TOIMINTOJEN JA TIETOJÄRJESTELMIEN KRIITTISYYDEN LUOKITTELU

TERVEYDENHUOLTO

KYBER-TERVEYS-HANKE
Janne Mutanen, Petri Tolonen & Pekka Vepsäläinen
TLP: White

HUOLTOVARMUUSKESKUS
Aleksanterinkatu 48 A, 00100 Helsinki • Puhelin 02950 510 00 • Fax 09 260 9584
www.huoltovarmuus.fi • etunimi.sukunimi@nesa.fi • Y-tunnus 02024196 • Kotipaikka HELSINKI

Tämä materiaali on tuotettu Huoltovarmuuskeskuksen Kyber-Terveys-hankkeessa kriittisyysluokittelun pilottiprojektien aikana. Sisältö on muotoutunut kehittämistyössä saatujen oppien ja palautteiden kautta. Kiitokset erityisesti osallistuneiden organisaatioiden edustajille kommenteista ja terveydenhuollon käytäntöjen esiintuomisesta.

SISÄLLYSLUETTELO

TIIVISTELMÄ

Lääkinnälliset laitteet ja sairaaloiden tietojärjestelmät ovat yhä useammin kytkettyinä tietoverkkoihin, toisiin tietojärjestelmiin ja internettiin, mikä usein mahdollistaa tehokkaamman hoitotyön, mutta toisaalta tuo tullessaan kyberuhkia, jotka voivat vaarantaa niin potilasturvallisuuden kuin potilaiden yksityisyyden suojankin. Sairaalan toiminnan ja potilashoitoon käytettyjen lääkinnällisten laitteiden ja tietojärjestelmien kriittisyyden arviointi ja määrittely muodostavat perustan jatkuvuuden suunnittelu- ja toteutustyölle. Laitteiden ja järjestelmien suuren lukumäärän vuoksi on tiedettävä, mihin rajalliset resurssit kannattaa kohdistaa ja millaisen palvelutasosopimuksen mikäkin palvelu tarvitsee. Kriittisyysluokittelu tuo siten tukea päätöksentekoon ja priorisointiin niin etukäteen tehtyjen varautumistoimenpiteiden, kuin häiriötilanteiden hallintaan ja toipumiseen liittyvien toimenpiteidenkin osalta. Kriittisyysluokitteluun liittyy olennaisesti tiedon, tietojärjestelmien ja tietoverkkojen kriittisyyden arviointi, mutta erityisesti sairaalaympäristössä on tärkeää ymmärtää potilaan hoitoon, potilasturvallisuuteen ja jatkuvuuden hallintaan liittyvät kriittisimmät toiminnot ja prosessit.

Sosiaali- ja terveydenhuollon organisaatioissa on tyypillisesti tunnistettu toiminnan kannalta kriittiset tietojärjestelmät. Usein järjestelmille on määritetty kriittisyyden perusteella palvelutaso, jonka mukaisesti järjestelmän ylläpitäjä tuottaa palvelulle ja palvelun taustalla olevalle tietojärjestelmälle tukipalvelua. Toteutetuissa kriittisyysluokittelun pilottiprojekteissa todettiin, että on tarpeen tarkastella myös organisaation ydintoimintaa tukevien palveluiden kriittisyyttä tietojärjestelmien kriittisyysarvioinnin lisäksi. Organisaation ydintoiminta on riippuvaista näistä toimintaa tukevista alipalveluista. Palvelusta riippuen jotkin alipalveluista ovat erittäin kriittisiä, eli alipalvelun katko voi pysäyttää ydinpalvelun tuotannon. Toiset alipalvelut ovat taas vähemmän kriittisiä, eli niiden katkosta huolimatta sairaalan tai yksikön toiminta voi kokonaisuutena jatkua varsin normaalisti.

Kriittisyysluokittelutyössä oli tavoitteena luoda malli tarkastelun kohteena olevan organisaation tai palveluyksikön ydinpalvelun palveluprosessin kuvaamiseen sekä ydinpalvelua tukevien alipalveluiden tunnistamiseen ja niiden kriittisyyden arviointiin. Saman mallin mukaisesti voidaan tunnistaa ydinpalvelun ja alipalveluiden tuottamiseen liittyvät tietojärjestelmät. Alipalveluiden kriittisyyden arviointi auttaa myös tietojärjestelmien kriittisyyden arvioinnissa.

Kriittisyysluokittelussa on hyvä käyttää viitekehyksenä parhaita käytäntöjä ja standardien mukaisia menetelmiä, jotta voidaan paremmin varmistua organisaation kyberturvallisuuden hallitusta toteutuksesta. Organisaation kyberturvallisuuden hallintaan voidaan käyttää esimerkiksi kansainvälisen ISO/IEC standardointiorganisaation ISO/IEC 27000 standardiperheeseen kuuluvia standardeja. Lisäksi yhdysvaltalaisen NIST viraston alaiset standardit ja viitekehykset ovat varsin yleisesti käytössä myös Euroopassa. Standardien mukaisten menetelmien käyttö edesauttaa myös kansallisella tasolla yhtenäisten toimintamallien syntymistä.

Kriittisyysluokittelutyön pilottikohteina oli kaksi sairaanhoitopiiriä. Dokumentissa ei kuvata näissä sairaanhoitopiireissä tehdyn työn sisältöä, vaan tavoitteena on tuoda esiin yleispäteviä ohjeita kriittisyysluokittelutyön kehittämiseksi. Työ oli osa Huoltovarmuuskeskuksen Kyber-Terveys-hanketta.

1 JOHDANTO

Tässä dokumentissa kuvataan tietojärjestelmien, lääkinnällisten laitteiden ja toimintojen kriittisyyden arviointi- ja kehitystyötä terveydenhuoltoalalla. Tavoitteena on auttaa sairaanhoitopiirejä, tulevia hyvinvointialueita ja muita sosiaali- ja terveydenhuollon organisaatioita määrittelemään toimintojen ja tietojärjestelmien kriittisyyttä kyberturvallisuuden näkökulmasta. Kriittisyyden arviointi ja määrittely muodostavat myös perustan toiminnan ja kriittisten tietojärjestelmien sekä lääkinnällisten laitteiden jatkuvuuden suunnittelu- ja toteutustyölle. Dokumentti on suunnattu terveydenhuollon tietohallinnon, tietoturvallisuuden ja prosessien kehittämisen ammattilaisille.

Kriittisyysluokittelutyö on kiinteässä yhteydessä organisaation riskienhallintaan. Kriittisyysluokittelua voidaan hyödyntää esimerkiksi tietojärjestelmien riskiarvioinnissa. Tämän avulla organisaatioille muodostuu käsitys kunkin tietojärjestelmän kriittisyydestä toimintokohtaisesti. Tämä puolestaan auttaa organisaatiota hankkimaan tietojärjestelmille ja niiden avulla tarjottaville palveluille oikean tasoisen palvelutasosopimuksen. Ajantasaisella palvelutasosopimuksella varmistetaan kustannustehokas palvelu erityisesti kriittisille palveluille ja tietojärjestelmille.

Kriittisyysluokittelu luo perustan toiminnan jatkuvuuden hallinnalle. ”Jatkuvuuden hallinta on ydintoimintojen varmistamista ennalta määriteltyjen mallien mukaan normaalioloissa, häiriötilanteissa ja poikkeusoloissa” (Vahti 2016). On tunnistettava tietojärjestelmien ja palveluiden kriittisyys sekä arvioitava riskien toteutumisen vaikutus palveluiden ja järjestelmien toimintakykyyn.

Jos kriittisyysluokittelua ei tehdä systemaattisesti, saattaa syntyä käsitys, jonka mukaan lähes kaikki tietojärjestelmät, lääkinnälliset laitteet ja toiminta on kriittistä. Tällöin varautumisessa ja häiriötilanteiden hallinnassa ei pystytä keskittymään aidosti hoitotyön kannalta tärkeimpien toimintojen ja järjestelmien turvaamiseen. Taloudellisia resursseja ja henkilöresursseja ei pystytä myöskään kohdentamaan oikein, jolloin saatetaan panostaa kohteisiin, jotka eivät olekaan niin kriittisiä, ja tällöin voi jäädä liian vähän resursseja tärkeimpien kohteiden turvaamiseen. Tehokas priorisointi toteutuu, kun toimintojen ja tietojärjestelmien kriittisyysluokittelua tehdään systemaattisesti ja sitä tarkistetaan säännöllisesti.

Onnettomuustutkintakeskus (OTKES) suosittaa tutkintaselostuksessaan (2/2019; tutkintatunnus Y2018-02) muun muassa seuraavia toimenpiteitä:

”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]

”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]

”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]

”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]

2 KÄSITTEITÄ

Jatkuvuuden hallintaan, varautumiseen ja kriittisyysluokitteluun liittyvät käsitteet eivät ole täysin yksiselitteisiä, eikä niitä käytetä eri yhteyksissä aina johdonmukaisesti. Keskeistä on erottaa toisistaan normaaliolot, normaaliolojen häiriötilanteet ja poikkeusolot. Seuraavassa on kuvattu jatkuvuussuunnittelun keskeisiä käsitteitä, joihin tämän dokumentin terminologiat nojaavat.

Alipalvelut. Alipalvelut ovat ydintoimintaa tukevia palveluita kuten esimerkiksi logistiikka, laitoshuolto, pesupalvelut, ravintohuolto ja välinehuolto. Tässä dokumentissa alipalvelut jaetaan kahteen kategoriaan: 1. tason alipalvelut (yllä kuvatut esimerkit) ja 2. tason alipalvelut (esimerkiksi sähkö, vesi, lämpö, happi ja tietotekninen infrastruktuuri). Ydintoiminnan ja alipalveluiden välillä on riippuvuussuhteita, joista on kerrottu tarkemmin kohdassa 5.1 *Toimintojen ja tietojärjestelmien riippuvuudet.*

Jatkuvuussuunnittelu. Jatkuvuussuunnittelu on osa organisaation tietoturvallisuutta, laadunvarmistusta ja riskienhallintaa. Jatkuvuussuunnittelun tarkoituksena on taata toimintojen jatkuvuus normaalioloissa, normaaliolojen häiriötilanteissa ja muissa erityistilanteissa. Tavoitteena on ennalta varautua mahdollisiin ongelmatilanteisiin.

Kriittisyysluokittelu. Kriittisyysluokittelulla tarkoitetaan kriittisyyden arviointia terveydenhuoltoyksikön tietojärjestelmille, lääkinnällisille laitteille ja toiminnalle. Tässä dokumentissa ei oteta kantaa kriittisyysluokittelun kriteeristöön, mutta annetaan malliesimerkkejä.

Kyberhäiriö. Yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu toteutunut kyberuhka, joka vaarantaa tietojen ja tarjottavien palveluiden tietoturvan sekä vaikuttaa organisaation toimintaan epäsuotuisasti.

Toipumissuunnitelma. Toipumissuunnitelma on jatkuvuussuunnitelman osa ja se sisältää ohjeet häiriötilanteesta toipumiseksi, toiminnan jatkamisesta kohti normaalia toimintaa.

Tukipalvelut. Tukipalveluilla tarkoitetaan tässä yhteydessä erityisesti tietojärjestelmiin ja lääkinnällisiin laitteisiin tarkoitettua tukea palvelutuottajien toimesta. Tukipalvelut ovat yksi osa alipalveluita.

Kyberturvallisuuden käsitteisiin ja sanastoon voi tutustua laajemmin osoitteessa https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

3 KRIITTISYYSLUOKITTELUN VIITEKEHYKSIÄ JA STANDARDEJA

Organisaation kyberturvallisuutta voidaan hallita ja kehittää monin eri tavoin. Käyttämällä alan parhaita käytäntöjä ja standardien mukaisia menetelmiä, voidaan paremmin varmistua, että organisaation kyberturvallisuutta toteutetaan hallitusti kokonaisuutena. Kyberturvallisuuden hallintaan voidaan käyttää esimerkiksi kansainväliseen ISO/IEC 27000 standardiperheeseen kuuluvia standardeja. Lisäksi yhdysvaltalaisen NIST viraston alaiset standardit ja viitekehykset ovat varsin yleisesti käytössä myös Euroopassa.

Standardien mukaisten menetelmien käyttö edesauttaa kansallisella tasolla yhtenäisten toimintamallien syntymistä. Standardoitujen menetelmien mukaisesti kriittisyysluokittelua voidaan tehdä samoin periaattein ja yhteneväisin menetelmin. Myös yhteistyö organisaatioiden välillä helpottuu ja tehostuu, kun useissa organisaatioissa käytetään samoja periaatteita ja menetelmiä. Lisäksi voidaan varmistaa omassa organisaatiossa käytettävien menetelmien perehdytys uusille työntekijöille.

Kriittisyysluokitteluun liittyy olennaisesti tiedon, tietojärjestelmien ja tietoverkkojen kriittisyyden arviointi. Sairaalaympäristöissä on tärkeää ymmärtää myös monimutkaisen terveydenhuollon järjestelmän kannalta kriittisimmät toiminnot potilasturvallisuuden ja sairaalan toiminnan jatkuvuuden kannalta. Kun sairaalan toimintojen kriittisyyttä arvioidaan systemaattisesti, saadaan kyberturvallisuuden hallinnan kehittämisen lisäksi tukea myös sairaalan toiminnan jatkuvuuden kehittämiseen kokonaisuudessaan.

Systemaattisesti toteutettu kriittisyysluokittelu voi osoittautua kyberhäiriötilanteissa erityisen arvokkaaksi jatkuvuuden hallinnan kannalta. Häiriötilanteissa pystytään nopeammin arvioimaan tehtävien päätösten vaikutuksia ja merkittävyyttä potilashoitoon. Häiriötilanteessa voidaan joutua pohtimaan mm. mitkä tietojärjestelmät pitäisi pystyä pitämään käytettävissä, jotta sairaalan ydintoiminnot voidaan pitää käynnissä. Jos järjestelmiä on jouduttu häiriötilanteessa ajamaan alas, on tärkeää ymmärtää, mitä järjestelmiä tulee ensimmäisinä ottaa uudelleen käyttöön, kun häiriötilanteesta palataan normaalitilaan.

3.1 ISO/IEC 27000 standardisarja

ISO 27000 sarjan standardeissa määritellään vaatimuksia ja parhaita käytäntöjä tietoturvallisuuden hallintajärjestelmän luomiselle, toteuttamiselle, käyttämiselle, valvonnalle, ylläpidolle ja parantamiselle. Standardissa esitetyt vaatimukset on kohtalaisen helposti sovellettavissa erilaisille organisaatioille niiden tyypistä, koosta tai luonteesta riippumatta. Yleensä ISO 27000 sarjassa viitataan ISO 27001 standardiin, jonka vaatimuksia voidaan käyttää organisaatioiden vaatimustenmukaisuuden sertifiointiin.

ISO 27000 sarja liittyy kriittisyysluokitteluun oleellisesti riskienhallinnan sekä tiedon luokittelun näkökulmista. ISO 27001 standardissa esitetään erilaisia riskien

hallintakeinoja, joista kriittisyysluokitteluun liittyy erityisesti ”*Suojattavan omaisuuden hallinta”.* Tähän liittyviä yksityiskohtaisempia hallintakeinoja ovat mm. *Suojattavan omaisuuden luetteloiminen* sekä *Tiedon luokittelu*. Suojattavan omaisuuden luetteloinnin kautta saadaan ymmärrys, mitä eri suojattavia kohteita organisaation tietoon ja tietojenkäsittelyyn liittyy. Nämä voivat olla varsinaisen tiedon lisäksi esimerkiksi tietojärjestelmiä ja laitteita, joissa tietoa käsitellään.

Tiedon luokittelun osalta hallintakeino määritellään seuraavasti: *Tieto on luokiteltava lakisääteisten vaatimusten, tiedon arvon ja kriittisyyden sekä sen luvattoman paljastumisen tai muokkaamisen aiheuttamien vaikutusten perusteella.* Tämä hallintakeino kattaa kriittisyysluokittelun näkökulmasta varsin laajasti sekä lainsäädännön, että organisaation jatkuvuuden kannalta huomioitavia seikkoja.

ISO 27002 standardi määrittelee tietoturvallisuuden hallintaa koskevia menettelyohjeita. Standardia voidaan käyttää käytännön ohjeistuksena, jonka pohjalta voidaan kehittää organisaation turvallisuusstandardeja ja tehokkaita turvallisuusjohtamisen käytäntöjä.

ISO 27799 standardissa määritellään ohjeet, jotka tukevat standardin ISO/IEC 27002 tulkitsemista ja toteuttamista terveydenhuollon toimialalla, ja tämä standardi toimii kyseistä kansainvälistä standardia täydentävänä oppaana.

3.2 Muita ISO/IEC standardeja

ISO 31000 standardi on keskeisin ISO-standardointijärjestön riskienhallintastandardi. Standardi soveltuu organisaation kaikkien riskien hallintaan laajuuden ja kattavuuden vuoksi. Se on hyvin sovellettavissa erilaisten organisaatioiden käyttöön. Kyseessä on ohjeistusstandardi, joka ei sisällä suoranaisia vaatimuksia, eikä sen käyttöä voi sertifioida.

ISO 22301 standardi pitää sisällään vaatimukset, jotka organisaation on täytettävä osana jatkuvuuden hallintaansa. Standardi pitää sisällään vaatimuksia ja se on sertifioitavissa.

Yksittäisiä hallintajärjestelmiä löytyy muillekin eri osa-alueelle kuten esimerkiksi laadunhallinta (ISO 9001) ja työterveys (ISO 45001).

3.3 NIST Cyber Security Framework (CSF)

NIST on Yhdysvaltain kauppaministeriön alainen virasto, jonka tehtävänä on mm. kehittää standardointia. NIST Cyber Security Framework viitekehyksen luonti aloitettiin vuonna 2014 presidentti Barack Obaman säädöksen pohjalta (Cybersecurity Enhancement Act of 2014). Säädöksen tavoitteena on parantaa Yhdysvaltain kriittisen infrastruktuurin kyberturvallisuutta. NIST kannustaa organisaatioita myös muokkaamaan viitekehyksen määrittelemää mallia organisaation tarpeiden mukaan, jotta siitä saataisiin mahdollisimman paljon hyötyä. CSF-kypsyysmalli perustuu organisaation tekemään itsearviointiin ja sen tarkoituksena on kustannustehokkaasti auttaa organisaatioita tunnistamaan, arvioimaan ja hallitsemaan kybertoimintaympäristöön liittyviä riskejä.

NIST CSF-kypsyysmalli jakautuu viiteen eri vaiheeseen: 1) Tunnistaminen, 2) Suojautuminen, 3) Havainnointi, 4) Reagointi ja 5) Palautuminen. Kaikkiin näihin vaiheisiin liittyy toimintojen ja tiedon kriittisyyden arviointi eri näkökulmista.

NIST CSF-kypsyysmallista löytyy kriittisyysluokitteluun oleellisesti liittyviä aiheita. Tunnistamiseen liittyen viitekehyksessä määritellään *Suojattavien kohteiden hallinta* seuraavasti: *Organisaation liiketoimintatavoitteiden saavuttamiseen tarvittavat tiedot, henkilöstö, laitteet, järjestelmät ja toimitilat on tunnistettu ja niitä hallitaan niiden suhteellisen tärkeyden ja organisaation riskistrategian mukaisesti.* Lisäksi *Liiketoimintaympäristö* määritellään seuraavasti: *Organisaation tehtävä, tavoitteet, sidosryhmät ja toiminnot ymmärretään ja ne on asetettu tärkeysjärjestykseen. Tätä tietoa käytetään kyberturvallisuuteen liittyvien roolien ja vastuiden määrittämiseen sekä riskipäätöksiin.*

3.4 Kybermittari

Yksi kriittisyysluokitteluun liittyvä työkalu on Kyberturvallisuuskeskuksen Kybermittari, jonka tarkoituksena on mitata organisaation kyberturvallisuuden kypsyyttä. Kartoituksen perusteella saadaan mitatuista osa-alueista tilannekuva, joka mahdollistaa toimialan ja sen organisaatioiden kyberturvallisuuden kypsyyden vertailun. Arviointimalli on suunnattu huoltovarmuuskriittisille yrityksille ja yhteisöille, mutta myös muut toimijat voivat käyttää sitä oman kyberturvallisuutensa arviointiin.

Arviointimallin tarkoituksena on mitata itsearviointi- ja haastattelutyyppisesti organisaation toimintamalleja, prosesseja ja tekniikoita, sekä arvioida organisaation tekemiä investointeja kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. Mallia voidaan käyttää myös työpajoissa, joihin on sitoutettu organisaation kannalta kriittisen toiminnan edustus ja sen sidosryhmät. Tulosten avulla pyritään tuottamaan asiantuntijoiden ja johdon kannalta ymmärrettävä kuvaus siitä, mitä kyberturvallisuuden riskejä organisaatio itse pystyy hallitsemaan, ja onko kaikki yhteiskunnan huoltovarmuuden kannalta olennaiset riskit tunnistettu.

Kybermittarin ovat kehittäneet Huoltovarmuuskeskus ja Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus yhdessä kriittisen infrastruktuurin organisaatioiden, yritysten, riskienhallinnan asiantuntijoiden ja viranomaisten kanssa. Mallin oikeudet omistaa Kyberturvallisuuskeskus, ja se on tarkoitettu avoimeksi työkaluksi, jota pyritään kehittämään edelleen yhdessä sitä käyttävien tahojen kanssa.

Kybermittari koostuu yhdestätoista eri kyberturvallisuuden osiosta, osioille esitetyistä tavoitteista sekä tavoitteiden täyttymistä mittaavista käytännöistä. Osiot on esitetty kuvassa 1, jossa näkyvät myös NIST-viitekehyksen viisi eri vaihetta.

KUVA 1. Kybermittarin osiot

3.5 Yhteenveto viitekehyksistä

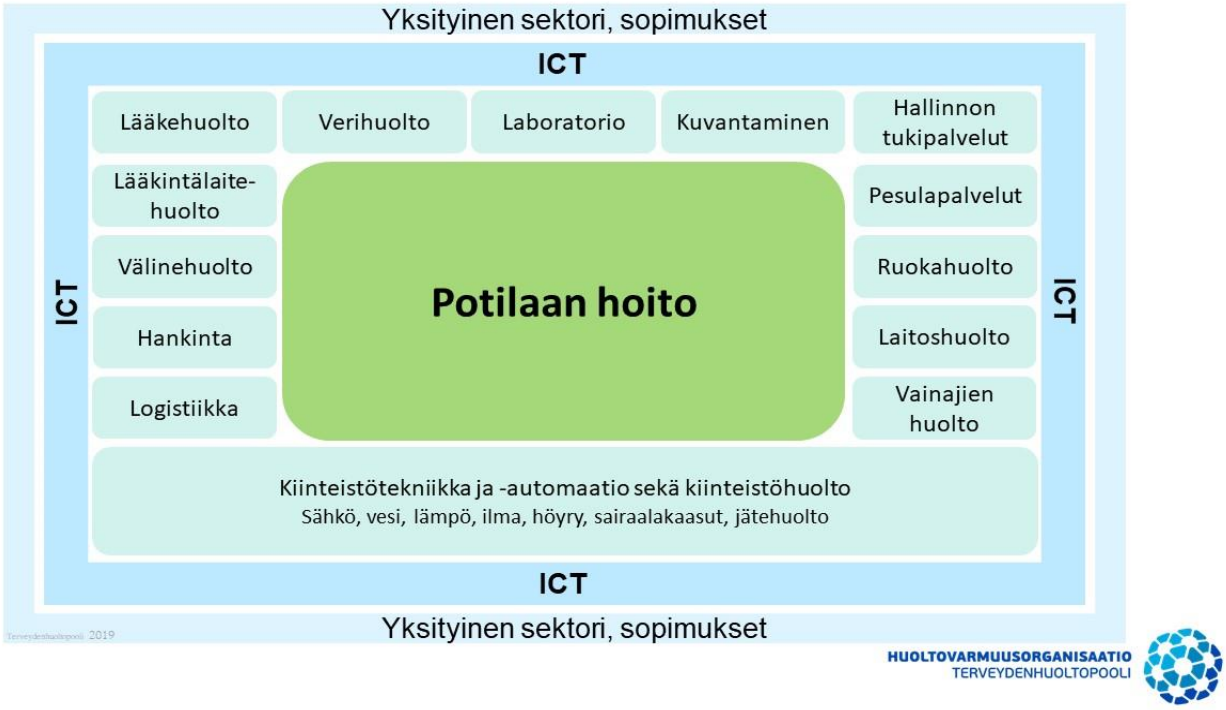
Yhteenvetona viitekehyksistä voidaan todeta, että edellä kuvatut viitekehykset soveltuvat kriittisyysluokittelun tarkasteluun varsin hyvin erityisesti kyberhäiriötilanteiden hallinnan näkökulmasta. Kriittisyysluokittelu tuo tukea päätöksentekoon ja priorisointiin niin etukäteen tehtyjen varautumistoimenpiteiden, kuin häiriötilanteiden hallintaan ja toipumiseen liittyvien toimenpiteidenkin osalta.

Kriittisyysluokittelun kannalta on hyvä myös ymmärtää, että riippumatta taustalla käytetystä viitekehyksestä, kriittisyysluokittelu auttaa terveydenhuollon organisaatiota kehittämään kokonaisuudessaan kyberturvallisuuden ja kokonaisturvallisuuden hallintaa. Sen myötä voidaan mm. perustella paremmin kyberturvallisuuteen liittyviä investointipäätöksiä ja tarvittavia kehittämistoimenpiteitä. Lisäksi toiminnan jatkuvaa arviointia tehdessä kriittisyysluokittelun avulla voidaan tunnistaa kohteet, joita esimerkiksi sisäisissä auditoinneissa tulee käydä läpi säännöllisesti.

4 KRIITTISYYSLUOKITTELU TERVEYDENHUOLLOSSA

4.1 Terveydenhuollon toimintaympäristö

Terveydenhuollon suuren lääkintälaite- ja tietojärjestelmämäärän vuoksi on tarpeen tunnistaa, mihin rajalliset resurssit kannattaa kohdistaa ja millaisen palvelutasosopimuksen mikäkin palvelu tarvitsee. Jotta ymmärrämme, missä toiminnoissa mikäkin laite tai järjestelmä on kriittinen, on selvitettävä myös terveydenhuollon yksikön toimintaprosessit. Palveluiden tuottajina voivat olla myös ulkoiset palvelutuottajat, jonka vuoksi toimittajahallinta on keskeisessä roolissa terveydenhuollon kokonaisuudessa. Tyypillinen sairaalan toimintaympäristö on esitetty kuvassa 2.



KUVA 2. Tyypillinen sairaalan toimintaympäristö.

Toiminnot ovat riippuvuussuhteessa toisiinsa. Toiminnoista potilaan hoito, laboratoriopalvelut ja kuvantaminen muodostavat ydinpalvelut. Niiden ympärillä on iso joukko tukipalveluita, jotka ovat alipalveluita ydinpalveluille. Alipalvelut voivat olla sairaalan omia palveluita tai ne voivat olla hankittu palveluna alihankkijoilta. Sen lisäksi sidosryhmiin kuuluvat muun muassa tietojärjestelmien laitteisto-, ohjelmisto- ja verkkopalveluita tuottavat toimittajat ja palvelukumppanit. Sairaalan tietoteknisen palvelun tuottaa joko sairaalan oma IT-yksikkö tai sopimussuhteessa oleva palvelun tuottaja.

Tietojärjestelmien näkökulmasta katsottuna tietojärjestelmiin liittyvä kerrostuma on esitetty kuvassa 3 ilman palvelutuotantoa.

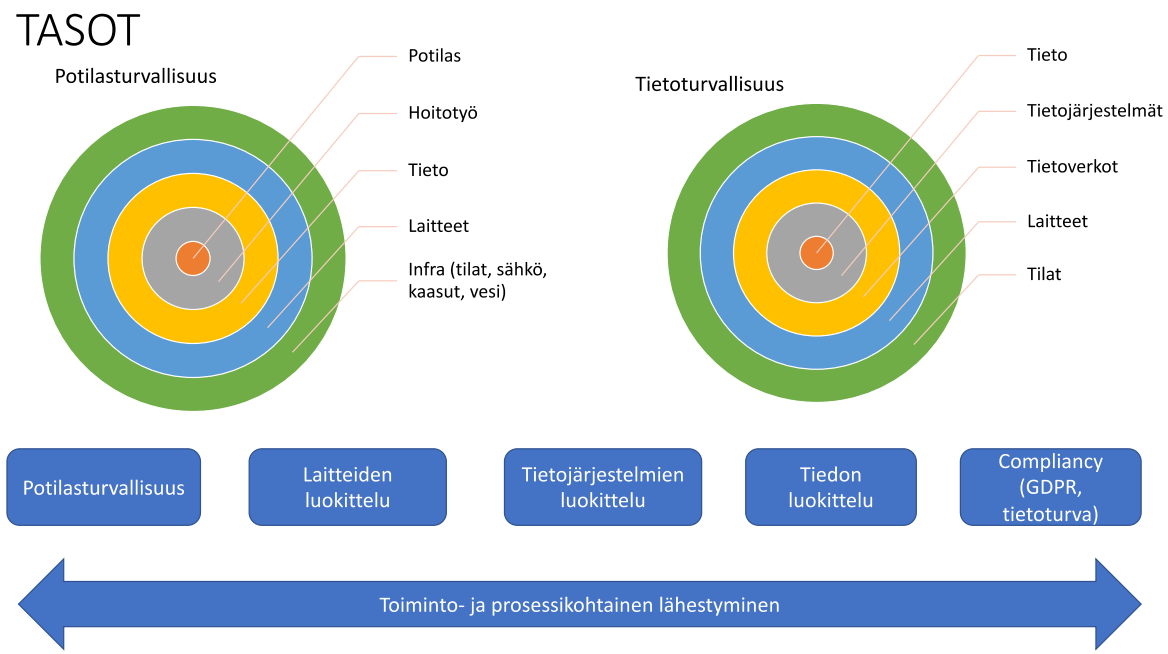
KUVA 3. Tietojärjestelmät ja niiden ympärillä olevat osa-alueet.

Potilaan kuuluu saada tarvitsemansa oikea hoito niin, että siitä aiheutuu hänelle mahdollisimman vähän haittaa. Laajemmin käsitettynä potilasturvallisuudella tarkoitetaan terveydenhuollossa toimivien ammattihenkilöiden, toimintayksiköiden ja organisaatioiden periaatteita ja toimintakäytäntöjä, joilla varmistetaan potilaiden terveyden- ja sairaanhoidon palvelujen turvallisuus. Tällöin potilaan hoidon turvallisuudella tarkoitetaan myös sairauksien ehkäisyn, diagnostiikan, hoidon ja kuntoutuksen turvallisuutta. Tietoturvallisuudella ei ole itseisarvoa, vaan sen pitää tukea potilaaseen kohdistuvaa hoitotyötä ja varmistaa työssä tarvittava tietoturvallisuus.

Potilastyö on yhä enemmän riippuvainen tietojärjestelmistä ja digitaalisista palveluista. Lääkinnälliset laitteet ja sairaaloiden tietojärjestelmät ovat kytkettyjä pilviratkaisuihin, tietoverkkoihin ja toisiin tietojärjestelmiin, mikä usein mahdollistaa tehokkaamman hoitotyön, mutta toisaalta tuo tullessaan kyberuhkia, jotka voivat vaarantaa niin potilasturvallisuuden kuin potilaiden yksityisyyden suojankin.

Kovin usein ajatellaan, että potilastietojärjestelmä on ainoa kriittinen osa potilastyötä. Potilastyössä jokin muu tietojärjestelmä tai laite voi kuitenkin olla samalla tavoin kriittinen potilasturvallisuudelle ja hoitotyön onnistumiselle. Jos palvelun-tuottajalla ei ole ajantasaista tietoa siitä, mikä merkitys kyseisellä tietojärjestelmällä on kliinisen yksikön toimintaan, ei sen toimintavarmuuteen ja palvelutasoon ole välttämättä kiinnitetty riittävästi huomiota. Häiriöt tällaisten järjestelmien toiminnassa voivat pahimmillaan aiheuttaa potilasturvallisuuteen liittyvien riskien toteutumisen, joten asiaan tulee kiinnittää huomiota.

Tietojärjestelmien ja toimintojen yhteinen kriittisyyden arviointi muodostavat kokonaisuuden, jolla on vaikutusta potilasturvallisuuteen. Kokonaisuuden muodostavat tasot on esitetty kuvassa 4.



KUVA 4. Kuvaus eri tasoista sekä potilasturvallisuuden että tietoturvallisuuden näkökulmasta.

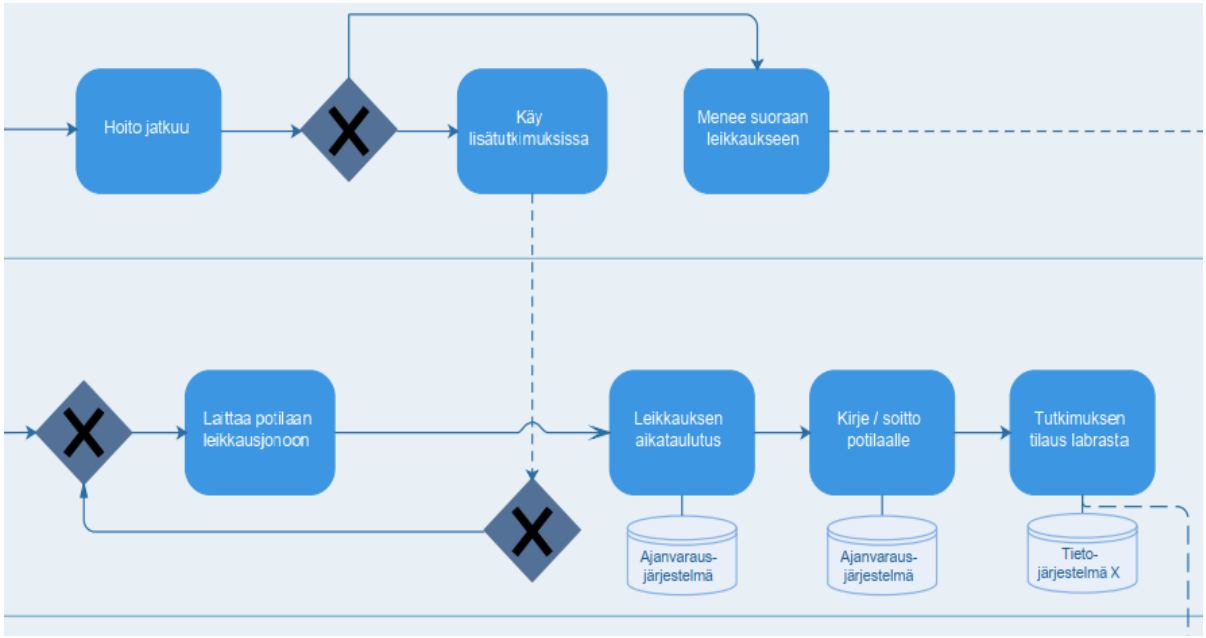
4.2 Prosessien kuvaaminen

Prosessien kuvaamisen tavoitteena on tunnistaa hoitoketjun eri vaiheet yksityiskohtaisesti, mikä auttaa tehostamaan toimintaa ja osoittamaan toiminnan kriittiset kohdat läpinäkyvästi. Toimintokohtaisten prosessien kuvaaminen yhtenäistää menettelyjä ja selkiyttää henkilökunnan työnjakoa sekä vastuuta ja siten parantaa toiminnan sujuvuutta. Tämä puolestaan myötävaikuttaa poikkeamien ja virheiden vähenemiseen. Hoitoyksikön toiminnot koostuvat useista eri alipalveluista, joita tuottavat yhä useammin hoitoyksikköön sopimussuhteessa olevat palvelutoimittajat tai heidän alihankkijansa. Terveydenhuollon organisaation yhdenmukainen toimintojen kuvaamistapa auttaa hoitoyksikön kaikkia toimijoita ymmärtämään toimintojen kriittisyyden. Näin voidaan varmistaa oikeatasoinen tiedonkulku riippuvuussuhteessa olevien toimijoiden välillä.

Prosessien kuvaamisen tärkeyttä ei voi liiaksi korostaa, sillä prosessien kuvaukset luovat perustan nykytilanteen kokonaisvaltaiselle ymmärtämiselle. Toiminnan tai tietojärjestelmien muutoksissa terveydenhuollon palvelutuotanto ei saa keskeytyä eikä laadussa saa tapahtua poikkeamia muutosten vuoksi. Potilasturvallisuussuunnitelmaohjeissa tuodaan esille, kuinka kokonaisvaltainen laadun- ja riskienhallinta vaatii organisaatiolta selkeän toimintatavan ja rakenteet. Laadun ja potilasturvallisuuden kehittäminen on oltava jatkuva työskentelytapa, jonka avulla mm. prosesseja kehitetään riskien arviointiin perustuen.

Prosessien kuvaaminen on tärkeää vähintään karkealla tasolla tietovuokaavioin. Tämä auttaa ymmärtämään nykytilaa ja helpottaa uusien hankintojen vaatimus-

määrittelyvaiheessa, jos esimerkiksi hankitaan prosessissa käytettävää tietojärjestelmää tai lääkinnällistä laitetta. Esimerkki prosessien kuvaamisesta on esitetty kuvassa 5.



KUVA 5. Esimerkki prosessikuvauksesta.

4.3 Jatkuva kehittäminen

Digitalisaatio muuttaa yhteiskunnan rakenteita ja erityisesti sote-sektorin toimintatapoja. Muutostarpeita ja -paineita aiheuttavat digitalisaation lisäksi taloudelliset rakennemuutokset, asiakkaiden ja työntekijöiden esille tuomat kehittämiskohteet, yhteiskunnan rakennemuutokset sekä lainsäädännön muuttuminen. Muutokset aiheuttavat organisaation toimintaan häiriötiloja, joiden vuoksi toiminnan laatu voi väliaikaisesti heiketä. Jatkuva kehittäminen on kuitenkin osa laatutyötä, jota voidaan tehdä myös häiriötilanteet minimoiden. Muutostarpeet eivät kasaudu liian monimutkaisiksi kehittämishaasteiksi, kun jatkuvan toiminnan kehittämiselle luodaan organisaatioon sopiva jatkuvan kehittämisen malli ja kulttuuri. Tämä vaatii organisaatiolta tiettyä kypsyystasoa tehdä jatkuvaa parannustyötä operatiivisen toiminnan keskellä. Potilaan hoito ja potilasturvallisuus tulee pitää keskiössä kaiken aikaa.

Jatkuva kehittäminen on osa laatujohtamista, jonka avulla on mahdollista kehittää parempaa asiakaspalvelua, asiakastyytyväisyyttä, henkilöstön tyytyväisyyttä ja kustannustehokkuutta. Jatkuvan kehityksen toimintamallissa on syytä pitää myös kyberturvallisuus ja tietosuoja mukana koko ajan, jotta näitä asioita ei tuoda päälle liimattuina jälkikäteen. Useimmissa valmiissa toiminnan kehittämisen viitekehyksissä tätä sivutaan, mutta edelleenkin liian ohuesti. Olkoon kyse uusien laitteiden tai järjestelmien hankinnasta tai toimintaa koskevien prosessien muuttamisesta, niin jo hankinta- tai muutosprojektin alkukartoitusvaiheessa kyberturvallisuusvaatimukset tulee huomioida.

Toiminnan jatkuvaa kehittämistä helpottaa, jos organisaatiolla on selkeä visio siitä, mihin suuntaan toimintaa kehitetään. On huomattavasti helpompaa luoda toiminnan kehittämisen strategia, jos visio on kirkas ja siitä on yhteinen näkemys organisaation johdolla.

Jatkuva kehittäminen lähtee liikkeelle nykytilan ymmärtämisestä. Mitä paremmin nykytila on dokumentoitu, sitä nopeammin muutoksia voidaan lähteä toteuttamaan. Dokumentointiin kannattaa siis kiinnittää huomiota. Tänä päivänä on saatavilla parempia dokumentaatiota tukevia sovelluksia ja tietojärjestelmiä kuin koskaan aiemmin. Selkeän nykytilanteen ymmärtämisen avulla voidaan luoda totuudenmukaisempi muutosvaiheen suunnitelma, joka toimii tiekarttana kohti tavoitetilaa.

Oikealla viestinnällä on suuri merkitys toiminnan kehittämisen onnistumisessa. Muutosvastarinta on vähäisempää, kun kaikki asianosaiset ovat tietoisia tapahtuvista muutoksista ja tavoitetilasta. Tällöin myös muutosvaiheen epäkohdat nousevat riittävän aikaisessa vaiheessa esille ja tarvittaviin korjausliikkeisiin jää paremmin aikaa. Se säästää myös kustannuksia.

Toimintakulttuurin muuttaminen vaatii myös riittävää koulutusta ja opastusta henkilökunnalle. Tämä korostuu erityisesti palvelujen tilaaja-tuottajamallissa, jossa palveluiden (tai osapalveluiden) tuottajana voi olla ulkopuolinen organisaatio. Koulutus voi tuoda myös tulevaan kehitystyöhön toteuttamiskelpoisia ideoita, joiden työstämiseen kannattaa luoda malli osaksi jatkuvaa kehittämistä. Kyberturvallisuutta tulee tarkastella koko toimitusketjun osalta.

5 KRIITTISYYSLUOKITTELUTYÖ KYBER-TERVEYS-HANKKEESSA

5.1 Toimintojen ja tietojärjestelmien riippuvuudet

Sosiaali- ja terveydenhuollon organisaatioissa on tyypillisesti tunnistettu toiminnan kannalta kriittiset tietojärjestelmät. Usein järjestelmille on määritetty kriittisyyden perusteella palvelutaso, jonka mukaisesti järjestelmän ylläpitäjä tuottaa palvelulle tukipalvelua. Palvelutaso on määritetty ainakin keskeisille operatiivisille järjestelmille. Monessa organisaatiossa on kuitenkin käytössä järjestelmiä, joita ei ole tunnistettu tai tarkoitettu kriittisiksi, mutta ne ovat ominaisuuksiensa vuoksi kuitenkin päätyneet suunniteltua kriittisempään roolin. Tällaisia järjestelmiä voivat olla esimerkiksi viestintäratkaisut sekä dokumenttienhallintajärjestelmät.

Sairaaloissa otetaan käyttöön tavanomaisia toimisto- ja viestintäjärjestelmiä muiden organisaatioiden tapaan. Näitä ratkaisuja ei välttämättä ole tarkoitettu kriittiseen käyttöön, kuten potilashoitoon. Käytännössä kuitenkin esimerkiksi sähköpostia ja pikaviestintäsovelluksia saatetaan käyttää sairaalan operatiivisessa toiminnassa ja potilashoidon tukena. Tyypillisesti nämä ratkaisut ratkaisevat ongelmia ja tarpeita, joihin potilastietojärjestelmät eivät vastaa. Tällaisia tarpeita voivat olla sekalaisten dokumenttien tallentaminen ja välittäminen tietoturvallisesti käyttäjältä toiselle, sekä välitön viestintä kahden tai useamman henkilön kesken.

Ensimmäisessä Kyber-Terveys-hankkeen pilottihankkeessa oli tarpeen tarkastella organisaation ydintoimintaa tukevien palveluiden kriittisyyttä – ei pelkästään toimintaa tukevien järjestelmien kriittisyyttä. Organisaation ydintoiminta on riippuvainen sitä tukevista alipalveluista. Näitä alipalveluita on listattu kuvissa kuusi ja seitsemän. Sote-palvelusta riippuen jotkin alipalveluista ovat erittäin kriittisiä, eli alipalvelun katko voi pysäyttää ydinpalvelun tuotannon. Toiset alipalvelut ovat taas vähemmän kriittisiä, eli niiden katkosta huolimatta sairaalan tai yksikön toiminta voi kokonaisuutena jatkua varsin normaalisti.

Organisaation ydinpalvelut	Palveluiden tuottamisen välineet	Tieto / data	Huomioita
Potilaan hoito, kuvantaminen, laboratoriopalvelut	Potilaskertomus (potilastietojärjestelmä), Laboratorio- ja kuvantamisjärjestelmät, Tehohoidon järjestelmä		Mitä palveluita ko. yksikkö tuottaa? Alihankinnat sisältäen sopimukset

1. tason alipalvelut	Palveluiden tuottamisen välineet (kunkin palvelun omat järjestelmät)	Tieto / data (kuka omistaa, missä saatavilla)	Huomioita
1 Logistiikka			
2 Laitoshuolto			
3 Lääkehuolto			
4 Pesulapalvelut			
5 Ravintohuolto			
6 Asiakirja- ja tiedon hallinta?			
7 Lääkintälaitteet ja niiden huolto			
8 Henkilöstöhallinto			
9 Taloushallinto			
10 Välinehuolto			
11 Hankintapalvelut			
12 Henkilö- ja toimitilaturvallisuus			
13 Tietohallinto, Service Desk ja muut th:n palvelut			
14 Veripalvelut			
15 Lähetit, postitus, monistus			

Organisaation ydinpalvelut	Palveluiden tuottamisen välineet	Huomioita
Potilaan hoito, kuvantaminen, laboratoriopalvelut	Potilaskertomus (potilastietojärjestelmä), Laboratorio- ja kuvantamisjärjestelmät, Tehohoidon järjestelmä	

2. Tason alipalvelut		
16 Tietotekninen infrastruktuuri		
17 Sähkö		
18 Vesi		
19 Lämpö		
20 Happi		

KUVAT 6 ja 7. Organisaation ydinpalvelut ja alipalvelut.

Kriittisyysluokittelu aloitettiin haastatteluilla (johto, hoitotyö, toimistotyö). Työssä hyödynnettiin valitun yksikön prosessikuvauksia. Haastattelujen tarkoituksena oli kartoittaa riittävän yksityiskohtaisesti koko yksikön kriittiset toimintakohdat, tietojärjestelmät, lääkinnälliset laitteet ja resurssit. Haastattelujen avulla saadun tiedon ja käytössä olleiden prosessikuvausten avulla syntyi kattava luettelo kyseisen yksikön kriittisistä pisteistä ja niiden nykytilasta.

5.2 Tietojärjestelmien kriittisyyden tarkastelu ilman riippuvuussuhteita

Toisessa Kyber-Terveys-hankkeen pilottihankkeessa kriittisyysluokittelutyössä keskityttiin tietojärjestelmien ja niihin liittyvien palveluiden kriittisyyden arviointiin. Lähtökohtana oli se, että järjestelmien kriittisyyttä arvioidaan kokonaisvaltaisessa merkityksessä kaikkien tietojärjestelmien käyttökohteet ja yksiköt huomioiden.

Kriittisyys luokiteltiin neljään eri luokkaan. Luokkaan yksi kuuluivat ne tietojärjestelmät, joiden toimintakatkot aiheuttavat välittömästi toimintahäiriöitä yhdelle tai useammalla yksikölle tai ne välillisesti voivat aiheuttaa laajan toimintahäiriön useammalle yksikölle sekä ne olivat keskeisessä suhteessa muihin tietojärjestelmiin. Luokkaan kaksi kuuluivat tärkeät tietojärjestelmät, joiden lyhytaikainen alhaalla olo ei vaaranna potilasturvallisuutta, mutta pitkäaikainen alhaalla olo aiheuttaa toiminnalle merkittäviä riskejä. Järjestelmä voi olla myös ajan mukaan kriisiytyvän toiminnon tietojärjestelmä, joka mahdollistaa lyhyet alhaalla olot, mutta ei pidempiä katkoja. Luokka kolme sisälsi hyödylliset tietojärjestelmät, joita ilmankin pystytään tietyn aikaa toimimaan. Järjestelmän alhaalla olo kuitenkin haittaa päivittäistä toimintaa ja vaatii yksiköiltä poikkeavia toiminnan järjestelyitä. Luokan neljä järjestelmät ovat merkitykseltään vähäisiä, joita ilman yksikön toiminta ei vaarannu eikä toiminnan laatu laske. Kuvassa 8 on esimerkki tietojärjestelmien kriittisyysluokituksesta.

TIETOJÄRJESTELMIEN KRIITTISYYSLUOKITTELU				
	Luokka 1	Luokka 2	Luokka 3	Luokka 4
Vaadittavat tiedot	**Kriittinen**	**Tärkeä**	**Hyödyllinen**	**Vähäinen**
Järjestelmän nimi	Pakollinen	Pakollinen	Pakollinen	Pakollinen
Omistaja	Määritettävä	Määritettävä	Määritettävä	Määritettävä
Pääkäyttäjä	Määritettävä	Määritettävä	Suositeltava	Suositeltava
Tekninen omistaja	Määritettävä	Määritettävä	Määritettävä	Määritettävä
Tietojärjestelmä- / palvelusopimus	Voimassa	Voimassa	Voimassa	Voimassa
Tietojärjestelmän ylläpitosopimus	Voimassa	Voimassa	Suositeltava	Suositeltava
Komponenttien ylläpitosopimukset	Voimassa	Voimassa	Suositeltava	Suositeltava
Käyttäjämäärä (lukumäärä)	Määritettävä	Määritettävä	Määritettävä	Määritettävä
Vaikutus sairaalan toimintoihin	Määritettävä	Määritettävä	Määritettävä	Määritettävä
Häiriön vaikutusanalyysi (BIA)	Pakollinen	Pakollinen	Suositeltava	Suositeltava
SLAt	Pakollinen	Pakollinen	Suositeltava	Suositeltava
Käyttökatkon max kokonaiskesto (MTD)	8 tuntia	16 tuntia	4 arkipäivää	2 viikkoa
Palautumisaika (RTO)	Alle 4 tuntia	Alle 8 tuntia	2 arkipäivää	1 viikko
Palautumispiste (RPO)	"-1 päivä"	"-1 päivä"	"-1 päivä"	Sovittava
Toipumissuunnitelma	Pakollinen	Pakollinen	N/A	N/A
Järjestelmädokumentaatio	Pakollinen	Pakollinen	Pakollinen	Pakollinen
Tuki sovellusvirtualisoinnille	Pakollinen	Suositeltava	Suositeltava	Suositeltava
Päätösmatriisi	Pakollinen	Pakollinen	Ei välttämätön	Ei välttämätön
Kuvaus ja käyttötarkoitus	Pakollinen	Pakollinen	Pakollinen	Pakollinen
Elinkaari (kesto)	Määritettävä	Määritettävä	Määritettävä	Määritettävä
Huoltokatkot sovittuna	Pakollinen	Pakollinen	Pakollinen	Pakollinen

KUVA 8. Tietojärjestelmien kriitttisyysluokittelu.

Yllä kuvatun tietojärjestelmäkohtaisen kriittisyyden arviointi paljastaa ristiriitatilanteet, joissa yksikön/osaston odotusarvo tietojärjestelmälle voi olla kriittinen tai tärkeä, mutta koko tietojärjestelmää koskevassa palveluketjussa on puutteita tai epäjohdonmukaisuuksia. Toisaalta tämän tyyppisellä tarkastelutavalla havaitaan myös ne tilanteet, joissa palvelutaso merkitykseltään vähäiselle tietojärjestelmälle on liiankin korkea. Lisäksi tietojärjestelmiin kohdistuva kriittisyysluokittelu mahdollistaa tarkemman tavan luoda taloudelliset laskelmat ja budjetin tietojärjestelmäympäristön tuottamiselle.

Tietojärjestelmien kriittisyysluokittelutyö luo perustan kyberturvallisuuden tarkastelulle tietojärjestelmäympäristössä. Kun arvioidaan tietojärjestelmän kriittisyyttä, niin samalla tarkastellaan sitä käyttöympäristöä, missä se toimii. Esimerkiksi jos tietojärjestelmä todetaan kriittiseksi, niin on luontevaa selvittää, millaisessa verkkoympäristössä kyseinen tietojärjestelmä toimii. Yhdistettynä riskienhallintatyöhön, saatetaan havaita, että kyseisen tietojärjestelmän kriittisyyden vuoksi verkon segmentoinnille on tehtävä muutoksia, jotta laite tai järjestelmä voidaan tarvittaessa eristää muusta ympäristöstä. Kyseessä oleva kriittisyyden tarkastelu voi paljastaa myös sen epäkohdan, että uudelleen segmentointia ei voida tehdä ilman laajempaa verkkoympäristön uusimishanketta.

Tuottamalla samanaikaisesti tietojärjestelmien kriittisyysluokittelutyön kanssa kyberturvallisuuden riskien arvioinnin, voidaan havaita ja korjata merkittäviäkin tietoturvallisuuden puutteita. Tämä puolestaan mahdollistaa häiriön vaikutusanalyysin (BIA) tekemisen, joka luo puolestaan perustaa jatkuvuus- ja toipumissuunnittelutyölle. Jatkuvuussuunnittelun prosessissa on huomioitava sekä yksikkötaso että organisaation taso. Toimintayksiköiden näkemykset tulee lopuksi yhdenmu-

kaistaa koko organisaation tasolla, jotta toimintojen keskinäinen kriittisyys ja tavoitetasot ovat yhteismitallisia. Jatkuvuus- ja toipumissuunnitelmat muodostavat hierarkkisen kokonaisuuden, jossa eri tasoiset jatkuvuus- ja toipumissuunnitelmat muodostavat jatkuvuuden hallinnan kokonaisuuden (Vahti 2016).

5.3 Havaintoja kriittisyysluokittelutyön menetelmistä ja vaiheista

Kriittisyysluokittelussa tulisi käydä läpi kaikki organisaation yksiköt, jotka oleellisesti liittyvät sairaalan toimintaan. Tähän sisältyy varsinaisten hoitoyksiköiden lisäksi sellaiset tukipalvelut, jotka ovat kriittisiä kliinisen työn kannalta. Työ on järkevä pilkkoa tiettyihin vaiheisiin, joiden avulla kriittisyysluokittelutyön kokonaisuus rakentuu. Kriittisyysluokittelutyölle kannattaa hakea johdon tuki ja kuvata ne hyödyt, joita kohteena oleva yksikkö saavuttaa työn tekemisellä.

Alla kuvataan hyväksi todettuja työvaiheita ja -menetelmiä kriittisyysluokittelutyön etenemiseksi. Työmenetelmiä ja toimintatapaa työn edistämiseksi kannattaa pohtia etukäteen, sillä niillä on suuri merkitys työn onnistumiselle ja tavoitteiden saavuttamiselle. Työ jaksotetaan ja kuvataan alla kolmella eri päävaiheella: aloitusvaihe, työn tekeminen ja työpajat sekä tulostyöpaja & raportointi.

5.3.1 Kriittisyysluokittelutyön vaiheet

Aloitusvaihe. Aloitusvaiheen tärkeimpiä tehtäviä on asettaa työlle selkeät tavoitteet. Samalla työhön nimetään työn omistaja, projektipäällikkö ja työhön osallistuvat avainhenkilöt, joiden kanssa työn tavoitteet ja sisältö käydään yksityiskohtaisesti läpi. Aikataulusta on syytä tehdä realistinen, mutta työn tekemisen jatkuvuuden kannalta aikataulusta tulee pitää mahdollisuuksien mukaan kiinni. Aloitustehtäviin kuuluvat ennakkotehtävät, joiden merkitystä ei voi liiaksi korostaa. Niiden avulla orientoidutaan tehtävään työhön sekä saadaan selkeä käsitys nykytilasta. Ennakkotehtävän tarkoituksena on saada vastauksia etukäteen laadittuun kyselyyn toiminnan, tietojärjestelmien ja lääkinnällisten laitteiden kriittisyydestä. Se on myös valmistautumista tuleviin työpajatyöskentelyihin. Aloitusvaiheessa kannattaa pitää aloitustapaaminen, jossa kaikille tulee selkeä käsitys tehtävästä työstä, sen tavoitteesta, menetelmistä, resursseista, vastuista ja aikataulusta.

Työn tekeminen ja työpajat. Työpajatyöskentely on tehokas tapa saada selville kunkin yksikön toiminnan ja tietojärjestelmien kriittiset pisteet. Työpajaan kutsutaan paikalle kussakin vaiheessa oleelliset henkilöt antamaan riittävällä tasolla tietoa yksikön toiminnasta ja tietojärjestelmistä, jotta käsitellyt asiat saadaan dokumentoitua. Esimerkiksi hoitoyksikön ylilääkäri sekä ylihoitaja, jotka tuntevat yksikön toiminnot, ovat oleellisia henkilöitä kutsuttaviksi mukaan toimintojen läpikäyntityöpajaan. Työpajan vetäjä on laatinut selkeän agendan työpajalle. Ennakkotehtävänä olleen kyselyn perusteella työpajatyöskentelystä saadaan tehokas ja tuloksiin johtava yhteistyö kunkin yksikön kannalta.

Työpajojen avulla varmistetaan tietojärjestelmien ja toimintojen kriittisyys, sillä se luo perustan koko työlle. Jos kriittisyyden arvioinnin alkuvaiheen työ tehdään puutteellisesti, niin virheet kertaantuvat lopputuloksissa. Työpajatyöskentelyyn tulee

osallistua tietoturva-asiantuntija, jolla on kyvykkyys arvioida kyberturvallisuuden tilaa ja puutteita. Samalla hän voi havaita sellaisia käytössä olevia tietoturvaratkaisuja, joista voi olla työlle jopa haittaa. Se puolestaan mahdollistaa uusien tietoturvakäytänteiden ja -ratkaisujen tuottamisen, joka puolestaan sujuvoittaa hoitotyön tekemistä.

Jos organisaation työn luonteen vuoksi työpajoja ei voida järjestää, niin siinä tapauksessa kannattaa käyttää yksilökohtaisia haastatteluja. On tärkeää saada kaikissa tarvittavissa rooleissa työskentelevät haastateltua, vaikkakin sitten yksittäisinä haastatteluina.

Seuraavana vaiheena tarkastellaan eri toimintojen kriittisyyttä kunkin hoitoyksikön toiminnan kannalta. Mitkä ovat sellaisia toimintoja, jotka eivät saisi pysähtyä lainkaan? Mitkä ovat mahdollisesti toimintoja, joiden pysähtyminen joksikin aikaa ei olennaisesti haittaa hoitoyksikön päivittäistä toimintaa. Kriittisyyden arviointi aikayksikössä on keskeistä työn onnistumiselle.

Toimintojen kriittisyyden tarkastelussa havaitaan varsin nopeasti, mitkä tietojärjestelmät tai lääkinnälliset laitteet ovat oleellisia toiminnan jatkuvuudelle. Tietojärjestelmien kriittisyyden tarkastelu kannattaa ensin tehdä myös itsenäisesti koko organisaatiotasolla ilman riippuvuutta yksikkötasoon. Sen jälkeen voidaan muodostaa matriisi, jolloin yhdistetään tietojärjestelmien kriittisyystasot eri yksiköistä.

Tällä menetellyllä saadaan koko sairaalan toiminnan kannalta kokonaiskuva siitä, mitkä sairaalan toiminnot, palvelut, resurssit ja tietojärjestelmät ovat sellaisia, joiden jatkuvuudesta tulee erityisesti huolehtia. Samalla saadaan käsitys organisaation toiminta- ja jatkuvuudenhallintakyvystä.

Työn tulosten tuottaminen ja raportointi. Kolmantena päävaiheena on työn tulosten kerääminen ja tuottaminen sellaiseen muotoon, että työn tuloksia voidaan esittää kaikille tietoja tarvitseville tahoille. Työn tulosten verifiointi kannattaa tehdä moniammatillisella tiimillä, jossa on mukana tietoturva-asiantuntija ja kliinisen yksikön edustajat. Työn tuloksista muodostetaan konkreettinen toimenpidelista jatkotyölle. Työn tulosten esittämistä varten kannattaa järjestää tulostyöpaja, jossa myös johto on edustettuna.

5.3.2 Menetelmistä

Kriittisyysluokittelutyön menetelminä pilottihankkeissa käytettiin:

- ennakkokyselyä
- roolikohtaisia haastatteluja
- työpajatyöskentelyä

Työn menetelmien valintaa kannattaa pohtia huolella, koska projektista ei saa tulla liian raskas. Aiemmin kerättyjä tietoja tulee hyödyntää niin paljon kuin mahdollista. Samalla on syytä luoda sellainen menetelmä, jota voi käyttää jatkossakin kriittisyyden arvioinnissa. Ennakkokyselyjen hyöty on kaksivaikutteinen: osallistujat saadaan orientoitumaan tehtävään työhön ja lisäksi työpajoihin käytetty aika saadaan minimoitua. Roolikohtaiset haastattelut ovat tärkeitä, koska kriittisyys-

luokittelu muodostuu eri tehtävissä työskentelevien näkemyksistä. Työpajatyöskentelyjen hyöty on siinä, että niissä kohtaavat organisaation eri asiantuntijat ja saadaan aikaan moniammatillista keskustelua kriittisyydestä. Työpajat on syytä pitää kuitenkin hyvin organisoituina ja ajallisesti 1-1,5 tunnin mittaisena, koska pidemmäksi aikaa useiden asiantuntijoiden osallistuminen yhtä aikaa on hankalaa.

5.4 Mitä resursseja tarvitaan?

Työpajatyöskentelyyn tarvittavat resurssit vaihtelevat yksikkökohtaisesti. Tarvittavia resursseja voivat olla:

- Johdon edustus
- Lääkärityön edustaja(t)
- Hoitotyön edustaja(t)
- Muut kliinisen yksikön edustajat (esim. ajanvaraus ja sihteeri)
- ICT-ammattilainen
- Tietoturva-ammattilainen
- Projektipäällikkö

5.5 Ennakkotehtävät

Ennakkotehtävät kannattaa luoda verkkokyselyksi niin, että tietojen kerääminen koko organisaatiotasolta luonnistuu mahdollisimman helposti. Kyselyyn kannattaa kiinnittää huomioita, jotta saadaan vastauksia jatkotyön kannalta oleellisiin kysymyksiin. Sen lisäksi kannattaa luoda sopiva tietojen analysointimenetelmä, jotta kerättyjen tietojen vertailu koko terveydenhuoltoyksikön tasolla onnistuu helposti.

5.6 Toiminnan jatkuva kehittäminen

Kyberturvallisuustyö on jatkuvaa toiminnan kehittämistä. Sen vuoksi on merkityksellistä luoda toimintamalli, jonka avulla jatkuva kehittäminen aidosti onnistuu. Toimivia muutosjohtamisen malleja on useita, joita ei tässä dokumentissa esitellä tarkemmin. Pilotoinnissa saatujen kokemusten perusteella yksikössä kannattaa olla vastuullinen henkilö tai henkilöt, jonka vastuulla jatkuva kehittäminen on. Toiminnan kehittämisen syklinä voi olla esimerkiksi vuosittainen tarkastelu tai sitten joka kerta, kun ympäristöön tehdään muutoksia. Muutosdokumentaation avulla tietojärjestelmään ja toimintoihin liittyvät muutokset ovat ajan tasalla myös kirjallisessa muodossa, jolloin niiden tarkasteluun ei jatkossa kulu liikaa aikaa. KyberTerveys-hankkeen havaintona oli se, että prosessikuvausten päivittäminen helpottaa oleellisesti asioista keskustelemista.

5.7 Kriittisyysluokittelutyön hyödyt

Tietoturvallisen toimintaympäristön keskiössä on riskienhallinta ja riskienhallinnan keskiössä on kriittisyysluokittelu. Toiminnan ja toimintaympäristön kriittisyyden

ymmärtäminen on siis keskeistä toiminnalle. Se luo perustaa myös kriisiviestinnälle. Hyötyjä voidaan kuvata seuraavasti:

- Kriittisten pisteiden tunnistaminen ja kriittisyysluokittelu on osa toiminnan jatkuvuuden suunnittelua ja riskienhallintaa.
- Yhteisen tilannekuvan muodostaminen ja kriisiviestinnän kehittäminen lisää toimintavarmuutta.
- Kriittisyysluokittelu ja jatkuvuuden suunnittelu antaa vankan pohjan myös budjettikeskusteluille ydintoiminnan mahdollistamiseksi.
- Tärkein hyöty on kuitenkin potilasturvallisuuden varmistaminen, toiminnan turvaaminen ja negatiivisten vaikutusten minimointi.

6 YHTEENVETO

Nykyaikainen sote-ympäristö on erittäin tekninen ja verkottunut kokonaisuus, joka on altis toiminnan häiriöille. Jotta erilaisiin riskeihin voidaan varautua, on organisaation tunnettava hyvin toimintansa – sen keskeiset palvelut ja alipalvelut sekä niitä tukevat tekniset resurssit. Lisäksi näistä palveluista ja resursseista on kyettävä erottamaan toiminnan kannalta kriittiset ja vähemmän kriittiset. Kompleksisessa toimintaympäristössä pääsee helposti syntymään toimintamalleja, jotka perustuvat epävirallisiin tai vailla tukea oleviin prosesseihin tai teknisiin välineisiin. Toisaalta tuetut ja hyväksytyt ratkaisut voivat päätyä käyttöön, johon niitä ei ole alun perin tarkoitettu.

Avain tällaisen kompleksisen toimintaympäristön hallintaan on kokonaisuuden tunteminen. Eräs keino päästä toivottuun tilanteeseen on toiminnan kriittisyysluokittelu. Sairaalan tai sen yksikön toiminnan pilkkominen pienempiin kokonaisuuksiin auttaa tunnistamaan kyseisen yksikön palveluiden tuottamisen keskeiset komponentit ja niiden riippuvuussuhteet. Kriittisyysluokittelu auttaa tunnistamaan ne toiminnot, joiden jatkuvuus on turvattava kaikissa tilanteissa sekä ne tietojärjestelmät ja muut välineet, jotka on oltava käytettävissä aina. Tämä kokonaisymmärrys luo perustan käsitykselle tarvittavista riskienhallintakeinoista – varahenkilöjärjestelyistä, tietojärjestelmäsopimusten palvelutasoista, erilaisista teknisistä järjestelyistä sekä tietoturvallisuuden kehittämistoimenpiteistä.

Kriittisyysluokittelutyö ei palvele ainoastaan tietoturvavastaavia, tietohallintoa tai teknisiä palveluita, vaan oman yksikön toiminnan tarkastelu on oppimismatka myös kyseisen yksikön johtajille ja asiantuntijoille. Paremman jatkuvuuden hallinnan lisäksi kriittisyysluokittelu auttaa kehittämään yksikön toimintaa sekä löytämään piileviä tehottomia toimintatapoja. Työ vaatii tiivistä yhteistyötä tietoturvayksikön, ICT-yksikön ja tarkasteltavan yksikön kesken. Organisaation johdon tuki on ehdoton edellytys kriittisyysluokittelutyön onnistumiselle.

7 LÄHTEET

Kyberturvallisuuskeskus. 2018. Kyberturvallisuuden sanasto. Viitattu 22.12.2021. https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Kyberturvallisuuskeskus. 2020. Kybermittari. Kybermittarin esittely, käyttöohjeet ja kybermittarin erikieliset versiot. Viitattu 22.12.2021. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari.

STM. 2019. Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019:14. Viitattu 22.12.2021. https://julkaisut.valtioneuvosto.fi/handle/10024/161683.

THL. 2011. Potilasturvallisuusopas. Potilasturvallisuuslainsäädännön ja -strategian toimeenpanon tueksi. Terveyden ja hyvinvoinnin laitos. Tampere: https://thl.fi/documents/10531/104871/Opas%202011%2015.pdf.

VAHTI. 2016. Toiminnan jatkuvuuden hallinta. Valtion tieto- ja kyberturvallisuuden johtoryhmä. Valtiovarainministeriö. Viitattu 22.12.2021. https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229.