotekniikan tietoturvan perustason suosituksia.

Ennen ohjausryhmän muodostamista laadittiin pienryhmänä puheenjohtajaorganisaation kanssa runko ohjeistuksen toteuttamiseksi. Ensimmäiseen ohjausryhmään tuotiin alustava etenemissuunnitelma ja sisällysluettelo hyväksyttäväksi toteutettavan työn etenemisen pohjaksi. Toimialakohtaisissa haastatteluissa käytiin alustavaa sisällysluetteloa läpi peilaten sen kattavuutta ja tarkoituksenmukaisuutta kohdealueen toimintaan. Saatujen kommenttien perusteella tarkennettiin painoituksia ja tehtiin muutoksia luetteloon. Ohjeistuksen rakenteen toteuttamisessa ja viestintäsuunnittelussa korostui, ettei kattavaa ohjeistusta oltu

aiemmin tehty verkottuneen talotekniikan tarpeisiin. Tavoitteena pidettiin yhteisen toimintatavan ja viitekehyksen muodostamista, jotta esimerkiksi kilpailutukset olisivat alalla vertailukelpoisempia, ja tietoturvallisten toimintamallien omaksumisesta tulisi alalle kilpailuetu, ja toisaalta myös asiakkaille mitattavissa oleva tavoiteltava ominaisuus. Ohjausryhmässä todettiin, että ohjeistusta pitää aktiivisesti kehittää tulevana vuosina muuttuva tekninen ympäristö ja asiakasvaatimukset huomioiden. "Pitää asettaa perustaso joka ei sulje jatkokehityksen mahdollisuuksia pois."

9.1 Arviointi ja lausuntomenetelmät

Ohjeaineisto käytettiin kahdella lausuntokierroksella marras-joulukuussa 2014. Lausuntopyyntö oli suunnattu ohjausryhmälle, mutta oli toisaalta avoinna myös julkisille kommentteille. Saatujen kommenttien perusteella tehtiin vähäisiä muutoksia ohjeistukseen. Ohjausryhmä hyväksyi aineiston luovutettavaksi toimitusprosessiin tammikuussa 2015. Toimitettu aineisto käytettiin vielä suunnatuilla lausunnoilla mm. Viestintäviraston kyberturvallisuusyksikössä ja STUL:n asiantuntijoilla. Näiden lausuntojen perusteella tarkennettiin esimerkiksi aineiston standardiviitteitä.

10 Tulokset

Konsultoivan työn tekemisessä on tärkeää havainnoida ja kannustaa osapuolia tuomaan esille ajatuksensa ja koostaa näistä kohteeseen toimeksiannon kannalta tarkoituksenmukainen lopputulos. Konsultointityössä on tärkeää tuntee konsultoitavan alueen parhaat käytännöt ja konsultoivan työn menetelmät, jotta voi tarvittaessa haastaa havaintoja ja ohjata työtä yleisesti hyväksi havaittuun suuntaan. Työskentelymenettelyksi valittiin teemahaastattelut ja ohjausryhmän joholla tapahtuva iterointiprosessi sekä vertaisarviointi, joka tuotti hyväksyttävän lopputuloksen ja julkaisukelpoisen ohjeistuksen.

Haastattelututkimuksen perusteella muokattiin ja painotettiin ohjeistusta ohjausryhmän näkemysten perusteella. Ohjeistuksesta muodostui noin 40-sivuinen kokonaisuus, jota ei laajuutensa vuoksi voitu julkaista ST-korttina. Jatkokehityskohteina on mainittu toimialakohtaiset tarkentavat ohjeet, jotka on luontevampaa työstää ST-kortin noin 4–10 sivuun mahtuviksi täsmällisiksi työmenetelmäohjeiksi.

Ohjeistusmateriaalin kohderyhmä oli laaja kattaen mm. kiinteistönomistajat, rakennuttajat, urakoitsijat ja suunnittelijat. Kohderyhmä huomioiden tuli ohjeistuksen olla riittävän yleisellä tasolla, jotta kukin toimiala ja kohderyhmä pystyy hyödyntämään ohjeistusta toimintansa viitekehyksenä. Ohjeistukseen päätettiin liittää johdannoksi toiminta-alueiden yleisesittely, jotta saataisiin yhteinen näkemys ohjeistuksen kohteista. Tietoturvan peruseriaatteet käytiin läpi, samoin kuin yhteisöjen riskienhallinnan ja seurannan periaatteet. Tietosuojasta nostettiin esiin muuttuvan lainsäädännön edellyttämät muutokset valvonnan ja ohjeistuksen suhteen. Sopimuksien laadinnassa korostettiin vertailukelpoisuutta tarjouspyyntöjen ja kilpailutusten suhteen sekä sopimuskumppaneiden valintaa ja jatkuvuuden huomiointia esimerkiksi immateriaalioikeuksien suhteen. Toimittajien ja asiakkaiden välisen vastuunjakon selkiyttämistä haettiin yhtenäisellä vastuunjakotaulukolla sekä periaatteellisilla vastuunjaoilla. Verkottuneen talotekniikan perustason tietoturvaa toteuttavat tahot sitoutuvat siihen, että urakoitsija vastaa järjestelmää luovutettaessa sen olevan ajantasainen, ja käytön aikaisesta ylläpidosta vastaa joko asiakas tai ylläpitokumppani sopimuksen mukaan.

Tietoturvatason todentamisesta, mittaamisesta ja arvioinnista sekä testaamisesta kirjoitettiin omat kappaleensa. Näissä korostui järjestelmällisyys ja suunnitelmallisuus sekä auditoinnin merkitys osapuolten motivaattorina. Uusien menetelmien ja -järjestelmien osalta korostettiin toimintatapojen vakiointia ja arviointia. Uusien teknologioiden osalta korostuivat etenkin pilvipalvelut sekä IPv6-tekniikan huomiointi järjestelmiä uusittaessa.

Kehitysehdotuksissa huomioitiin ohjeistuksen ensikertaisuus ja yleisluontoisuus ja annettiin kehitysehdotuksia toimialakohtaiselle tarkentamiselle sekä toiminnan kehittämiseksi esimerkiksi jatkuvan tietoturvaneuvottelukunnan muodossa. Sekä haastatellut että ohjausryhmä toivat positiivisena asiana esille yhtenäisen ohjeistuksen ja uskoivat yhteisen viitekehyksen helpottavan kaikkien osapuolten työtä.

Ohjeistusmateriaaliin laadittiin tarkistuslistat hallinnolliseen, tekniseen ja tilojenhallinnan tietoturvaan sekä julkaistiin lomakerunko verkottuneen taloteknisen järjestelmän tietoturvan itseauditointia varten. Liitemateriaalina ohjeistettiin taloyhtiöiden tietoturvatavoitteiden ja toimintamallin laatiminen sekä mainittiin keskeiset kirjallisuuslähteet. Ohjemateriaali toimitettiin Sähköinfon kustannusmenetelmien kautta

julkaistavaksi keväällä 2015 ja se on yleisesti saatavilla sähköisenä huhtikuusta 2015 ja kirjana kesästä 2015 alkaen.

10.1 Hallinnollinen kattavuus

Ohjeistusta laadittiin huomioiden koko palveluketju loppukäyttäjistä urakoitsijoihin. Kun samaa hallintomallia sovitetaan tuhansien käyttäjien organisaatioista yhden henkilön yksiköihin, joudutaan väistämättä sovittamaan asioita. Hallintomalliin tuotiin välineitä toiminnan sovittamiseksi myös pienempiin organisaatioihin. Asunto-osaakeyhtiöitä varten laadittiin ehdotus tietoturvaperiaatteiden määrittelystä ja hyväksyttämisestä. Samaa mallia voivat käyttää pienyritykset toimissaan. Yksityisten henkilöiden ja asiakkaiden suhteen toivotaan toimintamallien kehittyvän siten, että suoraan kuluttajille suunnatut järjestelmät ja laitteet voidaan liittää ja ylläpitää toimittajien ja urakoitsijoiden ylläpitämien menetelmien puitteissa. Tulevaisuudessa pitänee arvioida, toimivatko markkinat, vai tuleeeko laatia vielä erillinen ohjeistus yksityiskäyttäjien ja loppukäyttäjien toimintaohjeeksi verkottuneen talotekniikan tietoturvaan.

10.2 Tekninen kattavuus

Kohdealueen laajuuden johdosta ohjeistus jäi osin yleisluonteiseksi. Ohjetta on tarpeen täydentää toimialakohtaisilla detaljeihin paneutuvilla oheistuksilla. Joiltakin osin jouduttiin väljentämään alkuperäistä ohjeistusta sen johdosta, että markkinoilla ei ollut riittävän kehittyneitä kenttälaitteita. Tämän johdosta esimerkiksi ehdoton autentikointivaatimus ja kerrostaminen jätettiin kenttälaitteiden vaatimuksista pois ja tukeuduttiin ylemmillä kerroksilla tapahtuvaan segmentointiin ja autentikointiin.

Perustason vaatimuksia on syytä tarkastella muutaman vuoden välein ja korottaa vaatimustasoa uusissa asennuksissa sitä mukaa, kun markkinat monipuolistuvat.

Valmistajien ja urakoitsijoiden vastuuta korostettiin määrittämällä perustason toteutuksen tietoturvan vastuun urakoitsijalle luovutushetkeen saakka ja tästä eteenpäin sovitun vastuunjaon mukaan.

10.3 Työn julkisuusarvo ja tiedottaminen

Työn aikana aihe on kiinnostanut mediaa runsaasti. Työn etenemistä on seurattu mm. alan lehdistössä. Tekijä on kutsuttu useampaan seminaariin esiintymään aiheen pohjalta. Jakeluiden levikki on ollut yhteensä n. 15 000 lukijaa. Lisäksi seminaareissa ja esityksissä tiedon materiaalin julkaisusta ovat saaneet n. 1000 henkilöä.

11 Yhteenveto

Ohjeistusmateriaali julkaistiin huhtikuun lopussa 2015 Sähköinfo Oy:n toimesta, ja ohjausryhmän jäsenet ovat aiemmin ilmoittaneet sitoutuvansa ohjeen käytön edistämiseen. Ohjausryhmän kokoonpano kattaa käytännössä merkittävimmät verkottuneen talotekniikan tuottajat ja käyttäjät, joten voidaan olettaa, että ohjeistuksen käyttöönotto tulee olemaan kattava, ja että sillä tulee olemaan merkittävästi tietoturvaa parantava vaikutus kansallisesti. Ohjeistuksen vaikutuksia ja merkitystä voidaan arvioida muutaman vuoden päästä, kun riittävästi kohteita on saatu verkottuneen talotekniikan tietoturvan perustason piiriin. Ohjeistuksen kehittäminen tulee olemaan jatkuva prosessi, jossa on huomioitava ympäristön kehitys, muuttuvat uhkakuvat ja erityisesti kohderyhmän valmiudet ja mahdollisuudet ohjeen mukaisten ratkaisuiden käyttöön.

Verkottuneen taloteknisen järjestelmän vaatimuksissa korostuu eri osapuolten huomiointi ja toimintaympäristön vaatimusten tasapainotus suhteessa kohdeympäristön toiminnan vaatimuksiin ja riskitasapainoon. Tietoisuus vaikutuspiiristä ja vastuista edistää suunnitelmallisuutta. Yhtenäisen ohjeistuksen toivotaan toimivan yhdyssiteenä verkottunutta talotekniikkaa toteuttavien ja hankkivien tahojen välillä. Työ sai ohjausryhmän keskuudessa yleisen hyväksynnän ja sitä pidettiin merkittävänä avauksena verkottuneen talotekniikan tietoturvatyölle.

On todennäköistä, että loppukäyttäjät ja pienemmät toimijat haluavat hankkia vakioituja ja tuotteistettuja palveluita. Tietoisuus tavoiteltavasta toiminnan tasosta synnyttää kysyntää ja luo uusia markkinoita. Tietoturvan perustason hallinnasta tulee alan toimijoille kilpailuetu, ja tietoturvan perustason tavoittelu johtaa tasalaatuisempaan toimintaan koko palveluketjun osalta.

Lähteet

Ahiola, Anssi ja Degefa, Merkebu Zenebe. 2010. Sähköenergiansäästön potentiaali kotitalouksissa. *Publications in Power Systems and High Voltage Engineering 2010*. 2010. [Viitattu: 26. 04 2015.]

http://www.ece.hut.fi/enete/Energiansaasto_kotitalouksissa.pdf.

Cert-fi varoitus 1. 2013. Kyberturvallisuus Varoitukset. *Viestintäviraasto*. 13. 09 2013. [Viitattu: 25. 04 2015.]

<https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2013/varoitus-2013-01.html>.

Dalakov, Georgi. First computer virus of Bob Thomas. *history of computer*.

[Viitattu: 25. 4 2015.] <http://history-computer.com/Internet/Maturing/Thomas.html>.

Echelon raportti. 1999. EU parlamentti. 1999.

<http://www.europarl.europa.eu/highlights/fi/108.html>.

Garthner. 2015. *Information 2020 - Beyond Big Data*. STAMFORD , Garthner, 2015.

Helsingin yliopisto. 2011. valtiotieteen laitoksen yleisen historian johdantokurssi. *taloushistoriaa käsittelevät luentokalvot*. 2011.

Hyypä ym. 2012. Rakennus- ja kiinteistöalan tulevaisuudennäkymiä. *Metropolia*.

2012. [Viitattu: 26. 04 2015.]

http://www.metropolia.fi/fileadmin/user_upload/Tekniikka_ja_liikenne/Raksa/met_rakennusalan_tulevaisuudennakymia_web-1.pdf.

Kastner, Daniel;Wolfgang, Granzer ja Wolfgang, Kastner. Security for

KNXnet/IP. *KNX*. [Viitattu: 15. 05 2015.]

Kiinteistöliitto. 2014. Korjausbarometri 2014. 2014. [Viitattu: 06. 05 2015.]

Klemmari pysäytti junaliikenteen. 1997. Tietoviikko. 1997.

<http://www.tivi.fi/Uutiset/1997-03-17/Arkistojen-aarteita-N%C3%A4in-klemmari-pys%C3%A4ytti-Etel%C3%A4-Suomen-junat-3157931.html>.

Kämppi, Harri. 2011. KNX-väylätekniikka ja sen kustannusvertailu sairaalassa.

www.thesaus.fi. 2011. [Viitattu: 26. 04 2015.]

<http://www.theseus.fi/bitstream/handle/10024/29837/Inssityo.pdf?sequence=1>.

Laitinen, Terttu. 2011. KORJAUSRAKENTAMINEN 2030. 3. 1 2011. [Viitattu: 15. 5

2015.] <http://www.vtt.fi/inf/julkaisut/muut/2011/VTT-R-10398-10.pdf>.

Leppämäki, Laura. 1998. Tekniikan kehitys ja sen mallit. *Pro Gradu tutkielma,*

Jyväskylän yliopisto. 1998. [Viitattu: 06. 05 2015.]

<https://jyx.jyu.fi/dspace/bitstream/handle/123456789/8148/1320.pdf>.

Lexia. 2014. EU:n tietosuoja-asetus luo uudet tietosuojahaasteet yrityksille. *Lexia*.

2014. [Viitattu: 26. 04 2015.] <http://lexia.fi/fi/2014/07/01/eun-tietosuoja-asetus-luo-uudet-tietosuojahaasteet-yrityksille/>.

Majaniemi, Sami. 2014. *Älykäs kaupunki palveluna*. Helsinki : LVM, 2014.

Neittaanmäki, Pekka ja Lehto, Matti. 2014. Informaatioteknologian tiedekunnan

tutkimus ja koulutusstrategia. *Jyväskylän yliopisto, INFORMAATIOTEKNOLOGIAN TIEDEKUNTA*. 2014. [Viitattu: 26. 4 2015.]

Neuman, John Won. 1966. Theory of self Reproducinc automata. *cba.mit.edu/*.

MIT, 1966. [Viitattu: 19. 03 2015.]

<http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf>.

Paiho, Satu;ym. 2007. Talotekniikan kehitysnäkymiä. VTT, 2007. [Viitattu: 19. 03

2015.] <http://www.vtt.fi/inf/pdf/tiedotteet/2007/T2379.pdf>.

Piikkilä. 2006. Kiinteistöjen tiedonsiirtoväylät. [kirjan tekijä] Veijo Piikkilä. *ST käsikirja*

21. Helsinki : Sähkötieto ry, 2006, s. 267.

Pirainen, Antti ja Saarinen, Jani. 2015. Korjausrakentaminen muuttuu palveluksi, Raportti. *Korjausrakentamisen kehittäminen, Rakennettu ympäristö, Tekes.* 02 2015. [Viitattu: 26. 04 2015.] http://www.tekes.fi/globalassets/global/ohjelmat-ja-palvelut/ohjelmat/rakennettu-ymparisto/aineistot/korjausrakentamisen-kehittaminen_raportti_17-2-2015.pdf.

Santalainen, Timo. 2009. *Strateginen ajattelu ja toiminta.* Helsinki : Talentum, 2009.

Savolainen, Pekka;ym. 2013. *AMM Tietoturva.* Helsinki : VTT, 2013.

Seppo Tiilikainen, Jukka Manner. 2013. Suomen automaatioverkkojen haavoittuvuus. *Aalto.* 2013. [Viitattu: 26. 04 2015.] <https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf>.

Stenvall, Jari ja Virtanen, Petri. 2007. *Muutostsa Johtamassa.* Helsinki : Edita, 2007. ISBN: 978-951-37-4861-6 .

Ståhlberg, Mika. 2010. viestiupseeriyhdistys. 2010. [Viitattu: 19. 3 2015.] http://www.viestiupseeriyhdistys.fi/viestimies/vm4_10/Stuxnet_vm4_10.pdf.

Suomen Automaatioseura. 2010. *Teollisuusautomaation Tietoturva, verkottumisen riskit ja niiden hallinta.* Helsinki : Suomen Automaatioseura ry, 2010.

ST ohje 2015. *Verkottuneen talotekniikan tietoturvaohje* Espoo: Sähkötieto ry 2015, ISBN 978-952-231-163-4 (painettu) ISBN 978-952-231-152-8 (pdf)

Tietokonevirus sulki Nordean konttoreita Suomessa. 2003. Nordea, konserniviestintä. *Lehdistötiedote.* 2003. [Viitattu: 25. 04 2015.] http://newsroom.nordea.com/fi/2003/08/14/tietokonevirus-sulki-nordean-konttoreita-suomessa/?doing_wp_cron=1429954043.6163260936737060546875.

Tietosuoja, rekisteriseoste. 2009. 2009. [Viitattu: 14. 05 2015.] <http://www.tietosuoja.fi/fi/index/useinkysyttya/rekisteriseloste.html>.

Tietosuoja-asetus pakottaa julkisyhteisöt muuttamaan toimintamallejaan.

2014. Asianajajaliitto. 2014. [Viitattu: 14. 05 2015.]

http://www.asianajajaliitto.fi/viestinta/oikeudellisia_uutisia/euroopan_unioni/2014/stt_info_eu_n_yleinen_tietosuoja-asetus_pakottaa_julkisyhteisot_ja_yritykset_muuttamaan_toimintamallejaan.7865.news.

Tietotekniikka-alan osaamistarpeet. 2013. Teknologiateollisuus. 2013. [Viitattu: 14. 05 2015.]

https://teknologiateollisuus.fi/sites/default/files/file_attachments/elinkeinopolitiikka_osaaminen_osaajatarpeet_tietoturva-alan_ennakointiselvitys.pdf.

Tiilikainen, Seppo ja Manner, Juha. 2013. *Suomen automaatioverkkojen haavoittuvuus*. Helsinki : Aalto yliopisto, 2013.

tilakeskus, Tampereen kaupungin. 2005. Talotekniikan dokumentoiniohje. 17. 10 2005. [Viitattu: 15. 05 2015.]

http://www.tampere.fi/tiedostot/5kqZl7T17/tike_talotekniikanohje.pdf.

TJX:ltä 45 M luottokorttitietoa. 2007. Digitoday. 2007. [Viitattu: 19. 03 2015.]

<http://www.digitoday.fi/tietoturva/2007/03/30/tjxlta-vuoti-46-miljoonaa-korttinumeroa/20077954/66>.

Tokola, Hyyppä. 2004. *Konsultaatiotyön perusteita (Pekka Tokola, Harri Hyyppä)*. Oulu : Metanoia instituutti, 2004.

Työelämän tietosuoja. 2009. Tietosuojavaltuutettu. 2009. [Viitattu: 14. 05 2015.]

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/asiaatietosuojasta/0ek90IONL/Tyoelaman_tietosuoja_-kasikirja.pdf.

Vahti ohje. 2009. 2009. [Viitattu: 14. 05 2015.]

<https://www.vahtiohje.fi/web/guest/602>.

Vahti ohje; tietoturvallisuuden hallinnointimenetelmät. 2009. Vahti ohje.

2009. [Viitattu: 14. 05 2015.] <https://www.vahtiohje.fi/web/guest/test>.

Wiio, Osmo A. 1970-2009. Viestintä yleensä epäonnistuu – paitsi sattumalta. *Wiion lait viestinnästä ja tulevaisuudesta*. Espoo : Deltakirja, 1970-2009.

Wikileaks - informaationsodan alku. 2011. Yle. 2011. [Viitattu: 19. 03 2015.]
<http://yle.fi/aihe/artikkeli/2011/02/22/wikileaks-informaationsodan-alku>.

Vinha, Juha. 2015. Eistemääriä ei kannata lisätä, entä talotekniikkaa?
Rakennuslehti. 15. 2 2015. [Viitattu: 26. 4 2015.]
<http://www.rakennuslehti.fi/blogit/eristemaaria-ei-kannata-lisata-enta-talotekniikkaa/>.

Virus writers. 2003. Virus writers. CNN, 2003.
<http://edition.cnn.com/2003/TECH/internet/03/19/virus.writers.reut/>.

Zikopoulos, deRoos, Bienko, Bulio, Andrews. 2015. Bigdata beyond the hype. *a guide to conversation for today's data center*. Usa : Mc Graw-Hill, 2015, p. 358.

Åberg, Leif. 2000. *Viestinnän johtaminen*. Helsinki : Inforviestintä, 2000. ISBN 9789525123258.

Verkottuneen talotekniikan tietoturvaohje

JULKAISIJA

Copyright · Sähkötieto ry
Harakantie 18 B, 02650 Espoo
PL 55, 02601 Espoo
Puhelin 09 547 610
www.sahkotieto.fi

KUSTANTAJA

Sähköinfo Oy
Harakantie 18 B, 02650 Espoo
PL 55, 02601 Espoo
Puhelin 09 547 610
www.stul.fi

PÄÄTOIMITTAJA

Kimmo Arenius, Sähköinfo Oy

KIRJOITTAJA

Janne Ollenberg, Tietoturva ry

Sisällys

1 Johdanto

2 Käsitteitä

3 Tietoturvaan ja turvallisuuteen liittyvät säädökset, standardit ja ohjeet

3.1 Tietoturvan hallinnointi Suomessa

4 Palveluliiketoiminnan kehittyminen.

4.1 Rakennusautomaatioalan palveluliiketoiminta

4.2 Audiovisuaalisen viestintäalan palveluliiketoiminta

4.3 Turvallisuusalan palveluliiketoiminta

4.4 Palvelujen yhdyntyminen

5 Tietoturvan periaatteet verkottuneen talotekniikan järjestelmissä

5.1 Tietojärjestelmien ja verkottuneiden talotekniikkajärjestelmien ominaispiirteitä

5.2 Tietoturvauhat ja -haitat

5.3 Tietoturvan hallinnan periaatteet

5.4 Tietosuojan hallinta.

5.5 Sitoutuminen tietoturvaan ja tietoturvan kehittäminen

5.6 Riskien hallinta

5.6.1 Riskien arvottaminen ja riskikartoitus

5.7 Sopimukset

5.7.1 Sopimusten hallinta

- 5.7.2 Yleiset sopimusmallit ja niiden erityispiirteet
- 5.7.3 Sopimusriskien hallinta
- 5.8 Tietoturvatason todentaminen
- 5.9 Tietoturvatason arviointi
- 5.10 Tietoturvan mittaaminen ja testaus
 - 5.10.1 Ohjelmisto- ja tietoliikennejärjestelmien ja-tuotteiden tietoturvan testaus
 - 5.10.2 Toiminnan, tuotteiden ja palveluiden sertifiointit
- 6 Tietoturvan hallinta verkottuneen talotekniikan järjestelmissä
 - 6.1 Toimiminen monitoimittajaympäristössä
 - 6.2 Eri-ikäiset järjestelmät ja käyttöjärjestelmien elinkaari
 - 6.3 Vaatimukset toimittajille
 - 6.4 Vaatimukset asiakkaille
 - 6.5 Tietoturvavaatimusten tasapainotus
 - 6.6 Käyttäjien tunnistaminen.
 - 6.7 Sanomien ja kommentojen hallinta
 - 6.8 Poikkeamien hallinta.
 - 6.9 Jatkuvuussuunnittelu
 - 6.10 Toipumis- ja palautussuunnittelu
 - 6.11 Ratkaisujen vakiointi
 - 6.12 Muutosten arviointi ja testaus
 - 6.13 Liikenteen seuranta
 - 6.14 Verkkoyhteydet
 - 6.14.1 Langattomat tekniikat
 - 6.15 Uudet ratkaisut ja tekniikat
 - 6.15.1 Pilvipalvelut
 - 6.15.2 Ulkoisten järjestelmien käyttö ohjauksessa
 - 6.15.3 IPv6 ja internetin kehitys
- 7 Verkottuneen talotekniikan tietoturvan muistilista
 - 7.1 Yleinen muistilista
 - 7.2 Hallinnollinen muistilista
 - 7.3 Teknisen tietoturvan muistilista
 - 7.4 Tilaturvallisuuden muistilista
 - 7.5 Itsearviointi
- 8 Ehdotuksia verkottuneen talotekniikan tietoturvaa edistäviksi jatkotoimenpiteiksi
- 9 Esimerkki vastuunjakotaulukosta

10 Esimerkki taloyhtiön tietoturvasta

10.1 Esimerkki taloyhtiön tietoturvatavoitteista

10.2 Esimerkki taloyhtiön tietoturvatoimintamallista

11 Kirjallisuutta ja viitteitä.

12 Organisaatioita