Kyberturvallisuus

Ohje sosiaali- ja terveydenhuollon toimijoille

SOSIAALI- JA TERVEYSMINISTERIÖN JULKAISUJA 2019:14

Sosiaali- ja terveysministeriön julkaisuja 2019:14

Kyberturvallisuus

Ohje sosiaali- ja terveydenhuollon toimijoille

Sosiaali- ja terveysministeriö, Helsinki 2019

Sosiaali- ja terveysministeriö

ISBN PDF: 978-952-00-4085-7

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2019

Kuvailulehti

Julkaisija	Sosiaali- ja terveysministeriö		23.5.2019
Tekijät	Sari Vuorinen (toimittaja)		
Julkaisun nimi	Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille		
Julkaisusarjan nimi ja numero	Sosiaali- ja terveysministeriön julkaisuja 2019:14		
Diaari/hankenumero	5500H-VAL.0603	**Teema**	
ISBN PDF	978-952-00-4085-7	**ISSN PDF**	1797-9854
URN-osoite	http://urn.fi/URN:ISBN:978-952-00-4085-7		
Sivumäärä	62	**Kieli**	suomi
Asiasanat	sosiaali- ja terveydenhuolto, kyberturvallisuus, yhteiskunnan elintärkeät toiminnot, valmius, kokonaisturvallisuus, valmiussuunnittelu, varautuminen		

Tiivistelmä

Kyberturvallisuus on osa sosiaali- ja terveydenhuollon palveluiden valmiutta ja varautumista.

Ohjeen tarkoitus on antaa yleiskuva toimialaa koskevista kyberturvallisuuden periaatteista sekä olemassa olevista ohjeista ja suosituksista. Ohje perustuu Suomen kyberturvallisuusstrategian toimeenpano-ohjelmaan ja sillä tuetaan osaltaan yhteiskunnan elintärkeiden toimintojen varmistamista häiriötilanteissa.

Ohje ei esitä yksityiskohtaisia tai teknisiä toimenpiteitä kyberuhkan tunnistamiseen tai torjuntaan, vaan niitä varten toimijat saavat ohjausta muun muassa Kyberturvallisuuskeskukselta. Lisäksi esimerkiksi Terveyden ja hyvinvoinnin laitos on tuottanut määrittelyjä, määräyksiä ja koulutusmateriaalia toimialan tiedonhallintaan.

Ohje on tarkoitettu yleisohjeeksi sosiaali- ja terveydenhuollon toimijoille erilaisissa organisaatioissa ja se on valmisteltu sosiaali- ja terveysministeriön ja Kuntaliiton yhteisessä hankkeessa.

Tämän ohjeen ensimmäinen versio julkaistaan sosiaali- ja terveysministeriön julkaisusarjassa ja sitä tullaan päivittämään tarpeiden mukaan. Liitteinä on taustoittavaa ja syventävää tietoa.

Kustantaja	Sosiaali- ja terveysministeriö
Julkaisun jakaja/ myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Social- och hälsovårdsministeriet		23.5.2019
Författare	Sari Vuorinen (redaktör)		
Publikationens titel	Cybersäkerhet Anvisning för aktörerna inom social- och hälsovården		
Publikationsseriens namn och nummer	Social- och hälsovårdsministeriets publikationer 2019:14		
Diarie-/ projektnummer	5500H-VAL.0603	**Tema**	
ISBN PDF	978-952-00-4085-7	**ISSN PDF**	1797-9854
URN-adress	http://urn.fi/URN:ISBN:978-952-00-4085-7		
Sidantal	62	**Språk**	finska
Nyckelord	social- och hälsovård, cybersäkerhet samhällets vitala funktioner, övergripande säkerhet, beredskapsplanering, beredskap		

Referat

Cybersäkerheten är en del av beredskapen inom social- och hälsovårdstjänsterna.

Syftet med anvisningen är att ge en allmän bild av principerna för cybersäkerhet som gäller ansvarsområdet samt förefintliga anvisningar och rekommendationer. Anvisningen baserar sig på verkställighetsprogrammet för Finlands cybersäkerhetsstrategi och den stöder för sin del säkerställandet av samhällets vitala funktioner i störningssituationer.

Anvisningen presenterar inte detaljerade eller tekniska åtgärder för identifiering eller bekämpning av cyberhot, utan för detta får aktörerna handledning från bland annat Cybersäkerhetscentret. Dessutom har till exempel Institutet för hälsa och välfärd producerat definitioner, bestämmelser och utbildningsmaterial för informationshanteringen inom ansvarsområdet.

Anvisningen är avsedd som en allmän anvisning för aktörerna inom social- och hälsovården i olika organisationer och den har beretts i ett projekt som är gemensamt för social-och hälsovårdsministeriet och Kommunförbundet.

Den första versionen av denna anvisning kommer att publiceras i social- och hälsovårdsministeriets publikationsserie och den kommer att uppdateras enligt behov. Som bilagor finns information som ger bakgrunden och fördjupande information.

Förläggare	Social- och hälsovårdsministeriet
Distribution/ beställningar	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Social Affairs and Health		23rd May 2019
Authors	Sari Vuorinen (Editor)		
Title of publication	Cyber security Guidance for operators in the healthcare and social welfare sectors		
Series and publication number	Publications of the Ministry of Social Affairs and Health 2019:14		
Register number	5500H-VAL.0603	**Subject**	
ISBN PDF	978-952-00-4085-7	**ISSN (PDF)**	1797-9854
Website address (URN)	http://urn.fi/URN:ISBN:978-952-00-4085-7		
Pages	62	**Language**	Finnish
Keywords	social welfare and health care, cyber security, vital functions of society, readiness, comprehensive security, contingency planning, preparedness		

Abstract

Cyber security is part of preparedness and contingency planning in social welfare and healthcare services.

The purpose of the guidance document is to provide a general overview of the cyber security principles applicable to the sector and to introduce existing guidelines and recommendations. The guidance document is based on the implementation programme of Finland's Cyber Security Strategy, and it helps to secure the vital functions of society in abnormal conditions.

It does not provide detailed or technical measures for identifying or combating cyber threats; guidance for these is provided by agencies such as the National Cyber Security Centre. In addition, the National Institute for Health and Welfare has produced specifications, orders and training material for the sector's information management purposes.

The guidance document is intended as a general guideline for social welfare and health care operators in various organisations, and it has been jointly prepared by the Ministry of Social Affairs and Health and the Association of Finnish Local and Regional Authorities.

The first version of this document is published in a publication series of the Ministry of Social Affairs and Health, and it will be updated as and when necessary. More detailed background information is provided in the appended documents.

Publisher	Ministry of Social Affairs and Health
Distributed by/ publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Sisältö

LUKIJALLE

Suomalaisen varautumisen yhteistoimintamallia kutsutaan kokonaisturvallisuudeksi, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä. Sosiaali- ja terveydenhuollolla on tässä varautumisessa erittäin merkittävä rooli. Erilaisissa häiriötilanteissa muodostuu käytännössä aina tehtäviä sosiaalihuollolle, terveydenhuollolle ja ympäristöterveydenhuollolle.

Kokonaisturvallisuuden malli edellyttää, että toimialan valmius perustuu yhtenäisiin riskinarvioihin ja suunnitteluun. Näin varmistetaan kyky toimia erilaisissa häiriötilanteissa kansallisesti, alueellisesti ja paikallisesti ja yhteistyössä muiden toimijoiden kanssa.

Kyberhäiriötilanteisiin varautuminen ja niiden hallinta ovat osa sosiaali- ja terveydenhuollon organisaatioiden jokapäiväistä toimintaa ja jatkuvuudenhallintaa.

Toivon, että tämä kyberturvallisuuden ohje antaa hyviä käytännön suosituksia ja keinoja tähän tärkeään työhön sosiaali- ja terveydenhuollon toimijoille.

Sosiaali- ja terveydenhuollon valmiussuunnittelun yhtenäistämiseksi ja tueksi julkaistaan myös muita tähän liittyviä ohjeita, kuten jatkuvuudenhallintaa (Kuja-malli) ja sopimusperusteista varautumista koskien.

Helsingissä toukokuu 2019

Kansliapäällikkö Päivi Sillanaukee

Suositukset

- Kyberhäiriötilanteisiin varautuminen ja niiden hallinta ovat osa sosiaali- ja terveydenhuollon organisaatioiden jokapäiväistä toimintaa (uhkien yleisyys).
- Kyberturvallisuus on huomioitava organisaation kaikessa resursoinnissa osana palvelutuotantoa. Tämä tulee huomioida myös järjestelmien ja palveluiden hankinnassa (johdon rooli).
- Sosiaali- ja terveydenhuollon organisaation tulee määrittää varautumisessaan organisaation kriittiset toiminnot, tuotetut palvelut ja niihin liittyvät kriittiset järjestelmät, kuten laitteet ja ohjelmistot, joiden toiminta tulee varmistaa kaikissa tilanteissa (kriittisten toimintojen määrittely).
- Turvallisuuteen ja häiriötilanteisiin varautuminen lisää väistämättä kustannuksia. Kriittisen toiminnan osalta kapasiteettia on varattava niin, että häiriötilanteista pystytään selviämään. Kriittiset järjestelmät on kyettävä ylläpitämään valmistajan ohjeiden mukaisesti ja tekemään tarvittavat ohjelmistopäivitykset normaalitoimintaa häiritsemättä (kriittisten toimintojen ylläpito).
- Tietoturva- ja tietosuojaosaaminen on tärkeä osa sosiaali- ja terveydenhuollon henkilöstön ammattitaitoa (jokaisen vastuu).
- Kaikkien työntekijöiden tulee tietää, miten toimitaan, kun tietojärjestelmät eivät ole normaalisti käytössä. Vaihtoehtoisia toimintatapoja tulee harjoitella. Henkilöstön tietoturvaan liittyvää osaamista on varmistettava säännöllisesti (koulutus ja harjoittelu).
- Yhteistyö eri toimijoiden kesken tulee etukäteen sopia ja harjoitella (häiriötilanteen hallintamalli).

Johdanto

Kyberturvallisuusohje sosiaali- ja terveydenhuollon toimijoille on valmisteltu osana sosiaali- ja terveysministeriön ja Suomen Kuntaliiton kehittämishanketta ”Valmius- ja jatkuvuudenhallinta sote-rakenteissa”. Ohjeistus perustuu Suomen kyberturvallisuusstrategian toimeenpano-ohjelmaan 2011– 2017.

Kyberturvallisuus on osa sosiaali- ja terveydenhuollon palveluiden varmistamista ja kuuluu kokonaisturvallisuuteen. Sosiaali- ja terveydenhuoltoon kohdistuu kyberuhkia päivittäin. Tällä ohjeella tuetaan osaltaan yhteiskunnan elintärkeiden toimintojen ylläpitämistä ja varmistamista normaalioloissa ja häiriötilanteissa.

Kyberturvallisuusohjeen tarkoitus on antaa yleiskuva sosiaali- ja terveydenhuoltoa koskevista kyberturvallisuuden periaatteista sekä olemassa olevista ohjeista ja suosituksista. Näitä tietoja tarvitaan sote-palveluiden ohjauksessa, hankinnassa ja tuottamisessa, joten kohderyhminä ovat sosiaali- ja terveydenhuollon hallinnon ja käytännön toimijat.

Ohjeen tarkoitus ei ole antaa yksityiskohtaisia teknisluonteisia ratkaisuja kyberturvallisuuden parantamiseksi, koska siihen on saatavilla muun muassa Kyberturvallisuuskeskuksen tuottamaa erillistä materiaalia. Kyberturvallisuudella sosiaali- ja terveydenhuollossa turvataan hoidon ja palvelun laadukkuutta ja tehokkuutta. Tietoturvallisuus ja tietosuoja liittyvät kiinteästi tähän kokonaisuuteen, joten ohjeessa käsitellään myös tietoturvaan ja tietosuojaan liittyviä kysymyksiä.

Kyberturvallisuusohjeen työryhmässä ovat olleet edustettuina keskeisimmät kyberturvallisuuden asiantuntijat. Työryhmään kuuluivat: Lasse Ilkka, puheenjohtaja (sosiaali- ja terveysministeriö), Perttu Halonen (Traficom, Kyberturvallisuuskeskus), Jani Jussila (Suomen Kuntaliitto), Maritta Korhonen (Kela), Tuija Kuusisto (valtiovarainministeriö), Andrei Laurén (Terveyden ja hyvinvoinnin laitos), Kalle Luukkainen (Huoltovarmuuskeskus), Jaakko Pentti (SoteDigi Oy), Maarit Puhto (sosiaali- ja terveysministeriö), Jussi Rapeli (Varsinais-Suomen sairaanhoitopiiri), Jarkko Reittu (Terveyden ja hyvinvoinnin laitos), Kimmo Rousku (Väestörekisterikeskus), Jenni Siermala (Pohjois-Pohjanmaan sairaanhoitopiiri, SoteDigi Oy

3.1.2019 alkaen), Veijo Terho (ICT-palvelukeskus Vimana Oy), Teemupekka Virtanen (sosiaali- ja terveysministeriö) ja Sari Vuorinen, sihteeri (Suomen Kuntaliitto).

Ohjeen valmistelussa on ollut yhteistyötä myös muiden asiantuntijoiden, kuten esimerkiksi Huoltovarmuuskeskuksen Kyberterveys-hankkeen kanssa. Kiitos kaikille valmisteluun osallistuneille.

Kyberturvallisuusohje julkaistaan vain sähköisessä muodossa ja sitä tullaan päivittämään osana kansallisen valmiussuunnittelun ohjausta.

Sosiaali- ja terveydenhuollon toimintaympäristö

Sosiaali- ja terveydenhuollon ammattilaiset käyttävät digitaalisia palveluita työssään päivittäin. Palveluiden toteutuksessa tukeudutaan merkittävästi tieto- ja viestintäteknologiaan, kuten mobiiliteknologiaan, pilvipalveluihin, tekoälytoimintaan, IoT (Internet of things) ja ICMT[1] (Information, Communication and Medical Technology) -teknologiaan. Teknologian nopea kehitys lisää haasteita tuottaa palveluita tietoturvallisesti ja vaatimusten mukaisesti. Tietojärjestelmiin liittyvät häiriötilanteet ovat viime vuosina myös nousseet julkisuuteen aiempaa herkemmin, esimerkiksi Onnettomuustutkintakeskuksen tutkinta Helsingin ja Uudenmaan sairaanhoitopiirin tietojärjestelmien vakavista häiriöistä 7.-8.11.2017[2].

Suomi on kuulunut maailmanlaajuisesti digitalisaation hyödyntämisen edelläkävijöihin. Tietoja kerätään paljon, mutta niiden kansallinen yhdistäminen ja hyödyntäminen vaativat kehitystyötä. Toimialan ammattilaisilla tulee olla jokapäiväisessä asiakas- ja potilastyössä tarvittavat tiedot saatavilla digitaalisesti. Myös kansalaisilla on enenevästi pääsy omiin terveys- ja hyvinvointitietoihin. Niiden avulla kansalainen voi arvioida oman hyvinvointinsa tilaa sekä saada tietoa hänen tarpeitaan vastaavista palveluista ja miten hän voi itse edistää oman elämäntilanteensa paranemista.

Sosiaali- ja terveydenhuollossa tulee kiinnittää erityistä huomiota asiakas- ja henkilötietojen käsittelyyn tietojen arkaluonteisuuden vuoksi. Tietojen luottamuksellisuutta on suojattava yksityisyyden takaamiseksi. Tähän velvoittaa lainsäädäntö, mutta kyse on myös terveydenhuollon maineesta ja uskottavuudesta arkaluontoisten terveystietojen käsittelijänä.

1 ICMT = Information, Communication and Medical Technology. Termiä käytetään, kun viitataan sekä tietotekniikkaan että lääkintälaitteisiin.

2 https://www.turvallisuustutkinta.fi/fi/index/ajankohtaista/tiedotteet/2019/01/turvallisuustutkintahelsinginjauudenmaansairaanhoitopiirintietojarjestelmienvakavistahairioista7.-8.11.2017valmis-terveydenhuollontietojarjestelmattuleepitaakunnossa.html

Tietojen arkaluonteisuuteen liittyvän salassapidon lisäksi turvallisuudessa korostuvat tietojen eheys ja saatavuus. Potilaan hoito ja asiakkaan palvelu perustuvat tietoihin, joiden on oltava oikeita ja yhdistettävissä oikeaan potilaaseen. Tietojen täytyy olla käytettävissä juuri silloin, kun niitä tarvitaan.

Sosiaali- ja terveydenhuollon palveluita tuotetaan aiempaa enemmän myös potilaiden ja asiakkaiden kotiympäristöissä. Tietojärjestelmien käytöllä sosiaali- ja terveydenhuollossa tavoitellaan viime kädessä potilaiden ja asiakkaiden hyvää: hoidon ja palvelun laatua ja tehokkuutta. Kyberturvallisuudella lisätään tiedonkäsittelyn luottamuksellisuutta.

Teknisesti palveluiden käyttö vaatii myös kolmansien osapuolten digitaalisia palveluita, kuten sähköisiä tunnistuspalveluita.

Terveydenhuollon tietojärjestelmät

Terveydenhuollon kansallinen tietojärjestelmäarkkitehtuuri koostuu paikallisista, alueellisista ja kansallisista järjestelmistä. Paikalliset ja alueelliset järjestelmät toimivat varsinaisina operatiivisina järjestelminä, joita käytetään päivittäin. Kansalliset järjestelmät puolestaan huolehtivat tietojen varastoinnista ja jakelusta.

Tyypillinen paikallinen järjestelmä on potilastietojärjestelmä (PTJ), jonka avulla ammattilainen hallitsee potilaan tietoja ja omaa päivittäistä työtänsä. Keskeisiä kansallisia järjestelmiä ovat esimerkiksi kansallinen potilastiedon arkisto (Kanta) ja koodistopalvelu. Kanta-palvelut on tarkoitettu palvelemaan sekä sosiaali- ja terveydenhuollon ammattilaisia että kansalaisia. Kanta-palveluihin kuuluvat esimerkiksi potilastiedon arkisto, sähköinen lääkemääräys ja potilaan mahdollisuus katsoa omia terveystietojaan netin kautta (Omakanta).

Terveydenhuollossa potilaan tietojen käyttö edellyttää hoitavalta henkilöltä hoitosuhdetta potilaaseen. Hoitavalla ammattihenkilöllä on oikeus saada nähtäväkseen potilaskertomus ja velvollisuus tallettaa siihen omat merkintänsä. Kukin hoitoon osallistuva henkilö saa nähdä ne tiedot, joita oma osallistuminen edellyttää. Tietojen luovutus rekisterinpitäjien välillä perustuu potilaan suostumuksiin ja kieltoihin. Potilas voi kieltää tietojensa näkymisen toisen rekisterin pitäjän osalta.

Terveydenhuollon palveluntuottajat ovat liittäneet potilastietojärjestelmänsä kansallisiin palveluihin. Tuolloin he käyttävät koodistopalvelusta ladattuja koodistoja sekä hakevat ja päivittävät potilastiedot Kanta-palveluun. Terveydenhuollossa potilaan tilannetta seurataan jatkuvalla potilaskertomuksella, joka muodostuu erillisistä potilasasiakirjoista.

Kansallinen arkkitehtuuri perustuu keskitettyyn talletuspaikkaan, johon kaikki paikalliset ja alueelliset potilastietojärjestelmät tallettavat keskeiset potilastiedot. Kanta-palvelun potilastiedot ovat saatavissa alueelliseen järjestelmään, jollei potilas ole tietojen luovutusta kieltänyt. Alueellisessa järjestelmässä oman rekisterinpitäjän alaiset potilastiedot ovat käytettävissä ilmankin yhteyttä Kanta-palveluun. Kanta-palveluihin liitettävien tietojärjestelmien on läpäistävä sertifiointiprosessi, jonka osana on muun muassa tietoturvallisuuden auditointi.

Kansallisessa järjestelmässä tietoliikenneyhteyksien suojaukseen ja valvontaan on panostettu merkittävästi. Suurin osa järjestelmien välisestä tietoliikenteestä tapahtuu erillisissä verkoissa. Osa pienistä toimialan toimijoista käyttää palveluita julkisen verkon kautta, mikä altistaa erilaisille julkisen verkon häiriöille. Esimerkiksi Omakanta-palvelu toimii julkisten verkkojen kautta. Tämä palvelu ei ole yhteiskunnan kannalta kriittinen järjestelmä, mutta se on näkyvä ja hyökkäyksille altis järjestelmä. Lisäksi terveydenhuollon asiakkaat käsittelevät itseään koskevia tietoja omilla välineillään ja omissa ympäristöissään, jolloin arkaluontoisia tietoja saattaa vuotaa julkisuuteen asiakkaiden omien toimenpiteiden kautta.

Tähän järjestelmäkokonaisuuteen kohdistuneet kyberhyökkäykset ovat tapahtuneet yleensä joko julkisen verkon puolella tai paikallisissa järjestelmissä, jolloin ne eivät ole merkittävästi vaikuttaneet kansallisiin palveluihin. Ulkopuolisilla hyökkäyksillä on muun muassa häiritty Omakanta-palvelun toimintaa ja julkisen verkon kautta yhteyksiä käyttävien palvelunantajien toimintaa. Hyökkäykset itsessään ovat olleet tyypillisiä palvelunestohyökkäyksiä joko suoraan Kanta-palveluita vastaan tai verkon kriittisiä palveluita, kuten Väestörekisterikeskuksen palveluja vastaan.

Sairaalaympäristön erityispiirteitä

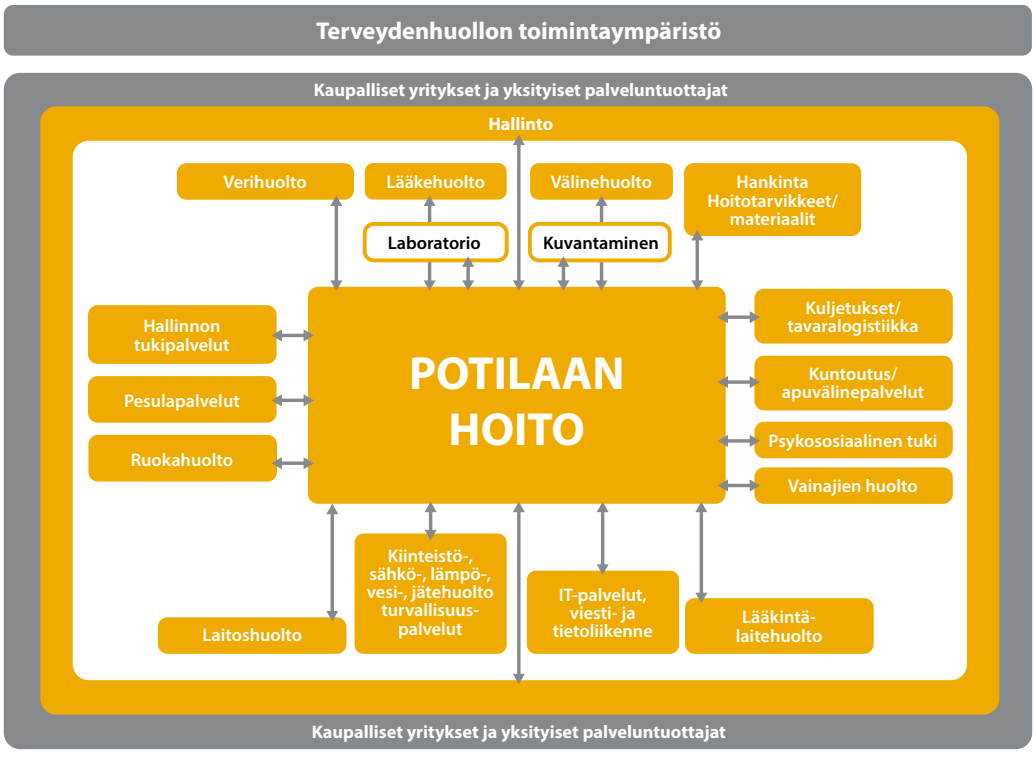
Terveydenhuollon tietojärjestelmien käytön yksi keskeinen toimintaympäristö on sairaala. Esineiden internetin käyttö (IoT, Internet of Things) on lisääntynyt merkittävästi terveydenhuollossa.

Sairaaloissa lääkinnälliset laitteet ovat yhä enenevissä määrin kytkeytyneinä internetiin, sairaaloiden tietoverkkoihin ja toisiin laitteisiin, mikä osaltaan lisää tietoturvariskejä. Nämä ovat teknologian kehittymisen ja myös ihmisten käyttötottumusten myötä yleistyneet ja arkipäiväistyneet. Lisähaasteena on se, että lääkinnällisten laitteiden hyväksyntäkriteereissä ei ole vielä riittävästi huomioitu kyberturvallisuusvaatimuksia.

Internetiin tai toisiin laitteisiin kytkeytyneet laitteet voivat tuoda uusia ja tehokkaampia hoitomenetelmiä sairaalaympäristöihin, terveydenhuollon eri toimijoille ja kotihoitoon. Kun sairaaloista kehitetään yhä älykkäämpiä, niiden toiminta ei enää rajaudu vain sairaalaympäristön sisälle. Kokonaisuudessa tulee huomioida kaikki erilaiset toimintaympäristöt, joissa laitteita, sovelluksia ja osa-alueita saatetaan käyttää.

Sairaala tarvitsee toimiakseen ison joukon tukipalveluita. Potilaan hoitoon liittyy suoraan tai välillisesti iso määrä muita toimintoja ja tukipalveluja. Hoidon jatkuvuus edellyttää, että tukipalvelut toimivat häiriötilanteissa. Sairaalan kyberympäristöön kuuluu myös tavanomaista toimistotietotekniikkaa. Esimerkiksi sairaalan maksuliikenteen häiriöt vaikuttavat sairaala-/terveyskeskusmaksujen laskutukseen potilailta, henkilökunnan palkkojen maksuun sekä lääke- ja hoitotarvikkeiden ostolaskujen maksuun toimittajille.

Alla olevassa kuvassa kuvataan tyypillistä terveydenhuollon toimintaympäristöä, jossa keskiössä on potilaan hoito ja siihen olennaisesti liittyvät laboratorio- ja kuvantamispalvelut.



Kuvio 1. Terveydenhuollon toimintaympäristö (Lähde: Terveydenhuoltopooli)

Terveydenhuollossa tulee huomioida potilastiedon lisäksi muita kyberturvallisuuteen liittyviä asioita. Tällaisia älysairaalan[3] osa-alueita ovat esimerkiksi:

- Etähoidon järjestelmät, joiden avulla voidaan joko seurata potilaan tilaa tai jopa tehdä hoitoon liittyviä toimenpiteitä, kuten lääkeannostelua.
- Verkottuneet lääkintälaitteet, jotka voivat olla kannettavia päätelaitteita, puettavaa teknologiaa tai esimerkiksi avustavia robotteja.
- Potilaiden tunnistamiseen käytettävät järjestelmät, kuten erilaiset älyrannekkeet tai biometriset skannerit.
- Verkkolaitteet, joiden avulla edellä mainittuja etälaitteita voidaan kytkeä sairaaloiden järjestelmiin.
- Mobiilipäätelaitteet, ja niissä olevat sovellukset, joiden avulla tarvittava tieto kulkee hoitohenkilökunnan mukana.
- Varsinaiset kliinisen hoidon tietojärjestelmät, joissa potilastietoa tallennetaan ja käsitellään.
- Itse tietosisältö, joka voi olla niin kliinistä potilastietoa kuin tutkimustietoa, henkilöstöön liittyvää tietoa tai sairaalan toimintaan liittyvää tietoa.
- Sairaalarakennusten kiinteistöautomaatio, joka tukee älysairaalan toimintaa, kuten automaattiovet ja älylukitukset, älykkäät LVIS-järjestelmät ja hoitohuoneiden automatiikkaan liittyvät järjestelmät tai instrumenttien steriloinnissa käytettävän höyryn tuotto.

Sosiaalihuollon tietojärjestelmät

Sosiaalihuollon kyberympäristö muodostuu tavallisen toimistotietotekniikan lisäksi pääasiassa sosiaalihuollon asiakastietojen käsittelyyn käytettävistä tietojärjestelmistä sekä niiden välisistä liityntärajapinnoista ja tietoverkoista. Käsiteltävä tieto voi olla tavanomaista henkilötietoa tai arkaluonteista sosiaalihuollon palveluihin liittyvää asiakastietoa, jonka suojaamiseen tulee kiinnittää erityistä huomiota. Lisäksi asiakastietojärjestelmään tehdään viranomaispäätöksiä, maksusuorituksia sekä maksusitoumuksia palveluntuottajille. Sosiaalihuollon ympäristöön liittyy kiinteistöjä koskevat järjestelmät, kuten valvonta- ja päällekarkausjärjestelmät.

Sosiaalihuollossa on aloitettu asiakastietojen valtakunnallisten tietojärjestelmäpalvelujen ja kansallisen asiakastietovarannon käyttöönotto. Sosiaalihuollon asiakastiedon arkisto on valtakunnallinen tietojärjestelmä, joka mahdollistaa keskitetyn sähköisen sosiaalihuollon

3 EU:n verkko- ja tietoturvaviraston (ENISA) 2016 julkaisu älysairaaloiden kyberuhkista https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

asiakastietojen arkistoinnin sekä tietojen aktiivisen käytön ja pysyvän säilyttämisen. Palvelun voivat ottaa käyttöön sosiaalihuollon palvelunantajat, jotka säilyttävät asiakasasiakirjoja sähköisesti. Arkistoa käytetään sosiaalihuollon asiakastietoja käsittelevällä järjestelmällä ja sen käyttö edellyttää Kanta-palvelujen asiakkuutta. Kansa-hankkeessa kehitetään sosiaalihuollon palveluita vuosien 2016-2020 aikana, muun muassa sosiaalihuollon asiakastiedon arkisto osana Kanta-palveluita.

Sosiaalihuollon uhkat liittyvät tällä hetkellä enimmäkseen siihen, että asiakkaan tiedot päätyvät ulkopuolisten käsiin. Jos asiakastietojärjestelmät eivät toimi, sosiaalihuollon tulee varajärjestelmin taata heikoimmassa asemassa oleville ruoka ja majoitus sekä tarpeellinen huolenpito laitoksissa asuville (vammaiset, lastensuojelu, tuetun asumisen yksiköt, vanhukset, mielenterveys- ja päihdeasiakkaat). Maksuliikenteen häiriöt vaikuttavat sosiaalihuollon asiakkaisiin. Häiriöt voivat vaikeuttaa sosiaaliturvan maksatuksia ja siten heikentää ihmisten toimeentuloturvaa. Kyse voi olla myös esimerkiksi pyrkimyksestä saada taloudellista etua. Tietojärjestelmissä olevia tai sinne kerättäviä tietoja saatetaan pyrkiä muuttamaan hakijalle edulliseksi, maksatustietoja voidaan yrittää muuttaa rahan ohjaamiseksi eri tahoille tai voidaan pyrkiä luomaan asiattomia maksatuksia.

Sosiaalihuollon palveluita tuotetaan aiempaa enemmän myös potilaiden ja asiakkaiden kotiympäristöissä. Häiriötilanteissa tulee turvata palvelut kotona palveluiden varassa asuville. Kyberturvallisuudella sosiaalihuollossa tavoitellaan potilaille ja asiakkaille hyvää hoitoa sekä palvelun laadukkuutta ja tehokkuutta. Teknisesti palveluiden käyttö vaatii myös kolmansien osapuolten digitaalisia palveluita, kuten sähköisiä tunnistuspalveluita.

Sosiaali- ja terveydenhuoltoon kohdistuvia kyberuhkia

Kyberrikolliset ovat erityisesti vuosina 2016-2018 suosineet tiedostoja salaavia kiristyshaittaohjelmia (crypto ransomware). Nämä haittaohjelmat pyrkivät uhrin tietokoneen saastutettuaan salaamaan koneen tiedostot. Rikolliset vaativat lunnaiden maksamista vastineeksi salauksen purkuavaimesta ja tiedostojen palauttamisesta. Kiristyshaittaohjelmista on tullut yksi kiusallisimmista kyberuhkista yksityishenkilöille, yrityksille ja muille organisaatioille. Maailmanlaajuisesti menetysten arvioidaan olevan satojen miljoonien dollarien luokkaa.

Organisaatioihin kohdistuneita kiristyshaittaohjelmatapauksia on aiemmin ollut lähinnä palvelualoilla, teollisuudessa sekä pankki- ja finanssimaailmassa. Sosiaali- ja terveydenhuollon sektorilla on viime vuosina ilmennyt muun muassa sairaaloihin kohdistuneita kiristyshaittaohjelmia. Niin sanottu WannaCry (tunnetaan myös nimillä wCry ja WanaCrypt0r) aiheutti laajaa ja vakavaa haittaa maailmanlaajuisesti useilla toimialoilla

toukokuussa 2017. Suomessa WannaCryn tiedetään löytyneen ainakin Turun yliopistollisessa keskussairaalassa kuvantamiseen liittyvistä tietokoneista. Suomea huomattavasti rajumpia vaikutuksia sattui Ison-Britannian National Health Service -järjestelmälle, koska sen tietoverkkojen segmentointi oli vähäistä ja päivittämättömiä tietokoneita paljon. Britanniassa jouduttiin jopa käännyttämään potilaita pois sairaaloiden ovelta.

Virtuaalivaluuttoja louhivat haittaohjelmat kuormittavat kaapatun tietokoneen resursseja, ja siten esimerkiksi sairaalaympäristössä potilashoidon tai sosiaalihuollossa asiakastiedon kannalta tärkeät järjestelmät eivät välttämättä toimi oikein tai aiheuttavat hidasteita toimintoihin.

Sosiaali- ja terveydenhuollon organisaatioissa kohdataan henkilöstön sähköpostin kautta tulevia tietojenkalasteluyrityksiä. Huijauksen kohteille on lähetetty esimerkiksi sähköpostiviesti, jonka aiheena on "Ladattu asia kirja". Viestissä on linkki Microsoft SharePoint -kirjautumissivun näköiselle sivulle, joka sijaitsee kuitenkin aivan muualla kuin pitäisi. Uhrin syöttäessä kirjautumissivulle esimerkiksi Office365-tilin käyttäjätunnuksen ja salasanan, ne päätyvät huijarille, joka saa organisaation sähköpostitilin niiden avulla haltuunsa. Haltuun otettuja sähköpostitilejä voidaan käyttää muun muassa laskutuspetoksiin, identiteettihuijauksiin tai haitallisen materiaalin levittämiseen.

Lääkintälaitteisiin kohdistuvia uhkia ja haavoittuvuuksia

Erilaisten laitteiden valmistajien etäyhteydet valmistamiinsa laitteisiin voivat aiheuttaa haavoittuvuutta. Valmistajat saattavat valvoa ja säätää etäyhteyden avulla lääkinnällisiä laitteita, kuten esimerkiksi sädehoitolaitteistoja. Käytäntö parantaa laitteiden vikojen ennakointia ja nopeuttaa niiden korjausta. Toisaalta käytäntö vaatii terveydenhuollon toimijoita avaamaan yhteyksiä sisäverkkojensa ja internetin välille, minkä turvallinen toteuttaminen vaatii tarkkoja tietoja etäyhteyksien tekniikasta sekä huolellista toteutusta ja valvontaa. Valmistajat eivät aina pysty tai halua kertoa yksityiskohtia etäyhteyksistään. Etäyhteyden muodostaminen myös siirtää terveydenhuollon palveluntarjoajan sisäverkon ulkorajan valmistajan sisäverkon ulkorajalle. Tällöin terveydenhuollon palveluntarjoajan on varmistuttava muun muassa sopimuksin siitä, että valmistajan oma tietoturva on vähintään samalla tasolla. Standardinmukaisten IT-prosessien hyödyntämistä suositellaan käytettäväksi lääkintälaitteiden verkottamisessa (esimerkiksi ITIL). [4]

Useissa lääkinnällisissä laitteissa on ohjelmistoja. Ohjelmistoista paljastuu usein virheitä eli haavoittuvuuksia, joiden hyväksikäyttö voi vaarantaa laitteiden oikean käytön. Lääkinnällisten laitteiden on oltava sovellettavien standardien ja muiden virallisten vaatimusten

4 https://tutcris.tut.fi/portal/files/12912971/Jauhiainen_Varri_selvitys_elokuu2017.pdf

mukaisia. Ohjelmistojen päivitys ja muut lääkinnällisten laitteiden korjaavat toimenpiteet ovat valmistajan vastuulla. Kun lääkinnällisen laitteen ohjelmistoa korjataan, täytyy valmistajan varmistaa sen vaatimustenmukaisuus uudestaan. Tämä aiheuttaa hitautta tunnettujen haavoittuvuuksien korjaamiseen laitteiden ohjelmistoista. Korjaukset käytössä ja varastossa oleviin laitteisiin vaatii usein vaivannäköä sekä valmistajilta että käyttäjiltä.

Käytettävyydeltään kankeat ohjelmistot voivat houkutella hoitohenkilökunnan kiertämään tietoteknisiä suojausmekanismeja, esimerkiksi useampi henkilö käyttää tietojärjestelmiä yhden ja saman henkilön käyttäjätunnuksilla tai että oletussalasanoja ei vaihdeta.

Toimintaympäristöön liittyviä uhkia

Terveydenhuollon toimitilojen avoimuus vaikeuttaa niiden kybertoimintaympäristön fyysistä suojaamista. Hyökkääjää, joka pääsee käsiksi suojattaviin digitaalisiin laitteisiin ja infrastruktuuriin, on vaikea havaita ja torjua. Koti- ja etähoidon kybertoimintaympäristöjen suojaaminen ja hallinta eivät usein ole hoitavan organisaation käsissä.

Sosiaali- ja terveydenhuollon kotiin vietävien palveluiden lisääntyminen tuo uudenlaisia haasteita sektorin kyberturvallisuudelle. Tulevaisuuden kyberuhkina voidaan nähdä muun muassa:

- Murtautuminen tietoverkkoon kytkettyihin lääkintälaitteisiin, huomioiden erityisesti kotihoidossa käytettyjen laitteiden kytkeytyminen tietoverkkoon potilaiden kotona hyvin erilaisissa ympäristöissä.
- RFID-sirujen[5] (käytetään esimerkiksi kulkutunnisteissa) kopiointi.
- Palvelunestohyökkäykset pilvipohjaisiin järjestelmiin, kuten potilas- ja asiakastietojärjestelmät tai Kanta-palvelu.
- Ihmisten tekemät virheet niin järjestelmien konfiguroinnin kuin erityisesti hoitohenkilökunnan näkökulmasta, koska verkottuneet laitteet vaativat usein erityisosaamista niin teknisen käytön kuin tietoturvan huomioinnin näkökulmasta.
- Järjestelmähäiriöt laitteissa olevien ohjelmistojen ja laitteet verkkoon liittävien verkkolaitteiden ja muiden verkkokomponenttien näkökulmista.
- Toimitusketjun ongelmat, esimerkiksi pilvipalvelun tarjoajan tai laitevalmistajan taholta.

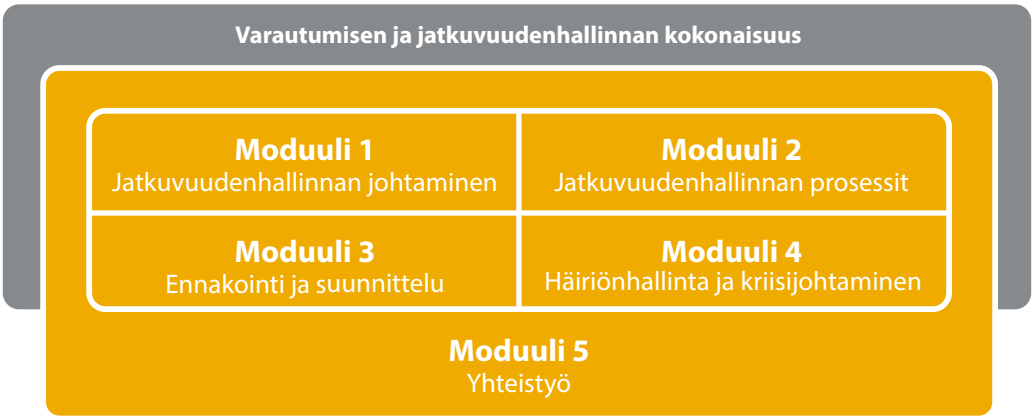
5 RFID= (radio frequency identification) radiotaajuinen etätunnistusmenetelmä

Varautuminen häiriötilanteisiin

Sosiaali- ja terveyspalveluiden varautuminen perustuu normaalioloissa tapahtuvaan laadukkaaseen toimintaan ja häiriötilanteiden ennakointiin. Organisaation kyky toimia ja tuottaa kriittiset palvelut myös häiriötilanteissa edellyttää johdon sitoutumista varautumisen ja toiminnan jatkuvuuden kehittämiseen sekä henkilöstön osallistamista ja osallistumista varautumisen toteuttamiseen.

Sosiaali- ja terveydenhuollon varautumisvelvoite perustuu muun muassa valmiuslakiin ja kyseistä toimintaa erityisesti koskeviin säädöksiin. Säädökset edellyttävät, että sosiaali- ja terveyspalveluita tuottavien organisaatioiden on valmiussuunnitelmin varauduttava häiriötilanteisiin ja poikkeusoloihin (esimerkiksi Valmiuslaki 1552/2011, 12§) . Organisaation valmiussuunnitelmaan kirjataan muun muassa eri toimijoiden vastuut ja roolit, häiriötilanteen hallinnan ja johtamisen järjestelyt sekä menettelyt häiriötilanteista toipumiselle.

Sosiaali- ja terveydenhuollon toimijoille julkaistaan ohjeistusta tukemaan valmiussuunnittelua ja jatkuvuudenhallintaa. Ohje[6] perustuu Suomen Kuntaliiton kehittämään Kuntien jatkuvuudenhallinta-konseptiin (KUJA) ja työkaluihin (muun muassa KUJA-arviointimalli)[7]. KUJA-mallin mukaista jatkuvuudenhallinnan kokonaisuutta kuvataan kuviossa 2.



Kuvio 2. Varautumisen ja jatkuvuudenhallinnan kokonaisuus (Lähde: KUJA-projekti, Suomen Kuntaliitto)

Keskeinen varautumistoimenpide on kriittisten toimintojen, palvelujen ja järjestelmien, kuten laitteiden ja ohjelmistojen määrittely. Niiden toiminta tulee turvata kaikissa

6 Valmius- ja jatkuvuudenhallintasuunnitelma. Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriö 2019:10.

7 KUJA-konsepti ja työkalut: www.kuntaliitto.fi/kuja

tilanteissa. Lisäksi on tunnistettava kriittiset tukipalvelut ja toiminnot, jotta kriittiset tehtävät kyetään hoitamaan.

Häiriötilannejohtaminen perustuu organisaation päivittäiseen johtamiseen. Organisaation johdon tulee huolehtia ja varmistua esimerkiksi riittävästä varautumisen resursoinnista, seurannasta ja ohjauksesta. Jatkuvuudenhallinta ja varautuminen, samoin kuin tietoturvallisuus, tulisi olla kiinteä osa organisaation muuta toimintaa, prosesseja ja palveluita.

Pitkäkestoisiin tietojärjestelmähäiriöihin on varauduttava ja niistä selviytymisen keinoja on suunniteltava ja harjoiteltava. Tarvittaessa organisaatioiden on kyettävä toimimaan poikkeustilanteessa ilman tietojärjestelmiä. Kriittisimmiksi luokiteltujen tietojärjestelmien luotettavuudesta tulee huolehtia esimerkiksi toimivien kahdennusten, suunniteltujen tilapäisratkaisujen, varaosien, erityiskomponenttien ja aktiivisten valvonta- ja huoltotoimien avulla[8].

Riskienhallinta

Riskienhallinnan avulla varmistetaan, että organisaatio toimii häiriötilanteissa. Riskianalyysien tekoon ja riskienhallintaan löytyy erilaisia työkaluja.

Riskienhallinnan avulla tunnistetaan kriittiset riskit. On tunnistettava palveluiden ja järjestelmien merkitys organisaation toiminnalle sekä arvioitava uhkien (mukaan lukien tietoturva- ja kyberturvallisuusuhkat) vaikutus palveluiden ja järjestelmien toimintakykyyn. Riskien arviointi on otettavaksi osaksi organisaation suunniteltua vuosikellon mukaista toimintaa. Sen lisäksi, että johto on tietoinen mahdollisista riskeistä, se myös arvioi ja hyväksyy riskien pienentämiseksi suunnitellut toimenpiteet ja seuraa niiden toteutumista.

Organisaatiossa tulee olla selkeät toimintaperiaatteet turvallisuusselvitysmenettelyjen suhteen. Organisaatiolla on velvollisuus huolehtia tiedon luokittelusta (oman tai muun viranomaisen omistaman) ja asianmukaisesta käsittelystä muun muassa varmistamalla tietoon oikeutetun henkilön luotettavuus.[9] Tämän osoittaminen tapahtuu henkilöturvallisuusselvitysmenettelyllä. Turvallisuusselvitysmenettely tulee organisaatioissa ulottaa niihin virka- ja työsuhteessa oleviin henkilöihin, joilla voi olla pääsy suojattaviin tietoihin ja/tai tiloihin.

8 VAHTI-ohje 2/2016 http://urn.fi/URN:ISBN:978-952-251-779-1

9 Turvallisuusselvityslaki 726/2014, Eduskunta hyväksyi HE284/2018 uudeksi tiedonhallintalaiksi 19.3.2018. Ko. laki sisältää myös tiedon luokittelun.

Yhtenä esimerkkinä riskienhallinnan työkalusta on VAHTI-ohje, jossa esitellään ISO31000-standardin käyttöä.[10] Standardit muodostavat viitekehyksen ja rungon toiminnan pitkäjänteiseen kehittämiseen. Liitteeseen 5 on kerätty merkittäviä standardeja ja viitekehyksiä terveydenhuollon näkökulmasta. Standardeista Suomessa ovat hyvin tunnettuja standardit ISO/IEC 27000 (tietoturvallisuus), 9000 (laatu) sekä 30000 (riskienhallinta). Liitteessä 5 on myös listattu tietoturvallisuuden auditointityökaluja sekä sertifiointimalleja.

Hankinnat ja sopimukset

Sopimusperusteinen varautuminen on tärkeä osa kokonaisvarautumista. Oman toiminnan jatkuvuus ja palveluiden häiriöttömyys varmistetaan myös ulkoistetuissa palveluissa, kuten tukipalveluissa ja materiaalitoimituksissa. Tietoturva, tietosuoja ja jatkuvuudenhallinta sisällytetään muun muassa palvelusopimuksiin.

Tietoturva- ja tietosuojariskit otetaan huomioon jo vaatimusmäärittely- ja hankintavaiheessa. Nämä on hyvä huomioida jo sopimusehdoissa. Hankintojen tietoturvavaatimuksissa huomioidaan hankinnan kohteen koko elinkaari hankintavaiheesta aina käytöstä poistoon saakka. Tietojenkäsittely-ympäristön suojauksista ja niiden tarkoituksenmukaisesta toiminnasta huolehditaan niiden koko elinkaaren ajan (ylläpito, hallinta ja valvonta). Muutoin hankittava laite tai tietojärjestelmä voi tietoturvan näkökulmasta olla vanhentunut nopeasti käyttöönoton jälkeen.

Huoltovarmuuskeskuksen kyberturvallisuutta koskevissa hankkeissa kehitetään tietoturvavaatimuskantaa, joka pohjautuu yleisimpiin tietoturvastandardeihin (esim. ISO27001). Samat periaatteet sopivat osin sairaalan laitteisiin ja teollisuusautomaatioon, joissa molemmissa on käytössä automaatiojärjestelmiä. Erityisesti lääkintälaitteiden tietoturvavaatimuksissa on havaittu kehittämisen tarvetta.

Tulevassa VAHTI100 -ohjeistuskokonaisuudessa avataan tiedonhallintalain tietoturvallisuuteen liittyvät kohdat yksityiskohtaisesti. Aiemmassa vastaavassa ohjeessa on mukana teknisen tietotekniikkaympäristön vaatimusten kuvauksia ja kilpailuttamiseen ja hankintoihin liittyviä työvälineitä.[11]

Tietoturvavaatimusten huomiointi hankinnoissa tarkoittaa käytännössä usein hankintoihin liittyvien prosessien kehittämistä. Jotta tietoturvavaatimukset saadaan sovitettua kuhunkin hankintaan oikealla tavalla, tulee organisaatiossa arvioida hankinnan vaatimuksia

10 VAHTI, Ohje riskienhallintaan, Valtiovarainministeriön julkaisuja 22/2017 http://urn.fi/URN:ISBN:978-952-251-862-0

11 Vahti 3/2012 Teknisen ympäristön tietoturvataso-ohje, https://www.vahtiohje.fi/web/guest/3/2012-teknisen-ymparistön-tietoturvataso-ohje Vahti100 -ohjeistus on valmisteilla.

riittävän aikaisessa vaiheessa. Tämä tarkoittaa kaikkien tarpeellisten osapuolten huomioimista hankintaprosessin eri vaiheissa, muun muassa hankintavaatimusten läpikäyntiä lääkintätekniikan, tietohallinnon ja tietosuojasta vastaavien osapuolten kanssa. Vaatimukset tulee varmistaa hankinnoissa sekä sopimuksissa.

Koulutus ja harjoittelu

Koulutuksen tavoitteena on, että jokainen työntekijä hallitsee organisaation tietoturva- ja tietosuojaperiaatteet ja osaa soveltaa niitä työssään. Tietoturva- ja tietosuojaosaaminen on osa ammattitaidon ylläpitoa ja täydennyskoulutusta. Perehdyttäminen tietoturvaan ja tietosuojaan alkaa jo työsuhteen alussa ja jatkuu koko työuran ajan. Organisaatioiden on pidettävä huolta työntekijöidensä tietoturva- ja tietosuojaosaamisen tunnistamisesta ja aktiivisesta kannustamisesta täydennyskoulutukseen.

Osana koulutusta järjestetään riskeihin, uhka-arvioihin, haavoittuvuuksiin ja tunnistettuihin kehittämiskohteisiin perustuvia harjoituksia. Harjoituksiin tulee osallistua myös tahoja, joilla on todellisissa häiriötilanteissakin keskeinen rooli. Näin varmistetaan, että harjoituksen tulokset jalkautuvat tehokkaasti käytännön toimintaan.

Kyberhäiriötilanteet voivat olla osa laajempaa vaikuttamista yhteiskunnan toimintoihin (hybridivaikuttamista). Siksi häiriötilanteissa tilannekuvan välittäminen suunnitelmien mukaisesti muille yhteistyötahoille ja omaa organisaatiota laajemmalle verkostolle on erittäin tärkeää.

Toimintamalli häiriötilanteessa

Kuviossa 3 on esitetty kyberhäiriötilanteiden toimintamallia yleisellä tasolla huomioiden paikallista, alueellista ja valtionhallinnon tason toimintaa. Kuvion malli perustuu terveydenhuollossa toimivaan viiden erityisvastuualueen malliin, joka on osoittautunut toimivaksi muun muassa Huoltovarmuuskeskuksen Kyberterveys-hankkeessa. Kyseessä on yleiskuvaus, jossa ei kuvata tarkasti organisaatioiden rakenteita tai vastuita. Jotta paikallista tasoa laajemmissa häiriöissä voidaan luoda tilannekuvaa ja tukea toimijoita tehokkaasti, tietoa tulee kerätä ja jakaa riittävän suurilla toiminta-alueilla. Muun muassa Huoltovarmuuskeskuksen hankkeissa tällaiseksi rakenteeksi terveydenhuollon osalta on luontaisesti muodostunut viiden erityisvastuualueen malli. Valtioneuvoston tasolla kyberhäiriötilanteissa oleellinen toimija on muun muassa Kyberturvallisuuskeskus. Ministeriöt tuottavat tilannekuvaa Valtioneuvoston tilannekeskukselle. Häiriötilannemallia tulee edelleen kehittää ja testata harjoituksissa.

Häiriötilanteen tunnistaminen ja reagointi

Kyberturvallisuuden häiriön käsittely alkaa siitä, kun joku huomaa poikkeaman kybertoimintaympäristössä. Käsittelyn alkuvaiheet ovat usein samanlaiset riippumatta organisaation perustehtävästä ja roolista. Poikkeama voi olla esimerkiksi:

- häiriö ICT-palveluissa
- ICT-palveluiden toimivuutta uhkaava tilanne kuten sähkökatko
- salassa pidettävän digitaalisessa muodossa olevan tiedon paljastuminen sivullisille

Keskeistä on arvioida häiriön tyyppi ja sen mahdollinen uhka organisaation toiminnalle, potilas- ja asiakasturvallisuudelle tai tietosuojalle tai yksityisyyden suojalle. Häiriö voi liittyä esimerkiksi potilastietojärjestelmään, lääkintälaitteen toimintaan tai tietojen siirtoon. Arvion perusteella on päätettävä, edellyttääkö häiriö välittömiä toimenpiteitä.

Häiriötilanteen toimintamallin kaaviossa häiriöilmoituksen vastaanoton esitetään tapahtuvaksi sote-palveluntuottajaorganisaatiossa, mutta toiminta on samanlaista muissakin organisaatioissa, jotka havaitsevat tai epäilevät kyberhäiriötä.[12]

Tietojärjestelmän ylläpitäjän tulee saada viivytyksettä tieto epäillystä tai havaitusta häiriöstä. Toimistoympäristön kyberhäiriöissä ilmoituspiste on tyypillisesti tietohallinnon tukipiste (helpdesk-toiminta). Lääkinnällisten laitteiden ollessa kyseessä ilmoituspiste voi olla organisaation ilmoittama vastuuhenkilö. Myös etähallittujen lääkinnällisten laitteiden, kuten kuvantamislaitteiden valmistajille, voi olla syytä ilmoittaa häiriöstä välittömästi.

Häiriön saattaa havaita tietojärjestelmän omistavan organisaation oma henkilökunta, asiakas, sopimuskumppani tai jokin ulkopuolinen taho. Tietojärjestelmän omistajalla ja ylläpitäjällä tulee olla useita kanavia häiriöilmoitusten käsittelyyn. Tietojärjestelmien käyttäjien tulee myös tietää, mille taholle häiriöstä tulee ilmoittaa. Tieto eri järjestelmien vastuutahoista kannattaa olla mahdollisessa tietohallinnon tukipisteessä.

Häiriötilanteen alussa ei usein ole tietoa siitä, onko häiriö syntynyt vahingossa vai tahallisesti. Tahallisen ja tahattoman häiriön käsittelyssä on kuitenkin joitakin merkittäviä eroja. Siksi tilannetta on arvioitava tilannekuvan täydentyessä toistuvasti uudelleen ja toimittava siten, että mahdolliselle kyberhyökkääjälle ei anneta harkitsemattomilla häiriönhallinnan toimenpiteillä etua.

12 Kaavion sote-palveluntuottajat-osassa kuvattu häiriönhallinnan prosessi vastaa VAHTI-ohjeessa Tietoturvapoikkeamatilanteiden hallinta esitettyä prosessia (Valtiovarainministeriön julkaisuja 8/2017, s. 15, Kuvio 2. Tietoturvapoikkeamien käsittelyprosessi). VAHTI-ohjeen termi tietoturvapoikkeama tarkoittaa samaa kuin tässä käytetty termi kyberhäiriö. http://urn.fi/URN:ISBN:%20978-952-251-930-6

Tietojärjestelmän omistaja arvioi tilanteen ja tekee tarvittaessa häiriöilmoituksen ("Alustava analysointi" -> "Onko kyberhäiriö?"). Jos tietojärjestelmän omistajan omassa henkilöstössä ei ole kykyä arvioida kyberhäiriötä, sen tulee sopia arvioinnin tekemisestä esimerkiksi järjestelmää ylläpitävän ICT-palveluntarjoajan kanssa.

Ensimmäinen häiriöilmoitus on harvoin niin yksityiskohtainen, että voitaisiin muodostaa luotettava tilannearvio pelkästään sen pohjalta. Häiriön ilmoittajalta kannattaa viivytyksettä kysyä lisää tietoja. Jos kyberhäiriön mahdollisuus voidaan luotettavasti sulkea pois, käsitellään tilanne normaalina tukipyyntönä ("Käsittely tukipalveluprosessien mukaisesti").

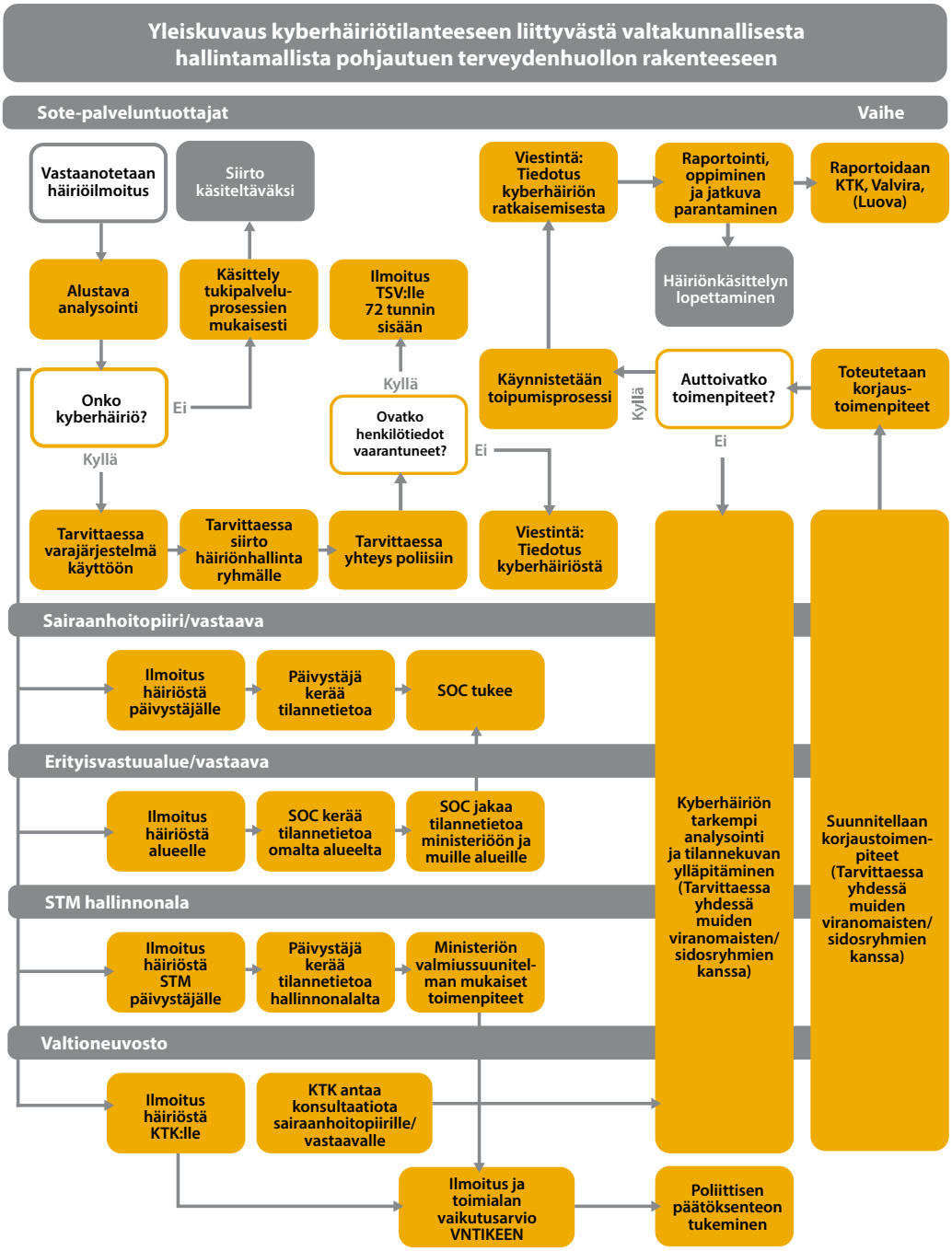
Kyberhäiriötilanteen hallinta

Jos ensiarvion perusteella häiriön epäillään olevan kyberhäiriö, on tietojärjestelmän omistajan käynnistettävä useita toimenpiteitä. Ensiksi on aloitettava vahinkojen rajoittaminen ja alustava toipuminen. Joissakin tilanteissa se voi tarkoittaa varajärjestelmän käyttöönottoa ("tarvittaessa varajärjestelmä käyttöön"). Usein tilanteen ensitietojen perusteella ei kyetä arvioimaan aiheuttaisiko esimerkiksi varajärjestelmän käyttöön siirtyminen enemmän haittaa potilaiden hoidolle ja asiakkaiden palvelemiselle kuin häiriön koetteleman järjestelmän käytön jatkaminen. Varajärjestelmän käyttöönottoa on harkittava uudestaan, kun tilannekuva täydentyy. On myös huomioitava mahdollinen vaikutus ja ilmoitusvelvollisuus Kanta-palveluihin.

Toiseksi järjestelmän omistajan pitää nostaa valmiutta käsitellä häiriötilannetta. Sen tulee harkita käsittelyn siirtoa kyberhäiriöiden käsittelyyn harjaantuneelle ryhmälle, joka voi koostua sen omasta henkilöstöstä tai jonka se on hankkinut sopimuskumppaniltaan ("Tarvittaessa siirto häiriönhallintaryhmälle").

Epäillystä rikoksesta kannattaa ilmoittaa poliisille ripeästi ("Tarvittaessa yhteys poliisiin"). Poliisi voi rikoksen torjumiseksi ja selvittämiseksi käyttää pakkokeinoja ja tiedonlähteitä, joiden käyttö ei muille viranomaisille ole mahdollista. Tietojärjestelmän omistajan on syytä laatia etukäteen ohje siitä, ketkä saavat tehdä sen nimissä rikosilmoituksen ja miten varmistetaan heidän tavoitettavuutensa myös vapaapäivinä ja loma-aikoina. ICT-palveluiden tuotantoon liittyvien kiireellisten päätösten teko kannattaa usein määrätä samojen henkilöiden tehtäväksi.

Kuviossa 3 on esitetty yleiskuvaus kyberhäiriötilanteen valtakunnallisesta hallintamallista pohjautuen terveydenhuollon rakenteeseen.



Kuvio 3. **Yleiskuvaus kyberhäiriötilanteeseen liittyvästä valtakunnallisesta hallintamallista pohjautuen terveydenhuollon rakenteeseen.**

Ilmoitus kyberhäiriötilanteesta valvontaviranomaisille

Kyberhäiriötilanteen ratkettua sosiaali- ja terveydenhuollon organisaation on varauduttava antamaan yksityiskohtainen selvitys aluehallintovirastolle häiriötilanteen

vaikutuksista potilasturvallisuuteen. Sosiaali- ja terveydenhuollon ammattihenkilöiden velvollisuutena on ilmoittaa terveydenhuollon laitteen tai tarvikkeen aiheuttamasta vaaratilanteesta myös valvovalle viranomaiselle (Valvira). Merkittävän kyberhäiriön hallinnan jälkitöihin kuuluu lisäksi EU:n verkko- ja tietoturvadirektiivin (nk. NIS-direktiivi) mukainen ilmoitus Valviralle.

Traficomin Kyberturvallisuuskeskukselle kannattaa tehdä vapaaehtoinen ilmoitus häiriöstä (kuviossa 3 "Ilmoitus poikkeamasta KTK:lle"), jotta se voi antaa neuvoja ja tukea poikkeamanhallinnassa (kuviossa 3 "KTK antaa konsultaatiota sairaanhoitopiirille tai vastaavalle"). Kyberturvallisuuskeskus pitää yllä valtakunnallista kyberturvallisuuden tilannekuvaa.

Tietojärjestelmän omistajan on aina arvioitava, onko häiriön yhteydessä tietosuoja vaarantunut ("Ovatko henkilötiedot vaarantuneet?"). Mikäli on tapahtunut henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys.

Kyberhäiriötilanteesta tiedottaminen

Riippumatta siitä, onko henkilötietojen suoja vaarantunut, tietojärjestelmän omistajan kannattaa tiedottaa tapahtuneesta niitä, joita häiriö koskee ("Viestintä: Tiedotus kyberhäiriöstä"). Yleiset kriisiviestintäohjeet sopivat myös kyberhäiriöistä tiedottamiseen.

Tietojärjestelmän omistajan on harkittava, onko tilanne niin vakava, että myös julkishallinnon ylempiä tasoja tai keskeisiä kumppaniorganisaatioita tulee informoida. Ilmoittamisen aiheista ja jaettavista tiedoista kannattaa keskustella sidosryhmien kanssa jo ennen kuin häiriöitä on tapahtunut.

Periaatteena on, että häiriöistä kannattaa mieluummin kertoa kuin jättää kertomatta. Julkisia sote-palveluita tuottavan organisaation tulee ilmoittaa omaa toimintaansa koskevista kyberhäiriöistä palveluiden tilaajille. Ylempiä hallintotasoja kiinnostaa ennen kaikkea häiriön syy, toipumissuunnitelma sekä ilmoittavan organisaation kyvykkyys suoriutua normaaleista tehtävistään. Kumppaniorganisaatiot ovat tyypillisesti kiinnostuneempia häiriön teknisistä yksityiskohdista, joiden avulla ne voivat arvioida omien suojaustensa riittävyyttä.

Tietoturvapoikkeaman tarkempi analysointi on käynnistettävä heti, kun siihen riittää henkilöitä välttämättömien ensitoimenpiteiden hoitamiselta ("Kyberhäiriön tarkempi analysointi ja tilannekuvan ylläpitäminen"). Tarkka analysointi edellyttää tarkistettujen faktojen

hankkimista siitä, mitä tapahtui, milloin, kenen tai minkä toimesta. Useimmiten tietokoneiden ja ICT-palveluiden lokitiedot ovat korvaamattoman arvokkaita. Myös etähallittujen lääkinnällisten laitteiden toimittajilla voi olla häiriön ymmärtämisen ja selvittämisen kannalta tärkeää metriikkadataa.

Analysointi edellyttää usein yhteistyötä sidosryhmien, kuten ICT-palveluntarjoajien, kanssa. Yhteistyöstä kannattaa sopia hyvissä ajoin: kenellä on oikeus pyytää mahdollisesti maksullista apua, minkälaisia tietoja saadaan jakaa, millä välineillä ja niin edelleen.

Analysoidun tilannetiedon perusteella tietojärjestelmän omistaja sidosryhmineen suunnittelee häiriön korjaamiseen tarvittavat toimenpiteet ("Suunnitellaan korjaustoimenpiteet"). Erityisesti jos häiriön aiheuttaja on päämäärätietoinen hyökkääjä, korjaustoimenpiteet (mukaan lukien tiedotus) tulee suunnitella niin, että hyökkääjän toiminta saadaan kerralla pysäytettyä. Korjaustoimenpiteisiin kuuluu myös todistusaineiston ja tapahtumalokien tallentaminen myöhempää käyttöä varten. Digitaalisen todistusaineiston tallentamiseen saa neuvoja poliisilta ja Kyberturvallisuuskeskukselta.

Korjaustoimenpiteistä on syytä tiedottaa järjestelmien ylläpitoon osallistuville henkilöstölle, johon toimenpiteet vaikuttavat. Tiedotteen sisältö voi olla yksinkertainen: ”nyt tehdään tällainen korjaus ja tunnin päästä tiedotamme, miten jatketaan”.

Tietojärjestelmän omistaja ja sen sidosryhmät toteuttavat korjaustoimenpiteet suunnitellusti ja koordinoidusti ("Toteutetaan korjaustoimenpiteet"). Korjaustoimenpiteiden vaikutusta tulee tarkkailla ("Auttoivatko toimenpiteet?"). Mikäli toimenpiteillä ei ollut riittävää vaikutusta, tulee kyberhäiriön analysointia ja korjausta jatkaa.

Kyberhäiriötilanteesta toipuminen ja oppiminen

Kun tietojärjestelmän omistaja on saanut akuutin häiriötilanteen hallintaan, tulee sen aloittaa toipuminen takaisin normaaliin toimintaan ("Käynnistetään toipumisprosessi"). Sekin kannattaa suunnitella ja varautua ennakkoon. Esimerkiksi jos poikkeaman aikana on ollut varajärjestelmä käytössä, pitää siihen kirjatut tiedot siirtää varsinaiseen järjestelmään osana toipumista. Sidosryhmille tiedottaminen poikkeamatilanteen loppumisesta on osa toipumista ("Viestintä: Tiedotus kyberhäiriön ratkaisemisesta").

Päivystävän henkilöstön tavoittaminen nopeasti ja varmasti on tärkeä osa terveydenhuollon palveluiden tuottamista. Yleisissä viestintäpalveluissa on joskus useiden tuntienkin pituisia toimivuushäiriöitä. Palvelunantajan tulee arvioida, miten pitkään se voi toimia ilman yleisiä viestintäpalveluita ja millä keinoilla se varautuu niiden häiriöihin. Usein käytettyjä varautumiskeinoja ovat:

- Varaliittymien hankkiminen useammalta eri teleyritykseltä
- Viranomaisradioverkon (VIRVE) käyttö matkapuhelinliittymien lisäksi
- Sairaalan sisäiset kuulutus- ja tiedotusjärjestelmät.

Häiriötilanteen jälkeen on järjestettävä tilaisuus, jossa käydään yhteisesti läpi tilanne ja sen vaikutukset sekä havaitut puutteet toiminnassa. Tilanteissa onnistuminen arvioidaan yhdessä häiriötilannetoiminnassa mukana olleiden työntekijöiden ja sidosryhmien kanssa. Vakavista vaaratilanteista ja häiriöistä tulee kerätä oleelliset tiedot ja jakaa kokemukset sekä johtopäätökset turvallisuuden ja toimintatapojen parantamiseksi kaikkien toimijoiden hyödyksi. Lisäksi määritellään, miten varmistutaan, että puutteet korjataan ja puutteiden korjaamista seurataan. Samalla olemassa olevat ohjeet ja suunnitelmat tarkastetaan ja korjataan.

Häiriötilanteet ovat arvokkaita tilaisuuksia oppia ja parantaa toimintaa ("Raportointi, oppiminen ja jatkuva parantaminen"). Poikkeamanhallintaa ei voida katsoa onnistuneesti päättyneeksi ennen kuin on tunnistettu onnistumisen kohdat, mahdolliset puutteet sekä toiminnan parannuskeinot. Tietosuojan ja tietoturvallisuuden omavalvontasuunnitelman ja omien valvonta- ja varautumistoimien dokumentointi on osa toipumis-, oppimis- ja kehittymisprosessia. Häiriötilanteista opitut asiat kannattaa jakaa Kyberturvallisuuskeskukselle, jolta saa palautetta ja joka voi raportoijan luvalla ja anonyymisti jakaa oppeja laajemmalle.

Sairaanhoitopiirien rooli kyberhäiriötilanteessa

Sairaanhoitopiirillä on oltava kyky ottaa vastaan ja käsitellä kyberhäiriöilmoituksia omia tietojärjestelmiään sekä sopimuksen perusteella sote-palveluita tuottavien organisaatioiden toimintaa koskien.

Sairaanhoitopiirin pitää arvioida kyberhäiriön vaikutus sen kykyyn suoriutua tehtävistään. Kyberhäiriöstä on ilmoitettava eteenpäin, jotta saadaan laajempi tilannekuva sekä alueellisesti että valtakunnallisesti. Usein kyberhäiriöt kohdistuvat samanaikaisesti useisiin organisaatioihin, jotka eivät ole saman sairaanhoitopiirin alueella tai edes saman erityisvastuualueen sisällä. Esitetyssä hallintamallissa kyberhäiriöistä on tehtävä ilmoitukset muille keskeisille viranomaisille edellä kuvatun hallintamallin mukaisesti. Erityisvastuualueella[13] pitää olla kyky ottaa vastaan ja arvioida kyberhäiriöilmoituksia omalta toiminta-alueelta ja muodostaa valtakunnallista tilannekuvaa yhdessä muiden alueiden ja Kyberturvallisuuskeskuksen kanssa.

13 Jotkut erikoissairaanhoidon palvelut järjestetään yli sairaanhoitopiirien rajojen yliopistosairaaloiden erityisvastuualueiden eli ns. miljoonapiirin pohjalta. Valtioneuvoston asetuksella 156/2017 säädetään, mitkä ovat erityisvastuualueita ja mitkä sairaanhoitopiirit kuuluvat kuhunkin erityisvastuualueeseen.

Sosiaali- ja terveysministeriön ja sen hallinnonalan laitosten rooli kyberhäiriötilanteessa

STM:n hallinnonalan laitokset ylläpitävät kykyä havainnoida ja reagoida kyberuhkiin samalla tavoin kuin toimialalla muutoinkin. Hallinnonalan laitokset ilmoittavat merkittävistä häiriöistä STM:lle ja Kyberturvallisuuskeskukselle. Valviralla on kyberhäiriöiden osalta lisäksi häiriöilmoitusten vastaanottajan rooli, kun kyseessä on lääkintälaitteisiin rinnastettavien potilastietojärjestelmien tai niiden osien häiriö.

STM:n valmiusyksikkö ylläpitää hallinnonalan häiriötilanteiden tilannejohtamisvalmiuksia sekä ministeriön jatkuvaa päivystysjärjestelmää. Poikkeavassa tilanteessa STM:n toimintaa johtaa aluksi valmiuspäivystäjä ja sen jälkeen toiminnan vastuuvirkamies, valmiuspäällikkö tai ministeriön johto. Poikkeuksellisessa tilanteessa ministeriön valmiusorganisaation tehtävä on ylläpitää valtakunnallista tilannekuvaa erityisesti huolehtien siitä, että STM:llä ja valtioneuvoston tilannekeskuksella on yhteinen tilannekuva. Lisäksi STM:n valmiusorganisaatio pitää yhteyttä tarpeen mukaan muiden ministeriöiden päivystäjiin, Valviraan, Kyberturvallisuuskeskukseen sekä toimialan toimijoihin. STM informoi hallinnon- ja toimialansa merkittävistä häiriöistä valtioneuvoston tilannekeskusta.

Kyberturvallisuuskeskuksen ja valtioneuvoston tilannekeskuksen rooli kyberhäiriössä

Kyberturvallisuuskeskus ottaa vastaan kaikkien toimijoiden ilmoituksia tietoturvaloukkauksista. Huoltovarmuuskriittisinä organisaatioina sairaanhoitopiirit saavat etuoikeutettua palvelua. Muita ilmoittajia Kyberturvallisuuskeskus palvelee heti, kun tilanne sen sallii.

Sairaanhoitopiirit voivat Kyberturvallisuuskeskuksen verkkolomakkeen kautta tehdä Valviralle EU:n verkko- ja tietojärjestelmien turvallisuutta koskevan direktiivin (NIS-direktiivi) edellyttämän ilmoituksen merkittävistä turvallisuuspoikkeamista. Halutessaan sairaanhoitopiiri voi antaa saman ilmoituksen tiedoksi Kyberturvallisuuskeskukselle. Kyberturvallisuuskeskus ei lähtökohtaisesti välitä sille ilmoitettuja tietoja muille niin, että muut voisivat tunnistaa ilmoituksen tekijän tai kyberhäiriön kohteen. Se ilmoittaa tiedot muille tahoille vain ilmoittajan luvalla tai jos häiriö uhkaa ihmisten terveyttä tai henkeä tai yhteiskunnan turvallisuutta.

Kyberturvallisuuskeskus neuvoo ilmoittajia tekemään ensitoimenpiteitä kyberhäiriön saamiseksi hallintaan. Saamiensa tietojen avulla Kyberturvallisuuskeskus pitää yllä kansallista kyberturvallisuuden tilannekuvaa. Se koordinoi häiriön hallinnassa tarvittavien organisaatioiden yhteistoimintaa varmistamalla häiriötä koskevan tiedon analysointia ja kulkemista toimijoiden välillä.

Kyberturvallisuuskeskuksella ei ole määräysvaltaa häiriöiden hallintaan muuten kuin yleisiä viestintäpalveluita tarjoavien teleyritysten osalta. Häiriön hallintaan osallistuvat tahot toimivat kukin oman toimivaltansa puitteissa.

Yhteiskunnan toimintoja merkittävästi häiritsevistä kybertapahtumista Kyberturvallisuuskeskus välittää tiedon valtioneuvoston tilannekeskukselle, joka käyttää tietoja oman tilannekuvansa täydentämiseen ja informoi tarvittaessa valtioneuvostoa. Tiedonkulku molempia reittejä hyödyntäen on tärkeää, jotta sekä sote-palvelutuotannon että digitaalisten järjestelmien jatkuvuusnäkökulmat tulevat huomioiduiksi.

Ohjeen ylläpito ja kehittäminen

Kyberturvallisuus on jatkuvasti ylläpidettävä ja kehitettävä prosessi, koska uhkatkin muuttavat muotoaan. Tätä ohjetta on tarkoitus käsitellä ja päivittää jatkuvana prosessina. Ohjeen ensimmäinen versio julkaistaan sosiaali- ja terveysministeriön julkaisusarjassa. Sosiaali- ja terveydenhuollon toimijat osallistuvat ohjeen päivitystyöhön.

Lähdeluettelo

Iyengar, A., Kundu, A., & Pallis, G. (2018). Healthcare Informatics and Privacy. IEEE Internet Computing, 22(2), 29-31.

Kansallinen riskiarvio 2018, Sisäinen turvallisuus. Sisäministeriön julkaisuja 2019:5. http://urn.fi/URN:ISBN:978-952-324-245-6

Kodin kyberopas – ohjeita digitaaliseen arkeen 2017, Turvallisuuskomitea. https://turvallisuuskomitea.fi/kodin-kyberopas-ohjeita-digitaaliseen-arkeen/

Kyber-terveys Uutiskirje 3/2018. 5.10.2018 – Hankintojen tietoturva. Huoltovarmuuskeskus

Kyberturvallisuuskeskuksen internet-sivut, Varoitus 3/2018 (päivitetty 7.1.2019). Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota! https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Miikael ja Martti Lehto 2017 (Jyväskylän yliopisto) Kyberturvallisuus sairaalajärjestelmissä, Osa 1. https://www.jyu.fi/it/fi/tutkimus/julkaisut/tekes-raportteja/kyberturvallisuus-sairaalassa_-14-8-17.pdf

Lääkärilehden verkkojulkaisu (8.6.2017). WannaCry-haittaohjelma löytyi TYKS:sta. https://www.laakarilehti.fi/ajassa/ajankohtaista/wannacry-haittaohjelma-loytyi-tyks-sta/

Onnettomuustutkintakeskus; Y2018-02 Helsingin ja Uudenmaan sairaanhoitopiirin tietojärjestelmähäiriöt 7.-8.2017. https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/OZnac1oRj/Y2018-02_HUS.pdf

Poliisin, CERT-FI:n ja F-Secure Pyj:n yhteinen sivusto verkkorikollisuuteen varautumisesta http://www.ransomware.fi/

Smart Hospitals – Security and Resilience for Smart Health Service and Infrastructures (2016). EU:n verkko- ja tietoturvaviraston (ENISA) julkaisu älysairaaloiden kyberuhkista. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals/at_download/fullReport

Sopimusperusteinen varautuminen. Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019:9.

Sosiaalihuollon valtakunnallisten tietojärjestelmäpalveluiden ja määrämuotoisen kirjaamisen toimeenpanohanke (Kansa-hanke). Hankesuunnitelma 2016–2020. Terveyden ja hyvinvoinnin laitos (THL). Ohjaus 10/2016. http://www.julkari.fi/bitstream/handle/10024/130563/URN_ISBN_978-952-302-660-5.pdf

Sosiaali- ja terveysministeriön hallinnonalan tietohallinnon linjaukset 2018-2022,

Sosiaali- ja terveysministeriön julkaisuja 11/2018. http://urn.fi/URN:ISBN:978-952-00-3949-3

Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitteiden saavuttamiseksi 2/2017, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. https://tietokayttoon.fi/julkaisu?pubid=17805

Suomen kyberturvallisuusstrategia ja toimeenpano-ohjelma 2017-2020. Turvallisuuskomitea. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

Terveydenhuoltoalan kyberuhkia (2016). Ohje 1/2016 Viestintävirasto, kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf

Tampereen Teknillisen Yliopiston tutkimus standardinmukaisten IT-prosessien hyödyntämistä lääkintälaitteiden verkottamisessa https://tutcris.tut.fi/portal/files/12912971/Jauhiainen_Varri_selvitys_elokuu2017.pdf

Valmius- ja jatkuvuudenhallintasuunnitelma. Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019:10.

Valtiovarainministeriön julkaisuja 8/2017 Tietoturvapoikkeamatilanteiden hallinta http://urn.fi/URN:ISBN:%20978-952-251-930-6

Valtiovarainministeriön julkaisuja 22/2017 Ohje riskienhallintaan http://urn.fi/URN:ISBN:978-952-251-862-0

Valtiovarainministeriön julkaisuja 2/2016, Toiminnan jatkuvuuden hallinta http://urn.fi/URN:ISBN:978-952-251-779-1

Valtiovarainministeriön julkaisuja 2/2012 ICT-varautumisen vaatimukset https://www.vahtiohje.fi/web/guest/2/2012-ict-varautumisen-vaatimukset

Valtiovarainministeriön julkaisuja 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta https://www.vahtiohje.fi/web/guest/2/2010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta

Viestintäviraston internet-sivut, Tietoturva nyt! (16.2.2018). WannaMine-haittaohjelma kierrättää vanhoja temppuja – ei aihetta erityiseen huoleen. http://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201802161123.html

Viestintävirasto Traficom, Kyberturvallisuuskeskus. Tietoturvan vuosi 2018. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan_vuosi_%2018_aukeamat.pdf

Vesihuoltolaitosten kyberturvallisuuteen uusia työkaluja kybervesi-hankkeesta, tiedote Huoltovarmuuskeskus 29.11.2018. https://www.huoltovarmuuskeskus.fi/vesihuoltolaitosten-kyberturvallisuuteen-uusia-tyokaluja-kyber-vesi-hankkeesta/

Von Solms, R., & Van Niekerk, J. (2013) From information security to cyber security Article in Computers & Security 38: 97-102.

Yhteiskunnan turvallisuusstrategia 2017, Valtioneuvoston periaatepäätös / 2.11.2017. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Liitteet

LIITE 1

Keskeisten kansallisten toimijoiden kuvaus

Aluehallintovirastot

Aluehallintovirastojen yleiset varautumistehtävät ovat:

- varautumisen yhteensovittaminen ja siihen liittyvä yhteistoiminnan järjestäminen, valmiussuunnittelun yhteensovittaminen,
- kuntien valmistussuunnittelun tukeminen,
- valmiusharjoitusten järjestäminen,
- alue- ja paikallishallinnon turvallisuussuunnittelun edistäminen,
- toimivaltaisten viranomaisten tukeminen niiden johtaessa turvallisuuteen liittyviä tilanteita alueellaan ja tarvittaessa niiden toiminnan yhteensovittaminen.

Aluehallintovirastoilla on valmius kerätä alueensa tilannekuvaa normaaliolojen laajoissa ja pitkäkestoisissa häiriötilanteissa.

Huoltovarmuuskeskus (HVK)

Huoltovarmuuskeskus on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta. Huoltovarmuuskeskuksen tehtäviin kuuluvat:

- julkishallinnon ja elinkeinoelämän yhteistoiminnan kehittäminen huoltovarmuusasioissa,
- huoltovarmuuden kannalta elintärkeiden teknisten järjestelmien toimivuuden varmistaminen,
- välttämättömän tavara- ja palvelutuotannon sekä sotilaallista maanpuolustusta tukevan tuotannon tukeminen,
- velvoite- ja turvavarastoinnin hoitaminen sekä
- valtion varmuusvarastoitavien materiaalien ylläpitäminen.

Kansaneläkelaitos (Kela)

Kela vastaa Kanta-palveluiden rakentamisesta, testauksesta ja ylläpidosta. Kela vastaa myös Kanta-palveluihin liittymisen teknisistä määrityksistä ja liittymisedellytysten

varmistamisesta. Lisäksi Kela toimii kansallisen Reseptikeskuksen rekisterinpitäjänä ja tietoteknisenä ylläpitäjänä.

Kanta-palveluihin liittyviltä tietojärjestelmiltä edellytetään sertifiointia, joka sisältää olennaisten vaatimusten toteuttamisen tietojärjestelmiin Terveyden ja hyvinvoinnin laitoksen määräysten mukaisesti. Lisäksi siihen kuuluu yhteistestausta Kanta-palvelun kanssa, tietoturvallisuuden arviointia niin sanotun hyväksytyn arviointilaitoksen kanssa sekä näiden tuloksena saatavaa vaatimustenmukaisuustodistusta.

Kyberturvallisuuskeskus (KTK)

Traficomin Kyberturvallisuuskeskuksen tehtävänä on seurata kyberturvallisuusuhkia ja koota kyberturvallisuutta koskevaa tietoa eri toimijoille. Merkittävistä kyberuhkista keskus varoittaa ja valistaa myös kansalaisia. Kyberturvallisuuskeskus toimii sekä julkisen että yksityisen sektorin kanssa. Kyberturvallisuuskeskus tarjoaa huoltovarmuuskriittisille organisaatioille, joihin monet sosiaali- ja terveydenhuollon organisaatiot kuuluvat, tehostettuja palveluita:

- etusija CERT-palveluissa,
- sote-alalle kohdennettua tiedon vaihtamista ja tilannearvioita ajankohtaisista kyberuhkista,
- sote-alan luottamuksellinen tiedonvaihtoryhmä (SOTE-ISAC), jonka jäsenorganisaatiot jakavat keskenään tietoa tapahtuneista turvallisuuspoikkeamista ja levittävät hyviä käytäntöjä muille alan toimijoille,
- neuvontapalvelu organisaation kyberturvallisuuden kehittämiseen sekä mahdollisuus vakavien tietoturvaloukkausten havainnointi- ja varoituspalveluun (HAVARO). Palvelu on tarkoitettu asiakasorganisaation muita tietoturvakontrolleita täydentäväksi toiminnoksi.

Neuvontapalvelulla Kyberturvallisuuskeskus tukee huoltovarmuuskriittisiä organisaatioita niiden arvioidessa kyberturvallisuutensa kehittämistarpeita. Kyberturvallisuuskeskus tekee myös kansainvälistä yhteistyötä terveydenhuoltoalan kyberturvallisuuden parissa. Se edustaa Suomea epävirallisessa terveydenhuoltoalan kyberturvallisuustoimijoiden Health CERTs -yhteisössä. Yhteisö vaihtaa tietoja terveydenhuoltoalan ajankohtaisista kyberuhkista ja alan kyberturvallisuuden kehittämisestä.

Yksityiset henkilöt, yritykset ja organisaatiot voivat ilmoittaa Kyberturvallisuuskeskukselle niihin kohdistuneista tietoturvaloukkauksista, kuten tietojen kalastelusta tai palvelunestohyökkäyksistä, sekä näiden loukkausten yrityksistä. Kyberturvallisuuskeskus tekee vakavuusarvion, jonka perusteella ryhdytään tarvittaessa lisätoimiin asian selvittämiseksi.

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira)

Valviralle kuuluu useita sosiaali- ja terveydenhuollon toimijoiden kyberturvallisuuteen liittyviä valvonta- ja toimeenpanotehtäviä.

Valvira esimerkiksi pitää yllä terveydenhuollon palvelin- ja ammattihenkilörekisteriä ja sen tietoihin perustuvaa rooli- ja attribuuttitietopalvelua. Rekisterin mukaan määräytyy muun muassa henkilöstön oikeus päästä Kanta-palveluiden tietoihin.

Terveydenhuollon laitteiden ja tarvikkeiden turvallisuuden valvonta kuuluu Valviralle.

Valvira valvoo sosiaali- ja terveydenhuollon tietojärjestelmien olennaisten vaatimusten toteutumista. Kokonaisuudessaan valvonta koskee kaikkia markkinoille jo saatettuja terveydenhuollon laitteita ja tarvikkeita sekä niiden ylläpitoa. Valmistajien ilmoitusvelvollisuuden lisäksi sosiaali- ja terveydenhuollon ammattihenkilöiden velvollisuutena on ilmoittaa terveydenhuollon laitteen tai tarvikkeen aiheuttamasta vaaratilanteesta valvovalle viranomaiselle.

Tehtäväkokonaisuus siirtyy 1.1.2020 alkaen Lääkealan turvallisuus- ja kehittämiskeskuksen (Fimea) tehtäväksi, kuitenkin niin, että asiakastietolain valvontatehtävät jäävät Valviralle. Siten esimerkiksi potilastietojärjestelmien vaaratilanneilmoitukset[14] selvitettäisiin Valvirassa.

Lisäksi Valviran tehtävänä on yhteistyössä Huoltovarmuuskeskuksen kanssa terveydenhuollon laitteiden ja tarvikkeiden huoltovarmuudesta kriittisten kohtien tunnistaminen ja toimenpide-ehdotusten tekeminen STM:lle.

Valviran kyberturvallisuuteen liittyvänä varautumistehtävänä on koota yhteistyössä STM:n kanssa tehtäviinsä liittyvää tilannekuvaa. Keskeinen tehtävä on myös ohjata ja tiedottaa aluehallintovirastoja.

Sosiaali- ja terveysministeriö (STM)

Sosiaali- ja terveysministeriö vastaa sosiaali- ja terveydenhuollon tiedonhallinnan strategisesta ohjauksesta, lainsäädännöstä sekä kansainvälisestä ja poikkihallinnollisesta yhteistyöstä. STM myös johtaa, valvoo ja yhteen sovittaa sosiaali- ja terveydenhuollon varautumista häiriötilanteisiin ja poikkeusoloihin. Tavoitteena on turvata väestön

14 https://www.valvira.fi/terveydenhuolto/terveysteknologia/valviralle-tehtavat-ilmoitukset/ilmoitus-vaaratilanteesta

toimeentuloturva ja toimintakyky kaikissa turvallisuustilanteissa. Ministeriössä valmiusasioista vastaa valmiusyksikkö. STM:n valmiusyksikkö ylläpitää hallinnonalan häiriötilanteiden tilannejohtamisvalmiuksia ja jatkuvaa päivystysjärjestelmää.

SoteDigi Oy

SoteDigi Oy on kehitysyhtiö, joka edistää sote-palveluiden digitalisaatiota ja yhteensovittamista Suomessa yhteistyössä sote-toimijoiden kanssa. SoteDigi Oy perustettiin maakunta- ja sote-uudistuksen valmisteluun liittyen.

SoteDigi keskittyy erityisesti

- toteuttamaan kansallisia sosiaali- ja terveydenhuollon uusia digitaalisia ratkaisuja, hankkeita ja hankintoja
- hillitsemään digitaalisilla ratkaisuilla sosiaali- ja terveydenhuollon menojen kasvua
- kehittämään teknologisen ympäristön, jossa asiakkaille on tarjolla parempia palveluita yhdenvertaisesti koko Suomessa.

Tietosuoja- ja tietoturvakysymykset ovat tärkeä osa sote-palveluiden digitalisaatiota, ja niihin kiinnitetään palveluiden kehitystyössä erityistä huomiota. Tietoturvatekninen testaus on keskeinen elementti SoteDigin järjestelmäkehitystyössä. Järjestelmien haavoittuvuudet pyritään löytämään jo ennen niiden pilotointi- ja käyttöönottovaihetta. Varautuminen häiriötilanteisiin ja jatkuvuudenhallinta suunnitellaan yhdessä IT-toimittajien ja palveluntarjoajan (Vimana Oy) kanssa siten, että mahdolliset tuotantokatkot ja niiden vaikutus voidaan kustannustehokkaalla tavalla minimoida.

Terveyden ja hyvinvoinnin laitos (THL)

Terveyden ja hyvinvoinnin laitoksella on ohjausrooli tiedonhallinnan kansallisessa kehittämisessä. THL muun muassa antaa määräyksiä järjestelmien vaatimuksien sisällöstä, merkittävistä poikkeamista ja niitä koskevista ilmoituksista, ja omavalvontasuunnitelmasta.

THL vastaa sosiaali- ja terveydenhuollon tietohallinnon operatiivisesta ohjauksesta. THL ohjaa sosiaali- ja terveydenhuollon palvelujen tuottajia ja apteekkeja palveluihin liittymisessä sekä tietojärjestelmien kehittämisessä. THL toimii yhteistyössä laajan yhteistyöverkoston kanssa. Lisäksi tilastoviranomaisena THL vastaa tilasto- ja rekisteritietovarantojen sekä kansallisten luokitusten ylläpidosta ja kehitystyöstä.

Valtioneuvoston tilannekeskus (VN TIKE)

Valtioneuvoston tilannekeskus kokoaa valtioneuvostolle tilannekuvaa turvallisuustapahtumista mukaan lukien kyberhäiriöistä. Tilannekeskuksesta säädetään sitä koskevalla lainsäädännöllä.

Valtiovarainministeriö (VM)

Valtiovarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä.

Lähtökohtina ovat jokaisen organisaation vastuu oman toimintansa tietoturvallisuudesta, säädöksissä määritellyt tietoturvavelvoitteet, valtioneuvoston periaatepäätös valtion tietoturvallisuuden kehittämisestä, Suomen kyberturvallisuusstrategia sekä VM:n antamat VAHTI-tietoturvaohjeet ja muut linjaukset.

Vimana Oy

Maakuntien ICT-palvelukeskus Vimana Oy perustettiin yhteisten ja kustannustehokkaiden ICT-palveluiden kehittämiseksi ja digitalisaation edistämiseksi.

Väestörekisterikeskus (VRK)

Väestörekisterikeskus on valtion virasto, joka toimii valtiovarainministeriön asettaman julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) toiminnasta vastaavana operatiivisena toimijana. VRK kehittää yhteistyössä Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kanssa julkiseen hallintoon suunnattavia tieto- ja kyberturvallisuuspalveluita. Väestörekisterikeskus tuottaa lisäksi maksullisia digitaalisen turvallisuuden asiantuntijapalveluita julkisen hallinnon asiakkaille.

Hankkeita

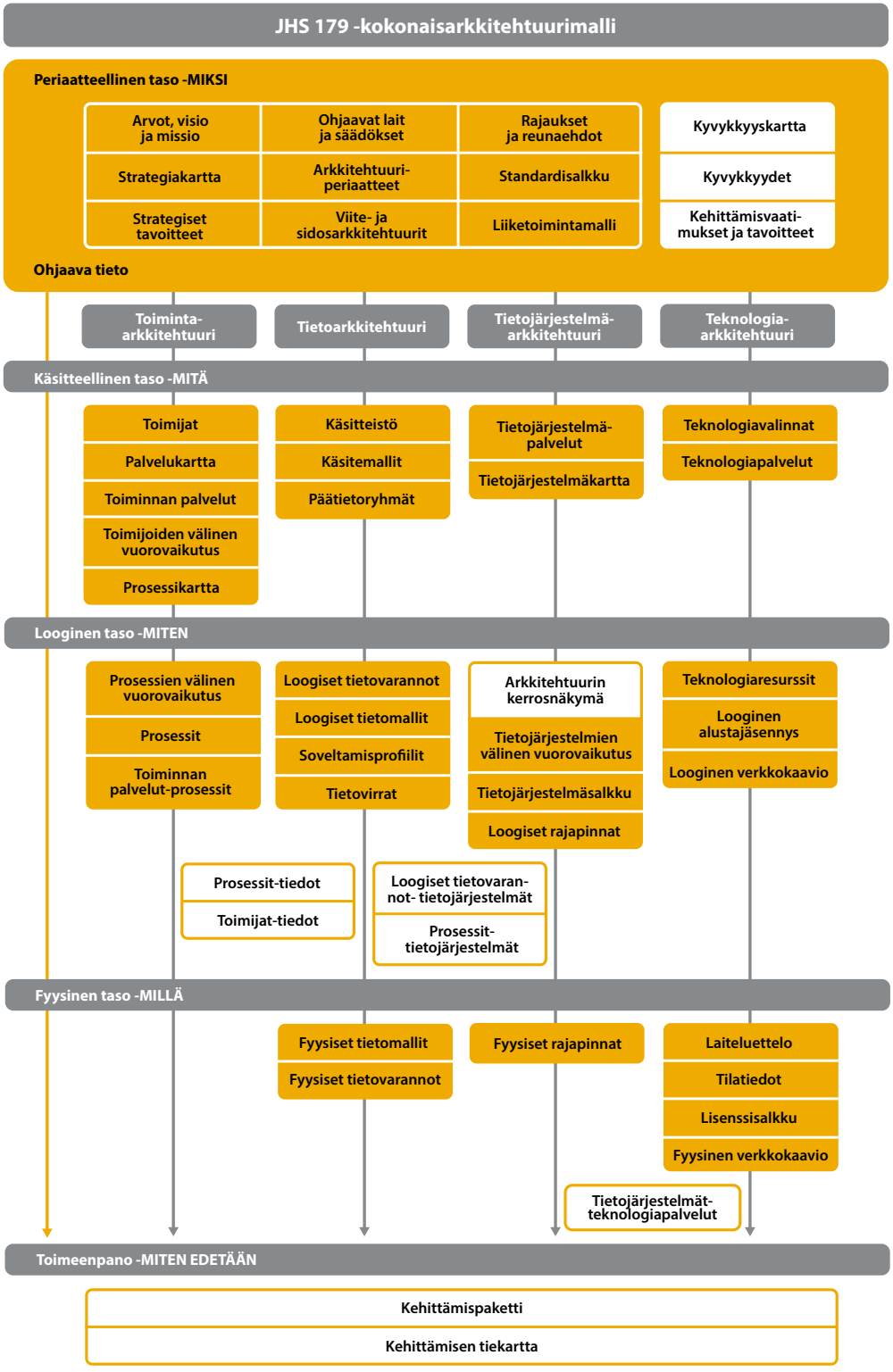
AKUSTI-foorumi

AKUSTI-foorumi on sosiaali- ja terveydenhuollon valtakunnallinen tietohallintoyhteistyöverkosto, jota operoidaan hallinnollisesti Suomen Kuntaliitossa toimivan sihteeristön kautta. Toiminnan rahoittavat sosiaali- ja terveysministeriö, yliopistolliset sairaanhoitopiirit ja kunnat.

Sosiaali- ja terveyspalveluiden toiminnan ja rakenteiden kehittäminen edellyttää kuntien ja sairaanhoitopiirien välistä sekä niiden ja valtionhallinnon toimijoiden välistä yhteistyötä sähköisen tiedonhallinnan ratkaisujen kehittämisessä. AKUSTI-foorumi osallistuu aktiivisesti valtakunnallisen tietohallintoyhteistyön suunnitteluun ja toimeenpanoon. AKUSTIn keskeisiin tehtäviin kuuluu edistää sosiaali- ja terveydenhuollon kokonaisarkkitehtuuritoimintaa (SOTE KA) sosiaali- ja terveysministeriötä tukevassa roolissa. Foorumin toiminnan tavoitteena on muun muassa varmistaa sosiaali- ja terveydenhuollon toimialalla jo tehdyn ICT-kehittämistyön tulosten tehokas hyödyntäminen.

JHS 179

Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) on luonut JHS 179 -kokonais-arkkitehtuurimallin.



Kuvio 4. **Arkkitehtuuri kuvausten viitekehys, JHS 179 (mukailtu)**

JHS-järjestelmän mukaiset suositukset koskevat valtion- ja kunnallishallinnon tietohallintoa. Sisällöltään JHS voi olla julkishallinnossa käytettäväksi tarkoitettu yhtenäinen menettelytapa, määrittely tai ohje. JHS-järjestelmän tavoitteena on parantaa tietojärjestelmien ja niiden tietojen yhteentoimivuutta, luoda edellytykset hallinto- ja sektorirajoista riippumattomalle toimintojen kehittämiselle sekä tehostaa olemassa olevan tiedon hyödyntämistä.

Kyberterveys-hanke

Kyberterveys-hanke on osa Huoltovarmuuskeskuksen Kyber 2020 -ohjelmaa, jonka viitekehyksenä toimii kansallinen kyberturvallisuusstrategia. Huoltovarmuuskeskuksen osin rahoittamaan hankkeeseen osallistuu useita sairaanhoitopiirejä, niiden ICT-palveluntarjoajia sekä Kyberturvallisuuskeskus. Hanke käynnistyi syksyllä 2017 ja jatkuu syyskuuhun 2019 asti. Pääosan hankkeen tuloksista tekevät siihen sitoutuneet sairaanhoitopiirit ja niiden ICT-palveluntarjoajat.

Hankkeen tavoitteena on luoda ja levittää terveydenhuoltoon kyberturvallisuuden toimintatapoja ja käytäntöjä, joilla kehitetään huoltovarmuuskriittisten organisaatioiden kyberturvallisuutta. Keskeisimpänä tavoitteena on kehittää sairaanhoitopiirien varautumista kyberturvallisuusuhkiin erityisesti potilashoitoon liittyvien kriittisten toimintojen osalta.

Kolme pääteemaa ovat kyberturvallisuutta koskeva koulutus alan henkilöstölle, tietotekninen tietoturvapoikkeamien havainnointi- ja reagointikyky sekä kyberturvallisuusvaatimusten huomioiminen laitteiden ja palveluiden hankinnoissa. Kehitystyössä ovat mukana muun muassa kaikki yliopistolliset sairaanhoitopiirit ja tuloksia jaetaan hankkeen edetessä kaikille sairaanhoitopiireille. Hankkeen tuloksia jaetaan ja niitä voi kysyä muun muassa Kyberturvallisuuskeskuksen sote-alan tiedonvaihtoryhmän (SOTE-ISAC) kautta.

VAHTI

Valtiovarainministeriö on asettanut VAHTIn (julkisen hallinnon digitaalisen turvallisuuden johtoryhmä) toimimaan julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. VAHTIn asema on kirjattu voimassa oleviin valtioneuvoston periaatepäätöksiin Suomen kyberturvallisuusstrategiasta 2013 ja valtionhallinnon tietoturvallisuuden kehittämisestä 2009. Lisäksi VAHTIlla on keskeinen rooli kyberturvallisuusstrategian toimeenpano-ohjelman toteuttamisessa.

VAHTI edistää myös 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.

VAHTIn tavoitteena on parantaa valtionhallinnon toimintoja kehittämällä tietoturvallisuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. VAHTI-ohjeistus kattaa kaikki tietoturvallisuuden osa-alueet.

Tietoturvaohjeet löytyvät osoitteesta: https://www.vahtiohje.fi (jossa muun muassa pdf-dokumentti tietoturvapoikkeamatilanteiden hallinnasta).

Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman 2018-2021 painopisteitä ovat:

digitaalisen turvallisuuden johtamisen ja riskienhallinnan kehittäminen, osaava henkilöstö, digiturvaosaamisen ja -tietoisuuden kehittäminen sekä uuden teknologian hyödyntäminen tehokkaasti palveluiden ja digiturvallisuuden toteuttamisessa.

Suosittelemme, että jokainen julkisen hallinnon organisaatio osallistuu JUDO-hankkeessa toteutettavaan Digitaalisen turvallisuuden yhteishankkeeseen, jossa tullaa kehittämään kaikkia viittä digitaalisen turvallisuuden (riskienhallinta – toiminnan jatkuvuus ja varautuminen – tietoturva – kyberturvallisuus – tietosuoja) osa-alueita vuosien 2019-2021 aikana.

Lisätietoa ja ilmoittautuminen: https://vrk.fi/osallistu-digiturva-yhteishankkeeseen

Lisätietoa JUDO-hankkeesta: https://vrk.fi/judo

Liite 2

Ohjaava lainsäädäntö

Sosiaali- ja terveydenhuollon digitalisaatiosta ja tiedonhallinnasta säädetään useissa laeissa ja asetuksissa. Lainsäädäntö ohjaa asiakas- ja potilastietojen hallintaa. Alla on mainittu oleellisimpia säädöksiä.

Valmiuslaki 1552/2011

Valmiuslain mukaan valtion viranomaisten ja laitosten sekä kuntien on varmistettava tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa. Valmius varmistetaan muun muassa valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin.

Arkistolaki 831/1994 ja Arkistolaitoksen ohjeet

Lakia ja ohjeita noudatetaan potilasasiakirjojen säilyttämisessä.

EU:n verkko- ja tietoturvadirektiivi 2016/1148 nk. NIS-direktiivi

Merkittävä osa kyberturvallisuuden lainsäädäntöä, joka sisältää määräyksiä toiminnan jatkuvuuden turvaamisesta yhteiskunnallisesti kriittisten palveluiden tarjoajille.

NIS-direktiivillä on suora yhteys kriittiseen infrastruktuuriin ja kansalliseen huoltovarmuuteen.

Merkittävän kyberhäiriön hallintaan kuuluu direktiivin mukainen ilmoitus Valviralle. NIS-direktiivin nojalla terveydenhuoltoalalla samat organisaatiot ovat velvollisia ilmoittamaan Valviralle kyberhäiriöiden ja muiden potilaiden turvallisuutta vaarantavien tapahtumien johdosta.

EU:n yleinen tietosuoja-asetus 2016/679 (GDPR)

Uusi henkilötietojen käsittelyä sääntelevä laki, jota on sovellettu kaikissa EU-maissa 25.5.2018 alkaen. Asetusta täydennetään ja täsmennetään kansallisella lainsäädännöllä.

Laki potilaan asemasta ja oikeuksista 785/1992

Laissa säädetään potilasasiakirjojen käsittelystä ja asiakirjoihin sisältyvien tietojen salassapidosta.

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 812/2000

Laissa säädetään asiakkaan oikeuksista hänen tietojensa käsittelyssä ja salassapidossa.

Laki sosiaalihuollon asiakasasiakirjoista 254/2015

Laissa säädetään asiakastietojen kirjaamisesta ja siihen liittyvistä velvoitteista sosiaalihuollossa.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007

Laissa säädetään julkisten ja yksityisten sosiaali- ja terveyspalveluiden asiakastietojen sähköisestä käsittelystä ja valtakunnallisista tietojärjestelmäpalveluista. Laissa on säädökset tietojen salassapidosta, luovutuksesta, arkistoinnista ja asiakkaan oikeuksista saada tietoa omista asiakastiedoistaan.

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä

Laki (HE 159/2017) astuu voimaan huhtikuun alussa 2019. Laki yhdenmukaistaa terveystietojen luovutusta koskevaa sääntelyä ja luo uuden lupaviranomaisen, joka voi koota ja yhdistellä anonymisoituja terveystietoja ilman erillistä lupamenettelyä. Lain myötä sosiaali- ja terveydenhuollon asiakastietoja sekä muita terveyteen ja hyvinvointiin liittyviä henkilötietoja voidaan käyttää aiempaa laajemmin muussakin kuin ensisijaisessa käyttötarkoituksessa. Tavoitteena on sujuvoittaa ja nopeuttaa lupakäsittelyä sekä tietojen yhdistelyä eri rekistereistä. Näin voidaan lisätä sote-tietoaineistojen käyttöä tutkimus- ja kehittämistoiminnassa.

Laki sähköisestä lääkemääräyksestä 61/2007

Laissa on säädökset sähköisten lääkemääräysten käsittelystä ja potilaan tiedonsaantioikeuksista. Laissa säädetään Kelan ylläpitämästä valtakunnallisesta reseptikeskuksesta ja -arkistosta.

Laki terveydenhuollon laitteista ja tarvikkeista annetun lain muuttamisesta HE 165/2017, TLT-lain muutokset 936/2017

Laki sisältää terveydenhuollon laitteista ja tarvikkeista annettuun lakiin (629/2010) tehdyt vähimmäistason muutokset, jotka tarvitaan em. lääkinnällisiä laitteita koskevien EU-asetusten ensi vaiheen kansallisessa täytäntöönpanossa.

Laki turvallisuusselvityksistä 726/2014

Lain avulla on pyritty luomaan tehokas menettely henkilöiden ja yritysten taustojen selvittämiseksi. Sen avulla osana yleisen edun suojaa turvataan turvallisuutta ja yhteiskunnan toimivuuden kannalta kriittisen infrastruktuurin toimivuutta. Henkilöturvallisuusselvityksiä on kolme eri tasoa (suppea, perusmuotoinen ja laaja henkilöturvallisuusselvitys).

Lääkinnällisiä laitteita koskevat EU-asetukset ns. MD-asetus 2017/ 745 ja IVD-asetus 2017/746

Asetuspaketissa vahvistetaan säännöt ihmisille tarkoitettujen lääkinnällisten laitteiden ja niiden lisälaitteiden markkinoille saattamisesta, asettamisesta saataville markkinoilla tai käyttöönotosta unionissa. Tavoitteena on parantaa lääkinnällisten laitteiden turvallisuutta. Asetuksessa määrätään muun muassa laiteiden valmistajille velvollisuuksia hallita ja vähentää laitteiden kyberturvallisuusriskejä. Asetus tulee vaiheittain sovellettavaksi keväästä 2020 alkaen. Asetus edellyttää, että ohjelmistoja sisältävät lääkinnälliset laitteet sertifioidaan niiden kyberturvallisuuden osalta ennen niiden tuontia markkinoille.

STM:n asetus potilasasiakirjoista 298/2009

Asetusta noudatetaan potilasasiakirjojen laatimisessa sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisessä.

Terveydenhuoltolaki 1326/2010

Laissa säädetään potilastietojen luovutuksesta ja käytöstä sairaanhoitopiirin ja sen alueella toimivien terveyskeskusten välillä.

Tietosuojalaki

Henkilötietojen käsittelyä koskeva uusi tietosuojalaki tuli voimaan 1.1.2019. Lailla täydennetään EU:n yleistä tietosuoja-asetusta.

Muut ohjaavat asiakirjat

Kansallinen riskiarvio 2018

Sisäinen turvallisuus. Sisäministeriön julkaisuja 2019:5

Valtioneuvoston periaatepäätös yhteiskunnan turvallisuusstrategiasta 2017

Kokonaisturvallisuuden yhteistoimintamalliin perustuva periaatepäätös yhteiskunnan turvallisuusstrategiasta yhtenäistää varautumisen kansallisia periaatteita ja ohjaa hallinnonalojen varautumista.

Valtioneuvoston päätös huoltovarmuuden tavoitteista 2018

Huoltovarmuustoiminnan painopistettä suunnataan lisääntyvästi kriittisen infrastruktuurin toimintakyvyn varmistamiseen materiaalisen varautumisen lisäksi. Erityisiä painopisteitä kriittisen infrastruktuurin toimintakyvyn turvaamisessa ovat energiansaannin varmistaminen, elinkeinoelämän kyberturvallisuusuhkiin varautumisen ja niistä toipumisen tukeminen, digitaalisen yhteiskunnan tietojärjestelmien sekä viestintäpalveluiden ja -verkkojen varmistaminen, turvatut paikannus- ja aikatietojärjestelmät sekä toimivat logistiset palvelut ja verkostot.

Suomen kyberturvallisuusstrategia ja toimeenpano-ohjelma vuosille 2017-2020

Suomen kyberturvallisuusstrategian toimeenpano-ohjelmassa vuosille 2017–2020 tarkastellaan kyberturvallisuuden kehittämistä valtion, maakuntien, kuntien, yritystoiminnan ja kolmannen sektorin muodostamassa palvelukokonaisuudessa.

Terveyden ja hyvinvoinnin laitoksen määräykset sosiaali- ja terveydenhuollon tiedonhallinnan vaatimusten yhdenmukaistamiseksi

Tietojärjestelmiin ja tiedonhallinnan ratkaisuihin kohdistuvia olennaisia vaatimuksia yhdenmukaistetaan valtakunnallisesti. Yhdenmukaistaminen ja siihen liittyvät määräykset kohdistuvat ratkaisujen toiminnallisuuteen, yhteen toimivuuteen ja tietoturvallisuuteen https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset

Koulutusmateriaali: https://www.slideshare.net/THLfi/tietoturvan-ja-tietosuojan-omavalvonta-suunnitelma-ja-toteuttaminen-131218

VALVIRAn määräykset

VALVIRA julkaisee sosiaali- ja terveydenhuollon toimijoille tarkoitettuja määräyksiä ja ohjeita. https://www.valvira.fi/julkaisut-ja-maaraykset

Valtiovarainministeriön VAHTI (julkisen hallinnon digitaalisen turvallisuuden johtoryhmä) kehittää ja ohjaa julkisen hallinnon digitaalisen turvallisuuden kehittämistä. Vahti kattaa kaikki tietoturvallisuuden osa-alueet. https://vm.fi/vahti

LIITE 3

Käsitteet

CERT-FI-ryhmä (Computer Emergency Response Team) – Liikenne- ja viestintäviraston (Traficom) Kyberturvallisuuskeskuksessa toimivan CERT-FI:n tehtäviin kuuluu verkko-, viestintä- ja lisäarvopalveluihin kohdistuvien tietoturvaloukkausten ennaltaehkäisy, havainnointi ja ratkaiseminen, tietoturvauhkista ja -asioista tiedottaminen sekä tiedon kerääminen.

Haavoittuvuus – alttius tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.

Henkilötietosuoja – järjestelyt, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.

Hybridivaikuttaminen – poliittisesti motivoitunut suunnitelmallinen toiminta, jolla pyritään saavuttamaan omat tavoitteet erilaisia, toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen. Hybridivaikuttamisen keinot voivat olla esimerkiksi taloudellisia, poliittisia tai sotilaallisia. Keinoja voidaan käyttää samanaikaisesti tai siten, että ne seuraavat toisiaan. Hybridivaikuttamista tehdään esimerkiksi informaatio-, kyber-, fyysisten ja taloudellisten operaatioiden avulla. Hybridivaikuttamisen takana voi olla joko valtiollinen tai ei-valtiollinen toimija.

Häiriötilanne – uhka tai tapahtuma, joka vaarantaa yhteiskunnan elintärkeitä toimintoja tai strategisia tehtäviä ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää. Häiriötilanteita voivat olla esimerkiksi vakavat luonnononnettomuudet tai ihmisen toiminnasta aiheutuvat häiriötilanteet. Häiriötilanteita voi esiintyä niin normaalioloissa kuin poikkeusoloissakin. Häiriötilanne voi koskea esimerkiksi koko valtakuntaa tai olla alueellinen tai paikallinen. Häiriötilanne voi myös liittyä ainoastaan johonkin toimintoon.

ICMT (Information, Communication and Medical Technology) Lääkintälaitteisiin liittyvää teknologiaa kuvaava yleistermi.

Jatkuvuudenhallinta – organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa.

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI – valtionhallinnon elin, joka käsittelee ja sovittaa yhteen valtionhallinnon keskeiset tietoturvan ja kyberturvallisuuden linjaukset (VAHTI-ohjeet).

Kansallinen turvallisuusauditointikriteeristö (Katakri) – viranomaisten käyttöön tarkoitettu arviointityökalu, jonka avulla voidaan arvioida kohdeorganisaation kykyä suojata viranomaisen turvallisuusluokiteltua tietoa.

Kiristyshaittaohjelma – haittaohjelma, joka salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta.

Kriittinen infrastruktuuri – perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi.

Kyberhäiriötilanne, kyberturvallisuuden häiriötilanne, kyberhäiriö – toteutunut kyberuhka, joka haittaa organisaation tai järjestelmän toimintaa.

Kybertoimintaympäristö; kyberympäristö – yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö.

Kyberturvallisuus – tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Keskeiset tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden, määritellään Suomen kyberturvallisuusstrategiassa (valtioneuvoston periaatepäätös 24.1.2013).

Kyberturvallisuuskeskus – Liikenne- ja viestintäviraston alaisen Kyberturvallisuuskeskuksen tehtävänä on seurata kyberturvallisuusuhkia ja koota kyberturvallisuutta koskevaa tietoa eri toimijoille. Merkittävistä kyberuhkista keskus varoittaa ja valistaa myös kansalaisia. Kyberturvallisuuskeskus toimii sekä julkisen että yksityisen sektorin kanssa. Kyberturvallisuuskeskus tarjoaa tehostettuja palveluita huoltovarmuuskriittisille organisaatioille, joihin monet sosiaali- ja terveydenhuollon organisaatiot kuuluvat.

Kyberuhka – mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon.

Kyberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös digitaalisessa viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista. Kyberuhkat voivat kohdistua yhteiskunnan elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria tai kansalaisia vastaan joko suoraan tai välillisesti. Ne voivat olla peräisin maan rajojen sisältä tai niiden ulkopuolelta.

Käyttöoikeuksien hallinta – menettelyt, joilla myönnetään, evätään tai muilla tavoin käsitellään käyttöoikeuksia palveluihin ja järjestelmäresursseihin.

Normaaliolot – yhteiskunnan pääsääntöinen tila, jossa yhteiskunnan elintärkeät toiminnot voidaan turvata ilman, että on tarpeen mahdollistaa viranomaisten tavanomaisesta poikkeava toimivaltuuksien käyttö. Vaikka yhteiskunnan tilassa olisi häiriöitä, kyseessä on normaaliolot, jollei valtioneuvosto yhteistoiminnassa tasavallan presidentin kanssa ole todennut poikkeusoloja. Normaalioloissa esiintyvät uhkat voidaan ehkäistä ennalta tai tarvittaessa torjua viranomaisten säännönmukaisin toimivaltuuksin ja voimavaroin sekä yritysten normaalein riskienhallinnan keinoin. Normaalioloissa rakennettavat järjestelmät ja muut toimenpiteet luovat perustan toiminnalle häiriötilanteissa ja poikkeusoloissa.

Palvelunestohyökkäys – tietoverkkohyökkäys, jolla pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai tietojärjestelmä.

Poikkeusolot – valmiuslaissa (1552/2011) tarkoitettu yhteiskunnan tila, jossa on niin paljon tai niin vakavia häiriöitä tai uhkia, että on tarpeen mahdollistaa viranomaisten tavanomaisesta poikkeava toimivaltuuksien käyttö. Poikkeusolojen vallitsemisen toteaa valtioneuvosto yhteistoiminnassa tasavallan presidentin kanssa.

Resilienssi – yksilöiden ja yhteisöjen kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä.

Riskianalyysi – toiminta, jossa tunnistetaan riskit ja arvioidaan vahinkotapahtuman todennäköisyys sekä odotettavissa olevat vahingot. Riskianalyysia voidaan tehdä erilaisilla menetelmillä kohteesta, toiminnasta ja tilanteesta riippuen. Vahinkotapahtumalla tarkoitetaan tapahtumaa, josta aiheutuu vahinko eli haittaa tuottava menetys.

Riskienhallinta – järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet. Riskienhallintaan kuuluu keskeisenä omavalvontasuunnitelma (tietoturvasuunnitelma). Riskienhallinnan keinoja ovat riskin välttäminen, siirtäminen, pienentäminen jakamalla ja

vahingontorjunnalla sekä riskin ottaminen. Varautumisessa riskienhallinta on useiden eri tahojen yhteistyötä. Sitä tekevät yritykset, eri toimialat ja viranomaiset, kunnat ja valtio. Viranomaisilla ja joillain yrityksillä on lakisääteinen velvollisuus laatia valmiussuunnitelmia, johon riskienhallinta kuuluu tärkeänä osana. Riskienhallintaan kuuluu myös riittävien resurssien määrittäminen.

Tietoturva, tietoturvallisuus – järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen.

Tietoturvahäiriö; tietoturvapoikkeama – yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti.

Tietoturvahäiriön hallinta; tietoturvapoikkeaman hallinta – toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi.

Tietoturvaloukkaus – oikeudeton puuttuminen tietoon tai tietojärjestelmään. Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.

Tietoturvavalvomo; (security operations centre, SOC) – organisaatio tai sen osa, jossa muodostetaan, seurataan ja analysoidaan tietoturvan tilannekuvaa, ehkäistään, tunnistetaan ja analysoidaan tietoturvahäiriöitä, dokumentoidaan niitä sekä reagoidaan niihin ohjeistuksen mukaisesti. Organisaatiolla voi olla oma tietoturvavalvomo tai valvomon palvelut voidaan ostaa ulkopuoliselta palveluntarjoajalta.

Tietoturvaloukkauksen tutkinta – toimenpiteet, jotka käynnistetään tietoturvaloukkauksen paljastuttua loukkauksen selvittämiseksi. Tietoturvaloukkauksen tutkinta voi käsittää muun muassa todistusaineiston turvaamista, forensiikkaa, haittaohjelma-analyysia, lokianalyysia tai yleisesti tietoturvaloukkauksen vaikutusten ja laajuuden selvittämistä.

Tietoturvavalvomo; tietoturvahallintakeskus – organisaatio tai sen osa, jossa muodostetaan, seurataan ja analysoidaan tietoturvan tilannekuvaa, ehkäistään, tunnistetaan ja

analysoidaan tietoturvahäiriöitä, dokumentoidaan niitä sekä reagoidaan niihin ohjeistuksen mukaisesti.

Tietoverkkovalvomo; verkkovalvomo – organisaatio tai sen osa, jossa hallinnoidaan ja valvotaan yhtä tai useampaa tietoverkkoa.

Tunnistus, tunnistaminen – menettely, jolla varmistetaan henkilön identiteetti tai esineen tai asian tunniste.

Turvallisuusselvitys – Suojelupoliisin tai puolustusvoimien tekemä selvitys henkilön taustasta tai organisaation vastuuhenkilöistä, tietoturvan tasosta ja sitoumusten hoitokyvystä.

Vaarailmoitus – Valmistajien ilmoitusvelvollisuuden lisäksi sosiaali- ja terveydenhuollon ammattihenkilöiden velvollisuutena on ilmoittaa terveydenhuollon laitteen tai tarvikkeen (lääkinnälliset laitteet) aiheuttamasta vaaratilanteesta valvovalle viranomaiselle, Valviralle niin pian kuin mahdollista.

Valmiussuunnittelu – normaalioloissa tapahtuva varautumisen suunnittelu. Valmiuslain (1552/2011) 12 § velvoittaa viranomaiset varautumaan muun muassa valmiussuunnittelun avulla. Valmiussuunnitteluprosessissa selvitetään muun muassa häiriötilanteiden ja poikkeusolojen vaikutukset organisaation tehtäviin ja toimintaan, toiminnassa ja tehtävissä tapahtuvat muutokset, toiminnan jatkuvuuden turvaaminen ja toimenpiteet normaalioloihin palaamiseksi. Valmiussuunnittelun yksi tärkeä osa on valmiussuunnitelman teko.

Varautuminen – toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa. Varautumistoimenpiteitä ovat muun muassa valmiussuunnittelu, jatkuvuudenhallinta, etukäteisvalmistelut, koulutus sekä valmiusharjoitukset.

Yhteiskunnan elintärkeä toiminto – toiminto, joka on välttämätön yhteiskunnan toimivuuden kannalta.

Lähde

Turvallisuuskomitea; Kyberturvallisuuden sanasto 2018
Turvallisuuskomitea ja Sanastokeskus TSK: Kokonaisturvallisuuden sanasto 2017

LIITE 4

Hajautetun ja keskitetyn järjestelmän edut ja haitat

Tietojärjestelmän infrastruktuurin monistaminen eri paikkoihin on tehokas keino fyysisten ja joidenkin digitaalisten ja yhteiskunnallistenkin uhkien hallitsemiseksi. Esimerkkejä tällaisista uhkista ovat tulipalo, tietoliikenteen häiriö tai työtaistelutilanne. Järjestelmän sijoittaminen eri paikkoihin luo luonnostaan pisteitä, joissa järjestelmän sisäistä tietoliikennettä keskitetään. Nämä paikat ovat hyviä myös digitaalisten uhkien, kuten haittaohjelmien leviämisen, torjumiseen.

Eri paikkoihin sijoitettujen tietojärjestelmän osien pitäminen synkronoituina keskenään vaatii huolellisuutta. Yksinkertaisimmillaan voi riittää VPN-yhteydet eri laitetilojen välillä, jolloin etäällä toisistaan olevat laitteet näyttäytyvät toisilleen kuin ne olisivat samassa sisäverkossa. Tuolloin synkronointiin voi käyttää samoja menetelmiä kuin samaan laitetilaan kahdennettujen laitteiden välillä.

Jos organisaation toiminta sietää pieniä tietojärjestelmän toiminnan keskeytyksiä, niin varautumiseksi voi riittää, että toinen puolikas järjestelmästä on olemassa, muttei käynnissä.

Mitä vähemmän toiminta sietää keskeytyksiä, sitä enemmän täytyy huolehtia siitä, että hajautetun järjestelmän osat ovat synkronoituja keskenään ja että käyttäjää palvelevan järjestelmän osan vaihdot eivät näy käyttäjälle. Usein riittää, että vain tietyt osat järjestelmästä, kuten tietokanta, ovat jatkuvasti synkronoituina ja toiset osat voivat olla hitaammassa valmiudessa.

Useaan paikkaan hajautetun järjestelmän toimivuuden ja turvallisuuden valvonta vaatii väistämättä useampien yksityiskohtien valvomista kuin yhteen paikkaan sijoitetun järjestelmän valvonta. Hyvän valmistelun jälkeen tehtävä työ vähenee, sillä myös valvontaa voidaan tuolloin automatisoida.

LIITE 5

Järjestelmien sertifioinnit ja auditoinnit sekä standardeja

Terveyden ja hyvinvoinnin laitoksen määräykset liittyen tiedonhallintaan sosiaali- ja terveysalalla https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset

Katakri – kansallinen turvallisuusauditointikriteeristö

Katakri on viranomaisten arviointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Vaatimukset eivät ole toteutusohjeita eivätkä sellaisenaan hankintojen turvallisuusvaatimuksiakaan. Kaikkia vaatimuksia ei tarvitse soveltaa kaikkiin tarkasteltaviin järjestelmiin.

Katakrin päätavoite on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa kohteen turvallisuustason auditoinnin yrityksessä tai muussa yhteisössä. Organisaatiot voivat myös käyttää Katakrin osia tietoturvallisen toimintansa kehittämisen suuntaviivoina. Katakri sisältää paljon viittauksia ISO/IEC 27000 -standardeihin. Tuorein Katakrin versio on vuodelta 2015.

ITIL (IT Infrastructure Library)

ITIL-viitekehykseen on koottu IT-palveluhallinnan parhaat käytännöt. AXELOS omistaa oikeudet hallintamalliin ja julkaisee ITILiin liittyviä dokumentteja. ITILissä määritetään palvelutuotannon prosessit, roolit ja toiminnot. ITIL on rakennettu kattamaan koko IT-palveluiden elinkaari:

- palvelustrategia
- palvelusuunnittelu
- palvelutransitio
- palvelutuotanto
- palvelun jatkuva parantaminen.

COBIT 5

COBIT 5 on kansainvälinen kokonaisarkkitehtuurimalli tietohallinnon johtamiselle sisältäen tietoturvallisuuden kehittämisen periaatteet. Lisätietoja arkkitehtuurimallista löytyy ISACAN kotisivuilta www.isaca.org

STANDARDEJA

Standardit muodostavat viitekehyksen ja rungon toiminnan pitkäjänteiseen kehittämiseen. Tähän on kerätty muutamia merkittäviä standardeja ja viitekehyksiä terveydenhuollon näkökulmasta. Standardeista ISO/IEC-standardit ovat hyvin tunnettuja Suomessa, joihin on sisällytetty tietoturvallisuuden hallinta.

Tietoturvallisuuden hallintajärjestelmä:

- on osa yleistä hallintajärjestelmää, joka liiketoimintariskien arviointiin perustuen luodaan ja toteutetaan
- käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena parempi tietoturvallisuus
- helpottaa yritysjohdon tietoturvatyön organisointia
- tulisi kattaa kaikki tietoturvan johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat menettelyt ja toimenpiteet
- ei ole yksittäinen dokumentti, vaan moniosainen prosessi, jota on kehitettävä jatkuvasti
- osia ovat muun muassa riskianalyysi ja tietoturvapolitiikka sekä tietoturva-, jatkuvuus- ja toipumissuunnitelmat
- ISO/IEC 27000 viittaa kasvavaan ISO/IEC-standardiperheeseen, jonka yhteinen otsikko on "Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät"
- tarjoaa suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin tietoturvallisuuden hallintajärjestelmissä
- myös muut 27-alkuiset tietoturvallisuuteen liittyvät standardit lasketaan toisinaan perheeseen kuuluvaksi.

ISO 27000-standardiperheen sisältö (olennaisimmat terveydenhuollossa):

- 27000:2015 – Yleiskatsaus ja sanasto
- 27001:2013 – Vaatimukset
- 27002:2013 – Tietoturvallisuuden hallintakeinojen menettelyohjeet/kontrollit
- 27003:2010 – Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita
- 27004:2009 – Mittaaminen
- 27005:2011 – Tietoturvariskien hallinta
- 27799:2016 – Terveydenhuolto. Tiedonhallinta terveydenhuollossa ISO/IEC 27002 avulla.

ISO 22301 -standardi käsittelee organisaation jatkuvuuden hallintaa muun muassa kyberturvallisuuden näkökulmasta.

Muuta hyödynnettävää tukimateriaalia

Suomen Standardisoimisliitto SFS SFS-EN ISO/IEC 27002:2017
Finnish Standards Association SFS 3
Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Information technology. Security techniques. Code of practice for information security controls (ISO/IEC 27002:2013 Including Cor 1:2014 and Cor 2:2015)

LIITE 6

Linjaukset julkisen hallinnon pilvipalveluista

Linjaukset julkisen hallinnon pilvipalveluista on laadittu valtiovarainministeriön (VM) päätöksen VM/276/00.01.00.01/2018 mukaisesti.

Linjaukset määrittävät, miten julkisen hallinnon organisaation omistamaa tietoa voidaan käsitellä pilvipalveluissa. Linjausten tavoitteena on tukea valtion ja kuntien päätöksentekoa niiden suunnitellessa ja hankkiessa uusia ICT-palveluita.

Linjaukset käsittelevät jaettuja resursseja (esimerkiksi laskentateho, tallennus-, varmuuskopiointi- ja tiedonsiirtokapasiteetti) tarjoavia ICT-palveluita, niin sanottuja pilvipalveluita. Uudet tietojärjestelmät ja prosessit hyödyntävät enenevässä määrin pilvipalveluteknologiaa. Sille ominaisia etuja ovat kustannustehokkuus, skaalautumiskyky, tietoturva, energiatehokkuus, joustavuus, innovatiivisuus. Pilvipalveluiden pääpalvelumalleja on viisi: oma konesali, isännöity konesali, infrastruktuuri palveluna (IaaS), ohjelmistoalusta palveluna (PaaS) ja ohjelmisto palveluna (SaaS). Päätoteutusmalleja on neljä: oma konesali, yksityinen pilvi, julkinen pilvi ja hybridipilvi.

Linjaukset:

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta.
2. Pilvipalveluissa on kiinnitettävä erityistä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen.
3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset.
4. Mikäli pilvipalvelu tai pilvipalveluteknologia tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita.
5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti sekä oleellisten sopimusehtojen muuttuessa.
6. Julkisen tiedon käsittelyä ei rajoiteta.
7. Ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu.

LIITE 7

Tekniset suojautumiskeinot ja muita ohjeita

Sote-sektorin organisaatiot joutuvat tänä päivänä hyvin monenlaisten kyberhyökkäysten kohteeksi. Tähän ohjeistukseen on koottu useista eri julkisista lähteistä saatavilla olevia ohjeita, erityisesti teknisen suojauksen näkökulmasta.

Ohjelmistojen pitäminen ajan tasalla on yksi tärkeimpiä perustoimenpiteitä suojauduttaessa erilaisten haittaohjelmien tartunnoilta. Mikäli esimerkiksi lääkintälaitteen yhteydessä olevaa tietokonetta tai ohjelmistoa ei voi päivittää lääkintälaitehyväksyntöjen vuoksi, tulee laitteen ympärille rakentaa erillinen suojaus, esimerkiksi verkkosegmentoinnin ja palomuurien avulla.

Euroopan verkko- ja tietoturvavirasto ENISA on julkaissut ohjeistuksia liittyen älykkäiden sairaaloiden kyberturvallisuuteen: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Yhdysvalloissa sairaalaympäristöjen kyberturvallisuuteen liittyvää ohjeistusta löytyy myös eri tahojen julkaisemana. Yhdysvaltain NIST-instituutin NCCoE (National Cybersecurity Center of Excellence) on julkaissut vuoden 2018 aikana muun muassa sairaaloiden IT-ympäristöihin liittyviä ohjeistuksia: https://www.nist.gov/programs-projects/security-health-information-technology

Erillisiä ohjeistuksia löytyy esimerkiksi infuusiopumppujen turvaamiseen: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf

Sekä kannettavissa laitteissa olevien terveystietojen turvaamiseen: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1.pdf

Norjan HelseCERT on kirjoittanut teknispainotteisia ohjeita järjestelmien ylläpitoon, koventamiseen ja käyttäjien ohjeistamiseen: https://www.nhn.no/helsecert/anbefalte-sikkerhetstiltak/

Mobiililaitteet ja niiden tietoturva

Sairaalan antamia mobiililaitteita lähtee sairaalasta ulos muun muassa tilanteissa, joissa asiakas tai sote-ammattilainen kirjaa mobiililaitteella terveystietoa joko pilven kautta tai suoraan sairaalan sisäverkosta julkaistuun palveluun. Eräs hyväksi havaittu suojauskeino on tehdä kutakin palvelua varten oma mobiili-internetin yhteysosoite (APN eli access point name). Yhteistyössä teleoperaattorin kanssa palvelu voidaan rajata näkymään vain

kyseisen yhteysosoitteen kautta internetiä käyttäville laitteille. Kun lisäksi ennakkoon tehdään tarkka arviointi tietoliikennetarpeista ja säädetään palvelua suojaavat muut tavanomaiset suojaukset (kuten palomuuri ja poikkeamien tarkkailu) asianmukaisesti, voidaan häiriöiden ja väärinkäytösten riski laskea siedettävälle tasolle.

Microsoftin Office 365 -ohjelmistot ja -palvelut, kuten sähköposti, ovat lähtökohtaisesti käytettävissä myös mobiililaitteilla. Monet mobiililaitteiden sovellukset eivät kuitenkaan tue käyttäjän tunnistamista usean tekijän menetelmillä. Esimerkiksi Apple iOS:n sähköpostisovellus ei tue usean tekijän tunnistautumista.

Rikolliset kalastelevat käyttäjien käyttäjätunnuksia ja salasanoja erittäin aktiivisesti ja yrittävät murtautua organisaation tietojärjestelmiin käyttäen kalastelemiaan salasanoja sekä sovelluksia, jotka eivät tue usean tekijän tunnistautumismenetelmiä. Jos organisaatio siis sallii työntekijöidensä kirjautua palveluihin ilman usean tekijän tunnistusta, se sallii sen myös rikollisille. Office 365 -tuotteita käyttävien organisaatioiden pitää siis valita, estävätkö ne heikomman tietoturvan sovellusten käytön kaikilta vai ottavatko ne tietomurtojen riskin.

Henkilökunnan järjestelmien käyttötavat (salasanakäytänteet, yhteiskäyttöiset tunnukset)

Tietojärjestelmien käyttäjien pitää pääsääntöisesti tunnistautua järjestelmiin henkilökohtaisilla käyttäjätunnuksillaan. Kertakirjautumisjärjestelmän käyttö on suositeltavaa, jotta tietojärjestelmien käyttäjien ei tarvitse muistaa useita eri käyttäjätunnuksia ja salasanoja.

Usean ihmisen keskenään jakamia käyttäjätunnuksia ei tule pääsääntöisesti sallia eikä käyttää. Järjestelmissä ja laitteissa, joissa ei käsitellä arkaluonteisia tietoja, jotka eivät tue useita käyttäjätunnuksia ja joihin pääsyä täytyy estää muilta kuin henkilökunnan jäseniltä, käyttäjäorganisaatio voi hyväksyä yhteiskäyttöisen tunnuksen käytön. Tällainen laite voi olla esimerkiksi sairaalan poliklinikan käytävälle sijoitettu ultraäänilaite.

Tietojärjestelmien käyttö ilman käyttäjän tunnistamista tulee pääsääntöisesti estää. Käyttäjäorganisaatio voi hyväksyä ilman käyttäjän tunnistusta käytettäväksi laitteen, jossa ei käsitellä arkaluonteisia tietoja ja joka on fyysisesti suojattu väärinkäytöksiltä. Tällainen laite voi olla esimerkiksi lukittuun vastaanottohuoneeseen sijoitettu ultraäänilaite.

Laite- ja järjestelmätoimittajien etäyhteydet

Etäyhteyksien tekniset vaatimukset ja käyttötavat tulisi määritellä jo sopimusta tehtäessä, jotta järjestelmän toimittaja saadaan sitoutumaan sairaalan haluamaan toimintamalliin. Sama etäyhteystapa ei käy kaikille toimittajille, mikä sairaalan vain täytyy hyväksyä.

Olennaista on, että verkonvalvonnalla, SOC:lla tai muulla sellaisella, olisi kyky tunnistaa sallitut ja luvattomat etäyhteydet nettiliikenteen joukosta. Tätä on vaikeaa toteuttaa 100 % kattavasti.

Haittaohjelmien leviäminen (kiristysohjelmat WannaCry)

Tietokonevirusten eli haittaohjelmien tarttumisen ja leviämisen estäminen perustuu ennen kaikkea turvallisesti käyttäytyviin tietokoneiden käyttäjiin, päivitettyihin ja turvallisesti määritettyihin ohjelmistoihin sekä haittaohjelmien torjuntaohjelmiston käyttöön. Mikäli haittaohjelma pääsee tarttumaan johonkin tietokoneeseen, sen leviämistä voidaan rajoittaa tietoverkkojen segmentoinnilla, verkkoon kytkettyjen päätelaitteiden tunnistamisella ja tietokoneiden käyttäjien ja prosessien käyttöoikeuksien rajoittamisella.

Verkkojen segmentointi tarkoittaa eri tarkoituksiin käytettävien kokonaisuuksien erottamista toisistaan galvaanisesti erillisillä johdotuksilla ja verkkolaitteilla, verkkolaitteiden erotustoiminnoilla (esimerkiksi virtual LAN), palomuureilla tai näiden keinojen yhdistelmillä. Esimerkiksi lääkintälaitteiden, potilashoidon työasemien ja normaalien toimistotyöasemien erottelu toisistaan on syytä tehdä kaikkialla. Tämä ontuu monissa sairaaloissa – verkot ovat usein isoja verkkoarkkitehtuuriltaan litteitä kokonaisuuksia. Sellaisessa verkossa saastuneella tietokoneella ei ole esteitä ottaa yhteyttä muihin koneisiin.

Verkkoon kytkettyjen päätelaitteiden tunnistus tehdään varmenteilla. Käytännössä liitettyjä laitteita ei useinkaan tarkisteta.

Päätelaitteiden sovellusten ja käyttäjien kirjoitusoikeuksien kartoitus yhteisiin resursseihin ja rajaus tulisi muuttaa entistä tiukemmalle. Usein käyttäjille ja sovelluksille annetaan laajoja kirjoitusoikeuksia. Ne lisäävät tiedostoja salaavien haittaohjelmien aiheuttamia tuhoja.

Sote-alan organisaatioille hyödyllisiä ohjeita (Traficomin Kyberturvallisuuskeskuksen ja VAHTIn ohjeita)

Selviytymisopas kiristyshaittaohjelmia vastaan – Kokemuksia kiristyshaittaohjelmista Suomessa ja neuvoja niistä selviytymiseen (005/2016 J). Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

Lokien keräys ja käyttö – Ohje lokitietojen tallentamiseen ja hyödyntämiseen (Ohje 4/2016). Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

Palvelunestohyökkäysten ehkäisy ja torjunta (Ohje 3/2016). Ohje käsittelee erityisesti julkisten www-palveluiden suojaamista palvelunestohyökkäyksiltä. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta.pdf

Verkkosivujesi pimeä puoli – Ohjeita sisällönhallintajärjestelmien kyberuhkien torjumiseksi (Ohje 2/2016). Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Sisallonhallintajarjestelmien_kyberuhkia.pdf

Verkkopalvelun ohjelmistoalustan valinta ja palvelun turvallinen ylläpito (Ohje 1/2011). Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/verkkopalvelun-ohjelmistoalustan-valinta-ja-palvelun-turvallinen-yllapito-ohje-12011

Terveydenhuoltoalan kyberuhkia (Ohje 1/2016). Lyhyt lintuperspektiivin katsaus sote-organisaatioiden johtajille. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf

Raportti: Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. Raportti sisältää kuvailuita kohdistetuista haittaohjelmahyökkäyksistä (engl. advanced persistent threat, APT) sekä ohjeita niiltä suojautumiseen. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf

Ohje 10/2014 Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön. Neuvoja matkapuhelinten kyberturvalliseen käyttöön ja ylläpitoon; sovellettavissa myös tablet-tietokoneisiin. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvavinkkeja_matkapuhelimen_turvalliseen_kayttoon.pdf

Langattomasti, mutta turvallisesti. Langattomien lähiverkkojen tietoturvallisuudesta (Ohje 2/2014). Neuvoja WLAN/WiFi-verkkojen kyberturvalliseen käyttöön ja ylläpitoon kuluttajien ja pienten yritysten näkökulmista. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Näin meitä huijataan! Verkossa yleisesti tavattuja huijausmenetelmiä (Ohje 1/2014, päivitetty 30.3.2017). Tietoa internetin kautta tehtävistä huijauksista ja neuvoja niiden välttämiseen sekä toimintaohjeita huijatuiksi joutuneille. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Nain_meita_huijataan.pdf

Salasanat haltuun – Neuvoja salasanojen käyttöön ja hallintaan (Joulukuun 2014 teeman koontijulkaisu). Neuvoja salasanojen valintaan, käyttöön ja hallintaan sekä ICT-palveluiden käyttäjille että ylläpitäjille. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Pilvipalvelujen turvallisuus. Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä (Ohje 5/2014). Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Kansainvälisesti toteutetun palvelun tietoturvasta tiedottaminen (Suositus 205/2014 S). Suositus siitä, miten teleyritysten tulisi kertoa tilaajille sellaisten viestintäpalveluiden tietoturvasta, jotka on toteutettu osin tai kokonaan Suomen ulkopuolella. Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Suositus_205_2014.pdf

Toiminnan jatkuvuuden hallinta (VM:n julkaisuja 2/2016) http://urn.fi/URN:ISBN:978-952-251-779-1

Tietoturvapoikkeamatilanteiden hallinta (VM:n julkaisuja 8/2017) http://urn.fi/URN:ISBN:%20978-952-251-930-6

ICT-varautumisen vaatimukset (VAHTI 2/2012) https://www.vahtiohje.fi/web/guest/2/2012-ict-varautumisen-vaatimukset

Kyberturvallisuus on osa sosiaali- ja terveydenhuollon palveluiden valmiutta ja varautumista.

Ohjeen tarkoitus on antaa yleiskuva toimialaa koskevista kyberturvallisuuden periaatteista sekä olemassa olevista ohjeista ja suosituksista. Ohje perustuu Suomen kyberturvallisuusstrategian toimeenpano-ohjelmaan ja sillä tuetaan osaltaan yhteiskunnan elintärkeiden toimintojen varmistamista häiriötilanteissa.

Ohje ei esitä yksityiskohtaisia tai teknisiä toimenpiteitä kyberuhkan tunnistamiseen tai torjuntaan, vaan niitä varten toimijat saavat ohjausta muun muassa Kyberturvallisuuskeskukselta. Lisäksi esimerkiksi Terveyden ja hyvinvoinnin laitos on tuottanut määrittelyjä, määräyksiä ja koulutusmateriaalia toimialan tiedonhallintaan.

Ohje on tarkoitettu yleisohjeeksi sosiaali- ja terveydenhuollon toimijoille erilaisissa organisaatioissa ja se on valmisteltu sosiaali- ja terveysministeriön ja Kuntaliiton yhteisessä hankkeessa.

Tämän ohjeen ensimmäinen versio julkaistaan sosiaali- ja terveysministeriön julkaisusarjassa ja sitä tullaan päivittämään tarpeiden mukaan. Liitteinä on taustoittavaa ja syventävää tietoa.

Internet: stm.fi/julkaisut

JULKAISUJEN MYYNTI:
julkaisutilaukset.valtioneuvosto.fi

ISSN PDF 1797-9854
ISBN PDF 978-952-00-4085-7