VIISAS KANGAS

JYVÄSKYLÄN KANKAAN KYBERTURVALLISUUSSTRATEGIA

Kesä 2015

Sisältö

1. Johdon tiivistelmä

Kankaan alueen kyberturvallisuusstrategian tavoitteena on määrittää ne strategiset linjaukset, joiden avulla tässä dokumentissa kuvattu kyberturvallisuuden visio tullaan saavuttamaan.

Älykäs kaupunki tai kaupungin osa, kuten Kankaan alue, koostuu kasvavasta määrästä tietoverkkoihin kytkettyjä laitteita ja järjestelmiä. Siinä missä perinteisillä alueilla muutoksia tapahtuu hitaasti, älykkäät kaupungit ja niiden järjestelmät kehittyvät nopeammalla syklillä. Voidaankin ajatella, että älykäs kaupunki ei ole missään vaiheessa valmis, vaan se on ajan myötä kehittyvä järjestelmien kokonaisuus. Kyberturvallisuuden näkökulmasta tämä tarkoittaa sitä, että turvallisuuden mahdollistaminen rakennusaikana on edelleen tärkeää, mutta painopiste kyberturvallisuuden varmistamisessa on jatkuvassa työssä koko alueen elinkaaren ajan.

Strategia määrittää kolme kulmakiveä, joihin kyberturvallisuuden kehittäminen ja operatiivinen toiminta Kankaan alueella tulisi perustaa. Kulmakivet ovat hallintamalli, sopimuksellinen velvoittaminen ja riskeihin perustuvat toimintasuunnitelmat. Kulmakivet on esitelty yksityiskohtaisesti dokumentin luvussa viisi. Kulmakivien taustalla vaikuttavat kolme yleisempää Kankaan alueen periaatetta; avoin, älykäs ja kokeileva.

Kulmakivien lisäksi strategia sisältää luvussa kuusi toiminnoittain jaoteltuja kannanottoja kyberturvallisuuden toteuttamiseen. Kannanotot ovat linjauksia, joita alueellisen kyberturvallisuuden kehittämisessä ja operatiivisessa toiminnassa tulisi noudattaa mahdollisuuksien mukaan. Kannanotot ovat sidoksissa strategian toimeenpanosuunnitelmissa esiteltyihin konkreettisiin toimenpiteisiin kyberturvallisen Kankaan alueen rakentamiseksi ja ylläpitämiseksi.

Kankaan alueen kyberturvallisuusstrategia perustuu merkittävästi pitkän aikavälin kehittämistoimintaa ohjaavan hallintamallin käyttöönottoon, koska jo pelkästään alueen rakentaminen tapahtuu usean kymmenen vuoden aikana. Tulevaisuuden uhkiin ei voida kattavasti varautua tänään, vaan on kehitettävä kyvykkyys, jolla toimintaympäristön muutoksiin voidaan varautua kaikista turvallisuuden näkökulmista. Tästä syystä on tärkeää luoda toimintamalleja, joilla kyberturvallisuutta kehitetään ja hallitaan jatkuvasti koko alueen elinkaaren ajan. Näin voidaan paremmin varautua tulevaisuuden uhkiin ja varmistaa alueen toiminnan jatkuvuus myös uhkien realisoituessa.

Hallintamallin toteuttamisesta vastuussa on Jyväskylän kaupunki. Alueen muita toimijoita ei voida pakottaa mukaan synnyttämään hallintamallia, joten kaupungin tulee resurssien ja koordinoinnin avulla tarjota toimijoille houkutteleva mahdollisuus osallistua kyberturvallisen Kankaan alueen kehittämiseen.

Kankaan alueen kyberturvallisuuden visio ei toteudu ilman riittävää resursointia. Kyberturvallisuus ei myöskään ole normaaleista operatiivisista toiminnoista irrallinen kokonaisuus, vaan sen pitäisi olla sisäänrakennettuna kaikessa toiminnassa. Siten myös kyberturvallisuuden resursointi tulisi tapahtua osana investointien ja operatiivisen toiminnan resursointia. Tämä tarkoittaa myös sitä, että hankinnoissa tulee toiminnallisten vaatimusten lisäksi kiinnittää aiempaa enemmän huomiota turvallisuusvaatimuksiin. Lisäksi strategiassa on tunnistettu, että joukkoistaminen voisi toimia uudenlaisena mahdollisuutena saada resursseja kyberturvallisuuden kehittämiseen julkisen ja markkinalähtöisen rahoituksen lisäksi.

2. Termit, lyhenteet ja viittaukset

2.1 Termit ja lyhenteet

Termi tai lyhenne	Kuvaus
Alueverkko	Alueellinen tiedonsiirtoverkko. Tässä dokumentissa alueverkolla ei tarkoiteta sähkönsiirtoverkkoa.
Avoin tieto, open data	Vapaasti saatavilla ja muokattavissa oleva tieto, jonka käyttöä, muokkausta ja uudelleenjakelua ei rajoiteta.
Henkilötieto	Kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. (Henkilötietolaki 523/1999)
ICT	Information and communication techonology, tieto- ja viestintäteknologia
IoT	Internet of Things, esineiden internet
JHS	Julkishallinnon suositukset
JYVSECTEC	Jyväskylän ammattikorkeakoulun kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus
Jäännösriski	Riskin jäljelle jäävä osuus, jota ei haluta tai voida poistaa.
KaPA	Kansallinen palveluarkkitehtuuri -hanke
Katakri	Kansallinen turvallisuusauditointikriteeristö
Kiinteistöverkko	Kiinteistöihin rakennettava verkko, jota käytetään kiinteistöautomaatiojärjestelmien tiedonsiirtoon.
Musta verkko	Kankaan alueen valokuituverkko, joka tullaan toteuttamaan osana kunnallistekniikan rakentamista.
Rova	Kansallisen palveluarkkitehtuurin Rooli- ja valtuutuspalvelu
Smart city, älykaupunki	Kaupunki, jolla pyritään parantamaan julkisia asioita ICT-pohjaisten ratkaisujen pohjalta eri sidosryhmien yhteistyöllä

2.2 Viitatut dokumentit

Antikainen Antti, ”*Risk-Based Approach as a Solution to Secondary Use of Personal Data*”, Helsingin yliopisto, 2014

Euroopan unionin neuvosto, ”*Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa*”, COM/2013/048 final - 2013/0027 (COD)

Euroopan unionin neuvosto, ”*Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö*”, 7.2.2013

Henkilötietolaki 523/1999, Helsinki, Oikeusministeriö, 22.4.1999.

Huoltovarmuuskeskus, ”*Mallilausekkeita – sopimuksen kohta toiminnan jatkuvuus*”, 15.5.2009

Huoltovarmuuskeskus, ”*Toiminnan jatkuvuuden hallinta*”, 15.5.2009

Information Commissioner’s Office (UK), ”*Anonymisation: managing data protection risk: code of practice*”, 2012

JUHTA - Julkisen hallinnon tietohallinnon neuvottelukunta, ”*JHS 189 Avoimen tietoaineiston käyttölupa*”, 11.12.2014

Jyväskylän kaupunki, ”*Viisas Kangas - Jyväskylän Kankaan ICT-ratkaisujen kokonaissuunnitelma*”, 2015

Liikenne- ja viestintäministeriö, ”*Matkaviestinverkon kuuluvuusongelmat matalaenergiarakennuksissa – työryhmän raportti*”, 1.10.2013

Liikenne- ja viestintäministeriö, ”*Älykäs kaupunki – Smart City Katsaus fiksuihin palveluihin ja mahdollisuuksiin*”, 13.5.2014

Puolustusministeriö, ”*Katakri - Tietoturvallisuuden auditointityökalu viranomaisille*”, 2015

Rakennustieto, “*Turvalliset työympäristöt. Toimitilat*”, RT 08-11097, 22.11.2012

Rossouw von Solms, Johan van Niekerk, “*From information security to cyber security*”, Computers & Security, Volume 38, October 2013, Pages 97-102, ISSN 0167-4048

Tietosuojavaltuutetun toimisto, ”*Henkilötietojen käsittely suostumuksen perusteella*”, 27.7.2010

Tietoyhteiskuntakaari 917/2014, Helsinki, Liikenne- ja viestintäministeriö, 7.11.2014

Turvallisuuskomitean sihteeristö, ”*Suomen kyberturvallisuusstrategia ja taustamuistio*”, 24.1.2013

Valtiovarainministeriö, ”*VAHTI 2/2013 Toimitilojen tietoturvaohje*”, 2013

Viestintävirasto, ”*Kiinteistöjen laitetilojen lukitus*”, 306/2015

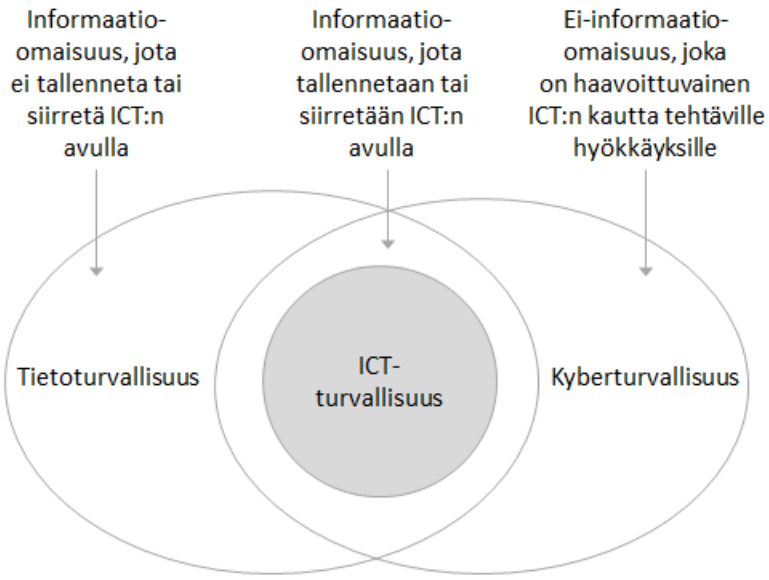
Viestintävirasto, ”*Määräys 65 kiinteistön sisäverkoista ja teleurakoinnista*”, 65A/2014

Viestintävirasto, ”*Suojaamattomia automaatiolaitteita suomalaisissa verkoissa*” 29.6.2015

3. Strategian taustoitus

3.1 Mitä on kyberturvallisuus?

Tässä strategiassa kyberturvallisuudella tarkoitetaan ensisijaisesti internetiin ja muihin tietoverkkoihin kytkettyjen laitteiden ja palveluiden turvallisuutta. Kuva 1 (von Solms & van Niekerk, 2013) jäsentää tietoturvallisuutta, ICT-turvallisuutta ja kyberturvallisuutta. Sen mukaan kyberturvallisuus pitää sisällään perinteisen tietoturvallisuuden lisäksi myös ei-informaatio-omaisuuden turvaamisen. Tällaista omaisuutta ovat esimerkiksi kiinteistöjen etäohjausjärjestelmät, jotka eivät varsinaisesti sisällä tietoa, mutta joilla voidaan tietoverkon kautta tehdä erilaisia toimintoja.



Kuva 1: Tietoturvallisuus, ICT-turvallisuus ja kyberturvallisuus

Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua.

Kyberturvallisuuden tarkastelussa ei pidä unohtaa kokonaisturvallisuuden eri näkökulmien huomioimista. Ihmisten ymmärrys, asenteet, ohjeistukset, toimintatavat ja fyysiseen tilaturvallisuuteen liittyvät seikat ovat tärkeitä ja vaikuttavat osaltaan myös kyberturvallisuuteen. Näin ollen esimerkiksi huolimaton tai taitamaton salasanojen käsittely voi johtaa ICT:n kautta tehtävään hyökkäykseen tai laitetilojen riittämätön fyysinen turvallisuus voi aiheuttaa uhan kyberturvallisuudelle. Tässä strategiassa tarkastellaan muita kokonaisturvallisuuden näkökulmia siinä laajuudessa kuin on tarpeen kokonaisuuden kyberturvallisuuden saavuttamiseksi.

3.2 Kyberturvallisuusuhat

Kankaan alue tulee olemaan Smart City teeman mukainen älykäs kaupunkialue, jossa hyödynnetään modernin tieto- ja viestintäteknologian mahdollisuuksia.

Teknologian kehittyminen, etäyhteydet sekä järjestelmien ja laitteiden tiiviimpi keskinäinen integroituminen mahdollistavat monia hyviä asioita, mutta lisäävät samalla

alueiden haavoittuvuutta ja kyberriskejä. Älykkäässä kaupunki-infrastruktuurissa on paljon kohteita, joihin kohdistuu uhkia. Älykkäät laitteet, automaatio, ohjausjärjestelmät, ihmisten käyttämät päätelaitteet ja tietoliikenneinfrastruktuuri muodostuvat yhä monimutkaisemmista ja useimmiten internetiin kytketyistä tietojärjestelmistä, mikä altistaa ne enenevässä määrin kyberturvallisuusuhille. Tulevaisuudessa tällaisten kohteiden lukumäärä tulee kasvamaan entisestään.

Kaupunkiympäristössä toimivien laitteiden suuresta määrästä johtuen niiden etäohjaus ja laitteiden keräämien tietojen siirto sähköisesti ovat välttämättömyyksiä. Tämän seurauksena laitteet ovat myös alttiimpia tietoverkkojen kautta tuleville hyökkäyksille.

Toteutuessaan kyberturvallisuusuhkilla voi olla älykkäässä kaupunkiympäristössä hyvin merkittävät vaikutukset. Ongelmatilanteiden seuraukset voivat olla sekä laajoja että vakavia. Laaja sähkö- tai tietoliikennekatkos tai ohjausjärjestelmän toimimattomuus voi halvaannuttaa koko alueen toiminnan.

Kyberturvallisuusuhkia voivat aiheuttaa tavallisten ihmisten virheellinen toiminta, teknologian ja järjestelmien virheet, kyberilkivalta, kyberrikollisuus, kyberterrorismi sekä kybersodankäynti.

Ohjelmistoista löytyy säännöllisesti haavoittuvuuksia, mikä altistaa niihin tukeutuvat järjestelmät hyökkäyksille. Järjestelmissä olevien haavoittuvuuksien hyödyntäminen, palvelunestohyökkäykset ja muut kyberturvallisuutta vaarantavat toimet ovat nykyään helppoja toteuttaa. Kankaan alue on suuren näkyvyyden vuoksi houkutteleva kohde, minkä vuoksi hyökkäykset eivät ole pelkästään uhkia vaan ennemminkin realiteetteja, joiden säännölliseen toteutumiseen tulee varautua.

Usein yksinkertaisilla ja edullisilla haittatoimenpiteillä voidaan aiheuttaa suuria vahinkoja, minkä vuoksi kyberuhilta suojautumisen kustannukset kasvavat. Kybermaailmassa suojautumisen kustannukset ovat tyypillisesti korkeammat verrattuna hyökkäyskustannuksiin.

Samaan aikaan, kun teknologia on kehittynyt ja puolustautumiseen on uudenlaisia menetelmiä, ovat myös hyökkäys- ja hyväksikäyttömenetelmät kehittyneet. Kun aiemmin palvelunestohyökkäyksen toteuttaminen vaati asiantuntemusta ja resursseja, niin nykyisin ei tarvita syvällisempää IT-osaamista.

Varautumisen lähtökohtana tulee olla kyberturvallisuuden riskianalyysi, jossa arvioidaan sekä riskin toteutumisen todennäköisyyttä että vaikutusten suuruutta. Toimenpiteet uhkien torjumiseksi tulee suhteuttaa riskiarvioinnin tuloksiin huomioiden suojautumisen kustannukset. Kaikilta uhilta ei voida suojautua, joten tavoitteena on kohottaa kybersietoisuutta järkevin kustannuksin.

3.3 EU:n kyberturvallisuusstrategia

Euroopan unionilla on vuonna 2013 laadittu kyberturvallisuusstrategia, jonka avulla EU:n laajuisesti pyritään hallitsemaan kyberavaruuden kehityksen myötä tapahtunutta toimintaympäristön muutosta. EU:n kyberturvallisuusstrategia perustuu seuraaviin periaatteisiin:

1. EU:n ydinarvot pätevät yhtä hyvin digitaalisessa kuin fyysisessäkin maailmassa
2. Perusoikeuksien, ilmaisunvapauden, henkilötietojen ja yksityisyyden suojaaminen
3. Pääsy kaikille
4. Demokraattinen ja tehokas monen toimijan hallinto

5. Yhteinen vastuu tietoturvan varmistamisesta

Periaatteet strategian takana pyrkivät takaamaan kaikille yhtäläiset oikeudet internetin käyttämiseen ja yksityisyyden suojaan sekä demokratian toteutumisen myös verkossa. Strategiassa tunnistetaan, että internetin toiminnasta ja operoinnista vastaavat pääasiassa yritykset, mutta on käynyt ilmeisemmäksi, että niille on kohdistettava regulaation kautta vaatimuksia liittyen läpinäkyvyyteen, vastuukysymyksiin ja tietoturvaan. Strategia itsessään perustuu viidelle painopisteelle, jotka ovat:

1. Verkon vakaus
2. Verkkorikollisuuden huomattava vähentäminen
3. Yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) liittyvän verkkopuolustuspolitiikan ja valmiuksien kehittäminen
4. Kyberturvallisuuteen liittyvien teollisten ja teknologisten voimavarojen kehittäminen
5. Johdonmukaisen kansainvälisen verkkotoimintapolitiikan luominen Euroopan unionille sekä EU keskeisten arvojen edistäminen

EU:n laajuiseen kyberturvallisuuden edistämiseen ja kehittämiseen liittyy monimutkainen ja haastava toimijaympäristö, jossa on vaihtelevia toimivaltuuksia. Tämän vuoksi EU tasoinen ohjaus ei ole vaihtoehto, vaan vastuu on siirretty jäsenmaille. EU tasolla toiminta on lähinnä kansallisia toimintoja tukevaa ja koordinoivaa, vaikka strategiassa onkin tunnistettu, että riskit ja uhat verkossa ylittävät valtiolliset rajat.

EU on myös ottamassa käyttöön verkko- ja tietoturvadirektiivin (network and information security, NIS), joka on julkaistu tunnisteella 2013/0027. Ehdotetulla NIS-direktiivillä on tärkeä osa EU:n kyberturvallisuusstrategian toteuttamisessa.

Ehdotuksen mukaan kaikkien EU:n jäsenvaltioiden, keskeisten internetyhtiöiden ja infrastruktuurien ylläpitäjien olisi varmistettava turvallinen ja luotettava digitaaliympäristö kaikkialla EU:ssa. Direktiivi koskee esimerkiksi sähköisen kaupankäynnin alustojen, verkkoyhteisöpalvelujen sekä liikenne-, pankki- ja terveydenhuoltopalvelujen tarjoajia. Verkko- ja tietoturva-alalla toiminta perustuu pääsääntöisesti tällä hetkellä vapaaehtoisuuteen, joten kansalliset valmiudet, yksityisen sektorin osallistuminen ja varautumistaso vaihtelevat huomattavasti eri jäsenvaltioissa. Tämän vuoksi direktiiviehdotuksen tavoitteena on yhtenäistää toimintaedellytyksiä ottamalla käyttöön kaikissa EU-maissa sovellettavat yhdenmukaiset säännöt.

3.4 Suomen kansallinen kyberturvallisuusstrategia

Suomen kansallinen kyberturvallisuusstrategia julkaistiin vuoden 2013 alussa. Kansallinen strategia määrittää vision, jossa Suomi pystyy toisaalta vahvan osaamisen mutta myös tiiviin ja luottamuksellisen yksityisen sekä julkisen sektorin yhteistyön kautta nousemaan kyberturvallisuuden kärkimaaksi. Vision perusteella Suomesta tulee kyberturvallisuuden edelläkävijä, joka pystyy turvautumaan kaikissa tilanteissa kyberuhkia vastaan.

Vision saavuttamiseksi strategia määrittää toimintamallin, jossa kyberturvallisuuden johtamisesta vastaa ylimmällä tasolla valtioneuvosto, mutta kukin ministeriö vastaa oman toimialansa kyberturvallisuuden organisoimisesta. Johtamisen perustana toimii tilannekuva, jonka muodostamiseksi tarvitaan laaja-alaista yhteistyötä viranomaisten, yritysten ja järjestöjen välillä sekä kansainvälistä yhteistoimintaa. Osaamisen oletetaan

kehittyvän keskeiseltä osin yritystoiminnan kautta, jota pyritään tukemaan erilaisin kannustimin ja lainsäädännöllisin keinoin.

Kansallinen kyberturvallisuusstrategia sisältää kymmenen linjausta vision saavuttamiseksi:

1. Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli.
2. Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä.
3. Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.
4. Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.
5. Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.
6. Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.
7. Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.
8. Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.
9. Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.
10. Strategian toimeenpanoa valvotaan ja toteumaa seurataan.

Strategian mukana julkaistussa taustamuistiossa todetaan, että toiminnan tuloksellisuus ja vaikuttavuus ovat suoraan riippuvaisia käytettävistä taloudellisista ja henkisistä voimavaroista.

3.5 Jyväskylä kansallisena kyberturvallisuuden toimijana

Jyväskylään on syntynyt vuoden 2010 jälkeen merkittävä kyberturvallisuuden osaamiskeskittymä. Jyväskylä valittiin vuonna 2013 Innovatiiviset kaupungit (INKA) -ohjelman kyberturvallisuuden osa-alueen vetäjäksi. Jyväskylässä toimii useita kyberturvallisuusalalla toimivia yrityksiä sekä julkishallinnon yksiköitä.

Jyväskylän ammattikorkeakoulu sekä Jyväskylän yliopisto tarjoavat molemmat kyberturvallisuuteen liittyviä opintokokonaisuuksia. Lisäksi ammattikorkeakoulun alaisuudessa toimii JYVSECTEC kyberturvallisuuden tutkimus-, koulutus- ja kehityskeskus, jolla on käytössään kansallisesti ainutlaatuinen kyberturvallisuuden testaus-, harjoitus- ja koulutusympäristö. Jyväskylän yliopistossa on mahdollista opiskella aihetta informaatioturvallisuuden maisteriohjelmassa sekä kyberturvallisuuden sivuainekokonaisuudessa.

3.6 Kankaan alue kyberturvallisuuden pilottiympäristönä

Kankaan alueesta on mahdollista rakentaa ympäristö, joka hyötyy Jyväskylän kyberturvallisuuden osaamiskeskittymästä sekä tarjoaa kyberturvallisuuden edelleen kehittämiseen uusia mahdollisuuksia. Toisaalta Kankaalle voidaan luoda kaupunkiympäristöä, jossa erityistä kyberturvallisuutta vaativat yritykset voivat toimia aiempaa helpommin.

Kankaan alueella on hyvät edellytykset toimia kyberturvallisuuden pilottiympäristönä. Alueen ICT-ratkaisujen periaatteissa oleva kyseenalaistava ote, Jyväskylän kaupungin vahva panostus alueen kehittämiseen, alueelle toteutettavat edistykselliset tekniset ratkaisut, oppilaitosten osallistuminen alueen kehittämiseen, ICT-yritysten kiinnostus alueesta, alueelle kaavaillut digitaalisuutta hyödyntävät palvelutoiminnot sekä alueen sopiva koko edesauttavat kaikki Kankaan alueen toimimista kyberturvallisuuden pilottiympäristönä.

Uudenlaiset teknologiset ratkaisut rakennettuna laajalle alueelle mahdollistavat uudenlaisten palveluiden kokeilemisen. Esimerkiksi alueellinen sähköinen kulunvalvonta voi toimia merkittävänä katalyyttinä palvelukehitykselle.

Aktiivinen oppilaitosten osallistuminen yhdistettynä kehittyneeseen teknologiaympäristöön mahdollistaa myös laajemmat poikkitieteelliset pilotointihankkeet, joilla voidaan kehittää uudenlaisia toimintamalleja esimerkiksi vanhusasumisen alueella. Tällöin teknologian kautta saavutettavia hyötyjä voidaan tutkia muillakin tutkimusaloilla kuin pelkästään ICT-toimialalla.

Kun pilotointi huomioidaan jo varhaisessa vaiheessa alueen suunnittelua ja rakentamista, parantavat pilotointimahdollisuuksien huomioonottaminen sopimuskäytännöissä, kerätyn tietoaineiston tietoturvallinen hallinta sekä alueportaalin hyödyntäminen pilotoinnissa tai siitä viestimisessä edelleen alueen edellytyksiä toimia pilotointiympäristönä.

Kyberturvallisuuden pilottiympäristön hyödyntäminen on hyvin vastuullista toimintaa eikä pilotoinnin yhteydessä voida ottaa riskejä Kankaan alueen asukkaiden turvallisuuden suhteen. Pilotointien huolellinen suunnittelu sekä pilotointiin osallistuvien ihmisten tietojen turvallinen käsittely ovat edellytyksinä pilotointien toteuttamiselle.

3.7 Strategian tuottaminen

Tämän strategian on tuottanut Jyväskylän kaupungin toimeksiannosta Relator Oy. Strategian kirjoittamisesta ovat vastanneet Relator Oy:n konsultit Riku Nykänen ja Olli Pitkänen. Strategian tavoitteiden ja sisällön tuottamiseksi on järjestetty useita työpajoja kesän 2015 aikana.

Strategian tuottamiseen ovat osallistuneet työpajoihin osallistumalla tai muuten strategiaa kommentoimalla seuraavat henkilöt organisaatioittain:

- Anne Sandelin, Jyväskylän kaupunki
- Tanja Oksa, Jyväskylän kaupunki
- Anu Hakala, Jyväskylän kaupunki
- Erkki Jaala, Jyväskylän kaupunki
- Mika Kataikko, Jyväskylän Seudun Kehittämisyhtiö Jykes Oy

- Pekka Vepsäläinen, Jyväskylän Seudun Kehittämisyhtiö Jykes Oy
- Miska Sulander, Cynetkey Oy
- Martti Lehto, Jyväskylän yliopisto
- Pasi Tyrväinen, Jyväskylän yliopisto
- Mika Karjalainen, Jyväskylän ammattikorkeakoulu
- Timo Taskinen, Tekes
- Kari Helislahti, Jyväskylän Energia Oy
- Janne Pirttimäki, Jyväskylän Energia Oy
- Jarkko Saarimäki, Viestintäviraston Kyberturvallisuuskeskus
- Sami Orasaari, Viestintäviraston Kyberturvallisuuskeskus

3.8 Strategian toteutumisen riskit

Strategian toteutumiseen kohdistuu monia riskejä, jotka voivat realisoitua aktiivisen turvallisuustoiminnan laiminlyömisen seurauksena. Kankaan alueen kyberturvallisuus ei toteudu itsestään. Liiketoimintalähtöisen palvelutuotannon tueksi tarvitaan kyberturvallisuuden valmiuksien huomioonottamista jo alueen suunnittelu- ja toteutusvaiheissa sekä myöhemmin aktiivista turvallisuusasioiden hallintaa koko elinkaaren ajan.

Merkittävin strategian toteutumisen riski on resurssien puute. Kuten kansallisen kyberturvallisuusstrategian, on myös Kankaan alueen kyberturvallisuusstrategian toteutuminen sidoksissa käytettävissä olevien resurssien määrään. Resurssien ei tarvitse olla kuitenkaan irrallisia kyberturvallisuuteen kohdistettuja resursseja, vaan kyberturvallisuus tulisi ottaa huomioon osana kaikkia alueen toimintoja, joihin se liittyy.

Resurssien puute voi myös myötävaikuttaa seuraavien riskien realisoitumiseen.

- Infrastruktuuri jää turvattomaksi: mikäli infrastruktuurin toteutuksessa ei huomioida riittävästi turvallisuusnäkökohtia, lisääntyy alueen haavoittuvuus. Infrastruktuurin turvattomuus voi johtaa siihen, että sen varaan ei uskalleta toteuttaa kaavailtuja palveluita ja Kankaan alueen visio älykkäästä kaupunkiympäristöstä jää toteutumatta.
- Aktiivisen valvonnan puuttuminen: kyberturvallisuus edellyttää kykyä havaita vaaralliset tilanteet sekä vaaratilanteissa aktiivisia toimenpiteitä tilanteen pysäyttämiseksi, vahinkojen korjaamiseksi ja havaittujen aukkojen tukkimiseksi. Mikäli tällaista valmiutta ei ole, voivat vahingot hyökkäystilanteissa nousta suuresti.
- Turvallisuuden jääminen suunnitteluasteelle: turvallisuusasioiden suunnittelu itsessään on hyvä asia, mutta käytännön hyödyt suunnittelusta saadaan vasta suunnitelmien toimeenpanon myötä. Ilman aktiivista toimeenpanon ohjausta ja varmistamista on suuri riski, että suunnitelmia ei toteuteta ja kyberturvallisuus jää pelkästään paperille.
- Sopimukselliset puutteet: Kankaan alue on monitoimijaympäristö, jonka kokonaisturvallisuus muodostuu eri toimijoiden tekemisistä. Mikäli eri toimijoiden turvallisuusvastuista ei ole sopimuksia, ei ole mahdollisuuksia edellyttää alueella

toimivilta tahoilta toimenpiteitä turvallisuuden edistämiseksi. Erityisesti tämä on otettava huomioon niiden tahojen kohdalla, jotka operoivat kriittistä infrastruktuuria ja hyödyntävät yhteisen infrastruktuurin palveluita ja tietoja.

- Tietoisuuden puutteellisuus: moni kyberturvallisuuden ongelmatilanne on seurausta tahattomasta virheellisestä toiminnasta. Kankaan alueella ihmiset tarvitsevat normaalia enemmän informaatiota älykkään kaupunginosan palveluista sekä niihin liittyvistä oikeanlaisista toimintamalleista. Tietoisuuden puute ja tahaton virheellinen toiminta vaarantavat erityisesti henkilöiden omaa turvallisuutta. Perusinfrastruktuuri on suojattava riittävästi tahattomien virheiden seurauksilta.
- Puutteelliset hallintakäytännöt: älykkään kaupunginosan teknologia, palvelut ja kyberturvallisuusuhat muuttuvat ajan myötä. Kyberturvallisuuteen liittyvät suunnitelmat, ohjeet ja toimintamallit edellyttävät säännöllistä ylläpitoa. Ilman ylläpitoa kyberturvallisuuteen liittyvät ratkaisut vanhenevat ja alue muuttuu kyberturvattomaksi.

3.9 Strategian linkittyminen muihin kehittämisohjelmiin

Tässä luvussa on esitelty muita Jyväskylän kaupungin ja kansallisia kehittämishankkeita, jotka tulisi huomioida Kankaan alueen kyberturvallisuuden kehittämisessä.

3.9.1 Kohti resurssiviisautta

Sitra ja Jyväskylän kaupunki kehittivät Kohti resurssiviisautta -yhteishankkeessa vuosina 2013–2015 toimintamallin, jonka avulla kaupungit ja kunnat voivat edistää luonnonvarojen viisasta käyttöä ja luoda edellytyksiä kestävälle hyvinvoinnille sekä tulevaisuuden menestykselle.

Resurssiviisaus on myös yksi Kankaan alueen teemoista, johon pyritään kestävän kehityksen ratkaisuilla. Yksi konkreettinen keino on siirtyä taloyhtiökohtaisista ratkaisuista alueellisiin ratkaisuihin, kuten keskitettyyn pysäköintiin ja yhteispihoihin.

3.9.2 Uusi sairaala –hanke 2020

Keski-Suomen keskussairaalan alueelle Kukkumäkeen valmistu täysin uusi keskussairaala vuonna 2020. Sairaalan toteutussuunnittelu ja rakentaminen alkavat vuonna 2016.

Uuden sairaalan rakentaminen on keino parantaa terveydenhuollon tehokkuutta, muuttaa rakenteita, prosesseja ja logistisia ratkaisuja sekä integroida perusterveydenhuollon, erikoissairaanhoidon ja osin sosiaalityön palveluita. Tätä kautta on mahdollista synnyttää uusia palvelukonsepteja, joita voidaan pilotoida Kankaan alueen Living Lab-ympäristössä.

Kankaan alueen ja uuden sairaalan toimintakonseptien rinnakkainen käsittely voisi auttaa löytämään aivan uudenlaisia kustannustehokkaita toimintamalleja.

3.9.3 Innovatiiviset kaupungit

Työ- ja elinkeinoministeriön Innovatiiviset kaupungit –ohjelman (INKA) tavoitteena on synnyttää korkeatasoisesta osaamisesta uutta liiketoimintaa ja uusia yrityksiä ja tätä

kautta luoda uusia työpaikkoja. Lähtökohta on tutkimuksen, koulutuksen, yritysten ja julkisen hallinnon tiivis paikallinen yhteistyö ja voimavarojen koonti.

Jyväskylä on valittu INKA-ohjelman kyberturvallisuudesta vastaavaksi kaupungiksi. Tavoitteena on kehittää kyberturvallisuusliiketoimintaa, luoda uusia alan yrityksiä ja saada ulkomaisia yrityksiä etabloitumaan Suomeen sekä muodostaa kansallinen kyberturvallisuuden innovaatiokeskittymä.

3.9.4 Muut älykkäät kaupunki-hankkeet

Kankaan alueen lisäksi Suomessa on jo meneillään useita muitakin älykaupunkihankkeita. Suurin meneillään olevista hankkeista on Helsingin vuonna 2013 aloittama Fiksu Kalasatama –hanke, jonka tavoitteena on tehdä Kalasatamasta älykkään kaupunkirakentamisen mallialue.

Fiksu Kalasatama http://fiksukalasatama.fi

Oulussa on alkanut Hiukkavaaran alueen älykaupunkihanke. Vanhalle kasarmialueelle rakentuu 20.000 asukkaan kaupunginosa, joka on käyttäjälähtöinen, älykkään energiatehokas ja neljän vuodenajan kaupunkielämän keskus. Lisäksi uusi Hiukkavaaran keskus palvelee 40 000 lähiseudulla asuvaa oululaista.

Hiukkavaara http://www.ouka.fi/oulu/hiukkavaara

Edellä mainittujen hankkeiden lisäksi on meneillään useita muita älykkääseen elämiseen ja asumiseen liittyviä hankkeita. Laajempaa tietoa sekä näistä hankkeista että yleisempää tietoa älykaupungeista löytyy Liikenne- ja viestintäministeriön julkaisusta ”*Älykäs kaupunki - Smart City, Katsaus fiksuihin palveluihin ja mahdollisuuksiin*”.

3.9.5 Kansallinen palveluväylä

Kansallinen palveluarkkitehtuuri on ohjelman, jonka tavoitteena on luoda yhteentoimiva digitaalisten palvelujen infrastruktuurin, jonka avulla tiedonsiirto organisaatioiden ja palvelujen välillä on helppoa. Palveluväylä on palveluarkkitehtuurin tiedonvälityskerros, joka määrittää miten tietoja ja palveluja välitetään eri tietojärjestelmien välillä. Väylä on tiedonvälityspalvelu, jonka avulla julkinen hallinto ja yritykset voivat hyödyntää muita väylään liittyneitä palveluita ja tietovarantoja.

Kankaan alueella on mahdollista rakentaa kansalaisten asiointipalveluita, joissa hyödynnetään kansallista palveluväylää. Pilottihankkeissa voidaan hyödyntää palveluväylää molempiin suuntiin eli tuottamalla palveluita ja tietovarantoja, joita voidaan käyttää muissa palveluissa palveluväylän kautta sekä tuottamalla palveluita, jotka käyttävät palveluväylän kautta saavutettavissa olevia tietovarantoja.

3.10 Strategian ja toimeenpanosuunnitelman elinkaari

Tätä strategiaa täydentää toimeenpanosuunnitelma, jossa on määritelty niitä konkreettisia toimenpiteitä, joita vision saavuttaminen edellyttää. Toimeenpanosuunnitelma sisältää suuntaa antavan aikataulutuksen, jossa on huomioitu se, että alueen rakentaminen on jo aloitettu. Näin ollen osa toimenpiteistä on eri järjestyksessä kuin ne olisivat, jos strategia olisi laadittu ennen rakentamisen aloittamista.

Molemmat dokumentit, sekä strategia että toimeenpanosuunnitelma, ovat tämän hetken näkemyksiä tilanteesta. Niitä tulee päivittää ja ylläpitää toimintaympäristön muuttuessa.

Dokumenteissa on pyritty välttämään liian yksityiskohtaisia teknologisia linjauksia, jotta niiden elinkaari olisi mahdollisimman pitkä.

4. Kyberturvallinen Kankaan alue

4.1 Kankaan alueen visio

”Visiona Viisas Kangas - Kankaalla asumisen ja elämisen arki on hyvää, sujuvaa ja turvallista viihtyisässä ympäristössä. Kangas on resurssiviisas ja työpaikkaympäristönä vetovoimainen.”

Kankaan paperitehtaan miljöö Jyväskylän keskustan kupeessa on muuttumassa viihtyisäksi ja resurssiviisaaksi alueeksi, jossa suojeltavien rakennusten osalta vaalitaan vanhaa, mutta toimintatapojen ja ratkaisujen osalta kokeillaan uutta perinteiset mallit kyseenalaistaen kaupungin ohjauksessa.

Alueelle tullaan toteuttamaan koko alueen kattavia ratkaisuja ja monien toimijoiden mahdollistava, integraatiot sisältävä toimintaympäristö. Keskeistä on, että valitut yhteiset palvelut ja toiminnot ovat käytettävissä kaikissa Kankaan kiinteistöissä ja kaikilla käyttäjillä. Kankaan ympäristö luo valmiuksia eikä rajoita innovatiivista palveluiden kehittämistä ja tarjoamista nykytilanteessa tai tulevaisuudessa.

”Kangas vetovoimainen edelläkävijä – ICT-ratkaisut tukemassa tavoitteita”

Keskeisinä ICT:n arkkitehtuuri- ja suunnitteluperiaatteina ovat kestävä kehitys, kokonaisturvallisuus, palveluiden saatavuus ja helppokäyttöisyys sekä yhteisöllisyys.

Älykkääseen kaupunkiin liittyviä palveluita Kankaan alueella tulevat olemaan mm. Kankaan alueelta kerättävä data-aineisto, joka voi toimia pohjana tutkimus- ja kehitystyölle, Kankaan alueen informaatiojärjestelmä, yhteinen tietoliikenneinfrastruktuuri, yhteinen sähköinen kulunvalvonta, kiinteistöihin toteutettava älykkyys, älykkäät pysäköintiratkaisut, turvakameraratkaisut, energiatehokkuutta lisäävät ratkaisut sekä sähköiset huoltopalveluita tehostavat ratkaisut.

Eri toimijat näkevät Kankaan erinomaisena Living Lab -alueena, jossa palveluiden käyttäjä voi osallistua tutkimus-, kehitys- ja innovointiprosessiin omassa arjessaan osana monitoimijaympäristöä. Kangas on potentiaalinen tulevaisuuden palveluiden testialusta.

”Viisas Kankaan alue tulevaisuudessa – pidemmän aikavälin visio”

Tulevaisuudessa teknologiset ratkaisut tulevat helpottamaan huomattavasti päivittäistä elämää. Vielä ei tiedetä tarkasti millä tavalla ja kuinka nopeasti tämä kehitys tapahtuu, mutta jo nyt on nähtävissä monia mahdollisuuksia, jotka ovat jo teknisesti toteuttamiskelpoisia.

Kiinteistöihin, kulkuneuvoihin, laitteisiin ja ohjausjärjestelmiin tulee enenevässä määrin älykkyyttä. Eri laitteiden ja ihmisten välinen sekä laitteiden keskinäinen vuorovaikutus lisääntyy. Teknologian käytettävyys tulee nousemaan aivan uudelle tasolle markkinavetoisesti, sillä käytettävyydeltään huonot ratkaisut eivät tule pärjäämään kilpailussa. Tiedonsiirto, -käsittely ja -tallennus kapasiteetit kasvavat entisestään. Älykäs teknologia arkipäiväistyy ja tulee olemaan olennainen osa päivittäistä elämää. Informaation saatavuus lisääntyy ja teknisesti kaikki informaatio on mahdollista saada kaikkien käyttöön.

Yhteiskunnan, kaupunkien ja kaupunginosien riippuvuus teknologisista ratkaisuista tulee lisääntymään entisestään älykaupunkien teknologioiden yleistyessä. Jo tällä hetkellä riippuvuus on osassa palveluita merkittävä, mutta jatkossa teknologia tulee vaikuttamaan yhä laajemmin.

Kaupunginosien ohjaus tulee muuttumaan. Lisääntyvä teknologia edellyttää ohjaus- ja valvontajärjestelmien samanaikaista kehittymistä. Manuaalisen työn osuus päivittäisessä operoinnissa ja valvonnassa pienenee ja ihmisen vastuulle jäävät enemmän päättelyä vaativat tehtävät, muutosten hallinta ja kokonaisuuden kehittämiseen liittyvät vastuut.

Yhteenvetona viisaasta tulevaisuuden kaupunginosasta voidaan todeta, että elämä tulee olemaan helpompaa, mutta riippuvuus teknologiasta lisääntyy. Siten hallinnan ja operoinnin automaation merkitys kasvaa. Tarkasti emme tiedä miten, mutta suunta on selvä.

Kaikki tämä edellyttää hyvin suurta harppausta turvallisuusasioissa!

4.2 Kankaan turvallisuusympäristön ominaispiirteitä

”Kankaan alue on paljon älykkäitä laitteita sisältävä tietointensiivinen ympäristö, jonka hyökkäyspinta-ala on suuri.”

Viisas-Kangas on toimintaympäristönä hyvin tieto- ja tietoliikenneintensiivinen, jossa eri toimijat hyödyntävät alueen tarjoamia palveluita ja tietoja käyttäen avoimia rajapintoja. Vaikka rajapinnat on ensisijaisesti tarkoitettu alueella olevien tai alueelle palvelua tarjoavien toimijoiden käyttöön, näkyvät ne muillekin – myös ei toivotuille tahoille.

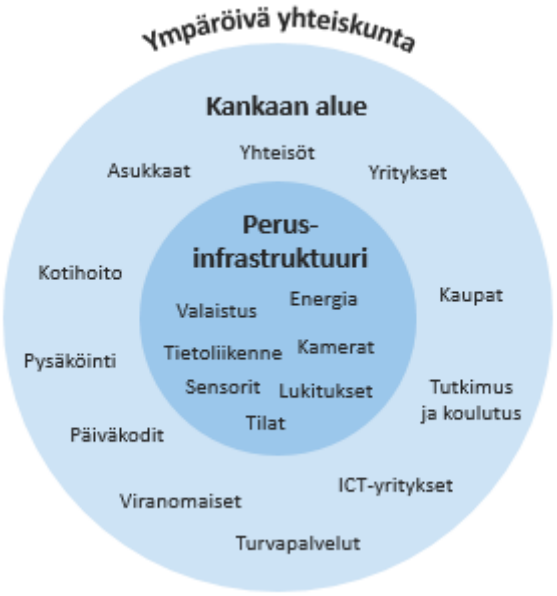
Kankaan alueella on monia erilaisia tietoja, laitteita, järjestelmiä, palveluita ja toimijoita. Tällaisessa toimintaympäristössä pääsynhallinnan, palveluiden ja järjestelmään kytkettyjen laitteiden turvallisuuden merkitys korostuu. Ympäristön heterogeenisuudesta johtuen ei ole mahdollista tehdä kaikille soveltuvia yksityiskohtaisia turvallisuuslinjauksia vaan linjaukset ja ratkaisut tulee suunnitella tapauskohtaisesti.

Hyökkäyspinta-ala on Kankaalla erilaisten laitteiden ja toimijoiden johdosta niin suuri, että turvallisuustoiminnan pääpaino on sietoisuuden kehittämisessä kustannustehokkaasti. Kustannustehokkuus on optimin hakemista suojautumisen kustannusten ja turvallisuusuhkien realisoitumisen kustannusten välillä.

4.3 Turvallisuusympäristön jäsennys

”Kankaan alueen kyberturvallisuuden ydin on alueen kriittisen infrastruktuurin sekä siihen liitettyjen laitteiden ja järjestelmien turvallisuus”

Turvallisuusympäristö voidaan jäsentää kriittiseen perusinfrastruktuuriin ja ”muuhun” Kankaan alueeseen (Kuva 2). Lisäksi ratkaisujen suunnittelussa tulee ottaa huomioon Kankaan ulkopuoliset alueet ja niillä suoritettava toiminta.



Kuva 2: Turvallisuusympäristön jäsennys

Kriittisellä infrastruktuurilla tarkoitetaan sitä osaa perusinfrastruktuurista, jota valtaosa toimijoista tarvitsee ja jonka toimimattomuus aiheuttaa merkittävää vahinkoa koko kaupunginosalle. Esimerkkeinä kriittisestä infrastruktuurista ovat energiaan, tietoliikenteeseen ja alueen turvallisuuteen liittyvät peruspalvelut.

Muulla Kankaan alueella tarkoitetaan kaikkea sitä Kankaan alueella sijaitsevaa infrastruktuuria ja palvelutoimintaa, joka ei ole kriittistä perusinfrastruktuuria. Suurin osa tulevasta Kankaan alueella suoritettavasta palvelutoiminnasta voidaan katsoa kuuluvaksi tähän luokkaan. Esimerkkeinä tällaisista palveluista ovat energiatehokkuutta parantavat palvelut ja vanhusten hoivapalveluita tarjoavat yritykset. Tunnusomaista tällaisille palveluille on se, että ne hyödyntävät omassa toiminnassaan Kankaan perusinfrastruktuurin tuottamia palveluita, mutta heidän toimintansa ei ole osa perusinfrastruktuuria.

Kankaan alueen perusinfrastruktuuriin ja muihin Kankaan alueen palveluihin liittyvää toimintaa suoritetaan myös Kankaan alueen ulkopuolella. Kankaan alueen ulkopuolella sijaitsevia toimijoita koskevat samat kriteerit kuin alueella sijaitsevia toimijoita niissä tilanteissa kun ne tuottavat palveluita Kankaan alueelle tai hyödyntävät Kankaan alueen infrastruktuuria esimerkiksi keräämällä tietoja.

Kukin toimija voi käyttää ja tuottaa useita eri palveluita Kankaan alueella. Turvallisuuden kannalta on olennaista, että toimijalle asetetaan kriteerit palvelukohtaisesti. Mikäli toimija tuottaa samalla prosessilla useita eri palveluita, tulee prosessin täyttää vaatimustasoltaan korkeimman palvelun kriteerit.

4.4 Kankaan alueen kyberturvallisuuden visio

”Turvallisuusratkaisut ovat tasapainossa teknologisen kehityksen ja vuorovaikutuksen lisääntymisen myötä syntyvien turvallisuusuhkien kanssa.”

Kyberturvallisuuden vision keskeinen elementti on tasapaino turvallisuuden uhkien ja niiden vaikutusten sekä turvallisuuden parantamiseksi tehtävien toimenpiteiden välillä.

Tähän päästään analysoimalla aihepiirikohtaisesti kyberturvallisuuteen kohdistuvat uhkatekijät ja suunnittelemalla toimenpiteet analyysin tulosten perusteella.

Teknologian kehittyminen myös tulevaisuudessa on varmaa. Samaan aikaan vuorovaikutus sekä laitteiden kesken että ihmisten ja laitteiden välillä lisääntyy luoden uuden tyyppisiä uhkia. Pidemmän aikavälin yksityiskohtaista kehitystä ei voida ennustaa etukäteen, minkä vuoksi tarvitaan säännöllistä turvallisuusympäristön kehittymisen seurantaa, tilanteen uudelleenarviointia ja uusia toimenpiteitä. Tätä varten tarvitaan hallintamalli, jonka avulla koordinoidaan eri osapuolten yhteistyötä ja päätöksentekoa.

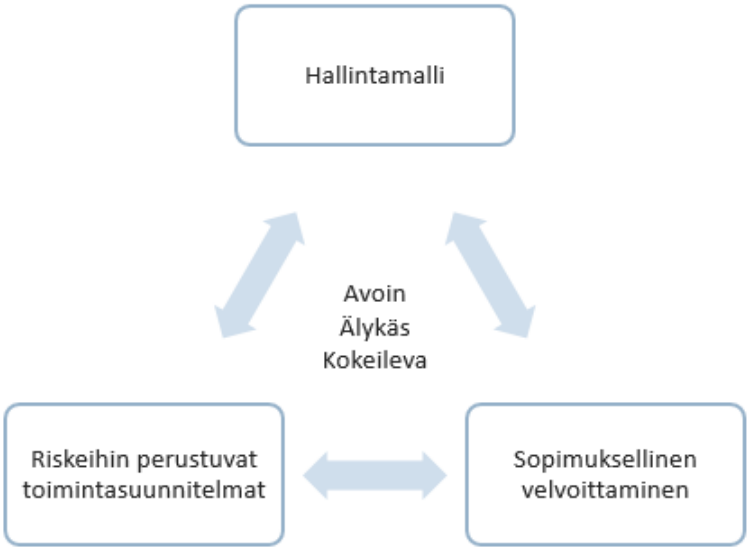
”Kyberturvallisuus – pidemmän aikavälin visio”

Pidemmän aikavälin kyberturvallisuuden kuvaaminen on aina enemmän tai vähemmän sivistynyt arvaus. Seuraavassa luettelossa on tunnistettu joitakin tulevaisuuden kyberturvallisuusympäristön elementtejä ja ominaispiirteitä. Luettelon sisältö perustuu tämän hetken tietämykseen ja voi muuttua nopeastikin kyberympäristön nopean kehityksen vuoksi.

- Verkkoon liitettyjen palveluiden ja laitteiden määrä tulee moninkertaistumaan, joka tulee edellyttämään entistä enemmän työtä turvallisuuden ylläpitämiseksi.
- Salausteknologioiden käyttö helpottuu ja yleistyy, mutta nykyiset salausmenetelmät muuttuvat teknologisen kehityksen myötä haavoittuvammiksi.
- Laitteiden ja palveluiden jako turvallisiin ja turvattomiin syvenee, jolloin turvallisia laitteita ja palveluita hankkivat ne, joilla on siihen varaa.
- Nykyiset teknologiat ja palvelut kehittyvät turvallisemmiksi, mutta markkinoille tulevat uudet teknologiat ja palvelut jakaantuvat edelleen turvallisuudeltaan eritasoisiin ratkaisuihin.
- Syntyy entistä enemmän rinnakkaisia verkkoympäristöjä, joilla on erilaisia turvallisuustasoja. Kriittiset toiminnot eriytetään tiukemmin valvottuihin verkkoihin myös jatkossa.
- Järjestelmien hyödyntäminen on mahdollista monin eri tavoin ja monenlaisilla päätelaitteilla. Päätelaite voi tapauskohtaisesti olla tietokone, mobiilipäätelaite, auto, avaimenperä, aktiivisuusranneke, jääkaappi tai mikä tahansa tulevaisuuden laite.

5. Kyberturvallisuusstrategian kulmakivet ja periaatteet

Kankaan alueen kyberturvallisuusstrategia perustuu kolmeen kulmakiveen, jotka ovat hallintamalli, riskeihin perustuvat toimintasuunnitelmat ja sopimuksellinen velvoittaminen. Näiden kulmakivien tarkoituksena on ohjata toimenpiteitä, joilla visio kyberturvallisesta Kankaan alueesta voidaan saavuttaa.



Kuva 3: Kyberturvallisuusstrategian kulmakivet ja periaatteet

Strategian kulmakivet eivät ole sinänsä yksittäisiä kohteita, vaan ne toimivat yhdessä kokonaisuutena, joilla perusta kyberturvallisen Kankaan alueelle voidaan muodostaa. Kulmakivien mukaisten toimenpiteiden toteuttaminen vaatii resursseja ja vision toteutumisen edellytyksenä on riittävä resursointi strategian toteuttamiseen.

5.1 Kankaan alueen yleisiä periaatteita

Strategian kulmakivien taustalla vaikuttavat Kankaan alueen yleiset periaatteet, jotka periytyvät laajemmin Kankaan alueen toimintasuunnitelmista myös osaksi kyberturvallisuusstrategiaa.

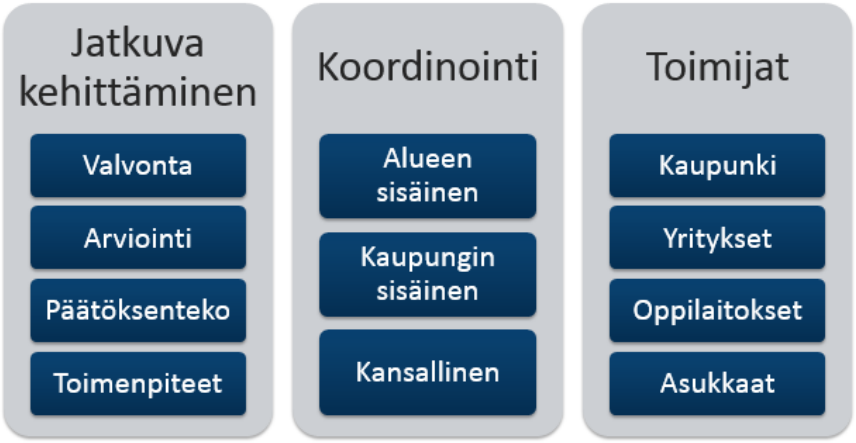
Avoimuus on periaate, jonka kautta kaikki alueen toimijat pääsevät osallistumaan alueen kehittämiseen. Avoimuutta on myös mahdollisuus tuoda uusia palveluita alueelle avoimia rajapintoja käyttäen tai antaa toimijoille läpinäkyvyys sopimusten turvallisuusehtoihin. Kyberturvallisuuden näkökulmasta avoimuus ei tarkoita kaiken tiedon automaattista avoimuutta, vaan tiedon tarpeettoman luottamukselliseksi määrittelyn välttämistä.

Älykkyys ilmenee Kankaan alueella monissa muodoissa. Uudet teknologiset ratkaisut tulevat olemaan älykkäitä ja tarjoamaan alueen asukkaille ja työntekijöille apua arkipäiväisiin ongelmiin. Toisaalta älykkyys ilmenee myös resurssiviisautena, jolloin alueelliset ratkaisut korvaavat perinteisiä taloyhtiökohtaisia toimintoja sekä infrastruktuurin ja ratkaisujen aiempaa pidempinä elinkaarina. Älykkyyteen liittyviä näkökulmia on kuvattu tarkemmin ”Viisas Kangas - Jyväskylän Kankaan ICT-ratkaisujen kokonaissuunnitelma” –dokumentissa.

Kankaan alue on kokeileva. Se ilmenee Living Lab –toimintojen kehittämisen kautta, mutta myös uudentyyppisten hallinto- ja resursointiratkaisujen kokeilemisena. Kankaan alueella toimivien ihmisten on kaavailtu toimivan aktiivisena uusien palveluiden ja tuotteiden pilotointiyhteisönä. Kangas haastaa perinteisiä malleja myös kyberturvallisuuden kehittämisessä.

5.2 Hallintamalli

Kyberturvallisuutta ei voida tuottaa pelkästään etukäteen, vaan kyberturvallisuus rakentuu ja kehittyy koko toiminnan ajan. Strategian ja toimeenpanosuunnitelman ylläpitäminen, kuten toimenpiteiden toteutumisen arviointikin, on jatkuva prosessi. Kyberturvallisuus ja ICT-toimintaympäristö muuttuvat nopeasti, joten on tärkeää muodostaa hallintamalli, jolla muutoksiin pystytään reagoimaan tarvittaessa nopeastikin.



Kuva 4: Kyberturvallisuuden hallintamallin tavoitteet

Tärkeä osa hallintamallia on turvallisuusasioiden päätöksenteko sekä toiminnan arviointi ja valvonta. Hallintamalli määrittää kuinka Kankaan alueen turvallisuutta johdetaan ja ketkä siihen osallistuvat. Niin kauan kuin hallintamallia ei ole määritelty ja otettu käyttöön, vastuu kyberturvallisuuden toteutumisesta on hajaantunut useille toimijoille, jolloin turvallisuusratkaisuista tulee hajanaisia. Vastuu hallintamallin määrittelystä ja käyttöönotosta on Jyväskylän kaupungilla.

Hallintamallia tarvitaan myös turvallisuustoiminnan koordinointiin. Kankaan alueen sisäistä koordinointia tarvitaan resurssiviisaan kyberturvallisuuden toteuttamiseen. Hallintamallissa kannattaa huomioida alueella toimivien yritysten ja yhteisöjen yhteistyömahdollisuudet kyberturvallisuuden kehittämisessä. Kankaan alueen kehittäminen tuottaa myös sellaisia tuloksia, jotka tulevat olemaan käytettävissä Jyväskylän alueella laajemmin. Näiden osalta tarvitaan myös paikallista laajempaa koordinointia. Kansallisella tasolla on meneillään myös muita älykaupunki-hankkeita sekä muita kyberturvallisuuteen liittyviä hankkeita, joten myös kansallisen tason koordinointia voi olla tarpeen harkita.

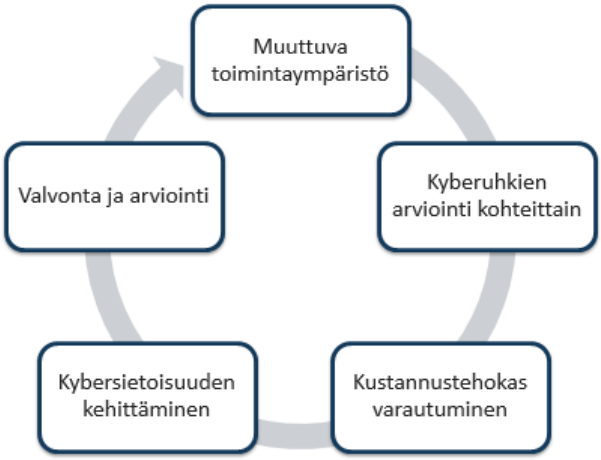
Hallintamallin tehokkuus perustuu siihen, että kaikki alueen toimijat saadaan sitoutettua kyberturvallisuuden kehittämiseen vähintään omalta osaltaan ja riittävään resursointiin osana alueen jatkuvaa kehittämistä.

Hallintamallin ei tarvitse olla keskittynyt pelkästään Kankaan alueen kyberturvallisuuteen, vaan se voi olla osa laajempaa kokonaisuutta, esimerkiksi koko

Jyväskylän kaupungin alueen ICT-palveluiden hallintaa. Tämä voi hankaloittaa alueen kaikkien toimijoiden sitouttamista, mutta helpottaisi toiminnan tulosten laajempaa käyttöä. Kankaan alue itsessään on kuitenkin suhteellisen pieni riittääkseen yksin ylläpitämään tehokasta hallintamallia.

5.3 Riskeihin perustuvat toimintasuunnitelmat

Kyberturvallisuus ja ICT-toimiala yleisesti kehittyvät nopeaa tahtia. Lisäksi älykkäät kaupungit muuttuvat entistä älykkäämmiksi. Kankaan alueen kyberuhat tulevat olemaan laajemmat aiemmin rakennettuihin kaupunginosiin verrattuna, koska uusi teknologia laajentaa hyökkäyspinta-alaa. Kyberuhat eivät rajoitu ainoastaan hyökkäyksiin, vaan älykäs kaupunki ja sen ICT-ratkaisut ovat entistä enemmän riippuvaisia sähköstä ja tietoliikenneyhteyksistä.



Kuva 5 Kyberturvallisuusriskeihin varautuminen

Turvallisuusasiantuntijat ovat olleet jo pitkään yhtä mieltä yhdestä asiasta; kaikkia uhkia vastaan ei voi suojautua. Toimintaympäristön jatkuva muuttuminen ja teknologian kehittyminen muodostavat uusi uhkia. Näin ollen ollaan tilanteessa, jossa joudutaan jatkuvasti arvioimaan järjestelmiin ja palveluihin kohdistuvia uhkia ja niiden vaikutuksia.

Uhka yhdessä toteutumistodennäköisyytensä kanssa muodostaa riskin, jota voidaan pienentää erilaisin vastatoimenpitein. Vastatoimenpiteiden tehokkuus ja kustannukset vaihtelevat, joten vastatoimenpiteet joudutaan suhteuttamaan käytettävissä oleviin resursseihin ja hyväksyttävissä olevaan jäännösriskiin. Jossain tilanteissa voidaan joutua toteamaan, että vastatoimenpiteet uhkien torjumiseksi ovat yksinkertaisesti liian kalliita suhteessa saavutettavaan hyötyyn, joten riskit hyväksytään sellaisenaan.

Kyberturvallisuuden tavoitteiden saavuttaminen vaatii käytännössä jatkuvaa riskienhallintaprosessia. Älykkäässä kaupungissa järjestelmät, niiden tarjoamat palvelut sekä niissä oleva tieto eivät ole keskenään samanarvoisia. Siinä missä on hyväksyttävissä, että katuvalaistuksessa saattaa esiintyä lyhyitä katkoja, samaa ei voida hyväksyä sähköisen lukituksen toiminnassa. Kankaan alueen kyberturvallisuuden kehittämisen kannalta on tärkeää, että resurssit kohdistuvat niiden uhkien torjuntaan, joilla on suurimmat vaikutukset suhteessa toteutumisen todennäköisyyteen. Koska sekä vaikutus että toteutumisen todennäköisyys voivat muuttua, joudutaan kaikkien kohteiden riskejä uudelleenarvioimaan säännöllisesti.

Riskienhallinta tulee sitoa osaksi hallintamallia, joka määrittelee prosessin toiminnasta vastaavat toimijat sekä raportointivelvollisuudet. Kukaan yksittäinen toimija ei voi olla vastuussa kokonaisuudessaan koko Kankaan alueen riskienhallinnasta, mutta hallintamallissa tulee ottaa kantaa eri toimijoiden väliseen kommunikointiin sekä riskienhallinnan koordinointiin. Keskeisessä roolissa ovat kriittisen infrastruktuurin toiminnasta vastaavat toimijat, mutta kokonaisturvallisuuden koordinoinnista vastaa kuitenkin Jyväskylän kaupunki.

Toimintasuunnitelmat, ja niiden osana myös riskianalyysit, tulisi tehdä jokaisen osa-alueen suunnittelun alkaessa. Näin tuloksia voidaan käyttää hyväksi tehokkaasti koko elinkaaren ajan ja ne tulevat huomioiduksi myös osana hankintoja ja sopimuksia.

Niiltä osin kuin riskienhallinnan prosessin tuloksena jäljelle jää jäännösriskejä, tulisi varmistua, että merkittävimpien riskien realisoitumisen varalta on olemassa toipumis- ja jatkuvuussuunnitelmat. Näiden suunnitelmien mukaista toimintaa tulisi harjoitella osana kansallisia kyberturvallisuusharjoituksia.

5.4 Sopimuksellinen velvoittaminen

Palveluiden ja tuotteiden kyberturvallisuus ei ole itsestäänselvyys nyky-yhteiskunnassa, vaikka julkisuuden kautta on kuitenkin ymmärrys kyberuhkien kehittymisestä entistä laajempaa. Tämä on tunnistettu esimerkiksi EU:n NIS-direktiivin luonnoksessa, joka esittää velvollisuuksia turvallisen digitaalisen ympäristön tuottamiseen.

Kuva 6 Sopimuksellisen velvoittamisen elementtejä

Turvallisuutta ei välttämättä saa, jos ei sitä vaadi. Pitkän aikavälin kannalta on luonnollisesti yritysten etu tarjota kyberturvallisia palveluita ja tuotteita asiakastyytyväisyyden ylläpitämiseksi, mutta kyberturvallisuuden kehittäminen tuotteisiin ja palveluihin vaatii resursseja. Sen vuoksi markkinoilta voi löytyä paljonkin tuotteita ja palveluita, joiden kyberturvallisuus ei ole asiakkaiden olettamalla tasolla.

Ensimmäinen askel kohti turvallisempia hankintoja on sopimuksellinen vaatiminen. Huoltovarmuuskeskuksen SOPIVA-suositukset ja -mallilausekkeet tarjoavat toimintaohjeita ja esimerkkejä turvallisempien palveluiden hankintaan. Lisäksi hankintojen kilpailutuksissa on mahdollista pisteytyksillä suosia järjestelmiä ja palveluita, joilla on turvallisuussertifikaatti tai todistus kolmannen osapuolen toteuttamasta turvallisuustestauksesta.

Sopimuksellinen vaatiminen tulee ottaa huomioon palvelutuotannon ketjuissa. ICT-alalla tyypillisiä ketjuja ovat verkkopalveluiden tuotantomallit, joissa palvelun myyjä hankkii ohjelmiston, tai joukon ohjelmistoja järjestelmäratkaisuun, sekä fyysisen

palvelinympäristön tai pilvipalvelualustan eri toimittajilta. Palvelutuotannon ketjuuntuessa kaikki palvelutuotantoon osallistuvat organisaatiot tulee velvoittaa samoihin vaatimuksiin.

Pelkkä sopimuksellinen vaatiminen ei kuitenkaan riitä, vaan on syytä varmistua, että toimittajien palvelut ja ratkaisut vastaavat vaatimuksia. Tämä voidaan toteuttaa auditointi- ja testausmenettelyillä, jotka on syytä suhteuttaa hankinnan kohteen kriittisyyteen. Kriittisissä hankinnoissa kyberturvallisuuden toteutumiseen on syytä panostaa hankinnan alkuvaiheesta alkaen, jolloin varmistetaan, että käyttöönotettavat järjestelmät ja palvelut vastaavat turvallisuudeltaan alueen normeja.

Sopimusten turvallisuusvaatimusten määrittelyssä voidaan soveltaa Kankaan alueen avoimuusperiaatetta laajemmin ja samalla kokeilla uudentyyppisiä toimintamalleja. Turvallisuusvaatimusmäärittelyt voitaisiin julkaista arviointia ja kommentointia varten ja näin saada parannettua sisällön laatua joukkoistamisen kautta. Tehtyjen sopimusten turvallisuusvaatimusten toteutumista on mahdollista valvoa julkaisemalla sopimusten turvallisuusehdot. Näin yksittäiset Kankaan alueen asukkaat, yritykset ja yhteisöt voivat osallistua sopimusten turvallisuusvaatimusten laadun parantamiseen resurssiviisaasti. On mahdollista, että vaikuttamismahdollisuuden kautta myös sitoutuminen turvallisuuden kehittämiseen kasvaa.

6. Strategiset kannanotot

6.1 Infrastruktuuri

Modernin kaupunkiympäristön infrastruktuurin ydin muodostuu sähkö- ja tietoliikenneyhteyksistä, rakennuksista sekä niihin liittyvistä perustoiminnoista kuten valaistus, lukitukset ja kiinteistöautomaatioon liittyvät palvelut.

Infrastruktuurin palvelut tuotetaan näihin tehtäviin valittujen palvelutuottajien toimesta. Palvelutyypistä riippuen palvelun tuottajia voi olla yksi tai useampia. Infrastruktuurin palveluiden tuottajat pystyvät hallinnoimaan Kankaan alueen infrastruktuuria ja hyödyntämään alueelta kerättyä dataa vastuualueensa puitteissa.

Infrastruktuurin palveluiden tuottamiseen kohdistuvat korkeat tietoturvavaatimukset, joita ovat mm.

- Hallinnassa käytettävien järjestelmien todennettu tietoturvallisuus
- Eriytetyt hallintaympäristöt kriittisten palveluiden hallinnassa
- Vahva käyttäjien tunnistaminen kriittisissä palveluissa
- Tietoturvalliset toimintamallit palveluiden tuottamisessa
- Todennetut varajärjestelyt poikkeustilanteiden hoitamiseksi
- Kyky ja valmius yhteistyöhön tilanteissa, jossa tarvitaan eri osapuolten yhteistyötä

Yksityiskohtaiset turvallisuusvaatimukset määräytyvät peruspalveluiden osalta tapauskohtaisesti. Vaatimuksia määriteltäessä on otettava huomioon uhan todennäköisyys, vaikutusten suuruus, suojautumisen kustannukset sekä turvallisten ratkaisujen saatavuus markkinoilta.

Infrastruktuurin palveluiden tuottamisen tulee perustua sopimuksiin, joissa on määritelty palvelun tuottajan turvallisuuteen liittyvät oikeudet ja vastuut. Palveluiden ja niiden tietoturvaratkaisujen sopimuspohjaisuus on erittäin tärkeä seikka monitoimijaympäristöissä, joissa eri osapuolten tulee saada luotettavaa tietoa toimintaympäristön eri osien tietoturvasta sekä eri tahojen vastuista niiden tuottamisessa.

6.1.1 Valokuitupohjainen alueverkko

”Alueverkko suojataan monitasoisesti.”

Alueen yleiseksi ja yhteiseksi tietoliikenneinfrastruktuuriksi Kankaalle rakennetaan valokuitupohjainen alueverkko eli niin sanottu musta verkko, joka toteutetaan rakentamalla ja hallinnoimalla fyysisten siirtoyhteyksien (kuituyhteydet, putket) infrastruktuuria.

Verkkoa vuokrataan kaikille palveluoperaattoreille ja alueen toimijoille, jotka osaltaan huolehtivat tietoliikenteen turvallisuudesta hallinnoimassaan fyysisessä infrastruktuurissa.

Tietoliikenneintensiivisen älykaupungin toimivuuden varmistaminen asettaa alueverkolle korkeat saatavuusvaatimukset, minkä johdosta.

- verkon liityntäpisteet on suojattava fyysisesti,

- alueverkon kaikki yhteydet tulee varmistaa fyysisesti erillisin varayhteyksin,
- verkon hallinnoinnista vastaavan tahon on monitoroitava verkon toimintaa poikkeamien havaitsemiseksi ja
- poikkeamatilanteissa on oltava valmius nopeisiin korjaaviin toimenpiteisiin tietoliikenteen palauttamiseksi jälleen toimintakuntoon.

Kriittiset liityntäpisteet, joilla on laaja vaikutus alueverkon toiminnan kannalta, tulee suojata vahvemmin. Tällaisia kriittisiä liityntäpisteitä ovat esimerkiksi alueverkon pääsolmupisteet. Kriittisissä liityntäpisteissä on

- lähtökohtaisesti kameravalvonta,
- erilliset verkkokohtaiset kytkentäkaapit
- ja mahdollisesti korotettu paloturvallisuuden huomiointi.

Koska verkko on alueellisesti melko pieni, verkon operointivastuu on suositeltavaa antaa kaupallisen verkko-operaattorin vastuulle, jolloin verkon jatkuva valvonta ja kunnossapito on mahdollista toteuttaa kustannustehokkaasti. Verkko-operaattorin velvollisuuksia kyberturvallisuuden toteuttamiseksi määrittää Tietokuntayhteiskuntakaaren luku 29, ” Viestintäverkkojen ja viestintäpalvelujen laatuvaatimukset”.

6.1.2 Alueen kriittisten palveluiden verkottaminen

”Kriittisiä toimintoja varten voidaan rakentaa rinnakkaisia fyysisiä verkkoja.”

Kriittisten kiinteistö-, turvatekniikan-, kunnallistekniikan ja muiden palveluiden tietoverkkoarkkitehtuurin tulee perustua erikseen suojattuihin turvallisiin alueisiin. Kankaan alueella tämä voidaan toteuttaa varaamalla valokuitupohjaisesta alueverkosta omia kuituja tähän käyttöön tai rakentamalla kokonaan rinnakkaisia fyysisiä valokuituverkkoja.

Rinnakkaisen verkon rakentamiskustannukset voivat olla merkittävästi edullisemmat kuin kriittisten toimintojen erottaminen omaan loogiseen, suojattuun verkkoon yhdessä fyysisessä verkossa. Kaikki rinnakkaiset verkot eivät kuitenkaan ole koko Kankaan alueen laajuisia, mutta hallintamallin kautta on huolehdittava, että verkkojen rakenteet on dokumentoitu ja toiminnan jatkuvuuden varmistamisen kannalta olennaisten osapuolten tiedossa.

Kankaan alueen kriittisten kiinteistö-, turvatekniikan-, kunnallistekniikan ja muiden palveluiden tietoverkkoarkkitehtuurin tulee perustua erikseen suojattuihin turvallisiin verkkoihin. Tämä voidaan toteuttaa varaamalla valokuitupohjaisesta alueverkosta omia kuituja tähän käyttöön.

Kriittisen verkkoinfrastruktuurin rakentamisessa tulisi noudattaa seuraavia linjauksia:

- Uusien verkkoyhteyksien on oltava mahdollista ilman aiemmin rakennetun infrastruktuurin purkamista ja uudelleenrakentamista.
- Rakennusvaiheessa tulisi varata ylimääräisiä erillisiä kuituja turvallisia erillisverkkoja varten käytettäväksi myöhemmin.

Edellä luetellut vaatimukset ovat tyypillisiä kriittisen infrastruktuurin palveluille esitettyjä turvallisuusvaatimuksia. Yksityiskohtaiset vaatimukset tulee suunnitella tapauskohtaisesti perustuen kohteen riskianalyysiin ja kohdealueeseen liittyviin

turvallisuusstandardeihin kuten esimerkiksi IEC 62443 (Industrial network and system security).

Kriittisten yhteispalveluiden tietoliikenteen tulisi täyttää seuraavia vaatimuksia.

- Yhteyksiin käytetään vahvoja suojausmenetelmiä sekä tietoliikenteen salausta.
- Kriittiset järjestelmät varmennetaan kahdentamalla.
- Fyysisenä suojauksena järjestelmien laitteet on sijoitettu lukittuihin kaappeihin ja laitetiloihin, joihin pääsyä valvotaan.
- Verkon liikennettä monitoroidaan säännöllisesti kapasiteetin riittävyyden varmistamiseksi ja poikkeamien havaitsemiseksi.
- Turvallisista verkoista rakennetaan suoria liityntöjä julkiseen internet-verkkoon vain erittäin painavista syistä. Jos liityntä rakennetaan, rajoitetaan sen liikenne molempiin suuntiin vain erikseen hyväksyttäviin kohteisiin ja protokolliin.

6.1.3 Kiinteistöautomaatio ja -kaapelointi

”Kiinteistöautomaatiojärjestelmien yhteydet toteutetaan ensisijaisesti erillisen kiinteistökaapeloinnin kautta.”

Jos katsotaan muutamia vuosikymmeniä vanhoja taloja ja toimitiloja, niissä ei ole osattu ottaa huomioon sähköntarpeen ja tietoverkkojen kehitystä. Vaikka langattomat verkot ovat tuoneet ratkaisun useisiin tietoverkkokaapeloinnin ongelmiin, silti kiinteää kaapelointia käyttämällä pystytään saavuttamaan korkeampia siirtonopeuksia sekä luotettavampia ja turvallisempia yhteyksiä kuin langattomilla ratkaisuilla.

Viestintävirasto on raportissaan ”*Suojaamattomia automaatiolaitteita suomalaisissa verkoissa*” tuonut esille, että edelleen suomalaisista tietoverkoista löytyy suojaamattomia kiinteistöautomaatiojärjestelmiä, vaikka asia on tuotu julkisuuteen jo aiemman tutkimuksen yhteydessä.

Yhteydet sekä kiinteistöautomaatiojärjestelmiin että niiden käyttämiin sensoreihin tulisi toteuttaa ensisijaisesti erillisen kiinteistökaapeloinnin kautta. Verkkoon pääsy ja kerättyjen sensoritietojen välitys tulisi rajoittaa vain erikseen sallittuihin kohteisiin. Näin verkon etäkäyttö olisi rajoitettu VPN-yhteyksin tai muun teknologian avulla vain erikseen sallituille laitteille, joka vähentää kiinteistöautomaatiojärjestelmiin kohdistuvaa luvatonta käyttöä. Lisäksi kiinteistöautomaatiojärjestelmissä on huolehdittava asianmukaisesta käyttöoikeuksien hallinnasta, jotta kyberturvallisuus ei vaarannu, vaikka joku saisi muodostettua luvattomasti yhteyden kiinteistöverkkoon.

Kiinteistöautomaatiojärjestelmien sensoriyhteyksien käyttämän erillisen kiinteistökaapeloinnin lisäksi kiinteistöissä tulee olla riittävä muu kaapelointi asukkaiden ja yritysten käyttöön sekä yksityisiä laitteita varten. Näin ollen muu asukkaiden tai yritysten verkkojen käyttö ei vaaranna kiinteistöautomaatiojärjestelmien käytössä olevan verkon saatavuutta.

Laitteiden internet (Internet of Things, IoT) tarkoittaa esineiden verkkoistumista eli yhä useammat laitteet liittyvät osaksi tietoverkkoja tulevaisuudessa. Tämä tulee tarkoittamaan sitä, että Kankaan alueen kiinteistöissä tulee olemaan entistä enemmän laitteita, jotka ovat kytkettynä tietoverkkoihin. Näiltä osin asukas tulee vastaamaan omien laitteidensa turvallisuudesta, kun taas taloyhtiön vastuulla on kiinteistöön liittyvät laitteet. Tästä syystä asukkaan IoT –laitteet käyttävät internet-kaapelointia tai

langattomia verkkoja, kun taas taloyhtiön hallinnoimat sensorit ja laitteet käyttävät erillistä kiinteistökaapelointia.

Kiinteistökaapeloinnin tarpeita on vaikeaa ennustaa Kankaan alueen rakennusvaiheen loppuun asti. Sen sijaan, että yritetään valita vuosikymmenet kestävä kaapelointitekniikka, onkin syytä keskittyä siihen, että miten kaapelointi voidaan vaihtaa myöhemmässä vaiheessa. Tähän toimii ratkaisuna kaapelireittien toteuttaminen jo rakennusvaiheessa, jolloin kaapeloinnit voidaan myöhemmin helposti lisätä.

6.1.4 WLAN-verkot

”Langattomia verkkoja käsitellään kuin julkisia verkkoja.”

Tämän hetkisen näkemyksen mukaan alueen kattavaa julkista WLAN-verkkoa ei olla toteuttamassa ja toisaalta kiinteistökaapeloinnilla vähennetään tarvetta alueelliselle langattomalle verkolle. Kuitenkin alueen suunnittelussa ja kiinteistöjen infrastruktuurin toteutuksessa huomioidaan tontinluovutusehdoissa tehtävät varaumat tarvittaville asennuspaikoille ja laitetiloille mahdollista myöhempää toteutusta varten. Lisäksi myöhemmin suunnitteluvaiheessa voidaan arvioida langattomien verkkojen rajattuja toteutuksia.

Kankaan alueella toimivat yritykset ja muut toimijat voivat rakentaa langattomia lähiverkkoja omiin tarpeisiinsa. Langattomien lähiverkkojen suojaustarpeet vaihtelevat tapauskohtaisesti lähinnä verkossa siirrettävän datan sisällön ja siihen kytkettyjen laitteiden perusteella.

Mikäli myöhemmin tehdään päätöksiä alueellisista langattomista lähiverkoista, arvioidaan niiden turvallisuusvaatimukset erikseen sen hetkisen tilanteen mukaan.

6.1.5 Mobiiliverkot

”Mobiiliverkkoja varten varataan kiinteistöihin suojaustasoltaan vastaavat tilat kuin kiinteää verkkoa varten.”

Operaattorit vastaavat matkapuhelinverkkojen rakentamisesta ja alueen puhelinverkon kuuluvuudesta. Tontinluovutusehdoissa varaudutaan siihen, että kiinteistöissä on varaukset tarvittaville asennuspaikoille, laitetiloille ja yhteysreiteille kattavaa palvelukattavuutta ja operaattoreiden toimintaa varten.

Matkapuhelinverkon teknisiin tarpeisiin varaudutaan tontinluovutusehdoissa ja aluekaapeloinnin, sekä kiinteistökaapeloinnin suunnitelmissa.

Matkapuhelinverkon laitetiloja koskevat samat turvallisuusvaatimukset kuin muitakin kriittisen infrastruktuurin käytössä olevia tiloja, eli niiden on oltava lukittuja ja valvottuja. Turvallisuusvaatimukset tulee tarkentaa suunnittelun yhteydessä.

Mobiiliverkkojen tietoturva on operaattorien vastuulla eikä tässä strategiassa aseteta erillisiä vaatimuksia niiden turvallisuudelle. Mobiileja tietoverkkoja hyödynnettäessä tulee tiedostaa, että niihin liittyy haavoittuvuuksia ja että tietoliikenne mobiiliverkoissa ei ole monissa tapauksissa suojattua päästä päähän.

Mobiiliverkkoja voidaan käyttää kriittisten verkkojen varayhteytenä edellyttäen, että ne käyttävät erillistä fyysistä kiinteän verkon yhteyttä. Näiltä osin mobiiliverkot voivat turvata kriittisiä toimintoja. Tämä mahdollisuus tulee huomioida suunniteltaessa toipumissuunnitelmia kriittisten toimintojen osalta.

Mobiiliverkkojen suunnittelussa tulee toisaalta huomioida kuuluvuus energiatehokkaissa taloissa. Tutkimuksen mukaan radiosignaalit voivat läpäistä uusien talojen rakenteet jopa sata kertaa (20 dB) heikommin verrattuna kymmenen vuotta vanhoihin rakennuksiin. Liikenne- ja viestintäministeriön asettaman työryhmän raportti ”*Matkaviestinverkon kuuluvuusongelmat matalaenergiarakennuksissa*” määrittää toimenpiteitä, joilla voidaan parantaa ehkäistä matkaviestinverkkojen kuuluvuusongelmia energiatehokkaissa rakennuksissa. Raportissa esitetyt toimenpiteet tulisi huomioida tontinluovutusehdoissa, jotta rakennuksissa varaudutaan matkapuhelinverkon käyttöön soveltuvalla kaapeloinnilla mahdollisiin kuuluvuusongelmiin.

6.1.6 Toimitila-arkkitehtuuri

”Osassa toimitiloista tulisi mahdollistaa korkean turvaluokan tilojen toteutus.”

Toimitilat ja niiden tekniset ratkaisut tulevat oletuksena sisältämään turvallisuuden perustarpeiden huomioinnin.

Toimitilojen suunnittelussa mahdollistetaan korkean turvaluokan tilojen toteuttaminen ja tilojen muunneltavuus. Käytännössä tämä tarkoittaa sitä, että vältetään vähintään osassa tiloista ratkaisuja, jotka vaikeuttavat korkeamman turvallisuusluokan tilojen rakentamista tai tekevät rakenteellisista muutoksista huomattavasti kalliimpia. Näin mahdollistetaan turvallisuuskriittisten toimijoiden sijoittuminen Kankaan alueelle.

Esimerkkejä ylimääräisiä kustannuksia aiheuttavista tekijöistä ovat ylimääräiset ovet ja ikkunat, jotka edellyttävät korkean turvaluokan tiloissa erityistä suojaamista. Parvekkeita ja muita ulokkeita tulee välttää mahdollisuuksien mukaan, jos niille ei ole selkeitä tarpeita. Lisäksi rakennusten sisätilat tulisi suunnitella siten, että hätäpoistumistiet eivät kulje muiden yritysten toimitilojen läpi.

Arkkitehdeille ja suunnittelijoille tulee tuottaa ohjeistus turvallisten toimitilojen toteuttamiseksi. Ohjeistuksessa tulee huomioida RT 08-11097 Turvalliset työympäristöt – ohje, Katakrin vaatimukset sekä Viestintäviraston ohjeistukset sekä VAHTI 2/2013 Toimitilojen tietoturvaohje.

6.1.7 Fyysinen pääsynhallinta

”Sähköinen lukitus ja kulunvalvonta mahdollistavat monia innovatiivisia palveluita.”

Fyysinen pääsynhallinta on osa Kankaan alueen turvallisuutta. Sähköinen kulunvalvonta ja lukitusjärjestelmä ovat Kankaan alueen tavoitteita, mutta vielä on epävarmaa toteutetaanko lukitus sähköisesti vai mekaanisesti.

Viisaan Kankaan ICT-ratkaisujen kokonaissuunnitelman mukaan Jyväskylän kaupunki edellyttää alueellisesti yhteensopivaa kulunvalvontaratkaisua kaikkiin kohteisiin. Siten tämän kyberturvallisuusstrategian lähtökohtana on sähköinen kulunvalvonta ja lukitusjärjestelmä, johon sisältyy etähallinta ja alueella liikkuvien käyttäjien kulkutunnisteet eli ”tägit”.

Jyväskylän yliopiston Agora Centerin tekemän selvityksen perusteella mekaanisen lukituksen kertakustannus on noin puolet edullisimmasta käyttökelpoisesta sähkölukitusratkaisusta (20k€/40k€). Huoneistoa kohden sähköisen ratkaisun lisäkustannus on siten suuruusluokkaa 500 €. Sähköinen lukitusratkaisu helpottaa

huomattavasti alueen palveluiden järjestämistä ja tuo niiden yhteydessä selkeitä kustannussäästöjä.

Sähköinen ratkaisu tuo mukanaan monia toiminnallisia hyötyjä, joilla parannetaan alueen turvallisuutta. Näitä ovat mm:

- Pääsyoikeudet voidaan määritellä kullekin käyttäjälle ja mahdollistetaan aikarajoitteiset kulkuoikeudet.
- Elektroniset avaimet voidaan poistaa järjestelmästä, mikä poistaa tarpeen uudelleensarjoitukselle ja alentaa kustannuksia.
- Elektroniset lukot tallentavat ovista kulkevien avainten tiedot ja kulkua tiloihin voidaan seurata, mikä ennalta ehkäisee väärinkäytöksiä. Jälkeenpäin voidaan todentaa millä avaimella on kohteeseen kuljettu.
- Turvalliset elektroniset avaimet ovat mekaanisia avaimia vaikeammin kopioitavissa. Mekaanisesti oikeanlaisella avaimella ei voi kulkea elektronisesti valvotusta ovesta. Kadonneet avaimet eivät aiheuta aukkoa turvallisuuteen, koska kulkuoikeudet voidaan poistaa välittömästi.

Verrattaessa sähköisen ratkaisun turvallisuutta ja toiminallisuutta lisääviä hyötyjä ratkaisun lisäkustannuksiin, voidaan sähköisen ratkaisun käyttöönottoa pitää erittäin perusteltuna ja sitä tulee ehdottomasti vaatia rakennusliikkeiltä tontinluovutusehdoissa.

”**Sähköisen lukituksen ja kulunvalvonnan ratkaisuihin kohdistuvat korkeat tietoturva- ja integroitavuusvaatimukset.”**

Sähköinen lukitusratkaisu ja kulunvalvonta ovat osa Kankaan alueen kriittistä perusinfrastruktuuria, joten sen fyysisen infrastruktuurin hallinta ja turvakäytäntöjen tulee täyttää korkean tason turvallisuusvaatimukset.

Viestintäviraston on laatinut Kiinteistöjen laitetilojen lukituksesta suosituksen 306/2015, jota voidaan hyödyntää kiinteistöjen laitetilojen turvallisuuden suunnittelussa.

Ratkaisun tulisi integroitua Kankaan alueen identiteetin hallintajärjestelmään, jolloin käyttö- ja kulkuoikeuksien hallinta yksinkertaistuu ja elinkaarikustannukset pienenevät.

Sähköisen lukituksen ja kulunvalvonnan toteuttamisessa haasteeksi voivat osoittautua erilaiset tekniset ratkaisut, joita tulee välttämättä alueen pitkän rakentamisajan myötä. Tietojärjestelmien osalta voidaan edellyttää integroitumista identiteetin hallintajärjestelmään, mutta fyysisten komponenttien yhteensopivuutta voi olla vaikeampi edellyttää. Sähköisen lukituksen fyysiset komponentit tulisi valita siten, että eri rakennuksissa käytettävät ratkaisut olisivat mahdollisimman yhteensopivia. Näin alueellisesti yhteisissä palveluissa voidaan välttyä useilta rinnakkaisilta laitteilta pääsynhallinnan toteutuksessa.

Jos alueen kaikki rakennuksiin ei tule sähköistä kulunvalvontaa alkuvaiheessa, olisi kuitenkin edellytettävä tontinluovutusehdoissa, että rakennuksiin tehdään valmius sähköisen lukituksen lisäämiseksi myöhemmin. Viestintäviraston ”*Määräys 65 kiinteistön sisäverkoista ja teleurakoinnista*” edellyttää kattavan huoneistokaapeloinnin tai kaapelireittien toteuttamista, joten tontinluovutusehdoissa olisi mahdollista vaatia vastaavaa kaapelointia tai kaapelireittien toteuttamista myös sähköisen lukituksen tarpeisiin.

6.1.8 Alueportaali

”Alueportaali toimii turvallisuusasioiden tärkeimpänä tiedotuskanavana.”

Kankaan alueportaali on verkkopalvelu, jolla on tärkeä rooli alueellisessa viestinnässä ja palveluiden koostamisessa. Portaalin kautta pystytään viestimään alueellista tapahtumista ja merkittävistä uutisista sekä välittämään muuta tietoa.

Kyberturvallisuuden kannalta alueportaalin tulisi toimia myös turvallisuusviestinnän kanavana. Tietoisuuden lisääminen on todettu useissa tutkimuksissa parhaaksi tavaksi parantaa kyberturvallisuutta. Näin ollen alueportaalilla olisi rooli kyberturvallisuuden kehittäjänä.

Portaalin osana tulee ottaa huomioon myös kriisiviestintä poikkeustilanteissa. Pääsy portaaliin ei voi olla edellytys tiedon saamiselle, vaan viestinnässä on huomioitava monikanavaisuus ja sosiaalisen median hyödyntämisen mahdollisuudet.

”Alueportaali koostaa sähköiset palvelut yhtenäiseksi kokonaisuudeksi.”

Alueportaali voisi toimia myös sähköisiä palveluita koostavana alustana. Palveluiden ei ole välttämätöntä teknisesti toimia samalla alustalla alueportaalin kanssa, mutta niiden tulisi olla yhdistettävissä saumattomasti osaksi portaalia. Portaalin tulisi kuitenkin tarjota tietoa uusien palveluiden kehittäjille esimerkiksi tietoturvaohjeistuksen muodossa. Alueportaalin kautta voidaan nähdä myös arkaluontoista henkilötietoa sekä tehdä palvelusopimuksia, joten alueportaalin teknisen ratkaisun tulee tukea vahvaa käyttäjän tunnistamista.

Tärkeä osa sovellusten turvallisuutta on käytettävyys (tässä yhteydessä ei tarkoiteta saatavuutta), jolla pystytään estämään inhimillisiä virheitä. Alueportaalin kautta tarjottaville palveluille tulisi laatia yhtenäiset käyttöliittymien suunnitteluperiaatteet, jolloin eri palveluntarjoajien tuottamat palvelut kuitenkin näyttäisivät yhtenäisiltä ja toimisivat yhtenäisen logiikan mukaisesti.

Alueportaaliin voivat sisältöä tuottaa useat eri sidosryhmät. Alueportaalin tulee kuitenkin hallinnoida ja valvoa sisällöntuotantoa turvallisuuden näkökulmasta. Lisäksi portaalin kautta voidaan yhdistää tietoa erilaisista lähteistä turvallisuudesta tietoisuuden lisäämiseksi. Samalla portaali tulee toimimaan alustana joukkoistamiseen liittyvien hankkeiden tiedottamisessa ja mahdollisesti myös toteuttamisessa.

6.1.9 Infrastruktuurin huolto ja ylläpito

”Infrastruktuurin ylläpito on hallittua ja säännöllistä.”

Perusinfrastruktuurin kybersietoisuuden ylläpitäminen vaatii jatkuvaa toimintaa. Merkittävä osa työstä itse asiassa tapahtuukin vasta ylläpitovaiheessa, eikä rakennusaikana. Näiltä osin tullaan tilanteeseen, että infrastruktuurin ylläpito on keskeisessä roolissa kybersietoisuuden saavuttamisessa. Tämä koskee erityisesti tietoliikenneinfrastruktuurin ylläpitoa, mutta myös kiinteistöhuoltoa laajemminkin.

Monitoimija ympäristössä ylläpidon tulee tapahtua hallitusti. Kaikkien alueen toimijoiden tekemät huolto- ja ylläpitotoimenpiteet tulee hallinnoida siten, että ylläpitoimet eivät aiheuta ongelmia alueen toiminnan jatkuvuudelle. Tämä koskee lähinnä infrastruktuurin ylläpitoa, mutta myös sähköisiin palveluihin liittyviä järjestelmiä, kuten identiteetin hallintajärjestelmää.

6.2 Turvallisuuden hallinta

6.2.1 Hallintamalli

”Teknologian ja turvallisuusuhkien jatkuva muuttuminen sekä monitoimijaympäristö edellyttävät aktiivista hallintamallia”

Kyberturvallisuus ei ole vain rakennusaikainen ja palveluiden käyttöönottoon liittyvä asia, vaan vaatii jatkuvia resursseja ja ohjausta. Kyberturvallisuuden uhat sekä varautumiseen käytettävissä olevat keinot tulevat muuttumaan voimakkaasti tulevina vuosina, minkä vuoksi kyberturvallisuuteen liittyviä käytäntöjä ja ohjeistoja tulee päivittää säännöllisesti.

Turvallisuusasiat edellyttävät yhteistyötä alueella toimivien tahojen välillä. Kyberturvallisuus on kokonaisuus, jossa turvallisuuden taso määräytyy heikoimman lenkin mukaan. Siksi on erityisen tärkeää että turvallisuusasiat koordinoidaan ja että kaikki osapuolet otetaan huomioon sekä ratkaisuja tehtäessä että niiden toteutumista valvottaessa. Hallintamallin tulee ottaa kantaa siihen kuinka alueen eri toimijat osallistuvat ja sitoutetaan kyberturvallisen alueen kehittämiseen ja ylläpitämiseen.

Hallintamallissa määritellään miten kyberturvallisuuteen liittyvien asioiden valmistelu, päätöksenteko ja toimeenpano suoritetaan. Hallintamallissa tulee ottaa huomioon alueen eri toimijat sekä ulkopuoliset tahot tarpeellisessa laajuudessa.

Kyberturvallisuuden hallintamalli ei eroa periaatteessa mitenkään muiden vastaavien yhteistoimintaa edellyttävien asiakokonaisuuksien hallinnasta. Kankaan alueen kyberturvallisuuden hallintamalli kannattaa integroida osaksi laajempaa hallittavaa kokonaisuutta sekä sisällön suhteen että alueellisesti esimerkiksi osaksi koko Jyväskylän kaupungin ICT asioiden hallintaa.

6.2.2 Sopimustenhallinta

”Sopimuksen ehdoksi turvallinen palvelu”

Kankaan alueen palveluiden tuottajina tulevat pääosin toimimaan alueen ulkopuolelta toimivat yritykset. Näillä yrityksillä ei ole muuta yhteyttä alueen kyberturvallisuuteen kuin palveluidensa ja niitä koskevien sopimusten kautta. Täten palvelun turvallisuuden kannalta, ainoa mahdollisuus edellyttää korkeampaa turvallisuustasoa, on sopimus.

Nykyisin on hyvin harvinaista, että sopimuksissa edellytetään konkreettisia toimia turvallisuuden ylläpitämiseksi. Tyypillisin turvallisuuteen liittyvä sopimuksen osa on saatavuudesta sopiminen eli niin kutsuttu Service Level Agreement (SLA). Toki turvallisuuskriittiset organisaatiot ovat sopimuksen liitteillä vaatineet merkittäviä toimia palvelutuottajiltaan, kuten esimerkiksi Kansallisen turvallisuusauditointikriteeristön (Katakri) mukaista auditointia. Katakri on monen Kankaan alueella tarjottavan palvelun kannalta ylimitoitettu, mutta sopimuksissa olisi kuitenkin mahdollista vaatia kevyempää turvallisuustasoa, jonka avulla voitaisiin varmistua vähintään perustason turvallisuudesta. Toisaalta Kankaan alueella voidaan edellyttää myös Katakrin mukaisia turvallisuusjärjestelyitä, jos palveluiden kriittisyys niin edellyttää.

Yksilön etujen kannalta on tärkeää huomioida sopimuksissa palvelun käyttäjien yksityisyyden suoja. Pilvipalveluiden yhteydessä on noussut esille uusi termi, yksityisyyden suojaustasosopimus eli Privacy Level Agreement (PLA). Sen tavoitteena on sopia palveluiden tarjoamasta yksityisyyden suojasta eli kuinka henkilötiedot on suojattu palvelussa. Kankaan alue voisi toimia pilottialueena, jossa palveluntuottajilta

edellytetään PLA –liitettä palveluyhtiön ja muiden alueen toimijoiden kanssa tehtävissä sopimuksissa.

Turvallisuuden edellyttämisessä sopimusten kautta pystytään tuottamaan materiaalia, joka hyödyttää Jyväskylän kaupunkia laajemminkin. Sopimuksen turvallisuus velvoitteet voidaan jakaa kolmeen kategoriaan:

- *Yleiset turvallisuusvelvoitteet* ovat kaikille järjestelmille ja palveluille yleisiä, kuten käyttäjäntunnistaminen ja tietoliikenneyhteyksien salaus.
- *Toimialakohtaiset turvallisuusvelvoitteet* liittyvät kyseisen toimialan erityispiirteisiin ja voivat olla johdettuja esimerkiksi laista tai standardeista.
- *Kohdetta koskevat turvallisuusvelvoitteet* ovat vaatimuksia kyseiselle hankinnan kohteelle Kankaan alueella. Nämä vaatimukset tulevat pääosin riskianalyysin perusteella.

Näistä kaksi ensimmäistä ovat yleisiä, joita voidaan hyödyntää myös kaupungin muissa kohteissa tehtävissä hankinnoissa. Ainoastaan viimeinen kohta, kohdetta koskevat turvallisuusvelvoitteet, on kyseiseen kohteeseen sidottu ja perustuu aina hankinnan kohteelle tehtävän riskiarvioinnin tuloksiin.

”Sopimusten turvallisuusvaatimukset eivät ole luottamuksellisia”

Perinteisesti sopimuksia pidetään luottamuksellisina. Ongelmana turvallisuusasioiden näkökulmasta luottamuksellisissa sopimuksissa on se, että ulkopuolinen taho ei voi arvioida tuotteen tai palvelun sopimuksen mukaisuutta. Joukkoistaminen ja laajemman yhteisön hyödyntäminen kuitenkin mahdollistaisi sopimusten kehittämisen resurssiviisaasti Kankaan alueen ideologian mukaisesti.

Jos sopimusten turvallisuusvaatimuksia kerättäisiin ja julkaistaisiin, niin alueen asukkaat ja yritykset voisivat osallistua myös niiden kehittämiseen. Julkaisemisen ei tarvitse tapahtua täysin vapaasti, vaan vaatimukset voidaan julkaista vaikka rajoitetummin alueportaalissa kirjautuneille käyttäjille.

Kehittäminen joukkoistamalla voi tapahtua kahteen suuntaan. Alueen toimijat voivat osallistua sopimusten turvallisuusvaatimusten määrittelyyn, jolloin voidaan vaikuttaa tuleviin sopimuksiin. Lisäksi on mahdollista, että tehtyjen sopimusten turvallisuusehdot ja –vaatimukset julkaistaan arviointia varten. Tämä vaatii kuitenkin tarkempaa kontrollia, koska tietojen julkaiseminen ei saa vaarantaa turvallisuutta. Toisaalta tässä yhteydessä olisi mahdollista hyödyntää oppilaitosyhteistyötä palveluiden turvallisuuden testaamisessa ja sopimusehtojen täyttymisessä ilman, että sopimusten turvallisuusvaatimukset julkaistaan laajasti.

6.2.3 Yksityisyyden suoja

”Yksityisyyden suoja on tiedon keruun perusta”

Sähköiset palvelut toteutetaan yksityisyyden suojaa kunnioittaen. Lähtökohtina palveluiden tuottamisessa ja niihin liittyvässä tietojen keruussa ovat läpinäkyvyys ja asukkaan oma päätösvalta tietojen hyödyntämisen laajuudesta. Tietoja tulisi käyttää vain siihen käyttöön, jota varten ne on kerätty ja kaikkeen muuhun tietojen hyödyntämiseen edellytetään asukkaan antama erillinen suostumus.

Suostumuksissa pyritään antamaan selkokielinen kuvaus kerättävistä tiedoista, miten niitä käytetään ja mitä haittaa tietojen luovuttamisesta voi olla. Suostumusta

annettaessa tulee erottaa suostumus varsinaiseen tietojen käyttötarkoitukseen ja muihin käyttötarkoituksiin.

Sensoreiden keräämä tieto on ensisijaisesti anonyymia. Osa palveluista voi kuitenkin edellyttää käyttäjätunnuksen luomista, eikä siten ole käytettävissä ilman asianmukaista henkilötietoa. On kuitenkin huomattava henkilötietolain mukaista henkilötietoa ovat kaikenlaiset luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat merkinnät, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Henkilön yksilöimisen mahdollistavien tietoaineistojen sekä henkilötietojen käsittelyssä ja säilyttämisessä tulee noudattaa henkilötietolain (523/1999) vaatimuksia. On huomioitava, että kaikki henkilötietojen käsittely edellyttää henkilötietolain mukaista käsittelyperustetta tai henkilönsuostumusta. Hallintamallin tulee ottaa myös kantaa siihen, kuka kontrolloi alueellisesti tietojen keräämistä ja on täten myös vastuussa henkilötietolain vaatimusten toteutumisesta. Hallintamallin kautta on myös määriteltävä toimintamallit erilaisiin käyttötapauksiin, kuten esimerkiksi miten toimitaan, kun henkilö peruuttaa suostumuksensa tietojen keräämiseen.

Julkaistaessa tietoja edelleen jatkohyödyntämistä varten tulee varmistaa että aineistosta on poistettu kaikki henkilötiedot ja että henkilö ei ole yksilöitävissä mistään tiedoista tai niiden yhdistelmistä.

6.2.4 Tunnistaminen ja pääsyoikeuksien hallinta

”Kankaan alueella tarvitaan keskitetty tunnistus- ja pääsynhallintapalvelu”

Lähtökohtana tunnistamisessa tulee olla henkilön yksilöllinen tunnistaminen. Riippuen käytettävästä palvelusta ja siinä käsiteltävästä tiedosta, voidaan edellyttää vahvaa tunnistamista. Vahva tunnistaminen on välttämättömyys osassa palveluita sekä infrastruktuurin haavoittuvuuden että alueella hallittavien tietojen sisällön arkaluontoisuuden vuoksi.

Vahvaa tunnistamista on edellytettävä vähintään kaikissa niissä palveluissa, joiden avulla hallitaan alueen kriittistä infrastruktuuria tai jotka mahdollistavat pääsyn henkilöistä kerättyyn yksityiskohtaiseen tietoon.

Alueportaalissa sekä muissa järjestelmissä käytetään ainoastaan henkilökohtaisia tunnuksia. Pääsyoikeudet järjestelmiin on suositeltavaa määritellä roolipohjaisesti kohteittain. Roolipohjainen pääsynhallinta helpottaa erityisesti järjestelmien hallinnointia, kun henkilöt voivat saada oikeuksia palveluihin ja tietoihin suoraan roolin perusteella, eikä tarvita raskasta pääsyoikeuksien päivitysprosessia aina henkilövaihdosten yhteydessä.

Sähköisen lukituksen tunnistusvälineet voivat liittyä pääsynhallintaratkaisuun. Nämä välineet voivat toimia itsessään pääsyavaimena niihin palveluihin, jotka eivät edellytä vahvaa tunnistamista. Lisäksi sähköisen lukituksen tunnistusvälineitä voidaan käyttää osana vahvaa sähköistä tunnistamista.

Keskitetyn identiteetinhallinnan haasteena tulevat olemaan perinteistä, hierarkkista käyttöympäristöä monimutkaisemmat suhteet identiteettien ja hallittavan tiedon välillä. Esimerkiksi asuntokohtaisesti voidaan määritellä käyttöoikeuksia järjestelmiin, jolloin vuokralaisella ja asunnonomistajalla molemmilla on pääsy asunnon lämpötilatietoon. Samaan aikaan kuitenkin sähköisen lukituksen yksityiskohtaiset kulkutiedot kuuluvat henkilötietolain alaiseksi henkilötiedoksi, joten asunnonomistajalla ei ole oikeutta nähdä

näitä tietoja, mutta vuokralaisella on. Lisäksi vuokralaisen oikeus nähdä kulkutietoja rajoittuu vain siihen ajanjaksoon, kun hän on asunnossa asunut.

Keskitetyn identiteetinhallinnan vaatimukset ja käyttötapaukset tulee määritellä tarkkaan ja etukäteen tulee varmistua tietojenkäsittelyn lainmukaisuudesta eri käyttötapauksissa. Tämän jälkeen voidaan edetä vasta suunnittelemaan identiteetinhallinnan teknistä toteuttamista vaatimusmäärittelyn pohjalta.

6.2.5 Valtuutusten ja suostumusten hallinta

”Tietojen keruun ja jatkohyödyntämisen tulee perustua henkilön antamaan suostumukseen”

Kankaan alueella on tiedonkeruuta, joissa yhtenä edellytyksenä on henkilön antama suostumus tietojen keruulle. Lisäksi on toiminnallisia tarpeita, joissa esimerkiksi henkilö voi valtuuttaa toisen henkilön tai palveluntuottajan pääsyn huoneistoonsa.

Älykäs ja toimiva kokonaisuus edellyttää, että valtuutukset on hallittu asianmukaisesti sekä tiedot valtuutuksista ovat helposti saatavissa ja ymmärrettävissä. Myös edelleenvaltuuttaminen on oltava helposti ymmärrettävissä ja tulkittavissa, jotta vältytään tilanteissa, jossa valtuutettu voi myöntää oikeuksia eteenpäin ilman alkuperäisen valtuuttajan suostumusta tai tarkoitusta. Palvelun avulla on pystyttävä kuvaamaan selkeästi ja yksinkertaisesti kuka valtuuttaa kenet ja mihin.

Valtuutustenhallintapalvelu on osa kyberturvallisen Kankaan alueen peruspalveluita ja sen ratkaisujen sekä hallintakäytäntöjen on täytettävä mm. henkilötietolain asettamat vaatimukset. Ratkaisujen tulisi integroitua Kansallisen palveluarkkitehtuurin (KaPA) Rooli- ja valtuutuspalveluun (Rova). Tällöin Rovan kautta myönnetyt valtuutukset olisivat automaattisesti käytössä myös Kankaan alueella.

Lisäksi hyvän tietojenkäsittelytavan ja kummankin osapuolen oikeusturvan kannalta on tarkoituksenmukaista, että myös rekisteröity saa itselleen kopion kirjallisesti antamastaan suostumuksesta kuten Tietosuojavaltuutetun toimisto on linjannut 27.7.2010 oppaassa ”Henkilötietojen käsittely suostumuksen perusteella”.

6.2.6 Todennetut ratkaisut

”Turvallisuuden testaamista tulee vaatia ja se pitää pystyä osoittamaan”

Merkittävä osa älykkäiden kaupunkien kyberongelmista on johtunut puutteellisesta testaamisesta. Kankaan alueelle tuotavia ratkaisuja tulisi testata turvallisuuden osalta sekä ennen käyttöönottoa että säännöllisesti käyttöönoton jälkeen. Testaamista voidaan vaatia sopimuksellisesti ja sen suorittaminen tulisi pystyä osoittamaan.

Testaamisessa on mahdollista hyödyntää oppilaitosyhteistyötä esimerkiksi JAMK:in kyberturvallisuuden JYVSECTEC -osaamiskeskusta hyväksi käyttäen. Näin pystytään myös kehittämään uudenlaista osaamista älykaupunkiympäristöjen testaamisesta.

6.2.7 Tietoturvapäivitykset

”Tietoturvapäivitysten tekemättä jättäminen on merkittävä uhka”

Eri ohjelmistojen löydetyt haavoittuvuudet ja niiden korjauspäivitykset ovat päivittäistä kyberturvallisuuden perustoimintaa. Löydetty haavoittuvuus lisää huomattavasti kyberturvallisuusriskiä kaikissa järjestelmissä, joita ei ole päivitetty.

Kankaalla kaikkien kriittisten järjestelmien tietoturvapäivitykset tulee hoitaa ajantasaisesti. Erityisesti yksityisiltä palveluntuottajilta tätä tulee edellyttää sopimusteknisesti vastaavasti kuin fyysisestä turvallisuuden hyväksyttävän tason ylläpitämistä.

Vastaavasti kuin muiden ylläpito ja huoltotoimien, myös tietoturvapäivitysten asentamisen tulee olla hallittua ja säännöllistä. Tätä tulee edellyttää sopimuksellisesti järjestelmien ja palveluiden toimittajilta.

6.3 Asuminen ja palvelut

6.3.1 Asukkaisiin ja asumiseen vaikuttavat linjaukset

”Läpinäkyvyys tietojen käyttämiseen ja sopimusehtoihin”

Kankaan alueella on mahdollisuus Smart City mallin mukaisesti kerätä tietoa sekä asukkaisiin että asumiseen liittyvistä lähteistä. Näitä tietoja voidaan käyttää asukkaille ja yrityksille tuotettavissa palveluissa sekä tarjota niitä tutkimuskäyttöön. Yksittäisen asukkaan kannalta huomio kiinnittyy siihen, että miten hän voi hallita hänestä kerättäviä tietoja ja niiden hyödyntämistä.

Alueen asukkaiden yksityisyyden suojan kannalta on tärkeää, että he tietävät mitä tietoja heistä kerätään ja miten tietoja käytetään. Lisäksi on tärkeää huomioida selkokielisyys sopimusehdoissa eli käyttäjän tulee tietää mihin hän sopimusta tehdessään sitoutuu ja mitä haittoja hänelle voi sopimuksen kautta aiheutua.

Alueellisen palveluyhtiön ja Living lab –toimijoiden olisi mahdollista toimia esimerkkiorganisaatioina kuinka palvelusopimuksista ja rekisteriselosteista saadaan muodostettua yksilön yksityisyyden suojaa palvelevia dokumentteja. Tällöin kyseiset dokumentit olisivat selkokielisiä kuvauksia, joiden takaavat yksilölle läpinäkyvyyden palvelutuotantoon ja tutkimustoimintaan, joissa heidän tuottamia tietojaan käytetään hyväksi. Esimerkiksi tutkimuksiin osallistujille olisi syytä selkeästi kommunikoida haitat ja riskit, joita tietojen luovuttamisesta voi aiheutua.

”Asukas vastaa huoneiston hankkimistaan järjestelmistä”

Asukkaille tarjotaan alueellisesti internet-yhteyttä huoneistoihin, joka toteutetaan kiinteistökaapeloinnin ja alueverkon kautta. Asukas on vastuussa huoneistossaan mahdollisesti verkkoon liittämistä laitteistaan ja niiden turvallisuudesta. On mahdollista, että Kankaan alueelle tulee kaupallisten toimijoiden tarjoamia internet-liittymään kuuluvia palveluita, kuten palomuuripalvelu tai haittaohjelmien suodatus.

Lähtökohtaisesti kuitenkin taataan asukkaan lakisääteinen verkkoneutraliteetti eli asukkaan liikennettä tietoverkoissa ei suodateta tai analysoida kuin poikkeustapauksissa tai asiakkaan ja palveluntarjoajan tekemän sopimuksen perusteella. Näin ollen kaupungin tai muiden alueellisten toimijoiden ei ole juurikaan mahdollista pakottaa asukkaita välttymään kyberuhilta esimerkiksi haittaohjelmia suodattamalla.

Vaikka vastuu huoneistoon hankkimistaan laitteista on asukkaalla, on tietoisuutta turvallisista järjestelmistä ja laitteista mahdollisuus parantaa alueportaalin kautta ja siten myös edistää alueen verkkojen kyberturvallisuutta. On kuitenkin nähtävissä, että tulevaisuudessakin käyttäjät jakaantuvat edelleen niihin, jotka ovat valmiita maksamaan turvallisista laitteista ja palveluista sekä niihin, jotka eivät välitä turvallisuusominaisuuksista.

6.3.2 Palveluliiketoiminta

”Palveluiden tuottajien tulee sitoutua alueen ja infrastruktuurin asettamiin turvallisuusvaatimuksiin”

Kankaan alueelle tulee sijoittumaan monia erilaisia yrityksiä, kuten ICT-palveluja kehittäviä yrityksiä, alueelle palveluita tarjoavia yrityksiä sekä alueella toimivia palveluita kehittäviä yrityksiä. Lisäksi alueella on monia muita toimijoita, kuten alueellinen palveluyhtiö, Kankaan kehitysyhtiö, aluekehittämiskumppanit sekä Jyväskylän kaupungin palvelutuotantoa.

Palveluliiketoimintaa harjoittavat yritykset toimivat Kankaan alueella pääasiassa normaalien turvallisuuskäytäntöjen mukaisesti eikä Kankaan alueella ole niihin erityistä vaikutusta. Poikkeuksen tästä muodostavat ne toiminnot, joissa yritys hyödyntää toiminnassaan Kankaan alueen älykästä infrastruktuuria sekä sitä kautta kerättyä tietoa.

Näissä tapauksissa yrityksen tulee sitoutua kyseisen infrastruktuuripalvelun tietoturvakäytäntöihin ja huolehtia omassa toiminnassaan että asetetut turvallisuuskriteerit täyttyvät.

Seuraavassa on joitakin esimerkkejä alueella tapahtuvan palveluliiketoiminnan tietoturvavaatimuksista.

- **Palveluyrityksen työntekijät käyttävät sähköistä kulunvalvontaa**, jonka avulla he pääsevät liikkumaan kiinteistöissä työtehtävien tarpeiden mukaan. Yrityksen on huolehdittava henkilöiden turvallisuusohjeistuksista tunnisteiden käytössä sekä yrityksellä on oltava selkeät prosessit, joiden avulla varmistetaan että tunnisteet ovat vain niiden henkilöiden käytössä, joilla on oikeus ja tarve liikkua kiinteistöissä. Älykkäillä ratkaisuilla voidaan oikeuksia rajata esimerkiksi asiakaskäynnin ajankohtaan.
- **Yrityksen työntekijällä on pääsy** taloyhtiöiden pysäköintitiloja ja vapaita paikkoja koskeviin **tietoihin**. Yritys noudattaa kyseisen tietopalvelun sekä pysäköintipalveluiden käytön yhteydessä sovittuja turvallisuusmenettelyitä.
- **Yritys kerää palvelemiensa asukkaiden henkilökohtaisia tietoja**. Yritys huolehtii, että kerätty data siirretään salattuna ja että dataa sisältävien järjestelmien käyttäjät tunnistetaan vahvasti ja että järjestelmät on testattu turvallisuusuhkia vasten. Yritys huolehtii luottamuksellisia tietoja keräävien järjestelmiensä ajantasaisista tietoturvapäivityksistä. Lisäksi yhtiö huolehtii siitä, että henkilöstö koulutetaan käsittelemään oikein arkaluontoisia tietoja.

6.4 Tutkimus- ja kehittämistoiminta

6.4.1 Living Lab –toiminta ja tutkimus- ja kehitysympäristö

”Living Lab –toiminta edellyttää dataoperaattoria ja henkilön tunnistamisen mahdollistavien tietojen poistamista”

Kankaan alue on potentiaalinen Living Lab -kohde, jossa palveluiden käyttäjä voi osallistua tutkimus-, kehitys- ja innovointiprosessiin.

Living Lab toiminnan yhteydessä kerätään monin eri keinoin dataa, joka voi sisältää arkaluontoista tietoa. Kerättävien tietojen sisältö ja arkaluontoisuus vaihtelevat tapauskohtaisesti, minkä vuoksi myös niiden käsittely ja turvallisuuskriteerit tulee

määritellä aineistokohtaisesti. Lähtökohta kriteereille on periaate: ”Mitä sensitiivisempi data, sitä tiukemmat kriteerit”.

Tietoaineistojen käsittelyn käytännön toimenpiteistä huolehtii erillinen dataoperaattori. Dataoperaattorin vastuulle kuuluu aineiston tallentaminen, aineiston turvallisesta käsittelystä huolehtiminen asetettujen kriteereiden mukaisesti sekä aineistojen edelleen välittäminen niille tahoille, jotka hyödyntävät aineistoja esimerkiksi tutkimustoiminnassa.

Sensorien tuottama data on usein valmiiksi anonyymiä. Siltä osin kun kerättävä tieto ei ole anonyymiä, on se anonymisoitava ennen edelleen luovuttamista tutkimuskäyttöön.

Tietoaineistojen hyödyntäjille asetettavat turvallisuuskriteerit riippuvat luovutettavan datan luonteesta. Koska lähtökohtaisesti tutkimuskäyttöön luovutettava data on anonyymiä, ei sen käsittelyyn tyypillisesti kohdistu erityisiä turvallisuusvaatimuksia.

Edellä kuvatun mukaiset tietoaineistot eivät ole täysin avoimia vaan aineistojen luovutuksista sovitaan tapauskohtaisesti erikseen.

”Kerättävä tieto on hallittava mahdollisuuksien mukaan keskitetysti”

Dataoperaattori voi hallinnoida pääsyä tietoon keskitetysti. Keskitetyllä hallinnalla tarkoitetaan tässä yhteydessä sitä, että tiedot kerätään keskitettyyn tietovarastoon sen sijaan, että se haettaisiin suoraan sensoreilta. Tällöin pääsy sensoreihin voi olla hyvin rajattua. Keskitetyssä hallinnassa on useita merkittäviä turvallisuusetuja verrattuna hajaantuneisiin tietosiiloihin.

Käyttöoikeudet voidaan sitoa identiteetin hallintajärjestelmän kautta alueellisiin oikeuksiin. Näin ollen alueelta pois muuttava asukas menettää automaattisesti oikeudet tietoihin, kun muutokset tehdään identiteetin hallintajärjestelmään.

Keskitetyn ympäristön ylläpito ja valvonta on helpompaa kuin useiden hajanaisten järjestelmien. Tämä lisää merkittävästi tietoturvallisuutta, koska kriittisiä päivityksiä ei tarvitse tehdä välittömästi useisiin kohteisiin.

Kaikkea tietoa ei voida kerätä keskitetysti, koska esimerkiksi sähkönkulutustieto siirtyy erillistä verkkoa pitkin sähköyhtiön omaan tietokantaan. Alueelle rakennettavista kiinteistöautomaatiojärjestelmistä kerättävä tieto tulisi kuitenkin mahdollisimman pitkälle saattaa keskitetyn hallinnan alaisuuteen.

”Uusien palveluiden turvallisesta kokeilemisesta on tehtävä mahdollisimman helppoa”

Tutkimus- ja kehitystoiminnan osana tapahtuvan pilotoinnin tulee tapahtua pääsääntöisesti palvelulähtöisesti eli pilotointiin osallistuva asukas tai yritys saa käyttöönsä palvelun, tuotteen tai hyötyy muuten pilottiin osallistumisesta. Pilottihankkeiden osallistujat sitoutuvat noudattamaan sopimusehtoja, jotka voivat edellyttää palvelun tuottamiseen tarvittavien tietojen luovuttamista. Esimerkiksi sähkönkulutusta optimoivaa palvelua on mahdotonta toteuttaa ilman yksityiskohtaista tietoa huoneiston sähkönkulutuksesta. Toisaalta asukkaan helpompi hyväksyä näiden tietojen luovuttaminen palvelun käytettäväksi, koska hän tietää tietojen käyttötarkoituksen.

Pilotointisopimusten tekeminen tulisi olla mahdollisimman helppoa. Alueportaali yhdistettynä vahvaan käyttäjän tunnistamiseen tarjoaa luonnollisen ratkaisun. Alueportaaliin tulisi rakentaa valmiit mallit, joilla sopimuksia voidaan tehdä ja allekirjoittaa sähköisesti. Alueportaalin ohjeistuksissa tulee huomioida, että osallistujille

kommunikoidaan pilottiin osallistumisen hyödyt, vastuut ja mahdolliset haitat selkeästi Kankaan alueen avoimuusperiaatteen mukaisesti.

”Pilotointi edellyttää tapauskohtaista turvallisuusharkintaa - perusasiat voidaan hoitaa etukäteen”

Alueportaalin kautta tapahtuvalla pilotoinnin hallinnalla tehostetaan ja helpotetaan varsinaisten pilotointien toteuttamista. Yhtenäiset toimintatavat eri pilotointihankkeiden välillä parantavat asukkaiden luottamusta. Yksittäisten pilotointien toteutusta varten tulee luoda valmiit toiminta-, tiedotus- ja sopimusmallit. Palautetietojen keruussa voidaan hyödyntää alueportaalin mahdollisuuksia.

Pilotointien turvallisuusnäkökohdat tulee suunnitella tapauskohtaisesti. Huomioitavia näkökohtia ovat:

- pilotoinnin yhteydessä kerättävä data ja sen sensitiivisyys
- osallistujien määrä
- pilotoinnin kesto
- osallistujilta edellytettävät toimenpiteet
- pilotissa tunnistetut uhat ja niiden realisoitumisen todennäköisyydet
- uhkien realisoitumisen vaikutukset pilotin osanottajiin
- lainsäädännölliset rajoitteet

Pilottihankkeiden toteuttaminen keskitetysti portaalin kautta mahdollistaa myös kolmannen osapuolen etukäteen suorittaman sopimusehtojen valvonnan muun muassa eettisistä näkökohdista. Näin osallistuja voi varmistua siitä, että kolmas osapuoli on varmistanut sopimusehtojen tasapuolisuuden kaikkien osapuolten kannalta.

Living Lab –konseptin haasteena voi olla markkinoilla nopeasti kehittyvät henkilökohtaisen informaation keräämisen ratkaisut, jotka eivät täytä tässä dokumentissa kuvattuja kyberturvallisuuden vaatimuksia. Kuluttajat ovat usein valmiita tinkimään käyttämiensä palveluiden ja tuotteiden turvallisuudesta helppokäyttöisyyden ja edullisuuden vuoksi. Uhkana on se, että nämä nopeasti kehittyvät markkinavetoiset palvelut kehittyvätkin nopeammin kuin Living Labin turvallisemmat, mutta kankeammat palvelut.

6.4.2 Avoin tieto

”Kankaan alueella on myös avointa tietoa”

Avoimesta tiedosta käytetään myös termejä avoin data ja open data.

Avoimen tiedon määritelmän mukaisesti aineiston tulee olla kokonaisuudessaan saatavilla käyttökelpoisessa ja muokattavassa muodossa Internetin kautta ja sen tulee olla lisensoitu niin, että sen käyttöä, muokkausta ja uudelleenjakelua ei rajoiteta.

Pääperiaatteet ovat:

- Aineiston tulee olla kokonaisuudessaan saavutettavissa ja ladattavissa julkisessa tietoverkossa.
- Tiedon on oltava uudelleenjaettavissa ilman käyttöehtorajoituksia. Näin mahdollistetaan aineistojen nopea hyödyntäminen ja tehokas yhdistely.

- Tiedon on oltava uudelleenkäytettävissä. Näin sallitaan aineistojen esteetön ja innovatiivinen käyttö edistyksellisiin ja yllättäviinkin tarkoituksiin.
- Aineiston on oltava vapaa teknisistä rajoitteista niin, ettei yllämainittujen kohtien mukaiselle toiminnalle ole teknisiä esteitä.
- Aineiston on oltava vapaa sosiaalisista ja organisatorisista rajoitteista, niin ettei henkilön työ, sijainti, asuinpaikka, organisaatiomalli (kuten kaupallinen tai ei-kaupallinen organisaatio), uskonto, poliittinen suuntautuneisuus tai etnisyys rajoita pääsyä tietoon.

Kankaan alueella kerättyä tietoa on periaatteessa mahdollista julkaista avoimena datana, mutta vielä ei ole tehty linjauksia siitä, mitä dataa ja missä laajuudessa tullaan julkaisemaan. On hyvin mahdollista, että avoimen datan sijaan tarjotaan puoliavointa dataa, joka edellyttää esimerkiksi rekisteröitymistä ja mahdollisten käyttöehtojen hyväksymistä. Living Lab –toimintojen rahoittamiseksi on myös mahdollista periä korvaus datan luovuttamisesta, mutta tällöin ei voida enää puhua edellä määritellyn mukaisesta avoimesta datasta.

Perinteinen rajoitus tietojen julkaisemisessa on käyttötarkoitussidonnaisuuden vaatimus, mikä edellyttää sitä, että kerättyjä henkilötietoja käytetään vain siihen tarkoitukseen mikä tietosuojaselosteessa on mainittu. Vaatimuksesta on kuitenkin mahdollista poiketa anonymisoimalla henkilötiedot, millä tarkoitetaan sitä että henkilötietoja sisältävästä tietomassasta poistetaan ne tiedot, joiden perusteella henkilö on tunnistettavissa. Anonymisoinnin myötä henkilötietolainsäädäntö ei enää sovellu dataan ja tiedot ovat vapaammin hyödynnettävissä. Anonymiteetin takaaminen on kuitenkin haasteellista.

Riskipohjainen lähestyminen tarjoaa parhaan mahdollisuuden datan hyödyntämiseen ja datan arvon säilyttämiseen. Riskipohjaisessa lähestymistavassa anonymisointimalli ja -tekniikat valitaan tietojen arkaluontoisuuden ja käyttötarkoituksen pohjalta. Myös datan mahdollinen käyttötarkoitus ja hyödyntävät tahot otetaan arvioinnissa huomioon. Onnistuneesti anonymisoitu data on taloudellisesti arvokasta, eikä yksityisyys vaarannu. (Antikainen, 2014)

Lisää aiheesta löytyy mm suosituksesta JHS 189 Avoimen tietoaineiston käyttölupa, henkilötietolaista sekä tietosuojavaltuutetun kannanotoista. Kotimainen ohjeistus avoimista tietoaineistoista ja anonymisoinnista on vielä vähäistä. Laajemmin aihepiiriä on käsitelty mm. Ison Britannian tietosuojavaltuutetun ohjeissa.

Kankaan alueella on tunnistettavissa avointa tietoa, joka voidaan julkaista vapaasti. Tällaisia tietoja ovat esimerkiksi summa tason tiedot erilaisista mittauksista, joista ei voida tunnistaa yksittäisiä asukkaita tai huoneistoja, eikä niihin liittyviä tapahtumia. Merkittävä osa kerättävästä tiedosta tulee kuitenkin olemaan luottamuksellista ja saatavuudeltaan rajoitettua. Tiedon omistaja on aina vastuussa siitä millä ehdoilla tietoa tullaan julkaisemaan ja lopulta myös siitä, että tietojen luovuttamisessa toimitaan lakien ja sopimusehtojen mukaisesti.

7. Yhteenveto

Kankaan alueelle tulee olemaan Suomen ensimmäinen älykaupunginosa, jossa kyberturvallisuus on huomioitu laajasti osana alueen suunnittelua. Älykäs kaupunki perustuu entistä tehokkaampaan ja laajempaan tieto- ja viestintäteknologian käyttöön, joka asettaa uusia haasteita kyberturvallisuuden hallinnalle ja jatkuvalle kehittämiselle. Kyberuhkia tulee jatkuvasti lisää ja samaan aikaan kasvava tietoverkkoihin kytkettyjen laitteiden määrä aiheuttavat, että turvallisuuden ylläpitämiseksi tarvittavien resurssien määrä tulee kasvamaan koko ajan.

Alueen visiona on Viisas Kangas, jossa asumisen ja elämisen arki on hyvää, sujuvaa ja turvallista viihtyisässä ympäristössä. Kyberturvallisuuden näkökulmasta usein vision sujuvuus ja turvallisuus nähdään vastakkain, mutta älykkäillä ratkaisuilla voidaan pyrkiä saavuttamaan molemmat yhtä aikaa.

Strategian kulmakiviksi, joilla visio pyritään ensisijaisesti saavuttamaan, on nostettu hallintamalli, sopimuksellinen velvoittaminen ja riskeihin perustuvat toimintasuunnitelmat. Näiden kulmakivien taustalla vaikuttavat lisäksi kolme Kankaan alueen yleisempää periaatetta; Kangas on avoin, älykäs ja kokeileva.

Kyberavaruus on nopeasti kehittyvä ja muuttuva toimintaympäristö. Sen vuoksi pitkälle tulevaisuuteen ulottuvia linjauksia on mahdotonta tehdä. Sen sijaan on luotava edellytykset kyberturvallisuuden ylläpitämiseksi tulevaisuudessa sekä kyvykkyys pystyä reagoimaan toimintaympäristössä tapahtuviin muutoksiin tarvittaessa nopeasti. Tämä edellyttää alueellisesti uudenlaista hallintamallia, jonka kautta voidaan mahdollistaa kyberturvallisen Kankaan alueen toiminta myös kyberuhkien kehittyessä.

Kankaan alueelle tulee suuri määrä erilaisia toimijoita, jotka hankkivat alueen kyberturvallisuuteen omalta osaltaan alueen kyberturvallisuuteen vaikuttavia palveluita. Alueen kyberturvallisuuden kannalta on ehdotonta, että toimijat osaavat hankkia turvallisia tuotteita ja palveluita. Hankinnoissa voi syntyä myös pitkiä alihankintaketjuja, eivätkä lopulliset palvelun tuottajat ole välttämättä tietoisia Kankaan alueen kyberturvallisuuden tavoitteista. Turvallisuusvaatimuksia tulee vyöryttää alihankintaketjussa eteenpäin sopimuksellisesti vaatimalla.

Kyberturvallisuuden hallinta tulisi rakentaa laajemminkin osaksi Jyväskylän kaupungin toimintamalleja, jolloin kyberturvallisuus tulisi huomioitua osana kaupungin normaaleja toimintoja. Toimintojen kehittäminen ei vaadi niinkään suurta rahoitusta, vaan enemmänkin tahtotilaa kehittää toimintamalleja kyberturvallisuuden huomioivaan suuntaan. Näin Kankaan alue voi toimia pilottiympäristönä koko kaupungin laajuiselle kyberturvallisuuden kehittämiselle.

Yksittäistä kohdetta ei kuitenkaan hallintamallin tai sopimustekstien avulla suojata, vaan suojaaminen edellyttää kohteen turvallisuusriskien arviointia sekä niihin varautumista. Kybersietoisuuden kannalta on tärkeää, että kyberriskejä analysoidaan kattavasti, jolloin kaikki kohteet tulevat suojatuksi niiden kriittisyyden kannalta riittävällä tasolla.

Kyberturvallisuuden toteutuminen ei ole kiinni ainoastaan tahtotilasta, vaan myös resursseista. Järjestelmien määrän kasvaminen kasvattaa myös tarvetta ylläpitotyölle. Jos aiempi trendi kyberhyökkäämisen ja -puolustautumisen välisen kustannuseron kasvusta jatkuu, vaatii kyberturvallisuuden ylläpitäminen jatkossa vielä enemmän resursseja. Alueellisesti kyberturvallisuuden kehittämiseen ja ylläpitämiseen tarvittavat resurssit eivät voi tulla ainoastaan markkinalähtöisesti, vaan tarvitaan myös täydentävää rahoitusta esimerkiksi Living Lab-konseptin toteuttamiseen.

Liite 1: Valokuituinfra ja verkon operointi

Tähän liitteeseen on koottu valokuituinfraan ja verkon operointiin liittyvät kannanotot.

- Alueverkko suojataan monitasoisesti. Alueverkon suunnittelussa huomioidaan kokonaisvaltaisesti kaikki turvallisuuden näkökulmat.
- Alueverkon suunnittelun osana tulee tehdä kattava riskiarviointi.
- Kriittisiä toimintoja varten voidaan rakentaa rinnakkaisia fyysisiä verkkoja. Valokuitu verkkoon voidaan rakennusvaiheessa tehdä varauksia rinnakkaisille verkoille.
- Kankaan alue on tietointensiivinen ympäristö, johon tulee varautua myös verkon kapasiteetin suunnittelussa.
- Alueellisen tietoverkon merkitys osana kriittistä infrastruktuuria tulee kasvamaan sähköisten palveluiden ja teknologisen kehityksen myötä, joten verkon saatavuus tulee korkealla tasolla, eivätkä yksittäisten laitteiden tai kaapeleiden rikkoutumiset saa aiheuttaa koko aluetta koskevia ongelmia.
- Kriittisissä verkon liityntäpisteissä on minimivaatimuksia korkeampi suojaustaso.
- Tärkeä osa verkon operointia on verkon kyberuhkien seuraaminen ja niihin varautuminen.
- Verkko-operaattori on sopimuksellisesti velvoitettu huolehtimaan ja osoittamaan, että verkon kyberuhkiin varautuminen täyttää alueelliset vaatimukset.
- Valokuituverkon poikkeustilanteita harjoitellaan säännöllisesti, esimerkiksi joka toinen vuosi.

Liite 2: Sähköinen kulunvalvonta ja lukitukset

Tähän liitteeseen on koottu sähköiseen kulunvalvontaan ja lukitukseen liittyvät kannanotot.

- Sähköinen lukitus on merkittävä mahdollistaja uudenlaisille, helppokäyttöisille palveluille. Sen vuoksi alueen innovatiivisten ratkaisujen mahdollistamiseksi, sitä tulisi edellyttää käytettäväksi kaikissa rakennuksissa.
- Sähköisen lukituksen ja kulunvalvonnan osalta tulee määritellä alueelliset vaatimukset sekä tietoturvan että integroitavuuden osalta. Tontinluovutusehdoissa tulee edellyttää, että kaikki alueella käytettävät järjestelmien tulee olla näiden vaatimusten mukaisia.
- Sähköiset lukitus ja kulunvalvonta järjestelmät kehittyvät alueen rakentamisen aikana ja eri kohteiden järjestelmät eivät tule olemaan ominaisuuksiltaan yhtenäisiä. Sen vuoksi järjestelmiä valittaessa tulee edellyttää niiden integroitumista keskitettyyn hallintaan, josta alueellinen palveluyhtiö vastaa.
- Sähköisen lukituksen ja kulunvalvonnan varajärjestelyt on suunniteltu siten, että ne soveltuvat kaikkien alueen toimijoiden tarpeisiin.
- Sähköisessä lukituksessa ja kulunvalvonnassa käytetään vahvoja suojausmenetelmiä sekä tietoliikenteen salausta.
- Kriittiset järjestelmät, käytännössä kaikki sähköiseen lukitukseen ja kulunvalvontaan liittyvät järjestelmät varmistetaan kahdentamalla.
- Sähköisiä lukitusjärjestelmiä ja kulunvalvonta ylläpidetään hallitusti ja säännöllisesti.

Liite 3: Kiinteistödatan kerääminen ja kiinteistöjen etähallinta

Tähän liitteeseen on koottu kiinteistödatan keräämiseen ja kiinteistöjen etähallintaan liittyvät kannanotot.

- Niin kauan kun kiinteistödata voidaan yhdistää henkilöön tai perheeseen, se on henkilötietoa, jota koskevat henkilötietolain rajoitukset ja tietojen keräämisen tulee perustua henkilötietolain mukaisiin henkilötietojen käsittelyn yleisiin edellytyksiin.
- Kiinteistöjen etähallinnasta ja kiinteistödatan säilyttämisestä vastaavat yritykset velvoitetaan sopimuksellisesti osoittamaan, että kyberturvallisuus on huomioitu toiminnassa ja teknisissä ratkaisuissa kohteiden kriittisyyden edellyttämällä tavalla.
- Kiinteistödatan välittäminen tapahtuu salattuna tietoverkoissa.
- Tietoliikenneyhteydet kiinteistödataa kerääviin sensoreihin toteutetaan ensisijaisesti kiinteistökaapeloinnin kautta.
- Huoneistokohtaisen kiinteistödatan kerääminen tulee aina tapahtua suostumukseen perustuen ja yksityisyyden suojaa kunnioittaen.
- Kiinteistöjen etähallintajärjestelmiä ylläpidetään säännöllisesti ja hallitusti.

Liite 4: Tontinluovutusehdoissa huomioitavia näkökohtia

Strategiassa esitetään useita toimenpiteitä kyberturvallisuuden kehittämiseen ja varautumiseen, jotka olisi syytä huomioida jo rakennusvaiheessa. Nämä toimenpiteet aiheuttavat kustannuksia rakennusvaiheessa, mutta voivat alentaa rakennuksen käyttöaikaisia kustannuksia, joten ne saattavat olla jopa kokonaistaloudellisesti edullisempia. Rakennusliikkeiden näkökulmasta katsottuna rakennuskustannukset ovat merkittävämpiä kuin elinkaarikustannukset, mutta rakennusliikkeitä voidaan velvoittaa tontinluovutusehtojen kautta toteuttamaan kokonaistaloudellisesti edullisempia ratkaisuja. Seuraavassa on koottu tästä strategiasta löytyviä kyberturvallisuuteen olennaisesti liittyviä näkökohtia, joita tulisi edellyttää tontinluovutusehdoissa.

- Rakennusten sisäverkkojen kaapeloinnissa tulee huomioida seuraavat varaukset joko ylimääräisinä kaapeleina tai kaapelireitteinä:
    - Erillinen kiinteistöverkko kiinteistöautomaatiojärjestelmiä ja niiden käyttämiä sensoreita varten.
    - Sähköisen lukituksen vaatima kaapelointi (vaikka sähköistä lukitusta ei vielä toteutettaisikaan).
    - Langattomien verkkojen tukiasemat (4G, WLAN jne).
- Tilavaraukset matkapuhelinverkkojen tukiasemille.
- Radioverkkojen mahdollisten kuuluvuusongelmien huomiointi (Liikenne- ja viestintäministeriö, ”Matkaviestinverkon kuuluvuusongelmat matalaenergiarakennuksissa – työryhmän raportti”, 1.10.2013).
- Sähköisen lukituksen teknisen ratkaisun tulee olla sellainen, että se on integroitavissa alueelliseen keskitettyyn kulunvalvontajärjestelmään.