VIISAS KANGAS

JYVÄSKYLÄN KANKAAN KYBERTURVALLISUUSSTRATEGIA

Kesä 2015
Sisältö

1. Johdon tiivistelmä .................................................................................................................. 5
2. Termit, lyhenteet ja viittaukset .......................................................................................... 6
   2.1 Termit ja lyhenteet ........................................................................................................... 6
   2.2 Viitatut dokumentit ......................................................................................................... 7
3. Strategian taustoitus ............................................................................................................. 8
   3.1 Mitä on kyberturvallisuus? .............................................................................................. 8
   3.2 Kyberturvallisuusuhat ..................................................................................................... 8
   3.3 EU:n kyberturvallisuusstrategia .................................................................................... 9
   3.4 Suomen kansallinen kyberturvallisuusstrategia ............................................................. 10
   3.5 Jyväskylä kansallisen kyberturvallisuuden toimijana ..................................................... 11
   3.6 Kankaan alue kyberturvallisuuden pilottiämpäristönä .................................................. 12
   3.7 Strategian tuottaminen .................................................................................................. 12
   3.8 Strategian toteutumisen riskit ..................................................................................... 13
   3.9 Strategian linkittyminen muihin kehittämisohjelmiin ..................................................... 14
      3.9.1 Kohti resurssiviisautta ............................................................................................ 14
      3.9.2 Uusi sairaala –hanke 2020 ...................................................................................... 14
      3.9.3 Innovatiiviset kaupungit ......................................................................................... 14
      3.9.4 Muut älykkäät kaupunki-hankkeet ......................................................................... 15
      3.9.5 Kansallinen palveluväylä ....................................................................................... 15
   3.10 Strategian ja toimeenpanosuunnitelman elinkaari ....................................................... 15
4. Kyberturvallinen Kankaan alue ............................................................................................ 17
   4.1 Kankaan alueen visio ..................................................................................................... 17
   4.2 Kankaan turvallisuusyhdistön ominaispiirteitä ............................................................. 18
   4.3 Turvallisuusyhdistön jäsenys ....................................................................................... 18
   4.4 Kankaan alueen kyberturvallisuuden visio .................................................................... 19
5. Kyberturvallisuusstrategian kulmakivet ja periaatteet .......................................................... 21
   5.1 Kankaan alueen yleisiä periaatteita .............................................................................. 21
   5.2 Hallintamalli ................................................................................................................... 22
5.3 Riskeihin perustuvat toimintasuunnitelmat .............................................................. 23
5.4 Sopimuksellinen velvoittaminen ............................................................................. 24
6. Strategiset kannanotot ................................................................................................. 26
6.1 Infrastrukturi ........................................................................................................... 26
  6.1.1 Valokuitupohjainen alueverkko ....................................................................... 26
  6.1.2 Alueen kriittisten palveluiden verkottaminen ............................................... 27
  6.1.3 Kiinteistöautomatio ja -kaapelointi ............................................................... 28
  6.1.4 WLAN-verkot .................................................................................................. 29
  6.1.5 Mobiiliverkot .................................................................................................. 29
  6.1.6 Toimittila-arkkitehtuuri ................................................................................. 30
  6.1.7 Fyysinen pääsynhallinta .................................................................................. 30
  6.1.8 Alueportaali .................................................................................................... 32
  6.1.9 Infrastruktuurin huolto ja ylläpito .................................................................. 32
  6.2 Turvallisuuden hallinta ............................................................................................ 33
    6.2.1 Hallintamalli .................................................................................................. 33
    6.2.2 Sopimustenhallinta ....................................................................................... 33
    6.2.3 Yksityisyyden suojaa .................................................................................... 34
    6.2.4 Tunnistaminen ja pääsyoikeuksien hallinta ............................................... 35
    6.2.5 Valtuutusten ja suostumusten hallinta ....................................................... 36
    6.2.6 Todennetut ratkaisut .................................................................................... 36
    6.2.7 Tietoturvapäivitykset .................................................................................... 36
  6.3 Asuminen ja palvelut ............................................................................................... 37
    6.3.1 Asukkaisiin ja asumiseen vaikuttavat linjaukset ........................................... 37
    6.3.2 Palveluliiketoiminta ..................................................................................... 38
  6.4 Tutkimus- ja kehittämistoiminta ........................................................................... 38
    6.4.1 Living Lab –toiminta ja tutkimus- ja kehitysympäristö .............................. 38
    6.4.2 Avoin tieto .................................................................................................... 40
7. Yhteenveto ................................................................................................................... 42
   Liite 1: Valokuituinfra ja verkon operointi ................................................................. 43
   Liite 2: Sähköinen kulunvalvonta ja lukitukset ......................................................... 44
Liite 3: Kiinteistödatan kerääminen ja kiinteistöjen etähallinta .......................................................... 45

Liite 4: Tontinluovutusehdoissa huomioitavia näkökohtia ............................................................... 46
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 järjestelmat kehittyvät nopeammalla syklillä. Voidaankin ajatella, että älykäs kaupunki ei ole missään vaiheessa valmis, vaan se on ajan myötä kehittävää 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.


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

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.

## 2. Termit, lyhenteet ja viittaukset

### 2.1 Termit ja lyhenteet

<table>
<thead>
<tr>
<th>Termi tai lyhenne</th>
<th>Kuvaus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alueverkko</td>
<td>Alueellinen tiedonsiirtoverkko. Tässä dokumentissa alueverkolla ei tarkoiteta sähkönsiirtoverkoaa.</td>
</tr>
<tr>
<td>Avoin tieto, open data</td>
<td>Vapaasti saatavilla ja muokattavissa oleva tieto, jonka käyttöä, muokkausta ja uudelleenjakelua ei rajoiteta.</td>
</tr>
<tr>
<td>Henkilötieto</td>
<td>Kaikenlaisia luonnollista henkilöä taikka hänän ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. (Henkilötietolaki 523/1999)</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communication technology, tieto- ja viestintäteknologia</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things, esineiden internet</td>
</tr>
<tr>
<td>JHS</td>
<td>Julkishallinnon suositukset</td>
</tr>
<tr>
<td>JYVSECTEC</td>
<td>Jyväskylän ammattikorkeakoulun kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus</td>
</tr>
<tr>
<td>Jäänärsriski</td>
<td>Riskin jäljelle jäävä osuus, jota ei haluta tai voida poistaa.</td>
</tr>
<tr>
<td>KaPA</td>
<td>Kansallinen palveluarkkitehtuuri -hanke</td>
</tr>
<tr>
<td>Katakri</td>
<td>Kansallinen turvallisuusauditointikriteeristö</td>
</tr>
<tr>
<td>Kiinteistöverkko</td>
<td>Kiinteistöihin rakennettava verkko, jota käytetään kiinteistöautomaatiojärjestelmien tiedonsiirtoon.</td>
</tr>
<tr>
<td>Musta verkko</td>
<td>Kankaan alueen valokuituvverkko, joka tullaan toteuttamaan osana kunnallistekniikan rakentamista.</td>
</tr>
<tr>
<td>Rova</td>
<td>Kansallisen palveluarkkitehtuurin Rooli- ja valtuutuspalvelu</td>
</tr>
<tr>
<td>Smart city, älykaupunki</td>
<td>Kaupunki, jolla pyritään parantamaan julkisia asioita ICT-pohjaisten ratkaisujen pohjalta eri sidosryhmien yhteistyöllä</td>
</tr>
</tbody>
</table>
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 verkkoko- ja tietoturvan varmistamiseksi koko unionissa", COM/2013/048 final - 2013/0027 (COD)

Euroopan unionin neuvosto, "Euroopan unionin kyberturvallisuusstrategia: Avoimen, turvallisen ja vakaa verkkoympäristö", 7.2.2013


Huoltovarmuuskeskus, "Mallilausekkeita – sopimuksen kohta toiminnan jatkuvuus", 15.5.2009

Huoltovarmuuskeskus, "Toiminnan jatkuvuuden hallinta", 15.5.2009


Jyväskylän kaupunki, "Viisas Kangas - Jyväskylän Kankaan ICT-ratkaisujen kokonaisuunnitelma", 2015

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

Liikenne- ja viestintäministeriö, "Älykäs kaupunki – Smart City Katsaus fiksuihin palveluihin ja mahdollisuksiin", 13.5.2014

Puolustusministeriö, "Katakri - Tietoturvallisuuden auditointityökalu viranomaisille", 2015


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

Tietoyhteiskunta 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, "Määryys 65 kiinteistön sisäverkoista ja teleurakoinnista", 65A/2014

Viestintävirasto, "Suojamaattomia automaatiolaitteita suomalaisissa verkoissa" 29.6.2015
3. Strategian taustoitus

3.1 Mitä on kyberturvallisuus?


Kuva 1: Tietoturvallisuus, ICT-turvallisuus ja kyberturvallisuus

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


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 monimutkaisemmin ja useimmiten internetin kytkeydyttä tietojärjestelmistä, mikä altistaa ne enenevässä määrin kyberturvallisuusuhille. Tulevaisuudessa tällaisten kohteiden lukumäärä tulee kasvamaan entisestään.


Kyberturvallisuusuhkia voivat aiheuttaa tavallisten ihmisten virheellinen toiminta, ekologi- ja järjestelmien virheet, kyberklikivalta, kyberrikollisuus, kyberterrorismi sekä kybersodankäynti.


Usein yksinkertaisilla edullisilla haattotoimenpiteillä voidaan aiheuttaa suuria vahinkoja, minkä vuoksi kyberuhilta suojautumisen kustannukset kasvavat. Kybermaailmassa suojautumisen kustannukset ovat tyyppillisesti korkeammalle verrattuna hyökkäyskustannuksiin.

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

Varautumisen lääkäkohta tulee olla kyberturvallisuuden riskianalyysi, jossa arvioidaan sekä riskin toteutumisen todennäköisyyttä että vaikutusten suuruutta. Toimenpiteet uhkien torjumiseksi tulee suhtautua riskiarviointiin tuloksiksi 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, ilmainsuvapaudeiden, henkilötietojen ja yksityisyysen 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 että niille on kohdistettava regulaation kautta vaatimukset liittyen läpinäkyvyyteen, vastuukysymyksiin ja tietoturvaan. Strategia itsessään perustuu viidelle painopisteelle, jotka ovat:

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


3.4 Suomen kansallinen kyberturvallisuusstrategia


Vision saavuttamiseksi strategia määrittää toimintamallin, jossa kyberturvallisuuden johtamisesta vastaa ylimmällä tasolla valltioneuvosto, mutta kuka 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 torvaamiseen osallistuvien viranomaisten ja muiden toimijoiden välisen 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 kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.

4. Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kyberkimmitetympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.

5. Puolustusvoimat luo yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua kyberuhkat ja -häiriöt tilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.

6. Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumien toimintaan.

7. Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.

8. Kansallisella lainsäädännöllä varmistetaan tehostettavat kyberturvallisuuden toteuttamisen edellytykset.


10. Strategian toimeenpanoa valvotaan ja toteumaa seurataan.

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

3.5 Jyväskylä kansallisena kyberturvallisuuden toimijana


3.6 Kankaan alue kyberturvallisuuden pilottiylpäristönä

Kankaan alueesta on mahdollista rakentaa ympäristö, joka hyöityy Jyväskylän kyberturvallisuuden osaamiskeskitävästä 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 pilottiylpäristönä. Alueen ICT-ratkaisujen periaatteissa oleva kyseenalaistava ote, Jyväskylän kaupungin vahva panostus alueen kehittämiseen, alueelle toteutettavat edistykselliset tekniset ratkaisut, oppilaitosten osallistuminen alueen kehittämiseen, ICT-rytysten kiinnostus alueesta, alueelle kaavallut digitaalisuutta hyödynnävät palvelutoiminnat sekä alueen sopiva koko edesauttavat kaikki Kankaan alueen toimimista kyberturvallisuuden pilottiylpäristönä.

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

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

Kun pilottointi huomioidaan jo varhaisessa vaiheessa alueen suunnittelua ja rakentamista, parantavat pilottointimahdollisuuksien huomioonottaminen sopimuskäytännöissä, kerätyn tietoaineiston tietoturvallinen hallinta sekä alueenopalatun hyödynnäminen pilottoinnissa tai siitä viestimisessä edelleen alueen edellytyksiä toimia pilottointiympäristönä.

Kyberturvallisuuden pilottiylpäristön hyödynnäminen on hyvin vastuullista toimintaa eikä pilottoinnin yhteydessä voida ottaa riskejä Kankaan alueen asukkaiden turvallisuuden suhteen. Pilottointien huolellinen suunnittelu sekä pilotointiin osallistuvien ihmisten tietojen turvallinen käsitteily ovat edellytyksinä pilottointien toteuttamiselle.

3.7 Strategian tuottaminen


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
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 myöhemmän aktiivista turvallisuusasioiden hallintaa koko elinkaaren ajan.

Merkitävän 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 huomioi riittävästi turvallisuusnäkökohtia, lisääntyy alueen haavoittuvuus. Infrastruktuurin turvattomuus voi johtaa siihen, että sen varaan ei uskalleta toteuttaa kaavaltujia palveluita ja Kankaan alueen visio älykkästä 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 suunnittelualasteelle: turvallisuusasioiden suunnittelun itsessään on hyvä asia, mutta kätännön hyödyt suunnittelusta saadaan vasta suunnittelujen toteutuksesta ja kyberturvallisuus kulkeutuu pelkästään paperille.

- Sopimukselliset puutteet: Kankaan alue on monitoimijaympäristö, jonka kokonaisturvallisuus on vaihdettava eri toimijoiden tekemisiä. Mikäli eri toimijoiden turvallisuusvastuuja ei ole sopimuksia, ei ole mahdollisuus edellyttää alueella...
3.9 Strategian linkittyminen muihin kehittämisohjelmiin

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

3.9.1 Kohti resurssiviisautta


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

3.9.2 Uusi sairaala – hanke 2020


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 pilottoida Kankaan alueen Living Lab-ympäristössä.

Kankaan alueen ja uuden sairaalan toimintakonseptien rinnakkainen käsitteily voisi auttaa löytää aivan uudenvuotuisia 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. Lähtökohtaa on tutkimuksen, koulutuksen, yritysten ja julkisen hallinnon tiiviis 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 innovaatiokeskitettymä.

3.9.4 Muut älykkäät kaupunki-hankkeet


Fiksu Kalasatama [http://fiksukalasatama.fi]

Oulussa on alkanut Hiukkavaaran alueen älykaupunkihanke. Vanhalle kasarmialueelle rakentuu 20.000 asukkaan kaupunginosan, joka on käyttäjälähtöinen, älykkään energiatehokas ja neljän vuodenajon kaupunkielämän keskus. Lisäksi uusi Hiukkavaaran keskus palvelee 40 000 lähiseudulla asuvaltaa oulualaista.

Hiukkavaara [http://www.ouka.fi/oulu/hiuukkavaara]

Edellä mainittujen hankkeiden lisäksi on meneillään useita muitakin älykkäseen elämiseen ja asumiseen liittyviä hankkeita. Laajempaa tietoa sekä näistä hankkeista että yleisempiä tietoa älykaupungeista löytyy Liikenne- ja viestintäministeriön julkaisusta ”Älykäs kaupunki - Smart City, Katsaus fiksuin palveluihin ja mahdollisuusiin”.

3.9.5 Kansallinen palveluväylä

Kansallinen palveluarkkitehtuuri on ohjelman, jonka tavoitteena on luoda yhteentoimivaa digitaalisten palvelujen infrastruktuurin, jonka avulla tiedonsiirto organisaatioiden ja palvelujen välillä on helppoa. Palveluväylä on palveluarkkitehturin tiedonvälityskerro, 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. Piilotihankkeissa 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 toimeenpanosuunnitelmän elinkaari

Tätä strategiaa tyydentää 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.
Dokumentteissa 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 hyvä, sujuvaa ja turvallista viihtyisässä ympäristössä. Kangas on resurssiviisas ja työpalikkaympäristönä 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.


"Kangas vetovoimainen edelläkävijä – ICT-ratkaisut tukemassa tavoitteita”

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


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


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 samanaikaisesta kehittymistä. Manuaalisen työn osuu
päivittäisessä operoinnissa ja valvonnassa pienenee ja ihmisen vastuulle jäävät
enemmän päätelöä vaatia tehtävät, mututosten 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,
onka hyökkäyspinta-ala on suuri."

Viisas-Kangas on toimintaympäristöön hyvin tieto- ja tietoliikenneintensiivinen, jossa eri
toimijat hyödyntävät alueen tarjoaman palveluita ja tietoja käyttäen avoimia rajapintoja.
Väikä rajapinnat on ensisijaisesti tarkoitetut alueella olevien tai alueelle palvelua
tarjoavien toimijoiden käyttöön, näkyvät ne muillekin – myös ei toivotuille tahole.

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 turvallisuuslinjausia
vaan linjauset ja ratkaisut tulee suunnitella tapauskohtaisesti.

Hyökkäyspinta-ala on Kankaalla erilaisten laitteiden ja toimijoiden johdosta niin suuri,
että turvallisuuskohtalaisuuden pääpaino on sietoisuuden kehittämisessä
kustannustehokkaasti. Kustannustehokkuus on optimin hakemista suojaautumisen
customuksen ja turvallisuusuhkien realisoitumisen kustannusten väliillä.

4.3 Turvallisuusympäristön jäsenys

"Kankaan alueen kyberturvallisuuden ydin on alueen kriittisen infrastrukturan
sekä siihen liitettynä 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.
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 omasta toiminnastaan 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 vaatimuksistaan 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 tyypissä uhkia. Pidemmän aikavälin yksityiskohtaisista 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 nopeasti teknologisen 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 tekniologi ja palvelut kehittyvät turvallisemmiksi, mutta markkinoille tulevat uudet tekniologiat ja palvelut jakaantuvat edelleen turvallisuudentojaan eritasoisin ratkaisuihin.
- Synty 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.

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 läpinäkyvyyttä sopimusten turvallisuusvaatimusten vastaamiseksi. Kyberturvallisuuden näkökulmasta avoimuus ei tarkoita kaiken tiedon automaattista avoimuutta, vaan tiedon tarpeettoman luottamukselliseksi määrittelyyn välttämistä.

Älykkyys ilmenee Kankaan alueella monissa muodoissa. Uudet teknologioiden ratkaisut tulevat olemaan älykkäitä ja tarjoamaan alueen asukaille ja työskentäville apua arkipäiviäisiin ongelmiin. Toisaalta älykyyyn ilmenee myös resurssiviisautensa, jolloin alueelliset ratkaisut korvaavat perinteisiä taloyhtiökohtaisia toimintoja sekä infrastruktuurin ja ratkaisujen aiempaa pidempiä elinkaarina. Älykkyyteen liittyviä näkökulmia on kuvattu tarkemmin "Viisas Kangas - Jyväskylän Kankaan ICT-ratkaisujen kokonaissuunnitelma" –dokumentissa.

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 jatkuvaa prosessi. Kyberturvallisuus ja ICT-toimintaympäristö muuttuvat nopeasti, joten on tärkeää muodostaa hallintamalli, jolla muutoksiin pystytään reagoimaan tarvittaessa nopeastikin.

Jatkuva kehittäminen

<table>
<thead>
<tr>
<th>Valvonta</th>
<th>Koordinointi</th>
<th>Toimijat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arviointi</td>
<td>Alueen sisäinen</td>
<td>Kaupunki</td>
</tr>
<tr>
<td>Päätöksenteko</td>
<td>Kaupungin sisäinen</td>
<td>Yritykset</td>
</tr>
<tr>
<td>Toimenpiteet</td>
<td>Kansallinen</td>
<td>Oppilaitokset</td>
</tr>
</tbody>
</table>

Kuva 4: Kyberturvallisuuden hallintamallin tavoitteet


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 keskitetty pelkästään Kankaan alueen kyberturvallisuuteen, vaan se voi olla osa laajempaa kokonaisuutta, esimerkiksi koko

5.3 Riskeihin perustuvat toimintasuunnitelmat


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

Uhka yhdessä toteutumistodennäköisyytensä kanssa muodostaa riskin, jota voidaan pientenä arvioimaan ja teknologian kehittyminen muodostavat uusi uhkia. Näin ollen ollaan tilanteessa, jossa joudutaan jatkuvasti arvioimaan järjestelmiin ja palveluihin kohdistuvia uhkia ja niiden vaikutuksia.

Urhoitamisessa ja arvioimassa voidaan pientä arvioimaan ja teknologian kehittyminen muodostavat uusi uhkia. Näin ollen ollaan tilanteessa, jossa joudutaan jatkuvasti arvioimaan järjestelmiin ja palveluihin kohdistuvia uhkia ja niiden vaikutuksia.

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 akutulostukseissa 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 suurin vaikutus suhteessa toteutumisen todennäköisyyteen. Koska sekä vaikutus että toteutumisen todennäköisyys voivat muuttaa, joudutaan kaikkien kohteiden riskiä uudelleenarvioimaan säännöllisesti.

Kuva 5 Kyberturvallisuusriskeihin varautuminen
Riskienhallinta tulee sitoa osaksi hallintamallia, joka määrittelee prosessin toiminnasta vastaavat toimijat sekä raportointivollisuudet. 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 hyväksikätevästi eri elinkaaren ajan ja ne tulevat huomioiduksi myös osana hankintatoja ja sopimuksia.

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

### 5.4 Sopimuksellinen velvottaminen

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

![Sopimuksellisen velvottamisen elementtejä](Image)

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 resoursesja. Sen vuoksi markkinoinnilla 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 pisteet yksillä suoraa 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 ketjuntuessa 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 alku vaiheesta alkaen, jolloin varmistetaan, että käyttöönotettavat järjestelmät ja palvelut vastaavat turvallisuudeltaan alueen normeja.

6. Strategiset kannanotot

6.1 Infrastruktuuri

Modernin kaupunkiymäärästä infrastruktuurin ydin muodostuu sähkö- ja tietoliikenneyhteyksistä, rakennuksista sekä niihin liittyvistä perustoiminnuista kuten valaistuist, lukituksist ja kiinteistöautomaatioon liittyvät palvelut.

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

Infrastruktuurin palveluiden tuottamiseen kohdistuvat korkeat tietoturvavaihtoehdot, joita ovat:

- Hallinnassa käyttettävien järjestelmien todennettu tietoturvallisuus
- Eriydet hallintaympäristöt kriittisten palveluiden hallinnassa
- Vahva käyttäjien tunnistaminen kriittisissä palveluissa
- Tietoturvalliset toimintamallit palveluiden tuottamisessa
- Todennetut varajärjestelyt poikkeusilmiöiden 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 tietoliikenneympäristööksi Kankaalle rakennetaan valokuitupohjainen alueverkko eli niin sanottu musta verkko, joka toteutetaan rakentamalla ja hallinnomaalla fyysisten siirtoyhteyksien (kuituyhteyst, putket) infrastruktuuria.

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

Tietoliikenneintensiivisen älykaupungin toimivuuden varmistaminen asettaa alueverkolle korkeat saatavuuksivaihtoehdot, minkä johdosta:

- verkon liityntäpisteet on suojattava fyysisesti,
alueverkon kaikki yhteydet tulee varmistaa fyysisesti erillisin varayhteyksin,
verkon hallinnoinnista vastaavan tähän on monitoroitava verkon toiminta
poikkeamien havaitsemiseksi ja
poikkeamatilanteissa on oltava valmius nopeisiin korjaaviin toimenpiteisiin

Kriittiset liityntäpiisteet, joilla on laaja vaikutus alueverkon toiminnan kannalta, tulee
suojata vahvemmin. Tällaisia kriittisiä liityntäpiisteitä ovat esimerkiksi alueverkon
pääasemapeiteet. Kriittisissä liityntäpiisteissä on

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

Koska verkkoon on alueellisesti melko pieni, verkon operointivastuu on suositeltavaa
antaa kaupallisena verkkoperaatörillä vastuulle, jolloin verkon jatkuva valvonta ja
kunnossapito on mahdollista toteuttaa kustannustehokkaasti. Verkkoperaatörillä
velvollisuus kyberturvallisuuden toteuttamiseksi määrittää

Kankaan alueella tämä voidaan toteuttaa varaamalla valokuitupohjaisesta alueverkosta
omia kuituja tähän käyttöön tai rakentamalla kokonaan rinnakkaisia fyysisiä
valokuituverkoja.

Rinnakkaisen verkon rakentamiskustannukset voivat olla merkittävästi edullisemmat
kuin kriittisten toimintojen erottaminen omakohtainen rakennus, jolloin verkkoon yhdessä
fyysisessä verkkossa. Kaikki rinnakkaiset verket eivät kuitenkaan ole koko Kankaan
alueen laajuisia, mutta hallintamallin kautta on huolehdittava, että verkkojen rakenteet
ongokumentoitu ja toiminnan jatkuvuuden varmistamisen kannalta olennaisten
osapuolten tiedossa.

Kankaan alueen kriittisten kiinteistö-, turvatekniikan-, kunnallistekniikan ja muiden palveluiden
tietoverkkokaartatehtävien tulee perustaa erikseen suojattuihin turvallisiin alueisiin.

Kriittisten toimintoja varten voidaan rakentaa rinnakkaisia fyysisiä verkoja.

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

Rinnakkaisen verkon rakentamiskustannukset voivat olla merkittävästi edullisemmat
kuin kriittisten toimintojen erottaminen omakohtainen rakennus, jolloin verkkoon yhdessä
fyysisessä verkkossa. Kaikki rinnakkaiset verket eivät kuitenkaan ole koko Kankaan
alueen laajuisia, mutta hallintamallin kautta on huolehdittava, että verkkojen rakenteet
ongokumentoitu ja toiminnan jatkuvuuden varmistamisen kannalta olennaisten
osapuolten tiedossa.

Kankaan alueen kriittisten kiinteistö-, turvatekniikan-, kunnallistekniikan ja muiden palveluiden
tietoverkkoarkkitehtuurin tulee perustaa erikseen suojattuihin turvallisiin

Kriittisten toimintoja varten voidaan rakentaa rinnakkaisia fyysisiä verkoja.

Kriittisten kiinteistö-, turvatekniikan-, kunnallistekniikan ja muiden palveluiden
tietoverkkoarkkitehtuurin tulee perustaa erikseen suojattuihin turvallisiin

Kriittisen verkkoinfrastruktuurin rakentamisessa tulisi noudattaa seuraavia linjauksia:

Uusien verkkoyhteyksien on oltava mahdollista ilman aiemmin rakennettun
infrastruktuurin purkamista ja uudelleenrakentamista.

Rakennusvaiheessa tulisi varata ylimääräisiä erillisiä kuituja turvallisia
erillisverkoja varten käytettäväksi myöhemmin.

Edellä luetellut vaatimukset ovat tyypillisiä kriittisen infrastruktuurin palveluille esitettyjä

Edellä luetellut vaatimukset ovat tyypillisiä kriittisen infrastruktuurin palveluille esitettyjä

Edellä luetellut vaatimukset ovat tyypillisiä kriittisen infrastruktuurin palveluille esitettyjä
turvallisuusvaatimuksia. Yksityiskohtaiset vaatimukset tulisi suunnitella

Edellä luetellut vaatimukset ovat tyypillisiä kriittisen infrastruktuurin palveluille esitettyjä
turvallisuusvaatimuksia. Yksityiskohtaiset vaatimukset tulisi suunnitella

tapaukskohtaisesti 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 suojausena järjestelmien laitteet on sijoitettu lukittuihin kaappeihin ja laitetiloihin, joihin pääsyä valvotaan.
- Verkon liikennettä monitordoidaan säännöllisesti kapasiteetin riittävyyden varmistamiseksi ja poikkeamien havaitsemiseksi.

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 suoratoistoa sekä luotettavampia ja turvallisempia yhteyksiä kuin langattomilla ratkaisuilla.

Viestintävirasto on raportissaan "Suojaamattomia automaatiolaitteita suomalaisissa verkkoissa" tuonut esille, että edelleen suomalaisista tietoverkkoista löytyy suojatamattomia kiinteistöautomaatiojärjestelmiä, vaikka asia on tuotu julkisuuteen jo aiemman tutkimuksen yhteydessä.


Kiinteistöautomaatiojärjestelmiän 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 käyttöä olemassa verkon saatavuutta.

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 kestävää kaapelointiteknikka, onkin syytä keskittyä siihen, että miten kaapelointi voidaan vaihtaa myöhemmässä vaiheessa. Tähän toimii ratkaisuna kaapelireittien toteuttaminen joten, jolloin kaapeloinnit voidaan myöhemmin helposti lisätä.

6.1.4 WLAN-verkot

"Langattomia verkkoja käsittelään kuin julkisia verkkoja."

Tämän hetkisen näkemynksen mukaan alueen kattavaa julkista WLAN-verkkoa ei olla toteuttamassa ja toisaalta kiinteistökaapeloinnin vähennetään tarvetta alueelliselle langattomalle verkolle. Kuitenkin alueen suunnittelussa ja kiinteistöjen infrastruktuurin toteutuksessa huomioidaan tontinluovutusehdotissa tehtävät varaukset tarvittaville asennuspaikoille ja laitetoihin 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 tapauksohaisesti lähinnä verkossa siirrettävän datan sisällön ja siihen kytkettyjen laitteiden perusteella.

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

6.1.5 Mobiiliverkot

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

Operaatiorit vastaavat matkapuhelinverkkojen rakentamisesta ja alueen puhelinverkon kuuluvuudesta. Tontinluovutusehdotissa varaudutaan siihen, että kiinteistöössä on varaukset tarvittaville asennuspaikoille, laitetoihin ja yhteysreiteihin kattava palvelukattavuutta ja operaatoreiden toimintaa varten.

Matkapuhelinverkon teknisiin tarpeisiin varaudutaan tontinluovutusehdotissa ja aluekaapeloinnin, sekä kiinteistökaapeloinnin suunnittelussa. Matkapuhelinverkon laitetoilta koskevat samat turvallisuusvaatimukset kuin muitakin kriittisten infrastruktuurin käytössä olevia tiloja, eli niiden on oltava lukittuja ja valvottuja. Turvallisuusvaatimukset tulevat tarkentaan suunnittelun yhteydessä.

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

Mobiiliverkkoja voidaan käyttää kriittisten verkkojen varayhteytenä edellyttäen, että ne käyttävät erillistä fysistä kiinteään verkon yhteyttä. Näillä osin mobiiliverkot voivat turvata kriittisiä toimintoja. Tämä mahdollisuus tulee huomioida suunnitelmaessa toipumissuunnitelmiä 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 energiatehokkaisissa rakennuksissa. Raportissa esitetyt toimenpiteet tulisi huomioida tontinluovutusehdossa, jotta rakennuksissa varaudutaan matkapuhelinverkon käyttöön soveltuvalla kaapeloinnilla mahdollisuuksien kulu vuosina.

6.1.6 Toimitila-arkkitehtuuri

"Osassa toimitiloja tulisi mahdollistaa korkean turvaluokan tilojen toteutus."


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 toetutetaanko 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 kulkumisdata ja niiden tarkastelu.

Jyväskylän yliopiston Agora Centerin tekemän selvityksen perusteella mekaanisen lukituksen kertakustannus on noin puolelta edullisimmaan sähköaleselle, joka tuottaa sähköä ratkaisuun lisämaksut äänijärjestelmässä. Kuinka mahdollistaa sähkömaksu sähkömaksunjärjestelmä 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 määrittää kullekin käyttäjälle ja mahdollistetaan alkarajoitteiset kulkuoikeudet.
- Elektroniset avaimet voidaan poistaa järjestelmästä, mikä poistaa tarpeen uudelleensarjoituksele ja alentaa kustannuksia.
- Elektroniset lukot tallentavat ovista kulkevien avainten tiedot ja kulkuun suunnatut tiedot voidaan seurata, mikä ennalta ehkäisee väärinkäytöksiä. Jälkeenpäin voidaan todentaa millä avaimella on kohteeseen kuljettu.

"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.


Jos alueen kaikki rakennuksiin ei tule sähköistä kulunvalvontaa alkuvaiheessa, olisi kuitenkin edellytettävän tontinluovutusehdotus ja sähköisen lukituksen lisäämisestä myöhemmin. Viestintäviraston "Määräys 65 kiinteistön sisäverkoista ja teleuralankokasta" edellyttää kattavan huoneistokaapelointilaitteistoa ja kaapelireittien toteuttamista, joten tontinluovutusehdotissa olisi mahdollista vaatia vastaavaa kaapelointiä 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 alueportaaliillä 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 mahdollisuutet.


Tärkeä osa sovellusten turvallisuutta on käytettävyys (tässä yhteydessä ei tarkoita 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.


6.1.9 Infrastruktuurin huolto ja ylläpito

"Infrastruktuurin ylläpito on hallittua ja säännöllistä."


Monitoimijaa ympäristössä ylläpidon tulee tapahtua hallitusti. Kaikkien alueen toimijoiden tekemät huoltotöitä ylläpitoon tulee hallinnoida siten, että ylläpitotoimet eivät aiheuta ongelmia alueen toiminnan jatkuvuudelle. Tämä koskee lähinnä infrastruktuurin ylläpitoa, mutta myös sähköisiä palveluihin liittyviä järjestelmiä, kuten identiteetin hallintajärjestelmiä.
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 heikoinman 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 huomioon alueen kyberturvallisuuden 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 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. Tätä palvelun turvallisuuden kannalta, ainoa mahdollisuus edellyttää korkeampaa turvallisuustasoa, on sopimus.


Yksilön etujen kannalta on tärkeää huomioida sopimuksissa palvelun käyttäjien yksityisyysen suojasta. Pilvipalveluiden yhteydessä on nousut esille uusi termi, yksityisyysen suojaustasopimus eli Privacy Level Agreement (PLA). Sen tavoitteena on sopia palveluiden tarjoamasta yksityisyysen suojasta eli kuinka henkilötiedot on suojaantumessa palvelussa. Kankaan alue voisi toimia pilottialueena, jossa palveluntuottajiltta...
edellytetään PLA –liitetään 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 riskiarviointin 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.


6.2.3 Yksityisyystä edellytetään

"Yksityisyystä edellytetään" sisältää palvelut toteutetaan yksityisyysyksen suojana kunnoittaaan. Lähtökohtina palveluiden tuottamisessa ja niihin liittyvässä tietojen keruussa ovat lapsinäkyyvys ja asukkaan oma päättävärla 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 selkokielen kuvaus kerättävistä tiedoista, miten niitä käytetään ja mitä haittaa tietojen luovuttamisesta voi olla. Suostumusta

---

14.8.2015
annettaessa tulee erottaa suostumus varsinaiseen tietojen käyttötarkoitukseen ja muihin käyttötarkoituksiin.

Sensoreiden keräämä tieto on ensisijaisesti anonyymi. Osa palveluista voi kuitenkin edellyttää käyttäjätunnukseksi, 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 kanssa yhteisessä taloudessa eläviä koskeviiksi.


Julkaisetaessa tietoja edelleen jatkohyödyntämästä varten tulee varmistaa että aineistosta on poistettu kaikki henkilötiedot ja että henkilö ei ole yksilöitävissä mistään tiedoista tai niiden yhdistelmissä.

6.2.4 Tunnistaminen ja pääsyoikeuksien hallinta

"Kankaan alueella tarvitaan keskitetty tunnistus- ja pääsynhallintapalvelu"

Lähtökohtana tunnistamisessa tulee olla henkilön yksilöllinen tunnistaminen. Riippuen käytettävää palvelusta ja siinä käsiteltävää tiedosta, voidaan edellyttää vahvaa tunnistamista. Vahva tunnistaminen on välttämätömyys osassa palveluita sekä infrastruktuurin haavoitumisen vuoksi.

Vahvaa tunnistamista on edellyttetävänä vähintään kaikissa niissä palveluissa, joiden avulla hallitaan alueen kriittistä infrastruktuurista tai jotka mahdollistavat pääasyn henkilöistä kerättyyn yksityiskohtaiseen tiedoon.

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

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

Keskittelyn identiteetinhallinnan haasteena tulevat olemaan perinteistä, hierarkkista käyttöympäristöä monimuotoisemmat suhteet identiteetien ja hallittavan tiedon välillä. Esimerkiksi asuntokohtaisesti voidaan määrittää käyttöoikeuksia järjestelmiin, jolloin vuokralaisella ja asunnonomistajalla molemmilla on pääsy asunnon lämpötilatietoon. Samaan alkaen kuitenkin sähköisen lukituksen yksityiskohtaiset kulkutiedot kuuluvat henkilötietolain alaiseksi henkilötiedoks, joten asunnonomistajalla ei ole oikeutta nähdä
näitä tietoja, mutta vuokralaisen oikeus nähdä kulkutietoja rajoittuu vain siihen ajanjaksoon, kun hän on asunnonsa asunut.

Keskitetyn identiteetinhallinnan vaatimukset ja käyttötapaukset tulee määrittää tarkkaan ja etukäteen tulee varmista tietojenkäsittelyn lainmukaisuudesta eri käyttötapauksissa. Tämän jälkeen voidaan edetä vasta suunnittelemana identiteetinhallinnan teknistä toteuttamista vaatimusmäärittelyn pohjalta.

6.2.5 Valtuutusten ja suostumusten hallinta

"Tietojen keruun ja jatkohyödyntämisen tulee perustua henkilön antamaan suostumukseen"

Kankaan alueella on tiedonkeruut, joissa yhtenä edellytyksenä on henkilön antama suostumus tietojen keruulle. Lisäksi on toiminnallisia tarpeita, joissa esimerkiksi henkilö voi valtuuttua toisen henkilön tai palveluntuottajan pääsyn huoneistoon.

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 välyttää 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 asetettomat 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 kirjallisesta antamastaan suostumuksesta mutta kuten Tietosuojavaltuutetun toimisto on linjannut 27.7.2010 oppaassa "Henkilötietojen käsittely suostumukseen perusteella".

6.2.6 Todennettut 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 hyväksä ymmärtäen. Nän pystytään myös kehittämään uudenlaista osaamista älykaupunkiympäristöjen testaamisesta.

6.2.7 Tietoturvapäivitykset

"Tietoturvapäivityysten tekemätä 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. Nämä tietoja voidaan käyttää asukkaille ja yrityksille tuotettavissa palveluissa sekä tarjota niitä tutkimusvälineiksi. Yksittäisen asukkaan kannalta huomio kiinnittyi siitä, että miten hän voi hallita hänen käyttämänsä tietoja ja niiden hyödyntämistä.

Alueen asukkaiden yksityisyysen suojaan kannalta on tärkeää, että he tietävät mitä tietoja heistä kerätään ja miten tietoja käytetään. Lisäksi on tärkeää huomioida selkokieletys osoittamaan että tietoja käytetään mihin hän sopimusta tehdessään sitoutuu ja mitä hänestä kerättävän tietoja ja niiden hyödyntämistä.

Alueellinen palveluyhtiön ja Living lab –toimijoiden olisi mahdollista toimia esimerkiksi organisaatioina kuinka palvelusopimuksista ja rekisteriselosteista saadaan muodostettua yksilön yksityisyysen suojaan palvelevia dokumentteja. Tällöin kyseiset dokumentit olisivat selkokieleliä tukevaa suostumusta, joiden takaavat yksilöllinen läpinäkövyyn palvelutuotantoon ja tutkimustaidonとなり、joissa heidän tuottamia tietojaan käytetään hyväks. Esimerkiksi tutkimuksiin osallistujille olisi syytä selkeästi kommunikoida haitat ja riskit, joita tietojen luovuttamisesta voi aiheutua.

"Asukas vastaa huoneiston hankkimistaan järjestelmistä"


Vaikka vastuu huoneistoon hankkimistaan laitteista on asukkaalla, on tietoisuutta turvallisista järjestelmistä ja laitteista mahdollisuus parantaa alueen palvelutoimintaa erityisesti turvallisuudesta. On kuitenkin nähtävissä, että tulevaisuudessa asukkaiden 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 asettamia 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, alueelle tarjoavia yrityksiä sekä palveluita kehittäviä yrityksiä, ja asemassa on jopa palveluyhtiöitä sekä Jyväskylän kaupungin palvelutuotantoa.

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

Näissä tapauksissa yritykset tulevat sitoutumaan kyseisen infrastruktuuripalvelun tietoturvakykäytäntöihin ja huolehtia omassa toiminnassaan että asetetut turvallisuuskriteerit täyttyvät.

Seuraavassa on joitakin esimerkkejä alueella tapahtuvan palveluliiketoiminnan tietoturvavointimukisista.

- **Palveluyrityksen työntekijät käyttävät sähköistä kulunvalvontaa**, jonka avulla he pääsevät liikkumaan kiinteistöissä työtehtävien tarpeiden mukaan. Yrityksen on huolehdittava henkilöiden turvallisuusohjeistuksista tunnisteen käytössä sekä yrityksellä on oltava selkeät prosessit, joiden avulla varmistetaan että tunnisteen ovat vain niiden henkilöiden käyttössä, joilla on oikeus ja tarve liikkua kiinteistöissä. Älykkällä ratkaisuilla voidaan oikeuttaa oikeutta tai oikeuksia asiantuntevien 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 turvallisuusuhkien vastaan. Yritys huolehtii luottamuksellisista tietoja keräävien järjestelmienä ajantasaisista tietoturvavapäivityksistä. 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 sensitiivisempia data, sitä tiukemmat kriteerit”.

Tietoaineistojen käsittelyyn käytännön toimenpiteistä huolehtii erillinen dataoperaattori. Dataoperaattorin vastuulla kuuluu aineiston tallentaminen, aineiston turvallisesta käsittelystä huolehtiminen asetettujen kriteereiden mukaisesti sekä aineistojen edelleen välittäminen niille taholle, jotta 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 sovitettavat tapauksiltaan erikseen.

"Kerättävä tieto on hallittava mahdollisuuksien mukaan keskitetysti”

Dataoperaattori voi hallinnoida pääsyä tietoon keskitetysti. Keskitetystä hallinnalla tarkoitetaan tässä yhteydessä sitä, että tiedot kerätään keskitettynä tietovarastoon sen sijaan, että se haetaisiin suoraan sensoreilta. Tällöin pääsy sensoreihin voi olla hyvin rajattua. Keskitetyssä hallinnassa on useita merkittäviä tietovarastojen hallinnangevuuksia.

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

Keskityksen hyväksyntä ja valvonta on helpompaa kun 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 kiinteistöautomatiojärjestelmissä kerättävä tieto tulisi kuitenkin mahdollisimman pitkälle saattaa keskitetyn hallinnan alaisuuteen.

"Uusien palveluiden turvallisesta kokeilemisesta on tehtävä mahdollisimman helppoa”


Pilottointisopimusten 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.

"Pilootointi edellyttää tapauskohtaista turvallisuusharkintaa - perusasiat voidaan hoitaa etukäteen”


Pilootointien turvallisuusnäkökohdat tulee suunnitella tapauskohtaistesti. Huomioitavia näkökohtia ovat:

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

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

Living Lab –konseptin haasteena voi olla markkinoilla nopeasti kehittyvät henkilökohtaisen information keräämisesta ja suorittaman sopimusehtojen valvonnan muun muassa eettisistä näkökohdista. Näin osallistuja voi varmistaa siitä, että kolmas osapuoli on varmistanut sopimusehtojen tasapuolisuuden kaikkien osapuolten kannalta.

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 käyttökohteissa 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 tietyöverkossa.
- Tiedon on oltava uudelleenjaettavissa ilman käyttöehdotuloitoksia. Näin mahdollistetaan aineistojen nopea hyödyntäminen ja tehokas yhdistely.
• Tiedon on oltava uudelleenkäytettävissä. Nän sallitaan aineistojen esteetön ja innovatiivinen käyttö edistyksellisiin ja yllättäväkiinkin tarkoituksiin.

• Aineiston on oltava vapaa teknisistä rajoitteista 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, politiin, suuntautuneisuus tai etnisyyys rajoitaa pääsyä tietoon.

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

Perinteinen rajoitus tietojen julkaisemisessa on käyttötarkoitusdennon siinä, että sen tarkoituksena on käyttöä vain siihen tarkoituksen mukää tietosuojaselosteen mukaisuus vaatimus, mikä edellyttää sitä, että kerättyä henkilötietoa käytetään vain vuodenniin ja siihen tarkoituksen mukää. Vaatimuksena on kuitenkin mahdollista poiketa anonymisoimalla henkilötiedot, millä tarkoitetaan sitä että henkilötietoja sisältävää tietomassasta poistetaan ne tiedot, joiden perusteella henkilö on tunnistettavissa. Anonymisoinnin myötä henkilötietolainsäädäntö ei enää sovelleta dataan ja tiedot ovat vapaaehtoisesti hyödynnettävissä. Anonymiteetin takaaminen on kuitenkin haasteellista.


Lisää aiheesta löytyy mm. suosituksesta JHS 189 Avoimen tietoaineiston käyttööluopa, henkilötietolain sekä tietosuojavaluutetun kannanotoista. Kotimainen ohjeistus aivoimista tietoaineistoista ja anonymisoinnista on vielä vähäistä. Laajemmin aihepiiriä on käsitetty mm. Ison Britannian tietosuojavaluutetun ohjeissa.

Kankaan alueella on tunnistettavissa avointa tietoa, joka voidaan julkaista vapaasti. Tällaisia tietoja ovat esimerkiksi summa tason tiedot erilaisista mitattuista, joista ei voida tunnistaa yksittäisiä asukkaita tai huoneistoja, eikä niin liittyviä tapahtumia. Merkittävä osa kerätävästä tiedosta tulee kuitenkin olemaan luottamuksellista ja saatavuudeltaan rajoitettua. Tiedon omistaja on aina vastuussa siitä millä ehdolla tietoa tullaan julkaisemanaan lopulta myös sitä, että tietojen luovuttamisessa toimitaan lakiin ja sopimusehtojen mukaisesti.
7. Yhteenveto

Kankaan alueelle tulee olemaan Suomen ensimmäinen älykaupunginoso, 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 kehittämisele. Kyberuhteja tulee jatkuvasti lisää ja samaan aikaan kasvava tietovälineiden yhteydittäminen ja tietoverkkojen hyökkäytäväsaikaa aiheuttavat, että kyberturvallisuuden ylläpitämiseksi tarvittavien resurssien määrä tulee kasvamaan koko ajan.

Alueen visiona on Viisas Kangas, jossa asumisen ja elämisen arki on hyvä, sujuva ja turvallista viihtyvällä ympäristöllä. Kyberturvallisuuden näkökulmasta usein vision sujuvuus ja turvallisuus nähään vastakkain, mutta älykkäillä ratkaisuilla voidaan pyrkiä saavuttamaan molemmat yhtä aikaa.

Strategian kulmakiviksi, joilla visio pyritään ensisijaisesti saavutumaan, on nostettu hallintamalli, sopimuksellinen velvoittaminen ja riskeihin perustuvat toiminto- ja suunnitelmat. Näiden kulmakivien taustalla vaikuttaa kolme Kankaan alueen yleisempää periaatetta: Kangas on avoin, älykäs ja kokeilevaa.


Kankaan alueelle tulee suurin määrä erilaisia toimijoita, jotka hankkivat alueen kyberturvallisuuteen omalta osaltaan nykyisen turvallisuuden vaikutavia palveluita. Alueen kyberturvallisuuden kannalta on ehdotonta, että toimijat hankkivat sekä kyberuhteja että kyberturvallisuuden suunnittelualaa, eivätkä lopulliset palvelut ole välttämättä kyberturvallisuuden ylläpitämiseksi tulevaa strategiaa.

Turvallisuusvaatimukset tulee sujuvasti ja älykkäissä toiminta- ja suunnittelu- ja nettisyöpä ja sujuvasti tulevat suojattavaksi niiden elvyttämiseksi ja kehittämiseksi. Kyberturvallisuuden toteutuminen ei ole kiinni ainoastaan toimintaympäristöin tai sopimustekstejä, vaan sujuvasti ja älykkaasti voidaan mahdollistaa kyberturvallisuuden toteutuminen sekä jatkuvan kehittymisen ja turvallisuuden ylläpitämisen kannalta forestoista ja kokeilevaa ainekuoria.

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 verkoja. Valokuituverkon voidaan rakennusvaiheessa tehdä varauksia rinnakkaisille verkoille.
- Kankaan alue on tietointensiivinen ympäristö, johon tulee varautua myös verkon kapasiteetin suunnittelussa.
- Alueellisen tietoverkon merkitys osana kriittistä infrastrukturia 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 kyberuhiin seuraaminen ja niihin varautuminen.
- Verkko-operaattori on sopimuksellisesti velvoitettu huolehtimaan ja osoittamaan, että verkon kyberuhiin 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 ominaisuusiltaan yhtenäisiä. Sen vuoksi järjestelmätä, 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 salauta.

- Kriittiset järjestelmät, käytännössä kaikki sähköiseen lukitukseen ja kulunvalvontaan liittyvät järjestelmät varmistetaan kahdentamalla.

- Sähköisiä lukitusjärjestelmiä ja kulunvalvonta ylläpidetään hallitusti ja säännöllisesti.
Liite 3: Kiinteistödataan kerääminen ja kiinteistöjen etähallinta

Tähän liitteeseen on koottu kiinteistödataan 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 kiinteistödataan säilyttämisestä vastaavat yritykset velvoitetaan sopimuksellisesti osoittamaan, että kyberturvallisuus on huomioitu toiminnassa ja teknisissä ratkaisuissa kohteiden kriittisyyden edellyttämällä tavalla.
- Kiinteistödataan välittäminen tapahtuu salattuna tietoverkoissa.
- Tietoliikenneyhteydet kiinteistödataan kerääviin sensoreihin toteutetaan ensisijaisesti kiinteistökaapeloinnin kautta.
- Huoneistokohtaisen kiinteistödataan kerääminen tulee aina tapahtua suostumuksen perusteella 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 elinkaariikustannukset, 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.
- Sähköisen lukituksen teknisen ratkaisun tulee olla sellainen, että se on integroitavissa alueelliseen keskitettyyn kulunvalvontajärjestelmään.