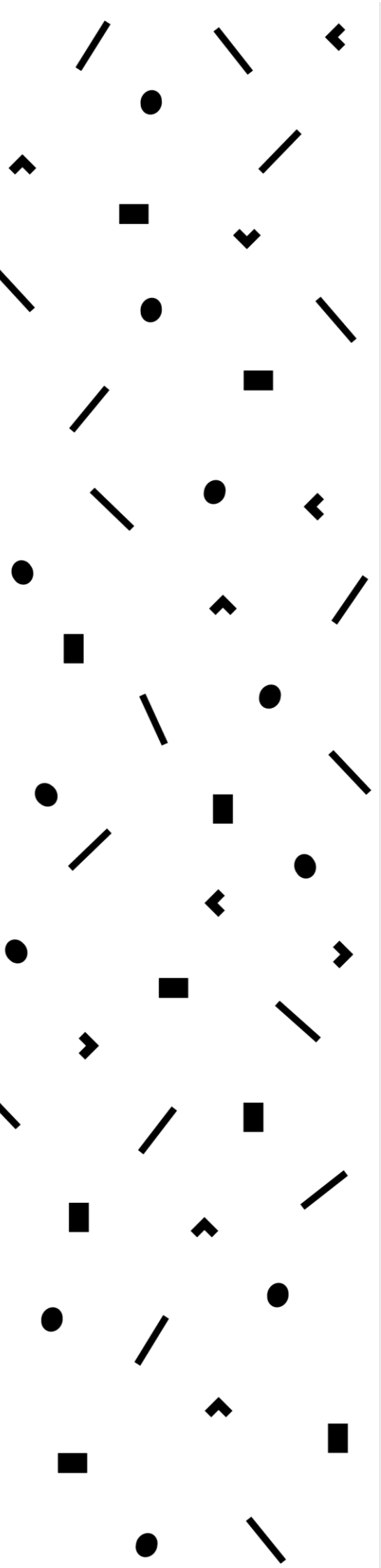


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Lääkintälaitteen turvallinen liittäminen sairaalan tietoverkkoon

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka, Insinööri (AMK)
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2017
Jyrki Vartiainen

Lahden ammattikorkeakoulu
Tietotekniikka, Insinööri (AMK)

VARTIAINEN, JYRKI:

Lääkintälaitteen liittäminen turvallisesti sairaalan tietoverkkoon

Tietoliikennetekniikan opinnäytetyö, 86 sivua, 7 liitesivua

Kevät 2017

TIIVISTELMÄ

Sairaalassa lääkintälaitteilla diagnosoidaan, tarkkaillaan potilasta, hoidetaan potilaan sairautta tai vammaa. Potilaasta saatava tieto halutaan saada sähköisesti sairaalan tietojärjestelmiin. Sairaalassa kaikki potilaan hoitoon liittyvät asiakirjat ovat osa sähköistä sairaskertomusta. Lääkintälaitteiden sairaalan verkkoon liittäminen tuo hyötyjen lisäksi tietoturvariskejä ja riskien minimoimiseksi opinnäytetyössä etsittiin ratkaisuja lääkintälaitteen tietoturvan parantamiseksi.

Opinnäytetyössä tutkittiin lääkintälaitteisiin vaikuttavaa lainsäädäntöä ja direktiivejä. Lääkintälaitteita verkotettaessa on huomioitava IEC 60601-1- ja IEC 60601-1-1 -standardien vaatimukset koskien lääkintälaitteiden sähköturvallisuutta. Lääkintälaitteiden tietoturvassa on huomioitava luottamuksellisuus, eheys ja saatavuus. Lääkintälaitteen tuottama tieto on oltava käytettävissä oikeaan aikaan, muuttumattomana vain niillä henkilöillä, joilla on oikeus tietoon.

Verkkoon liitetyn lääkintälaitteen tietoturvaa voidaan parantaa koventamalla lääkintälaitetta laitteistopohjaisesti ja ohjelmistopohjaisesti. Koventamisella laitteiston asetuksia määritellään tietoturvallisemmaksi. Lääkintälaitteen tietoturvaa voidaan parantaa ilman laitteistoon kohdistuvia muutoksia verkon segmentoinnilla, palomuurein ja verkkoliikenteen analysoinnilla. Lääkintälaitteisiin valmistajan salliessa voidaan asentaa tietoturvaohjelmisto, joka suojaa haittaohjelmilta, ja tietoturvapäivityksiä, jotka korjaavat haittaohjelmien hyödyntämiä tietoturva-aukkoja.

Tulevaisuudessa kaikki lääkintälaitteet tullaan liittämään verkkoon, koska kaikki potilaan diagnoosissa, tarkkailussa ja hoidossa tuotettu informaatio halutaan hyödynnettäväksi potilaan hoidossa. Lääkintälaitteiden käytön turvaaminen tulee olemaan kriittinen kehityskohde sairaaloiden tietoturva-asiantuntijoille.

Asiasanat: lääkintälaite, Standardi IEC 60601-1, tietoturva

Lahti University of Applied Sciences
Degree Programme in Information Technology

VARTIAINEN, JYRKI: Connecting a medical device securely to a hospital network

Bachelor's Thesis in telecommunications, 86 pages, 7 pages of appendices

Spring 2017

ABSTRACT

Medical devices are used in diagnostics, monitoring and treating a patient's illness or injury in hospitals. It is preferable to have the patient information in electronic form in hospital information systems. In a hospital all documents on the treatment of a patient are part of a computerized medical record. Connecting medical devices to a hospital network has benefits but also information security risks, and to minimize these risks this thesis reviewed for solutions for improving information security of a medical device.

The thesis reviewed the legislation and the EU directives affecting medical devices. The requirements of IEC 60601-1- and IEC 60601-1-1 -standards concerning the electrical safety of medical devices have to be observed when connecting medical devices to a network. The information security of medical devices has to take into account aspects of confidentiality, integrity and availability. The information produced by a medical device must be available unaltered to the approved personnel at the correct time.

The information security of a medical device connected to a network can be enhanced by hardening the device either through hardware or software. When hardened, the settings of a device are adjusted towards enhanced information security. The security of a medical device can be improved without making changes to the device itself, via network segmentation, firewalls and network data analysis. If the medical device's manufacturer permits it, it is possible to install security software on the device, to protect against malicious programs and security patches to fix security flaws with a potential for exploitation.

In future all medical devices will be connected to a network to take advantage of all information produced in patient diagnostics, observation and treatment for a patient's care. Securing the usage of medical devices will be a crucial aspect for development for information security experts at hospitals.

Keywords: medical device, Standard IEC 60606-1-1, information security

SISÄLLYS

1 JOHDANTO

Opinnäytetyön tavoite on parantaa sairaalan verkkoon liitettävien lääkintälaitteiden tietoturvaa. Opinnäytetyö tehtiin sairaalaan lääkintätekniikalle, joka vastaa sairaalan lääkintälaitteiden elinkaaresta. Opinnäytetyötä ei ole rajattu erityisesti mihinkään sairaalaan.

Lääkintälaitteilla diagnosoidaan, tarkkaillaan potilasta, hoidetaan potilaan sairautta tai vammaa. Elektroniset lääkintälaitteet sisältävät käytännössä aina tietokoneen. Tietokone voi olla ohjelmoitava logiikkapiiri tai sulautettu tietokone. Lääkintälaitetta ei välttämättä osata tunnistaa tietokoneeksi.

Opinnäytetyön teoriaosuudessa tutustutaan lääkintälaitteisiin vaikuttavaan lainsäädäntöön, direktiiveihin ja standardeihin. Teoriaosuudessa tutustutaan tietoturvan perusteisiin. Niiden pohjalta lähdettään selvittämään käytäntöjä, joilla parannetaan verkkoon liitettävien lääkintälaitteiden tietoturvaa.

Opinnäytetyössä selvitetään lääkintälaitteiden verkkoon liitettävyyttä ja sitä mitä lääkintälaitteen hankintaprosessissa pitää ottaa huomioon lääkintälaitteiden tietoturvan parantamiseksi. Verkkoon liitettäville lääkintälaitteille luodaan toimintamallit, joiden soveltuvuus testataan sairaalaan hankittavilla lääkintälaitteilla. Toimintamallien pohjaksi otetaan sairaalan vakioituun työasemaan kohdistuvat käytännöt ja selvitetään, soveltuvatko ne sellaisenaan lääkintälaitteiden tietoturvan parantamiseen.

2 LÄÄKINTÄLAITE HOITOALUEELLA

2.1 Lääkintälaitedirektiivi ja laki terveydenhuollon laitteista

Lääkintälaitteista EU-tasolla määrätään lääkintälaitedirektiivillä 93/42/ETY. Lääkintälaitedirektiivi (MD-direktiivi) koskee lääkinnällistä laitetta, kaikkia laitteeseen liittyviä tarvikkeita ja laitteiden käyttöön tarvittavia ohjelmistoja, kun laitetta käytetään valmistajan tarkoittamalla tavalla ihmisen

- sairauksien diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen
- vammojen tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin
- anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun
- hedelmöityksen säätelyyn.

Direktiivissä määritellään yleisenä vaatimuksena, että laitteiden suunnittelussa ja valmistuksessa on varmistuttava, ettei laitetta käytettäessä suunnitelluissa olosuhteissa tarkoituksen mukaisesti vaaranneta potilaan tai muun henkilön terveyttä tai turvallisuutta. Käyttäjien tai muiden henkilöiden turvallisuutta tai terveyttä ei vaaranneta laitteiden käyttöön liittyvissä riskeissä, jos riskit ovat hyväksyttäviä potilaalle saatuun etuun nähden. Lääkintälaitevalmistajan velvollisuus on poistaa tai minimoida riskit potilaalle tai laitteen käyttäjälle. Tarvittaessa on velvoite toteuttaa tarvittavat suojelutoimenpiteet ja hälytysmekanismit riskeille, joita ei voida poistaa kokonaan. Laitteen käyttäjiä on informoitava laitteeseen tai sen käyttöön liittyvistä riskeistä, joita ei ole voitu poistaa kokonaan. Laitteen käyttäjille on ilmoitettava käyttöohjeessa, jos ne johtuvat suojelutoimenpiteiden riittämättömyydestä. (Lääkintälaitedirektiivi 93/42/ETY)

KUVIO 1. CE-merkki (IEC 60601-1, 2005)

Lääkintälaitteessa CE-merkin (KUVIO 1) käyttö on pakollista EU-alueella. Valmistaja osoittaa CE-merkillä lääkintälaitteen täyttävän sitä koskevat olennaiset Lääkintälaitedirektiivin vaatimukset. Lääkintälaitteen valmistaja antaa lääkintälaitteesta vaatimuksenmukaisuusvakuutuksen, jossa kerrotaan, mitkä vaatimuksenmukaisuusmääräykset laite täyttää. Vaatimuksenmukaisuusvakuutuksessa ilmoitetaan ilmoitetun laitoksen nimi ja numero, mikäli vaatimuksenmukaisuuteen liittyvässä arvioinnissa on käytetty ulkopuolista tarkastuslaitosta. Lääkintälaitteen CE-merkissä on ilmoitettu tarvittaessa ilmoitetun laitoksen (notified body) numero. (Laki terveydenhuollon laitteista ja tarvikkeista 629/2010 § 9, 13; Lääkintälaitedirektiivi 93/42/ETY.)

Terveydenhuollon laitteista ja tarvikkeista määrätään Laissa terveyden huollon laitteista ja tarvikkeista 629/2010. Lailla pannaan käytäntöön lääkintälaitedirektiivi 93/42/ETY kansallisella tasolla. Laissa viitataan aktiivisiin implantoitaviin lääkinnällisiin laitteisiin ja laboratoriodiagnostiikassa käytettäviin laitteisiin. Laki määrää toiminnanharjoittajan noudattamaan valmistajan ohjeita koskien laitteen kuljetusta säilytystä, asennusta ja huoltoa. Laki määrää myös toiminnanharjoittajan tekemään ilmoituksen vaaratilanteesta laitteen valmistajalle tai valtuutetulle edustajalle tietoonsa tulleista vaaratilanteista, kun on epäilty tai on todettu vaaratilanteen johtuneen laitteessa olevasta viasta tai puutteellisuudesta.

Lääkintälaitteita saa käyttää vain ammattimainen käyttäjä, joka on koulutettu käyttämään kyseistä laitetta turvallisesti siinä käyttötarkoituksessa, johon laite on suunniteltu. Käyttäjältä vaaditaan koulutuksen lisäksi tarvittava kokemus lääkintälaitteen käyttöön. Käyttäjän on varmistuttava, että laitetta ylläpidetään ja huolletaan valmistajan

oheistuksen mukaisesti ja henkilö joka asentaa, korjaa tai huoltaa laitetta, omaa tarvittavan ammattitaidon ja asiantuntemuksen. Mikäli laitteessa on havaittu vaaratilanne, joka olisi voinut johtaa tai johti potilaan, käyttäjän tai muun henkilön vaaraan, johtuen terveydenhuollon laitteen ominaisuuksista, suorituskyvyn poikkeamasta tai häiriöstä, riittämättömästä merkinnästä, puutteellisuudesta tai virheellisestä käyttöohjeesta tai virheellisestä käytöstä, tulee tilanteesta laatia vaaratilanneilmoitus ja poistaa laite välittömästi käytöstä. (Laki terveydenhuollon laitteista ja tarvikkeista 629/2010 , § 1, § 17, § 24 - 26.)

2.2 Standardit 60601-1 ja 60601-1-1

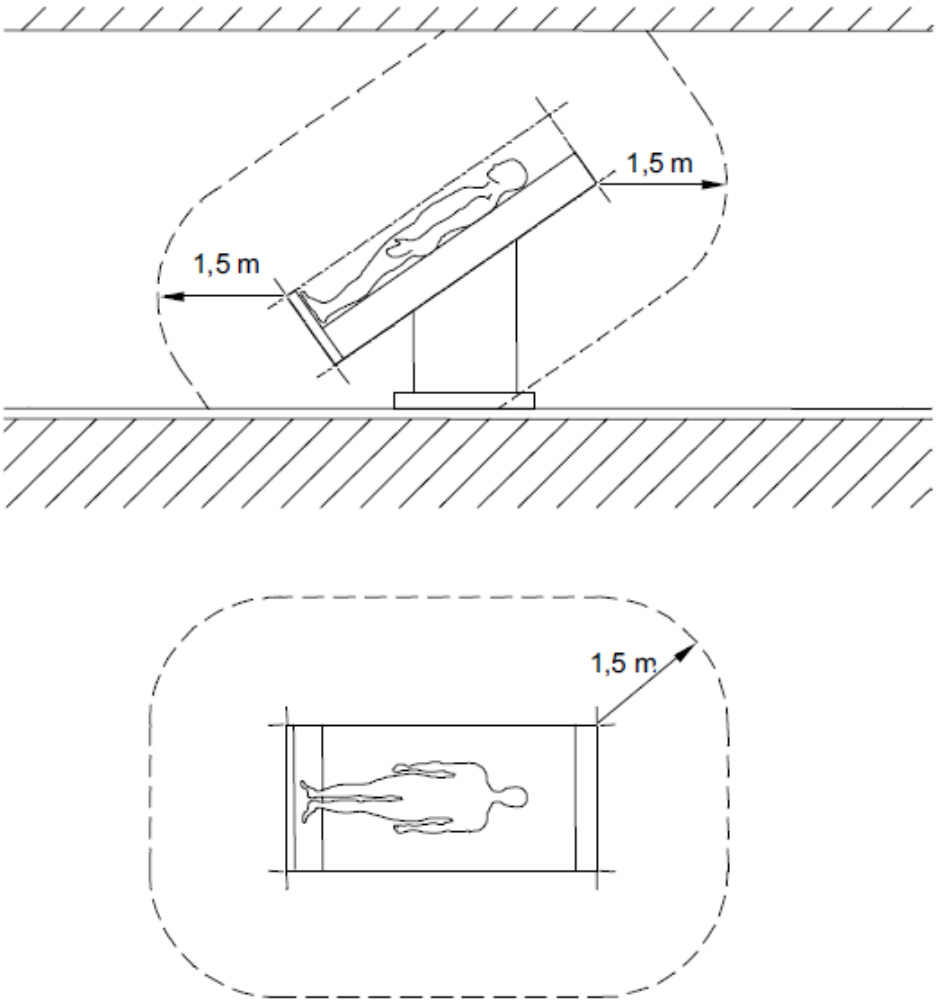
Sähkökäyttöinen lääkintälaite on laite, jonka laitteen valmistaja on määritellyt lääkintälaitteeksi. Laitteessa on liityntäosa, joka siirtää energiaa potilaaseen tai potilaasta tai ilmaisee tällaisen energian siirtymistä. Laite on vain yhdellä liitynnällä yhteydessä sähköverkkoon. Sähkökäyttöisten lääkintälaitteiden yleiset turvallisuusvaatimukset määritellään IEC-standardissa 60601-1, jossa määritellään vaatimuksia suojamaadoittamisesta, liityntäosien erottamisesta ja sallituista vuotovirroista ja miten vuotovirtoja mitataan erinäisissä vikatilanteissa. IEC-standardi 60601-1-1 täydentää standardia 60601-1 koskien lääkintälaitejärjestelmiä.

Standardeissa määriteltyjen sähköturvallisuuteen liittyvien vaatimuksien tarkoituksena on vähentää riskiä, ettei laitteen käyttäjälle tai potilaalle aiheutuisi kohtuutonta riskiä vikatilanteessa. Laitteen täyttäessä vaadittavat standardit yleisesti katsotaan laitteen täyttävän lain terveydenhuollon laitteista ja tarvikkeista. (IEC 60601-1-1, 2000; IEC 60601-1, 2005.)

2.3 Lääkintätila ja hoitoalue

Lääkintätilassa potilasta tutkitaan, valvotaan tai hoidetaan sähkökäyttöisellä lääkintälaitteella. Hoitoalueeksi kutsutaan lääkintätilassa aluetta, jolla on tahattomasti tai tarkoituksella mahdollista syntyä fyysinen

yhteys potilaan ja lääkintälaitteen välille tai yhteys voi muodostua potilaan ja lääkintälaitetta koskettavan henkilön välille. Potilaan sijainnin ollessa ennalta tiedossa lääkintätilassa käytetään 1,5 metrin turvaetäisyyttä (KUVIO 2) kaikkiin suuntiin potilaasta, mikäli potilaan sijaintia ei voi ennalta määritellä on tilassa otettava huomioon kaikki mahdolliset potilaan sijainnit. (IEC 60601-1, 2005; SFS6000-7-710, 2007.)

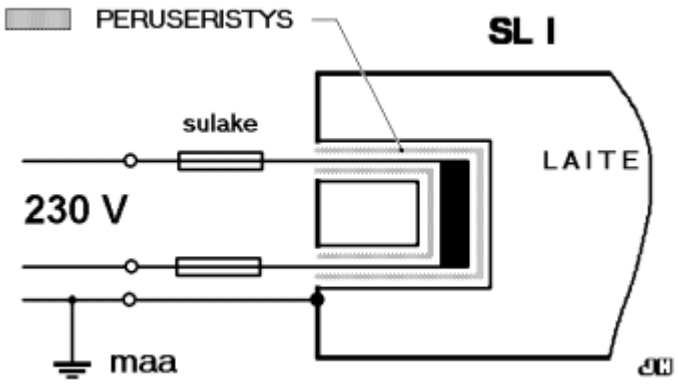


KUVIO 2. Hoitoalue (IEC 60601-1, 2005)

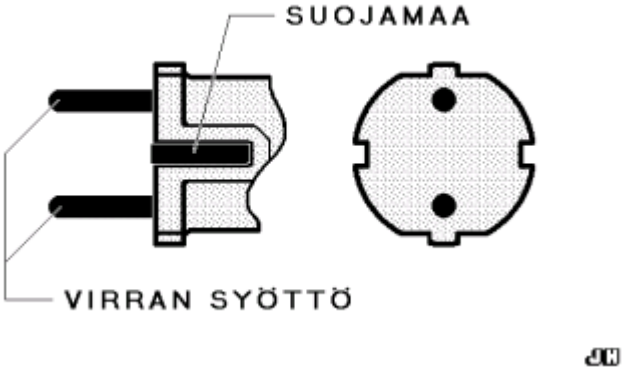
3 LÄÄKINTÄLAITTEEN SÄHKÖTURVALLISUUS

3.1 Lääkintälaitteiden luokittelu

Laissa terveydenhuollon laitteista lääkintälaitteet luokitellaan neljään tuoteluokkaan, jotka ovat I, II a, II b ja III. Standardi 60601-1 määrittää lääkintälaitteiksi luokat I ja II, mitkä perustuvat siihen, miten lääkintälaitteen suojaus sähköiskua vastaan on toteutettu. Tuoteluokkia ja standardin 60601-1 luokkia ei pidä sekoittaa keskenään. Suojausluokan I laitteissa (KUVIO 3) kaikki laitteen kosketeltavat osat on kytketty sähköverkonsuojajohtimeen eli suojamaahan ja jännitteelliset osat on erotettu. Nämä kaksi mekanismia suojaavat sähköiskulta. Suojausluokan I laitteen tunnistaa liitäntäjohdon pistotulpasta, jossa on suojamaa sivuilla suojaliuskoina (KUVIO 4). (IEC 60601-1, 2005.)

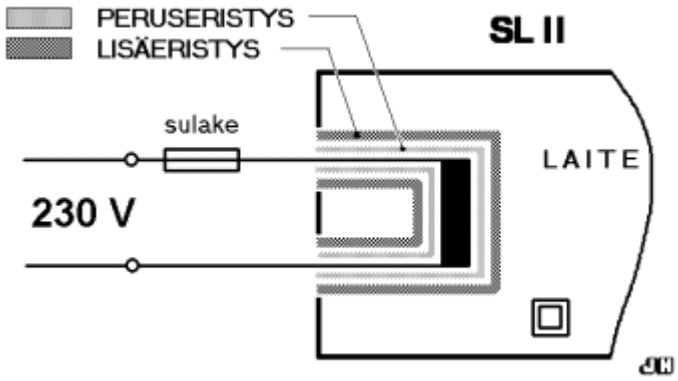


KUVIO 3. Suojausluokan I laite (Honkanen 2002, 4)

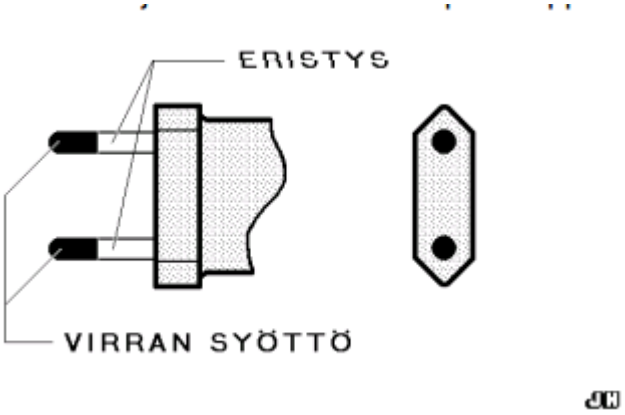


KUVIO 4. Suojausluokan I laitteen pistotulppa (Honkanen 2002, 5)

Suojausluokan II laitteissa (KUVIO 5) ei ole suojamaata vaan niiden sähköturvallisuus perustuu peruseristyksen lisäksi lisäeristykseen. Suojausluokan II laitteen kotelo on joko eristysainetta, joka ei johda sähköä tai metallikotelo. Eristysainekoteloisen laitteen suojaus perustuu laitteen koteloon, joka peittää kaikki laitteen johtavat osat. Metallikoteloisen laitteen sähköiskun suojaus perustuu kaksoiseristykseen joka eristää laitteen verkko-osan täysin kotelosta. Suojausluokan II laitteeseen ei voi muodostua maavuotovirtaa, koska laitteessa ei ole suojamaajohdinta. Suojausluokan II laitteen tunnistaa liitäntäjohdon pistotulpasta (KUVIO 6) ja Suojausluokan II laitteen merkistä (KUVIO 7). (Laki terveydenhuollon laitteista ja tarvikkeista 629/2010, § 7; IEC 60601-1, 2005.)



KUVIO 5. Suojausluokan II laite (Honkanen 2002, 4)

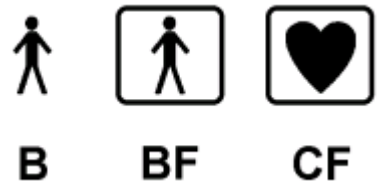


KUVIO 6. Suojausluokan II laitteen pistotulppa (Honkanen 2002, 5)

KUVIO 7. II luokan laitteen merkki (Honkanen 2002, 5)

3.2 Lääkintälaitteen potilasliitynnät

Lääkintälaitteille suoritetaan ennen käyttöönottoa, määräaikaishuollon tai vian korjauksen yhteydessä sähköturvallisuusmittaus, jolla varmistetaan lääkintälaiteen täyttävän standardin 60601-1 vaatimukset sähköturvallisuuden osalta. Lääkintälaitteen potilasliitynnät on määritetty kolmeen eri tyyppiin. B-, BF- ja CF-tyypin liitännät eroavat toisistaan käyttötarkoituksen, suojauksen ja vuotovirtojen raja-arvojen suhteen. Potilasliityntöjen läheisyydessä on Kuvion 8 mukainen symboli. Sähkökäyttöisen lääkintälaitteen potilasliityntään ei ole mahdollista kytkeä laitteen muihin liityntöihin tulevia liittimiä. Kytkeminen saattaisi aiheuttaa vaaraa potilaalle mahdollisesti suurentuneina vuotovirtoina. (IEC 60601-1, 2005.)



KUVIO 8. Potilasliityntäsymbolit (Honkanen 2002, 6)

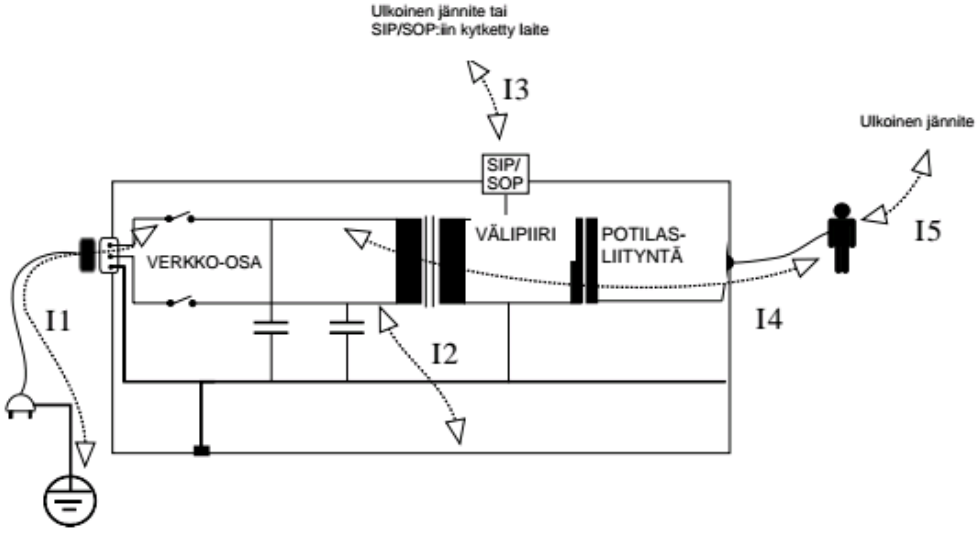
B-tyypin potilasliityntää käytetään käytännössä vain ihon pinnalle tulevissa liitynnöissä. B-tyypin potilasliityntä voidaan käyttää kehon sisäisesti, jos liitynnän toimintaa ei käytetä sydämen läheisyydessä. BF-tyypin potilasliityntää käytetään useimmiten ihon pinnalla, mutta liityntää voidaan käyttää muuten samoilla periaatteilla kuin B-tyypin liityntää. BF-tyypin liityntä eroaa B-tyypin liitynnästä, että BF-tyypin liityntä on täysin eristetty laitteen muista osista. Eristettyä liityntää kutsutaan kelluvaksi liitynnäksi. Tyyppisymbolissa neliö kuvastaa liitynnän eristystä.

CF-tyypin potilasliityntä on kelluva kuten BF-tyypin liityntä. CF-tyypin liityntä on kaikkein parhaiten eristetty ja liityntä soveltuu sydämen läheiseen toimintaan. CF-tyypin liityntää voidaankin käyttää kaikkiin lääkintälaitteen toiminnallisuuksiin. Potilasliitynnät voivat olla defibriloinnin kestäviä, jolla varmistetaan potilasta voitavan defibriloida turvallisesti potilas kytkettynä lääkintälaitteeseen, ilman potilaan tai lääkintälaiteen vaarantumista. Kuvion 9 mukainen symbooli on aina defibrilloinnin kestävän liitännän läheisyydessä. (IEC 60601-1, 2005.)

KUVIO 9. Difibrilomisen kestävän potilasliitynnän tunniste (Honkanen 2002, 6)

3.3 Turvallisuusmittauksen keskeisimmät termit

Sähkökäyttöisissä lääkintälaitteissa muodostuu ei-toiminnallisia vuotovirtoja, jotka hakeutuvat ylemmästä potentiaalista alempaan potentiaaliin eristysten yli. Mahdollisia kulkureittejä ovat laitteen runko, potilas, käyttäjä, suojamaatien muu osa tai huonosti eristävä materiaali. Huollon suorittamat vuotovirtamittaukset ovat tärkeä osa lääkintälaitteen turvallisuuden varmistamisprosessia. Mittauksilla voidaan seurata laitteen sähköturvallisuuden tasoa. Käyttöönottotarkistuksessa saadaan laitteelle lähtötasot erilaisille vuotovirroille, joiden kasvaminen laitteen elinkaaren aikana saattaa indikoida vikaa eristyksessä, mikä ilmenee ajan kanssa, jolloin vuotovirrat saattavat kasvaa yli määriteltyjen raja-arvojen. Sähköturvallisuusmittaukset suoritetaan standardin 60601-1 mukaisesti. Mittaukset suoritetaan valmistajan oheistuksen mukaisesti jäljitettävästi kalibroidulla mittalaitteella joka soveltuu mittaukseen. Mittaustulokset tallennetaan seurantajärjestelmään. (Pöyhönen & Kylmälä 2004, 80 - 81; IEC 60601-1, 2005; Laki terveydenhuollon laitteista ja tarvikkeista 629/2010, § 26.)



KUVIO 10. Lääkintälaitteessa syntyviä vuotovirtareittejä (Pöyhönen & Kylmälä 2004, 81)

Standardi 60601-1 määrittää kolme vuotovirtaa, joita ovat maa-, kosketus- ja potilasvuotovirta. Lääkintälaitteeseen muodostuvat vuotovirrat ja niiden

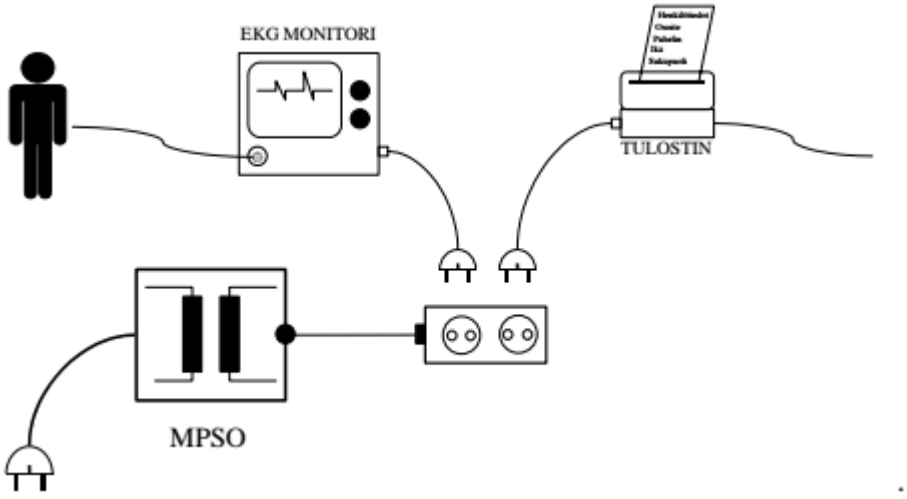
kulkureitit ovat seuraavat (KUVIO 10): Virta I1 kuvaa maavuotovirtaa, joka hakeutuu laitteen verkko-osasta laitteen maapotentiaaliin eli laitteen suojajohtimeen normaalissa tilanteessa. Maavuotovirran arvoa rajoitetaan, koska suojajohtimen pettäessä on riskinä virran kulkeutuminen potilaan tai käyttäjän kautta maadoitukseen. Virta I2 kuvaa kosketusvuotovirtaa joka hakeutuu laitteen jännitteellisistä osista koteloon tai kotelon osasta ulkoisen yhteyden kautta maapotentiaaliin. Kosketusvuotovirta saattaa kulkeutua helposti laitteen koteloon koskettavan potilaan tai käyttäjän kautta maapotentiaaliin. Laitteen kosketeltavat johtavat osat tästä syystä ovat yleensä maadoitettuja. Virta I4 ja I5 kuvaavat potilasvuotovirtoja, jotka hakeutuvat potilaan kautta maapotentiaaliin. Virran I4 tapauksessa laite vuotaa potilasvuotovirtaa laitteen potilasliitynnän kautta maapotentiaaliin. Virran lähteen ollessa ulkopuolinen jännite virta I5 kulkeutuu potilaan tai laitteen kautta maapotentiaaliin. Virran I3 tapauksessa virranlähteenä on lääkintälaitteeseen liitetty tietokone, jonka virtalähde ei täytä standardin 60601-1 vaatimuksia. Ulkopuolelta tuleva vuotovirta kasvattaa maa-, kosketus- ja potilasvuotovirtoja.

Lääkintälaitteessa potilasliitynnät antavat potilaalle standardissa 60601-1 vaatimusten mukaan potilaalle suojan sähköiskua vastaan. Sallitut potilasvuotovirtojen raja-arvot riippuvat lääkintälaitteen potilasliityntöjen tyypin mukaan. CF-tyypin potilasliitynnällä varustetun lääkintälaitteen potilasvuotovirtojen raja-arvot ovat tiukimmat, koska CF-tyypin potilasliityntää on sallittu käyttää sydämen läheisissä toiminnoissa. B- ja BF-tyypin potilasliitynnöistä mittatavat suurimmat sallitut potilasvuotovirrat ovat 0,1 mA normaalissa tilanteessa ja CF-tyypin potilasliitynnöillä suurin sallittu potilasvuotovirta on 0,01 mA normaalissa tilanteessa. Standardin 60601-1 vuotovirtojen rajoittamisella on tarkoitus suojata potilasta virran vahingoittavalta vaikutukselta. (Pöyhönen & Kylmälä 2004, 80 - 81; IEC 60601-1, 2005.)

3.4 Lääkintälaitejärjestelmät

Lääkintälaitejärjestelmä on käsitteenä hyvin laaja ja selkeää rajanvetoa ei ole helppo tehdä siitä, millainen laitteisto kokonaisuudessaan muodostaa lääkintälaitejärjestelmän. Standardia 60601-1 on laajennettu koskemaan lääkintälaitejärjestelmiä standardilla 60601-1-1, joka määrittelee lääkintälaitejärjestelmälle seuraavat kriteerit, joista jonkun on toteuduttava:

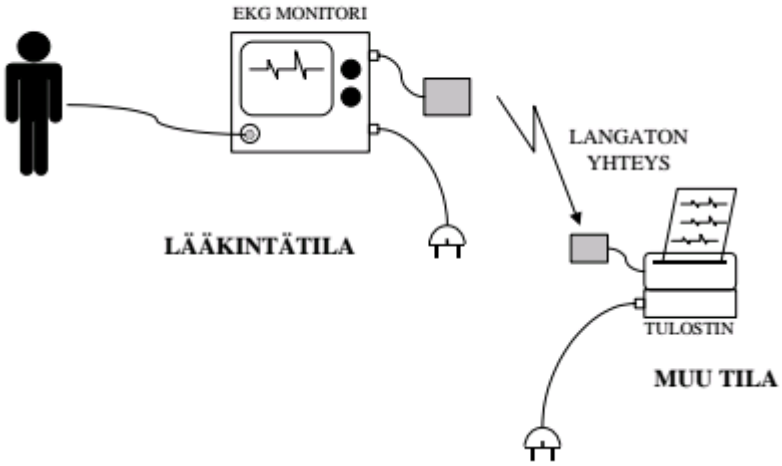
- sähkökäyttöinen lääkintälaitejärjestelmä
- moninapainen siirrettävä pistorasiaryhmä (MSO)
- toiminnallinen yhteys.



KUVIO 11. Lääkintälaitejärjestelmä moniosaisella siirrettävällä sähköpistokeryhmällä (Pöyhönen & Kylmälä 2004, 32)

Sähkökäyttöinen lääkintälaitejärjestelmä (KUVIO 11) muodostuu kahdesta tai useammasta laitteesta, joista vähintään yksi on sähkökäyttöinen lääkintälaite ja laitteet on yhdistetty toisiinsa toiminnallisella yhteydellä tai moninapaisella siirrettävällä pistorasiaryhmällä. Toiminnallinen yhteys (KUVIO 12) toteutuu, kun lääkintälaitejärjestelmän lääkintälaitteen ja muun laitteen tai toisen lääkintälaitteen välillä siirretään signaali, tieto, teho tai muu materiaali sähköisellä tai muulla yhteydellä. Galvaanisen yhteyden

lisäksi kelpaa langaton yhteys muuhun laitteeseen. Toiminnallinen yhteys ei vaikuta lääkintälaitteen tai lääkintälaitejärjestelmän sähköturvallisuuteen, ellei yhteys ole galvaaninen tai muuten sähköä johtava.

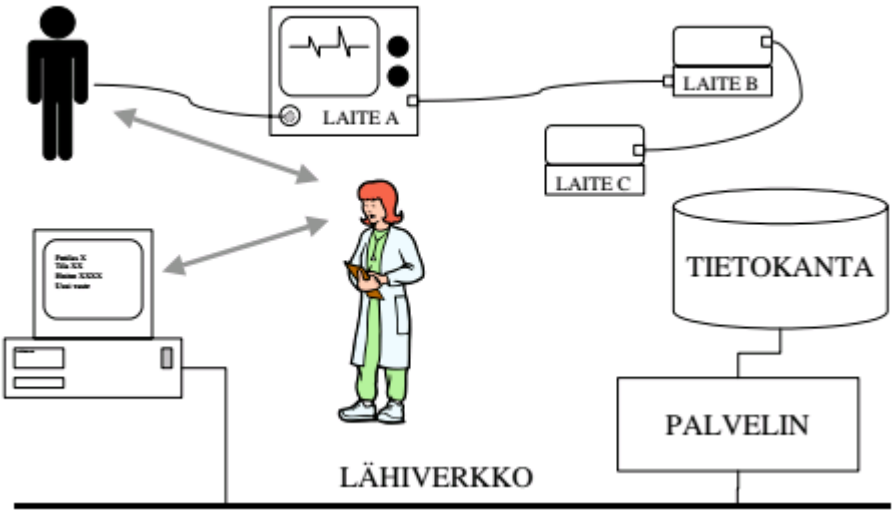


KUVIO 12. Lääkintälaitejärjestelmä toiminnallisella yhteydellä (Pöyhönen & Kylmälä 2004, 32)

Lääkintälaitejärjestelmän yksittäisiä lääkintälaitteita koskevat standardin 60601-1 sähköturvallisuusvaatimukset. Lääkintälaitejärjestelmän sähköturvallisuusvaatimukset tulevat standardista 60601-1-1. Käytännössä tämä tarkoittaa, että järjestelmän osalta samantyyppisten yhdistettyjen potilasliityntöjen sallitut kokonaispotilasvuotovirrat ovat viisinkertaiset verrattuna yksittäiseen lääkintälaitteeseen. Riippumatta siitä kuinka monta laitetta on järjestelmässä. Yksittäinen laite ei saa ylittää laitteelle tai liitynnöille määritettyjä maksimivuotovirtoja. (IEC 60601-1, 2005; IEC 60601-1-1, 2000; Pöyhönen & Kylmälä 2004, 31 - 34.)

Lääkintälaitejärjestelmän pitää täyttää lääkintälaitejärjestelmälle määritellyt sähköturvallisuusvaatimukset, vaikka järjestelmässä olisi ei-lääkinnällisiä laitteita (KUVIO 13), Lääkintälaitteet A, B ja C muodostavat lääkintälaitejärjestelmän. Kuvassa näkyvä ihminen siirtää lääkintälaitejärjestelmästä tietokoneen avulla potilastietoja palvelimelle ja potilastietokantaan. Potilastietojärjestelmien ohjelmistot ovat

lääkintälaitteita, ja niiden työasemien hoitoalueella pitäisi olla lääkintälaite-standardit täyttäviä. Tällaisissa tapauksissa on hankala sanoa, mihin lääkintälaitejärjestelmä päättyy. Sähköturvallisuuden kannalta lääkintälaitejärjestelmään kuuluvat vain laitteet A, B ja C, koska muihin laitteisiin ei ole olemassa galvaanista yhteyttä. Laitteiden A, B ja C pitää täyttää sähköturvallisuusmittauksessa 60601-1-1 mukaiset vaatimukset sähköturvallisuudelle. Erillisen tietokoneen hoitoalueella pitää täyttää 60601-1 vaatimukset, vaikka galvaanista yhteyttä ei ole laitteisiin A, B ja C. (IEC 60601-1-1, 2000; Pöyhönen & Kylmälä 2004, 31 - 34.)



KUVIO 13. Lääkintälaitejärjestelmä (Pöyhönen & Kylmälä 2004, 33)

Lääkintälaitejärjestelmiä koottaessa pitää huomioida, että lääkintälaitejärjestelmän pitää täyttää sille asetetut vaatimuksenmukaisuus asennuksen tai myöhemmin tehdyn muutoksen jälkeen. Vaatimuksenmukaisuus varmennetaan tarkistuksella, testaamisella tai analyysillä, kuten standardin 60601-1 alakohdat määrittävät. Yksittäiselle laitteelle suoritettuja turvallisuustestejä ei toisteta järjestelmälle. Sähköturvallisuusmittauksilla varmistutaan lääkintälaitejärjestelmän sähköturvallisuudesta. (IEC 60601-1-1, 2000.)

4 TIETOTURVA

4.1 Tietoturvan periaatteet

Tietoturvallisuudelle alan kirjallisuus ja eri organisaatioiden standardit tarjoavat toisistaan poikkeavia määritelmiä. Näissä määritelmissä on sama perusajatus; suojata organisaation tärkeintä omaisuutta, tietoa, jonka pitää olla luotettavaa, nopeasti saatavilla, oikeassa muodossa ja vain henkilöiden, joilla saatavilla, on oikeus tietoon.

Tiedon lisäksi tietoturva pitää sisällään tietojenkäsittelylaitteistot ja tiedon siirtämiseen käytetyt tiedonsiirtoyhteydet, jotka on suojattu luvattomalta käytöltä. Tietojärjestelmistä halutaan saada luotettavasti ja aukottomasti tieto, ketkä ovat käsitelleet tietojärjestelmissä olevaa tietoa. (Järvinen 2002, 21 - 22; Hakala, ym. 2006, 4-5.)

4.2 CIA-malli tietoturvassa

Tietoturva voidaan klassisesti määritellä tiedon arvoon perustuen, jolloin tietoturvan osa-alueet ovat luottamuksellisuus (confidentality), eheys (integrity) ja käytettävyys (availability), jotka muodostavat niin sanotun CIA-mallin (KUVIO 14). Järjestelmien ja tiedon omistajien vastuulla on turvata, ettei mikään näistä kolmesta osa-alueesta vaarannu missään tilanteessa.

KUVIO 14. CIA-malli (Gibson 2016, 8)

Luottamuksellisuus (confidentality) tarkoittaa tietojen olevan vain tietoon oikeutettujen henkilöiden käytettävissä. Lupa tietojen käsittelyyn on annettu etukäteen. Laitteistojen ja järjestelmien luottamuksellisuutta suojataan käyttäjätunnuksin ja salasanoin. Käyttäjät tunnistetaan ja autentikoidaan, jonka jälkeen käyttäjänhallinta rajoittaa oikeuksia tietoon tai järjestelmään. Salakirjoitusmenetelmiä käytetään suojaamaan tietoa, kun sitä siirretään paikasta toiseen, tällöin tieto ei paljastu ulkopuoliselle tiedonsiirron salakuuntelussa tai tietojenkäsittelylaitteiston joutuessa vääriin käsiin. Salausta käytettäessä on varmistuttava, että käytetyssä salausmenetelmässä ei ole haavoittuvuuksia ja menetelmä on luotettava. (Järvinen 2002, 22; Hakala, ym. 2006, 4; Gibson 2016, 8 - 9.)

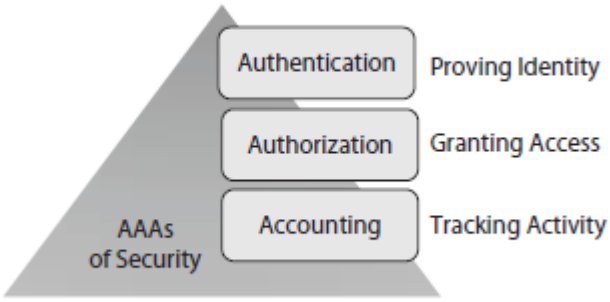
Eheydellä (integrity) tarkoitetaan sitä, että käytettävissä oleva tiedon pitää olla oikeaa ja tieto ei sisällä virheitä eikä tietoja pääse ulkopuoliset muuttamaan tai poistamaan. Virheiden määrää voidaan pyrkiä rajoittamaan erilaisin teknisin ratkaisuin. Sovelluksen tekijä voi määrittää syötteen tarkistuksia, lisäämällä tallennus- ja tiedonsiirto-operaatioihin tarkistussummia tai tiivisteitä, joilla tarkistetaan tiedon tallentuvan oikein. Tiivistettä käytettäessä voidaan vain tunnistaa, onko tieto muuttunut. Muutettuun tietoon ei voi luottaa ja on tärkeätä tunnistaa, että tietoa yritetään muuttaa. Käyttölokeja voidaan käyttää tiedon eheyden turvaamiseen, jos tunnistetaan tiedon muuttaminen ja tiedon muuttamisajankohta. Tällöin voidaan käyttölokeista selvittää, kuka on muuttanut tietoa. Tiedon eheyden voi rikkoa tietokonevirus tai kiintolevylle tullut vika-alue. Eheyden kannalta tiedoston sisällä aiheutunut eheysvika on tietoturvan kannalta hankala ongelma, koska eheysvika saatetaan havaita vasta kun tiedostoa yritetään käyttää. Mikäli varmuuskopioista ei löydy ehyttä versiota tiedostosta, niin eheysongelma muuttuu saatavuusongelmaksi. (Järvinen 2002, 22 - 23; Hakala, ym. 2006, 5; Gibson 2016, 10 - 12.)

Saatavuudella (availability) tarkoitetaan tiedon olevan saatavilla oikeassa muodossa ja riittävän nopeasti. Saatavuutta voidaan parantaa käyttämällä tarkoitukseen riittävän tehokkaita ja vikasietoisia tietojenkäsittely- ja tiedonsiirtolaitteistoja. Tietojenkäsittelyyn valitaan mahdollisimman hyvin

tiedonkäsittelyyn soveltuvat ohjelmistot. Tietoa saatetaan tarvita paljon tallennushetkeä myöhemmin, tällöin pitää huomioida, että ohjelmistot pystyvät käsittelemään tallennettua tietoa. Tiedon saatavuutta voidaan häiritä palvelunestohyökkäyksin, jolloin hyökkääjä ei pyri rikkomaan luottamuksellisuutta murtautumalla eikä eheyttä muuttamalla tietoa. Säännöllisellä varmistuksen tekemisellä ja tietojen palauttamisen testauksella parannetaan saatavuutta. (Järvinen 2002, 24; Hakala, ym. 2006, 4 - 5; Gibson 2016, 12 - 13.)

4.3 Muita tietoturvan perusteita

Käyttöoikeuksilla sallitaan tai rajoitetaan käyttäjän oikeuksia tehdä muutoksia tietoon tai käytössä olevaan järjestelmään. Käyttöoikeuksien myöntämisperiaatteena voidaan pitää sitä, että lähtökohtaisesti käyttäjälle myönnetään vähimmäisoikeudet työtehtävän hoitamiseen liittyvään tietoon tai työtehtävässä käytettävään järjestelmään, jolla he voivat tehdä työnsä. Käyttöoikeudet poistetaan käyttäjältä välittömästi, kun hän ei tarvitse niitä työtehtävässään. Käyttöoikeuksien hallinnasta löytyy yleensä huomautettavaa tietoturva-auditoinneissa. Keskitetty käyttöoikeuksien hallintajärjestelmä parantaa käyttöoikeuksien hallintaa, koska tällöin ei tarvitse järjestelmäkohtaisesti käydä muuttamassa käyttöoikeuksia. Järjestelmien ylläpitäjät tarvitsevat korotettuja käyttöoikeuksia ohjelmistojen asennukseen tai järjestelmän asetusten muuttamiseen. Ylläpitäjille luodaan ylläpitotunnus rajoitetun käyttäjätunnuksen rinnalle, jota käytetään vain ylläpitotehtävissä, joissa rajoitetut käyttöoikeudet eivät riitä. Ylläpitotunnusten käyttöä seurataan käytönvalvonnalla. (Laaksonen, ym. 2006, 151, 176 - 178; Gibson 2016, 13 - 14.)



KUVIO 15. AAA tietoturvassa (Gibson 2016, 17)

4.4 AAA-tietoturvassa

Tietoturvan AAA muodostuu todentamisesta (Authentication), valtuutuksesta (Auhthorizaton) ja tilastoinnista (Accounting) (KUVIO 15). Todentamisella (Authentication) tarkoitetaan tietojenkäsittelylaitteiden ja tietojenkäsittelylaitteita käyttävien henkilöiden luotettavaa tunnistamista. Käyttäjät yleensä tunnistetaan käyttäjätunnuksella ja salasanalla. Valtuutuksessa (Authorization) ylläpitäjä on määrittänyt käyttöoikeudet resurssille. Käyttäjän yrittäessä käyttää resurssia järjestelmä tarkistaa, onko käyttäjällä oikeutta käyttää resurssia. Jos oikeudet riittävät, käyttäjä voi käyttää resurssia, muuten käyttö estetään. Tilastoinnissa (Accounting) käyttäjän toimet tallennetaan käyttölokiin niiltä osin kuin on määritelty. Käyttäjän käyttäessä resurssia järjestelmä tallentaa lokiin, kuka on käyttänyt resurssia, milloin ja mistä. Tilastoinnilla voidaan tunnistaa väärinkäytön yritykset tai poikkeava käyttäjän toiminta. Kaikkia käyttäjän toimia ei ole tarpeen tallentaa, vain sellaiset, joissa on mahdollisuus väärinkäytöksiin. Tilastoinnin toteutuminen vaatii kaikkien käyttäjien todentamista, määritelty käyttöoikeudet seurattavaan resurssiin ja käyttölokin kertymistä resurssin käytöstä. (Järvinen 2002, 24 - 27; Hakala, ym. 2006, 6; Gibson 2016, 17 - 18.)

Pääsynvalvonnalla (Access Control) tarkoitetaan tietojenkäsittelyinfrastruktuurin suojaamista luvattomalta käytöltä. Luvatonta käyttöä on ulkopuolisen käytön lisäksi oma henkilökunta voi

käyttää tietojenkäsittelylaitteistoja ja tietoliikenneyhteyksiä omiin käyttötarkoituksiinsa. Luvaton käyttö vaarantaa organisaation tietojärjestelmien eheyden ja luotettavuuden. Pääsynvalvonnan osa-alue on myös käytön seuranta (audit log), jolla seurataan, kuka on tuottanut, katsellut tai muokannut tietoa. Tiedon käytön lisäksi voidaan seurata luvallisia ja luvattomia yrityksiä kirjautua järjestelmiin, työasemiin, verkon aktiivilaitteisiin tai sovelluksiin. Lokien seurannalla on mahdollista löytää vahingossa tai tahallisesti tapahtuneita tietoturvarikkeitä. (Järvinen 2002, 27; Hakala, ym. 2006, 5 - 6.)

Kiistämättömyydellä (non-repudiation) tarkoitetaan tiedon alkuperän ja olemassa olevan tiedon käytön varmistamista tallentamalla käyttölokiin tiedon lähde ja se kuka tietoa on käyttänyt. Luvallinen ja luvaton käyttö voidaan tunnistaa käyttämällä käyttäjäntunnistusmenetelminä älykortteja tai turvatunnistelaitetta, joihin on tallennettu henkilön tunnisteet ja käyttölupa. (Hakala, ym. 2006, 5.)

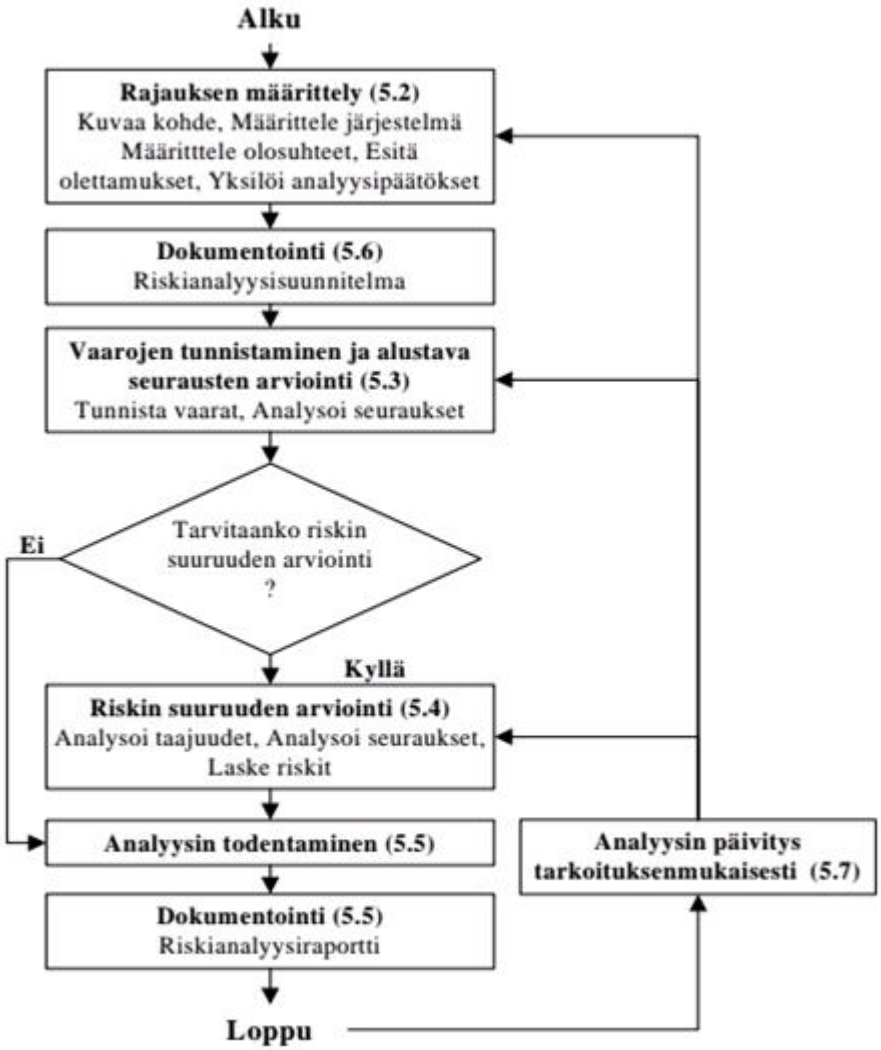
4.5 Tietoturvapolitiikka ja riskien hallinta

Tietoturvapolitiikka on yrityksen johdon hyväksymä tietoturvan kulmakivi. Tietoturvapolitiikka pitää sisällään näkemyksen tietoturvan päämääristä, periaatteista ja toteuttamisesta. Samalla myös linjataan mitä tietoturva-asioita kehitetään jatkossa. Tietoturvapolitiikka voi olla julkinen tai salainen. Julkinen tietoturvapolitiikka kuvaa esimerkiksi yrityksen internet-sivuilla asiakkaille ja työntekijöille yrityksen arvot, näkemykset ja tavoitteen. Tietoturvan osalta salainen tietoturvapolitiikka pitää sisällään menettelytapojen kuvauksia ja yksityiskohtaisia toimintaohjeita.

Seuraukset / Todennäköisyys	*Lievästi haitallinen*	*Haitallinen*	*Erittäin haitallinen*
Epätodennäköinen	VÄHÄINEN RISKI	SIEDETTÄVÄ RISKI	KOHTALAINEN RISKI
Todennäköinen	SIEDETTÄVÄ RISKI	KOHTALAINEN RISKI	MERKITTÄVÄ RISKI
Erittäin todennäköinen	KOHTALAINEN RISKI	MERKITTÄVÄ RISKI	**SIETÄMÄTÖN RISKI**

KUVIO 16. Yksinkertaistettu riskianalyysimatriisi (Suomen automaatioseura 2010)

Ennen kuin tietoturvapolitiikan periaatteita voidaan määrittää, tietoturvauhat ja tietoturvariskit pitää tunnistaa. Uhkien osalta yleensä katsotaan, mikä vaarantaa yrityksen liiketoiminnan, ja niitä turvataan tietotekniikalla. Kun uhat on tunnistettu, niin jokaisesta uhasta laaditaan riskiarvio. Riskin vakavuuden määrittelyssä voidaan käyttää riskianalyysimatriisia (KUVIO 16). Riskianalyysiprosessissa (KUVIO 17) määritellään ensimmäisenä järjestelmä, jota ollaan analysoimassa, ja se millaisissa olosuhteissa. Riskianalyysisuunnitelmaan dokumentoidaan, mitä ollaan analysoimassa. Riskiin liittyvät uhat tunnistetaan ja uhkien toteutumisen vaikutukset analysoidaan. Mikäli riskin suuruutta ei tarvitse arvioida, voidaan analyysilla todentaa riski ja laatia raportti. Riskin suuruudessa analysoidaan uhkien toteutumisen taajuus ja laaditaan tarkempi analyysi uhkien toteutumisen seuraamuksista. Riskin taloudelliset vaikutukset selvitetään, kuinka paljon uhkien toteutuminen ja torjunta maksavat. Riskinvaikutuksen kaava on vahingon kustannukset kerrottuna vahingon todennäköisyydellä. Riskin suuruuden arvio lisätään dokumentointiin. Riskianalyysit tulisi päivittää säännöllisesti, koska uhat vaihtelevat ja uhkien toteutumisen vaikutukset muuttuvat ajan kanssa. (Järvinen 2002, 113 - 114; Pöyhönen & Kylmälä 2004, 5; Hakala, ym. 2006, 5.)



KUVIO 17. Riskianalyysin työnkulku (Pöyhönen & Kylmälä 2004, 16)

Lääkintälaitteissa tietoturvariskin arviointi tehdään potilaalle tulevan haitan suhteessa tietoturvauhan käytettävyyteen ja tietoturvauhan toteutumisen todennäköisyyteen. Potilaan haitat voidaan ryhmitellä 5 tasoon (KUVIO 18). Tasolla yksi potilaalle aiheutuu haittana vaivaa tai väliaikainen epämukavuus. Haitan suurentuessa tasolle kaksi, potilaalle aiheutuu tilapäinen vamma tai vajaatoiminta, joka ei vaadi lääketieteellistä hoitoa. Tasolla kolme potilaalle aiheutuu tilapäinen vamma tai vajaatoiminta joka vaatii lääketieteellistä hoitoa. Haitan vakavuuden noustessa tasolle 4, vamma tai vajaatoiminta jää pysyväksi. Pahin mahdollinen haitta potilaalle on kuolema, joka on mahdollista toteutua tasolla 5. (FDA 2016, 17.)

KUVIO 18. Tietoturvauhkien riskinhallinta lääkintälaitteissa (FDA 2016, 16)

4.6 Tietoturvauhan vakavuuden arviointi

Tietoturvauhan vakavuuden luokittelun mittarina käytetään CVSS:ää (Common vulnerability scoring system), jonka avulla saadaan tietoturvauhasta standardiarvo. Arvon avulla uhan vaikuttavuutta ja tasoa voidaan verrata tiedossa oleviin ja tulevaisuuden uhkiin. Tietoturvauhan CVSS-arvo ilmaistaan yhden desimaalin tarkkuudella ja arvo on väliltä 0,0-10,0. Arvo 0 ilmaisee uhan olevan olematon ja arvo 10 ilmaisee pahinta mahdollista uhkaa. CVSS:ää ylläpitää FIRST (Forum of Incident Response and Security Teams), ja Suomessa FIRSTin kuuluu muun muassa Kyberturvallisuuskeskus. (First.org inc, 2017.)

Tietoturvauhka pisteytetään perusmittaristolla (Base Metric), johon kuuluvat kuusi tekijää, jotka kuvaavat haavoittuvuuden ominaisuuksia: hyökkäystapa, hyökkäyksen monimutkaisuus, hyökkääjän tunnistautumis-vaatimus, luottamuksellisuus, eheys ja saatavuus. (First.org inc, 2017.)

Hyökkäystapa (Access Vector, AV) kuvaa tietoturvauhan hyödyntämiseen tarvittavaa yhteystavassa yrityksen ei julkiseen sisätietoliikenneverkkoon. Yhteystapa kuvataan kolmella arvolla, jotka ovat Local (L), Adjacent Network (A) ja Network (N). Local vaihtoehdolla, hyökkääjän tarvitsee päästä fyysisesti sisäverkkoon hyödyntääkseen haavoittuvuutta. Adjacent Network vaihtoehdolla, hyökkääjällä tarvitsee olla pääsy sisäverkkoon.

Network vaihtoehdolla, haavoittuvuutta on mahdollista hyödyntää verkon yli. (First.org inc, 2017.)

Hyökkäyksen monimutkaisuus (Access Complexity, AC) kuvaa hyökkäyksen monimutkaisuutta, kun haavoittuvuutta hyödyntävä hyökkääjä on päässyt käsiksi haavoittuneeseen järjestelmään. Monimutkaisuus kuvataan arvoilla jotka ovat High (H), Medium (M) ja Low (L). Monimutkaisuutta kuvatessa High vaihtoehdolla järjestelmään pääsyyn vaaditaan erityisolosuhteet. Erityisolosuhteita ovat hyökkääjän hallussa olevat korotetut käyttöoikeudet tai hyökkäys perustuu käyttäjän manipulointiin, joka pitäisi helposti tunnistaa. Monimutkaisuutta kuvatessa Medium-arvolla hyökkääjällä on pääsy rajoitettuun määrään järjestelmiä tai pääsy järjestelmään rajoitetuin oikeuksin. Low-arvolla hyökkäys ei ole hyödynnettävissä. (First.org inc, 2017.)

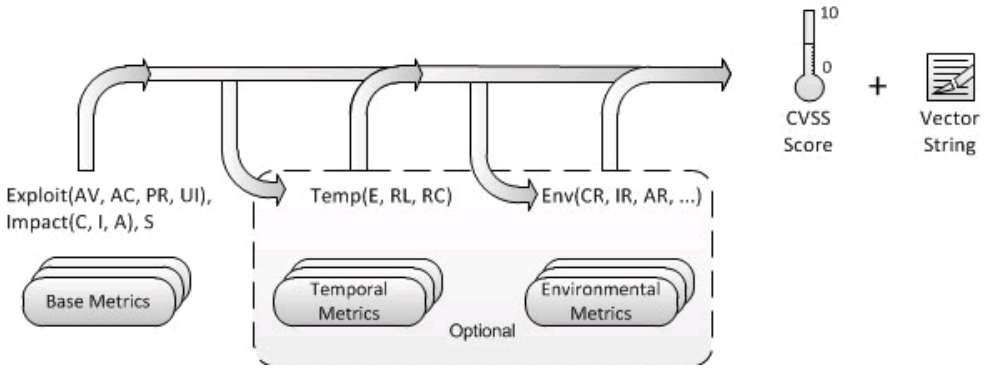
Hyökkääjän tunnistautumisvaatimus (Authentication, AU) kuvaa tunnistaumiskertojen määrä ennen kuin hyökkääjä voi hyödyntää haavoittuvuutta järjestelmässä. Tunnistautumisvaatimusta kuvataan arvoilla Multiple (M), Single (S) ja None (N). Multiple tarkoittaa, että haavoittuvuuden hyödyntämiseksi hyökkääjän pitää tunnistautua kahdesti tai useammin, vaikka hyökkääjän ei tarvitsisi saada haltuunsa kuin yhdet tunnisteet. Single tarkoittaa, että hyökkääjän pitää tunnistautua kerran. None tarkoittaa, ettei hyökkäykseen tarvita tunnistautumista. (First.org inc, 2017.)

Jäljelle jäävät kolme tekijää, luottamuksellisuus, eheys ja saatavuus kuvaavat, kuinka haavoittuvuutta hyödynnettäessä tietoturvan kulmakivet vaarantuvat. Kaikilla arvot ovat samat None (N), Partial (P) ja Complete (C). Jos hyökkäyksessä luottamuksellisuus (Confidentiality Impact) ei vaarannu lainkaan, luokitus on None. Luottamuksellisuuden vaarantumisen riski ollessa olennainen luokitus on Partial. Luottamuksellisuuden täydellisesti vaarantuessa luokitus on Complete. Jos haavoittuvuudella ei ole vaikutusta suojattavan tiedon eheyteen, arvo on None. Mikäli tiedostoja on voinut rajoitetusti muokata, on arvo Partial.

Luokituksella Complete hyökkääjä on voinut muokata järjestelmän tietoja vapaasti. (First.org inc, 2017.)

Jos hyökkääjällä ei ole mahdollisuuksia käyttää järjestelmän resursseja tai kaistanleveyttä, saatavuus arvioidaan arvolla None. Osittainen resurssien hyödynnettävyys voi vaikuttaa järjestelmän toiminnallisuuteen, jota arvioidaan arvolla Partial. Täydellinen järjestelmän resurssien vapaasti käyttöön saaminen arvioidaan arvolla Complete. (First.org inc, 2017.)

CVSS-arvoa määritettäessä voidaan käyttää tarkentavia mittareita: ajallinen (Temporal) ja käyttöympäristö (Enviromental). Ajallisella mittarilla voidaan käyttää Temporal Score Metrics -mittaristoa, jossa voidaan määritellä, onko haavoittuvuudelle olemassa jo hyökkäyskoodi. Käyttöympäristön osalta voidaan määrittää Target Distrubution -mittariston kautta, kuinka suuri prosentuaalinen osuus käyttöympäristön järjestelmistä on haavoittuvaisia. (First.org inc, 2017.)



KUVIO 19. CVSS-laskentamalli (First 2017)

5 LÄÄKINTÄLAITTEISIIN KOHDISTUVAT TIETOTURVAUHAT JA SUOJAUTUMISTEKNIIKAT

Sairaaloiden tietoverkoissa on tyypillisesti päätelaitteita, joilla on pääsy internetiin, palvelimia, verkonaktiivilaitteita ja lääkintälaitteita. Sairaalan toiminnassa kriittisiä järjestelmiä ovat luonnollisesti potilastietojärjestelmät, niihin potilaista tietoa tuottavat lääkintälaitteet ja lääkintälaitejärjestelmät. Verkkoon liitettäviin lääkintälaitteisiin kohdistuvat samat tietoturvauhat kuin mihin tahansa muuhun verkkoon liitettyyn laitteeseen. Lääkintälaitteiden kautta voidaan tehdä sairaalan verkkoon hyökkäyksiä, jos lääkintälaitteilla on pääsy internetiin, tai lääkintälaitteisiin on päästy sairaalan verkon ulkopuolelta vaarantamaan niiden tietoturvaa. (Trapx Labs 2015, 5, 9 - 10; Enisa 2016, 17, 19; Trapx Labs 2016, 5 - 6, 11.)

Lääkintälaitteet voivat olla mustia aukkoja sairaalan tietoturvatiimeille, koska lääkintälaitteisiin ei välttämättä voida asentaa sairaalan käyttämiä tietoturvaohjelmistoja teknisten esteiden tai valmistajan kiellon takia. Lääkintälaitteita ei välttämättä tunnisteta tietokoneiksi, koska käyttäjällä ei ole käyttöliittymää, joka viittaisi lääkintälaitteen olevan tietokone. Lääkintälaitteiden ylläpito ja päivitykset tehdään laitevalmistajan toimesta. Lääkintälaitteisiin ei pidä asentaa ohjelmistoja tai tietoturvapäivityksiä ilman valmistajan lupaa. Luvaton ohjelmistoasennus saattaa vaarantaa laitteiston toimivuuden ja siten aiheuttaa vaaratilanteen. Lääkintälaitevalmistajien ei tarvitse hyväksyttää viranomaisilla lääkintälaitteisiin asennettavia tietoturvapäivityksiä, joten laitevalmistajien pitäisi pystyä hyväksymään julkaistut tietoturvapäivitykset lääkintälaitteisiin asennettavaksi kohtuullisella aikataululla. Valitettavasti osa lääkintälaitteista on suljettuja järjestelmiä, joissa ajetaan käyttöjärjestelmää, jota ei ole päivitetty tai johon ei ole saatavilla tietoturvapäivityksiä. Hankittava lääkintälaite voi olla vanhentunut käyttöjärjestelmältään, koska lääkintälaitteiden kehitystyö kestää noin 3 vuotta suunnittelusta valmistukseen, ja laitevalmistaja on keskittänyt resurssinsa uuden laitteen suunnitteluun. (Trapx Labs 2015, 5, 9 - 10; Enisa 2016, 17, 19; Trapx Labs 2016, 5 - 6, 11.)

Sairaalan työasemiin ja palvelimiin asennetut tietoturvapäivitykset paikkaavat tietoturva-aukkoja, jotka ovat hyödynnettävissä lääkintälaitteissa. Paikattua tietoturva-aukkoa ei voi hyödyntää, jolloin sairaalan tietoturvaohjelmistot eivät havaitse uhkaa. Syynä haavoittuvuuksien käytettävyyteen on tietoturvapäivitysten asentamattomuus tai käytetään käyttöjärjestelmää johon ei ole tietoturvapäivityksiä saatavilla. Lääkintälaitteisiin kohdistettuja vanhojen virusten variantteja on löydetty, kun tietoturvayhtiöt ovat tutkineet sairaalaan kohdistuneita tietoturvahyökkäyksiä. Nämä lääkintälaitteisiin kohdistetut virukset etsivät vanhentuneita tai päivittämättömiä käyttöjärjestelmiä, vältellen sairaalan tietoturvan valvontajärjestelmiä tai tietoturvaohjelmistoilla suojattuja tietokoneita. Lääkintälaitteita joiden tietoturva on rikkoutunut tietoturvauhan takia, voidaan hyödyntää laajemmassa sairaalaan kohdistuvassa hyökkäyksessä. (Trapx Labs 2015, 5, 9 - 10, 13; Enisa 2016, 17, 19; Trapx Labs 2016, 5 - 6, 11.)

5.1 Haittaohjelmat

Haittaohjelmalla tarkoitetaan ohjelmaa, joka pyrkii aiheuttamaan tietokoneelle haittaa, vahinkoa tai levittämään itseään. Ensimmäiset haittaohjelmat olivat virukset 80-luvun alkupuolella. Viruksen pyrkimys on tartuttaa tietokone ja levittää itseään eteenpäin käyttäjän tietämättä. Virukset kuten muut haittaohjelmat eivät enää Ambulance-viruksen tapaan esitä tietokoneen ruudulla ASCII-animaatiota ilman vahinkoa tiedostoille. (Järvinen 2012, 178; F-Secure 2017.)

Lääkintälaitteisiin on kohdistunut perinteisten haittaohjelmien lisäksi lääkintälaitteisiin kohdennettuja haittaohjelmia, jotka ovat pyrkineet antamaan ulkopuoliselle hyökkääjälle pääsyn sairaalan verkkoon ja tietojärjestelmiin. Tietoturvaohjelmistot eivät havaitse näitä ohjelmia mikäli niitä ajetaan järjestelmissä joissa haavoittuvuudet ovat paikattu. Haittaohjelma saattaa liikennöidä salattuna jolloin sisältöä ei voida havaita tietoturvaohjelmistoilla. Haittaohjelmat pyrkivät luomaan hyökkääjälle takaoven jota hyökkääjä voi hyödyntää varastaakseen potilastietoja tai

levittää kiristyshaittaohjelmaa, joka kryptaa tiedot, lähettää purkuavaimen hyökkääjälle ja vaatii salausavaimesta lunnaita. (Trapx Labs 2015, 5, 9 - 10; Enisa 2016, 17; Trapx Labs 2016, 14, 22.)

5.2 Haittaohjelmien jakelukanavat

Rikolliset lähettävät käyttäjälle sähköpostin jonka tarkoituksena on saada käyttäjä avaamaan saastunut liitetiedosto, joka pitää sisällään haittaohjelman tai paikkaamatonta tietoturva-aukkoa hyödynnetään lataamaan tietokoneelle internetistä haittaohjelma. Sähköposti voidaan väärentää jolloin liitetiedosto vaikuttaa aidolta laskulta tai lähetysluettelolta. Vaihtoehtoisesti käyttäjä voidaan yrittää houkutella avaamaan sähköpostista linkki murretulle www-sivustolle jossa käyttäjä harhautetaan lataamaan tietokoneelle tärkeäksi käyttöjärjestelmäpäivitykseksi naamioitu haittaohjelma. (Jackson 2010, 366 - 367; Järvinen 2012, 181 - 182.)

WWW-sivusto joutuu tietomurron uhriksi kun tietomurron tekijät asentavat palvelimille haittaohjelmiston. Käyttäjä houkutellaan murretulle www-sivustolle sähköpostin kautta lähetetyllä viestillä. Käyttäjä avaa www-sivun, jolloin haittaohjelmisto selvittää käyttäjän selaimen, selaimen käyttämät lisäosat ja niiden versiot. Haittaohjelmisto vertailee omaan tietokantaansa käyttäjän käyttämää selainta ja lisäosia etsien paikkaamattomia haavoittuvuuksia. Käyttäjän koneelle ladataan paikkaamatonta haavoittuvuutta hyödyntäen haitta-ohjelma ilman käyttäjän tarvetta klikata tai ladata sivustolta mitään. (Jackson 2010, 362 - 365; Järvinen 2012, 183 - 184; Viestintävirasto 2015.)

5.3 Verkkoyhteyttä hyödyntävä hyökkäys

Sairaalaan kohdistuu verkon kautta hyökkäyksiä, joiden kohteena ei ole lääkintälaiteet vaan potilastietojärjestelmät ja niiden sisältämät potilastiedot. Yhdysvalloissa suurimmissa potilastietojen varkauksissa on viety miljoonien potilaiden potilastiedot yhdessä hyökkäyksessä. Sairaalat suojaavat sisäverkkonsa palomuurein, tunkeilijan

havaitsemis/torjuntajärjestelmin. Työasemat ja palvelimet ovat ajan tasalla tietoturvan osalta. Lääkintälaitteilla saattaa olla suora pääsy internetiin. Lääkintälaitteissa olevat haavoittuvuudet mahdollistavat haittaohjelmien saastuttavan laitteen ja lataavan laitteeseen takaoven muodostavan haittaohjelman, joka avaa pääsyn sairaalan verkkoon. Verkkoon päästyään rikolliset voivat saastuttaa suuren määrän suojaamattomia lääkintälaitteita ja käyttää niitä omiin käyttötarkoituksiinsa. Haittaohjelma saattaa päästä suojattuun lääkintälaiteverkkoon valmistajan huoltomiehen käyttämän saastuneen USB-muistitikun avulla. Haittaohjelma asentaa itsensä lääkintälaitteeseen huomaamatta.

Pelkkä palomuurisuojaus ei riitä turvaamaan lääkintälaitteita verkon kautta tulevilta tietoturvauhilta tai sairaalan muuta verkkoa lääkintälaitteiden aiheuttamilta uhilta. Verkossa olevia saastuneita tai hakkeroituja laitteita voidaan etsiä niin sanotuin hunajapurkkien (honeypot) avulla. Honeypot on päivittämätön suojaamaton laite tai se emuloi haavoittuvaa laitetta. Lääkintälaitteet voivat olla osana botnettiä, jolla voidaan aiheuttaa palvelunestohyökkäys sairaalan verkosta ulkopuoliseen tai sisäiseen kohteeseen. Sairaalanverkon sisäpuolella tehty palvelunestohyökkäys voi aiheuttaa tilanteen, jossa potilastietojen käytettävyys vaarantuu. Vaarallisin muoto lääkintälaitteeseen kohdistuvasta hyökkäyksestä on laitteen toiminnan tai tietojen muuttaminen. Laitteeseen ei voi tällöin luottaa tai se ei toimi oikein. Laitteen muokkaus saattaa vaarantaa potilaan turvallisuuden muokkaamalla luotuja suojamekanismeja. (Trapx Labs 2015, 15, 19; Enisa 2016, 21 - 22; Trapx Labs 2016, 5, 8, 17.)

5.3.1 Palomuuri

Palomuurein voidaan verkon sisällä erottaa verkon osia kokonaan toisistaan ja kontrolloida millainen liikennöinti on sallittu verkkojen tai verkkoon liitettyjen laitteiden välillä. Palomuureja on verkkopohjaisia ja laitepohjaisia. Verkkopohjaiset palomuurit eivät vaadi muutoksia tai asennuksia verkkoon liitettyihin laitteisiin. Yleisimmät käyttöjärjestelmät

tarjoavat laitekohtaisia palomuureja joilla voidaan suojata laitetta siihen kohdistuvalta tietoliikenteeltä. Palomuurisääntöjen ylläpito voi olla hankalaa, koska palomuurien ylläpitäjä ei saa tietoonsa järjestelmän poistumista käytöstä tai ylläpitäjälle ei ilmoiteta muutoksista. Tästä syystä palomuurien säännöt pitäisi säännöllisesti tarkistaa ja käyttämättömät säännöt poistaa. Palomuurien sääntöjen luonnissa pitää alun perin vaatia tarkat tiedot käytettävistä IP-osoitteista ja protokollista. Palomuurin avauspyyntö saattaa olla puutteellinen ja virheellisesti avataan laitteiden X ja Y välille kaikki protokollat ja palomuurisääntöjä suunnitellaan tiukennettavaksi myöhemmin. (Andreasson, Koivisto, 2013, 71 - 72.)

Ensimmäisen sukupolven palomuurit ovat paketinsuodatukseen perustuvia tilattomia palomuureja. Palomuuri suodattaa liikennettä pääsynvalvontalistan (Access control list, ACL) mukaan käyttäen parametreina:

- lähdeosoitetta
- kohdeosoitetta
- lähdeporttia
- kohdeporttia
- tietoliikenneprotokollaa.

Palomuurisäännöissä oletuksena sallitaan erikseen yhteys ja oletuksena kaikki mikä ei ole sallittu kielletään. Jokainen käytetty yhteys vaatii oman sääntönsä, joka kasvattaa ACL:n suureksi. Monet sovellukset määrittävät lähdeportiksi satunnaisen portin väliltä 1024-65535, jolloin jokaiselle lähdeportille pitää luoda oma sääntö. Jokainen paketti tarkistetaan, onko paketti sallittu pääsynvalvontalistalla sallituissa säännöissä, joka saattaa ilmetä palomuurin suorituskyvyn heikentymisenä. (Frahim, ym. 2014, 2; Gibson 2016, 125 - 127.)

Toisen sukupolven palomuurit ovat tilalliseen pakettisuodatukseen (Stateful Packet Instpection, SPI) perustuvia palomuureja jotka osaavat tarkistaa kuuluuko saapuva paketti jo avattuun tietoliikenneyhteyteen. Palomuuri tarkistaa oletuksena kuuluuko paketti olemassa olevaan

avoimeen yhteyteen. Jos paketti ei kuulu avoimeen yhteyteen, niin palomuuri tarkistaa pääsynvalvontalistan säännöistä onko yhteys sallittu, mikäli yhteys on sallittu, palomuuri tallentaa avatun yhteyden tilatauluun (state table). Paketin saapuessa verkon ulkopuolelta tarkistetaan tilataulusta, onko paketti sallittu vertailemalla tilataulun arvoja paketin kohdeosoitteeseen ja -porttiin Käytännössä palomuurin sisäpuolelta voidaan avata yhteys ulkopuolelle, mutta ulkopuolelta ei voida avata yhteyttä sisäpuolelle. (Frahim, ym. 2014, 2, 6; Gibson 2016, 127.)

Kolmannen sukupolven palomuurit ovat sovelluspalomuurit, jotka toimivat sovelluskerroksella. Sovelluspalomuuri analysoi läpikulkevien pakettien sisällön ja estää väärän sisältöisten pakettien pääsyn verkosta pois tai verkkoon. Sovelluspalomuurilla voidaan rajoittaa sallittu liikenne tiettyihin ylemmän tason protokolliin kuten HTTP ja SMTP, jolloin muu liikenne ei läpäise palomuuria vaikka se käyttäisi samoja portteja kuin HTTP tai SMTP. Neljännen sukupolven palomuurit ovat uhkien torjuntajärjestelmiä (unified threat management UTM), jotka pitävät sisällään perinteisen palomuurin ominaisuuksien lisäksi haittaohjelmien tunnistuksen ja torjunnan, sähköpostin sisällön suodatuksen ja internet sivujen sisällön suodatuksen. (Frahim, ym. 2014, 8; Gibson 2016, 127 - 128.)

5.3.2 Tunkeutumisen havaitsemis- ja estojärjestelmät

Tunkeutumisen havaitsemisjärjestelmällä (Intrusion Detection System, IDS) pystytään havaitsemaan ja suojaamaan verkon laitteita hyökkääjiltä. IDS pystyy havaitsemaan verkkoon tunkeutumisyritykset tarkkailemalla verkkoliikennettä ja järjestelmien lokeja. Passiivinen IDS tekee vain hälytyksen mahdollisesta hyökkäyksestä. Aktiivinen IDS voi muokata palomuurin pääsynvalvonta listaa ja estää verkkoliikenteen kohteeseen hälytyksen lisäksi. IDS voi toimia verkko- tai laitepohjaisena ratkaisuna. (Krutz & Vines, 2003, 48 - 49, 62 - 63; Gibson 2016, 275 - 282.)

Verkkopohjaisessa ratkaisussa NIDS monitoroi verkkoliikennettä verkon aktiivitaitteisin asennetun agentin avulla, tai laitteiston yksi tietoliikenneportti voi olla määritetty välittämään kaikki liikenne port

mirroring:n avulla NIDS:lle. NIDS ei näy tunkeutujalle, koska laitteille ei asenneta mitään. Tämä tekee NIDS:sta tunkeutujalle näkymättömän tavan suojata työasemia ja palvelimia. Laitepohjaisessa ratkaisussa (HIDS) työasemiin ja palvelimiin asennetaan IDS-ohjelmisto, joka monitoroi laitteen toimintaa. Laitepohjaisen ratkaisun heikkous on laitteisiin asennettava ohjelmisto, jonka hyökkääjä voi sammuttaa ja siivota lokeista jäljet hyökkäyksestä pois. NIDS pystyy monitoroimaan laitteessa ajettavia prosesseja ja ohjelmistoja. Tunkeutujanestojärjestelmä (Intrusion Prevention System, IPS) on IDS:n kehittyneempi muoto, yksinkertaistettuna IPS on aina aktiivinen IDS. Verkkopohjainen IPS asennetaan verkon reunalle, sisäverkon ja internetin väliin. Tällöin IPS seuraa verkkoliikennettä ja voi tarvittaessa estää haitallisen liikennöinnin muuttamalla palomuurin sääntöjä. (Krutz & Vines, 2003, 48 - 49, 62 - 63; Gibson 2016, 275 - 282.)

Tunnusmerkkipohjaisessa menetelmässä verkkopohjaiset IDS ja IPS vertaavat lokeja ja verkkoliikennettä tietokannassa oleviin tunnusmerkkeihin. Laitepohjaiset vertaavat laitteesta monitoroitavia parametreja tietokannan tunnusmerkkeihin. Jos tunnusmerkistö täyttyy, tehdään hälytys ja mahdolliset toimet tunkeutujan torjumiseksi. Tunnusmerkkipohjaisella menetelmällä on kaksi heikkoutta, menetelmä ei tunnista hitaita tunkeutumisia, jotka suoritetaan pitkän ajanjakson aikana, myöskään tuntemattomia hyökkäyksiä ei tunnisteta. Vääriä hälytyksiä tulee vähän ja ne saadaan standardimuodossa, jolloin hälytyksen aiheuttaja on helppo tulkita. Tunnusmerkki-tietokantaa pitää päivittää jatkuvasti ja uudet merkistöstä poikkeavat hyökkäykset jäävät huomaamatta. (Krutz & Vines, 2003, 48 - 49, 62 - 63; Gibson 2016, 275 - 282.)

Tilastollisiin poikkeuksiin perustuvassa menetelmässä verkkopohjainen IDS ja IPS määrittää valvottavan verkon normaalin käyttöprofiilin. Laitepohjaisissa ratkaisuissa luodaan laitteistosta vastaava profiili. Profiiliin merkitään normaali käyttötilanne. Tällä menetelmällä voidaan havaita uuden tyyppisiä hyökkäyksiä, koska ne aiheuttavat tilastollisen poikkeaman jota verrataan aiemmin luotuun profiilin. Menetelmän

heikkoutena on mahdollisuus tulkita hyökkäykseksi tilanne, jossa verkon liikenne poikkeaa normaalista ilman verkkoon kohdistuvaa uhkaa. (Krutz & Vines, 2003, 48 - 49, 62 - 63; Gibson 2016, 275 - 282.)

6 VERKKOON LIITETTÄVÄT LÄÄKINTÄLAITTEET

Lääkintälaitteen verkkoon liittämisen pitää tuottaa olennaista hyötyä potilaan hoidossa. Olennainen hyöty on lääkintälaitteen tuottaman potilasdatan tallentaminen potilastietojärjestelmiin. Potilastietojärjestelmiin tallennettu tieto on nopeasti ja helposti hoitohenkilökunnan saatavilla. Lisäksi keskusvalvomoissa voidaan verkon kautta seurata potilaspaikoilta tulevia potilasvalvontalaitteiston tietoja, jolloin hoitohenkilökunnan ei tarvitse olla potilashuoneissa seuraamassa potilaan tilaa. Joissain tilanteissa lääkäri voi seurata toisessa kiinteistössä tehtävää tutkimusta reaaliaikaisesti etäyhteyden kautta, jolloin lääkärin työaikaa ei mene siirtymisessä toiseen paikkaan.

6.1 Laiterekisterianalyysi lääkintälaitteiden verkkoon liitettävyydestä

Lääkintätekniikan laiterekisteriin on lakisääteisesti tallennettu kaikki sairaalan käytössä olevat lääkintälaitteet ja niille tehdyt huoltotoimenpiteet. Lääkintätekniikka vastaa lääkintälaitteiden elinkaaresta, laitteen hankintaprosessista, hankinnasta laitteen käytöstä poistoon ja turvalliseen hävittämiseen.

Lääkintätekniikan rekisteriin ei ole merkitty, onko laite liitetty verkkoon, jolloin ei ole tiedossa tarkkaa määrää, kuinka monta lääkintälaitetta on sairaalan verkossa. Laiterekisterissä on noin 65 000 lääkintälaitetta tai lääkintälaitejärjestelmää. Lääkintälaitteiden verkkoon liitettävyyttä tutkittiin lääkintälaitteen kauppanimen mukaan, joka on lääkintälaitteen yleinen kaupallinen nimi, sekä lääkintälaitteiden laitenimikkeen perusteella, joka kuvaa lääkintälaitteen toiminnallisuutta.

Kauppanimen perusteella rekisteristä löytyi 15500 yksilöityä kauppanimeä. Tarkastellessa kauppanimiä ilmeni yksittäisiä laitteita olevan rekisterissä 9250 kappaletta. Näiden joukossa löytyi kauppanimiä jotka vaikuttivat virheellisiltä kirjauksilta. Kauppanimessä virheelliseltä kirjaukselta vaikuttava ero saattaa erottaa kaksi eri laitetta toisistaan. Selkeät kirjoitusvirheet on helppo korjata, mutta vaativat asiantuntemusta tunnistaa

eri mallimerkinnät kirjoitusvirheistä. Lääkintälaitehankinnat analysoitiin vuosilta 2015 ja 2016. Vuonna 2015 sairaalaan oli hankittu 8500 lääkintälaitetta, 1700 yksilöivällä kauppanimellä. Vuonna 2016 oli hankittu 5000 lääkintälaitetta, 1500 yksilöivällä kauppanimellä. Lääkintälaitteen verkotettavuutta kauppanimen perusteella selvitettäessä käytännössä jokaisen laitteen käyttö- tai huoltomanuaalista olisi tarkistettava, onko laite mahdollista liittää verkkoon. Laitevalmistaja voi myös kieltää lääkintälaitteen verkkoon liittämisen, vaikka se olisi fyysisesti mahdollista. Kauppanimen perusteella verkkoon liittävistä lääkintälaitteista olisi saatu tarkka lukumäärä. Pelkästään vuoden 2016 laitehankintojen läpikäynti on satojen tuntien urakka. Jos laitteen manuaalista verkotettavuuden tarkistaminen veisi aikaa 15 minuuttia laitetta kohden laite, niin vuonna 2016 hankittujen lääkintälaitteiden läpikäyntiin kauppanimen perusteella kestäisi 375 tuntia.

TAULUKKO 1. Lääkintälaite liitettävissä suoraan verkkoon

Laitteiden hankinavuodet	Lukumäärä	25 yleisintä laitenimikettä % kaikista laitteista	lkm	% suoraan verkkoon liitettäviä	lkm	Yli 10 laitetta samalla nimikkeellä lkm	% suoraan verkkoon liitettäviä	lkm
1980-2016	65 162	44 %	28 552	7 %	4 671	63542	16 %	10114
2007-2016	43 836	48 %	20 949	9 %	4 122	42600	9 %	4006
2011-2016	25 000	49 %	12 275	8 %	1 979	23917	8 %	1893
2014-2016	17 596	53 %	9 308	10 %	1 756	16546	10 %	1651
2015-2016	13 474	57 %	7 643	10 %	1 395	12515	10 %	1296
2016	5 003	52 %	2 592	8 %	398	4061	8 %	323

Laiterekisteristä erilaisia laitenimikkeitä löytyi 950 kappaletta. 25 yleisintä laitenimikettä muodostaa 44 prosenttia koko lääkintälaitekannasta. Yleisimpiä lääkintälaitteita ovat infuusiopumput, potilasvalvontamonitorit ja niiden mittausmoduulit, sairaalasängyt, kuume- ja verenpainemittarit ja tutkimusvalaisimet. Yleisimmistä lääkintälaitteista voidaan 7 prosenttia tyypillisen käyttötarkoituksen mukaisesti liittää suoraan verkkoon. Esimerkkejä tyypillisesti verkkoon liitettävistä lääkintälaitteista ovat lääkintälaitteet, joilla tehdään kuvantamis- tai laboratoriotutkimuksia. Laitenimikkeiden osalta tarkisteltiin laitenimikkeet, joissa on vähintään 10 laitetta. Koko laitekannan osalta tämä tarkoittaa 16 prosenttia, joka on 10000 lääkintälaitetta. Arviota verrattiin vuosien 2015 ja 2016 lääkintälaitehankintoihin. Vuosina 2015 ja 2016 hankituista lääkintälaitteista tyypillisesti 8-10 prosenttia voidaan liittää suoraan

verkkoon. Taulukossa 1 näkyvien verkkoon liitettävien lääkintälaitteiden osuus on 8-10 prosenttia, kun laitehankintoja tarkistettiin viimeisiltä vuosilta. Jos tarkastellaan kaikkia laitteita, joita on samalla nimikkeellä yli 10 kappaletta. Tällöin suoraan verkkoon liitettävien laitteiden osuus kasvaa 8 - 10 prosentista 16 prosenttiin.

6.2 Tietokoneet lääkintälaitteissa

Lääkintälaitteet eivät tänä päivänä koostu pelkästään logiikkapiireistä, aktiivisista ja passiivisista komponenteista. Lääkintälaitteissa ohjelmoitavilla digitaalisilla mikropiireillä (FPGA), sovelluskohtaisilla mikropiireillä (ASIC) tai mikrokontrollerilla voidaan toteuttaa samat halutut toiminnallisuudet kuin erillisillä komponenteilla. Mikropiirien käyttö vähentää laitteiden suunnittelu- ja valmistuskustannuksia. Komponenttien määrän väheneminen parantaa laitteiden luotettavuutta. Lääkintälaitteiden mikropiireissä ajetaan reaaliaikaista (RTOS) tai sulautettua (Embedded) käyttöjärjestelmää.

Lääkintälaitteen liittäminen tietokoneeseen tai tietoliikenneverkkoon muodostaa toiminnallisen yhteyden toteutumisen näkökannasta riippuen aina lääkintälaitejärjestelmän. Tietokoneeseen tai tietoliikenneverkkoon yhdistettävät lääkintälaitteet/lääkintälaitejärjestelmät päätettiin jakaa kolmeen ryhmään:

- lääkintälaite, joka sisältää sulautetun tietokoneen
- lääkintälaite, joka sisältää integroidun tietokoneen
- lääkintälaitejärjestelmät, joka sisältää erillisen tietokoneen.

Käytännössä kaikki kolme esimerkkitapausta sisältävät aina tietokoneen.

6.2.1 Sulautetun tietokoneen sisältävä lääkintälaite

Käytännössä kaikki elektroniikkaa sisältävät lääkintälaitteet ovat sulautettuja järjestelmiä. Sulautetun tietokoneen tai integroidun tietokoneen sisältävän tietokoneen erottaminen toisistaan ei ole

yksinkertaista, koska lääkintälaitteeseen integroitu tietokone saattaa olla sulautettu järjestelmä. Järjestelmässä ajetaan samanlaisella raudalla sulautettua käyttöjärjestelmää kuin sulautetun tietokoneen sisältävässä lääkintälaitteessa. Sulautetun tietokoneen sisältävä lääkintälaite määriteltiin seuraavasti ”Sulautetun tietokoneen sisältävä itsenäisesti toimiva lääkintälaite, jota ei voida kytketä suoraan tietoliikenneverkkoon.”

Sulautetun tietokoneen sisältävä lääkintälaite voidaan liittää tietokoneeseen, jonka avulla tutkimusdata siirretään erillisellä ohjelmistolla sairaalan tietojärjestelmiin. Tyypillisesti käyttöjärjestelmä on reaaliaikainen käyttöjärjestelmä (RTOS) tai sulautettu Linux. Itsenäisesti ilman tietokonetta toimiva lääkintälaite, joka on mahdollista liittää tietokoneeseen, muodostaa tietokoneen kanssa lääkintälaitejärjestelmän. Verkkoon liittämisessä on aina huomioitava lääkintälaitteisiin kohdistuvat sähköturvallisuusvaatimukset. Tietokone on analysointi- tai katselutyöasema, jolla käsitellään lääkintälaitteen tuottamaa tutkimusdataa, joka tallennetaan sairaalan tietojärjestelmiin.

6.2.2 Lääkintälaite, joka sisältää integroidun tietokoneen

Integroidun tietokoneen sisältämä lääkintälaite määriteltiin seuraavasti: ”Lääkintälaitteen tietokone on kiinteä osa lääkintälaitetta”. Tietokonetta ei voi perinteisesti mieltää tietokoneeksi, tietokone voi olla sulautettu tai lääkintälaitteen kotelon sisällä oleva erillinen tietokone, joka ei näy käyttäjälle. Lääkintälaitteen päälle laittamisen jälkeen lääkintälaite voi käynnistyä suoraan lääkintälaitteen käyttöliittymään ilman suoraa indikaatiota laitteiston käyttöjärjestelmästä. Integroidun tietokoneen sisältämä lääkintälaitteen käyttöjärjestelmä on tyypillisesti Windows tai Linux. Käyttöjärjestelmä on sulautettu, työasema- tai palvelinversio-käyttöjärjestelmästä. Lääkintälaite on liitettävissä suoraan sairaalan tietoliikenneverkkoon. Integroiduissa laitteissa verkkoliitännät ovat yleensä 60601-1 mukaisesti suojattu.

6.2.3 Erillisen tietokoneen sisältävä lääkintälaite

Erillisen tietokoneen tarvitseva lääkintälaite on aina lääkintälaitejärjestelmä, koska lääkintälaite ei toimi itsenäisesti ilman tietokonetta toiminnallinen yhteys toteutuu. Tietokone voi olla normaali toimistotietokone, palvelin tai lääkintälaitetiloihin tarkoitettu Medical-PC. Jos laitteen tietokone ei ole Medical-PC, lääkintälaitejärjestelmä on varustettava lääkintäerotusmuuntajalla. Laitteiston käyttöjärjestelmä on Windows tai Linux. Erillisen tietokoneen sisältävissä lääkintälaitteissa verkko ja oheislaite liitännät eivät ole 60601-1 mukaisesti eristetty vaan niissä käytetään ulkoisia erottimia.

7 LÄÄKINTÄLAITTEEN ELINKAARI

Lääkintälaitteen elinkaari sairaalassa alkaa lääkintälaitteen hankinnasta sairaalaan. Asennuksen ja vastaanottotarkistuksen jälkeen lääkintälaite on osana potilaan hoitoa. Lääkintälaite määräaikais huolletaan ja viat korjataan yleensä niin kauan kuin laitteelle saadaan varaosia tai laitteen korjaus on järkevää. Laitteen poistuessa käytöstä se hävitetään asianmukaisesti.

7.1.1 Hankintaprosessi, koekäyttö

Lääkintälaitteen elinkaari alkaa hankinnasta. Hankintaa suunniteltaessa osastolla on tiedossa millainen lääkintälaite tarvitaan potilaan hoidossa. Osasto ottaa yhteyttä lääkintätekniikkaan ja hankintayksikköön. Hankinnassa voi olla kyse hankkeesta, puitesopimukseen perustuvasta hankinnasta, puitesopimuskilpailutuksesta tai suorahankinnasta. Puitesopimuskilpailutuksessa lääkintälaitteen hankinta kilpailutetaan julkisen hankintalain mukaan. Hankittavalle laitteelle määritetään vaatimukset ja vaatimusten pohjalta pyydetään lääkintälaitetoimittajilta tarjoukset. Vaatimukset täyttävän lääkintälaitteen osalta tehdään hankintapäätös.

Hankintaprosessissa kilpailutuksen osana lääkintälaitteita voidaan koekäyttää varmistamaan, että lääkintälaite soveltuu käyttötarkoitukseen ja täyttää vaatimukset. Vaatimuksena voi olla integraatio olemassa olevaan potilastietojärjestelmään. Koekäytön yhteydessä todennetaan että vaatimukset toteutuvat käytännössä.

7.1.2 Tilaus, asennus ja vastaanottotarkistus

Hankinnasta tehdään hankintapäätös, jonka perusteella tehdään tilaus. Päätös voi perustua kilpailutukseen, puitesopimukseen tai se voi olla suorahankinta. Laitetoimittaja ottaa vastaan tilauksen. Laitetoimittaja toimittaa laitteen sairaalaan valmiiksi koottuna ja käyttökuntoon asennettuna. Laitetoimittaja sopii vastaanottotarkistuksesta

lääkintätekniikan kanssa, joka tarkistaa laitteen olevan tilauksen mukainen ja täyttävän laitteelle määrätyt vaatimukset. Lääkintätekniikka suorittaa lääkintälaitteelle sähköturvallisuusmittaukset, joilla varmistetaan lääkintälaitteen sähköturvallisuus potilaalle ja lääkintälaitetta käyttävälle hoitohenkilökunnalle. Lääkintälaite rekisteröidään lääkintätekniikan laiterekisteriin.

7.1.3 Määräaikaishuollot ja vian korjaukset

Vastaanottotarkistuksen jälkeen laite otatetaan käyttöön. Yleensä lääkintälaitehankinta sisältää käyttökoulutuksen, johon hoitohenkilökunta ja lääkintätekniikan asiantuntija osallistuvat. Lääkintälaitteelle tehdään valmistajan ilmoittamat määräaikaishuollot ja tarvittaessa vian korjaukset asiantuntevan ja koulutetun henkilön toimesta, määräaikaishuollot ja viankorjaukset voi suorittaa laitetoimittaja, valmistaja tai lääkintätekniikka.

Tyypillisiä määräaikaishuoltovälejä lääkintälaitteille ovat 12 ja 24 kuukautta. Jos lääkintälaitteelle ei ole määritetty huoltoväliä käytetään 36 kuukautta määräaikaishuoltovälinä. Määräaikaishuollon yhtenä tärkeimpänä osana on sähköturvallisuusmittaus laitteelle tehtävien muiden huoltotoimien lisäksi. Sähköturvallisuusmittaus varmentaa että laite on sillä hetkellä sähköturvallinen käyttää. Mittaustulosten huononeminen eli vuotovirtojen kasvu voi indikoida laitteen turvallisuuden heikentymistä.

7.1.4 Lääkintälaitteen poistaminen

Kun laitetta ei ole kannattavaa korjata tai lääkintälaitteeseen ei saa varaosia tai tarvikkeita, laite poistetaan käytöstä ja romutetaan. Asiakas voi poistattaa käytöstä tarpeettomia tai käyttötarkoitukseen sopimattomia laitteita, jotka kierrätetään toiseen yksikköön ”laitepörssin” tai lainalaitteiden muodossa. Lääkintälaitteen poistoikä on keskimäärin 8 vuotta.

7.2 Tietokoneen elinkaaren vertaaminen lääkintälaitteen elinkaareen

Käyttöjärjestelmän elinkaarella tarkoitetaan aikaa käyttöjärjestelmän julkaisusta käyttöjärjestelmän tuen loppumiseen. Yleisesti käyttöjärjestelmän tuen loppuminen tarkoittaa, ettei käyttöjärjestelmälle tule uusia tietoturvapäivityksiä. Tietoturvapäivitykset korjaavat käyttöjärjestelmässä olevia ohjelmointivirheitä, jotka saattavat muodostaa tietoturva-aukon, jota haittaohjelma tai hakkeri voi hyödyntää.

Tietokoneen elinkaari on samanlainen kuin lääkintälaitteen elinkaari. Tietokoneiden elinkaarenhallinta pitää sisällään tilaamisprosessin, käyttöönoton asennuksineen, käytönaikaisen tuen ja sovellusten ylläpidon sisältäen ohjelmistoinvestoinnit. Tietokoneen poistuessa käytöstä tietokone hävitetään tietoturvallisesti.

Lääkintälaitteen elinkaari ei lopu käyttöjärjestelmän tuen loppumiseen tai tietokoneen takuun loppumiseen. Lääkintälaitevalmistaja on saattanut määritellä lääkintälaitejärjestelmän tietokoneen käyttöjärjestelmineen kun laite on tuotu markkinoille. Valmistaja korjaa vain potilasturvallisuuteen vaikuttavat viat ohjelmistoissa tai käyttöjärjestelmässä.

Sairaalassa oli vuonna 2016 kaksi lääkintälaitehankintaa joissa tietokoneen käyttöjärjestelmä oli Windows xp. Laitteet olivat potilaan hoitoon soveltuvimmat laitteet ja vanhentunut käyttöjärjestelmä ei ole perustelu syy kieltää laitehankintaa. Toisessa tapauksessa lääkintälaitevalmistaja oli huomioinut tämän ja kieltänyt lääkintälaitteen liittämisen verkkoon. Toisessa tapauksessa laitteen olisi saanut liittää sairaalan verkkoon, huolimatta että laite ei ole tietoteknisessä mielessä turvallinen. Laitetoimittajista toinen on päivittänyt laitteiston tukemaan Windows 7 käyttöjärjestelmää. Kyseisiä laitteita ei liitetty sairaalan verkkoon.

Lääkintälaitteiden tukemat käyttöjärjestelmät ovat yleensä jäljessä yleistä käyttöjärjestelmien julkaisutahtia. Sairaalan siirryttäessä 2014 Windows XP käyttöjärjestelmästä Windows 7:ään. Osa lääkintälaitetoimittajista julkaisi Windows 7-yhteensopivat ohjelmistot keväällä 2014. Osa

laitteistoista ei saanut päivitettyä Windows 7:lle. Näitä laitteistoja poistettiin verkosta tai hankittiin tilalle korvaavia laitteita. Yleisesti Windows 10-tukea ei ole laajasti saatavilla. Markkinoilla on joitain uusia lääkintälaitteita, jotka ovat vain Windows 10-tuella varustettuja.

7.3 Hankintaprosessin nykytilan analyysi

Lääkintälaitteen hankinta lähtee osaston tarpeesta hankkia lääkintälaite potilaan hoitoa tai tutkimusta varten. Osasto on ottanut yhteyttä lääkintätekniikkaan. Lääkintätekniikasta on nimetty asiantuntija, joka tuntee laiteryhmän, johon hankinta kohdistuu. Lääkintätekniikan asiantuntija osaa arvioida halutun laitteen soveltuvuutta käyttöön luotettavuuden, ylläpidettävyyden ja laitteen huollon suhteen.

Sairaalassa on käytössä lääkintälaitteiden tarjousta pyydettäessä tai tilausta tehdessä liitteenä ”Tarjottavan lääkintälaitteen tekniset tiedot”-lomake. Lomakkeen tarkoitus on ollut saada laitetoimittajalta ennakkoon tieto koskien lääkintälaitteiden tietoturvaa ja tietoteknisistä tarpeista esimerkkinä tarve liittää lääkintälaite sairaalan tietoverkkoon tutkimusdatan siirtämiseksi potilastietojärjestelmään.

”Tietotekniset taustatiedot”-lomake ei ole ollut mukana jokaisessa tilauksessa, jolloin sen funktio ennakkotiedon saamisessa ei ole täyttynyt. Lomakkeen pohjalta on tietohallinnon prosesseihin saatu ennen laitteen käyttöönottoa heräte. Heräte on voinut tarkoittaa että lääkintälaitteen lisäksi sairaalaan tarvitaan vakioitu työasema potilastiedon purkua ja siirtämistä sairaalan tietojärjestelmiin, tai lääkintälaitteen liittämistä sairaalan verkkoon. Herätteen saatuaan tietohallinto on voinut toimittaa tarvittavat tietotekniset palvelut lääkintälaitteeseen liittyen.

Hankintaprosessissa ei ole ollut mukana tietohallinnosta nimettyä asiantuntijaa. Tämä on saattanut aiheuta kiireellisiä tietoteknisiä tuki tai hankinta pyyntöjä tietohallinnolle. Lääkintälaite on ollut tarve liittää verkkoon heti, koska laitetoimittajan asentaja on paikalla. Verkkoon liittäminen vaatii tiettyjä perustietoja koskien tietoliikenneyhteyksiä, mihin

verkon osaan laite liitetään ja tarvitaanko sairaalan vakioituun työasemaan ohjelmistoasennuksia.

7.4 Parannettu hankintaprosessi

Parannetussa hankintaprosessissa on korjattu vanhan hankintaprosessin puutteita. Osasto määrittelee hankintasuunnitelmassaan (LIITE 1 kohta 1) lääkintälaitteen verkkoon liittämisen tarpeen. Osasto ottaa yhteyttä, (LIITE 1 kohta 2) lääkintätekniikan asiantuntijaan ja tietohallinnon asiantuntijaan hankintasuunnitelman tekemiseksi, tavoitteena hankkia potilaan hoitamiseen tai tutkimiseen paras saatavilla oleva laitteisto. Hankintasuunnitelma menee hyväksyttäväksi. Hyväksynnän jälkeen hankintaa lähdetään toteuttamaan hankintasuunnitelman aikataulun mukaisesti. Jos lääkintälaite on verkkoon liitettävä, hankintadokumentteihin liitetään ”Tietotekniset taustatiedot”-lomake, joka on pakko täyttää. (LIITE 1 kohta 3.). Lääkintälaitteen verkkoon liittäminen toimii herätteenä tietohallinnolle asiantuntijan nimeämiselle hankinnalle. Tietohallinnon tuotantoprosesseista (LIITE 1 kohta 4) tulevat sairaalan yleiset tietoturva- ja tietotekniset vaatimukset, jotka ovat lähtökohtana lääkintälaitehankinnassa. Yleiset vaatimukset eivät kumminkaan saa estää potilaan hoidon kannalta parasta laitehankintaa.

Verkkoon liitettävän lääkintälaitteen hankintaspesifikaatioon osallistuu osaston kanssa lääkintätekniikan asiantuntija ja tietohallinnon asiantuntija. Hankintaan kuuluu (LIITE 1 kohta 5) lääkintälaitteen koekäyttö sairaalan verkossa. Tietohallinnon edustaja tekee työpyynnön tietohallinnon tuotantoprosesseille, jotka toteuttavat tarvittavat järjestelyt niin että koekäyttö voidaan toteuttaa. Tarjouspyyntö valmistellaan yhdessä osaston, hankintayksikön, lääkintätekniikan ja tietohallinnon kanssa. ”Tietotekniset taustatiedot”-lomake on pakollinen. Sairaalan tietoturva ja tietotekniset vaatimuksia on voitu määrittää kokonaan tai osittain hankintaspesifikaatioon. Hankintaprosessi, (LIITE 1 kohta 7) sisältää hankintailmoituksen julkaisun hankintayksikön toimesta, Laitetoimittajat tekevät tarjoukset, hankintayksikkö avaa tarjoukset ja tarkistaa tarjouksen

kelpoisuuden. Hankintayksikkö antaa hankintailmoituksen täyttävät tarjoukset vertailtavaksi.

Saadut tarjoukset vertaillaan (LIITE 1 kohta 8) osaton, lääkintätekniikan ja tietohallinnon näkökannasta. Vertailun osapuolet antavat kommentit tarjotun laitteiston soveltuvuudesta käyttöön. Vertailun pohjalta osasto tekee hankintapäätöksen, johon pyydetään puolto lääkintätekniikasta. Saadun puollon jälkeen hankintayksikkö tekee tilauksen (LIITE 2 kohta 9).

Tilauksen lähetyksen jälkeen lääkintätekniikka, tietohallinto ja laitetoimittaja aloittavat Tietoteknisen vuoropuhelun (LIITE 2 kohta 10). Vuoropuhelussa käydään läpi ”tietotekniset taustatiedot”-lomake, sairaalan tietoturva-, tietoteknisten vaatimukset, laitetoimittajan rajoitteet ja tarpeet. Vuoropuhelun perusteella hankittavaa laitteistoa koskien luodaan tarvittava dokumentaatio ja tietoturvaratkaisut niin, että laite on tietoturvallinen käyttää sairaalan verkossa. Vuoropuhelun on tarkoitus olla jatkuvaa laitetoimittajien ja sairaalan välillä että lääkintälaitteiden tietoturvaa voidaan parantaa.

Toimittaja ilmoittaa tilauksen vastaanottamisen jälkeen tietohallinnolle toimitusaikatauluarvion (LIITE 2 kohta 11). Tietohallinnon asiantuntija tilaa tarvittavat tietotekniset ratkaisut tietohallinnon tuotantoprosesseilta. Tilaukset tallentuvat tietohallinnon työnohjausjärjestelmään Lääkintälaitetoimituksen edetessä toimittaja (LIITE 2 kohta 12) ilmoittaa tarkan toimitusaikataulun tietohallinnon asiantuntijalle, joka tarvittaessa päivittää tuotantoprosessien tiketteihin aikataulun. Toimittaja sopii lääkintätekniikan kanssa vastaanottotarkistuksen (VOT) ajankohdan ja paikan.

Kun lääkintälaite on toimitettu sairaalaan (LIITE 2 kohta 14), toimittaja suorittaa yhteistyössä tietohallinnon kanssa tietotekniset asennukset kuten verkkoon liittämisen. Tarvittavat tiedot tallennetaan tietohallinnon rekisteriin. Lääkintätekniikan VOT-prosessi tarkistaa lääkintälaiteen täyttävän tilauksen ja laitteiston vaatimustenmukaisuuden. Vastaanottopöytäkirja toimitetaan hankintayksikköön (LIITE 2, kohta 15)

joka tarkistaa laskun ja vastaanottopöytäkirjasta toimituksen olevan tilauksen mukainen. Lääkintälaitteen tiedot tallennetaan lääkintätekniikan rekisteriin. Lääkintätekniikan ja tietohallinnon rekistereihin tallennetaan kummankin yksikön inventaarionumerot että rekisterimerkinnät osataan yhdistää toisiinsa (LIITE 2 kohta 16).

7.5 Dokumentoinnin parantaminen

Hankintaprosessin läpikäynnin yhteydessä huomattiin ”Lääkintälaitteen tietotekniset tiedot”-lomakkeen vaativan ajantasaistamista. Lomakkeesta puuttuivat lääkintätekniikan ja tietohallinnon asiantuntijan yhteystiedot koskien laitehankintaa jotka lisättiin uuteen lomakkeeseen (LIITE 3) Vanhalla lomakkeella tiedusteltiin lähes samat tiedot kuin uudella lomakkeella.

Uudessa lomakkeessa ensimmäisellä sivulla kysytään:

- Sisältääkö lääkintälaite tietokoneen vai tarvitaanko sairaalan työasema? (LIITE 4)
- Onko saatavilla analyysi/katselutyöasema/ohjelmistoa ja tarjotaanko sitä laitteen mukana? (LIITE 5)
- Saako lääkintälaitteen liittää verkkoon? (LIITE 6)
- Tarvitaanko etäyhteyttä laitteen ylläpitoon? (LIITE 6)
- Tarvitaanko erillistä palvelinta tai onko mahdollista hankkia erillinen palvelin? (LIITE 7)

Lomakkeen ensimmäiseltä sivulta saadaan suoraan tieto tarpeista ja kielloista. Jos kysymyksiin on vastattu kyllä, seuraavilla sivuilla kysytään tarkempia yksityiskohtia koskien lääkintälaitteen tietokonetta, erillistä analysointityöasemaa tai -ohjelmistoa, tarvetta verkkoyhteydelle, etäyhteydelle ja palvelimelle. Yksityiskohtien lisäksi kysytään toimittajan asiantuntijan yhteystiedot ja onko sairaalassa aiemmin liitetty lääkintälaite verkkoon, asennettu katseluohjelmisto, onko etäyhteyttä tai onko olemassa palvelinta. Laitetoimittajat tietävät lääkintälaitteet joita ovat toimittaneet aiemmin sairaalan, koska laki terveydenhuollon laitteista

määrää toimittajan pystyvän jäljittämään lääkintälaitteet, mikäli valmistajalta tulee lääkintälaitetta koskeva tiedote, jossa lääkintälaitteen potilasturvallisuuden todetaan vaarantuneen. Lomakkeella saadaan tätä kautta myös tieto sairaalassa olevista lääkintälaiteista, joita ei muuten tunnistettaisi.

8 LÄÄKINTÄLAITTEIDEN TIETOTURVAN PARANTAMINEN

Lääkintälaitteiden tietoturvaa voidaan parantaa monin tavoin. Yleisenä ohjeena pidetään, että laitevalmistajan pitää hyväksyä tietoturvan parantamiseen käytetyt ratkaisut. Tietoturvan parantamisen toimet, jotka kohdistuvat Windows-laitteisiin, mutta samoja periaatteita voidaan soveltaa muihin käyttöjärjestelmiin. Osa ratkaisuista pitäisi laitteen hankintaa suunnitellessa määrittää pakolliseksi vaatimukseksi. Tietoturvan parantamiseksi tehdyt toimet on hyvä dokumentoida ja dokumentointi tallentaa luotettavaan sijaintiin.

8.1 Koventaminen

Koventaminen tietokonelaitteistossa tarkoittaa ominaisuuksien ja asetusten tiukentamista normaalista. Koventamista voidaan toteuttaa laite ja ohjelmistotasolla.

8.1.1 Laitepohjainen koventaminen

Laitetasolla koventaminen tarkoittaa laitteiston asetusten tai ominaisuuksien muutamista tietoturvan parantamiseksi. Laitteen Bios/UEFI-asetuksissa määritetään laite käynnistymään vain paikalliselta kiintolevyltä. Estämällä käynnistäminen ulkoiselta medialta esimerkiksi USB-tikulta estetään kiintolevyllä olevaan tietoon käsiksi pääseminen. USB-tikulta käynnistettäessä, on mahdollista kopioida laitteeseen tallennettuja tietoja tai muokata laitteen asetuksia. On olemassa valmiita levykuvia, joiden avulla on mahdollista selvittää paikallisen administrator-tunnuksen salasana, ja saada tunnuksen ja salasanan avulla pääsy laitteeseen ylläpito-oikeuksin. Bios/UEFissa voidaan poistaa käytöstä tarpeettomat liitännät, jolloin vapaaseen porttiin liitetyllä USB-tikulta ei ole mahdollista tarpeettomasti kopioida tietoja. Laitteen käytön kannalta tarpeettomat verkkoliitynnät pitää deaktivoida, jolloin laitetta ei voida liittää verkkoon. Deaktivoimalla langattoman verkkokortin käyttöjärjestelmästä laitetta ei voi yhdistää langattomaan verkkoon. Bios/UEFiin tehdyt

muutokset suojataan määrittämällä Bios/UEFIin salasana, joka estää luvattoman asetusten muuttamisen.

8.1.2 Ohjelmistopohjainen koventaminen

Ohjelmistopohjaisessa koventamisessa pienennetään työasemaan kohdistuvaa hyökkäysrajapintaa. Ohjelmistopohjaisen koventamisen lähtökohdaksi voi ottaa: kaikki mikä ei ole laitteiston toimivuuden kannalta erikseen sallittua, on kiellettyä. Lähtökohtaisesti laitteistoon asennetaan vain käytön kannalta välttämättömät ohjelmistot. Kaikki palvelut, jota ei tarvita sammutetaan. Mitä enemmän ohjelmistoja tai palveluita on laitteistoon asennettu tai käytössä, niin sitä todennäköisempää on niissä olevan tietoturva-aukon hyödyntäminen. Laitteistolla ei lähtökohtaisesti ole tarvetta päästä internetiin tai sähköpostiin, jolloin laitteeseen ei asenneta selainta tai sähköpostiohjelmistoa. Internet-selaimista poistetaan laajennukset käytöstä, ellei niitä tarvita laitteiston käytössä. Internet ja sähköpostiliikenne estetään. Laitteiston ohjelmistopalomuuri aktivoidaan ja vain tarvittava liikenne sallitaan. Palomuurisäännöissä kaikki julkisesta IP-osoiteavaruudesta tuleva liikennöinti kielletään oletusarvoisesti.

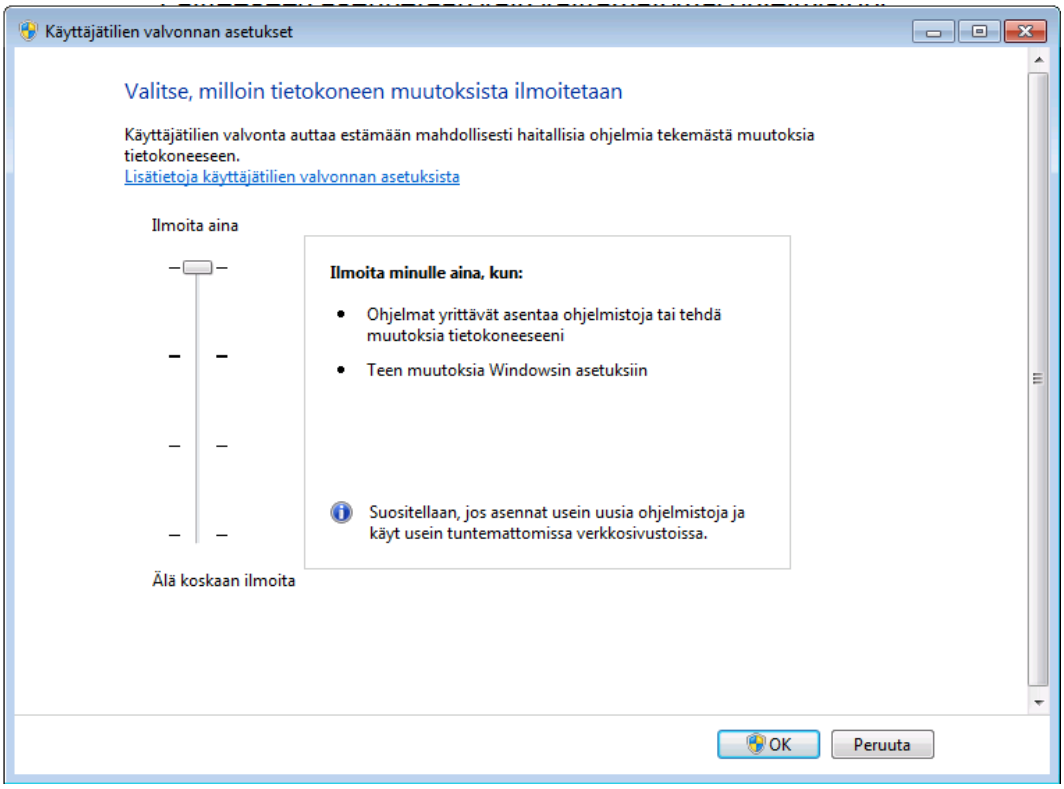
Laitteistosta otetaan ns. autoplay-toiminnallisuus pois. Autoplay ominaisuudella on lähtökohtaisesti helpotettu alun perin CD-ROM-levyillä olevien ohjelmien tai asennusohjelmien käynnistämistä. Käyttäjän ei tarvinnut hakea CD-asemasta oikeaa tiedostoa suoritettavaksi. Laitteisto käynnisti automaattisesti ohjelmiston CD-ROM-levyltä. Autorun-toiminnallisuus on CD-rom-levyjen lisäksi DVD-levyillä, USB-muistitikuilla ja ulkoisilla USB-asemilla. Aseman juuressa on autorun.ini josta Windows automaattisesti käynnistää määritellyn ohjelman. Haitta-ohjelmat hyödyntävät tätä toiminnallisuutta, jos sitä ei ole deaktivoitu. Laitteista määritellään kaikki etäkäyttöön liittyvät toiminnallisuudet pois käytöstä. Windows-laitteissa on oletuksena Remote Assistance päällä, joka mahdollistaa haitta-ohjelmille tai hyökkääjille yhden hyökkäysvektorin. Remote Assistancen lisäksi Remote Desktop-toiminnallisuus pitää deaktivoida. Windows laitteissa on DCOM-toiminnallisuus (Distributed

Component Object Model), joka mahdollistaa tietokoneen komponenttien kommunikoinnin verkon yli, jolloin tietokoneessa voidaan verkon yli suorittaa ohjelmia. Laitteiston käytön vaatiessa DCOM:n käyttöä, se sallitaan. Tällöin laitteen palomuurisäännöissä on huomioitava DCOM:n tarvitsemat portit ja mistä osoitteesta yhteys sallitaan laitteeseen.

8.1.3 Tunnukset ja käyttöoikeudet

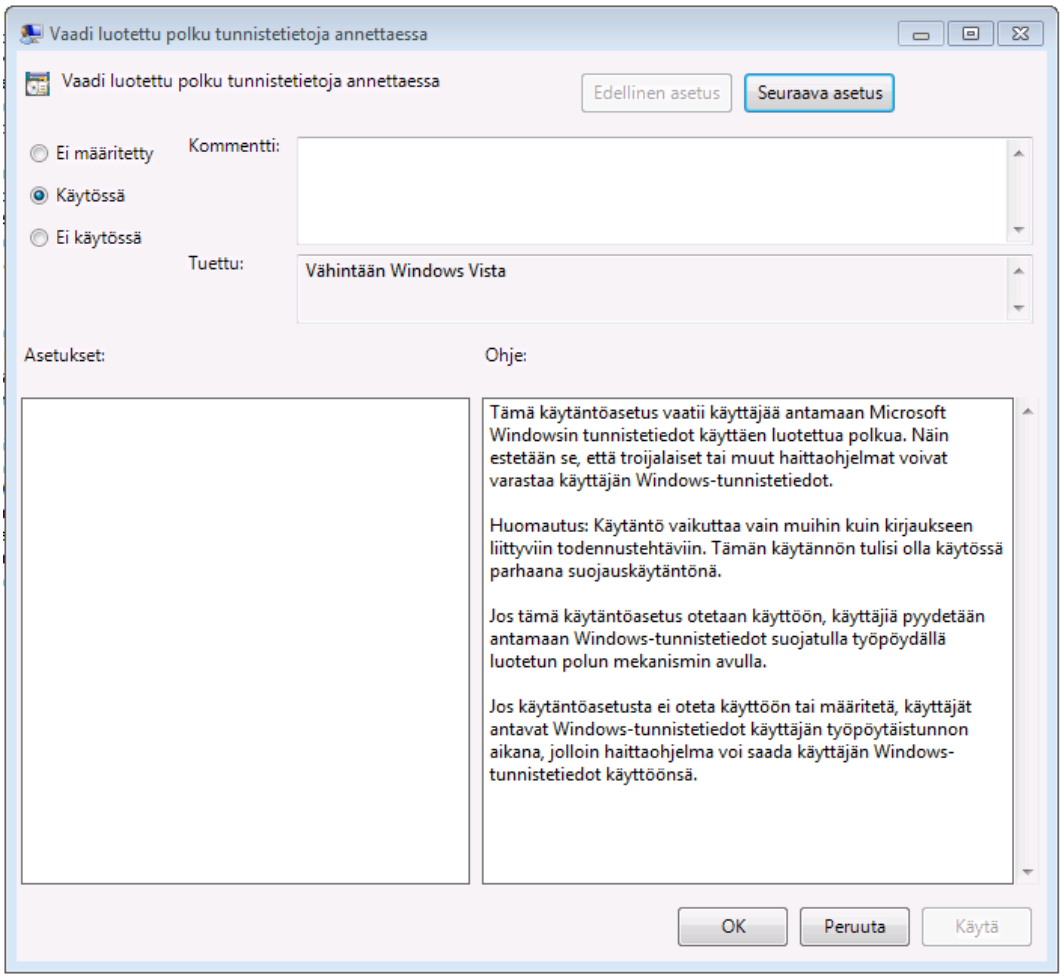
Laitteen kaikissa käyttäjätunnuksissa pitää olla salasana suojaus. Oletussalasanat pitää vaihtaa riittävän vaikeisiin. Laitteen asetuksista määritetään enimmäismäärä, kuinka monta kertaa käyttäjätunnus salasanayhdistelmän voi antaa väärin, ennen kuin tunnus lukkiutuu väliaikaisesti. Salasanasuojaus ja tunnusten lukittuminen hidastaa haitta-ohjelman tai hyökkääjän pääsyä koneelle. Salasanakäytännöt määrittää sairaalan tietoturvapolitiikka. Paikallisen järjestelmänvalvoja-tunnuksen (administrator) nimen vaihto suojaa laitteistoa, koska olemassa oleva oletustunnus ei ole tiedossa. Muut kuin käytössä olevat tunnukset deaktivoidaan, laitteiston käyttöön luodaan oma tunnus, jolla on käyttäjäoikeudet, ellei laitteiston käyttö vaadi ylläpito-tason tunnuksia. Tietokoneen paikallisen järjestelmänvalvojan (administrator-tunnuksen) deaktivointi domainiin liitetyssä tietokoneessa on haasteellinen tilanne. Jos Domainiin liitetyn tietokoneen paikallinen järjestelmänvalvoja-tunnus deaktivoidaan ja laite menettää luottosuhteen Domain-ympäristöön, tällöin laitteistoon on hyvin hankala päästä kirjautumaan ylläpito-tasoisin tunnuksin.

.

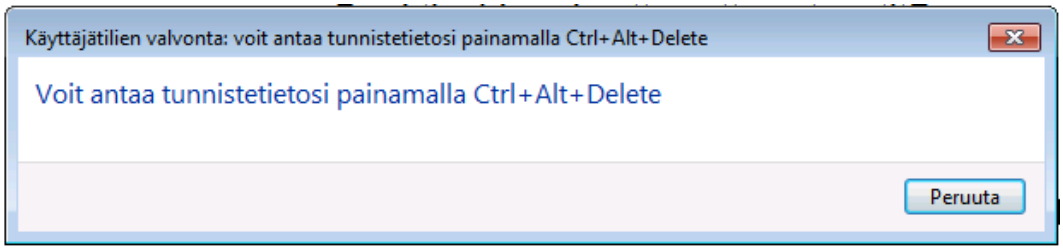


KUVIO 20. UAC-asetus

Windows Vistasta lähtien on Windows työasemissa ja Server 2008 lähtien palvelimissa ollut käyttäjätilien valvonta (User Access Control,UAC)(KUVIO 20) jolla voidaan määrätä pakolliseksi ylläpitotunnuksen tunnuksen ja salasanan antaminen vaikka käyttäjä olisi kirjautuneena tietokoneelle ylläpitotasoisilla tunnuksilla. Salasana varmistus tulee aina kun käyttäjä tekee muutoksia Windowsiin (muuttaa asetuksia/asentaa ohjelmia) tai ohjelmistojen tehdessä muutoksia tietokoneeseen. Ylläpitotasoisia tunnuksia voi suojata Group policyllä (KUVIO 21), joka pakottaa painamaan ”CTRL-ALT-DEL”-yhdistelmää (KUVIO 22) ennen käyttäjätunnuksen ja salasanan antamista. Tämä estää haittaohjelmia varastamasta käyttäjätunnuksia ja salasanoja ylläpitäjältä.



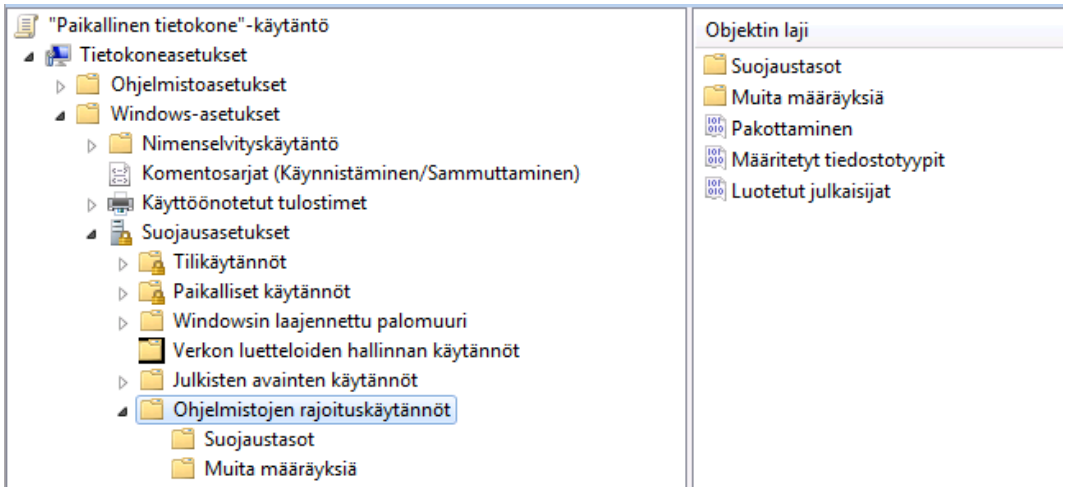
KUVIO 21. Crtl-Alt-Del hyväksynnän pakottaminen UAC:n yhteyteen



KUVIO 22. Ilmoitus CTRL-ALT-DEL yhdistelmänpainamisesta

Windowsin Software Restriction Policyllä voidaan rajoittaa mistä kansioista ohjelmistoja voidaan käynnistää ja minkä tyyppiset tiedostot on sallittua avata. Määrityksiä ovat (KUVIO 23): Suojaustaso joka määrittää voiko ohjelmiston käynnistää minkä tasoisilla oikeuksilla. Oletustasolla ohjelmistojen käyttöä ei rajoiteta. Tiukin rajoitus sallii ohjelmistojen käynnistämisen vain sallituilla ehdoilla, kaikki muut on kielletty. Suojaustasot asetuksella määritetään käyttäjän käyttöoikeuksien vaikutus sallittuihin ohjelmiin, jotka käyttäjä voi käynnistää. Ei Sallittu asetuksin, käyttäjä ei voi käynnistää ohjelmaa, jos ohjelmistoa ei ole erikseen sallittu. Oletuksena käyttäjän käyttöoikeudet periytyvät sovellukselle. Näiden kahden tason välissä ohjelma käynnistyy aina käyttäjätason oikeuksin riippumatta käyttäjän oikeuksista. Muita määrityksiä-asetuksissa suojaustason määritykset kohdennetaan oletuksena vain järjestelmä-kansioihin. Oletuksena on sallittu ohjelmistojen oletus asennuskansiosta: C:\Program Files ja C:\Program Files (x86). Kansioiden asetuksissa on määritetty ohjelman käynnistys oletuksena käyttäjän oikeuksin. Muut määritykset kohtaan lisätään ohjelman asennuskansio, jos se on joku muu sijainti kuin oletus asennuskansio. Määritetyt tiedostotyypit asetuksella määritetään, mitä tiedostotyyppejä kohdellaan avatessa kuin ne olisivat

ohjelmistoja.



KUVIO 23. Software Restriction Policy

Asetuksista pakottaminen voidaan määrityksen pakottaminen asettaa koskemaan kaikkia ohjelmatiedostoja, niiden käyttämiä ohjelmakirjastoja ja paikallisia järjestelmänvalvojia.

8.1.4 Tietoturvaohjelmistot

Laitevalmistaja määrittää sallitut virustorjuntatuotteet. Lähtökohtaisesti sairaalan käytössä oleva virustorjuntaohjelmisto kelpaa. Perustellusta syystä laitevalmistaja voi ilmoittaa, että käytetään muuta tuotetta. Verkkoon liitettävän laitteiston osalta sairaalan pitää määrittää virustorjuntaohjelmisto pakolliseksi laitteisiin, johon sen asentaminen on teknisesti mahdollista. Laitetta käytettäessä ilman verkkoa ei ole mahdollista päivittää virustorjuntaohjelmiston tunnistetietoja aktiivisesti, jolloin virustorjunta ei voi tunnistaa uusia uhkia. Sairaalan toimistotyöasemille on hankittu keskitetysti hallittu virustorjunta-ohjelmisto.

Taulukosta 2 ilmenee keskeisimmät erot paikallisesti asennetun ja keskitetysti hallitun virustorjuntaohjelmiston välillä. Keskitetysti hallitun virustorjunnan suurimmat edut ovat ohjelmiston toiminnan valvonta, hälytykset näkyvät muuallakin kuin paikallisesti ja hälytyksistä saadaan keskitetty raportti. Keskitetysti hallittu virustorjuntaohjelmisto on määritellyin väliajoin yhteydessä hallintajärjestelmään hakeakseen uusia

päivityksiä tai asetuksia. Kommunikointia hallintajärjestelmän välillä seurataan. Jos laitteisto on selvästi käytössä, mutta virustorjunta ohjelmisto ei ole kommunikoinut hallintajärjestelmän kanssa, virustorjuntaohjelmisto vaatii mahdollisesti paikallisesti tehtävän tarkistuksen. Virustorjuntaohjelmisto myös ilmoittaa hälytykset ja havainnoinnin hallintajärjestelmään, josta saadaan keskitetty raportti kaikista hälytyksistä. Paikallisen asennuksen etuna on käytännössä, että voidaan valita vapaasti käytettävä tuote. Haittapuolena on se, että kukaan ei valvo ohjelmiston toimintaa ja hälytykset näkyvät vain paikallisesti. Tietoturvariskiä kasvattaa päivitysten hakeminen internetistä.

TAULUKKO 2. Paikallisesti ja keskitetysti hallitun virustorjunnan erot

Paikallinen virustorjunta ohjelmiston asennus	Keskitettysti hallittu virustorjunta
Voidaan käyttää mitä tahansa soveltuvaa tuotetta	Yleensä rajoittuu sairaalassa yleisesti käytettyyn tuotteeseen
Päivitykset yleensä vaativat pääsyn internettiin	Keskitetyt päivitykset hallintajärjestelmän kautta
Asetukset määritettävä paikallisesti	Asetukset voidaan määrittää keskitetysti
Ohjelman toimintaa ei valvota	Ohjelmiston toimintaa valvotaan
Hälytykset vain paikallisesti	Hälytykset keskitettyyn järjestelmään
Hälytyksistä ei raporttia	Hälytyksistä rapotti

8.1.5 Windows-tietoturvapäivitykset

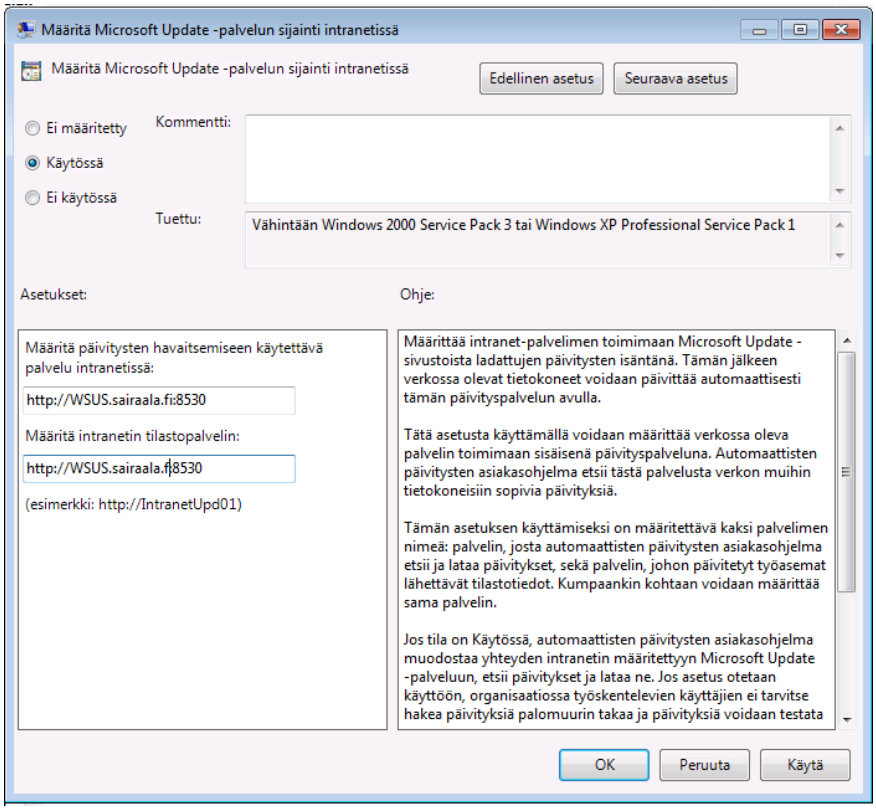
Yksikertaisimmillaan normaaleissa Windows työasemissa Microsoftin julkaisemat tietoturva päivitykset asentuvat automaattisesti Windows update-toiminnallisuudella, ilman että käyttäjän tarvitsee valita mitään.

Sairaalassa käytettäviä ohjelmistoja on paljon. Osa sovelluksista on normaaleja toimistosovelluksia, osa sovelluksista on potilaan hoidossa tai diagnostiikassa käytettyjä potilastietojärjestelmiä. Microsoftin julkaisemat tietoturvapäivitykset testataan julkaisun jälkeen, etteivät ne aiheuta ongelmia ohjelmien toimivuuden kanssa. Osa työasemista on työasemia,

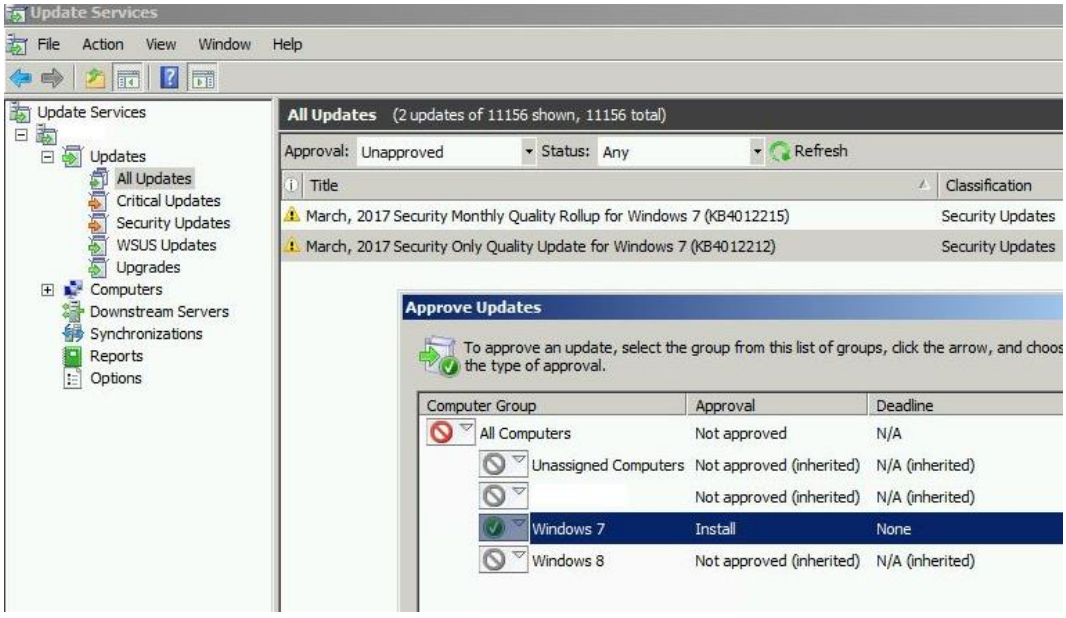
joilla tietoturvapäivitykset pilotoidaan, ennen kuin kaikki sairaalan työasemat päivitetään. Yksikertaisimmillaan Active Directoryn Group Policyllä määritetään, että työasemat hakevat tietoturvapäivitykset WSUS-palvelimelta. WSUS-palvelmille on määritetty pilottikoneet ja loput koneet. Tietoturvapäivitykset hyväksytään ennen kuin ne voidaan asentaa työasemiin.

Tietoturvapäivitysten asentaminen on hankalampaa lääkintälaitteisiin kuin normaaleille sairaalan työasemille, koska lääkintälaitteisiin asennettavat sovellukset ja päivitykset pitää hyväksyttää laitetoimittajalla tai laitevalmistajalla. Lääkintälaitteeseen asennettu hyväksymätön tietoturvapäivitys saattaa vaarantaa potilasturvallisuuden. Osassa lääkintälaitteista laitteen huoltomanuaalissa saattaa lukea, että Windows updatesta pitää olla asennettuna kaikki päivitykset ennen lääkintälaiteen sovellusohjelmiston asennusta. Yleensä laitevalmistaja auditoi päivitykset ennen kuin ne voidaan asentaa työasemille.

Lääkintälaitteisiin, jotka eivät ole Active Directoryssä voidaan paikallisiin Group policyn (KUVIO 24) avulla määritellä Windows updaten sijaan kohteeksi WSUS-palvelin. WSUS-palvelimelta päivitykset voidaan aktivoida tietylle koneryhmälle (KUVIO 25). Tarvittaessa tietoturvapäivitykset voidaan pilotoida pienessä määrässä lääkintälaitteita. Mikäli pilotoinnissa ei ole esiintynyt ongelmia liittyen tietoturvapäivityksiin, niin tietoturvapäivityksiä voidaan laittaa jakeluun loppuihin lääkintälaitteisiin porrastetusti, tai jättää tietyt päivitykset jakelematta.



KUVIO 24. Group policy WSUS-asetukset



KUVIO 25. Tietoturvapäivityksen hyväksyntä WSUS-palvelimella

Osa lääkintälaitteista on täydellisessä toimittajan ylläpidossa, jolloin vain laitetoimittajan sertifioimat huoltohenkilöt saavat muuttaa laitteiston asetuksia. Mahdolliset tietoturvaohjelmistot ja tietoturvapäivitykset

hyväksytään asennettavaksi huoltohenkilöiden toimesta vasta tehtaan testauksen ja hyväksynnän jälkeen. Tietoturvapäivityksen hyväksyminen voi kestää 3 - 6 kuukautta.

8.2 Työasemaratkaisut

Lomakkeen perusteella selvitetään millainen tietokone lääkintälaite on tai millaisen tietokoneen se tarvitsee. Lomakkeella huomioidaan mahdollinen analysointi/katseluohjelmisto tai -työasema. Tietokone voi olla sairaalan vakioitu työasema, sairaalan Active Directoryyn liitetty työasema tai muu työasema

8.2.1 Sairaalan vakioitu työasema

Vakioitua työasemaa voidaan käyttää tapauksissa, joissa potilaalle ei aiheudu vaaraa tai kohtuutonta haittaa, mikäli tietokonetta kohtaa tietoturvapoikkeama. Käytännössä tämä tarkoittaa tutkimuksia, joissa lääkintälaite mittaa potilaasta määriteltyä parametria ja tutkimusdata tallennetaan potilastietojärjestelmään. Tietokone voi olla sairaalan tai laitetoimittajan työasema. Laitetoimittajan työaseman on sovelluttava vakioitavaksi.

Vakioidun työaseman käyttö tuo vaatimuksia kokonaisuudelle:

- Tietokoneen käyttöjärjestelmän asennus asennusjärjestelmän avulla
  Käyttöjärjestelmä Windows 7 Enterprise
- Kokonaisuuden on toimittava käyttäjätason tunnuksin
- Kokonaisuuden toimivuus testataan sovellustestauksessa.
- Tietokoneessa on sairaalan tietoturvaohjelmisto
- Tietokoneeseen asennetaan tietoturvapäivityksiä säännöllisesti
- User Access Control (UAC) on tietokoneessa aktiivinen
- Tietokoneella on sairaalan perusohjelmisto asennettuna.
  Perusohjelmistoon kuuluvat toimistosovellukset, sähköposti,

internet-selain ja pääsy Internetiin. potilastietojärjestelmän ohjelmistot
- Tietokoneelle ei saa tallentaa paikallisesti potilastietoja
- Tietokoneen kiintolevy on salattu
- Tietokoneen palomuuri on päällä

8.2.2 Sairaalan Active Directoryyn liitetty työasema

Lääkintälaitejärjestelmän tietokone liitetään sairaalan Active Directoryyn, joka sisältää keskitetyn hallinnan koskien virustorjuntaa ja tietoturvapäivitysten jakelua. Erona vakioituun tietokoneeseen on potilaalle aiheutuvan vaaran tai haitan suurempi riski tietoturvapoikkeaman osalta. Lääkintälaitteissa voi olla myös rajoituksia tietoturvapäivitysten jakeluaikatauluissa johtuen lääkintälaitevalmistajan tietoturvapäivitysten validointi käytännöistä.

Sairaalan Active Directoryyn liitetyn työaseman käyttö tuo vaatimuksia kokonaisuudelle:

- Tietokoneen käyttöjärjestelmä asennetaan asennusjärjestelmästä tai käyttöjärjestelmä on asennettu käsin. Windows 7 Enterprise tai Pro
- Lähtökohtaisesti kokonaisuuden on toimittava käyttäjätason tunnuksin.
- Tietokoneessa on sairaalan tietoturvaohjelmisto.
- Tietokoneeseen asennetaan tietoturvapäivityksiä säännöllisesti. Valmistaja hyväksyy tietoturvapäivitykset kohtuullisella aikataululla.
- User Access Control (UAC) on tietokoneessa oletuksena aktiivinen
- Tietokoneeseen ei asenneta mitään ylimääräisiä ohjelmistoja kuin valmistajan hyväksymät
- Tietokoneella ei ole pääsyä Internettiin tai sähköpostiin.
- Paikallisesti potilastietojen tallennusta ei suositella
- Tietokoneen kiintolevy on oletuksena salattu
- Tietokoneen palomuuri on päällä

Lääkintälaiteen rooli potilaan hoidossa on kriittinen, lääkintälaiteen toiminta häiriö voi aiheuttaa potilaalle vamman tai hoitoketjun viivästyminen voi aiheuttaa vamman. Liitetyt tietokoneet ovat omassa AD-haarassa, jossa voidaan pienelle joukolle koneita sallia poikkeuksia oletus asetuksiin. Laitteet ovat normaalissa lääkintälaiteverkossa, jossa erikseen on sallittu liikennöinti tarvittaviin palvelimiin.

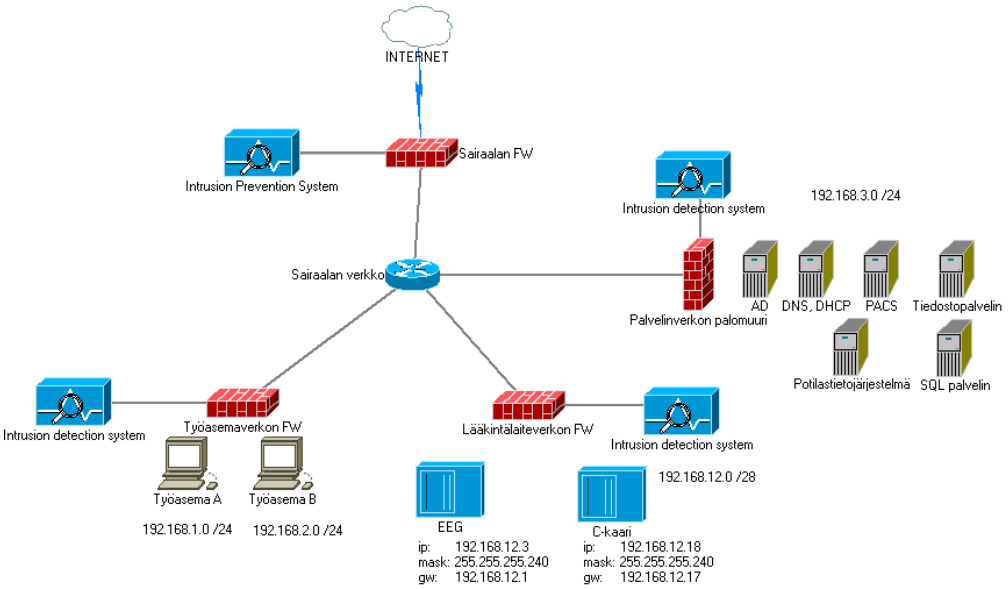
8.2.3 Muut työasemat

Muut työasemat kategoriaan menevät kaikki lääkintälaitteet joita ei voida liittää sairaalan vakioituun työasemaan tai liittää sairaalan Active Directoryyn. Laitetoimittaja voi kieltää laitteen liittämisen Active Directoryyn, kieltää virustorjuntaohjelmisto asennuksen tai kieltää tietoturvapäivitysten asentamisen. Laite voi olla teknisesti mahdoton liittää Active Directoryyn.

Laitteet ovat kovennetussa lääkintälaiteverkossa, josta on sallittu vain minimi liikennöinti lääkintälaiteverkosta ulospäin. Laitteille määritetään lääkintälaiteverkon palomuuriin sallitut kohdeosoitteet, -portit ja tietoliikenneprotokollat sallituiksi joita tarvitaan potilaan hoidossa tarvittavan tai tuotettavan tiedon tallentamiseen sairaalan tietojärjestelmiin.

9 SAIRAALAN TIETOVERKKO JA LÄÄKINTÄLAITEVERKKO

Sairaalan verkkoon on (KUVIO 26) liitetty työasemat, palvelimet ja lääkintälaitteet. Sairaalan sisäverkon ja julkisen verkon välissä on palomuuri, jota valvoo tunkeilijantorjuntajärjestelmä (IPS). IPS voi tietoturvauhan uhatessa käynnistää torjuntatoimenpiteet automaattisesti, pahimmassa tapauksessa irrottaa sairaalan sisäverkon internet-yhteydestä. Sairaalan tietohallinto ylläpitää ja valvoo verkkoa, työasemia ja palvelimia. Työasemat, palvelimet ja lääkintälaitteet on jaettu omiin verkkoihin, jotka on suojattu omin palomuurein. Verkkoja valvotaan tunkeilijan havaitsemisjärjestelmin. Palomuurit on määritelty sallimaan yhteyden avaamisen verkon sisältä ja väliaikaisesti tallentavat ACL:n palaavan tietoliikenteen säännöt. Tällöin palomuuriin ei tarvitse määrittää kiinteillä säännöillä tietoliikenneyhteyden paluuliikennettä. Esimerkissä sairaalan verkkoon liitetään kolme lääkintälaitetta ja yksi katselutyöasema. Lääkintälaitteet liitetään kolmella eri tavalla sairaalan verkkoon. Spirometrialaite käyttää sairaalan vakioitua työasemaa. EEG-laite integroidaan sairaalan Active-Directoryyn ja EEG-tutkimuksia voidaan katsella vakioidulta työasemalta. C-kaarta ei voida integroida sairaalan Active Directoryyn.



KUVIO 26. Sairaalan verkko

Sairaalan verkkoon on määritetty kaksi työasema verkkoa, palvelimille oma verkko ja kaksi lääkintälaiteverkkoa (TAULUKKO 3). Työasemaverkkoihin liitetään vain sairaalan vakioituja työasemia. Työasemat saavat IP-osoitteen DHCP-palvelimelta. Vlan100 on tarkoitettu yleiseksi työasemaverkoksi, josta on pääsy internetiin ja palvelinverkkoon. Vlan101 on työasemaverkko, josta on lisäksi pääsy lääkintälaiteverkkoihin. Tällä toimella rajataan pääsy lääkintälaiteverkkoihin vain työasemille joilla on oikeasti tarve. Palvelimet ovat oman palomuurin suojassa Vlan102:ssa. Sairaalan verkkoon liitetyt lääkintälaitteet tarvitsevat kolmea palvelinta joiden IP-osoitteet on annettu taulukossa 4. Spirometrialaite tarvitsee yhteyden SQL-palvelimen toimiakseen. EEG-laite tarvitsee yhteyden SQL- ja tiedostopalvelimen. C-kaari tarvitsee yhteyden PACSiin. Sairaalassa on kaksi lääkintälaiteverkkoa: Vlan103 ja Vlan104. Vlan103 on EEG-laitteille tarkoitettu verkko, jossa on sallittu oletuksena Active Directoryn tarvitsemat tietoliikenneyhteydet, koska EEG-laite liitetään sairaalan Active Directoryyn. Vlan104 on RTG-laitteille tarkoitettu verkko, josta sallitaan vain minimiliikenne palvelinverkkoon. Lääkintälaiteverkkojen aliverkot on luotu käyttämään VLSM:ää, joka mahdollistaa IP-osoiteavaruuden tehokkaan hyödyntämisen, jolloin ei tuhlata IP-osoitteita.

TAULUKKO 3. Sairaalan Vlanit ja ip-osoiteavaruudet

192.168.1.0 /24	Vlan100	työasema verkko 1
192.168.2.0 /24	Vlan101	työasema verkko 2
192.168.3.0/24	Vlan102	Palvelinverkko
192.168.12.0 /28	Vlan103	Lääkintälaiteverkko EEG
192.168.12.16 /28	Vlan104	Lääkintälaiteverkko RTG

TAULUKKO 4. Sairaalan palvelimet

Palvelimet	
192.168.3.2 /24	SQL-palvelin
192.168.3.3 /24	Tiedosto-palvelin
192.168.3.4 /24	PACS

9.1 Sairaalan vakioitua työasemaa hyödyntävä USB-liitäntäinen spirometrialaite

Spirometria laite on USB-liitäntäinen lääkintälaite, joka liitetään USB-liitännällä sairaalan vakioituun työasemaan, jolloin toteutuu toiminnallinen yhteys. Spirometrialaite muodostaa tietokoneen kanssa lääkintälaitejärjestelmän, jolloin on huomioitava lääkintälaitejärjestelmiä koskevat vaatimukset. Lääkintälaitteen potilasliityntä on BF-tyyppiä. Potilas ja laite ovat yhteydessä toisiinsa 2 metriä pitkällä sähköäjohtamattomalla letkulla, vuotovirtoja tällöin ei ole mahdollista muodostua. Periaatteessa lääkintälaite on mahdollista viedä pois hoito-alueelta. Normaalisti tietokone ja näyttö saavat sähkönsä omista pistokkeista, koska kyseessä on lääkintälaitejärjestelmä. Hyväksytyt toteutukset ovat seuraavat:

- Käytetään Medical-hyväksyttyä tietokonetta,
- Käytetään kannettavaa tai niin sanottua All-in-one-tietokonetta, Käytettäessä kiinteää verkko yhteyttä on verkkoliitäntä isoloitava Medical-hyväksytyllä verkkoerottimella,
- Tietokone ja näyttö saavat sähkönsä MSO:n kautta. Verkkoliityntää käytettäessä kiinteää yhteyttä isoloitava Medical-hyväksytyllä verkkoerottimella,

- Lääkintälaite on liitetty Medical hyväksytyllä USB-erottimella tietokoneeseen.

Spirometrilla voidaan diagnosoida potilaan keuhkojen toimintahäiriöitä. Yleisimmät tutkittavat vaivat ovat keuhkoputken ahtautuminen ja keuhkotilavuuden pieneneminen. Spirometrilla voidaan arvioida astmalääkityksen riittävyyttä. Tutkimukset tehdään spirometrilaitteella ja ohjelmistolla. Tutkimukset tallennetaan keskitettyyn tietokantaan. Raportit tallennetaan potilastietojärjestelmiin. Ennen laitteiston hankintaa oli sairaalassa aloitettu ohjelmiston päivittäminen uuteen versioon. Laitteisto saapui, kun päivitettyä versiota oltiin pilotoimassa.

Laitteen hankintahinta ei ylitä kilpailutusrajaa, jolloin hankinta tapahtuu suorahankintana hankintayksikön kautta ja ”lääkintälaitteen tietotekniset tiedot”-lomake täytetään. Lomakkeesta ilmenee, että laite tarvitsee sairaalan tietokoneen ja että sairaalassa on keskitetty tietokanta spirometriatutkimuksille. Laitetoimittaja pystyy nimeämään sairaalan teknisen asiantuntijan.

9.1.1 Riskianalyysi spirometrialaitteesta

Spirometria-laitteistolle tehtiin riskianalyysi, jossa arvioitiin, mitä vaikutusta potilaan hoitoon on tiedon muuttumisella, käytön estävällä vialla ja tietoliikennevialla. Tiedon muuttuminen kuvastaa haitta-ohjelman tai hakkerin muuttaneen tutkimuksen tietoja. Käytön estävä vika kuvastaa tilannetta, jossa haittaohjelma on muuttanut laitteiston käyttökelvottomaksi. Tietoliikennevika kuvastaa tilannetta, jossa sairaalan tietoliikenneverkko on hakkerin toimista johtuen käyttökelvoton.

Tiedon muuttaminen: Potilaan tutkimustulokset analysoi lääkäri, joka katsoo kokonaiskuvaa potilaan terveydentilasta. Mikäli kliiniset oireet eivät vastaa potilaan terveydentilaa, niin potilaalle määrätään uusintatutkimus tai lisätutkimuksia. Hoitaja pystyy arvioimaan tutkimuksen laatua ja potilaan yhteistyökykyä. Laitteen kalibrointi tarkistetaan ennen jokaista potilasta.

Käytön estävä: Tutkimuksen tekeminen ei onnistu ollenkaan tai potilaalle tehtävä tutkimus epäonnistuu. Potilalle aiheutuva haitta on tutkimuksen siirtäminen toiseen ajankohtaan tai tutkimuksen uusiminen.

Tietoliikennevika: Tietoliikennevian sattuessa laitteisto toimii niin sanotussa stand-alone-tilassa, jolloin tutkimuksia voidaan tehdä tallentamalla tutkimustulokset väliaikaisesti tietokoneelle. Tutkimukset siirtyvät tietokantaan, kun verkkoyhteys tietokantapalvelimelle toimii taas. Tietoliikenneviasta ei aiheudu haittaa potilaalle.

9.1.2 Vaatimukset ja tietoturvamääritykset

Spirometrialaitteen kanssa päätettiin käyttää sairaalan vakioitua työasemaa, joka on liitetty sairaalan työasemaverkkoon 1. Tietokone saa IP-osoitteen sairaalan DHCP-palvelimelta. Laitteistovaatimuksena on Windows 7 (32- tai 64-bittinen versio), laajakuvanäyttö ja 1 vapaa USB-portti. Käytännössä mikä tahansa moderni tietokone täyttää vaatimukset.

Laitteistovaatimukset:

- Windows 7 32- tai 64-bittinen
- laajakuvanäyttö
- prosessori 1 Ghz
- muisti 2 Gt tai enemmän
- 1 vapaa USB-portti.

Laitetoimittaja ilmoitti, että ohjelmisto toimii käyttäjätason tunnuksin, jolloin se täyttää vaatimukset sairaalan vakioidun työaseman käytön edellytykset. Käyttöoikeuksista kaikki oikeudet tarvitsi antaa vain ohjelmiston asennuskansiossa settings.ini-tiedostoon ja paikallisille tietokannoille, joita käytetään, kun ohjelmistolla ei ole yhteyttä SQL-palvelimeen. SQL-palvelin oli jo valmiiksi työasemien sallitun liikenteen säännöissä. Virustorjunnasta laitetoimittaja ilmoitti, että ohjelmiston asennuskansiota ja paikallisia tietokantoja ei saa skannata käytön aikana.

Tietoturvaan liittyvät vaatimukset:

- Virustorjuntaohjelmisto ei saa skannata ohjelman asennuskansiota ja Offline-toiminnallisuuden paikallisia tietokantoja.
- Käyttäjä tarvitsee kaikki oikeudet asennuskansiossa settings.ini tiedostoon ja Offline-toiminnallisuuden tietokantojen kansioon
- Tietoturvapäivitykset saa asentaa
- tietokoneen palomuuriin tarvitsee avata SQL-tietokantan käytön vaatimat portit,
- Ohjelmisto toimii käyttäjätason tunnuksin.

9.1.3 Testaus ja asennusprosessi

Spirometria-ohjelmisto on testattu toimivaksi sairaalan vakioiduilla työasemilla. Ohjelmistotestauksella varmistetaan ohjelmiston toimivuus sairaalan vakioidussa työasemassa ja testataan yhteensopivuus muiden sairaalassa käytettävien ohjelmistojen kanssa. Spirometria-tutkimuksia on tehty ohjelmiston vanhoilla versioilla sairaalassa vuosia, jolloin käyttöympäristö on tiedossa. Käyttöympäristön tuntemuksen johdosta ohjelmistojen yhteensopivuustestauksia täytyi toteuttaa vain niille sovelluksille, jotka olivat käytössä lääkintälaitekäytössä olevilla työasemilla ja lääkärien työasemilla, joihin oli asennettu ohjelmiston katseluversio.

Ohjelmistoasennus on paketoitu, jolloin ohjelmisto voidaan asentaa asennusjärjestelmästä, tai lähituki voi käynnistää ohjelmiston työasemalle ohjelmistokirjastosta käsin. Sovelluspaketoinnissa ohjelmiston asennus automatisoidaan yleensä MSI-paketoituun sovellukseen MST-tiedostolla, jossa on vastaukset asennuksen aikaisiin kysymyksiin.

Ohjelmiston lisenssit on tallennettu keskitettyyn tietokantaan, ja vain ensimmäisen kerran katseluohjelmistoa asennettaessa työasemalle tarvitaan lisenssiavain. Tietohallinnon rekisteristä on helposti nähtävissä asennetut ohjelmistot, niiden versiot ja käyttörooli. Laiterekisteristä on helppo myös jatkossa tarkistaa, mikäli ohjelmiston laitteistovaatimukset muuttuvat. Laiterekisteristä on löydettävissä vakiotyöasemien kokoonpanot, jolloin on helppo tarkistaa laitteiston tarkemmat tiedot.

Uusi sovellusversio ei ollut tietokantojen osalta yhteensopiva vanhan version kanssa, jolloin päätettiin siirtyä erillisestä virtualisoidusta SQL-palvelimesta SQL-klusteriin. Sovellustoimittajalta varmistettiin, että tietokannat toimivat klusterissa ja SQL-client toimii pakotetussa salatussa yhteydessä työasemalle asennettavan SQL-clientin ja SQL-klusterin välillä. Yhteyden toimivuus testattiin, kun tietokantaympäristö todettiin toimivaksi ja vanhasta ympäristöstä migroitiin potilaat ja mittausdata uuteen tietokantaan.

Pilotoinnissa testattiin yhdellä mittaustyöasemalla sovelluksen toimivuus oikeassa käyttöympäristössä ja kaikkien asetusten oikeellisuus. Yksikön kaikki spirometriohjelmistot päivitettiin uuteen versioon.

Pilotointiasennuksia tehtäessä huomattiin joka kuudennen asennuksen epäonnistuvan päivitettäessä vanhaa versiota. Syytä toimimattomuuteen ei löytynyt. Tästä syystä hylättiin asennusjärjestelmän kautta tehtävä keskitetty päivittäminen ja päätettiin tehdä päivitys poistamalla käsin asennetut vanhat versiot manuaalisesti ja siivoamalla ohjelmiston jälkeensä jättäneet rekisterimerkinnät ja kansiot tiedostoineen.

9.2 Sairaalan Active Directoryyn liitetty EEG-tutkimuslaitteisto

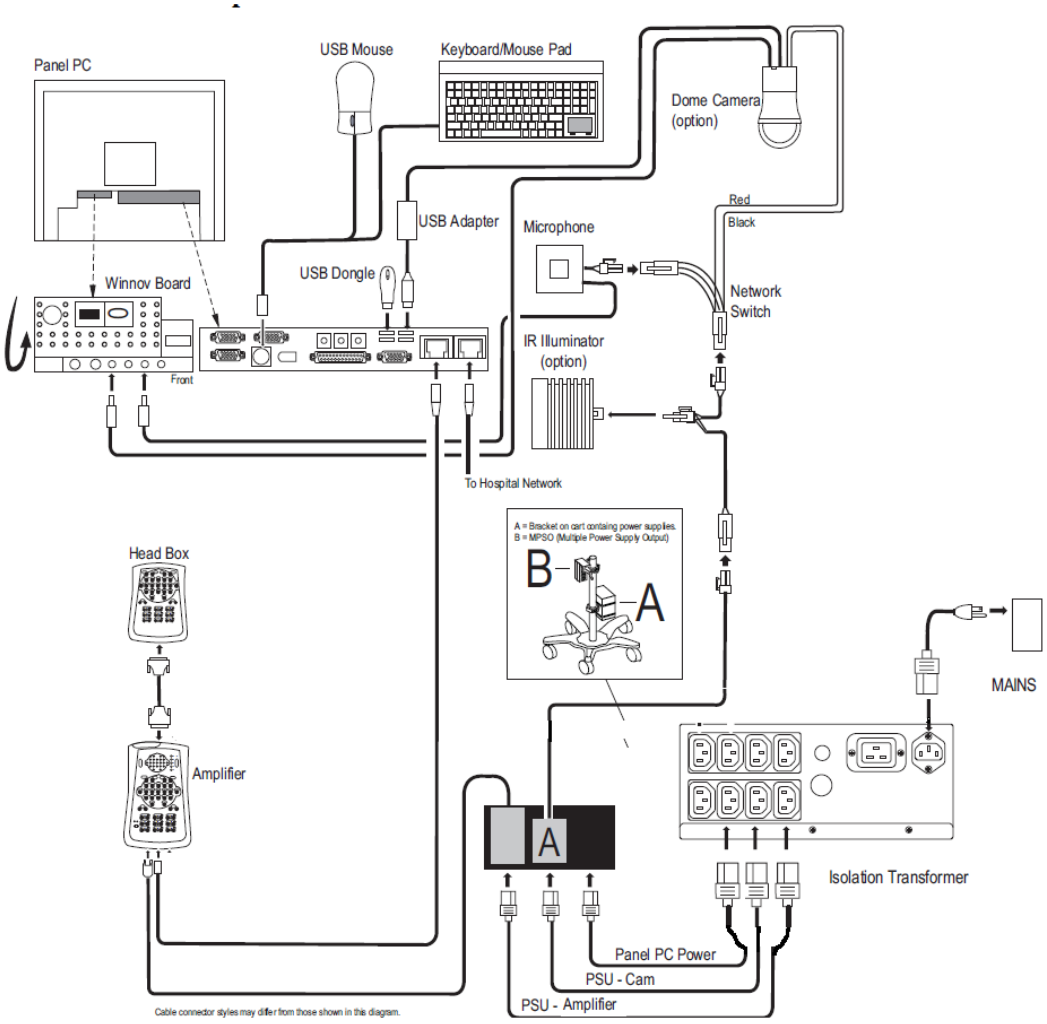
EEG-tutkimuslaitteisto on lääkintälaitejärjestelmä, joka koostuu EEG-vahvistimesta, tietokoneesta, lisälaitteista ja ohjelmistosta. EEG-laitteisto on liitetty sairaalan AD-ympäristöön, joka mahdollistaa EEG-laitteiston integroinnin sairaalan tietojärjestelmiin, tietoturvapäivitysten jakelun ja katseluohjelmiston integroinnin järjestelmään. Tutkimukset tallentuvat potilas- ja tutkimustietojen osalta keskitettyyn SQL-tietokantaan ja tutkimusdataa sisältävät tiedostot tiedostopalvelimelle. Lääkintälaitejärjestelmän tietokone on Medical-hyväksytty ja laitteen verkkoliitännät ovat Medical-hyväksytysti eristetty; laitteisto saa sähkönsä lääkintäsuojamuuntajan kautta, jolloin laitteiston vuotovirrat pysyvät hyväksytyllä tasolla, vaikka laitteistoon kuuluu ei-Medical-hyväksytty kamera.

Laiteen hankintahinta ylittää kilpailutusrajan, jolloin hankinta tapahtuu hankintayksikön kilpailutuksella hankintaprosessin kautta, ”lääkintälaitteen tietotekniset tiedot” -lomake tulee olla täytetty. Lomakkeesta ilmenee heti, että toimittaja on toimittanut sairaalaan aiemmin vastaavia laitteita. Laitetoimittaja pystyy nimeämään yhteyshenkilön sairaalasta.

EEG-tutkimuksessa rekisteröidään aivojen sähköistä toimintaa potilaan ollessa valveilla tai unessa. Tutkimuksella selvitetään epilepsiaa, kohtauksellisia oireita ja tajunnan häiriöitä. Toiminnallinen yhteys toteutuu EEG-vahvistimen kautta.

EEG-vahvistin on liitetty tietokoneeseen CAT-5-kaapelilla, joka on niin sanottuun Medical-PC:hen, joka täyttää 60601-1 vaatimukset lääkintälaiteelle potilashoitoalueella. EEG-vahvistimen lisäksi tietokoneeseen on kytketty verkon kautta ohjattava videokamera ja aktiivinen mikrofoni. Tietokoneessa on kaksi verkkoliitäntää, joista verkkoliityntä A on varattu liittymiselle sairaalan verkkoon. Verkkoliitäntään B on kytketty erillinen kytkin, johon on liitetty EEG-vahvistin ja videokameran ohjaus. Laitteen verkkoliitännät ovat 60601-1 mukaisesti eristetty, jolloin erillistä verkkoisolaattoria ei tarvita. Sähkönsyöttö lääkintälaitejärjestelmään on toteutettu lääkintäsuojaerotusmuuntajan kautta, jolloin vuotovirrat pysyvät 60601-1 ja 60601-1-1 määrittämien vaatimusten sisällä.

EEG-laitteiston kaaviokuva



KUVIO 27. Kaaviokuva EEG-laitteistosta

9.2.1 Riskianalyysi EEG-tutkimuslaitteistosta

Laitteistolle tehtiin riskianalyysi, jossa arvioitiin, mitä vaikutusta potilaan hoitoon on tiedon muuttumisella, käytön estävällä vialla ja tietoliikennevialla. Tiedon muuttuminen kuvastaa haittaohjelman tai hakkerin muuttaneen tutkimuksen tietoja. Käytön estävä kuvastaa tilannetta, jossa haittaohjelma on muuttanut laitteiston käyttökelvottomaksi. Tietoliikennevika kuvastaa tilannetta, jossa sairaalan tietoliikenneverkko on hakkerin toimista johtuen käyttökelvoton.

Tiedon muuttaminen: Ohjelmisto käyttää tutkimusdatassa suljettua formaattia, minkä johdosta tutkimusdatan muuttaminen huomattaisiin

välittömästi tutkimusta katsottaessa. Potilastietojen muuttaminen aiheuttaisi sen, että tutkimusta ei voida yhdistää oikeaan potilaaseen. Tutkimusdata ei tällöin vastaa potilaan kliinisiä oireita.

Käytön estävä: Tutkimuksen tekeminen ei onnistu ollenkaan tai potilaalle tehtävä tutkimus epäonnistuu. Toimimaton laite vaihdetaan toimivaan. Kesken tutkimuksen tapahtuva käytön esto aiheuttaa riskin tutkimusdatan katoamisesta, jolla saattaa olla potilaan diagnoosia viivästyttävä vaikutus. Diagnoosin viivästyminen saattaa aiheuttaa potilaalle haittaa.

Tietoliikennevika: Laitteisto toimii niin sanotussa stand-alone-tilassa. Tutkimusdata ei siirry palvelimelle, eikä tutkimusta ole mahdollista katsoa etänä. Tietoliikennevika saattaa aiheuttaa potilaan hoidon viivästymisen.

9.2.2 Vaatimukset ja tietoturvamääritykset

EEG-laite tulee valmistajalta toimivana kokonaisuutena, jolloin laitteiston vaatimukset täyttyvät. EEG-laitteen käyttöjärjestelmä uudelleen asennetaan sairaalan toimesta. Tällöin varmistutaan, ettei sairaalan verkkoon liitetä saastunutta laitetta. EEG-laite liitetään EEG-lääkintälaiteverkkoon, jolloin se saa IP-osoitteen sairaalan DHCP-palvelimelta. EEG-laitteeseen määritetään EEG-vahvistimen ja Loopback-adapterin vaatimat IP-osoitteet (TAULUKKO 5). Katseluohjelmisto asennetaan sairaalan vakioituun työasemaan, joka liitetään työasemaverkkoon 2, koska katseluohjelmistolla on tarve katsella realiaikaisesti EEG-laitteella tehtävää tutkimusta.

Laitteistovaatimukset:

- Windows 7 64-bit Enterprise tai Pro
- vähintään 1280x1024 resoluution näyttö
- prosessori i7 2600
- muisti 8 Gt tai enemmän
- lääkintälaitteessa 2 kpl 1 Gb:n verkkokorttia ja 1 PCI-Express-korttipaikka.

Laitetoimittaja ilmoitti, että lääkintälaite vaatii ylläpito-tason tunnukset, katseluohjelmiston osalta riittää käyttäjä-tason tunnukset. Käyttöoikeuksista lääkintälaitteessa ja katseluohjelmistossa täytyi antaa kaikki oikeudet ohjelman asennuskansioon, Online ja Offline-toiminnallisuuksien kansioihin ja rekisterissä HKEY_LOCAL_MACHINE\SOFTWARE\EEG-ohjelmistohaaraan. Palomuurista piti avata yhteydet taulukon 5 mukaisesti lääkintälaitteelle ja työasemalle. EEG-lääkintälaiteverkon ja työasemaverkon 2 välille avattiin tarvittavat tietoliikenneportit. Palomuurisääntöjen hallinnointi tehdään Group Policyllä. Ohjelma tallentaa tutkimusdatan paikalliseen verkkojakoon, minkä takia loopback-adapteri on konfiguroitava käyttämään tiettyä IP-osoitetta ja palomuurista avattava SMB-ajon käyttämät portit.

Tietoturvaan liittyvät vaatimukset:

- Virustorjuntaohjelmisto saa skannata ohjelmiston asennuskansiota ja Online- ja Offline-toiminnallisuuden kansiota.
- Käyttäjälle on annettava kaikki oikeudet ohjelmiston asennuskansioon, Online- ja Offline-toiminnallisuuksien kansioihin ja rekisteriin ohjelmiston haaraan.
- Tietoturvapäivitykset saa asentaa.
- Ohjelmisto toimii lääkintälaitteessa ylläpitotasoisin tunnuksin, katseluohjelmisto toimii käyttäjätason oikeuksin katselutyöasemassa.
- Lääkintälaite ei tarvitse päästyä internetiin tai sähköpostiin.
- Palomuuriin tarvitsee lääkintälaitteessa avata yhteyksiä SQL- ja tiedostopalvelimelle, EEG-vahvistimelta tulevalle datalle ja EEG-vahvistimen ohjaukselle ja etäkäytölle (TAULUKKO 6).

TAULUKKO 5. EEG-laitteen ja katselutyöaseman IP-määritykset

Lääkintälaite EEG			
192.168.12.0 /28	DCHP	EEG lääkintälaiteverkko	
192.168.250.2 /24	Static	EEG-vahvistimen verkkokortti	
192.168.250.16 /24	Static	Vahvistin malli A	
192.168.250.32 /24	Static	Vahvistin malli B (optio)	
192.168.250.51 /24	Static	Kameran ohjaus (optio)	
192.168.250.51 /24	Static	IP-kameran video (optio)	
EEG-katselu työasema			
192.168.2.0 /24	DHCP	Vakioitu työasema	

TAULUKKO 6. EEG-laitteen ja katselutyöaseman palomuurisäännöt

Lääkintälaite EEG					
Inbound					
Lähdeosoite	lähdeportti	protokolla	Kohdeosoite	Kohdeportti	Toiminto
192.168.2.0 /24	49152-65535	TCP	192.168.12.0 /28	137,139	SMB
192.168.2.0 /24	49152-65535	UDP	192.168.12.0 /28	138	SMB
192.168.2.0 /24	49152-65535	TCP	192.168.12.0 /28	135	Dcom
192.168.250.51 /24	4001	UDP	192.168.250.2 /24	4002	Video IP-kamerasta
192.168.250.16 /24	26666-26669	UDP	192.168.250.2 /24	26666-26669	EEG-vahvistimesta data
192.168.250.32 /24	26666-26669	UDP	192.168.250.2 /24	26666-26669	EEG-vahvistimesta data
192.168.251.0 /24	49152-65535	TCP	192.168.251.0 /24	137,138,139	SMB
Outbound					
192.168.12.0 /28	49152-65535	TCP	192.168.3.2 /24	1433	SQL-yhteys
192.168.12.0 /28	49152-65535	TCP	192.168.3.3 /24	137,139	SMB
192.168.12.0 /28	49152-65535	UDP	192.168.3.3 /24	138	SMB
192.168.12.0 /28	49152-65535	UDP	192.168.2.0 /24	5000-5020	Dcom
192.168.12.0 /28	49152-65535	UDP	192.168.2.0 /24	6050-6080	EEG-data
192.168.12.0 /28	49152-65535	TCP	192.168.2.0 /24	7120	Video
192.168.250.2 /24	49152-65535	TCP	192.168.250.16 /24	26666-26669	EEG-vahvistimen ohjaus
192.168.250.2 /24	49152-65535	TCP	192.168.250.32 /24	26666-26669	EEG-vahvistimen ohjaus
192.168.250.2 /24	49152-65535	TCP	192.168.250.51 /24	2380	Kameran ohjaus
192.168.251.2 /24	49152-65535	TCP	192.168.251.2 /24	137,138,139	SMB
EEG-katselu Työasema					
Inbound					
192.168.12.0 /28	5000-5020	UDP	192.168.2.0 /24	49152-65535	Dcom
192.168.12.0 /28	6050-6080	UDP	192.168.2.0 /24	49152-65535	EEG-data
192.168.12.0 /28	7120	TCP	192.168.2.0 /24	49152-65535	Video
Outbound					
192.168.2.0 /24	49152-65535	TCP	192.168.12.0 /28	137,139	SMB
192.168.2.0 /24	49152-65535	UDP	192.168.12.0 /28	138	SMB
192.168.2.0 /24	49152-65535	TCP	192.168.12.0 /28	135	Dcom
192.168.2.0 /24	49152-65535	TCP	192.168.3.2 /24	1433	SQL-yhteys
192.168.2.0 /24	49152-65535	TCP	192.168.3.3 /24	137,139	SMB
192.168.2.0 /24	49152-65535	UDP	192.168.3.3 /24	138	SMB

9.2.3 Testaus ja asennusprosessi

Tietokone on uudelleen asennettu sairaalan toimesta ja laitteisto on liitetty sairaalan Active directory -ympäristöön. Active Directoryssä laite on liitetty erilliseen lääkintälaitehaaraan, joka mahdollistaa erilaiset asetukset

verrattuna normaaliin toimistotietokoneeseen sairaalassa. Erona normaaleihin toimistotietokoneen asetuksiin on esimerkiksi se, ettei lääkintälaitteen työasemalla pääse internetiin. Lääkintälaitteella tehdään potilastutkimuksia, internet yhteydestä ei saavuteta lisäarvoa tutkimukselle. Lääkintälaite liitetään EEG-lääkintälaiteverkkoon.

Työasemissa on minimaalisen käyttöjärjestelmä asennuksen lisäksi, sairaalan keskitetty virustorjunta ja tietoturvapäivitysten jakelujärjestelmän vaatimat ohjelmistot. Laitetoimittaja on ilmoittanut, ettei laitteen työtiedostoja ja ohjelmiston tiettyjä prosesseja saa skannata, jolloin ne on poistettu aktiivisen skannauksen piiristä. Työasemalla voi tarvittaessa tehdä manuaalisen skannauksen, kun sen ohjelmisto ei ole käytössä. Tietoturvapäivitysten osalta lääkintälaitteen manuaali mainitsee, että ennen sovellusohjelmiston asennusta laitteelle on asennettava kaikki Windows updatesta saatavat päivitykset. Tietoturvapäivitysten asennukselle on tehty malli, jossa laitteet A ja B ovat pilottilaitteita ja niihin asennetaan ensin uudet tietoturvapäivitykset, tietohallinnon jakeluryhmä ilmoittaa muutamaa päivää ennen asennuksia tulevasta jakelusta. Pilottikoneilla testataan kaksi viikkoa laitteiden toimivuutta ongelmitta. Pilottijakson sujuttua ilman ongelmia, asennetaan tietoturvapäivitykset sovittuna ajankohtana jakelusuunnitelman mukaisesti. Laitteet on numeroitu ja päivitykset asennetaan ensin parittomiin laitteisiin. Kun päivitykset on asennettu onnistuneesti ilman ongelmia, päivitykset asennetaan parillisiin laitteisiin. Yksiköissä, joissa on vain yksi laite käytössä, tietoturvapäivitykset asennetaan aina viimeisessä ryhmässä. Tällä varmistetaan, että ainoan laitteen toimivuus ei vaarannu päivityksen takia, joka saattaa aiheuttaa laitteiston toimimattomuuden. Tietoturvapäivitysten asennusta seurataan asennusjärjestelmän lokeista. Tällöin voidaan tunnistaa laitteet, joihin asennukset eivät ole onnistuneet tai laitteet jotka ovat olleet pois päältä asennusajan kohtana.

Katseluohjelmisto on sovellustestattu ja ohjelmisto on paketoitu. Ohjelmiston kautta potilashallinta tapahtuu keskitetyn tietokannan kautta. Käyttäjien pääsyä tietokantaan hallitaan Active Directoryn käyttäjäryhmän ja tietokannan sisäisen käyttäjähallinnan kautta. Käyttäjä pitää lisätä

ohjelmiston käyttäjäryhmään, joka antaa keskitetysti käyttöoikeuden SQL-palvelimella olevaan tietokantaan ja tiedostopalvelimella olevaan levyjakoon. Levyjako ei näy normaalisti käyttäjälle. Lisäksi itse tietokantaan pitää käydä lisäämässä jokainen käyttäjä käsin, koska tietokannan sisään rakennettu käyttäjänhallinta ei tue käyttäjäryhmien avulla tapahtuvaa käyttäjien hallintaa.

Tutkimusdata tallentuu lääkintälaitteen tietokoneen kiintolevylle tutkimusta tehdessä. Tutkimusdata siirtyy palvelimille pitkissä tutkimuksissa 30 minuutin välein ja lyhyissä tutkimuksissa tutkimuksen loputtua. Toiminto on automatisoitu ja käyttäjän ei tarvitse tehdä muuta kun lopettaa tutkimus.

EEG-tutkimuksista lääkärit tekevät diagnoosin erillisellä katseluohjelmistolla. Katseluohjelmistossa näkyvät tekeillä olevat tutkimukset, tehdyt tutkimukset, jotka odottavat lausuntoa, sekä tutkimukset jotka on lausuttu. Ohjelmisto ei sisällä itsessään integraatiota sairaalan potilastietojärjestelmiin, koska järjestelmälle ei ole luvattu Windows 10 -tukea ja sairaala on siirtymässä käyttämään alueellista asiakas- ja potilastietojärjestelmää.

Lääkärin on mahdollista katsoa käynnissä olevaa tutkimusta lääkintälaitteella kahdessa eri moodissa: katselutilassa, jossa lääkäri näkee vain tekeillä olevasta tutkimuksesta tulevan datan pienellä viiveellä tai vaihtoehtoisesti lääkäri voi käyttää etähallintatilaa, jolloin lääkäri näkee tutkimuksen suorana ja pystyy tarvittaessa tekemään laitteen asetuksiin muutoksia. Lääkintälaitteen etäkäyttömahdollisuuden takia lääkärityöasemat tullaan siirtämään omaan verkkoonsa, josta etäkäyttöön tarvittavat protokollat ja portit on avattu EEG-laitteiden lääkintälaiteverkkoon. Sairaalan normaaleilta työasemilta ei ole pääsyä lääkintälaiteverkkoon.

9.3 Sairaalan verkkoon liitetty C-kaari

C-kaari on lääkintälaitejärjestelmä, joka sisältää integroidun tietokoneen. C-kaari on liikuteltava läpivalaisulaite, jolla kuvataan liikkuvia kehonosia ja

kehon sisäistä rakennetta. Tyypillinen käyttöympäristö on leikkaussali. Laitteisto täyttää lääkintälaitedirektiivin vaatimukset, käytettäessä kiinteää verkkoyhteyttä laitteiston verkkoliitännän eristys selvitettiin, ja se täyttää 60601-1 vaatimukset. C-kaari ei sisällä tunnistettavaa tietokonetta.

Laitteen hankintahinta ei ylitä kilpailutusrajaa, jolloin hankinta tapahtuu hankintayksikön hankintaprosessin kautta ja ”lääkintälaitteen tietotekniset tiedot” -lomake on täytetty. Lomakkeesta ilmenee, että laite voidaan liittää sairaalan PACS-järjestelmään.

9.3.1 Riskianalyysi C-kaaresta

Laitteistolle tehtiin riskianalyysi, jossa arvioitiin, mitä vaikutusta potilaan hoitoon on tiedon muuttumisella, käytön estävällä vialla ja tietoliikennevialla. Tiedon muuttuminen kuvastaa haittaohjelman tai hakkerin muuttaneen tutkimuksen tietoja. Käytön estävä kuvastaa tilannetta, jossa haittaohjelma on muuttanut laitteiston käyttökelvottomaksi. Tietoliikennevika kuvastaa tilannetta, jossa sairaalan tietoliikenneverkko on hakkerin toimista johtuen käyttökelvoton.

Tiedon muuttaminen: Viallinen potilasdata näkyy heti laitteen monitorilla. Tutkimusta tehtäessä kuvataan salissa olevaa potilasta, jolloin potilastietojen muuttuminen ei kuvaustilanteessa aiheuta haittaa potilaan hoidolle.

Käytön estävä: Tutkimuksen tekeminen ei onnistu ollenkaan tai potilaalle tehtävä tutkimus epäonnistuu. Toimimaton laite vaihdetaan toimivaan. Kesken tutkimuksen tapahtuva käytön esto aiheuttaa riskin tutkimusdatan katoamisesta, jolla saattaa olla potilaan diagnoosia viivästyttävä vaikutus. Diagnoosin viivästyminen saattaa aiheuttaa potilaalle haittaa.

Tietoliikennevika: Laitteisto toimii niin sanotussa stand-alone -tilassa. Mikä ei vaikuta kuvaustilanteessa potilaan hoitoon.

9.3.2 Vaatimukset ja tietoturvamääritykset

C-kaaren tapauksessa ilmeni heti, että laitteistoa ei voi integroida sairaalan Active Directoryyn tai muuten hyödyntää sairaalan tietoturvaohjelmistoja. Laitetoimittaja vastaa laitteiston ylläpidosta. C-kaari on liitetty kiinteällä IP-osoitteella RTG-lääkintälaiteverkkoon. Laitteisto sisältää verkkoon liitetyn Linux-tietokoneen jonka toiseen verkkoliittimeen on yhdistetty Windows-tietokone. Windows tietokoneella ei ole suoraa yhteyttä sairaan verkkoon. Linux-tietokone hoitaa C-kaaressa kuvaukseen liittyvät toiminnallisuudet ja Windows-tietokone hoitaa C-kaaressa läpivalaisututkimusten käsittelyn. Windows-tietokoneesta läpivalaisututkimukset lähetetään PACSiin. Käytännössä palomuuriin tarvitsi lisätä seuraava Outbound sääntö:

- Lähdeosoite 192.168.12.18 /28
- Lähdeportti 1024-65535
- Protokolla TCP
- Kohde osoite 192.168.3.4 /24
- Kohdeportti 104

Laitetoimittajan kanssa keskusteltiin laitteiston koventamisesta. Laitevalmistaja on varautumassa FDA:n vaatimuksiin. EU:ssa ei vielä ole vaatimuksia lääkintälaitteiden tietoturvan koventamisen suhteen.

Laitteistovaatimukset: laite on toimiva kokonaisuus

- Laite sisältää Windows ja Linux tietokoneet
- 100 Mbit/s verkkoyhteys
- Dicom standardin mukainen kuvantamistutkimusten arkistointijärjestelmä (PACS)

Tietoturvaan liittyvät vaatimukset:

- Laitetta ei saa muuttaa
- Vain laitetoimittaja päivittää laitteistoa.

9.4 Lääkintälaitteen tietoturvan parantaminen

Lääkintälaitteen tietoturvaan kohdistuu riskeinä (TAULUKKO 7): Tiedon muuttaminen, käytön estyminen ja tietoliikenne vika. Laitteen tuottamaan tietoon pitää pystyä luottamaan, kun tiedon perusteella tehdään potilaan hoitoon liittyviä päätöksiä.

Tiedon muuttaminen voi koskea potilastietoja, jolloin tietoa ei voida yhdistää oikeaan potilaaseen. Laitteen toimintaparametrit voivat muuttua jolloin laitteiston tuottama tieto ei ole vertailu kelpoista aiemman tiedon kanssa tai potilaan hoidossa tärkeä tieto ei näy tai näkyy väärin. Laitteen tuottamaa tietoa voidaan muuttaa jolloin potilaan hoidossa tarvittava tieto ei näy oikein tai tieto korruptoituu kokonaan.

Lääkintälaitteen käytön estävä tietoturva uhka huomataan heti, koska lääkintälaite ei toimi oikein. Sairaalassa on varauduttu lääkintälaitteen hajoamiseen toiminnassa, jolloin viallinen laite korvataan toisella. Käytön estävän tietoturvapoikkeaman selvittäminen saattaa olla hankalaa, koska lääkintälaite poistetaan käytöstä ja sammutetaan. Tietoturvapoikkeamasta ei tällöin välttämättä jää todisteita.

Tietoturva-uhan aiheuttama tietoliikennevika ei yleensä estä lääkintälaitteen käyttöä. Tietoliikenne häiriöt ja - viat on huomioitu lääkintälaitteen suunnittelussa. Potilaan hoito saattaa viivästyä, koska tieto ei siirry lääkintälaitteesta potilastietojärjestelmään. Sairaalassa on yleisesti varauduttu tietoliikenne vikoihin poikkeama suunnitelmissa. Tietoliikennevika voi johtua tietoturvapoikkeamasta ja koskettaa koko verkkoa tai yksittäistä laitetta tai laitteistoa verkossa.

TAULUKKO 7. Active Directoryyn liitettävien lääkintälaitteiden riskit ja Active Directoryyn liittämisen vaatimukset

Laite	Riski	Vaatimukset
Sairaalan vakioitu työasema	Tiedon muuttaminen	Laitteiston koventaminen
	Käytön estävä	Käyttöjärjestelmä asennetaan sairaalan asennusjärjestelmästä
	Tietoliikenne vika	Laitteistoon asennetaan sairaalan tietoturva-ohjelmisto
		Laitteistoon asennetaan säännöllisesti tietoturvapäivitykset
		Kokonaisuus toimii käyttäjätason tunnuksin
		UAC on päällä
		Laitteistoon voidaan asenneta muita ohjelmistoja
		Laitteistolla on päästy Internettiin tai sähköpostiin
		Potilastietoja ei tallenneta paikallisesti
		Laitteiston kiintolevy on salattu
		Laitteiston palomuuri on aktiivinen
Sairaalan Active Directoryyn liitetty lääkintälaite	Tiedon muuttaminen	Laitteiston koventaminen
	Käytön estävä	Käyttöjärjestelmä asennetaan sairaalan asennusjärjestelmästä tai käyttöjärjestelmä on asennettu käsin
	Tietoliikenne vika	Laitteistoon asennetaan sairaalan tietoturva-ohjelmisto
		Laitteistoon asennetaan säännöllisesti valmistajan hyväksymät tietoturvapäivitykset
		Kokonaisuus toimii lähtökohtaisesti käyttäjätason tunnuksin
		UAC on lähtökohtaisesti päällä
		Laitteistoon ei asenneta kuin laitetoimittajan hyväksymiä ohjelmistoja
		Laitteistolla ei ole päästyä Internettiin tai sähköpostiin
		Potilastietoja ei tallenneta paikallisesti
		Laitteiston kiintolevy on oletuksena salattu
		Laitteiston palomuuri on aktiivinen

Lääkintälaite voidaan liittää sairaalan Active Directoryyn kahdella tavalla. Käytetään sairaalan vakioitua työasemaa tai lääkintälaite liitetään Active Directoryyn ja sille määritellään omat asetukset. Lääkintälaitteen laitteisto-asetukset kovennetaan. Koventamisessa estetään laitteen käynnistäminen

kuin kiintolevyltä ja Bios/UEFI suojataan salasanalla. Koventamisella estetään laitteiston käynnistäminen muulta kuin luotetulta medialta.

Sairaalan vakioitua työasemaa käytettäessä käyttöjärjestelmä on asennettu aina sairaalan asennusjärjestelmän avulla. Active Directoryyn liitettävän lääkintälaitteen käyttöjärjestelmä voidaan asentaa myös tarvittaessa käsin. Käyttöjärjestelmän uudelleen asennus poistaa mahdollisesti laitteistoon muualta tarttuneet haitta-ohjelmat. Käyttöjärjestelmän asennuksen yhteydessä laitteistoon asennetaan sairaalan tietoturva-ohjelmisto ja asennetaan tietoturvapäivitykset. Vakioituun työasemaan päivitykset asennetaan sairaalan tietoturvapolitiikan mukaisesti. Active Directoryyn liitetyssä lääkintälaitteen osalta lääkintälaitteen valmistajan kanssa sovitaan käytännöt tietoturva-päivitysten osalta. Tietoturva-ohjelmisto ja tietoturvapäivitykset suojaavat laitteistoa haitta-ohjelmilta ja korjaavat tietoturva-aukkoja.

Active Directoryyn liitetyssä lääkintälaitteessa ei välttämättä voida käyttää samoja asetuksia kuin sairaalan vakioidussa työasemassa. Vakioidussa työasemassa käyttäjällä on käyttäjätason tunnukset. Active Directoryyn liitetyssä laitteistossa voidaan joutua antamaan käyttäjälle ylläpito-tasoiset tunnukset, että laitteisto toimii oikein. Käyttäjätasoisilla tunnuksilla laitteiston-asetuksiin ei voi tehdä muutoksia tai laitteistoon ei voi asentaa ohjelmistoja. Jos käyttäjä ei voi tehdä laitteiston asetuksiin muutoksia, niin haitta-ohjelmistot eivät voi toimia käyttäjän tunnuksilla laitteistossa. Jos lääkintälaitteessa joudutaan antamaan käyttäjälle ylläpito-tasoiset oikeudet, laitteistoa pitää valvoa muuten teknisesti. Ylläpito-tasoiset tunnukset pitää rajata vain kyseiseen lääkintälaitteeseen ja samoja tunnuksia ei saa käyttää muissa laitteissa. Sairaalan vakioidussa työasemassa UAC joka tarkoittaa käyttäjätilien valvontaa on aina päällä. Active Directoryyn liitetyissä lääkintälaitteessa UAC voidaan joutua kytkemään pois käytöstä, koska lääkintälaite ohjelmisto on huonosti toteutettu. UAC varmistaa laitteistoon kohdistuvat muutokset asetuksiin tai ohjelmisto asennukset pyytämällä ylläpito-tasoisten tunnusten salasanaa varmistamaan käyttäjän hyväksynnän muutoksille tai asennukselle.

Sairaalan vakioidulla työasemasta on pääsy Internettiin ja sähköpostiin, jotka ovat haitta-ohjelmien leviämiskanavia. Sairaan vakioituun työasemaan asennetaan potilastietojärjestelmiä ja normaalit toimisto-ohjelmistot. Active Directoryyn liitetyssä lääkintälaitteessa ei ole perustetta päästä Internettiin tai sähköpostiin. Lääkintälaitteeseen ei saa asentaa kuin valmistajan hyväksymät ohjelmistot. Muiden ohjelmistojen asentaminen saattaa haitata lääkintälaitteen toimintaa.

Sairaalan vakioituun työasemaan ja Active Directoryyn liitettyyn lääkintälaitteeseen ei tallenneta potilastietoja paikallisesti, koska laitteiston rikkoutuessa tiedot menetetään tai haitta-ohjelmisto voi tuhota tiedot. Laitteistojen kiintolevyt ovat oletuksena salattu estämään ulkopuolisen pääsyn käsiksi käyttöjärjestelmään siirtämällä kiintolevyn toiseen laitteistoon ja muokkaamalla tietoja. Lääkintälaitteen osalta laitevalmistaja voi kieltää kiintolevyn salauksen.

Sairaalan vakioidun työaseman ja Active Directoryyn liitetyn lääkintälaitteen käyttöjärjestelmän palomuuri on aktiivinen. Laitteistokohtaisella palomuurilla voidaan suojata laitteisto tehokkaasti tunkeutumisyrityksiltä. Lääkintälaite-ohjelmisto tarvitsemat tietoliikenne yhteydet sallitaan erikseen palomuurissa.

10 YHTEENVETO

Opinnäytetyön tavoitteena oli tutkia, kuinka sairaalan tietoverkkoon liitettävän lääkintälaitteen tietoturvaa voidaan parantaa. Lääkintälaitteiden verkotuksessa pitää huomioida Laki terveydenhuollon laitteista, Lääkintälaitedirektiivi ja sähköturvallisuus-standardit IEC 60601-1 ja 60601-1-1 yleisen tietoturvan lisäksi.

Lääkintälaitteiden elinkaari on pitkä, ja EU:ssa ei ole lääkintälaitteiden tietoturvaa koskevaa direktiiviä, joka velvoittaisi lääkintälaitevalmistaja huolehtimaan lääkintälaitteiden tietoturvasta koko elinkaaren ajan. Lääkintälaitetta ei välttämättä osata tunnistaa tietokoneeksi. Käytännössä kaikki elektroniset lääkintälaitteet sisältävät vähintään ohjelmoitavan logiikan tai sulautetun tietokoneen, vaikka niitä ei voisi liittää verkkoon.

Lääkintälaitteen hankinnassa on huomioitava tarve liittää lääkintälaite verkkoon. Lääkintälaitteille pitää luoda oma tietoturvapolitiikka ja tehdä lääkintälaitteita kohdistuvista tietoturvauhista riskianalyysi, jossa huomioidaan potilaaseen kohdistuva riski. Lääkintälaitteen toimimattomuus pahimmillaan saattaa aiheuttaa potilaan kuoleman. Lääkintälaitteisiin kohdistuvia riskejä ovat tiedon muuttaminen, jolloin laitteen antamaan tietoon ei voi luottaa, käytön estävä vika, jolloin laitetta ei voi käyttää, ja tietoliikennevika, jolloin laitteen tuottama tieto ei siirry potilastietojärjestelmään.

Lääkintälaitetta hankittaessa on huomioita mahdollinen tarve liittää lääkintälaite sairaalan verkkoon. Lääkintälaitteille luodaan oma palomuurein suojattu lääkintälaiteverkko, jota valvotaan IDS:llä. Lääkintälaiteverkkoja voi olla sairaalassa useita, jolloin voidaan erilaiset lääkintälaitteet erottaa omiin verkoihin.

Lääkintälaitteen hankintaprosessi analysoitiin ja analyysinpohjalta tehtiin prosessiin muutoksia. Lääkintälaitteille määritettiin kaksi tapaa liittää laite sairaalan verkkoon ja keskitettyyn hallintaan Active Directoryn avulla. Lääkintälaiteen työasemana käytetään sairaalan vakioituitua työasemaa, Lääkintälaite liitetään sairaalan Active Directoryyn ja lääkintälaite liitetään

sairaalan verkkoon ilman yhteyttä Active Directoryyn. Active Directoryyn liittämisen vaatimuksena on laitevalmistajan hyväksyminen liitokselle ja laitetoimittaja hyväksyy asennettavaksi sairaalan tietoturvaohjelmiston ja laitteistoon voidaan asentaa säännöllisesti tietoturvapäivityksiä. Active Directoryyn liittämisen vaatimukset ovat samankaltaiset sairaalan vakioidulla työasemalla ja Active Directoryyn liitetyllä lääkintälaitteella. Liitetylle lääkintälaitteelle voidaan sallia poikkeuksia asetuksiin huomioiden laitteen käyttötarkoitus. Kummassakin tapauksessa laitteiston käyttöjärjestelmä uudelleen asennetaan sairaalan toimesta. Vakioidussa työasemassa käyttöjärjestelmä asennetaan aina asennusjärjestelmän kautta, mutta liitettävän lääkintälaitteen tapauksessa voidaan käyttöjärjestelmä asentaa käsin.

Vakioitua työasemaa käytetään käyttäjätasoisin tunnuksin, työasemalla on pääsy internetiin ja sähköpostiin. Työasemalla on asennettu muitakin ohjelmistoja kuin lääkintälaitteen sovellus. Käyttäjätilien valvonta on aktiivinen. Active Directoryyn liitetyssä lääkintälaitteessa voidaan näistä määrityksistä poiketa, mutta laitteistolla ei ole pääsyä internetiin tai sähköpostiin. Active Directoryyn liitettyyn lääkintälaitteeseen voidaan määrittää käyttäjälle ylläpito-tasoiset tunnukset vain kyseiseen laitteistoon, jos laitteen käyttö vaatii korotettuja oikeuksia. Tarvittaessa käyttäjätilien valvonta voidaan poistaa käytöstä. Liitettyyn lääkintälaitteeseen saa asentaa vain laitevalmistajan hyväksymiä ohjelmistoja.

Sairaalan verkkoon liitettävistä lääkintälaitteista kolmeen hankittuun lääkintälaitteeseen sovellettiin käytäntöön vaatimuksia. USB-liitäntäiselle spirometria-laitteelle soveltui parhaiten liittäminen sairaalan vakioituun työasemaan. Spirometria-laitteen ohjelmisto soveltuvuus vakioidun työaseman kanssa käytettäväksi testattiin ja laitteen valmistajalle sopi, että spirometria-laitteen kanssa käytetään sairaalan vakioitua työasemaa. Sairaalan kaikki keskitettyyn spirometria-tietokantaan liitetyt laitteet päivitettiin käyttämään uutta ohjelmistoversiota, joka tukee keskitettyä ohjelmistoasennusta. Tulevaisuudessa ohjelmistoasennukset ja päivitykset tulevat tapahtumaan keskistetyn ohjelmistonjakelujärjestelmän kautta, joka mahdollista nopean version päivityksen ilman, että jokaisella työasemalla

tarvitsee käydä paikan päällä tekemässä asennus. EEG-tutkimuslaitteisto päätettiin liittää Active Directoryyn ilman vakiointia, koska laitteisto vaatii toimiakseen ylläpito-tasoiset tunnukset ja laitteistolla ei ole tarvetta päästä internetiin tai sähköpostiin tutkimuksia tehtäessä. Laitteistolle määritettiin omat asetukset Active Directoryyn ja laitteiston toiminta testattiin yhdessä laitetoimittajan kanssa. Laitteistolle määritettiin suunnitelma tietoturvapäivitysten asentamiseksi. Tietoturva-päivitykset testataan kahdella laitteella ennen kuin niitä aletaan asentamaan muihin käytössä oleviin EEG-laitteisiin. EEG-laitteisiin tietoturvapäivitykset asennetaan kahdessa erässä, millä on tarkoitus pienentää riskiä päivityksen asennuksen epäonnistumisesta johtuen. C-kaari ei soveltunut liitettäväksi Active Directoryyn, joten sille määriteltiin erilliseen lääkintälaiteverkon ja sairaalan sisäverkon palomuuriin avattavaksi laitteen käytössä tarvittavat tietoliikenneyhteydet.

Opinnäytetyön perusteella sairaala sai parannetun ehdotuksen uudeksi hankintaprosessin, jossa tietohallinto on mukana aktiivisesti lääkintälaitteen hankinnassa. Hankintaprosessissa saadaan täytetty ”lääkintälaitteen tietotekniset tiedot” -lomake, jota hyödynnetään tilattaessa lääkintälaitteen tarvitsemat tietotekniset palvelut tietohallinnolta. Verkkoon liitettäville lääkintälaitteille luotiin kolme eri toimintamallia liittää laite sairaalan verkkoon. Näiden toimintamallien pohjalta lääkintälaitteelle voidaan helposti määrittää parhaiten soveltuva toteutus lääkintälaitteen verkkoon liittämiselle.

Lääkintälaitteiden verkkoon liitettävyys tulee tulevaisuudessa merkittävästä lisääntymään. IoT tulee lääkintälaitteisiin ja niiden antureihin. Lääkintälaitteiden tuottamaa tietoa tullaan tulevaisuudessa analysoimaan kokonaisvaltaisesti potilaan hoidossa ja diagnostiikassa. Lääkintälaitteiden tietoturvan kehittäminen tulee olemaan lähitulevaisuuden suurimpia haasteita, koska lääkintälaitteiden tietoturvan toteuttamista ei määrätä EU:ssa direktiivillä erikseen. Potilaan hoito saattaa vaarantua tietoturvapoikkeaman takia.

Tietoturvan merkitys tulee korostumaan lähitulevaisuudessa, koska verkkorikollisuus on kasvussa. Erilaiset haittaohjelmat lisääntyvät koko ajan ja kaikkien verkkoon liitettyjen laitteiden tietoturva on uhattuna, jos laitteissa ei ole tietoturvaohjelmistoa ja niihin ei asenneta tietoturvapäivityksiä. Laitteiden käyttöympäristöä pitää seurata teknisin järjestelmin ja esiintyviin uhkiin reagoida.

LÄHTEET

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tallinna: Tietosanoma.

Andreasson, A. Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan Käsikirja 1. Helsinki: Tietosanoma.

Enisa 2016. Cyber security and resilience for Smart Hospitals. [viitattu 15.3.2017]. Saatavissa: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Frahim, J. Santos, O. & Ossipov, A. 2014. Cisco ASA: All-in-One Next-Generation Firewall, IPS and VPN Services. Indianapolis: Cisco Press.

FDA 2016. Center for devices &radiologocial health. [viitattu 20.2.2017]. Saatavissa: https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf

First.org inc 2017. Common Vulnerability Scoring System v3.0. [Viitattu 24.2.2017]. Saatavissa: https://www.first.org/cvss/specification-document

F-Secure 2017. AmbulanceThreat description: [viitattu 4.3.2017]. Saatavissa: https://www.f-secure.com/v-descs/ambulanc.shtml

Gibson, D. 2016. SSCP Systems Security Certfied Pratitioner All-in-one Exam Guide. New York: McGraw-Hill Education.

IEC 60601-1, 2005. Medical elelectrical equipment 2rd edition, Part 1: General requirements for basic safety and essential performance. Geneve: International Electrotechical Commission.

IEC 60601-1-1, 2000. Medical elelectrical equipment 2nd edition, Part 1-1: General requirements for safety, Colleteral standard: Safety requirement for medical electrical systems. Geneve: International Electrotechical Commission.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docento.

Honkanen, J. 2002. Sähköturvallisuus [viitattu 1.2.2017]. Saatavissa: http://www.kolumbus.fi/jukka.u.honkanen/tdata/sahkotur.pdf

Jackson, C. 2010. Network Security Auditing. Indianapolis: Cisco Press.

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo.

Järvinen, P. 2012. Arjen Tietoturva. Jyväskylä: Docendo.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Krutz, R. & Vines, R. 2003. Tietoturvasertifikaatti - CISSP, Helsinki: IT Press.

Laki terveydenhuollon laitteista ja tarvikkeista 629/2010

Lääkintälaitedirektiivi 93/42/ETY

Pöyhönen, I. & Kylmälä, K. 2004. Terveydenhuollon laadunhallinta Lääkintälaitejärjestelmien turvallisuus. Helsinki: Lääkelaitos.

SFS6000-7-710, 2007. Pienjännitesähköasennukset. Osa 7-710: Erikoistilojen ja -asennuksien vaatimukset. Lääkintätilat. Helsinki: Suomen Standardisoimisliitto.

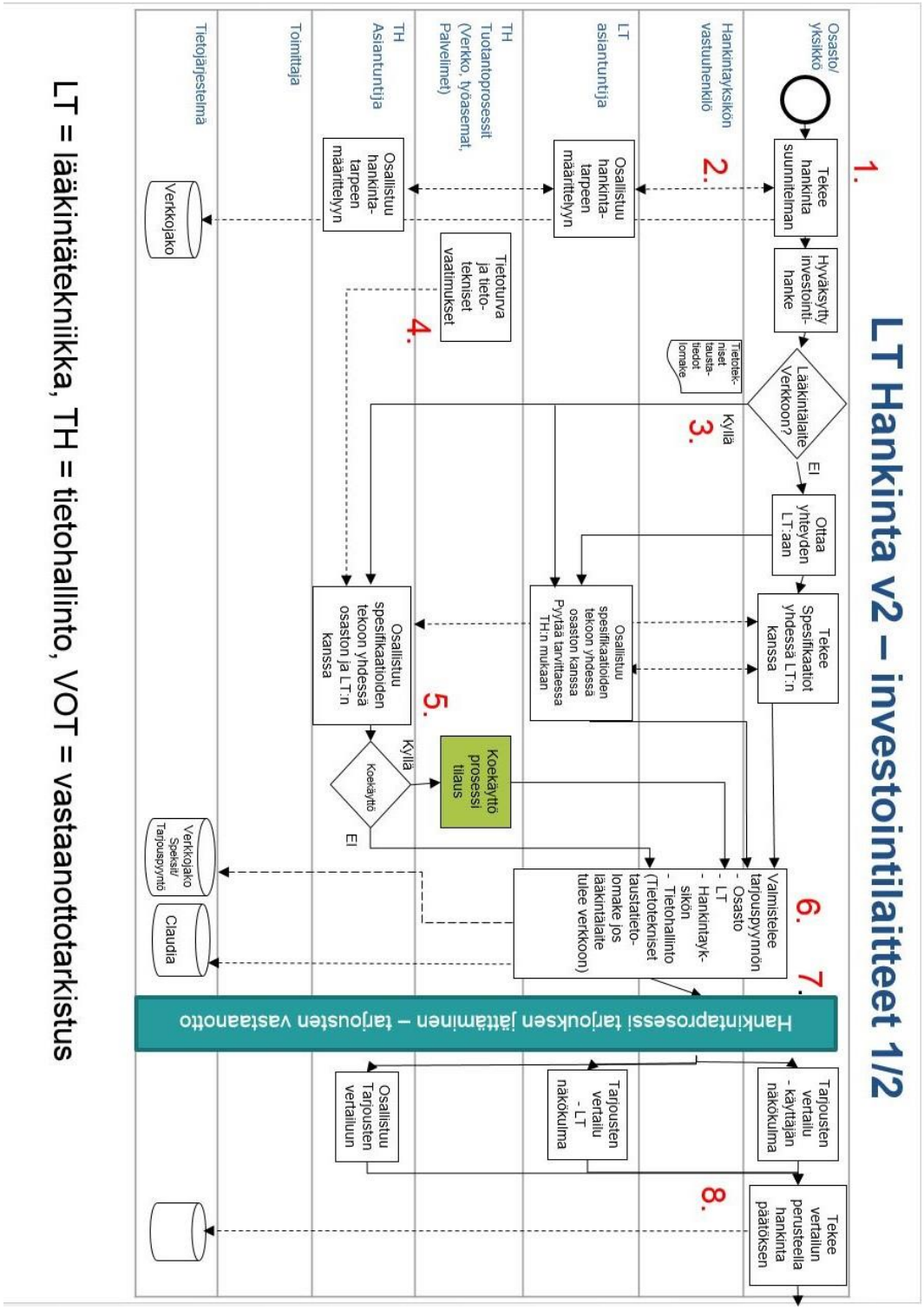
Suomen Automaatioseura ry 2005. Teollisuusautomaation tietoturva, Verkottumisen riskit ja niiden hallinta.[viitattu 20.2.2017]. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

Trapx Labs 2015. ANATOMY OF AN ATTACK. [Viitattu 2.3.2017]. Saatavissa: https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf

Trapx Labs 2016. Hospitals Under Siege. [viitattu 2.3.2017]. Saatavissa: http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf

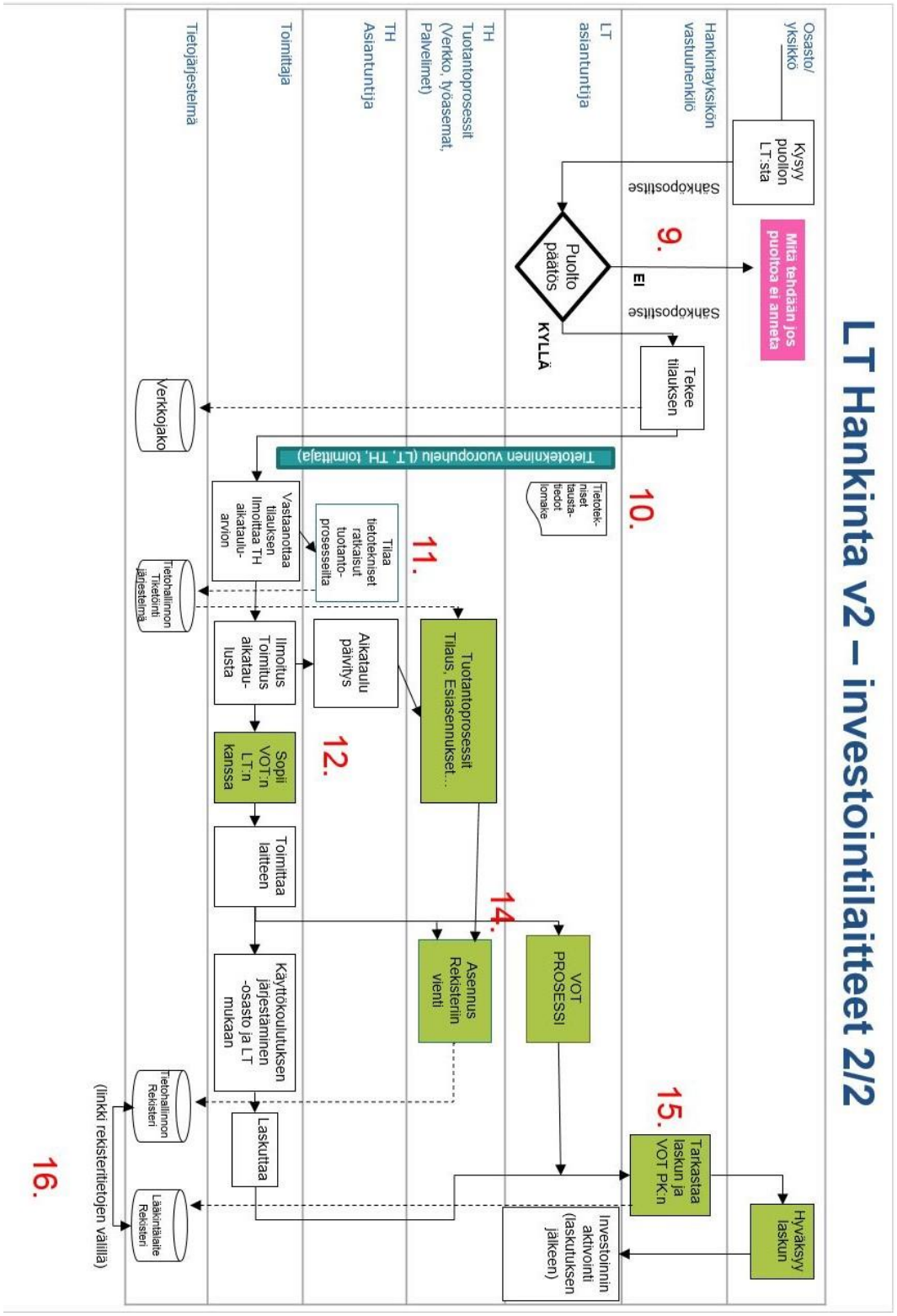
Viestintävirasto 2015. Haittaohjelma tarttuu, vaikka et klikkaisi mitään - osa 2. [viitattu 23.2.2017]. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/09/ttn20150928041.html

LIITTEET



LT = lääkintätekniikka, TH = tietohallinto, VOT = vastaanottotarkistus

LIITE 1 Hankintaprosessi osa 1



LIITE 2 Hankintaprosessi osa 2

Lääkintälaitteen tietotekniset ennakkotiedot

Pyydämme tarjoajaa täyttämään tämän lomakkeen ja toimittamaan sen tarjouksen mukana. Sairaala pyytää tarjottavaan laitteeseen liittyviä teknisiä tietoja, jotta voidaan varautua esim. mahdolliseen laitteen palvelin- ja työasematarpeeseen. Tässä tarjouspyynnön liitteessä pyydettäviä tietoja ei käytetä tarjousten vertailuun, pisteytykseen tai hankintapäätöksen tekemiseen, ellei tarjouspyynnössä nimenomaisesti ilmoiteta tässä lomakkeessa kysyttävien teknisten ominaisuuksien kuuluvan tarjousten vertailukriteereihin.

TARJOUSPYYNNON TIEDOT (HANTINTA YKSIKKO TAYTTAA)

LAAKINTATEKNIIKAN YHTEYSHENKILON YHTEYSTIEDOT

TIETOHALLINNON YHTEYSHENKILON YHTEYSTIEDOT

1 LAITTEEN TARJOAJAN TIEDOT JA YHTEYSHENKILO TEKNISISSA KYSYMYKSISSA

2 TARJOTTAVAN LAAKINTALAITTEEN KAUPPANIMI JA LAITETYYPPI

3 LAAKINTALAITTEEN/JARJESTELMAN TIETOTEKNISET TAUSTATIEDOT

3.1 Tarjottu kokonaisuus sisältää tietokoneen tai lääkintälaiteeseen on integroitu tietokone tai tarvitaan sairaalan toimittama tietokone

☐ Ei ☐ Kyllä, Mikäli vastasit kyllä täytä lomakkeen kohta 5 Lääkintälaitteen tietokoneen tiedot

HUOM! Tietokoneella tarkoitetaan yleisesti tunnustettavaa tietokonelaitteistoa.

3.2 Tarjottun lääkintälaitteen/järjestelmän mukana tulee tai siihen on mahdollista hankia erillinen analysointi/katseluohjelmisto/työasema

HUOM! Tietokone ei ohjaa lääkintälaitetta.

☐ Ei ☐ Kyllä, Mikäli vastattu kyllä täytä kohta 6 Analysointi/katselutyöasema/ohjelmisto

Jos vastaus on Kyllä, kuvaile lyhyesti, mitä hyötyä Analysointi/katseluohjelmistosta on käyttäjälle.

3.3 Tarjottu lääkintälaitteen saa liitää verkkoon

☐ Ei ☐ Kyllä, Mikäli vastasit kyllä täytä lomakkeen kohta 7 Verkkoyhteys

HUOM! Mikäli laitetta ei saa liittää verkkoon niin laitetoimittajan pitää merkitä selkeästi kielto, mikäli laitteessa on tietoliikenneportti

3.4 Tarjotaanko lääkintälaitteeseen/järjestelmään etäyhteydellä toteuttettua ylläpitoa

☐ Ei ☐ Kyllä, Mikäli vastasit kyllä täytä lomakkeen kohta 8 Etäyhteys

3.5 Tarjottu lääkintälaite/järjestelmä vaatii toimiakseen palvelimen tai siihen on mahdollista hankkia erillinen palvelin

☐ Ei ☐ Kyllä, Mikäli vastasit kyllä täytä lomakkeen kohta 8 Palvelin

Jos vastaus on Kyllä, kuvaile lyhyesti, mitä hyötyä palvelimesta on.

Mikäli kaikkiin yllä oleviin vastaus on Ei niin riittää että lomake allekirjoitetaan (kohta 4) ja toimitetaan tarjouksen mukana

4 PVM JA ALLEKIRJOITUS

Pvm	Tarjouksen tekijän allekirjoitus sekä nimenselvennys

LIITE 3 Lääkintälaitteen tietotekniset ennakkotiedot Sivu 1

5 LAAKINTALAITTEEN TIETOKONEEN TIEDOT

5.1 Samanlainen lääkintälaite on aiemmin liitetty sairaalan verkkoon

☐ Kyllä ☐ Ei

Mikäli vastattu kyllä, niin tarkenna missä

5.2 Toimittajan yhteyshenkilö lääkintälaitteen tietokonelaitteiston osalta

5.3 Ilmoita laitteen tietokoneen käyttöjärjestelmä ja versio. Kuvaa laitteiston tietoturvapäivitysten sekä virustorjuntaohjelmistojen toimittaminen ja asentaminen.

5.4 Lääkintälaitteen tietokone

☐ Kyseessä on integroitu laite joka sisältää tietokoneen käyttöjärjestelmineen ja ohjelmistoineen

☐ Laitetoimittajan/valmistajan toimittama työasema

☐ Sairaalan toimittama työasema, Mikäli käytetään sairaalan työasemaa laitteisto täyttää vaatimuksenmukaisuus määräykset

Mikäli käytetään sairaalan työasemaa ilmoita hyväksytyn työaseman tiedot tai laitteisto ja ohjelmistovaatimukset

5.5 Lääkintälaitteen/järjestelmän voi liittää sairaalan Active Directory

☐ Ei

☐ Kyllä, kuittaa tuetut käyttöjärjestelmät.
(sairaala käyttää tällä hetkellä Windows 7 Enterprise)

☐ Windows 7 Enterprise ☐ Windows 10 Enterprise

☐ Windows 7 Pro ☐ Windows 10 Pro

Vaatimkset Active Directoryyn liittmämiseen ovat:
1. virustorjunta ja virustorjunnan keskitetyn valvonnanon-hjelmisto
2. tietoturvapäivitysten jakelujärjestelmä

5.6 Tarvitaan sairaalan n työasema. Työasemaan ei liitetä Activce Directory-ympäristöön.

☐ Ei ☐ Kyllä

5.7 Mitä varusohjelmistoja lääkintälaitteen tietokoneelle ei saa asentaa

Tietohallinto ylläpitää työaseman käyttöjärjestelmiä ja varusohjel-mistoja ☐	Laitetoimittaja ylläpitää työaseman käyttöjärjestelmiä ja varusohjelmistoja ☐

5.8 Työaseman virustorjunta

Voiko työasemaa valvoa virustorjuntaohjelmistolla?

☐ Kyllä ☐ Ei

Jos vastaus on Kyllä, ilmoita tuetut virustorjuntatuotteet.	Jos vastaus on Ei, niin perustele kielto asentaa virustorjunta
Sairaala vastaa virustorjuntaohjelmistojen päivityksistä työasemalla ☐	Laitetoimittaja vastaa virustorjuntaohjelmistojen päivityksistä työasemalla ☐

LIITE 4 Lääkintälaitteen tietotekniset ennakkotiedot Sivu 2

6 ANALYSOINTI/KATSELUTYOASEMA / OHJELMISTO

6.1 Onko kyseessä erillinen työasema vai erillinen ohjelmisto

☐ Työasema ☐ Ohjelmisto

6.2 Tarjottua katselu/analysointityöasemaa/ohjelmistoa on asennettu aiemmin sairaalaan

☐ Kyllä ☐ Ei

Mikäli vastattu kyllä, niin tarkenna missä

6.3 Toimittajan yhteyshenkilö koskien analysointi/katselutyöasemaa/ohjelmistoa

6.4 Käytettävä työasema tai työasema johon analyysi/katseluohjelmisto asennetaan

☐ Laitetoimittajan/valmistajan toimittama erillinen työasema

☐ sairaalan toimittama työasema

☐ Sairaalan vakioitu työasema

Windows 7 Enterprise, virustorjunta ja virustorjunnan keskitetyn valvonnanonhjelmisto, tietoturvapäivitysten jakelujärjesetelmä

6.5 Analysointi/katselu ohjelmiston perustiedot

Ohjelmiston kauppanimi

Ilmoita ohjelmistontukemat käyttöjärjestelmät ja versiot.

Ilmoita ohjelmistonminivaatimukset työaseman teknisen ominaisuuksien osalta osalta

6.6 Katseluohjelmiston asennus ja konfigurointi hoidetaan sairaalan vakioituihin työasemiin

Laitetoimittaja toimesta	Sairaalan toimesta
☐	☐

6.7 Tukeeko ohjelmisto asennusta/päivitys asennusjärjestelmällä

☐ Kyllä ☐ Ei

6.8 Erillinen työaseman voi liittää sairaalan Active Directory

☐ Ei

☐ Kyllä, kuittaa tuetut käyttöjärjestelmät.
(Sairaala käyttää tällä hetkellä Windows 7 Enterprise)

☐ Windows 7 Enterprise ☐ Windows 10 Enterprise

☐ Windows 7 Pro ☐ Windows 10 Pro

Vaatimkset Active Directoryyn liittmämiseen ovat:
1. virustorjunta ja virustorjunnan keskitetyn valvonnanon-hjelmisto
2. tietoturvapäivitysten jakelujärjesetelmä

6.9 Työaseman ylläpito

Mitä varusohjelmistoja työasemalle ei saa asentaa

Tietohallinto ylläpitää työaseman käyttöjärjestelmiä ja varusohjelmistoja	Laitetoimittaja ylläpitää työaseman käyttöjärjestelmiä ja varusohjelmistoja
☐	☐

6.10 Työaseman virustorjunta

Voiko työasemaa valvoa virustorjuntaohjelmistolla?

☐ Kyllä ☐ Ei

Jos vastaus on Kyllä, ilmoita tuetut virustorjuntatuotteet.	Jos vastaus on Ei, niin perustele kielto asentaa virustorjunta

Sairaala vastaa virustorjuntaohjelmistojen päivityksistä työasemalla	Laitetoimittaja vastaa virustorjuntaohjelmistojen päivityksistä työasemalla
☐	☐

7 VERKKOYHTEYS

7.1 Tarjottu lääkintälaite on aiemmin liitetty sairaalan verkkoon

☐ Kyllä ☐ Ei

Mikäli vastattu kyllä, niin tarkenna missä

7.2 Laitetoimittajan yhteyshenkilö verkkoyhteyksien osalta

7.3 Lääkintälaitteen/järjestelmän voi liittää

☐ Kiinteään verkoon

☐ Langattomaan verkoon

7.4 Lääkintälaitteen/järjestelmän verkkoliitännät ovat eristetty 60601-1 mukaisesti, jos ei niin laitetoimittajan vastuulla on toteuttaa eristys 60601-1 mukaisesti

☐ Kyllä ☐ Ei

7.5 Ilmoita tuetut langattoman verkon teknologiat ja salausstandardit

8 LAITTEEN YLLAPITO ETAYHTEYDELLA

8.1 Onko tarjottava laite tai palvelin tarkoitus liittää etäyhteydellä toimittajan huoltokeskukseen?

☐ Ei ☐ Kyllä, Lääkintälaite on tarkoitus liittää etäyhteyteen

☐ Kyllä, Erillinen analyysi/katselutyöasema on tarkoitus liittää etäyhteytteen

☐ Kyllä, Palvelin on tarkoitus liittää etäyhteyteen

8.2. Jos vastaus edelliseen kysymykseen on KYLLA, onko toimittajalla ja sairaalalla jo voimassa oleva etäyhteyssopimus?

☐ Kyllä ☐ Ei

8.3. Jos vastaus edelliseen kysymyksen on KYLLA, edellyttääkö tarjottava laite muutoksia olemassa olevaan etäyhteyteen?

☐ Kyllä ☐ Ei

8.4 Jos tarvitaan uusi etäyhteys tai muutos olemassa olevaan etäyhteyteen, ilmoita etäyhteyden tekninen toteutustapa.

8.5 Jos toimittajalla ei ole etäyhteyttä sairaalaan, mutta laitteen ylläpito edellyttää etäyhteyttä, ilmoita yhteyshenkilö etäyhteyden osalta

9 Palvelin

9.1 sairaalassa on olemassa oleva palvelinasennus
☐ Kyllä ☐ Ei
Mikäli vastattu kyllä, niin tarkenna mikä ja missä

9.2 Yhteyshenkilö palvelin ohjelmistonosalta

9.3 Käytetään Tietohallinnon tarjoamaa palvelinta.
☐ Kyllä ☐ Ei

☐ Windows, ilmoita tuetut käyttö-järjestelmäversiot ja servicepackit	☐ Unix tai Linux, ilmoita tuetut käyttö-järjestelmäversiot	☐ Muu, mikä? Ilmoita tuetut käyttö-järjestelmäversiot

9.4 Palvelin ohjelmisto tukee virtualisointia.
☐ Kyllä ☐ Ei
Ilmoita tuetut virtualisointiratkaisut

Mikäli palvelinohjelmisto ei tue virtualisointia ja tarvitsee fyysisen palvelimen. ilmoita syy:

9.5 Palvelinten ylläpito
Mitä varusohjelmistoja palvelimelle asennetaan

Tietohallinto ylläpitää palvelimen käyttöjärjestelmiä ja varusohjel-mistoja ☐	Laitetoimittaja ylläpitää palvelimen käyttöjärjestelmiä ja varusohjelmistoja ☐

9.6 Palvelinten virustorjunta
Voiko laitteen palvelinta valvoa virustorjuntaohjelmistolla?
☐ Kyllä ☐ Ei

Jos vastaus on Kyllä, ilmoita tuetut virustorjuntatuotteet.	Jos vastaus on Ei, niin perustele kielto asentaa virustorjunta.
Sairaala vastaa virustorjuntaohjelmistojen päivityksistä palvelimella ☐	Laitetoimittaja vastaa virustorjuntaohjelmistojen päivityksistä palvelimella ☐

9.7. Laitteen palvelinta/palvelimia voidaan valvoa sairalan virustorjuntaohjelmistolla,
☐ Kyllä ☐ Ei