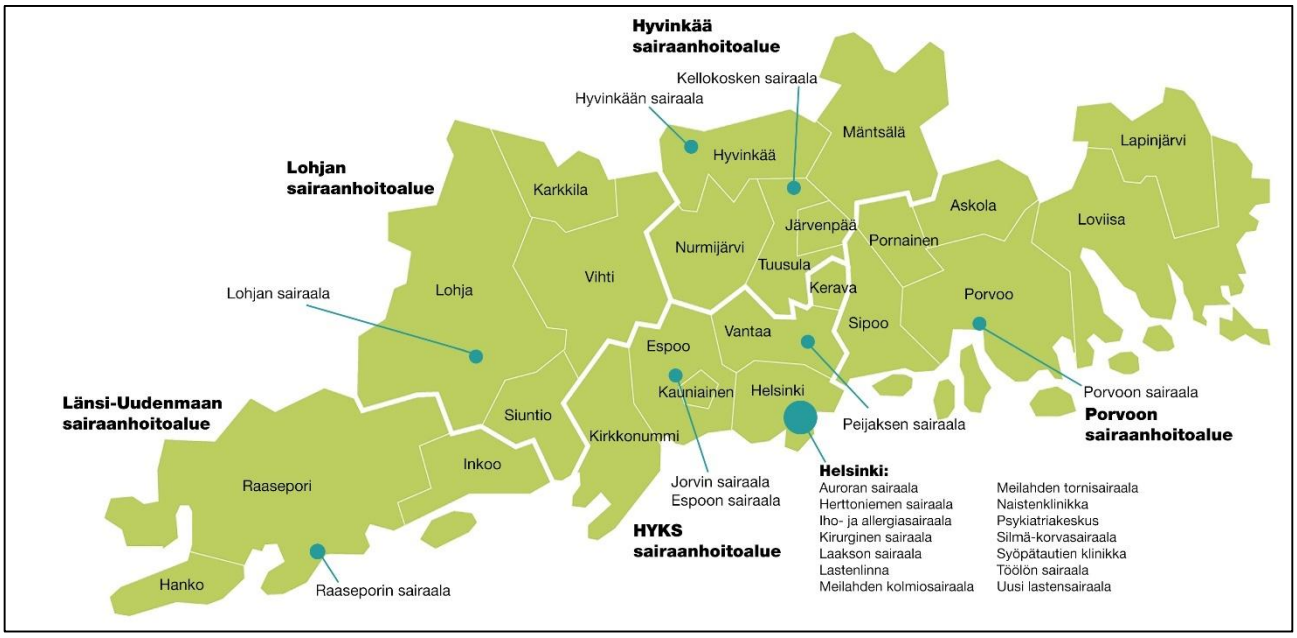
Helsingin ja Uudenmaan sairaanhoitopiirin tietojärjestelmähäiriöt 7.–8.11.2017



Y2018-02

ALKUSANAT

Onnettomuustutkintakeskus päätti 27.3.2018 turvallisuustutkintalain (525/2011) 2 §:n nojalla tutkia Helsingin ja Uudenmaan sairaanhoitopiirin (HUS) toiminnassa 7.–8.11.2017 tapahtuneet tietojärjestelmien häiriöt. Sosiaali- ja terveysministeriö esitti tapauksista Onnettomuustutkintakeskukselle 21.3.2018 tutkintapyynnön, joka otettiin turvallisuustutkintalain 17 §:n 2 momentin 3 kohdan mukaisesti huomioon tutkinnan aloittamista harkittaessa. Turvallisuustutkinnan tarkoituksena on yleisen turvallisuuden lisääminen, onnettomuuksien ja vaaratilanteiden ehkäiseminen sekä onnettomuuksista aiheutuvien vahinkojen torjuminen. Turvallisuustutkintaa ei tehdä oikeudellisen vastuun kohdentamiseksi.

Tutkintaryhmän johtajaksi nimettiin erikoistutkija Timo Naskali ja jäseniksi VTM Kari Ylönen, TkL Petri Pommelin, dosentti, LT Alpo Vuorio ja LL Simo Piitulainen. Tutkinnanjohtaja oli johtava tutkija Kai Valonen.

Turvallisuustutkinnassa selvitetään tapahtumien kulku, syyt ja seuraukset sekä tehdyt pelastustoimet ja viranomaisten toiminta. Tutkinnassa selvitetään erityisesti, onko turvallisuus otettu riittävästi huomioon onnettomuuteen johtaneessa toiminnassa sekä onnettomuuden tai vaaran aiheuttajina taikka kohteina olleiden laitteiden ja rakenteiden suunnittelussa, valmistuksessa, rakentamisessa ja käytössä. Lisäksi selvitetään, onko johtamis-, valvonta- ja tarkastustoiminta asianmukaisesti järjestetty ja hoidettu. Tarvittaessa on myös selvitettävä mahdolliset puutteet turvallisuutta ja viranomaisia koskevissa säännöksissä ja määräyksissä.

Tutkintaselostus sisältää selostuksen onnettomuuden kulusta, onnettomuuteen johtaneista tekijöistä ja onnettomuuden seurauksista sekä asianomaisille viranomaisille ja muille toimijoille osoitetut turvallisuussuositukset sellaisiksi toimenpiteiksi, jotka ovat tarpeen yleisen turvallisuuden lisäämiseksi, uusien onnettomuuksien ja vaaratilanteiden ehkäisemiseksi, vahinkojen torjumiseksi sekä pelastus- ja muiden viranomaisten toiminnan tehostamiseksi.

Onnettomuuteen osallisille sekä tutkittavan onnettomuuden alalla valvonnasta vastaaville viranomaisille on varattu tilaisuus antaa lausuntonsa tutkintaselostuksen luonnoksesta. Lausunnot on otettu huomioon tutkintaselostusta viimeisteltäessä. Yhteenveto lausunnoista on tutkintaselostuksen lopussa. Yksityishenkilöiden antamia lausuntoja ei turvallisuustutkintalain mukaisesti julkaista.

Tutkintaselostus ja tiivistelmä on julkaistu Onnettomuustutkintakeskuksen verkkosivuilla osoitteessa *www.turvallisuustutkinta.fi*.

Tutkinnan tunnus: Y2018-02
Tutkintaselostus 2/2019
ISBN: 978-951-836-535-1 (PDF)

Kannen kuva: HUS

SISÄLLYSLUETTELO

1 TAPAHTUMAT

1.1 Tapahtumien kulku

Helsingin ja Uudenmaan sairaanhoitopiirin (HUS) tietoliikenneverkkoon tuli häiriö tiistaina 7.11.2017 kello 12.15. Verkon käyttäjät kokivat häiriön tietojärjestelmien toimimattomuutena. Keskeisin ongelma oli Uranus-potilastietojärjestelmässä[1], mutta ongelmia ilmeni myös automaatiolaboratorion järjestelmissä, synnytystietojärjestelmässä, hoitajakutsujärjestelmässä, lankapuhelimissa ja apteekin lääkerobotissa. Kyseessä ei ollut täydellinen tietoliikenteen katko, vaan yhteydet toimivat ajoittain.

Uranukseen oli kirjautunut häiriön alkaessa yli 7 000 käyttäjää. Uranuksen sovellustukeen alkoi tulla useilta käyttäjiltä ilmoituksia muutamassa minuutissa häiriön alkamisesta.[2]

Sovellustuki ilmoitti yhteysongelmista HUS Tietohallinnolle, joka alkoi johtaa korjaavia toimenpiteitä. Tietohallinto lähetti häiriöstä HUSin johdolle tekstiviestitiedotteen kello 12.36 normaalin käytännön mukaisesti. Uranus-palveluntuottajan sovellustuki tarkisti Uranus-potilastietojärjestelmän toiminnan omassa konesalissaan[3]. Sovellus toimi, joten vika vaikutti olevan tietoliikenneyhteydessä HUSin konesalin ja Uranus-palveluntuottajan konesalin välillä.

HUSin tietoliikenneverkkoa valvoo ympärivuorokautisesti ylläpitopalveluntuottaja, joka alkoi selvittää asiaa yhdessä HUS Tietohallinnon kanssa. Vika oli sellainen, että jatkuva verkkovalvonta ei sitä tunnistanut. Ongelma paikallistui HUSin konesalissa olleisiin kahteen rinnakkaiseen runkokytkimeen (A ja B), joiden toimintaa ohjasi yhteinen ohjelmisto.

Paikan päälle mennyt asiantuntija havaitsi, että runkokytkimistä oli kadonnut yksi reititysprosessi. Reititysprosessin uudelleenkäynnistys tai muu tavanomainen ylläpitotoimenpide ei poistanut häiriötilannetta, joten ratkaisua haettiin käynnistämällä ensisijaisesti liikenteestä huolehtiva kytkin A uudelleen kello 14.30.

Kytkimen A yksi linjakortti vaurioitui uudelleenkäynnistyksen yhteydessä, joten häiriö jatkui. Kortti otettiin irti ja laitettiin takaisin, mutta se ei auttanut. Kytkimessä B oli sama häiriötilanne kuin kytkimessä A, minkä lisäksi B:n reititysprosessi oli jumissa. Kytkin B ei siten myöskään toiminut normaalisti, vaikka sen piti kahdentaa kytkin A. Kytkimessä A oli lisäksi ollut 23.10.2017 reititysprosessiongelma, jonka jälkeen sen kautta mennyt Uranus-yhteyden kahdennus ei todennäköisesti enää toiminut. Kytkintä B ei yritetty käynnistää uudelleen ennen kuin korvaava linjakortti on saatu, koska pelättiin myös sen rikkoutumista.

HUS Tietohallinto aloitti korvaavan linjakortin hankinnan ohi ylläpitopalvelun tuottajan ottamalla yhteyttä suoraan laitevalmistajan edustajaan noin kello 15. Edustaja aloitti linjakortin toimitusprosessin. Hieman myöhemmin tietohallinto alkoi selvittää korvaavan kortin saamisen mahdollisuutta myös omien verkostojensa kautta.

Kello 16.30 tietohallinnossa alettiin valmistella viallisen linjakortin ohittamista väliaikaisesti, jotta Uranus-yhteydet saataisiin toimimaan. Poikkeusjärjestelyä ei ollut ennakkoon suunniteltu, vaan se oli tilanteen mukainen. Väliaikaisratkaisu saatiin toteutettua kello 17.30, jonka jälkeen yhteydet alkoivat toimia paremmin. Tämän jälkeen kytkin B käynnistettiin uudelleen onnistuneesti.

---

1 Uranus on HUSin palveluna ostama erikoissairaanhoidossa käytettävä potilastietojärjestelmäkokonaisuus. Keskeisin osa Uranusta on sähköinen potilaskertomus Miranda.

2 Potilastietojärjestelmän tietokannat ovat Uranus-palveluntuottajan konesalin palvelimilla, joihin järjestelmän käyttäjät ovat yhteydessä omalta työasemaltaan tietoliikenneverkon kautta.

3 Konesali (myös tietokonesali, datakeskus tai palvelinkeskus) on huone tai rakennus, jossa on useita tietokoneita ja niiden oheisjärjestelmiä, jotka tallentavat ja käsittelevät suuria määriä dataa.

Tietohallinnon omien verkostojensa kautta hankkima linjakortti saatiin paikalle kello 17.45. Kello 18 linjakortti oli vaihdettu ja tietoliikenneyhteydet alkoivat palautua normaaliksi, kun väliaikaisratkaisulla olleet reitit ykset siirrettiin uudelle linjakortille. Kello 18.20 saatiin paikalle laitevalmistajan edustajan toimittama linjakortti, joka jätettiin varaosaksi. Tietoliikennehäiriön todettiin kello 19 olevan ohi.

Hoitohenkilökunta koki häiriön monenlaisena toiminnan vaikeutumisena. Potilastietojärjestelmästä ei voitu lukea potilaiden tietoja, eikä siihen voitu kirjoittaa tietoja. Laboratoriolähetteet kirjoitettiin käsin paperille, jotka käytiin viemässä laboratorioon. Ennen katkoa annetuista lääkityksistä ei ollut varmaa tietoa. Myös puhelinyhteyksissä oli ongelmia. Katkon pituudesta ei saatu arviota, mikä vaikeutti korvaavien toimintojen suunnittelua. Vaikutukset eri sairaaloissa olivat verkon rakenteen vuoksi erilaisia.

Seuraavana aamuna eli keskiviikkona 8.11.2017 kello 9 jälkeen Uranus-sovelluksen käyttäjät havaitsivat sovelluksen toiminnassa merkittävää hitautta. Uranuksen sovellustuki sai kello 9.13 alkaen useilta käyttäjiltä ilmoituksia häiriöistä. Uranus-palveluntuottaja havaitsi sovelluspalveluiden seurannan avulla kuormitusta ja sovellusperäisiä tietokantalukkoja[4].

Uranus-palveluntuottaja alkoi normaalin ylläpitomenettelyn mukaisesti poistaa tietokantalukkoja sekä käynnistää uudelleen eri palveluja. Kello 12 kaikki tietokantalukot oli saatu poistettua. Kaikki ohjelmat toimivat, mutta hitaasti. Tilanne oli parantunut aamusta, mutta ei ollut normaali.

Tietoliikenteen laitteistovian poissulkemiseksi Uranus-palveluntuottaja oli siirtänyt kello 10 konesalin 1 palomuurin toiminnallisuuden konesalin 2 varmentavaan laitteeseen, mutta erityisesti kirjautumisessa Uranukseen oli edelleen ongelmia.

Konesalissa 1 olleen palomuurin muistin havaittiin täyttyneen. Uranus-palveluntuottaja teki laitevalmistajan ohjeistuksen mukaisesti konesalin 1 palomuurialustan ohjelmistollisen uudelleen käynnistyksen, jotta täyttynyt muistialue olisi tyhjentynyt. Tällä palomuurin toiminnallisuuden oletettiin palautuvan normaaliksi.

Kello 14.06 Uranus-palveluntuottaja siirsi palomuuritoiminnallisuuden takaisin konesaliin 1. Siirto aiheutti kaikkien kyseistä jaettua laitealustaa käyttäneiden yhteyksien katkeamisen, koska palomuuri ei oletuksesta huolimatta ollut kunnossa. Siten toiminnallisuus siirrettiin kello 14.14 takaisin konesaliin 2.

Kello 16.30 Uranus-palveluntuottaja korvasi HUSin pyynnöstä palomuurin reitittävällä yhteydellä, jonka jälkeen häiriö oli ohi. Muutos aiheutti vielä kello 22 jälkeen Uranus-tietokantapalvelimessa hitautta. Seuraavana aamuna ruokahuollon ohjelmassa oli kirjautumisongelmia. Molemmat häiriöt saatiin korjattua nopeasti.

Hoitohenkilökunta koki keskiviikkona tapahtuneen potilastietojärjestelmän häiriön enimmäkseen samanlaisena kuin edellisen päivän häiriönkin. Toisen päivän häiriö kohdistui ainoastaan potilastietojärjestelmään, mutta kohdistui sairaalan toimintojen kannalta aktiivisempaan ajankohtaan.

1.2 Tiedonkulku ja tilanteesta selviytyminen

HUSin johtohenkilöstö sai tiedon ensimmäisen päivän häiriöstä laajalla jakelulla Tietohallinnon lähettämällä tekstiviestillä. Tekstiviestissä todettiin häiriön ilmeneminen, mutta se ei si-

[4] Tietokantalukko syntyy, kun tietokannan tietue lukitaan koko tiedon päivitykseen liittyvän toimintoketjun ajaksi muilta käyttäjiltä. Lukitus voi jäädä päälle esimerkiksi tietoliikenteessä esiintyvän häiriön vuoksi.

sältänyt tietoa häiriön vakavuudesta tai kestosta. Vastaavia tekstiviestejä tulee vuosittain joitakin kymmeniä. Yleensä häiriöt saadaan korjattua niin nopeasti, ettei erityisille toimenpiteille ole tarvetta. Tässä tapauksessa tilanne jatkui ja vaikutukset kasvoivat vähitellen.

Häiriötä koskevan tekstiviestin aikaan HUSin valmiusyksikön henkilöistä keskeiset turvallisuus- ja valmiusjohtaja sekä lääkintäpäällikkö olivat neuvottelussa sellaisessa suojatilassa, johon matkaviestimiä ei voinut ottaa mukaan. He saivat tiedon vasta myöhemmin iltapäivällä saavuttuaan suojatilasta ulos.

HUSin viestintä sai tiedon häiriöstä kello 14, kun mediaa palvelevaan puhelimeen tuli yhdeltä medialta kysely häiriöstä. Tilanteen poikkeuksellisuus alkoi selvitä vähitellen. Tilanteesta ja häiriön laajuudesta oli vaikea saada kokonaiskuvaa.

Johtajaylilääkäri teki kello 14.30 päätöksen jatkuvuussuunnitelman käyttöönotosta. Julkisuuteen HUS tiedotti tilanteesta kello 14.44 tiedotteella. Tiedotteessa esitettiin arvio, että osa kiireettömistä toimenpiteistä joudutaan siirtämään häiriön johdosta ja että hätätoimenpiteet hoidetaan normaalisti.

Virka-ajan lähestyessä päättymistään johtajaylilääkäri päätti kutsua koolle HUSin valmiusjohdon, koska oli ilmennyt, että häiriö pitkittyy ja ulottuu koko Uudenmaan alueelle. Valmiusjohto kokoontui vs. johtajaylilääkärin[5] johdolla kello 16.45. Tähän asti HUS Tietohallinnon tilannejohto oli hoitanut tilanteen korjaavia toimenpiteitä. Vika oli paikallistettu, korvaava komponentti oli tulossa ja häiriön arvioitiin olevan ohi viimeistään parin tunnin kuluttua. Valmiusjohto jakoi arviota tilanteen korjautumisesta eri sairaaloihin käytössä olevin keinoin, mutta tietoa ei saatu jaettua systemaattisesti kaikille osastoille. Valmiusjohto purettiin kello 19.15.

Seuraavan päivän häiriötä alettiin käsitellä HUSin johdossa normaalin organisaation voimin. HUSin sisäinen tiedottaminen tapahtui intranetin välityksellä. HUS tiedotti uudesta häiriöstä sosiaali- ja terveysministeriöön (STM) kello 11.15. Julkisuuteen HUS tiedotti tilanteesta kello 12.11 tiedotteella, jonka mukaan potilastietojärjestelmässä oli havaittu uusi ongelma. Tiedotteen mukaan palvelun uudelleenkäynnistyksen jälkeen tietojärjestelmä oli toiminut lähes normaalisti, mutta järjestelmässä oli edelleen ollut häiriöitä. Kaikkien HUSin toimipisteiden todettiin olevan toiminnassa.

Kello 12.35 alkaen johtajaylilääkärin koolle kutsuma valmiusjohto alkoi johtaa tilannetta. Edellisen päivän kokemusten perusteella valmiusjohdon kokoukseen kutsuttiin myös tietohallinnon edustaja, mikä helpotti valmiusjohdon tilannekuvan muodostamisessa. HUS lähetti iltapäivän aikana julkisuuteen neljä tiedotetta, joista viimeisin lähetettiin kello 17.27. Tiedotteen mukaan potilastietojärjestelmä toimi lähes normaalisti. Korjaustoimia oli tehty iltapäivän aikana, ja tilannetta seurataan illan ja yön aikana.

HUSin valmiusjohto kokoontui vielä kolmantena aamuna tarkkailemaan tilannetta. HUS tiedotti kello 9.56, että potilastietojärjestelmä toimii normaalisti ja että leikkauksia ei ole peruttu. Konsernitason valmius purettiin kello 14.

HUSin tietohallinto oli korotetussa valmiudessa viikonvaihteen yli.

Sosiaali- ja terveysministeriö sai tiedon ensimmäisen päivän häiriöstä Valtioneuvoston tilannekeskukselta kello 15.23. STM valmiusyksikön henkilöstö jakoi tietoa STM:n valmiustoi-

---

[5] Tapahtuma-aikaan HUSissa oli kaksi johtajaylilääkäriä. Viran vakituinen viranhaltija keskittyi erityisesti tulossa olleen suuren organisaatiouudistuksen valmisteluun. Johtajaylilääkärin päivittäisten tehtävien hoitoa varten oli nimetty vs. johtajaylilääkäri.

mikunnalle, johon kuuluvat kansliapäällikkö, osastopäälliköt sekä valmiusyksikön ja viestinnän henkilöstöä. STM:n valmiuden kannalta keskeiset henkilöt olivat samassa tilaisuudessa tiedon tultua, joten he pystyivät heti arvioimaan tietoa keskenään. Arvion perusteella STM:n tilannekeskuksen toiminta päätettiin käynnistää.

STM:n tilannekeskus oli yhteydessä HUSiin saaden sieltä viimeisimmän tiedon tapahtuneesta. STM oli yhteydessä myös Kyberturvallisuuskeskukseen, Valtioneuvoston tilannekeskukseen sekä Sosiaali- ja terveysalan lupa- ja valvontavirastoon (Valvira).

Tilannekuvansa perusteella STM otti esille HUSin kanssa potilaiden ohjaamisen muihin sairaaloihin. STM oli yhteydessä muihin yliopistollisiin sairaaloihin tiedustellen, oliko heillä häiriöitä tietojärjestelmissä ja mikä olisi heidän valmiutensa ottaa vastaan HUSin potilaita. Häiriöitä ei muualla ollut. HUSin oman tilannekuvan perusteella potilaiden ohjaamiseen muihin sairaaloihin ei ollut syytä.

Kello 19.25 STM sai HUSista tiedon, että tilanne on ohi. STM:n tilannekeskus välitti tämän tiedon Valtioneuvoston tilannekeskukselle. Kello 19.40 STM:n tilannekeskustoiminta lopetettiin ja vastuu tilanteen seuraamisesta jäi päivystäjälle.

Seuraavan aamun häiriöstä STM sai tiedon kello 11.15 HUSin johtajaylilääkärin soitettua STM:n päivystäjälle. Päivystäjä jakoi tietoa STM:n sisällä. STM:n tilannekeskustoiminta aloitettiin kello 12.30. STM tiedusteli muilta yliopistollisilta sairaaloilta tietoja heidän mahdollisista häiriöistään. Sellaisia ei ollut. STM:ssä pohdittiin jälleen potilassiirtojen tarvetta. Tilannekeskus oli aktiivisesti yhteydessä Valtioneuvoston tilannekeskukseen, Kyberturvallisuuskeskukseen ja Valviraan. Kello 16.15 STM:n tilannekeskustoiminta lopetettiin ja vastuu tilanteen seuraamisesta jäi päivystäjälle.

Valtioneuvoston tilannekeskus sai tiedon ensimmäisen päivän häiriöstä mediaseurannan kautta kello 15.12. Tilannekeskus välitti tiedon kello 15.23 alkaen muun muassa STM:n päivystäjälle ja Kyberturvallisuuskeskukseen. Tilanteen korjautumisesta tilannekeskus sai tietää STM:n päivystäjältä kello 19.32. Tämän tiedon tilannekeskus välitti laajalla viranomaisjakelulla kello 20.09.

Toisen päivän häiriön Valtioneuvoston tilannekeskus havaitsi mediaseurannan avulla noin kello 11. Päivän aikana se sai tietoja tilanteen kehittymisestä STM:ltä sekä Kyberturvallisuuskeskukselta. Kello 18.24 tilannekeskus välitti tietoa päivän tapahtumista laajalla jakelulla eri virastoille.

Molemmat häiriöt olivat tilannekeskuksen päivittäisen sidosryhmille ja valtion ylimmälle johdolle suunnatun turvallisuuskatsauksen ensimmäisenä aiheena.

Valvira sai tiedon ensimmäisen päivän häiriöstä, kun yksi henkilökuntaan kuuluva havaitsi asian mediasta kello 16.22. Ylijohtaja soitti HUSin johtajaylilääkärille, jolta hän sai viimeisimmät tiedot tilanteesta. Ylijohtaja tiedotti tilanteesta kello 16.50 Valviran sisällä sekä STM:ään. Valvira seurasi tilannetta loppupäivän ajan. Myöhemmin illalla Valvira tiedotti tapahtuneesta Etelä-Suomen aluehallintovirastoon.

Valvira sai tiedon toisen päivän häiriöstä STM:stä kello 11.17. Tilannetta seurattiin koko päivän ajan. Ylijohtaja antoi medialle haastatteluja valvovan viranomaisen näkökulmasta. HUS ja Valvira sopivat keskenään, että Valviran edustaja menee televisiohaastatteluun Yleisradion alueuutisiin kello 18 jälkeen.

Valvira sai HUSilta tietoliikennehäiriöstä vaaratilanneilmoituksen.

Kyberturvallisuuskeskus sai tiedon ensimmäisen päivän tietoliikennehäiriöstä mediaseurannan kautta kello 15.20. Kyberturvallisuuskeskus oli yhteydessä HUSiin, josta kerrottiin kyseessä olevan laitevika. Kyberturvallisuuskeskus seurasi tilannetta Havaro-järjestelmän[6] avulla ja muilla tavoin eikä havainnut merkkejä ulkoisesta vaikuttamisesta.

Kyberturvallisuuskeskus oli yhteydessä Valviraan sekä STM:ään. HUSin tietohallinto teki omaaloitteisen ilmoituksen Kyberturvallisuuskeskukselle kello 17.40. HUS oli illan aikana useasti yhteydessä Kyberturvallisuuskeskukseen päivittäen tilannekuvaa. Kyberturvallisuuskeskus raportoi päivän tapahtumista liikenne- ja viestintäministeriölle (LVM).

Toisen päivän häiriö selvisi Kyberturvallisuuskeskukselle mediaseurannan kautta. HUSin tietohallinto teki ilmoituksen häiriöstä kello 13.53. Kyberturvallisuuskeskuksella ei ollut havaintoja ulkoisesta vaikuttamisesta, mistä se raportoi Valtioneuvoston tilannekeskukselle sekä LVM:n päivystäjälle.

1.3 Seuraukset

Häiriöt vaikuttivat koko HUSin alueella siten, että pääsy potilaiden tietoihin estyi kokonaan tai osittain. Tällöin jouduttiin toimimaan puutteellisin tiedoin ja erityisesti vakavasti sairaiden potilaiden hoito vaarantui. Vaikutuksia oli lähes kaikkien potilaiden hoitoon. Yksi leikkaus peruttiin häiriön johdosta.

Häiriöt eivät johtaneet Potilasvakuutuskeskukseen tehtyihin potilasvahinkoilmoituksiin eivätkä kanteluihin tai valvonta-asioihin Etelä-Suomen aluehallintovirastossa tai Valvirassa. Potilasvahinkoja ei tutkinnassa ilmennyt.

HUSin henkilökunnan tekemien potilasturvallisuuteen liittyvistä HaiPro-ilmoituksista yhdessäkään potilaalle aiheutunutta haittaa ei ollut luokiteltu vakavaksi. Tilanteeseen liittyviä ilmoituksia tehtiin 127.

HUSin henkilökunnan tekemiä riskeihin liittyviä HUS-Riskit-ilmoituksia tehtiin häiriön vuoksi kuusi. Ilmoituksissa kerrottiin tapahtuneista potilasturvallisuuden vaarantumisista, mutta ei raportoitu potilasvahinkoja.

Keskiviikkona 8.11.2017 kello 14.06–14.14 Uranus-palveluntuottajan konesalissa 1 tapahtunut yhteyksien katkeaminen vaikutti HUSin ohella muihinkin kyseistä jaettua palomuurialustaa käyttäneisiin asiakkaisiin. Katkon vaikutuksista heidän toimintaansa ei ole tietoa.

[6] Havaro-järjestelmä on huoltovarmuuskriittisille toimijoille ja valtionhallinnolle suunnattu tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä. Sen tarkoitus on tuottaa tietoa tietoturvaloukkauksista, jotta organisaatiot voivat suojautua niiltä ja rajoittaa vahinkoja. Liikenne- ja viestintävirasto vastaa järjestelmän ylläpidosta.

2 TAUSTATIEDOT

2.1 Tapahtumaympäristö, laitteet ja järjestelmät

HUSin tietoliikenteen ydin muodostuu kolmesta verkosta, jotka ovat HUSnet-runkoverkko, HUSnet-alueverkko ja HUSnet-lähiverkko. Tietoliikenneongelmat vaikuttivat tietojärjestelmien käyttöön koko runkoverkon alueella.

Runkoverkko yhdistää Hyksin, Hyvinkään, Lohjan, Länsi-Uudenmaan sekä Porvoon sairaanhoitoalueet. Alueverkko muodostaa kokonaisuuden, johon on liitetty muun muassa HUSin laboratoriotoimintojen (HUSLAB) ja HUS-Kuvantamisen toimipisteitä. Alueverkon käyttö mahdollistaa esimerkiksi röntgenkuvien ja laboratoriotulosten katselun HUSin eri toimipisteistä. Lähiverkko tarkoittaa rakennusten sisäistä tietoliikenneverkkoa, jonka avulla työasemat ja erilaiset lääkintälaitteet yhdistetään HUSnet-verkkoon. Lähiverkkoa käytetään esimerkiksi silloin, kun työasemalta tulostetaan yhteiskäyttöiselle verkkotulostimelle.

HUSin tietoliikenneverkossa on noin 200 verkkoliittymää, 2 200 tietoliikennelaitetta ja noin 4 500 WLAN-tukiasemaa. Verkon rakentamisesta, hallinnasta ja ympärivuorokautisesta valvonnasta vastaa ulkopuolinen ylläpitopalveluntuottaja.

Tietoliikenne HUS-runkoverkon ja muiden verkkojen välillä kulki runkoverkon kahdennetun runkokytkimen (Nexus C7010). kautta. Kaksi fyysistä runkokytkintä (A ja B) muodosti yhden loogisen runkokytkimen. Kytkimet toimivat aktiivi-aktiivi-mallin mukaan. Toinen kytkimistä kontrolloi kytkinten välistä kommunikointia ja kytkinparin toimintaa. Vikatilanteessa parin toinen kytkin ottaa toiminnallisuudet hoitaakseen tavoitteena minimoida viasta aiheutunut haitta.

Runkokytkimet olivat olleet päällä yhtäjaksoisesti noin kahdeksan vuotta. Uudelleenkäynnistyksen vaatineita huoltotoimenpiteitä kuten ohjelmistopäivityksiä ei ollut tehty. Laitevalmistajan (Cisco Systems Inc) tuki[7] runkokytkimien linjakorttien muistimoduuleille oli loppumassa joulukuussa 2017 ja ohjelmiston osalta päättynyt kesäkuussa 2017. HUS Tietohallinto oli aloittanut uuden korvaavan laitteen asennuksen. Uudemman sukupolven laitteet oli hankittu vanhojen runkokytkimien rinnalle, mutta niiden käyttöönotto oli kesken.

Keskeisin tietojärjestelmä HUSin toiminnan kannalta on Uranus-potilastietojärjestelmä, joka koostuu muun muassa potilaskertomusosiosta, potilashallinnosta ja toiminnanohjauksesta. Potilaskertomusosioon kirjataan esitiedot, havaintoarvot, hoitokertomus, kertomustekstit, lääkitys, nestehoidot, määräykset, riskitiedot, diagnoosit, toimenpiteet ja sanelut. Potilashallinto- ja toiminnanohjausosioon kirjataan henkilötiedot, lähetteet, konsultaatiot, jonot ja varaukset.

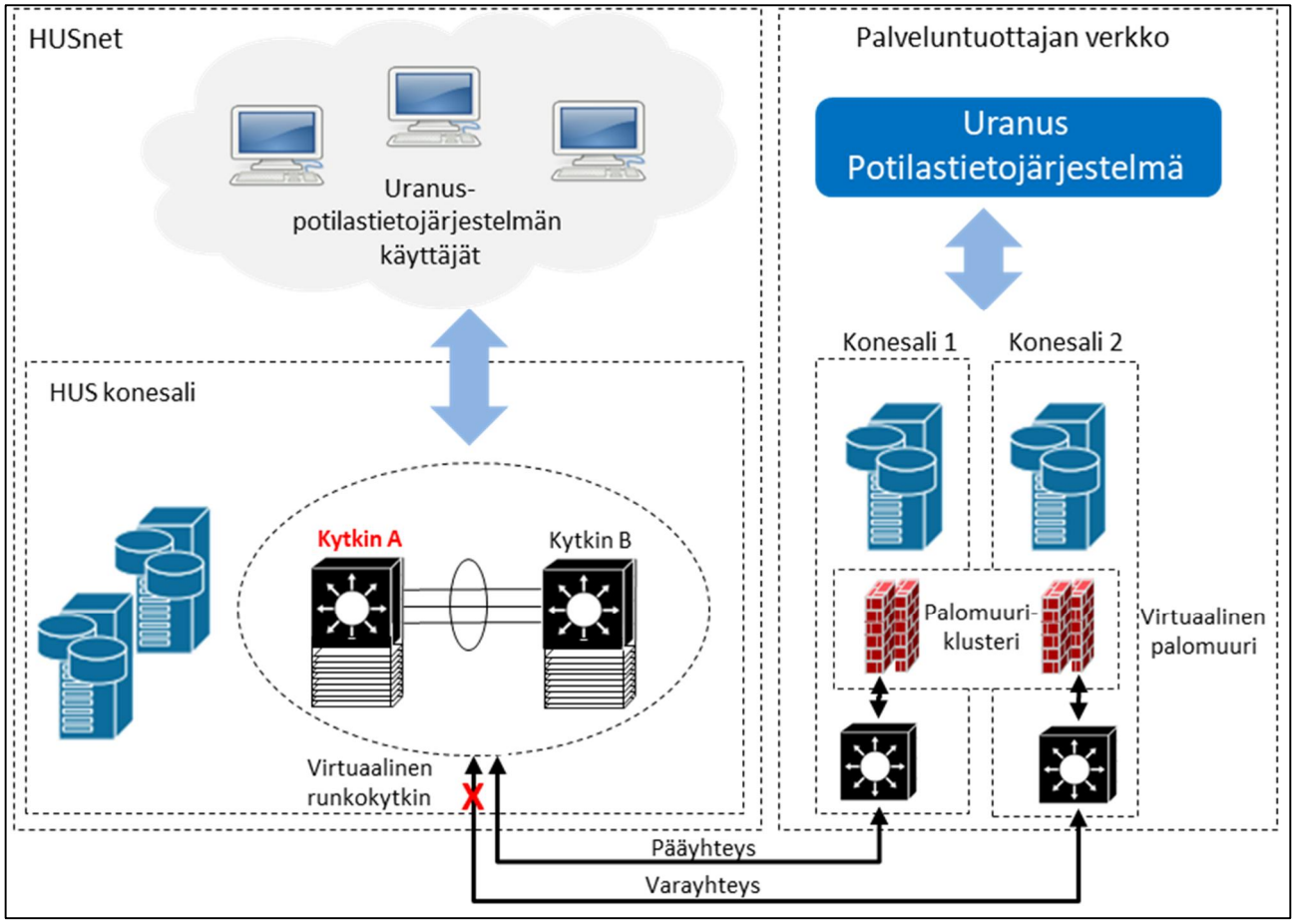
Uranus-potilastietojärjestelmästä on työpöytäintegraation (Ariel) kautta yhteys laboratoriojärjestelmään sekä kuvantamisen järjestelmään, joita voi käyttää myös suoraan kirjautumalla niihin erikseen ilman Uranusta. Järjestelmät ovat käytettävissä tällä tavalla jokaisen suunnitellun Uranus-päivityksen vaatiman tai muun käyttökatkon aikana.

Uranus-järjestelmän tuesta, ylläpidosta ja kehityksestä sekä käyttöpalveluista vastaa Uranus-palveluntuottaja. Järjestelmä toimii Uranus-palveluntuottajan konesalissa olevilla palvelimilla, johon järjestelmän käyttäjät muodostavat yhteyden tietoliikenneverkon kautta.

---

[7] Laitevalmistaja voi ilmoittaa päivämäärän, johon asti tuotteelle annetaan palvelusopimusten ja takuuehtojen mukaista palvelua ja tukea. Kyseisen päivämäärän jälkeen tuote valmistajan näkökulmasta poistuu käytöstä.

Tiistain 7.11.2017 häiriötä oli edeltänyt 23.10.2017 reititysongelma runkokytkimessä A, josta ylläpitopalveluntuottaja oli tehnyt runkokytkimien valmistajalle teknisen tukipyynnön[8]. Vastauksessa tukipyyntöön kehotettiin käynnistämään reititysprotokolla uudelleen. Tätä oli jo ehditty kokeilla, mutta se ei ollut poistanut ongelmaa. Lisäksi vastauksessa todettiin, että tuki käytettävälle ohjelmistoversiolle oli jo päättynyt ja ehdotettiin ohjelmiston versiopäivitystä, joka mahdollisesti voisi ratkaista ongelmat. Ohjelmiston päivitys olisi vanhan ohjelmistoversion vuoksi ollut monivaiheinen ja vaatinut komponenttien vaihtoja vanhaan laitteistoon. Uuden laitteiston käyttöönotto oli jo valmisteilla, joten HUS Tietohallinto ei katsonut ohjelmistopäivitystä tarkoituksenmukaiseksi. Uranus jäi todennäköisesti yhden yhteyden varaan. Ylläpitopalveluntuottaja tunnisti tilanteen, mutta tieto yhden yhteyden varaan jäämisestä ei kunnolla välittynyt HUS Tietohallinnolle. Ylläpitopalveluntuottaja ehdotti selvittelyjen jälkeen eli viikkoa myöhemmin kytkimen A yhteyksien siirtoa uusiin jo hankittuihin runkokytkimiin. Siirtoa alettiin valmistella 2.11.2017.



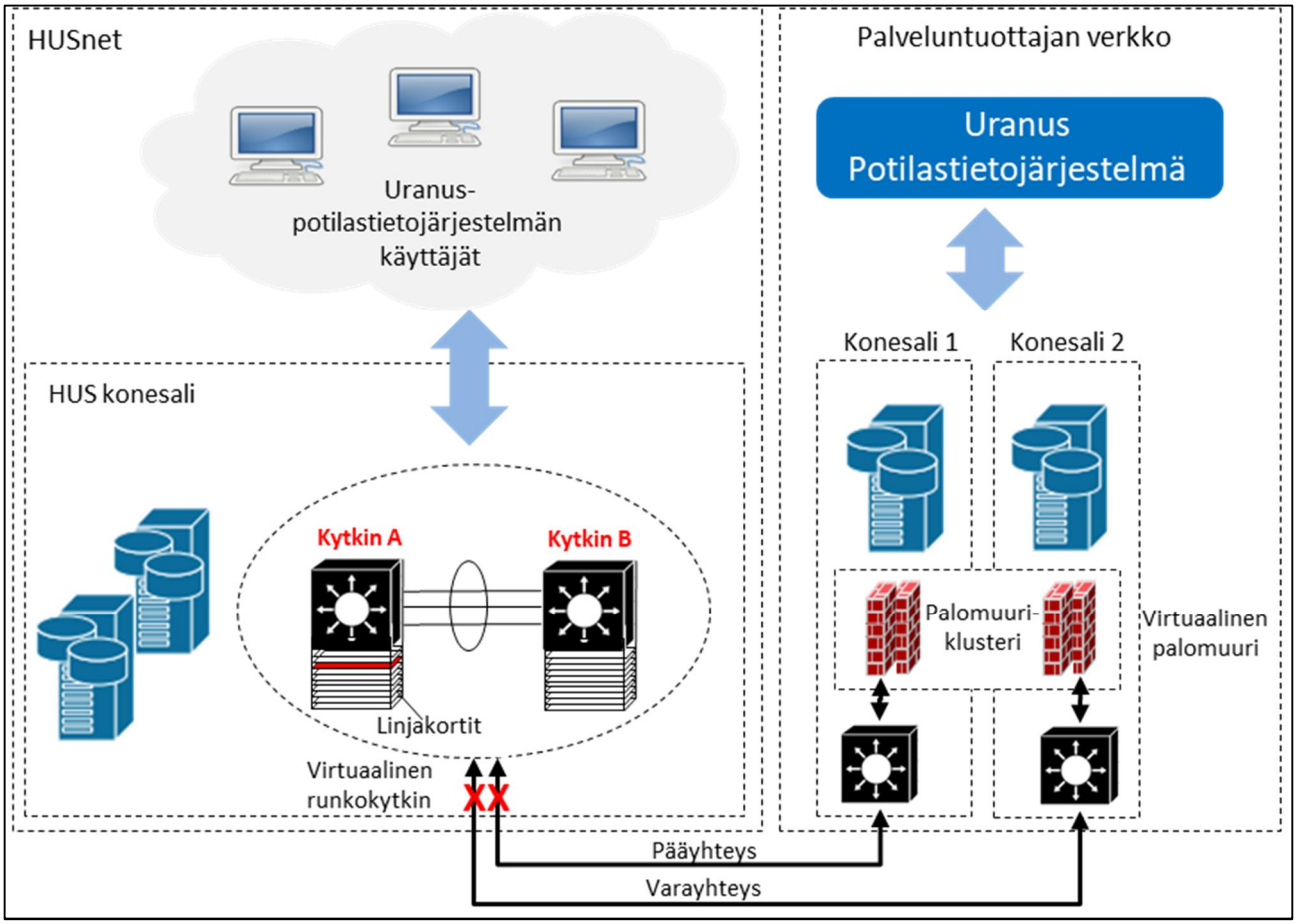
Kuva 1. Tilanne 23.10.2017 jälkeen. Kytkimeen A tullut vika vaikutti siten, että Uranus-potilastietojärjestelmän kahdennetusta yhteydestä toinen oli todennäköisesti poikki. Käyttäjien kannalta Uranus pysyi toiminnassa. (Kuva: OTKES)

Uranus-yhteyden häiriön selvityksessä runkokytkimissä havaittiin 7.11.2017 runkoreititysprosessin vioittuminen. Häiriö oli laajavaikutteisempi kuin 23.10.2017 ja kohdistui molempiin runkokytkimiin ja siten kaikkiin Uranuksen käyttäjiin sekä myös muuhun tietoverkon toimintaan. Vika olisi todennäköisesti ilman mahdollista kahdennuksen puuttumistakin aiheuttanut

[8] Laitevalmistaja Ciscon Technical Assistance Center (TAC) tarjoaa asiakkaille palvelua, jossa asiakas voi tehdä teknisen tukipyynnön saadakseen opastusta ongelman ratkaisemiseksi.

häiriön Uranus-yhteyteen. Reititysprosessin uudelleenkäynnistys tai muukaan toimenpide ei poistanut häiriötilannetta. Runkokytkin A jouduttiin käynnistämään uudelleen katkaisemalla virta. Tällöin yksi kytkimen kymmenestä linjakortista rikkoutui. Samassa yhteydessä havaittiin kytkimessä B olevassa reititysprosesseissa häiriötilanne. Kytkintä B ei uskallettu käynnistää uudelleen, koska pelättiin linjakortin rikkoutumista siitäkin.

Riskinarvioinnin perusteella todettiin, että on tärkeintä saada Uranus-yhteydet toimimaan esimerkiksi väliaikaisratkaisulla. Kun uusi linjakortti saapuisi yritettäisiin kytkimen B uudelleen käynnistämistä ja sen toimiessa linjakortin vaihtamista kytkimeen A. Tietoliikenteen ohjaaminen väliaikaisesti toimivalle reititykselle toteutettiin rakentamalla virtuaaliset tietoliikenneyhteydet muuttamalla runkokytkimen sisäisiä linkityksiä toimivalle linjakortille.



Kuva 2. Tilanne 7.11.2017 ennen kuin Uranus-yhteys saatiin toimimaan väliaikaisratkaisulla. Häiriö vaikutti merkittävästi sekä Uranus-potilastietojärjestelmän pää- että varayhteyden toimintaan. Kytkimestä A rikkoutui yksi linjakortti uudelleenkäynnistyksen yhteydessä. (Kuva: OTKES)

Runkokytkimissä A ja B esiintyi samanlainen reititysongelma, jonka aiheutti yhteisessä reititysprosessissa ilmennyt häiriö. Laitteiden kahdentaminen ei ole ratkaisu ohjelmistotason ongelmiin. Reititysprosessi on yhteinen koko verkolle eli sitä ei voi kahdentaa TCP/IP-verkoissa[9]. Osa reitityksistä toimi häiriöstä huolimatta. Konesalia lähellä olevien sairaaloiden

[9] TCP/IP on laajasti käytetty kahden Internet-liikennöinnissä käytettävän tietoliikenneprotokollan yhdistelmä (TCP = Transmission Control Protocol ja IP = Internet Protocol). IP-protokolla huolehtii pakettien reitittämisestä oikeaan kohteeseen kullekin laitteelle yksilöllisen IP-osoitteen avulla. TCP-protokolla puolestaan huolehtii pakettien luotettavasta siirtymisestä kohteiden välillä.

yhteydet kulkivat saman runkokytkimen kautta, joten niillä oli enemmän muihin kuin Uranus-järjestelmään liittyviä yhteysongelmia kuin kauempana olevilla sairaaloilla.

Laitevalmistaja Cisco on julkaissut 6/2016 Nexus 7000 -sarjan runkokytkimen muistikomponenttiongelmaa koskevan tiedotteen[10]. Tiedotteen mukaan muistikomponentin sisältävä linjakortti ei mahdollisesti käynnisty uudelleen yli 24 kuukauden yhtäjaksoisen päällä olon jälkeen, jos runkokytkimen ohjelmisto päivitetään tai sille tehdään muita ylläpitotoimia, jotka edellyttävät virran kytkemisen pois ja päälle.

Keskiviikkona 8.11.2017 Uranus-potilastietojärjestelmässä havaittu merkittävä hitaus johtui Uranus-palveluntuottajan Vahti[11]-ohjeiden vaatimukset täyttävän palomuurin poikkeavaan tilaan joutumisesta. Palomuuri oli otettu käyttöön Uranus-yhteydelle joitakin viikkoja aikaisemmin. HUSLABin laboratoriojärjestelmän puskuriin oli edellisen päivän tietoliikennehäiriön aikana jäänyt laboratoriotutkimusten tuloksia. Tietoliikenneyhteyksien palattua normaaliksi laboratoriojärjestelmä oli alkanut lähettää tuloksia Uranus-järjestelmään. Kukin vastaus oli tietomäärältään pieni, mutta vastauksia oli poikkeuksellisen suuri määrä.

Palomuurin tietoliikennettä tarkkaileva IPS-järjestelmä[12] tulkitsi liikenteen epänormaaliksi ja alkoi automaattisesti tutkia liikennettä. Normaalista poikkeavan liikenteen tutkintaan tarkoitettu muistialue täyttyi aiheuttaen palomuurille poikkeavan tilan. Kaikki liikenne palomuurin läpi hidastui merkittävästi. Potilastietojärjestelmäsovellukseen syntyi tietokantalukkoja tietoliikenneyhteyksien kadotessa. Tietokantalukko syntyy, kun tietokannan tietue lukitaan koko tiedon päivitykseen liittyvän toimintoketjun ajaksi muilta käyttäjiltä. Lukitus voi jäädä päälle esimerkiksi tietoliikenteessä esiintyvän häiriön vuoksi. Uranus-palveluntuottaja poisti tietokantalukkoja käynnistämällä sovelluspalveluita uudelleen.

Yhteyksien merkittävä määrä ei aiheuttanut itse palomuurin kapasiteetille ongelmaa, koska datan määrä oli vähäinen. Palomuurin kapasiteettia ja kuormitusta valvovaan valvontajärjestelmään ei tullut hälytyksiä.

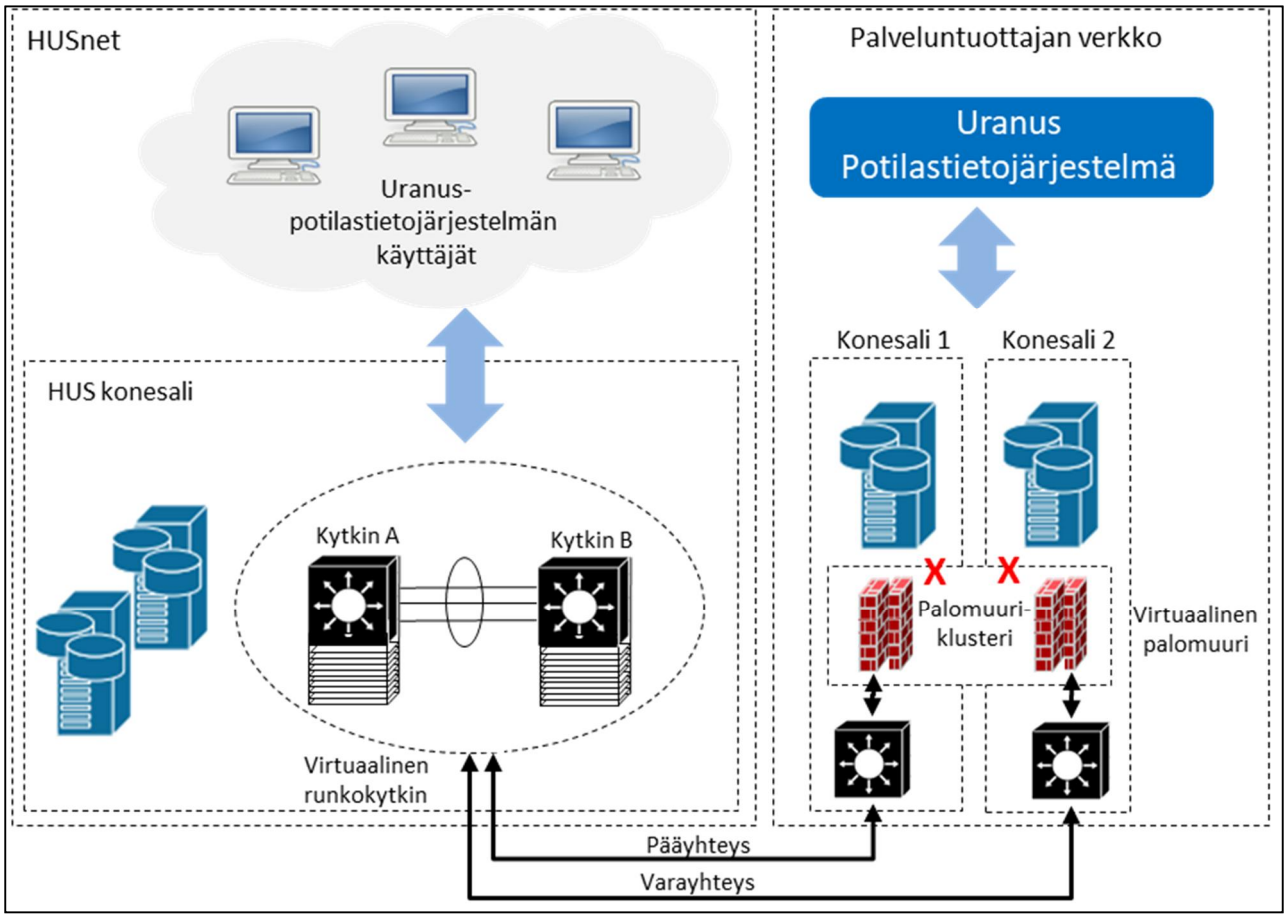
Palomuuria yritettiin palauttaa normaalitilaan käynnistämällä se ohjelmistollisesti uudelleen laitevalmistajan ohjeistuksen mukaisesti. Tietoliikenne oli siksi aikaa siirretty varmentavalle palomuurille, mutta ongelmat järjestelmiin kirjautumisessa eivät olleet poistuneet. Käynnistyksen olisi pitänyt tyhjentää muisti. Kun yhteydet siirrettiin takaisin uudelleen käynnistyksen jälkeen, huomattiin että palomuuri ei päästänyt enää läpi mitään liikennettä. Tietoliikenne siirrettiin takaisin varmentavalle laitteelle. HUS Tietohallinnon päätöksellä palomuuri poistettiin käytöstä Uranus-yhteydestä ja korvattiin reitittimellä, jolloin Uranus-yhteys palasi. Seuraavana päivänä vikaantuneelle palomuurialustalle tehty virran pois ja päälle kytkeminen tyhjensi muistin ja palomuuri alkoi toimia normaalisti.

---

10 Field Notice (FN) 63751, https://www.cisco.com/c/en/us/support/docs/field-notices/637/fn63751.html , haettu 25.10.2018. Field notice -ilmoituksella Cisco tiedottaa asiakkaita merkittävistä seikoista, joita ei luokitella hälytystasolle, mutta jotka usein vaativat asiakkaalta toimenpiteitä.

11 Vahti = Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

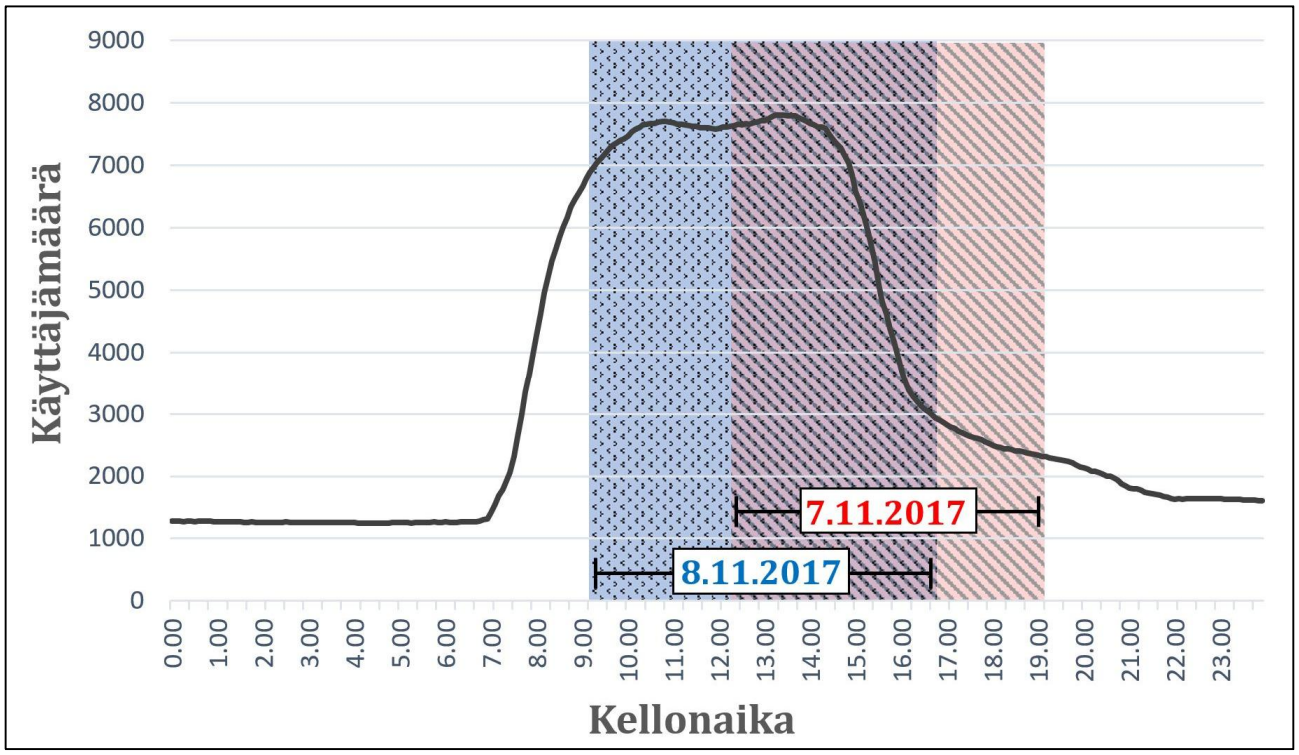
12 IPS = *Intrusion Prevention System,* tunkeilijan havaitsemisjärjestelmä



Kuva 3. Häiriöitä Uranus-potilastietojärjestelmän käyttöön 8.11.2017 aiheutui palomuurin muistialueen täyttymisestä ja potilastietojärjestelmäsovellukseen syntyneistä tietokantalukoista. (Kuva: OTKES)

2.2 Olosuhteet

HUSin Uranus-potilastietojärjestelmän käyttäjämäärä vastaa sairaaloiden vuorokausirytmiä. Aamuyöllä toiminnat ovat rauhallisimmillaan. Arkisin aamulla kello 7 alkaen toiminnat käynnistyvät nopeasti ja toiminta on aktiivisinta kello 14 saakka. Tämän jälkeen toimintojen määrä laskee ensin nopeasti kello 16 saakka ja sen jälkeen hitaammin saavuttaen aamuyötä vastaavan tason noin kello 22.

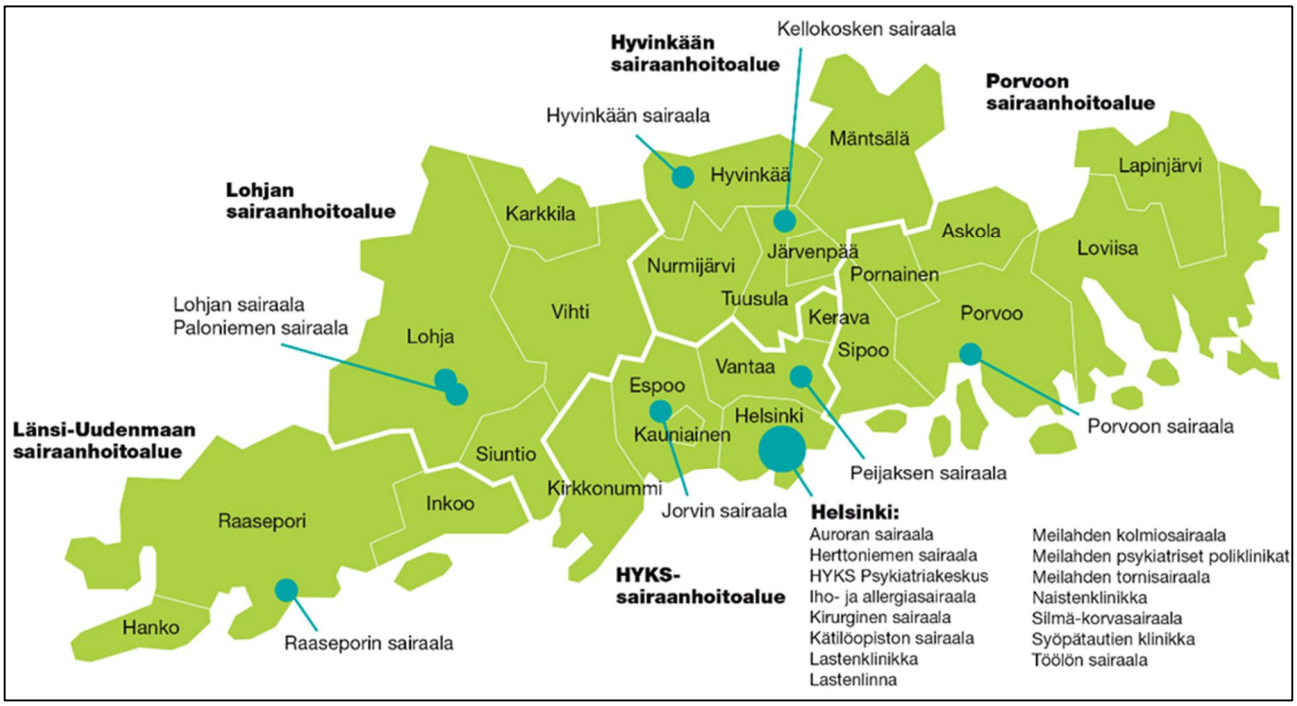


Kuva 4. Uranus-potilastietojärjestelmän käyttäjämäärä normaalina arkipäivänä. Kuvaan merkitty punaisella vinoviivoitetulla alueella 7.11.2017 ja sinisellä rasterikuviolla 8.11.2017 tapahtuneen tietoliikennehäiriön kesto (Kuva: HUS, merkinnät: OTKES)

2.3 Henkilöt, organisaatiot ja turvallisuusjohtaminen

Helsingin ja Uudenmaan sairaanhoitopiiri (HUS) on kuntayhtymä, joka tuottaa erikoissairaanhoidon palveluja 24 jäsenkunnan tarpeisiin. Alue on jaettu viiteen sairaanhoitoalueeseen, joita ovat HYKSin, Hyvinkään, Lohjan, Porvoon ja Länsi-Uusimaan sairaanhoitoalueet. HUS-kuntayhtymällä on 21 sairaalaa, minkä lisäksi HUS hoitaa potilaita Auroran ja Herttoniemen sairaaloissa.

HUSin sairaaloissa työskentelee noin 24 000 henkilöä ja tytäryhtiöissä lisäksi noin 600 henkilöä. Sairaalat hoitavat vuosittain yli 540 000 potilasta. HUSin alueella asuu yli 1,6 miljoonaa asukasta.



Kuva 5. HUSin alue häiriöiden aikaan. Alue jakautuu viiteen sairaanhoitoalueeseen. (Kuva: HUS)

HUS Tietohallinto on yksi HUSin tukipalveluista. Se toimittaa tietojärjestelmä- ja tietotekniikkapalveluita HUS kuntayhtymälle sekä sen yhteistyökumppaneille. HUS Tietohallinnossa työskentelee noin 350 henkilöä. Keskeisiä tietojärjestelmiä ovat potilastietojärjestelmät, talous- ja henkilöstöhallinnon järjestelmät sekä tukipalveluyksiköiden järjestelmät. Tietohallinto huolehtii käyttötukipalveluiden järjestämisestä sekä vastaa osaltaan koulutuksen järjestämisestä laitteille ja tietojärjestelmille. HUS Tietohallinto tiedottaa erilaisista tietotekniikan häiriöistä tekstiviestein sekä intranetissä. HUS Tietohallinnolla on laatusertifikaatti ISO 9001:2015.

HUS Tietohallinnolla oli sopimus potilastietojärjestelmäkokonaisuudesta Uranus-palveluntuottajan kanssa (CGI Suomi Oy) ja vastaavasti sopimus ulkoisen ylläpitopalveluntuottajan (Hewlett Packard Enterprise) kanssa tietoliikenneverkon rakentamisesta, hallinnasta ja ympärivuorokautisesta valvonnasta. Sopimuksessa oli muun muassa määritelty verkon aktiivilaitteiden sekä ohjelmistojen päivitys, seuranta ja asennus sekä korjausajat eri komponenteille.

Sopimukseen sisältyy muutoksenhallintamenettely, jolla suunnitellaan, kommunikoidaan, koordinoidaan, toteutetaan ja valvotaan IT-infrastruktuuriin tehtäviä muutoksia. Neljännesvuosittain on neuvottelu, jossa käydään läpi ylläpitopalveluntuottajan ehdotukset päivitettävistä ja uusittavista laitteista ja ohjelmistoista.

Ylläpitopalveluntuottaja vaihtui vuoden 2017 alussa. Runkokytkimiin liittyvät sopimukset ja ylläpitovastuut siirtyivät uudelle ylläpitopalveluntuottajalle 1.7.2017. Aikaisempi ylläpitopalveluntuottaja oli ensisijainen toimija häiriöiden selvittelyssä, koska sopimuksiin kuului avustaminen mahdollisissa siirtymävaiheen aikaisissa ongelmissa.

Ohjelmisto- ja laitepäivitystarpeista on keskusteltu aika ajoin HUS Tietohallinnon ja ylläpitopalveluntuottajan välillä. Varsinkin häiriötilanteiden jälkikäsittelyssä on tarkasteltu päivitysten ajantasaisuutta. Edellisen kerran ennen 23.10.2017 häiriötä kyseisen runkokytkimen päivitystarpeita oli arvioitu elokuussa 2016 ilmenneiden reititysongelmien selvittelyn yhteydessä. Tuolloin oltiin ajauduttu tilanteeseen, jossa ohjelmistopäivitys olisi edellyttänyt myös

laitekokoonpanon päivittämistä. Tästä luovuttiin, koska kokonaan uuden laitteiston käyttöönotto oli suunniteltu ja ajoitettu tammikuulle 2017. Tämä käyttöönotto viivästyi.

Varautumista ja toiminnan jatkuvuutta hallitaan ylätasolla sairaanhoitopiirin valmiusohjeella, joka oli päivitetty keväällä 2017. Ohjeen perusteella on laadittu muita konsernitason suunnitelmia, kuten Lääkinnän valmiussuunnitelma ja Kriisiviestintäohje. Myös nämä asiakirjat oli päivitetty keväällä 2017. HUS Tietohallinto on laatinut Tietotekniikka ja viestintätekniikkapalvelujen jatkuvuussuunnitelman sekä Uranus-potilastietojärjestelmälle oman jatkuvuussuunnitelman.

HUSin riskienhallintajärjestelmä (HUS-Riskit) on ollut käytössä vuodesta 2010 alkaen. Järjestelmä edesauttaa muun muassa poikkeama- ja ongelmatilanteiden sekä riskien hallintaa ja ennaltaehkäisyä. Järjestelmällä ei käsitellä potilaan hoitoon liittyviä hoitovirheitä tai vahinkoja, vaan pyritään turvaamaan häiriötön toimintaympäristö. Kaikilla henkilökuntaan kuuluvilla on oikeus tehdä järjestelmään ilmoituksia esimerkiksi tapaturmista, laitehäiriöstä tai laatupoikkeamista. Vuonna 2017 järjestelmään tehtiin yli 6 600 ilmoitusta.

Tutkittavana olevista häiriöistä HUS-Riskit-järjestelmään tehtiin kuusi ilmoitusta. Vakavin oli laaja ilmoitus erään sairaalan teho-osaston kokemuksista. Leikkaussaliin vietiin illan aikana kaksi tehohoidossa ollutta potilasta, joiden potilastiedot perustuivat muistinvaraiseen suulliseen raportointiin eikä tietoja voitu tarkistaa. Myös aikataulutettujen lääkitysten tiedot olivat muistinvaraisia. Tietoa lääkkeen antamisesta, annetun nesteen määrää tai muita kriittisiä riskitietoja, kuten allergioita, ei voitu varmistaa. Yksi potilassiirto osastolle estyi, koska tarkkoja aikataulutettuja lääkityksiä ei pystytty tulostamaan. Laboratoriopyynnöt tehtiin paperilla. Osaston sisäiset puhelimet, sähköinen sisäinen puhelinluettelo ja ovipuhelimet eivät toimineet. Tiedotusta tilanteesta saatiin vasta aivan katkon loppuvaiheessa. Viisi muuta häiriöilmoitusta olivat vähäisempiä.

Potilasturvallisuustyö HUSissa perustuu riskienarviointiin, toiminnan jatkuvaan kehittämiseen ja turvallisuuden ylläpitämiseen. Tavoitteena on estettävissä olevien, hoidosta aiheutuvien haittojen minimointi. Tärkeää tietoa saadaan vaaratapahtumien HaiPro-raportointijärjestelmästä, johon henkilökunta voi ilmoittaa vaaratapahtumat. Vuonna 2017 järjestelmään tehtiin yli 21 000 ilmoitusta eli keskimäärin lähes 60 ilmoitusta vuorokaudessa. Kaikki vaaratapahtumat käsitellään tapahtumayksikössä ja käsittelyn perusteella päätetään jatkotoimet vaaratapahtumien ehkäisemiseksi ja toiminnan kehittämiseksi. Potilasturvallisuusraportti laaditaan vuosittain[13].

HaiPro-järjestelmään tehtiin tiistain 7.11.2017 häiriöstä 107 ja keskiviikon 8.11.2017 häiriöstä 20 ilmoitusta. Häiriöihin liittymättömiä ilmoituksia oli kyseisinä päivinä 53 ja 58. Osa tietoliikennehäiriöön liittyvistä ilmoituksista koski vain yhtä potilasta, mutta useissa ilmoituksissa oli tehty yhteenveto vaikutuksista useamman potilaan hoitoon. Osassa ensimmäiselle päivälle kirjatuista ilmoituksista käsiteltiin samalla myös toisen päivän häiriö.

Näistä 127 HaiPro-ilmoituksesta kuvautuu tietojärjestelmähäiriön aiheuttama huomattava haitta potilastyölle. Ilmoitusten käsittelijöiden arvion mukaan noin kolmasosassa ilmoitetuista tilanteista potilaalle aiheutui tilanteesta lievä haitta. Kohtalaiseksi haitta oli arvioitu muutamassa tapauksessa. Vakavia haittoja potilaille ei raportoitu. Osassa ilmoituksia tietojärjestelmähäiriö oli kuvattu lyhyesti tai ainoastaan viitattu yleisesti tiedossa olleeseen tietojär-

[13] Vuoden 2017 potilasturvallisuusraportti http://www.hus.fi/potilaalle/laatu-ja-potilasturvallisuus/potilasturvallisuus-hussa/Documents/HUS%20Potilasturvallisuusraportti%202017.pdf , haettu 26.10.2018

jestelmähäiriöön. Useassa ilmoituksessa tietojärjestelmähäiriön aiheuttama haitta potilastyölle oli kuvattu analyyttisesti ja myös potilasturvallisuusvaikutusta oli arvioitu. Esille tuli myös esityksiä käytännön ratkaisuiksi tiedonkulun ongelmiin.

2.4 Viranomaisten ennalta ehkäisevä toiminta

2.4.1 Sosiaali- ja terveysministeriö (STM)

STM ohjaa valtakunnallisten yhtenäisten lääketieteellisten hoidon perusteiden toteutumista. STM:lle kuuluu erikoissairaanhoidon yleinen suunnittelu, ohjaus ja valvonta. Terveydenhuollon varautumisen yleiseen ohjaamiseen liittyen STM on muun muassa laatinut oppaita[14] ja raportteja[15]. STM järjestää säännöllisesti koulutuspäiviä, joissa käsitellään myös turvallisuuteen ja varautumiseen liittyviä asioita.

2.4.2 Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira)

Valviran tehtäviä määrittävät useat lait. Valviran tehtävänä on varmistaa potilasturvallisuutta ja edistää terveydenhuoltopalvelujen laatua ennaltaehkäisemällä epäasianmukaisia hoito- ja toimintakäytäntöjä ja puuttumalla säädösten vastaiseen tai muutoin virheelliseen menettelyyn tai laiminlyönteihin. Aluehallintovirastot ovat ensisijaiset sosiaali- ja terveydenhuoltoa ohjaavat ja valvovat viranomaiset alueellaan. Valviralle kuuluvat sosiaali- ja terveydenhuollon ohjaukseen ja valvontaan liittyvät asiat erityisesti silloin, kun kyseessä on periaatteellisesti tärkeät tai laajakantoiset asiat, useaa aluehallintoviraston aluetta tai koko maata koskevat asiat. Lisäksi Valviralle kuuluu terveydenhuollon ammattihenkilöstön ohjaukseen ja valvontaan liittyviä asioita sekä aluehallintovirastojen ohjaus niiden toimintaperiaatteiden, menettelytapojen ja ratkaisukäytäntöjen yhdenmukaistamiseksi.

Valviran toteuttama valvonta on suunnitelmallista ja jälkikäteistä. Suunnitelmallista, ennakoivaa valvontaa toteutetaan Valviran ja aluehallintovirastojen yhdessä laatimien valvontaohjelmien ja -suunnitelmien mukaisesti. Valvontaohjelmakaudella 2016–2019 viranomaisvalvonnan painopiste on toimintayksiköiden omavalvonnan tukemisessa ja varmistamisessa.

Valvira valvoo myös terveydenhuollon laitteiden ja tarvikkeiden (TLT)[16] sekä niiden käytön turvallisuutta. Myös ohjelmisto[17] tai tietojärjestelmä[18] voi olla terveydenhuollon laite. Tietojärjestelmiin liittyvissä säädöksissä viitataan tietoliikenneyhteyksiin vain tietoturvaa koskevissa kohdissa. Terveydenhuollon tietoliikennetekniset ratkaisut eivät ole TLT-säädösten piirissä.

---

14 *Terveydenhuollon valmiussuunnitteluopas,* STM:n oppaita 2002:5; *Riskienhallinta ja turvallisuussuunnittelu - Opas sosiaali- ja terveydenhuollon johdolle ja turvallisuusasiantuntijoille,* STM:n julkaisuja 2011:15.

15 *Alueellinen varautuminen ja valmiussuunnittelu sairaanhoitopiireissä,* STM:n raportteja ja muistiota 2014:37.

16 Terveydenhuollon laitteella tarkoitetaan lain terveydenhuollon laitteista ja tarvikkeista (629/2010) mukaan instrumenttia, laitteistoa, välinettä, ohjelmistoa, materiaalia tai muuta yksinään tai yhdistelmänä käytettävää laitetta tai tarviketta, jonka valmistaja on tarkoittanut käytettäväksi ihmisen a) sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen; b) vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin; c) anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun; taikka d) hedelmöittymisen säätelyyn.

17 Ohjelmiston määritteleminen terveydenhuollon laitteeksi vaatii lähes poikkeuksetta tapauskohtaista arviointia. Tarkemmin määrittelystä on säädetty EU:n viranomaisohjeessa, http://www.valvira.fi/documents/14444/37132/sw_luokitteluohje_2012-03-13.pdf, haettu 23.8.2018.

18 Terveydenhuollon TLT säännösten mukaisten tietojärjestelmien ja tiedonhallinnan yleiset vaatimukset on säädetty laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja yksityiskohtaiset olennaiset vaatimukset Terveyden ja hyvinvoinnin laitoksen määräyksissä, https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveys-alalla/maaraykset-ja-maarittelyt/maaraykset.

2.4.3 Aluehallintovirasto

Aluehallintoviraston tehtävänä on muun muassa varautumisen ja valmiussuunnittelun yhteensovittaminen, kuntien valmiussuunnittelun tukeminen sekä alue- ja paikallishallinnon turvallisuussuunnittelun edistäminen. Tarkastelu rajoittuu organisaatioiden ylätasolle ja eri organisaatioiden väliseen yhteistyöhön.

Aluehallintovirasto järjestää vuosittain maakunnallisen valmiusharjoituksen vuorotellen alueensa eri maakuntien eri alojen toimijoiden kanssa. Valmiusharjoitusta edeltäen aluehallintoviraston sosiaali- ja terveydenhuoltoyksiköt pyytävät harjoittelevan maakunnan kunnilta ja sairaanhoitopiiriltä päivitetyt valmiussuunnitelmat. Uudenmaan valmiusharjoitus on järjestetty viimeksi vuonna 2016 ja seuraavaa on suunniteltu vuodelle 2020. Aluehallintovirasto tarjoaa harjoituksen yleispuitteet. Eri organisaatiot voivat itse suunnata harjoitteluaan itselleen ajankohtaisiin harjoitusaiheisiin.

Etelä-Suomen aluehallintovirasto osallistuu HUSin, Valviran ja aluehallintoviraston puolen vuoden välein järjestettävään yhteistyökokoukseen. HUSin johto esitteli tietojärjestelmähäiriötä ja siitä selviämistä tuoreeltaan 15.11.2017 olleessa kokouksessa.

2.4.4 Huoltovarmuuskeskus

Huoltovarmuuskeskus on työ- ja elinkeinoministeriön (TEM) hallinnonalan laitos. Sen tehtävänä on erityisesti varautumista koordinoimalla ja ohjaamalla yhteistyössä muiden viranomaisten ja elinkeinoelämän kanssa varmistaa, että yhteiskunnalle kriittisimmät järjestelmät toimivat kaikissa tilanteissa. Huoltovarmuuskeskus suunnittelee ja rahoittaa muun muassa erilaisia tietojärjestelmien ja tietoliikenteen varmennus- ja varajärjestelyitä.

Huoltovarmuuden varmistamisessa elinkeinoelämän ja julkishallinnon välinen yhteistyö on ratkaisevassa asemassa. Huoltovarmuuskeskus tukee tätä yhteistyötä muun muassa kehittämällä ja kouluttamalla yrityksille jatkuvuudenhallinnan työkaluja, toteuttamalla yritysten ja viranomaisten yhteisiä harjoituksia sekä tukemalla ja ohjaamalla toimialojen ja niiden yhteystyöelinten eli poolien toimintaa.

Terveydenhuoltopooli on sopijaosapuolten ja viranomaisten yhteistyöelin. Se on varautumisorganisaatio, eikä sillä ole valmiustehtäviä. Poolin toiminta perustuu Huoltovarmuuskeskuksen, HUSin, Lääketeollisuus ry:n, Sailab ry:n sekä Apteekkitavaratukkukauppiaat ry:n väliseen sopimukseen. Poolin muodostavat sitä johtava poolitoimikunta, poolin toimisto ja alan yritykset. Poolin tehtävänä on hoitaa selvitys-, suunnittelu- ja järjestelytehtävät, jotka ovat tarpeen terveydenhuollon materiaalisen huoltovarmuuden ja sen edellyttämien logististen toimintojen varmistamiseksi sekä normaaliajan vakavissa häiriötilanteissa että poikkeusoloissa. Pooli muodostaa oman toimialansa huoltovarmuuden valtakunnallisen strategisen tilannekuvan. Pooli tekee riskikartoituksia ja osallistuu ja edistää asiantuntemuksellaan eri toimijoiden ja toimialojen yleistä varautumista. Jokainen organisaatio vastaa kuitenkin itse valmiussuunnittelustaan ja jatkuvuuden hallinnastaan. Pooli järjestää valmiuskoulutusta, seminaareja ja harjoituksia.

2.5 Tilanteessa toimineet viranomaiset ja niiden toimintavalmius

2.5.1 Sosiaali- ja terveysministeriö (STM)

STM:n valmiusyksikkö ylläpitää hallinnonalan häiriötilanteiden tilannejohtamisvalmiuksia ja STM:n päivystysjärjestelmää. STM:llä on jatkuva päivystys. Poikkeavassa tilanteessa STM:n

toimintaa johtaa aluksi valmiuspäivystäjä ja sen jälkeen substanssivirkamies, STM:n valmiuspäällikkö tai STM:n johto. STM:llä ei ole operatiivisessa tilanteessa johtamisvastuita muihin organisaatioihin nähden.

STM:n valmiusorganisaation yksi tehtävä on antaa tarvittaessa toimeksianto hallinnonalan valtakunnallisille toimijoille[19]. STM on nimennyt HUSin yhdeksi vastuuorganisaatioksi tiettyihin toimialan valtakunnallisiin valmiustehtäviin. HUS huolehtii muun muassa lentoevakuointivalmiudesta, vakavien palovammapotilaiden hoidosta ja Myrkytystietokeskuksen toiminnasta.

Poikkeuksellisessa tilanteessa STM:n valmiusorganisaation tehtävä on ylläpitää valtakunnallista tilannekuvaa erityisesti huolehtien siitä, että STM:llä ja Valtioneuvoston tilannekeskuksessa olisi yhteinen tilannekuva. Lisäksi valmiusorganisaatio pitää yhteyttä tarpeen mukaan muiden ministeriöiden päivystäjiin, Valviraan, Kyberturvallisuuskeskukseen ja muihin sairaanhoitopiireihin.

2.5.2 Kyberturvallisuuskeskus

Viestintäviraston osana toimineen[20] Kyberturvallisuuskeskuksen tehtävänä on seurata kyberturvallisuusuhkia ja koota kyberturvallisuutta koskevaa tietoa eri toimijoille. Kyberturvallisuuskeskus toimii sekä julkisen että yksityisen sektorin kanssa. Huoltovarmuuden kannalta kriittisten toimijoiden kohdalla keskus varoittaa uhkaavista tietoturvapoikkeamista sekä pyydettäessä avustaa kyberuhkiin varautumisessa. Kyberturvallisuuskeskus myös tukee näiden tahojen harjoitustoimintaa antamalla asiantuntijatukea harjoitusten suunnitteluun ja järjestämiseen. Merkittävistä kyberuhista keskus varoittaa ja valistaa kansalaisia. Saadessaan ilmoituksen mahdollisesta kyberhäiriöstä Kyberturvallisuuskeskus tekee tapauksesta vakavuusarvion, jonka perusteella ryhdytään tarvittaessa lisätoimiin asian selvittämiseksi. Kyberturvallisuuskeskuksella on jatkuva toimintavalmius.

2.5.3 Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira)

Merkittävä osa Valviran terveydenhuoltoon kohdistamasta valvonnasta on jälkikäteistä. Jälkikäteinen valvonta käynnistyy usein Valviralle tulleiden kantelujen tai ilmoitusten perusteella. Valvira voi käynnistää valvontatoimenpiteet myös oma-aloitteisesti, esimerkiksi julkisuudessa esiintyneiden tietojen perusteella.

Valviralla ei ole sellaisia välitöntä reagointia edellyttäviä tehtäviä, jotka vaatisivat päivystysjärjestelyjä.

Terveydenhuollon laitteen tai tarvikkeen (TLT) aiheuttamasta vaaratilanteesta on aina tehtävä ilmoitus Valviralle niin pian kuin mahdollista. Vakavasta vaaratilanteesta on ilmoitettava kymmenen vuorokauden ja läheltä piti -tilanteesta 30 vuorokauden kuluessa. HUS teki TLT-säädösten mukaisen vaaratilanneilmoituksen 7.11.2017 tietoliikennehäiriöstä Valviraan 21.11.2017, vaikka häiriö ei ollut näiden säädösten tarkoittamissa laitteissa.

Valviran erityisenä tehtävänä on ohjata ja valvoa erikoissairaanhoitoa muun muassa silloin, kun kysymyksessä on periaatteellisesti tärkeät tai laajakantoiset asiat. Tähän tehtävään liittyen Valvira teki 17.11.2017 HUSille selvityspyynnön 7.–8.11.2017 tapahtuneesta tietoliikennehäiriöstä.

---

19 Terveydenhuoltolain (1326/2010) 38 §:n mukaan valtio voi osallistua terveydenhuollossa tarvittavan valmiuden ylläpitämiseen ja erityistilanteiden hoitamiseen rahoittamalla sellaista toimintaa, jonka korvaaminen valtion varoista on erityisestä syystä tarkoituksenmukaista. Toimintaa varten STM voi nimetä ja valtuuttaa valtakunnallisia toimijoita.

20 1.1.2019 alkaen Liikenne- ja viestintäviraston yhteydessä

HUS antoi Valviralle selvityksen 4.1.2018. Selvityksen mukaan HUS oli aloittanut useita toimenpiteitä tietoliikennejärjestelmän valvontaan, sisäiseen hälyttämiseen, HUS-konsernin valmiusjohdon toimintaan sekä viestintään liittyen. Tietoliikenneverkon elinkaareen ja huollon mahdollistamiseen huoltoikkunoin oli kiinnitetty huomiota.

Valvira antoi 14.2.2018 asiassa päätöksen, jonka mukaan asia ei anna Valviran osalta aihetta enempiin toimenpiteisiin. Päätöksessä Valvira toteaa, että HUSin selvityksessä oli kuvattu kattavat kehitystoimenpiteet, joiden toteuttamisella voidaan perustellusti katsoa voitavan ennaltaehkäistä vastaavan kaltaisia häiriötilanteita ja lieventää niiden vaikutuksia sekä parantaa häiriötilanteiden hallintaa ja ongelmien korjaamista.

2.5.4 Valtioneuvoston tilannekeskus

Valtioneuvoston kansliassa toimii valtioneuvoston tilannekeskus, joka tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista koottua tilannekuvaa. Tilannekeskuksessa on jatkuva päivystys. Tilannekeskus yhdistää eri viranomaisilta ja avoimista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille.

2.6 Tallenteet

Tutkintaryhmällä on ollut käytössään eri toimijoiden laatimia raportteja, jotka ovat perustuneet tietoliikenneverkon toimintaan liittyviin tallenteisiin.

2.7 Säädökset, määräykset, ohjeet ja muut asiakirjat

2.7.1 Terveydenhuollon valmiussuunnitteluopas

Sosiaali- ja terveydenhuollon valmiussuunnittelun ohjeistusta ollaan uusimassa[21]. Häiriöiden aikaan voimassa oli vuonna 2002 julkaistu Terveydenhuollon valmiussuunnitteluopas[22]. Sen mukaan terveydenhuollon laitoksen on varauduttava suunnitelmissaan koko tietoverkkonsa lamautumiseen ja sen toiminnan korvaamiseen muilla keinoin. Hyvillä työtavoilla voidaan minimoida tietokonehäiriöiden vaikutuksia päivittäiseen työhön. Vastaanottopotilaista voidaan tehdä listaukset paperille ja varmistaa näin vastaanoton jatkuminen. Myös laboratorio ja röntgen voivat käyttää erilaisia listauksia varmistaakseen päivittäisen työn jatkumisen atk-häiriön aikana. Oppaan mukaan tietoverkon kaatuminen merkitsee terveydenhuollon yksikössä paluuta vuosia taaksepäin työtavoissa. Tuolloin käytetään kynää, paperia, faksia ja puhelinta sekä jopa lähettiä asioiden hoitoon. Tietokonehäiriön aiheuttamat ongelmat on helppo testata sulkemalla tietokoneet vaikkapa vain päiväksi.

2.7.2 HUSin valmiusohjeet ja -suunnitelmat

HUSin valmiusohjeen mukaan varautumista ja jatkuvuuden hallintaa johdetaan pääsääntöisesti samoilla periaatteilla kuin muutakin palveluntuotantoa. Kunkin organisaation johtajalla ja esimiehellä on toiminnallinen kokonaisvastuu. HUS-konsernin varautumista johtaa toimitusjohtaja. Hänen alaisuudessaan varautumista ohjaa johtajaylilääkäri ja hänen alaisuudessaan toimivat turvallisuus- ja valmiusjohtaja sekä lääkintäpäällikkö. Sairaanhoitopiirillä on valmius- ja turvallisuustoimikunta, jonka tehtävänä on linjata ja kehittää varautumista.

---

21 Uusi valtakunnallinen valmiussuunnitteluohje sosiaali- ja terveydenhuoltoon on valmistumassa STM:n ja Kuntaliiton yhteishankkeena, https://alueuudistus.fi/valmius-ja-jatkuvuudenhallinta-sote-rakenteissa-hanke , haettu 23.10.2018. Uusi ohjeistus laitetaan sen valmistuttua STM:n valmiusyksikön sivuille, https://stm.fi/valmiusasiat.

22 STM:n oppaita 2002:5, http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/70059/stmopas2002-15.pdf?sequence=1&isAllowed=y, haettu 17.10.2018.

Sairaanhoitoalueen johtaja vastaa sairaanhoitoaluetasoisen varautumisen suunnittelusta. Muista poiketen HYKS-sairaanhoitoalueen tulosyksiköiden valmiussuunnitteluvelvoite toteutuu sairaalakiinteistökohtaisen lääkinnällisen valmiussuunnitelman kautta. Tulosyksikön tulee tunnistaa omaan toimialansa kriittisimmät hoitoprosessit. Tulosyksikön tulee laatia arvio siitä, kuinka ja missä järjestyksessä eri hoitoprosesseista kyetään luopumaan, mikäli toiminnan edellytykset heikkenevät kriittisesti.

Kullekin sairaalakiinteistölle on nimetty valmiuspäällikkö, joka vastaa sairaalan lääkinnällisen valmiuden ajantasaisuudesta ja eri toimialojen suunnitelmien synkronoinnista. Valmiuspäällikkökokouksissa seurataan ja kehitetään sairaalatoimintojen lääkinnällistä varautumista ja suunnitelmien yhteensopivuutta.

Sairaaloissa on sairaalakohtainen valmiustoimikunta, jonka tehtävänä on pitää valmiussuunnitelma ajan tasalla. Sairaalalla tulee olla jatkuvuudenhallinnan suunnitelma osana turvallisuus- ja pelastussuunnitelmaa.

Suunnitelmissa tulee käsitellä organisaation valmiudet jatkaa toimintaa muun muassa kriittisen tietojärjestelmän toimintakatkoksen aikana.

HUSilla on valmiuspäivystäjä jatkuvassa varalla olossa. Valmiuspäivystäjän tehtävä on arvioida häiriöstä saadut tiedot ja niiden pohjalta ryhtyä tilanteen edellyttämiin toimenpiteisiin. Valmiuspäivystäjä ilmoittaa häiriöstä johtajaylilääkärille, joka voi kutsua koolle tarvittaessa HUSin valmiusjohdon. Valmiusjohdon tehtävänä on pitää yllä tilannekuvaa ja valmistautua nostamaan konsernin toiminnallista ja viestinnällistä valmiutta sekä päätöksentekovalmiutta.

HUSin lääkinnän valmiussuunnitelmassa yhdeksi uhkakuvaksi on kirjattu tietojärjestelmän häiriö. Suunnitelman mukaan laaja-alaisten ja pitkäkestoisten toimintahäiriöiden varalle tulee toimintayksiköissä olla suunnitelmat toteuttaa välttämättömät potilashoitoon liittyvät toiminnot ilman tietotekniikkaa. Tämä edellyttää valmiutta kirjata potilastiedot ja muu dokumentaatio manuaalisesti ja toteuttaa kriittiset laboratoriotutkimukset ja kuvantamispalvelut poikkeusjärjestelyin.

Uranus-potilastietojärjestelmän jatkuvuussuunnitelmassa kuvataan menettelyt, joita hoitohenkilökunnan tulee noudattaa käyttökatkoksen tapahtuessa. Suunnitelman mukaan Tietohallinto tiedottaa sisäisesti yllättävistä käyttökatkoksista sähköpostilla, puhelimitse ja/tai intranetin avulla. Katkon aikana potilaiden henkilötiedot sekä ilmoittautumis-, poistumis- ja käyntitiedot kirjataan tätä varten suunnitetuille lomakkeille. Potilaskertomusten tekstit voidaan kirjoittaa työaseman tekstinkäsittelyohjelmalla. Vuodeosastolla määräykset, hoitokertomustiedot ja vastaavat kirjataan käsin hoitosuunnitelmalomakkeelle. Katkon jälkeen kirjatut tiedot siirretään tietojärjestelmään.

Digisanelu tai sanelun purkaminen ei ole mahdollista käyttökatkon aikana. Suunnitelman mukaan käyttökatkot ovat yleensä lyhyitä ja järjestelmän korjaantumista voidaan odottaa noin kaksi tuntia, jonka jälkeen voidaan siirtyä kasettisaneluihin.

Uranus-jatkuvuussuunnitelman liitteessä on mainittu internetosoitteet, joiden kautta pääsee suoraan muun muassa laboratorio- ja kuvantamispalveluiden järjestelmiin. Näitä osoitteita on mahdollista käyttää tilanteissa, joissa vika rajoittuu esimerkiksi vain potilastietojärjestelmään ja sen yhteyksiin.

Tietoliikenne- ja viestintätekniikkapalveluiden jatkuvuussuunnitelmassa asiakkaan erityisen kriittisiksi toiminnoiksi on tunnistettu muun muassa leikkaukset, tehohoito ja päivystys sekä kuvantaminen ja laboratoriotoiminnot niihin liittyen. Myös elvytyshälytykset ja lääkitystiedot ovat erityisen kriittisiä. Lähes kaikki kriittiset toiminnot ovat riippuvaisia HUSnet-

verkkopalvelun toiminnasta. Useimmat verkon keskeiset komponentit on kahdennettu. Molempien runkokytkimien menettäminen yhtä aikaa voi suunnitelman mukaan johtua muun muassa ohjelmistovirheestä, konfigurointivirheestä tai tahallisesta verkkohyökkäyksestä.

Suunnitelman mukaan häiriötilanteen pitkittyessä hoitohenkilöstö odottaa noin 15 minuuttia, jonka jälkeen ryhdytään toimimaan osaston oman jatkuvuussuunnitelman mukaan.

Tunnistettuina riskeinä on muun muassa muutoksenhallintaprosessin noudattamatta jättäminen sekä kahdennusten ja palautusten testaamattomuus.

HUSin tietoliikenneverkkoja valvotaan palveluna hankitulla valvontajärjestelmällä. Yksittäisen komponentin vikaantumiseen varaudutaan kriittisten komponenttien kahdennuksella ja palveluntoimittajan huoltopalvelusopimuksilla.

Suunnitelmassa todetaan, että tietohallinnon ja kliinisten yksiköiden valmiussuunnitelmien välillä ei ole toiminnassa mitään relaatiota eli yksiköt päättävät toiminnastaan itse. Suunnitelman mukaan käytäntö on osoittanut, että valmiussuunnitelmia ei yksiköissä kovin laajalti tunneta. Yksiköissä ei häiriötilanteissa osata käyttää muita varajärjestelyjä vaan odotetaan tietohallinnon ratkaisuja.

HUSin kriisiviestintäohjeen mukaan kriisitilanteessa viestintä keskitetään. Viestinnän tavoite on muun muassa välittää oikea kuva tilanteesta henkilökunnalle, potilaille ja heidän omaisille sekä sidosryhmille ja julkisuuteen. Viestinnällä myös tiedotetaan muutoksista palveluissa.

2.7.3 HUS Tietohallinnon laatukäsikirja

Tietohallinnon laatukäsikirja koostuu yleisen osan lisäksi Asiakkuuksien hallinta, Ydinprosessi ja palvelun elinkaaren hallinta, Tuotteet ja palvelut sekä Tukiprosessit -kokonaisuuksista. Laatukäsikirjan mukaan Tietohallinnon toiminta-ajatus on turvata ICT-toimintavarmuus ja jatkuvuus. Jatkuvuuden ja riskien hallinta on mainittu Laatukäsikirjassa yhtenä tukiprosessina.

2.7.4 Julkisen hallinnon digitaalisen turvallisuuden ohjeet

Valtiovarainministeriön (VM) asettama julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI)[23] toimii julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä.

ICT-toiminnan[24] varautumisesta häiriö- ja erityistilanteisiin koskevassa ohjeessa[25] tavoitteena on parantaa ICT-varautumista erityisesti ministeriöissä ja hallinnonalojen organisaatioissa. Toiminnan ja palvelujen jatkuvuuden takaaminen ja tiedon turvaaminen edellyttävät palveluverkoston varautumista ICT-toiminnan häiriötilanteisiin. Keskeistä on varmistua, että palveluverkosto kykenee normaaliajan vakavissa häiriötilanteissa ja yhteiskunnan turvallisuusstrategian mukaisissa erityistilanteissa jatkamaan toimintaansa asetettujen vaatimusten mukaisesti. Normaaliolojen häiriötilanteita varten toteutetut toimintamallit ja ratkaisut ovat perusta erityistilanteiden hoitamiselle ja toiminnalle poikkeusoloissa.

---

23 VAHTI edistää julkishallinnon toiminnan digitalisaatiota huolehtimalla tarkoitustenmukaisen turvallisuuden vaatimuskehikon laatimisesta ja ylläpitämisestä. Tähän kuuluvat myös turvallisuuteen sekä ICT-toiminnan jatkuvuuteen liittyvät tarkastukset, hyväksynnät ja arvioinnit sekä tieto- ja kyberturvallisuusharjoitustoiminnan edistäminen.

24 ICT = *information and communication technology,* tieto- ja viestintätekniikka

25 VAHTI-ohje 2/2009

Teknisen ympäristön tietoturvataso-ohje[26] on osa valtionhallinnon tietoturvallisuutta koskevan asetuksen[27] täytäntöönpanon ohjausta yhdessä asetuksen täytäntöönpano-ohjeen sekä sisäverkko-ohjeen[28] kanssa. Ohje on suunnattu ICT- ja tietoturvahenkilöstölle tietoturvatasojen teknisen toteuttamisen tueksi. Ohjeeseen sisältyy teknisen tietotekniikkaympäristön vaatimusten kuvauksia sekä esimerkkejä ja kilpailuttamiseen liittyviä tietoturvanäkökohtia koskien ICT-palveluja. Ohjeeseen liittyy myös työvälineitä, joita toimijat voivat hyödyntää tuottaessaan tai hankkiessaan ICT-palveluita.

Toiminnan jatkuvuuden hallinnan ohjeen[29] tarkoituksena on antaa suosituksia organisaation toiminnan turvaamiseksi kehittämällä varautumis-, jatkuvuus-, toipumis- ja valmiussuunnittelua. Suunnitelmien avulla organisaatio voi varautua erilaisiin normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Ohje on kohdennettu valtionhallinnon ja julkishallinnon organisaatioille. Ohje tukee Suomen kyberturvallisuusstrategian täytäntöönpanoa.

VAHTI-vaatimusten mukaan kriittisten palvelujen verkko-, palvelin- ja laiteympäristöt varmennetaan esimerkiksi kahdentamalla. Verkkoinfrastruktuurin hankintaan ja kehittämiseen tulee olla määrämuotoinen prosessi. Muutokset verkkoon testataan, katselmoidaan ja toteutetaan muutoshallintaprosessin mukaisesti. Verkolle tehdään riskianalyysi ja tämän tuloksena keskeiset verkon aktiivilaitteet, kuten runkokytkimet, niiden keskeiset komponentit sekä verkkolaitteiden väliset yhteydet tarvittaessa kahdennetaan vikasietoisuuden kasvattamiseksi.

2.8 Muut tutkimukset

2.8.1 Kysely HUSin henkilöstölle

Onnettomuustutkintakeskus teki HUSin hoitohenkilöstölle kyselyn, jonka tavoitteena oli saada käsitys häiriön vaikutuksista potilaiden hoitoon. Kysely kohdennettiin ensihoitoon ja päivystyspoliklinikoille sekä kirurgisille, teho- ja synnytysosastoille. Kysely toteutettiin noin puoli vuotta tapahtuman jälkeen. Kyselyssä vastaajia pyydettiin kuvailemaan, millaisia ongelmia häiriöt aiheuttivat potilaiden hoidon sujuvuuteen tai turvallisuuteen. Toiseksi vastaajilta pyydettiin tietoa, millaisia ohjeita ja keinoja oli käytettävissä tilanteesta selviytymiseen.

Vastauksia saatiin 119 kaikkiaan 13 sairaalasta. Huolimatta aikaviiveestä vain yksittäisissä vastauksissa koettiin vaikeaksi palauttaa tapahtumia mieleen jälkikäteen. Vastauksissa korostuivat koetut ongelmat. Vastauksissa ei juurikaan kerrottu onnistumisista, mikä saattoi johtua kysymystenasettelusta.

Ensihoidon oma tietojärjestelmä toimi. Kuitenkaan ensihoito ei pystynyt hyödyntämään hoidettavien potilaiden esitietoja sairaalan järjestelmistä ja tämän vuoksi konsultaatiot potilaan taustatietojen saamiseksi eivät toimineet.

Laboratoriokokeet määrättiin paperilähetteellä, jotka oli vietävä laboratorioon. Vastaavasti laboratoriovastaukset oli toimitettava tulosteena pyynnön tehneeseen yksikköön, mistä syntyi viiveitä. Leikkauksien aikana otettujen patologisten tuorenäytteiden lähetteen toimittamiseen ja vastausten saamiseen jouduttiin tekemään erilliset järjestelyt, jotka hidastivat toimintaa. Potilaiden veriryhmätietojen selvittämisessä oli ongelmia.

---

26 VAHTI-ohje 3/2012
27 618/2010
28 VAHTI-ohje 2/2010 ja VAHTI-ohje 3/2010
29 VAHTI-ohje 2/2016

Röntgeniin yhteydenpito oli hankalaa. Lähetteet vietiin paperilla. Lausunnot toimitettiin tulosteina. Leikkauksen aikana kuvien avaaminen ei aina onnistunut, jotta olisi voitu tarkistaa leikkaukseen liittyviä tietoja.

Potilaiden lääkityksestä ei ollut varmaa tietoa. Joillakin osastoilla potilaista oli tulostettuja lääkelistoja, mikä mahdollisti lääkityksen. Muille lääkityksiä jouduttiin selvittämään muun muassa kysymällä asiasta potilaalta itseltään, jos se oli mahdollista. Erityisen hankala tilanne oli verenohennukseen liittyvässä lääkityksessä. Tyypillisesti nämä lääkitykset voivat liittyä leikkauksen jälkeiseen hoitoon ja niiden annostelussa saatetaan tarvita myös laboratoriokokeita. Potilaiden lääkeaineallergioista ei saanut tietoja.

Kirjauksia sähköisiin potilastietojärjestelmiin ei voinut tehdä. Kirjauksia tehtiin käsin paperille sekä yksittäisissä tapauksissa työasemalla toimiviin ohjelmiin. Huolenaiheena oli mahdollisten potilassiirtojen yhteydessä hoitotietojen välittäminen uuteen hoitopaikkaan.

Lääkärin määräykset jouduttiin prosessoimaan paperisina. Tällöin haasteeksi muodostui se, että kyseiset määräykset saattoivat koskea erilaisia hoito- ja tutkimustoimenpiteitä. Samaa määräystä käsitteli useampi henkilö. Määräysten kokonaisuuden toteutumista oli vaikeaa seurata.

Puhelimista osa ei toiminut. Tilannetta hankaloitti kokonaiskuvan puuttuminen siitä, mitkä puhelimet toimivat ja mitkä eivät. Henkilökunta siirtyi käyttämään omia puhelimia ja teki listoja toimivista puhelinnumeroista. Osittain hyödynnettiin hälytyslistoja, mutta niiden numeroissa oli puutteita.

Muissa tietoverkkoon liittyvissä järjestelmissä oli myös häiriöitä, joiden ilmeneminen tuli henkilöstölle yllätyksenä. Ovien sähkölukkojen häiriöt sitoivat hoitohenkilökuntaa. Potilaan hoitohenkilökunnan kutsujärjestelmissä oli toimimattomuutta. Hälytysjärjestelmissä, kuten elvytyshälytysjärjestelmässä, oli myös ongelmia.

Päivystyspoliklinikoilla ensihoidon tuoman potilaan luovutukseen kului normaalia enemmän aikaa, joten ensihoitoyksikkö oli yksittäisen potilaan hoidossa kiinni pitempään. Sisään kirjauksia sähköiseen järjestelmään ei voitu tehdä. Päivystyspoliklinikoilla oli vaikeuksia päästä selville, keitä potilaita oli sisällä päivystyksessä. Potilaiden hoidon kiireellisyysluokitus jäi puutteelliseksi. Tämä johti yksittäisissä tapauksissa tilanteisiin, joissa potilas unohtui ja hoito hidastui merkittävästi. Potilaista ei ollut käytettävissä taustatietoja, mikä vaikeutti tilannetta erityisesti, jos potilas ei itse pystynyt kertomaan tietojaan.

Uloskirjaus ei toiminut ja potilaiden jatkohoito-ohjeiden antaminen oli vaikeaa. Joitakin päivystyspotilaita kotiutettiin ja heidän hoidon uudelleen suunnittelu vei aikaa.

Leikkauksiin jouduttiin lähtemään ilman potilaan normaaleja esitietoja, minkä koettiin haitanneen merkittävästi leikkaustoimintaa. Leikkausten jatkohoidoissa heräämöissä oli epävarmuutta, koska leikkauksen aikana annetuista nesteytyksistä ja lääkityksistä saatettiin saada pelkistetty raportointi. Erityisen häiriöalttiina koettiin tilanne sellaisissa pitkissä leikkauksissa, jotka olivat meneillään häiriön alettua. Tällöin leikkauksen aikana potilaan tiedot menetettiin yhtäkkiä.

Sairaalan kriittisissä erityistoiminnoissa on sellaisia lääkärin tekemiä valvontatehtäviä, joissa hän seuraa yhtäaikaisesti useampaa eri paikassa olevaa potilasta valvontamonitorien kautta. Tietoliikennehäiriö katkaisi valvontamonitorien yhteydet.

Yliopistosairaalassa on joitakin akuuttilääketieteen erityispäivystystoimintoja, joissa toiminnan onnistuminen vaatii normaalia kuvantamistoimintaa ja sekä laboratoriotoimintaa. Tällaisten toimintojen menestyksellisen hoitamisen koettiin olleen uhattuna.

Häiriötilanteesta selviäminen oli kuvattu sairaaloiden jatkuvuussuunnitelmassa. Häiriön ilmettyä otettiin käyttöön jatkuvuussuunnitelman mukaisesti paperiset röntgen- ja laboratoriolähetteet sekä paperiset hoitosuunnitelmat. Kaikissa toimipisteissä ei ollut valmiiksi kopioituja paperiversioita ja kopioimiseen kului aikaa.

Jatkuvuussuunnitelman ongelmaksi koettiin, että se lähtökohtaisesti oli tehty ajatellen lyhyttä tietoliikennekatkoa. Pitempään katkoon ei ollut suunnitelmaa. Päivystävien lääkäreiden ohjekansioita oli liian vähän. Henkilökohtainen kansio olisi olennaisesti helpottanut tilannetta.

Jossakin yksikössä käytettiin ylimääräistä sihteeriä papereiden kuljetukseen. Saneluohjelmiston varajärjestelmänä olleiden irtosanelimien toimintakunnosta ei ollut pidetty huolta ja niiden käyttöönottoon kului aikaa.

Tilannetiedotus koettiin useissa vastauksissa huonoksi. Yksiköiden välillä oli tiedotuksessa suuria eroja. Tietoa tuli muun muassa kuulutuksien avulla, mutta niistä puuttui suunnitelmallisuus ja jatkokuulutukset.

Ennakkosuunnittelussa haluttiin potilasturvallisuusasioiden liittämistä kiinteämmin valmiussuunnitteluun.

Häiriön jälkeen paperille kirjattujen potilastietojen siirtäminen tietojärjestelmään oli työlästä ja siinä vaiheessa tiedoissa ilmeni puutteita.

2.8.2 Tutustuminen esimerkkisairaalan toimintaan

Tutkinnassa tutustuttiin HUS-alueen erään sairaalan työhön ja osastojen johtamiseen tietoliikennehäiriön aikana.

Häiriön vaikutukset alkoivat näkyä heti toiminnan vaikeutumisena, mutta aktiivisia ennalta suunniteltuja muutoksia toimintaan tehtiin vain vähän. Monessa tilanteessa valittiin parhaalta vaikuttava toimintatapa niillä tiedoilla, kokemuksella, laitteilla ja resursseilla, joita oli sillä hetkellä käytössä.

Osa henkilöstöstä totesi, että ryhdytään toimimaan jatkuvuussuunnitelman mukaan. Osa kuultavista ei ollut tietoisia sairaalan tai osaston ohjeiden tarkasta sisällöstä eikä osannut hyödyntää ohjeita häiriön aikana. Ohjeen olemassaolo tiedettiin, mutta sen löydettävyys, sisältö tai konkreettinen hyödynnettävyys häiriötilanteessa ei ollut tarkasti selvillä. Lisäksi oli epätietoisuutta, kuinka kauan tulisi odottaa, ennen kuin aletaan toimia ilman tietojärjestelmiä ja käyttää esimerkiksi paperilähetteitä potilailla. Tämä perustui siihen, että tietojärjestelmien häiriöt ovat usein olleet lyhytkestoisia ja käytännöllisin tapa on ollut odottaa häiriön päättymistä.

Käytännön siirtyminen häiriötilanteessa toimimiseen vaihteli. Esimerkiksi tarvittavat tarvikkeet ja laitteet ilman tietojärjestelmiä toimimiseen oli joissain tapauksissa etsittävä. Pääosin paperisia kaavakkeita oli käytettävissä, mutta esimerkiksi sanelukoneiden saatavuutta ja käyttöönottoa ei ollut mietitty. Toimivia laitteita alettiin etsiä häiriön keston pitkittyessä. Joissakin paikoissa paperilomakkeilla on muutenkin toimittu vielä varsin hiljan, joten paluu ilman tietojärjestelmiä toimimiseen sujui jouhevasti.

Sairaalahenkilöstö joutuu normaalissa arjessa sopeutumaan erilaisiin ruuhka- ja kiiretilanteisiin sekä toimintaan niillä tiedoilla, jotka ovat saatavilla. Tämä toimintamalli näkyi myös tietoliikennehäiriön aikana. Häiriöstä huolimatta toiminta jatkui osaston potilaille tyypillisiä hoitotoimenpiteitä tehden, mutta niiden tekeminen hankaloitui ja hidastui. Toimenpiteitä jouduttiin tekemään vajaiden tietojen varassa. Esimerkiksi potilaista ei ollut käytettävissä riittäviä ennakkotietoja aiemmista sairauksista ja lääkityksestä. Osastoilla ymmärrettiin, että tilanne

saattaa vaarantaa potilasturvallisuutta. Aktiivinen ja järjestelmällinen häiriötilanteen ohjeiden mukainen tilanteen johtaminen ja päätösten teko osastotasolla oli vähäistä. Tilanteen normalisoitumista jäätiin odottamaan ilman toiminnan muutoksia. Esimerkiksi lisätyövoimaa ei pyydetty tai työvuorojärjestelyjä muutettu, vaikka ilman tietojärjestelmiä toimiminen aiheutti lisätyötä ja hidasti toimintaa.

Sisäinen tiedonkulku oli vähäistä. Osastoilla häiriötilanteesta ja sen arvioidusta kestosta ei ollut tietoa. Tämä loi tilanteen, jossa esimerkiksi johtamiseen liittyen päätösten tekeminen hankaloitui. Niin ikään osastojen tilannetietojen kerääminen ja koostaminen esimerkiksi koko sairaalan tilannekuvan saamiseksi oli vähäistä.

Henkilöstä ja paikasta riippuen vaihteli myös se, oliko joitakin tietojärjestelmiä hyödynnettävissä. Internet, intranet ja sähköposti toimivat monilla. Osa henkilökunnasta onnistui käyttämään joitakin potilaiden hoitoon liittyvistä ohjelmista. Esimerkiksi osa tarkasteli onnistuneesti laboratoriotuloksia suoraan laboratoriojärjestelmästä, mutta potilastietojärjestelmän kautta niitä ei tietoliikennekatkoksen takia voinut tarkastella. Eri henkilöillä oli myös erilaiset valmiudet tietoteknisten järjestelmien käyttöön.

Toimintaa sairaalaa koskevassa tietojärjestelmähäiriöissä ei ollut kuultavien mukaan harjoiteltu. Huoltokatkoista oli tiedotettu etukäteen ja silloin oli ennakolta varauduttu niihin. Nyt tositilanteessa jouduttiin hakemaan yhteisiä ja toimivia toimintamalleja. Osastoittain tehdyt ratkaisut ja toimintamallit saattoivat aiheuttaa hämmennystä potilaiden siirtyessä toisille osastoille.

Joissakin paikoissa hyödyllisiksi osoittautuivat käytännön työtä normaalistikin helpottamaan tehdyt paperiset dokumentit, jotka säilyivät käytettävinä tietoliikennekatkon aikana.

Häiriön jälkeen tilanteesta ei kyselty kokemuksia eikä havaintoja tai kerätty hyviä käytäntöjä. Myöskään konkreettisia muutoksia toimintaan tai uusiin häiriöihin valmistautumiseen ei kuultavien mukaan ollut tehty.

2.8.3 Valviralle tehdyt TLT-vaaratilanneilmoitukset

Valviralle oli 1.1.2017–27.4.2018 tehty valtakunnallisesti 215 tietojärjestelmiä koskevaa vaaratilanneilmoitusta. Suurin osa niistä liittyi eri valmistajien potilastietojärjestelmien virheisiin ja ongelmiin, tietojärjestelmien yhteistoimintaan ja tietojärjestelmien käyttökatkoihin. Tapahtumat ovat aiheuttaneet riskejä tai vaikuttaneet potilaan hoidon suunniteltuun toteutukseen. Esimerkkejä ilmoituksissa kuvatuista tilanteista:

- Tehohoidon tietojärjestelmä ei toiminut, jolloin potilaiden tiedot eivät olleet käytettävissä. Katkoja esiintyi ennen virheen korjaamista useita kertoja.
- Palvelinalustan häiriö aiheutti potilastietojärjestelmän epävakautta ja täydellistä toimimattomuutta. Häiriö alkoi kello 11.30 ja kesti yli 24 tuntia. Päivystyspotilaan lääkitystiedot eivät olleet tietojärjestelmän toimimattomuuden vuoksi saatavilla, minkä vuoksi potilas ei saanut yöllä määrättyä antibioottiannosta lainkaan.
- Kuvatietojärjestelmä lakkasi lähettämästä lausuntoja kuvantamisen toiminnanohjausjärjestelmään suunnitellun tietojärjestelmäpäivityksen yhteydessä. Häiriötilanne kesti yli 14 tuntia. Tutkimusten lausunnot eivät olleet lääkäreiden saatavilla ja diagnoosia odottaneiden potilaiden hoitopäätös viivästyi.
- Asiakas- ja potilastietojärjestelmässä oli havaittu uuden version käyttöönoton jälkeen useita ongelmia. Esimerkiksi lääkemääräysten uusinnassa ilmennyt häiriö aiheutti virheellisiä lääkemääräyksiä ja -listoja. Valvira julkaisi asiasta tiedotteen 19.3.2018

- Potilastietojärjestelmä lakkasi toimimasta aamulla kello seitsemän aikaan. Koko erikoissairaanhoito siirtyi varajärjestelmän käyttöön. Kolme ja puoli tuntia kestänyt järjestely hidasti potilashoitoa ja aiheutti merkittävän potilasturvallisuusriskin.
- Potilastietojärjestelmän versiopäivitykseen oli suunniteltu puolesta yöstä aamuseitsemään jatkuva käyttökatko. Katkos pitkittyi ja päättyi vasta kello 15, koska testauksessa havaittiin käyttöönoton estävä virhe. Sairaalassa toimittiin varajärjestelyin ja käyttäjiä informoitiin puolen tunnin välein katkon pitkittymisestä. Potilaan kertomustiedosta oli käytössä katkoa edeltävä tilanne. Esimerkiksi laboratoriotoimintaan, kuvantamiseen ja leikkauksiin liittyvät järjestelmät toimivat normaalisti. Toiminta vaikeutui hoitavissa yksiköissä merkittävästi, koska näin pitkään katkoon ei ollut varauduttu.

Ilmoitusten joukossa oli yksi ulkopuolisen palveluntuottajan konesalipalveluihin liittyvä häiriötilanne sekä muutama tietoturvallisuuteen liittyvä tapahtuma sisältäen haittaohjelmahavainnon ja yhden tietomurron.

Kahdessa ilmoituksessa oli kyse laajasta tietoliikennehäiriöstä, joista toinen oli tutkittavana oleva HUSin häiriö. Toinen oli häiriö Raahen seudun hyvinvointikuntayhtymän tietoverkossa, josta ilmoituksen Valviralle tekivät sekä käyttäjä että valmistaja. Käyttäjät eivät päässeet kirjautumaan potilastietojärjestelmään 30.8.2017 noin kello 16 alkaen. Katko jatkui seuraavaan aamuun. Vika johtui siitä, että osa työasemista reitittyi virheelliseen IP-osoitteeseen. Kun tietoliikenneasiantuntijat saivat päivitettyä IP-osoitteen työasemiin, ongelma korjaantui. Tietoverkon runkoverkon päivitys oli tehty häiriötä edeltävänä päivänä.

2.8.4 Pirkanmaan sairaanhoitopiirin tietoliikennehäiriö 28.–29.5.2018

Pirkanmaan sairaanhoitopiirissä (PSHP) oli maanantain ja tiistain 28.–29.5.2018 välisenä yönä laaja tietoliikennehäiriö. Sairaanhoitopiirin omien raporttien mukaan häiriö vaikutti kaikkiin PSHP:n ja sen yhtiöiden toimipisteisiin keskussairaalan kampuksella, Pirkanmaalla, Keski-Suomessa ja Kanta-Hämeessä. Häiriön aikana kaikkien tietoliikenteen varassa olevien laitteiden ja järjestelmien toiminta estyi. Häiriö alkoi illalla 28.5.2018 noin kello 21 ja täydellinen tietoliikennekatko kesti 3,5 tuntia. Tilanne saatiin palautettua vaiheittain normaaliksi 29.5.2018 kello 3 mennessä.

Tietoliikennekatkosta aiheutui häiriöitä tietojärjestelmien lisäksi muun muassa hoitajakutsujärjestelmään, kulunvalvontaan ja ovien lukituksiin. Myös sähköisten lääkekaappien ovien avaaminen ei häiriön aikana onnistunut. Koska keskeinen potilastietojärjestelmä oli poissa käytöstä, hoitotyössä tarvittavia tietoja ei ollut kaikilta osin käytettävissä. Potilaiden hoito ja lääkitseminen hidastuivat. Häiriön sijoittuminen myöhäisiltaan ja yöhön lievensi vaikutuksia, koska tarve järjestelmien käyttöön on silloin pienintä. Eniten häiriö vaikeutti päivystyksen toimintaa. Siltä varalta, että hoitoon olisi tullut potilas, jonka hoito olisi edellyttänyt toimivia tietoliikenneyhteyksiä, sovittiin siirtojärjestelyistä lähimpään toiseen keskussairaalaan tai HUSiin tai TYKSiin. Esimerkiksi aivoverenkiertohäiriön liuotushoitoa mahdollisesti tarvitsevan laboratoriotutkimusten tekeminen olisi vienyt ilman tietoliikenneyhteyksiä liikaa aikaa. Tämän tyyppisiä potilastilanteita ei tullut häiriön aikana. Jotkin lääkitykset myöhästyivät aikatauluistaan, koska sähköisiä lääkekaappien ovia ei saatu auki häiriön aikana. Monessa hoitotilanteessa aiheutui epätietoisuutta, koska ennen katkoa tehdyt, mutta vielä toteutumattomat, esimerkiksi muutetut lääkemääräykset tai tilatut tutkimukset eivät olleet saatavilla. Näin ollen nämä eivät toteutuneet, ellei uusi työvuoro tehnyt uusia pyyntöjä tai määräyksiä paperisena.

Tapahtumat alkoivat, kun Tekonivelsairaalan kytkimille oltiin tekemässä elinkaarivaihtoa hallittuna muutoksena. Tätä tehdessä verkon havaittiin lakanneen toimimasta. Vian luultiin olevan paikallinen ja mahdollisesti tekeillä olevaan muutokseen liittyvä, kunnes noin 15 minuutin kuluttua ilmeni, että suuri määrä verkkolaitteita hälyttää valvomoon. Tällöin vian laajuus paljastui koskemaan laajasti PSHP:n verkkoa.

Palvelunestohyökkäyksen mahdollisuus saatiin suljettua pois varhaisessa vaiheessa. Häiriöselvityksen alkuvaiheessa havaittiin, että tietoliikenneverkon runkokytkimeen ei saada yhteyttä. Kahdennetun runkokytkimen aktiivinen kytkin (A) käynnistettiin tämän takia uudelleen, jotta liikenne siirtyisi järjestelmän toiselle kytkimelle (B). Liikenteen ohjautumista kahdentavalle kytkimelle B ei kuitenkaan tapahtunut. Yksityiskohtaiset lokitiedot menetettiin uudelleenkäynnistymisen myötä. Uudelleen käynnistetty kytkin A ei käynnistynyt normaalisti, vaan jäi niin sanottuun *recovery*-tilaan. Myöhemmin selvisi, että kytkin B oli myös käynnistämässä itseään uudelleen. Osittaisia yhteyksiä palautui, mutta uusia hälytyksiä sekä vanhoja toimimattomia yhteyksiä ilmeni edelleen. Korjaustoimenpiteiden aikana havaittiin, että sulkemalla toimimattomia yhteyksiä kytkimeltä B, ne palautuivat toimimaan kytkimen A kautta. Lopulta kytkimestä B oli suljettu kaikki muut paitsi kytkinten väliset yhteydet ja verkon liikenne palautui normaalille tasolle. Molemmat kytkimet ja siten kahdennus saatiin palautettua hallitusti 29.5.2018 kello 14.30–19.00.

Runkokytkimet oli uusittu toukokuussa 2017, jolloin myös kahdennusten toiminta oli testattu eri skenaarioilla. Varmaa syytä tapahtumalle ei saatu, koska runkolaitteiden toimintaan liittyneet yksityiskohtaiset lokitiedot menetettiin. Todennäköisin tapahtuman aiheuttanut skenaario muodostui useammasta virheellisesti toimivasta linkistä runkokytkimien ja niihin kytkettyjen keräävien kytkimien välillä. Osassa keräämiä kytkimiä oli ohjelmistoversio, joka toimi virheellisesti tietoliikenneympäristössä käytössä olevassa konfiguraatiossa. Virhetoiminta aiheutti häiriöitä, joissa linkki sammuu loogisella tasolla noin sekunniksi ja palautuu uudelleen toimintaan. Tämä heilunta aiheutti epävakautta verkkoon ja lisäsi runkokytkimen prosessorin kuormitusta. Heilunnan vaikutukset eivät olleet tulleet ilmi aiemmin, koska kahdennus vähensi sen seurauksia eikä ongelma näkynyt verkon valvonnassa.

Toinen runkokytkimelle kuormitusta aiheuttanut seikka oli maanantaina 28.5.2018 aamupäivällä kytketty kahdentava kuitu runkokytkimen ja keräävän kytkimen välille. Kytkentä ja konfiguraatio olivat jääneet ristiriitaan keskenään ja aiheuttivat heilumista, mikä kuormitti runkokytkimiä.

Näiden seikkojen yhteisvaikutuksesta runkokytkinten kuormitus on kumuloitunut ja ylikuormittunut, jolloin ne eivät ole enää pystyneet palvelemaan verkon liikennettä.

Tapahtuman vuoksi pääsy potilaiden hoitoon liittyviin tietoihin estyi 3,5 tunniksi esimerkiksi potilastietojärjestelmä Uranuksen, laboratoriojärjestelmän ja kuvantamisjärjestelmän osalta. Erona tutkittavana olevaan HUSin häiriöön oli se, että tietojen käyttö estyi kokonaan.

2.8.5 Tukholman uudessa Karoliinisessa sairaalassa tapahtunut häiriö 21.11.2017

Ruotsissa uudessa Karoliinisessa yliopistosairaalassa oli 21.11.2017 merkittäviä ongelmia ensin sydänpotilaiden langattomissa valvontalaitteissa. Sen jälkeen koko tietoverkko lakkasi toimimasta. Ongelmat olivat heti esillä useissa tiedotusvälineissä, mutta ilmeisesti ainakaan julkista raporttia aiheesta ei ole saatavissa. Selvityksiä, yksityiskohtia tai johtopäätöksiä ei Ruotsista yrityksistä huolimatta saatu.

Tiedotusvälineiden mukaan yhdelle potilaalle aiheutui vakavia seurauksia sydänpotilaiden valvontalaitteiden vikojen vuoksi. Viat johtivat siihen, että saapuvia potilaita ohjattiin toisiin

sairaaloihin. Valvonnan tarpeessa olleet sydänpotilaat puolestaan joutuivat pysymään sängyissään langallisen valvonnan ulottuvissa ja henkilökunnan määrää piti lisätä.

Vian korjaaminen oli iltapäivän loppupuolella vielä kesken, kun koko tietoverkko kaatui. Käytettävissä olevien tietojen mukaan vika oli kahdennetussa runkokytkimessä, johon oli tekeillä ennakkoon suunniteltu kortin vaihto. Kun kortti vaihdettiin, ilmeni odottamaton vika ja kaikki liikenne tietoverkossa pysähtyi. Tietoliikenne saatiin kulkemaan kolmen tunnin korjaustoimien jälkeen kello 19.30. Kytkimen toiminta oli kuitenkin edelleen epävakaata, joten uusia ongelmia ilmeni kaksi päivää myöhemmin. Sairaala joutui kohottamaan valmiutta uudelleen. Sairaalan tietohallinnon mukaan vian syyt ovat tiedossa, mutta niitä ei ainakaan julkisista lähteistä näyttäisi löytyvän. Tahallisia verkon vahingoittamispyrkimyksiä ei havaittu.

2.8.6 Potilastietojärjestelmähäiriö Keski-Suomessa 22.10.2018

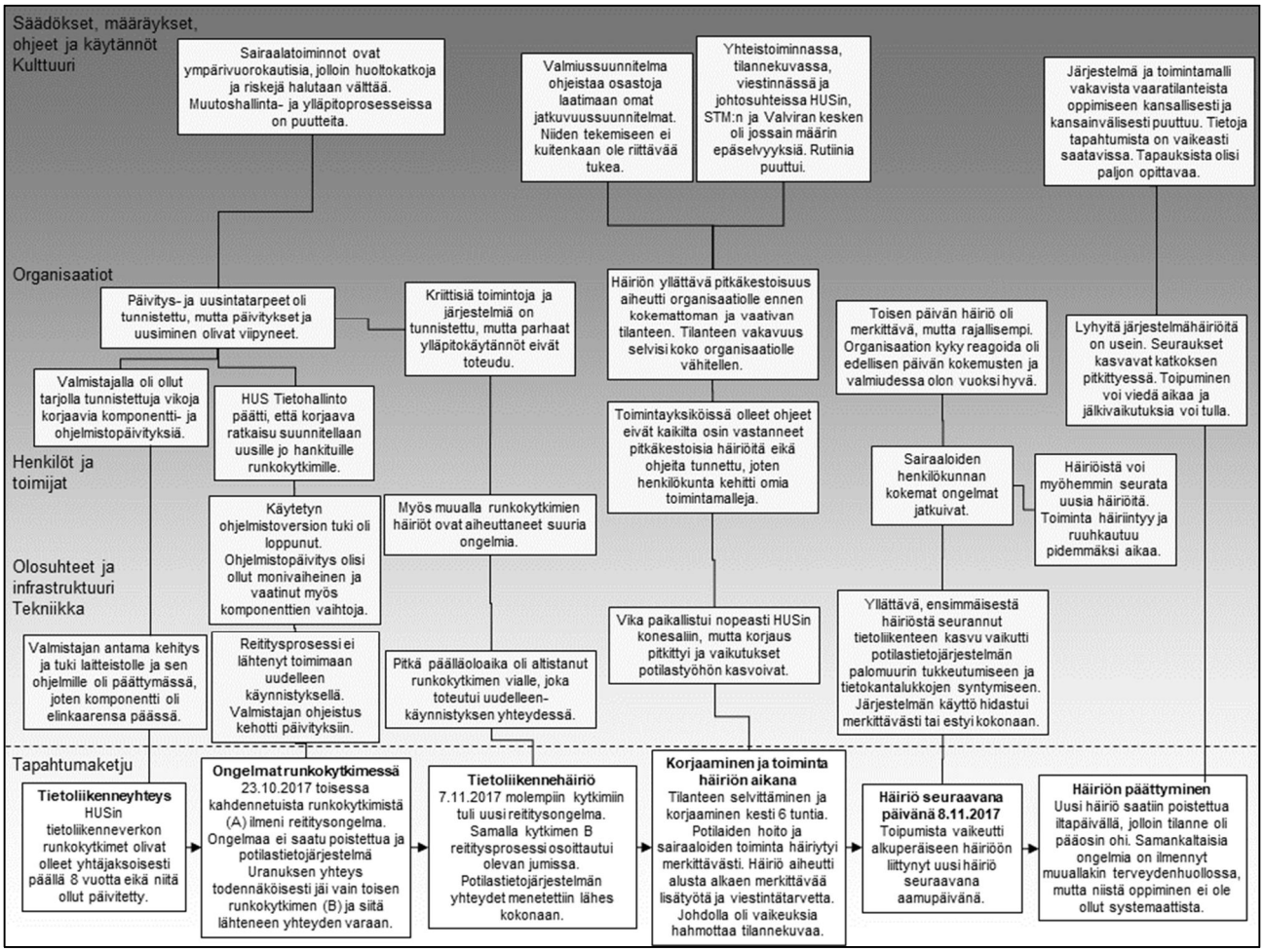
Tutkinnan aikana 22.10.2018 tapahtui myös Keski-Suomessa tietojärjestelmähäiriö, joka haittasi terveydenhuollon toimintaa Jyväskylän lähistöllä usean kunnan alueella sekä Keski-Suomen keskussairaalassa. Tutkintaryhmä sai tietoja tapahtuneesta Jyväskylän kaupungilta ja sairaanhoitopiiriltä. Häiriön syynä oli nimipalveluihin tehty muutostyö. Muutos oli testattu ja suunniteltu etukäteen, mutta tuotantoympäristöön toteutettuna se ei toiminut suunnitelman mukaisesti. Häiriö aiheutti terveydenhuollon Effica-potilastietojärjestelmän toimimattomuutta koko iltapäivän ajan. Vaikutuksia oli palveluiden ruuhkautumiseen myös muina päivinä.

Terveysasemat ja päivystys pystyttiin pitämään auki ja kiireelliset asiat saatiin hoidettua. Vakavia seurauksia ei tullut. Ongelmat olivat monin tavoin samanlaisia kuin HUSin häiriössä. Asiakas- ja potilastietoja ei saatu auki, jolloin ei tiedetty milloin potilaita tulee eikä nähty laboratorio-, kuvantamis- ja lääkitystietoja. Tapahtui ruuhkautumista ja viivästyksiä tietojen kirjaamisessa. Kriittisiä tietoja potilaiden terveydentilan muutoksista ei nähty. Takaisinsoittoja ja reseptejä jäi tekemättä. Potilaiden vastaanotto päivystykseen oli selvästi tavallista hitaampaa, mikä aiheutti ruuhkautumista. Osastoilla olleista potilaista oli tulostettu toimintahäiriöiden varalle tulotekstit, kriittiset tiedot ja lääkelistat. Arviota vian kestosta ei saatu, mikä vaikeutti toimintojen suunnittelua.

Kehitettävää todettiin olevan ainakin varautumisessa, muutosten testauksessa ja ulkoisessa viestinnässä. Ongelmatilanteessa arvioitiin tarvittavan jatkossa monikanavaista viestintää ja myös kykyä vastata puhelintiedusteluihin.

3 ANALYYSI

3.1 Tapahtuman analysointi



Kuva 6. Tutkinnassa laadittu Accimap-analyysikaavio.

3.1.1 Tietoliikenneyhteys

Potilastietojärjestelmän yhteyksistä huolehtivat runkokytkimet olivat olleet yhtäjaksoisesti päällä kahdeksan vuotta. Ohjelmistoja ja komponentteja ei ollut päivitetty vuosien saatossa valmistajan antamien suositusten mukaisesti, vaikka valmistajalla olisi ollut tunnistettuja vikoja korjaavia päivityksiä. Valmistajan antama tuki runkokytkimen komponenteille oli päättymässä ja ohjelmistoille tuki oli jo päättynyt. Kokonaisuus oli elinkaarensa päässä. Runkokytkimiä ja tietoliikenneyhteyksiä oli kahdennustarkoituksessa kaksi, mutta reititysprosessi oli yhteinen molemmille runkokytkimille.

3.1.2 Ongelmat runkokytkimessä

Potilastietojärjestelmän yhteyksistä huolehtivassa runkokytkimessä oli reititysongelmia noin kaksi viikkoa ennen tutkittavana olevia häiriöitä. Ongelmaa tuolloin selvitettäessä todettiin, että niiden kunnollinen korjaaminen vaatisi sekä ohjelmisto- että komponenttipäivityksiä.

Koska runkokytkin ja siihen liittyvä tietoliikenneyhteys oli kahdennettu, potilastietojärjestelmä toimi jäljellä olleen toisen runkokytkimen ja yhteyden varassa. Yhteys jäi todennäköisesti siihen tilaan, jossa kahdennusta ei enää ollut uuden mahdollisen häiriön varalle. Ylläpitopalveluntuottaja tunnisti yhden yhteyden varaan jäämisen, mutta tieto ei kunnolla siirtynyt

HUS Tietohallintoon. Ylläpitopalveluntuottaja esitti ratkaisuksi yhteyden siirtämistä uusille reitittimille, koska uudet laitteet olivat olemassa ja niihin siirtyminen oli muutenkin tapahtumassa lähiaikoina. Tiedossa oli, että vanhat laitteet olivat elinkaarensa lopussa ja hankalasti ylläpidettävät eivätkä ohjelmistot ja komponentit olleet ajan tasalla. Kommunikaatio ei ylläpitopalveluntuottajan ja HUS Tietohallinnon välillä kunnolla onnistunut, joten siirtoon ei välittömästi ryhdytty.

Runkokytkimen ja sen ohjelmiston kriittisyys sairaalan toiminnalle oli ollut toimijoiden tiedossa. Uuden laitteiston asennus oli käynnissä, mutta sen käyttöönotto ei ollut edennyt suunnitelman mukaan. Uusiminen oli suunniteltu vasta vuodelle 2017, jolloin tuki oli jo päättymässä. Siitäkin aikataulusta oltiin myöhässä lähes vuosi. Laitteita oli käytetty pitkään.

Sairaalatoiminnot ovat ympärivuorokautisia, jolloin tietoliikenneverkon tarve on jatkuvaa. Tietoliikenteen katkoja pyritään välttämään. Muutoksen tekeminen tietoverkossa sisältää aina riskin jostain ennakoimattomasta häiriöstä. Näitä riskejä halutaan välttää, mikä johti siihen, että toimintaa vanhoilla vielä toimivilla komponenteilla ja ohjelmistoilla jatkettiin. Päivitystarpeita kertyi useita, mikä tarkoitti ajan tasalle saattamisen muuttumista työläämmäksi ja riskialttiimmaksi. Päivitystarpeiden kumuloiduttua voidaan todeta, että muutoshallinta- ja ylläpitoprosesseissa oli puutteita.

3.1.3 Tietoliikennehäiriö

Tiistaina 7.11.2017 runkokytkimessä ilmeni jälleen vikaa. Sen vaikutus ulottui tällä kertaa molempiin reitittimiin, joten ilman mahdollista kahdennuksen puuttumistakin se olisi häirinnyt Uranus-yhteyttä pahoin.

Prosessien ja laitteen uudelleenkäynnistys ei korjannut häiriötä. Sen sijaan kävi niin, että toisesta runkokytkimestä rikkoutui yksi linjakorteista. Ongelmat uudelleenkäynnistymisessä ovat vaarana erityisesti silloin, kun sitä ei ole tehty pitkään aikaan. Tässä tilanteessa ongelmia oli mahdollisesti odotettavissa, sillä laitevalmistajalla oli julkaistu tieto vikaantumismahdollisuudesta.

HUSissa on pyritty tunnistamaan kriittisiä toimintoja ja järjestelmiä, mutta siitä huolimatta parhaat ylläpitokäytännöt eivät toteutuneet. Runkokytkimien ja niihin liittyneen potilastietojärjestelmän kriittisyys on ilmeinen. Potilastietojärjestelmä on keskeisin potilaiden hoitoon liittyvä järjestelmä. Se ei voi toimia, jos tietoliikenne estyy runkokytkimien kohdalla. Vakavia runkokytkinhäiriöitä on ollut muuallakin terveydenhuoltoalalla.

3.1.4 Korjaaminen ja toiminta häiriön aikana 7.11.2017

Tietoliikennehäiriön alettua hoitohenkilökunta jäi aluksi odottamaan yhteyksien palautumista. Häiriöitä eri tietojärjestelmissä on melko usein, ja useimmiten ne poistuvat pienellä odottelulla. Johto sai tiedon häiriöstä tekstiviestillä, jossa ei ollut tietoa tilanteen vakavuudesta tai kestosta.

Yhteyden katkeaminen aiheutti merkittävää häiriötä potilaiden hoitoon ja sairaalan toimintaan. Osastoilla oli pakko ottaa käyttöön erilaisia jatkuvuuden hallintaan liittyviä toimia, joista merkittävä osa oli ennakkoon suunnittelemattomia.

Osastoilla kaivattiin tietoa häiriön odotetusta kestosta, jotta jatkuvuuden hallintaan liittyvät toimet olisi voitu mitoittaa oikein. Tätä tietoa ei tullut. Osastoilla olleet ohjeet eivät vastanneet pitkäkestoista häiriötä. Henkilökunnan toimintakyky osastoilla vaihteli häiriön aikana, eikä kaikkia keinoja osattu käyttää.

Vika paikallistettiin melko pian HUSin konesaliin, mutta korjaus pitkittyi. Yhteydet saatiin kuntoon noin kuuden tunnin kuluttua häiriön alkamisesta.

Häiriön pitkittyminen aiheutti organisaatiolle ennen kokemattoman ja vaativan tilanteen. Ymmärrys tilanteen vaativuudesta kasvoi pikkuhiljaa, mikä johti siihen, että organisaation toimenpiteet käynnistettiin viiveellä. Kun organisaatiotasolla alettiin puhumaan jatkuvuussuunnitelmaan siirtymisestä, olivat osastot käytännössä toteuttaneet vastaavanlaisia toimia vaihtelevin tavoin jo yli kahden tunnin ajan.

Valmiussuunnitelmaan kirjatun periaatteen mukaan osastojen tulee itse laatia jatkuvuussuunnitelmansa pitkäkestoista tietoliikennehäiriötä varten. Niiden tekemiseen ei kuitenkaan ole ollut riittävää tukea, joten suunnittelu on ainakin joissain paikoissa jäänyt vaillinaiseksi. Tietojärjestelmähäiriöstä selviytymistä on mahdollista olennaisesti helpottaa suunnittelemalla vaihtoehtoisia paikallisia toimintamalleja.

Tilanne tuli julkisuuteen noin kolme tuntia häiriön alkamisesta, jonka jälkeen HUSin ulkopuoliset toimijat aktivoituivat. STM aloitti tilannehuonetoiminnan. Valviran ylin johto seurasi tilannetta. Tiedonvaihtoa oli, mutta yhteistoiminnassa, tilannekuvassa, viestinnässä ja johtosuhteissa HUSin, STM:n ja Valviran välillä oli jossain määrin epäselvyyksiä. Rutiini tällaisen tilanteen hoitamisesta puuttui.

Saatuaan tiedon tapahtuneesta Kyberturvallisuuskeskus pystyi seuraamaan tilannetta reaaliaikaisesti Havaro-järjestelmän avulla ja muilla tavoin. Merkkejä ulkoisesta vaikuttamisesta ei ollut.

3.1.5 Häiriö seuraavana päivänä 8.11.2017

Häiriötä seuraavan päivän aamuna potilastietojärjestelmän käytössä havaittiin uudelleen merkittävää hitautta, mikä häiritsi edellisen päivän häiriöstä toipumista. Häiriö sattui edellistä päivää hankalampaan ajankohtaan, koska häiriön alkaessa useat sairaalan toiminnot, kuten leikkaukset, olivat käynnissä.

Häiriö oli seurausta edellisen päivän häiriöstä. Laboratoriojärjestelmä oli lähettänyt poikkeuksellisen paljon vastauksia potilastietojärjestelmään, koska niitä oli kertynyt edellisen häiriön johdosta. Palomuuri tulkitsi tilanteen epänormaaliksi ja alkoi tutkia liikennettä. Poikkeavan liikenteen tutkintaan tarkoitettu muistialue täyttyi aiheuttaen palomuurille poikkeavan tilan. Samalla potilastietojärjestelmäsovellukseen syntyi tietokantalukkoja tietoliikenneyhteyksien kadotessa. Potilastietojärjestelmä ei ollut taaskaan käytettävissä.

Uranus-palveluntuottaja teki erilaisia toimenpiteitä ongelman ratkaisemiseksi. Lopulta palomuuri poistettiin käytöstä potilastietojärjestelmän osalta, jolloin potilastietojärjestelmän yhteys alkoi toimia.

Edellisen häiriön ollessa tuoreessa muistissa organisaatio pystyi reagoimaan edellistä päivää paremmin, vaikkakaan organisaatio ei erityisesti ollut korotetussa valmiudessa. Uusi häiriö koski vain potilastietojärjestelmää, joten esimerkiksi intranet, internet ja puhelimet toimivat kaikkialla. Muun muassa sisäinen tiedottaminen oli edellistä päivää helpompaa. Myös ulkoinen tiedottaminen oli aktiivista ja tilannetta ennakoivaa.

Laajan häiriön vaikutukset jatkuvat tilanteen korjaamisen jälkeen. Käsin tehtyjä kirjaamisia joudutaan viemään järjestelmiin ja katkoksen aikana kertyy tekemättömiä töitä. Lisäksi häiriöllä voi olla teknisiä odottamattomia jatkoseurauksia, kuten tässä tapauksessa uusi vastaavanlainen häiriö. Siihen pitää varautua.

3.1.6 Häiriön päättyminen

Uusi häiriö saatiin poistettua iltapäivän lopuksi, jonka jälkeen toiminta alkoi palata normaaliksi. Häiriön korjaamisen yhteydessä tehdyt muutokset aiheuttivat pienellä viiveellä vielä kaksi vähäisempää ongelmaa, joita ei osattu ennakoida.

Terveydenhuollossa on ollut muitakin muun muassa runkokytkimiin liittyviä vakavia tietoliikennehäiriöitä. Tapauksista olisi paljon opittavaa, mutta terveydenhuollosta puuttuu vakavista vaaratilanteista oppimisen systemaattinen toimintamalli sekä kotimaassa että kansainvälisesti. Kunnollisia kaikkien toimijoiden saatavilla olevia yhteenvetoja ei tehdä. Osaltaan tietojen saantia hankaloittaa tietoteknisten järjestelyjen ja varautumisen salassa pidettävät näkökohdat, mutta julkisen tason raportointi olisi silti mahdollista.

3.2 Viranomaisten toiminnan analysointi

Aluehallintoviraston tehtävänä on yhteensovittaa alueellisten toimijoiden valmiussuunnittelua. Säännöllisiin valmiusharjoituksiin liittyen aluehallintovirasto valvoo, että toimijat ovat päivittäneet valmiussuunnitelmansa. Valvonta ei kohdistu suunnitelmien yksityiskohtiin tai toimintamalleihin yksittäisissä sairaaloissa tai osastoilla.

Valviran valvontasuunnitelman mukainen etukäteinen valvonta on tällä hetkellä terveydenhuollon omavalvonnan tukemista. Valviran ennen häiriöitä toteuttama valvonta ei ulottunut tutkinnan kohteina olleisiin keskeisimpiin asioihin, kuten tietojärjestelmien luotettavuuteen ja häiriöihin varautumiseen. Häiriöiden jälkeen Valvira pyysi asiasta selvityksen, teki valvontapäätöksen ja on pitänyt asioita ilmoituksensa mukaan esillä viranomais- ja verkostoyhteistyössään.

4 JOHTOPÄÄTÖKSET

Johtopäätökset sisältävät onnettomuuden tai vaaratilanteen syyt. Syyllä tarkoitetaan erilaisia tapahtuman taustalla olevia tekijöitä ja siihen vaikuttavia välittömiä ja välillisiä seikkoja.

1. Tietoliikennehäiriöt liittyivät potilastietojärjestelmän kannalta tärkeään runkokytkimeen. Runkokytkimen käyttöikä oli päättymässä ja sitä oli käytetty yhtäjaksoisesti pitkään. Ohjelmistopäivityksiä ja niiden vaatimia laitteistopäivityksiä oli tekemättä. Laitteiston uusiminen oli vireillä, mutta se oli viipynyt.

   Johtopäätös: Terveydenhuollon tärkeimpienkään järjestelmien osia ei aina ylläpidetä niiden kriittisyyden vaatimalla tavalla.

2. Tutkitun häiriön ensimerkit olivat 23.10.2017 ilmenneessä reititysongelmassa, jonka jäljiltä tietoliikenneyhteyden kahdennus todennäköisesti jäi puuttumaan. Uudet ongelmat aiheuttivat kaksi laajaa häiriötä potilastietojärjestelmän käyttöön 7.–8.11.2017. Vaikutuksia oli myös seuraavina päivinä. Häiriöt liittyivät toisiinsa.

   Johtopäätös: Tietoteknisen häiriön korjaustoimet tai yhteyskatkokset saattavat aiheuttaa uusia häiriötilanteita esimerkiksi seuraavassa kuormitustilanteessa. Häiriön jälkeen tarvitaan korotettua valmiutta tietohallinnossa, käyttäjäorganisaatioissa ja valmiusorganisaatioissa.

3. Terveydenhuollossa tapahtuu tietojärjestelmähäiriöitä aika ajoin. Isoja ongelmia toiminnalle ei yleensä aiheudu, koska häiriö usein saadaan korjattua nopeasti. Tässä tapauksessa häiriö pitkittyi ja ongelmat potilastyössä alkoivat kasvaa. Pikkuhiljaa oli pakko kehittää tapoja selviytyä, mutta se ei ollut kaikkialla suunnitelmallista. Kaikkia keinoja tilanteen helpottamiseksi ei osattu käyttää.

   Johtopäätös: Pitkään tietojärjestelmähäiriöön ei ole kunnolla varauduttu kaikissa sairaaloissa ja osastoilla. Toisin sanoen jatkuvuussuunnittelussa ja suunnitelman käyttöön siirtymisessä on puutteita. Suunnitteluun ja harjoitteluun ei ole riittävää ohjausta ja tukea.

4. Ylätason johtamistoimet HUSissa ja viranomaisilla käynnistyivät kohtuullisen hyvin, mutta yhteistoiminnassa, tilannekuvassa, viestinnässä, johtosuhteissa ja johtamistavoissa oli haparointia. Häiriötilanne oli HUSille ja viranomaisille laajuudessaan ennen kokematon. Toisena päivänä tilanne oli koetun vuoksi jo hieman helpompi.

   Johtopäätös: Riippuvuus tietojärjestelmistä kasvaa, mutta toisaalta kyky selviytyä ongelmatilanteista paranee kokemusten myötä. Toimintamalleja pitää kehittää myös muiden organisaatioiden kokemusten avulla. Tiedonvaihtoa ja oppimista ei kuitenkaan kunnolla tapahdu, mikä pätee kaikkiin terveydenhuollon vakaviin tapahtumiin.

5 TURVALLISUUSSUOSITUKSET

5.1 Kriittisten tietojärjestelmäkomponenttien tunnistaminen

Tietojärjestelmähäiriöt liittyivät vaurioituneeseen runkokytkimeen ja laajemmin katsottuna tietoliikenneyhteyteen, jonka kautta koko sairaanhoitopiirissä käytetään Uranus-potilastietojärjestelmää. Kuten häiriön vaikutukset osoittavat, yhteyden ja runkokytkimen toimivuus oli potilaiden hoidon kannalta erittäin tärkeä.

Onnettomuustutkintakeskus suosittaa, että

Sosiaali- ja terveysministeriö ohjaa sairaanhoitopiirejä määrittelemään tärkeimpien tietojärjestelmien ja niiden komponenttien kriittisyyden potilasturvallisuuden näkökulmasta. Kriittisimmiksi luokiteltujen järjestelmien luotettavuudesta tulee huolehtia esimerkiksi toimivien kahdennusten, suunniteltujen tilapäisratkaisujen, varaosien, erityiskomponenttien ja aktiivisten valvonta- ja huoltotoimien avulla. Asia on otettava huomioon myös tulevissa terveydenhuoltouudistuksissa. [2019-S8]

5.2 Järjestelmien ylläpito

Runkokytkimen käyttöikä oli päättymässä. Laite oli myös ollut yhtäjaksoisesti päällä kahdeksan vuoden ajan. Toteutunut vikamahdollisuus oli ollut valmistajan tiedossa, joten kytkimeen oli ollut tarjolla sekä ohjelmisto- ja laitteistopäivityksiä. Päivityksiä ei ollut tehty ja uusiminen oli viipynyt.

Laitteen ikä ja pitkä yhtäjaksoinen päälläolo lisäsi kytkimelle tehtävien toimenpiteiden riskiä, joten kynnys päivityksille oli kasvanut. Laite oli tärkeä sairaanhoitopiirin toiminnan kannalta, joten katkoksia ei yleisesti haluta. Päivityksiä on mahdollista tehdä suunnitellusti ilman katkoksia, mutta ne saattavat kuitenkin johtaa erilaisiin odottamattomiin ongelmiin. Mitä pidempään huoltotoimet viipyvät, sitä hankalammaksi tilanne menee.

Onnettomuustutkintakeskus suosittaa, että

Sosiaali- ja terveysministeriö varmistaa, että terveydenhuollon toimijoilla on tietojärjestelmien ja niiden komponenttien huolto-, päivitys- ja uusimisohjelma, jota noudatetaan ja seurataan. Päivitystarpeiden seuranta pitää olla huolehdittu. Päätöksenteko huoltotoimista pitää olla selkeä, jotta toimenpiteet eivät jää viipymään. [2019-S9]

5.3 Jatkuvuussuunnittelu ja harjoittelu sairaaloiden osastoilla

Sairaaloissa ja osastoilla pitää pystyä toimimaan poikkeustilanteessa ilman tietojärjestelmiä. Toimintakyky toteutuneissa katkoksissa vaihteli, eikä kaikkia keinoja osattu käyttää. Riippuvuus tietojärjestelmistä kasvaa koko ajan.

Onnettomuustutkintakeskus suosittaa, että

Sosiaali- ja terveysministeriö huolehtii, että potilasturvallisuuden kannalta riskialttiilla osastoilla on tietojärjestelmähäiriöt huomioon ottava jatkuvuussuunnitelma, sen edellyttämät toimenpiteet, ohjeet ja hankinnat tehtynä sekä säännöllistä harjoittelua. Terveydenhuollon tulevissa uudistuksissa on varmistettava, että varautumisen valvonta on jatkossa riittävää. [2019-S10]

Ilmeisiä keinoja, joita katkoksista selviämiseksi tulisi suunnitella, ovat esimerkiksi henkilöresurssien käyttö tietojen kuljettamiseen, valmiudet työvuoromuutoksiin, toimintojen priorisoinnit, tietojärjestelmiä korvaavien laitteiden ja papereiden olemassaolo sekä mahdollisuudet käyttää järjestelmiä jotain toista kautta.

5.4 Terveydenhuoltoalan vaaratilanteista oppiminen

Vakavia tietojärjestelmähäiriöitä on tapahtunut useita. Erityisesti vakavista häiriöistä voidaan oppia ja kehittää niiden perusteella toimintatapoja. Käytössä on vaaratapahtumien raportointijärjestelmät, mutta silti tietoa tapahtumista ei kattavasti saada, se ei leviä kaikille tarvitseville eivätkä laajavaikutteiset kehittämistoimet lähde käyntiin. Erityisesti tiedon välittymistä sairaanhoitopiirien välillä on syytä kehittää. Myös ulkomaisista tapahtumista voidaan oppia. Tarve ei rajoitu pelkästään tietojärjestelmäongelmiin, vaan yleisemmin potilasturvallisuutta tavalla tai toisella merkittävästi vaarantaneisiin tapahtumiin.

Onnettomuustutkintakeskus suosittaa, että

Sosiaali- ja terveysministeriö huolehtii, että terveydenhuollon alalle kehitetään tietojenkeruu ja tiedonjakojärjestelmä, jonka avulla kaikista vakavasti potilasturvallisuutta uhanneista tapahtumista kerätään oleelliset tiedot ja muodostetaan ja julkaistaan turvallisuuden parantamisen kannalta olennaiset johtopäätökset koko toimialan hyödyksi. [2019-S11]

Tietoja on myös ulkomaisilla tutkintaviranomaisilla ja muilla toimijoilla.

5.5 Toteutetut toimenpiteet

Helsingin ja Uudenmaan sairaanhoitopiirin mukaan tilannetta ja siitä saatuja oppeja on käyty läpi usealla foorumilla niin sisäisesti kuin ulkopuolellakin. Osastoilla on käyty läpi jatkuvuussuunnitelmia. Jatkuvuuden hallinta on noussut esiin sekä tietojärjestelmähäiriöiden että tapahtuneiden sähkökatkosten yhteydessä. Uuden sote-tietojärjestelmä Apotin suunnittelussa ja toiminnallisen ohjeistuksen laadinnassa on korostettu tapahtumasta saatuja oppeja. Uusi potilastietojärjestelmä kykenee tukemaan häiriötilannetoimintoja aikaisempaa paremmin, vaikka verkkoyhteydet väliaikaisesti menetetään.

HUS Tietohallinnossa on uusittu toimintaprosesseja, ohjeistusta ja tekniikkaa. Uranus-yhteyttä valvotaan jatkossa niin, että valvontajärjestelmä hälyttää tietoliikenteen tason laskiessa 20 % normaalista. Tietoliikennepalveluille on sovittu huoltoikkuna, mikä helpottaa muutoshallintaa, päivitystoimenpiteitä ja säännöllisiä kahdennustestauksia.

Uudet runkokytkimet on otettu käyttöön. Reitit ykset on jaettu useammalle fyysiselle laitteelle, mikä auttaa häiriötilanteiden ja muutosten aiheuttaminen riskien hallinnassa. Uranus-yhteyteen liittyvä jaettu palomuuriympäristö on korvattu yksinomaan HUSin käyttöön varatulla kahdennetulla palomuurilla.

Valviran HUSin selvityksestä 14.2.2018 antaman päätöksen mukaan asia ei anna Valviran osalta aihetta enempiin toimenpiteisiin. Valvira on päätöksensä jälkeen tuonut kertomansa mukaan toistuvasti ja voimakkaasti esiin viranomais- ja verkostoyhteistyössään sitä, että HUS:ssä saadut kokemukset häiriötilanteiden hallitsemisessa ja korjaamisessa otettaisiin huomioon myös laajemmin muissa maamme terveydenhuollon toimintayksiköissä.

Helsingissä 11.1.2019

Kai Valonen	Timo Naskali	Simo Piitulainen
Petri Pommelin	Alpo Vuorio	Kari Ylönen

LÄHDELUETTELO

Tutkinta-aineisto

1) STM:n kirje Helsingin ja Uudenmaan sairaanhoitopiirin 7.–8.11.2017 tapahtuneiden tietojärjestelmähäiriöiden tutkimiseksi, 21.3.2018
2) Valviran selvityspyyntö koskien HUS:ssä esiintyneitä tietoliikennehäiriöitä, 17.11.2017
3) HUSin selvitys Valviralle 4.1.2018
4) Valviran valvontapäätös koskien häiriön selvitystä, 14.2.2018
5) Hewlett-Packard Enterprisen selvitysraportteja ja aineistoa häiriöihin ja runkokytkimen ylläpitoon liittyen
6) CGI:n selvitykset 7. ja 8.11.2017 häiriötilanteesta Uranus-palvelussa
7) Cisco Field Notice FN-63751
8) HUSin 7.–9.11.2017 julkaisemat häiriöön liittyvät tiedotteet
9) 7.–8.11.2017 ajanjaksolle kohdistuneet HUS HaiPro ilmoitukset
10) 7.–8.11.2017 ajanjaksolle kohdistuneet HUS-Riskit ilmoitukset
11) HUS:n tuottamaa häiriöön liittyvää aineistoa, esityksiä, organisaatiokaavioita ym.
12) HUS valmiusohje, 13.3.2017
13) HUS Lääkinnän valmiussuunnitelma, 30.3.2017
14) HUS potilasturvallisuussuunnitelma 2017–2018
15) HUS kriisiviestintäohje, 13.5.2016
16) HUS Tietohallinnon aineistoa verkoista, laitteista, ohjelmistoista, ylläpidosta ja sopimuksista
17) HUS Tietohallinnon laatukäsikirjan pääluvut
18) HUS Tietohallinnon tietoliikenne- ja viestintätekniikkapalveluiden jatkuvuussuunnitelma
19) Uranus-potilastietojärjestelmän jatkuvuussuunnitelma
20) HUS potilasturvallisuusraportit 2016 ja 2017
21) HUSin selvitys sen häiriön jälkeen toteuttamista toimenpiteistä
22) Tietoja häiriön vaikutuksista muihin sairaanhoitopiireihin sekä niiden ohjeita tietojärjestelmähäiriöiden aikana toimimiseen
23) Pirkanmaan sairaanhoitopiirin raportti ja aineistoa 28.–29.5.2018 tapahtuneesta tietoliikennehäiriöstä, 1.6.2018
24) Keski-Suomen sairaanhoitopiirin selvityksiä 22.10.2018 olleesta Effica-potilastietojärjestelmän häiriöstä
25) Sairaaloiden eri tietoliikennehäiriöihin liittyviä uutisia ja muuta media-aineistoa.
26) Valtioneuvoston tilannekeskuksen tapauksesta keräämää, kokoamaa ja tuottamaa aineistoa
27) Valtioneuvoston tilannekeskuksen Turvallisuusasioiden teemakatsaukset 12/2017 ja 6/2018
28) STM:lle häiriötilanteesta kertynyttä aineistoa, yhteenvetoja, tilannekatsauksia ja -seurantaa
29) Kyberturvallisuuskeskuksen tapauksesta keräämää ja tuottamaa aineistoa
30) AVIn, Valviran ja Potilasvahinkokeskuksen tiedot häiriön vaikutuksista potilaille
31) OTKESin tekemän HUS:n sairaaloiden potilasturvallisuuden kannalta kriittisissä yksiköissä tapahtuman aikana työvuorossa olleille suunnatun kyselyn tulokset.
32) Valviran valmiussuunnitelma, 1.9.2017
33) Valviran toimintakertomus 2017
34) Valviralle tulleet tietojärjestelmiin liittyneet vaaratilanneilmoitukset ajanjaksolta 1.1.2017-30.4.2018
35) Valmius- ja jatkuvuudenhallinta soterakenteissa -hankkeen aineistoa, Kuntaliitto
36) VAHTI-ohjeita, www.vahtiohje.fi
37) Kuulemiset

YHTEENVETO TUTKINTASELOSTUSLUONNOKSESTA SAADUISTA LAUSUNNOISTA

Tutkintaselostusluonnos on ollut lausunnolla sosiaali- ja terveysministeriössä, Sosiaali- ja terveysalan lupa- ja valvontavirastossa, Etelä-Suomen aluehallintovirastossa, Helsingin ja Uudenmaan sairaanhoitopiirissä, Hewlett Packard Enterprisessa, CGI Suomi Oy:ssä ja Cisco Systems Inc:llä.

Sosiaali- ja terveysministeriö toteaa lausunnossaan, että digitaalisen toimintaympäristön toimintavarmuus ja häiriöiden estäminen, sietäminen ja niistä nopea toipuminen ovat toimialalle ja yhteiskunnalle erittäin keskeisiä jatkuvuuden hallinnan osioita. Potilastietojärjestelmän toimivuus on potilasturvallisuudelle erittäin tärkeää. Tapahtuneesta on tärkeää saada oppia koko kansallisen kokonaisuuden näkökulmasta, ei pelkästään terveydenhuollon osalta.

STM:n mukaan se saa tutkintaselostuksen avulla tärkeää palautetta STM:n ja sen hallinnonalan ja toimialan toimijoiden keskinäisen yhteistyön parantamiseksi erilaisissa yhteiskunnan häiriötilanteissa. Saatuja oppeja pyritään huomioimaan päivitettävänä olevassa sosiaali- ja terveydenhuollon valmiussuunnitteluohjeistuksessa. Nämä asiat tulevat hyvin esille tutkintaselostuksen luonnoksen johtopäätöksissä.

Lisäksi STM esitti lausunnossaan täsmennyksiä kahteen STM:n toimia koskevaan kohtaan sekä suositusten sanamuotoihin.

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) pitää hyvänä, että Onnettomuustutkintakeskus on laajentanut tutkintatoimintaansa terveydenhuollon alueelle. Siten voidaan vaikuttaa potilasturvallisuuden parantumiseen.

Valvira esittää, että tutkintaselostuksen alkusanoissa määriteltäisiin tutkinnan tavoite konkreettisemmin kohdistuen tarkasteltavaan häiriöön. Lisäksi Valvira esittää lausunnossaan täsmennyksiä sen tehtäviä ja toimintaa kuvaaviin kohtiin sekä korostaa ottaneensa häiriöiden oppeja ponnekkaasti esille eri yhteyksissä. Valvira olisi myös kaivannut enemmän tutkintaa siitä, miten teknisten järjestelmien päivityksiin ja uusimisiin liittyvät tärkeät päätökset tehtiin ja miten niitä käsiteltiin HUSin organisaatiossa. HUS-konsernin sisäistä ja eri viranomaisten välistä yhteistoimintaa, tilannekuvan luomista, viestintää ja johtamista analysoidaan tutkintaselostuksessa melko lyhyesti. Kantaa ei myöskään oteta sairaanhoitopiirin Valviralle kuvaamiin kehittämistoimiin.

Lausunnoissa todetaan moniin ilmenneisiin häiriöihin viitaten, että sairaaloilla ja terveysasemilla on oltava suunnitellut ja vaihtoehtoiset toimintatavat sekä varajärjestelmät. Lääketieteellisten laitteiden tulisi myös olla mahdollisuuksien mukaan eriytettynä hallinnollisista verkoista ja työasemista.

Valvira pitää tutkintaselostusluonnoksessa esitettyjä turvallisuussuosituksia hyvinä ja toteuttamiskelpoisina. Turvallisuustutkinnalla on jo itsessään vaikutusta turvallisuuteen. Turvallisuuden parantaminen ja onnettomuuksista oppiminen edellyttävät, että toimija käsittelee onnettomuustutkinnan tulokset ja ryhtyy asianmukaisiin korjaaviin toimenpiteisiin. Ohjaavilla ja valvovilla viranomaisilla on toteutusten seurannassa tärkeä rooli.

Helsingin ja Uudenmaan sairaanhoitopiiri (HUS) pitää lausunnossaan hyvänä sitä, että onnettomuustutkintaa laajennetaan myös tietojärjestelmien virheellisistä tai puutteellisesta toiminnasta aiheutuviin ongelmiin. Kyseistä tutkintaa HUS pitää uraauurtavana ja menetelmällisesti vaativana, koska tutkintamenettelyt ovat olemassa fyysisiä onnettomuuksia varten.

HUS korostaa hiipivästi edenneen kriisin haasteita johtamiselle ja esittää asiaan liittyen täsmennyksiä. Lisäksi lausunnon mukaan selostuksessa jää liian vähälle huomiolle se, että henkilökunta toimi erittäin haastavassa tilanteessa rauhallisesti, ammattimaisesti ja määrätietoisesti siten, ettei potilasturvallisuus vakavasti vaarantunut ja noin tuhannesta kirurgisesta operaatiosta vain yksi peruttiin potilasturvallisuusriskeihin liittyen. Kokonaiskuva ja toiminnan volyymi huomioiden ohjeistus ja koulutus olivat asianmukaisella tasolla tilanteen vakavuus, laajuus ja kesto huomioiden.

HUS tuo esille, että erilaisista häiriö- ja uhkatilanteista ilmoittamista on harjoiteltu ja menettely toimii hyvin. Sairaanhoitopiiri tekee ilmoituksen STM:n valmiuspäivystäjälle ja Valviraan matalalla kynnyksellä. Täsmällisempää suunnittelua ja harjoittelua sen sijaan tarvitaan siihen, millaisia johtamistoimenpiteitä valtion viranomaiset tällaisessa tilanteessa tekevät ja mitkä ovat operatiivisen vastuuorganisaation vastuulla. Tähän rajapintaan liittyvä määrittelemättömyys nousi esiin tässäkin tapauksessa, mutta ei lopulta vaikuttanut toiminnan johtamiseen eikä tuloksiin.

HUS esittää lausunnossaan täsmennyksiä sen valtakunnallisiin tehtäviin, terveydenhuoltopoolin tehtäviin sekä tiettyihin tietoteknisiin yksityiskohtiin.

HUSin mukaan selostuksen luonnoksessa kokonaisuutena kiinnitetään huomiota tärkeisiin näkökohtiin ja haavoittuvuuksiin, jotka koskevat kaikkia terveydenhuollon toimialan toimijoita. Analysoimalla tapahtuneita häiriötilanteita ja nostamalla esiin kehittämistarpeita kyetään parantamaan organisaatioiden jatkuvuudenhallinnan prosesseja ja häiriötilanteiden toimintavalmiuksia. Vain näin yhteiskuntamme häiriötilannesietoisuus lisääntyy.

CGI Suomi Oy ilmoittaa lausunnossaan, ettei sillä ollut huomautettavaa tutkintaselostuksen luonnoksesta.