

Jatkuvuudenhallinta ja pilvipalvelut – Miksi portit eivät aukene meille?

Tuomo Pekkarinen

Taustaa

IT-INVESTOINNIT Teemu Laitila 26.5. klo 10:12

Suomalaissairaala kahdentaa it:tä ja parantaa palvelutasoa 15 miljoonalla



JAA
ARTIKKELI



Kuopion yliopistollinen sairaala aikoo panostaa jopa 15 miljoonaa euroa it-varautumiseen ja kyberturvaan kolmen seuraavan vuoden aikana. Investointien tarkoituksena on varmistaa, että sairaala pystyy toimimaan kaikissa poikkeustilanteissa.

- **Tietoliikennekatkos 8/2015**
- Digitalisaatio
 - Toimintaympäristön muuttuminen mm. paperiton sairaala –hanke
- EU:n 14.4.2016 hyväksymä uusi yleinen tietosuoja-asetus ja sen tuomat vaatimukset vuoteen 2018 mennessä
- Palvelutasojen puuttuminen Istekin ja PSSHP:n välisistä palvelusopimuksista
- ➔ **Sairaalan toiminnan kokonaisriskiarvio, jonka seurauksena varautumishanke käynnistyy 2016**
- Suunnittelun pohjalla
 - Standardit kuten ISO 27001, ISO 27002, ISO 27005, ISO 27799, ISO 31000
 - Vahti vaatimukset, vahti korotettu taso
 - Posa 2016 – oman toiminnan turvaaminen
 - **Kriittiset käyttötapaukset toiminnan näkökulmasta ja niihin liittyvät ICMT-järjestelmät ja -palvelut**

Tavoitteena toteuttaa korkean käytettävyyden ICT-ympäristö, joka:

- mahdollistaa huoltotoimenpiteiden tekemisen 24/7 siten, että ne eivät aiheuta katkoja toimintaan
- varmistaa yhteistoiminta-alueen laajuisten palveluiden 24/7 saatavuus
- varmistaa potilastiedon
 - saatavuus
 - eheys
 - luottamuksellisuus
- mahdollistaa paremman potilasturvallisuuden ja sairaalan toimintojen jatkuvuuden hallinnan
- mahdollistaa digitalisaatiosta aiheutuvien riskien hallinnan
- mahdollistaa kriittisten järjestelmien katkottoman käytettävyyden



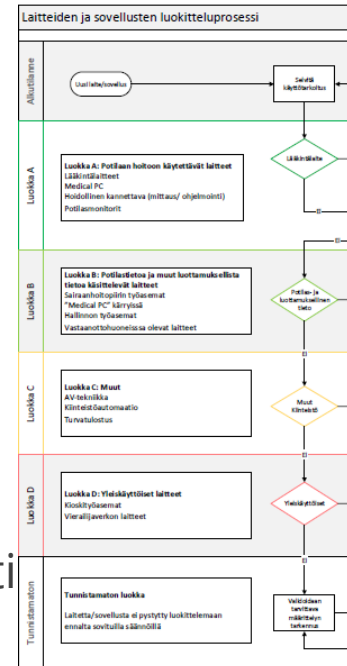
ICT-varautumishanke 2016-2020



Varautumishankkeen tuloksia

• Tietoliikenne

- Vikasietoinen runkoverkko
- Verkot segmentoitu sekä käyttötarkoituksen, että laitemäärien mukaan
- Laiteluokat segmentoitu omiin verkkolohkoihin siten, ettei verkkolohkossa olevien laitteiden määrä ylitä xx laitteen rajaa
- Eri rooliset palvelimet ym. eriytetty omiin dedikoituihin verkkolohkoihin
- Verkkosegmenttien suojaustasot ovat luokittelun mukaisesti suojattu palomuurauksella ja mm. sovellus- sekä käyttäjätietoisuudella



Varautumishankkeen tuloksia

- **Kapasiteettipalvelut**

- Toisen fyysisen konesalin käyttöönotto
- Tietojärjestelmien fyysinen hajauttaminen
- Kriittisten tietojärjestelmien virtualisointi 100%

Varautumishankkeen tuloksia

- **Tietoturva**

- Sopimuskäytäntöjen kehittäminen
 - Tietoturvan, tietosuojaan ja jatkuvuuden hallinnan huomioiminen palvelusopimuksissa
 - Palvelukohtaisten jatkuvuussuunnitelmien kehittäminen
- Tietoturva- ja tietosuojariskien huomioiminen jo vaatimusmäärittely- ja hankintavaiheessa
- Jatkovaa riskien arviointia kokonaisarkkitehtuurin kaikilla tasoilla koko käyttöönottoprojektin ajan -> muutoksissa ja määräajoin
 - Koskettaa sekä tietojärjestelmiä, lääketieteellisen tekniikan ratkaisuja, kiinteistöautomaatiota, iot-laitteita yms.

Varautumishankkeen tuloksia

- 24/7 valvomotoiminta
 - Havainnointikyvyn lisääminen (hyökkäysikkunan pienentäminen)
 - SIEM, tunnisteet, heuristiikka, anomaliteettien havainnointi
 - Reagointikyvyn lisääminen -> Triage -> Incident response (tietoturvapoikkeamien reaaliaikainen käsittely), rajoittamiskyvykkyys, forensiikka, ilmoituskyvykkyys
- Säännölliset haavoittuvuusskannaukset ja korjaustoimet
- Muutoksenhallinnan kehittäminen
- Verkostojen hyödyntäminen (toimialan muut toimijat, viranomaiset, cert-fi, kyberturvallisuuskeskus, hvk, pv ...) ja tiedonjakaminen

Varautumishankkeen tuloksia

- Kolmansien osapuolten etäyhteyskäytäntöjen kehittäminen
 - Henkilökohtaiset tunnukset
 - Lokitietojen kerääminen
 - Pääsyn rajoitus vain välttämättömiin resursseihin
 - Sopimuskäytännöt käytettäessä toimittajien omia etäyhteysteknologioita

Varautumishankkeen tuloksia

- Sovellus- ja käyttäjätietoisten "hiekkalaatikko" -ratkaisujen käyttöönotto
 - Toimintaan liittymättömien sovellusten estäminen mm. palomuurin avulla (ulko- ja sisäverkon suojavyöhykkeet)
 - Legacy -järjestelmien eristäminen muusta verkosta sovellustietoisuuden avulla
 - Ulkopuolisille tarjottavien palveluiden julkaisu ja esim. kumppaneiden yhteyksien rajoittaminen käyttäjä- ja sovellustietoisuuden avulla

Varautumishankkeen tuloksia

- Käyttövaltuushallinnan automatisointi IAM/IDM -ratkaisulla
- Mobiilipäätelaitteiden keskitetty hallintaratkaisu

Varautumishankkeen tuloksia

- Sairaalan toiminnan kannalta kriittisten tietojärjestelmien ja -palveluiden tunnistaminen ja luokittelu (+30 tietojärjestelmää tai palvelua)
 - Luokittelun perusteella palvelutasot 99,5 - 99,99%

**Potilastietojärjestelmät
Laboratoriojärjestelmät
Patologian järjestelmät
Tehohoidon järjestelmät
Veritilausjärjestelmät
Anestesiatietojärjestelmät
Leikkaustoiminnan ohjaus
Tiedonvälitysrajapinta
Kuvantamisen järjestelmät**

**Synnytyskertomus
Hoitajakutsujärjestelmät
Keskusvalvontajärjestelmät
Toiminnanohjausjärjestelmät
Turvallisuusjärjestelmät ja kiinteistöautomaatio
Viestintäratkaisut
Muut toiminnan kannalta kriittiset järjestelmät**

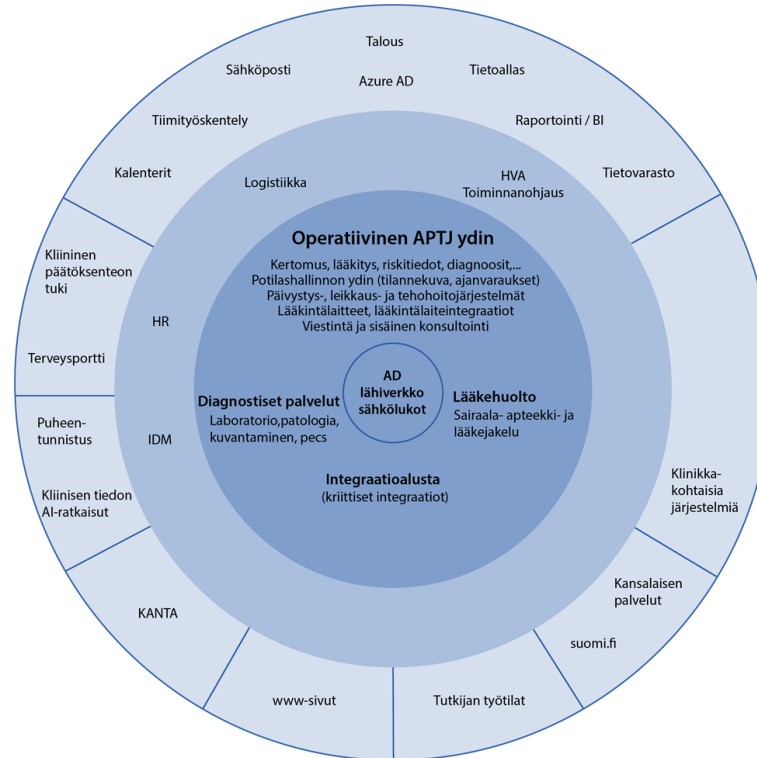
ICT-varautumishankkeen jälkeen hallinnollisesti (valmistuneita)

- Tietoturvan ja tietosuojaan hallintamallin kehitys
 - (noudattaa soveltuvin osin ISO 27001, ISO 27701, ISO 27005)
 - Tietoturva- ja tietosuojapolitiikka
 - Henkilörekisterin ja tietoturvan vastuut
 - Tietoturvan perustason määrittely
 - Sovellettava lainsäädäntö
- Periaatteita (prosessikuvauksia)
 - Tietoturva ja tietosuoja hankinnoissa ja projekteissa
 - Tietoturva ja tietosuojavaatimukset
 - Tietoturva- ja tietosuojariskienhallinta
 - Tietoturvapoikkeamien ja henkilötietojen tietoturvaloukkausten käsittely

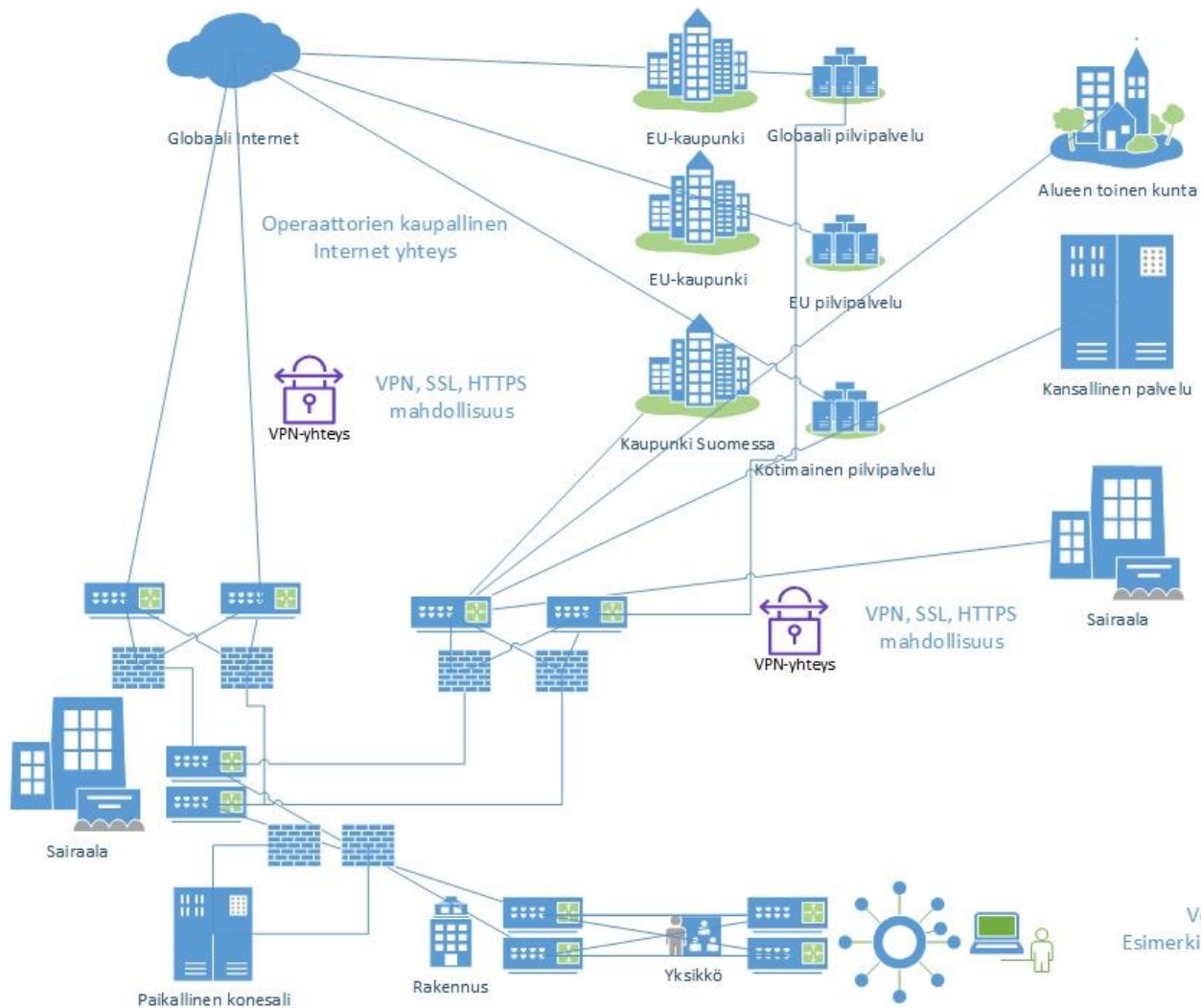
ICT-varautumishankkeen jälkeen teknisesti (työn alla, tulossa)

- **Microsoft ympäristön suojauksen jatkokehitys**
 - **Lisenssitason nosto, prosessikehitys, tekniset kyvykkyudet**
- Tietojen luokittelun ja suojauksen jatkokehitys
 - Sallitun käytön politiikka, tekniikka, koulutus, turvalliset työtilat
- Lokienhallinnan jatkokehitys ja laajennus
- SOC-palvelun laajennukset ja jatkokehitys
- Tietoturva-arvioinnit siirtyville järjestelmille
- Sovellustason ja API:en suojauksen kehittäminen
- Haavoittuvuuksien valvonnan kehitys
- Kovennusten jatkokehitys (palvelimet, työasemat)
- **Zero Trust arkkitehtuurin kokonaissuunnittelu ja toteutus (osin jo toteutettu)**
- Keskeisten palveluiden tietoturva-auditoinnit (toistuvasti)
- Tulevaisuudessa vanhentuvien käyttöjärjestelmä, tietokanta ja ohjelmistoversioiden päivitykset
- **Salatun liikenteen purku/analysointi korkean riskin liikenteen osalta**
- ICT-palveluiden hallintamallin jatkokehitys mm. jatkuvan riskien arvioinnin ja hallinnan osalta koko elinkaaren ajan ja muutoshallinnan kehitys
- **DDoS suojauksen jatkokehitys, arkkitehtuurimuutokset**

Esimerkki palveluiden sijoittelusta sipulimalliin



Lähde: (Akusti
Sote-
tietojärjestelmät
pilvipalveluina
soveltamisohje)



Pilvipalveluiden jatkuvuuden hallinta

- Skenaariotarkastelu
- Käyttötapaukset
- Palvelutuotannon mallit
- Arkkitehtuuri
- Riskit ja uhat

Erilaisia uhka skenaariota

- Skenaario 1: Verkkoyhteydet Suomeen ovat poikki
 - Skenaario 2: Sairaalan tietoliikenne on kokonaan poikki
 - Skenaario 3: Lähikonesali ei käytettävissä
 - Skenaario 4: Kansalliset palvelut pois käytöstä
-
- Lähde: Akusti Sote-tietojärjestelmät pilvipalveluina soveltamisohje

Erilaisia käyttötapauksia (esimerkkejä)

- Kansalaisten tiedottaminen (internet sivut)
- Kansalaisten asiointipalvelut
- Operatiivinen APTJ ydin
- Diagnostiikka (esim. PACS)
- Oheispalveluiden tuottamiseen käytettävät järjestelmät (esim. kanttiini tai pysäköintilaitos)

Erilaisia palvelutuotannon malleja (esimerkkejä)

- Globaali pilvipalvelu Internetin kautta käytettynä
- EU pilvipalvelu Internetin kautta käytettynä
- EU pilvipalvelu dedikoidulla tietoliikenneyhteydellä (esim. Express Route)
- Suomalainen pilvipalvelu Internetin kautta käytettynä
- Suomalainen (pilvi)palvelu dedikoidulla yhteydellä (esimerkiksi MPLS / musta kuitu / alueverkot)
- Oma tai ICT-palveluntuottajan konesali paikallisesti

Yleinen tiedotussivusto	Verkko yhteydet Suomeen ovat poikki	Sairaalan tietoliikenne on kokonaan poikki	Lähikonesali ei käytettävissä	Kansalliset palvelut pois käytöstä	Huomioita
Globaali pilvipalvelu Internetin kautta käytettynä	Tiedotus ei toimi, jos ei ole Suomalaista /omaa palvelua	Sivujen päivittäminen hankaloituu	Sivujen päivittäminen hankaloituu	Ei vaikutusta	
EU pilvipalvelu Internetin kautta käytettynä	Tiedotus ei toimi, jos ei ole Suomalaista /omaa palvelua	Sivujen päivittäminen hankaloituu	Sivujen päivittäminen hankaloituu	Ei vaikutusta	
EU pilvipalvelu dedikoidulla tietoliikenneyhteydellä	Tiedotus ei toimi, jos ei ole Suomalaista /omaa palvelua	Sivujen päivittäminen hankaloituu	Sivujen päivittäminen hankaloituu	Ei vaikutusta	
Suomalainen pilvipalvelu Internetin kautta käytettynä	Ei vaikutusta kotimaassa (jos internet toimii kansalaisilla)	Sivujen päivittäminen hankaloituu	Sivujen päivittäminen hankaloituu	Ei vaikutusta	
Suomalainen (pilvi)palvelu dedikoidulla yhteydellä	Ei vaikutusta kotimaassa (jos internet toimii kansalaisilla)	Sivujen päivittäminen hankaloituu	Sivujen päivittäminen hankaloituu	Ei vaikutusta	
					Todennäköisesti huono idea sijoittaa ainakaan kokonaan omaan saliin palvelunestohyökkäyksen riskin vuoksi (voi vaikuttaa muihin palveluihin / kaistaan). Kyetäänkö kapasiteettia lisäämään esimerkiksi pandemian tms. yhteydessä?
Oma tai ICT-palveluntuottajan konesali	Globaali tiedottaminen ei toimi	Sivujen päivittäminen hankaloituu	Sivujen päivittäminen hankaloituu	Ei vaikutusta	
PACS					
Globaali pilvipalvelu Internetin kautta käytettynä	Kuvat eivät ole käytettävissä	Kuvat eivät ole käytettävissä	Kuvat eivät ole käytettävissä (työasemien laamaantuminen AD/DNS yms.)	Kansallisten palveluiden tiedot ja kirjaukset ei	Käytännössä hyvin hankala toteuttaa tietosuojan vuoksi
EU pilvipalvelu Internetin kautta käytettynä	Kuvat eivät ole käytettävissä	Kuvat eivät ole käytettävissä	Kuvat eivät ole käytettävissä (työasemien laamaantuminen AD/DNS yms.)	Kansallisten palveluiden tiedot ja kirjaukset ei	
EU pilvipalvelu dedikoidulla tietoliikenneyhteydellä	Riippuu katkeako myös dedikoitu yhteys	Riippuu katkeako myös dedikoitu yhteys	Kuvat eivät ole käytettävissä (työasemien laamaantuminen AD/DNS yms.)	Kansallisten palveluiden tiedot ja kirjaukset ei	
Suomalainen pilvipalvelu Internetin kautta käytettynä	Ei vaikutusta jos internet toimii suomessa	Kuvat eivät ole käytettävissä	Kuvat eivät ole käytettävissä (työasemien laamaantuminen AD/DNS yms.)	Kansallisten palveluiden tiedot ja kirjaukset ei	
Suomalainen (pilvi)palvelu dedikoidulla yhteydellä	Ei vaikutusta	Riippuu katkeako myös dedikoitu yhteys	Kuvat eivät ole käytettävissä (työasemien laamaantuminen AD/DNS yms.)	Kansallisten palveluiden tiedot ja kirjaukset ei	
Oma tai ICT-palveluntuottajan konesali	Ei vaikutusta	Ei vaikutusta	Kuvat eivät ole käytettävissä	Kansallisten palveluiden tiedot ja kirjaukset ei	
Kassajärjestelmä (Kanttiini, parkkialue)					
Globaali pilvipalvelu Internetin kautta käytettynä	Pysäköintiä ja pullia ei voi maksaa	Pysäköintiä ja pullia ei voi maksaa	Pysäköintiä ja pullia ei voi maksaa (jos työasemat eivät toimi)	n/a	Voi olla haastava maksamiseen liittyvän regulaation vuoksi
EU pilvipalvelu Internetin kautta käytettynä	Pysäköintiä ja pullia ei voi maksaa	Pysäköintiä ja pullia ei voi maksaa	Pysäköintiä ja pullia ei voi maksaa (jos työasemat eivät toimi)	n/a	
EU pilvipalvelu dedikoidulla tietoliikenneyhteydellä	Riippuu katkeako myös dedikoitu yhteys (ja toimiiko korttien varmennus palveluntarjoajalle)	Riippuu katkeako myös dedikoitu yhteys ja toimiiko korttien varmennus palveluntarjoajalle	Pysäköintiä ja pullia ei voi maksaa (jos työasemat eivät toimi)	n/a	
Suomalainen pilvipalvelu Internetin kautta käytettynä	Ei vaikutusta jos internet toimii suomessa (ja toimiiko korttien varmennus palveluntarjoajalle)	Pysäköintiä ja pullia ei voi maksaa	Pysäköintiä ja pullia ei voi maksaa (jos työasemat eivät toimi)	n/a	
Suomalainen (pilvi)palvelu dedikoidulla yhteydellä	Ei vaikutusta jos korttien varmennus toimii palveluntarjoajalle	Riippuu katkeako myös dedikoitu yhteys ja jos korttien varmennus toimii	Pysäköintiä ja pullia ei voi maksaa (jos työasemat eivät toimi)	n/a	
Oma tai ICT-palveluntuottajan konesali	Ei vaikutusta jos korttien varmennus toimii palveluntarjoajalle	Pysäköintiä ja pullia ei voi maksaa (jos yhteys varmennukseen ei toimi)	Pysäköintiä ja pullia ei voi maksaa	n/a	

Arkkitehtuuri

- On keskeistä ymmärtää:
 - **Käyttötapaukset**
 - Mihin käytetään, kuka käyttää?
 - **Katkon vaikutukset**
 - Mitä operatiivista toimintaa ei voida toteuttaa ilman ja mitä se tarkoittaa esim. potilaiden hoidon kannalta
 - **Riippuvuudet** muista järjestelmistä, infrasta ja tietoliikenneyhteyksistä

Jatkuvuuden hallinta on kokonaisriskien hallintaa

- Riski = uhka * haavoittuvuus * vaikutus
- Uhka = Esimerkiksi rikollisjengin kyvykkyys ja mahdollisuus tehdä tietomurtoja
- Haavoittuvuus = esimerkiksi aukko ohjelmistossa tai prosessissa, jota on mahdollista hyödyntää
- Vaikutus = vaikutus toiminnalle, esimerkiksi potilaiden hoidolle
- **Riskienhallintakeinoina on esimerkiksi palvelutuotantomallin valinta**

Kiitos!