Kyberhäiriöiden hallinta

KÄSIKIRJA TERVEYDENHUOLLON TOIMIJOILLE

BUSINESS FINLAND

JYVSECTEC by jamk

MAAILMALLA ON UUTISOITU *lukuisista kyberhyökkäyksistä terveydenhuollon organisaatioihin koronakriisin aikana ja myös Suomessa on tapahtunut vakavia kyberhäiriötilanteita. Euroopassa kiristyshaittaohjelmilla terveydenhuollon organisaatioihin tehtyjen hyökkäysten määrä oli vuoden 2020 lokakuussa 36 %:a suurempi kuin syyskuussa. Yhdysvalloissa kiristyshyökkäykset kohdistuivat lokakuussa eniten terveydenhuoltoalaan ja ne lisääntyivät jopa 71%:a syyskuuhun verrattuna. Check Point -tietoturvayrityksen mukaan terveydenhuoltoalaan kohdistuvista kyberhyökkäyksistä onkin tulossa globaali trendi.* [1]

[1] Varoitus: kyberhyökkäyksistä sairaaloihin tulossa globaali trendi, kasvu Euroopassa ”hälyttävää”, Tekniikka & Talous 2020

Sisältö

TEKSTI
Vesa Vertainen, Elina Suni, Marko Vatanen, Jari Hautamäki, Tuukka Laava ja Juha Piispanen

KUVITUS Valtteri Mäntylä-Blå ja Heli Sutinen

TAITTO Heli Sutinen

JULKAISIJA
Jyväskylän ammattikorkeakoulu, IT-instituutti | JYVSECTEC

PROJEKTI
Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä | Business Finland

Johdanto

Käsikirjan esittely

Tämän käsikirjan tarkoitus on kehittää terveydenhuollon ympäristöihin liittyviä kyberhäiriöiden hallinnan prosesseja ja toimintaohjeita, jotta voidaan varmistaa yhteiskunnan kannalta kriittisen terveydenhuollon toiminnan jatkuvuus myös kyberhyökkäysten tapahtuessa.

Käsikirja liittyy kiinteästi koronakriisin aiheuttamien haasteiden ratkaisemiseen kyberhäiriöiden hallinnassa muuttuvassa maailmassa. Pääteemat ovat valikoituneet yhteistyökumppaneiden kanssa käytyjen keskusteluiden pohjalta tärkeiksi kehittämisen kohteiksi. Käsikirjan sisältämät prosessit, ohjeet ja tarkistuslistat on esitetty helposti käytäntöön vietävässä muodossa. Tekniset asiasisällöt ja termit on selitetty lukijalle. Käsikirjan kohderyhmänä on kaikki terveydenhuollon toimijat, mutta erityisesti eri kokoisten terveydenhuollon organisaatioiden kyber- ja digiturvallisuudesta päättävät tahot sekä kyber- ja digiturvallisuudesta vastaavat työntekijät.

Projektin virallisten yhteistyökumppaneiden, Terveyden ja hyvinvoinnin laitoksen, Huoltovarmuuskeskuksen ja Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen lisäksi yhteistyötä on tehty sairaanhoitopiirien kanssa. Yhteistyötä on tehty myös Healthcare Cyber Range -hankkeen, Kyber-Terveys-hankkeen ja Telian kanssa. Käsikirja on toteutettu projektissa **Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä** (1.8.2020 - 31.1.2021). Projektin toteuttajana toimi Jyväskylän ammattikorkeakoulun IT-instituutti/JYVSECTEC kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus ja rahoittajana innovaatiorahoituskeskus Business Finland.

BUSINESS FINLAND

HUOLTOVARMUUSKESKUS

thl

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

JYVSECTEC by jamk

Käsikirjan käyttö

Tässä käsikirjassa **kyberhäiriöiden hallinta** on jaettu seuraaviin osa-alueisiin:

- **kyberhäiriöihin varautuminen**
- **kyberhäiriöiden käsittely ja reagointi**
- **kyberhäiriöistä palautuminen ja oppiminen**

Käsikirjaan on lisäksi nostettu omaksi osa-alueekseen **koronakriisin aikaiset kokemukset**, koska kriisin aikana on syntynyt uudenlaisia uhkaskenaarioita muun muassa etätyön yleistyessä uusilla aloilla. Kyberturvallisuusuhat ovat myös yleisesti lisääntyneet terveydenhuollossa koronakriisin aikana.

Käsikirja on tarkoitettu helposti sisäistettäväksi kokonaisuudeksi kyberhäiriöiden hallinnan kehittämiseen nimenomaan terveydenhuollossa. Käsikirjasta saa kattavasti tietoa kybervarautumiseen liittyen, joka on erittäin tärkeä vaihe kyberhäiriöiden hallintaa. Lisäksi käsikirjaa voidaan hyödyntää myös vaiheessa, jossa uhka on jo realisoitunut häiriöksi ja vaatii nopeaa reagointia, kuten myös jälkianalyysissä, jossa palautuminen normaaliin toimintaan ja häiriöiden välttäminen tulevaisuudessa korostuu (sekä näiden kahden vaiheen ennakoinnissa).

Käsikirja sisältää vinkkejä, linkkejä tiedon lähteille sekä nopeasti hyödynnettäviä tarkistuslistoja kyberhäiriönhallinnan eri vaiheisiin sekä koronakriisin aikana nousseisiin uudenlaisiin uhkatilanteisiin.

Käsikirjan käsitteistö

Ohessa on käsikirjan kannalta oleellinen tekninen käsitteistö selitettynä.

CERT | COMPUTER EMERGENCY RESPONSE TEAM

CERT-toiminnalla tarkoitetaan tietoturvaloukkausten ennaltaehkäisyä, havainnointia, ratkaisua ja tietoturvauhkista tiedottamista.

Ensiarvio | TRIAGE

Poikkeaman/häiriön ja uhkatapahtuman arviointi, kategorisointi ja priorisointi.

Esineiden internet | INTERNET OF THINGS, IOT

Fyysiset internetiin kytketyt laitteet, jotka pystyvät aistimaan ympäristöään ja viestimään tai toimimaan aistimansa perusteella älykkäästi.

Häiriön käsittely | INCIDENT RESPONSE, IR

Kuvaa organisaation prosessia käsitellä kyberhyökkäyksiä. Käytetään minimoimaan vaikuttavuutta organisaation liiketoimintaan, tutkimaan ja rajaamaan hyökkäystä, sekä palautumaan hyökkäyksestä.

Kyberhäiriö/-poikkeama | CYBER INCIDENT

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

Mitigoida | MITIGATE

Kyberhyökkäysten yhteydessä käytettynä tarkoitetaan hyökkäyksen vaikutuksen lieventämistä.

Poikkeamanseuranta | INCIDENT TRACKING

Poikkeamatilanteen tutkinnan ja käsittelyn seuranta. Systemaattista selkeää toimintaa ja raportointia tutkinnan vaiheiden ja löydösten kirjaamiseen sekä tilanteen johtamiseen.

SIEM | SECURITY INFORMATION AND EVENT MANAGEMENT

Järjestelmä, joka tarkkailee organisaation tietojärjestelmiä ja -verkkoja sekä hälyttää havaitessaan niissä normaalista poikkeavaa toimintaa.

Tietoturvavalvomo | SECURITY OPERATIONS CENTER, SOC

Yksikkö, joka valvoo organisaation tietoturvan tilannekuvaa, ennaltaehkäisee ja tunnistaa kyberpoikkeamia.

Tunnistetiedot | INDICATORS OF COMPROMISE, IOC

Tunnistetut ominaisuudet ja tekniset tiedot hyökkäyksestä. Voi olla määrämuotoista tai vapaata kuvausta riippuen tunnistetiedon tyypistä.

Uhkatapahtuma | SECURITY EVENT

Tapahtuma, joka koskee tietomurtoa, turvakontrollien kiertämistä tai muuta sääntöjen vastaista toimintaa. Voi olla esimerkiksi automaattisia hälytyksiä erilaisista kontrolleista. Tapahtuma ei vielä itsessään tarkoita, että kyseessä olisi kyberpoikkeama tai kyberhäiriötilanne.

Vastetoimi | RESPONSE

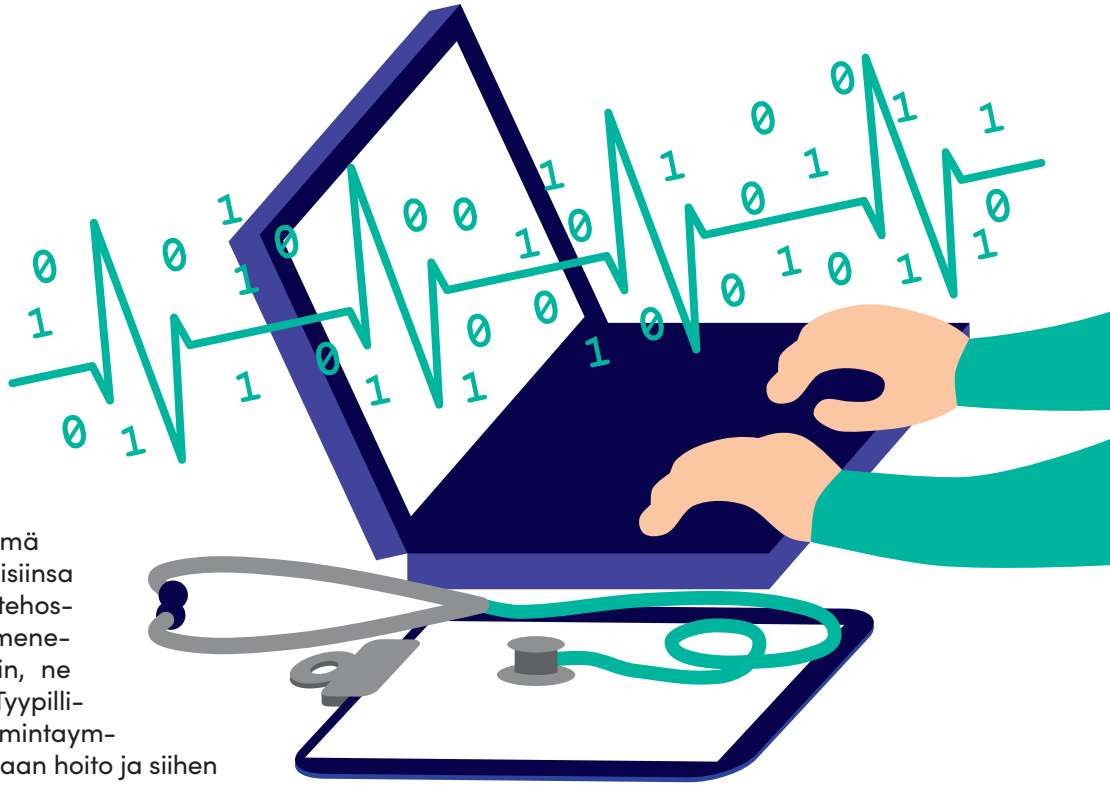
Vastetoimet sisältävät toimenpiteet kyberhyökkäyksen analysoimiseen, mitigoimiseen ja eristämiseen. Vastetoimet ovat oleellinen osa poikkeamasta palautumista.

Kyberturvallisuuden sanasto

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

Sanasto on luotu helpottamaan alalla työskentelevien tai muuten kyberturvallisuuden kanssa tekemisissä olevien työtä. Sanasto on syntynyt Huoltovarmuuskeskuksen, Turvallisuuskomitean ja Sanastokeskus TSK:n yhteistyönä.

Kyberturvallisuus terveydenhuollossa



Suomen kyberturvallisuusstrategiassa 2019 yhdeksi kolmesta strategisesta linjauksesta on nostettu kyberturvallisuuden osaamisen kehittäminen – arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina. Linjauksessa painotetaan, että yhteiskunnan kyberturvallisuuden ja elinkeinoelämän näkökulmasta on keskeistä, että kyberturvallisuus saadaan osaksi myös muiden kuin kyberturvallisuustuotteita ja -palveluita tai -ratkaisuja tuottavien yritysten toimintaa. Yhä merkittävämmässä roolissa nähdään tulevaisuudessa yritykset ja toimijat, joiden varsinainen (liike)toiminta on kyberturvallisuusalan ulkopuolella, mutta joiden toimintaan kyberturvallisuus ja siihen liittyvät häiriöt vaikuttavat merkittävästi. Muun muassa terveydenhuollon on katsottu kuuluvan tällaisiin aloihin. [2]

Esineiden internet (IoT, Internet of Things) laitteet ovat yleistyneet maailmalla ja myös sairaalaympäristöissä, jolloin yhä useammat lääkinnälliset laitteet ovat verkkoon kytkettyjä. Lääkinnällisten laitteiden hyväksymiskriteereissä ei ole vielä riittävän hyvin otettu huomioon kyberturvallisuusvaatimuksia. Samalla, kun nämä verkkoon ja usein myös toisiinsa kytketyt kehittyneet laitteet tehostavat ja luovat uusia hoitomenetelmiä sairaalaympäristöihin, ne myös lisäävät kyberuhkia. Tyypillisessä terveydenhuollon toimintaympäristössä on keskiössä potilaan hoito ja siihen olennaisesti liittyvät laboratorio- ja kuvantamispalvelut [3]. Toimintaympäristö on laaja ja monimuotoinen ja se sisältää kyberturvallisuuden näkökulmasta kriittisiä teknisiä järjestelmiä, laitteita ja sähköistä informaatiota. Näistä esimerkkejä ovat sähköiset potilastiedot, kyber-fyysiset järjestelmät kuten sairaalalaitteet, lääkinnälliset tietojärjestelmät, kirurgiset laitteet ja leikkausrobotit, IoT-laitteet kuten kuntoilulaitteet, hyvinvointilaitteet ja –sovellukset.

[2] Suomen kyberturvallisuusstrategia 2019
[3] Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. STM 2019

Kyberhyökkäyksen vaikutuksista terveydenhuollossa

Terveydenhuollon organisaation joutuessa kyberhyökkäyksen kohteeksi vaikutukset voivat olla hyvin merkittäviä ja laajoja.

Kyberhyökkäyksen vaikutukset voivat ulottua:

- **potilasturvallisuuteen**
- **hoidossa tarvittavien tietojärjestelmien toimintaan**
- **potilaiden sekä työntekijöiden tietojen yksityisyyteen ja turvallisuuteen**
- **sairaalan maineeseen**
- **sairaalan talouteen** ja [4]
- **sairaalan toimintakykyyn**.

Terveydenhuolto on erityisen haavoittuvainen kyberhyökkäysten näkökulmasta. Työn luonne tekee siitä äärimmäisen herkän palveluiden häiriöille. Sairaalan tietojärjestelmiin tai tietoliikenneverkkoon kohdistuneen hyökkäyksen vuoksi toimenpiteet voivat viivästyä tai pysähtyä ja tällä voi olla hyvin haitallisia vaikutuksia potilasturvallisuuteen. Lisäksi taloudelliset seuraukset ovat merkittäviä ja ne voivat olla myös pitkäaikaisia, kuten sairaalan mainehaitatkin. Kyberhyökkäyksen keskeyttämän hoidon seuraukset voivat ulottua sairaalan ulkopuolelle esimerkiksi apteekkien ja sairausvakuutusyhtiöiden toimintaan [5]. Potilasturvallisuus voi vaarantua myös älykkäiden sairaalalaitteiden jouduttua hyökkääjien manipuloimiksi. Potilaalle voidaan toimittaa esimerkiksi väärä lääkitys, mikä voi johtaa vakaviin haittoihin tai jopa kuolemaan. Myös esimerkiksi anestesiajärjestelmää, jossa on hengityslaite, voidaan manipuloida vikaantumaan leikkauksen aikana. [6]

Henkilökohtaiset terveystiedot ovat pimeillä markkinoilla arvokkaampia kuin luottokortti- tai henkilötiedot. Siksi verkkorikollisilla on suurempi peruste kohdistaa hyökkäys lääketieteellisiin tietokantoihin, jotta he voivat myydä tietoja tai käyttää niitä omaksi edukseen. [7]

> *Potilasturvallisuus voi vaarantua myös älykkäiden sairaalalaitteiden jouduttua hyökkääjien manipuloimiksi. Potilaalle voidaan toimittaa esimerkiksi väärä lääkitys, mikä voi johtaa vakaviin haittoihin tai jopa kuolemaan.*

[4] Kyberturvallisuus sosiaali- ja terveydenhuollossa, JYU 2019
[5] The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review, BMC Medical Informatics and Decision Makin 2019
[6] A Lifeline: Patient Safety & Cybersecurity, Public-Private Analytic Exchange Program 2019
[7] Data Breaches: In the Healthcare Sector, CIS Center for Internet Security 2020

Kyberturvallisuuden toimijat Suomen terveydenhuollossa

Suomen kyberturvallisuusstrategiassa (2019) mainitaan, että kyberturvallisuuden varautuminen edellyttää yhteiskunnan eri toimijoiden, julkishallinnon ja elinkeinoelämän välistä yhteistyötä ja osaamisen vahvistamista eri sektoreilla [2]. Yhteistoiminta on siis kyberturvallisuudessa erittäin tärkeää.

Ohessa on esitelty sosiaali- ja terveydenhuollon alan tiedonvaihtoryhmä (SOTE-ISAC) ja vapaaehtoisorganisaatio (Kyber-VPK) sekä lueteltu terveydenhuollon kyberturvallisuuden keskeiset kansalliset toimijat.

Tiedonvaihtoryhmä SOTE-ISAC

Sosiaali- ja terveydenhuollon alan tiedonvaihtoa varten perustettu luottamuksellinen tiedonvaihtoryhmä SOTE-ISAC kehittää sosiaali- ja terveysalojen toimijoiden kykyä suojautua kyberuhkilta ja -riskeiltä. Kyberturvallisuuskeskuksen tarjoamat ISAC-tiedonvaihtoryhmät (ISAC = Information Sharing and Analysis Centre) ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. Ryhmien päätarkoitus on jakaa tietoa ja kokemuksia sekä lisätä tätä kautta organisaatioiden ja toimialojen kykyä suojautua digitaalisilta uhkilta. Lisää tiedonvaihtoryhmistä tämän dokumentin kappaleessa **Kyberturvallisuuteen liittyvän tilannetiedon jakaminen.**

| https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

Vapaaehtoisorganisaatio Kyber VPK

On hyvä tiedostaa, että on olemassa myös vapaaehtoisorganisaatioita, joilta saa apua kyberturvallisuuteen liittyvissä palveluissa. Vapaaehtoista tukea terveydenhuollon toimijoille kyberturvallisuusasioissa tarjoaa KyberVPK-organisaatio, joka on noin kolmenkymmenen suomalaisen kyberasiantuntijan muodostama vapaaehtoisorganisaatio. Organisaatio perustettiin auttamaan terveydenhuollon toimijoita ja muiden kriittisten toimintojen tuottajia kyberuhkien ratkaisemisessa ja ennaltaehkäisemisessä. Jäsenet työskentelevät päivätyössään Suomen eturivin IT-alan yrityksissä, mutta KyberVPK:n asioissa kaikki toimivat vapaa-ajallaan eivätkä edusta työnantajiaan.

| https://kybervpk.fi/

Valkohattuhakkeri tarkoittaa eettistä, hyväntahtoista ja lakia noudattavaa tietoturva-ammattilaista, -tutkijaa ja/tai -harrastajaa. Valkohattuhakkeri auttaa yrityksiä ja näiden asiakkaita vastuullisesti ilmoittamalla löydöksistään suoraan yrityksiin.

Keskeiset kansalliset toimijat

ALUEHALLINTOVIRASTOT
| https://www.avi.fi/

DIGIFINLAND (ENT. SOTEDIGI OY, JOHON LIITTYI OSAKSI VIMANA OY 1.2.2020)
| https://digifinland.fi/

DIGI- JA VÄESTÖTIETOVIRASTO (DVV)
| https://dvv.fi/digiturva

HUOLTOVARMUUSKESKUS (HVK)
| https://www.huoltovarmuuskeskus.fi tai https://www.huoltovarmuuskeskus.fi/toimialat/terveydenhuolto/

KANSANELÄKELAITOS (KELA)
| https://www.kela.fi/kela-tietotalona

KESKUSRIKOSPOLIISIN KYBERRIKOSTORJUNTAKESKUS
| https://poliisi.fi/kyberrikokset

LIIKENNE- JA VIESTINTÄVIRASTO TRAFICOMIN KYBERTURVALLISUUSKESKUS
| https://www.kyberturvallisuuskeskus.fi

SAILAB -MEDTECH FINLAND SUOMESSA TOIMIVIEN TERVEYSTEKNOLOGIAYRITYSTEN EDUNVALVONTA- JA VAIKUTTAJAJÄRJESTÖ
| https://www.sailab.fi/

SOSIAALI- JA TERVEYSALAN LUPA- JA VALVONTAVIRASTO VALVIRA
| https://www.valvira.fi/terveydenhuolto

SOSIAALI- JA TERVEYSMINISTERIÖ (STM)
| https://stm.fi/etusivu

TERVEYDEN JA HYVINVOINNIN LAITOS (THL)
| https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla

VALTIONEUVOSTON TILANNEKESKUS (VN TIKE)
| https://vnk.fi/turvallisuus-ja-varautuminen/tilannekeskustoiminta

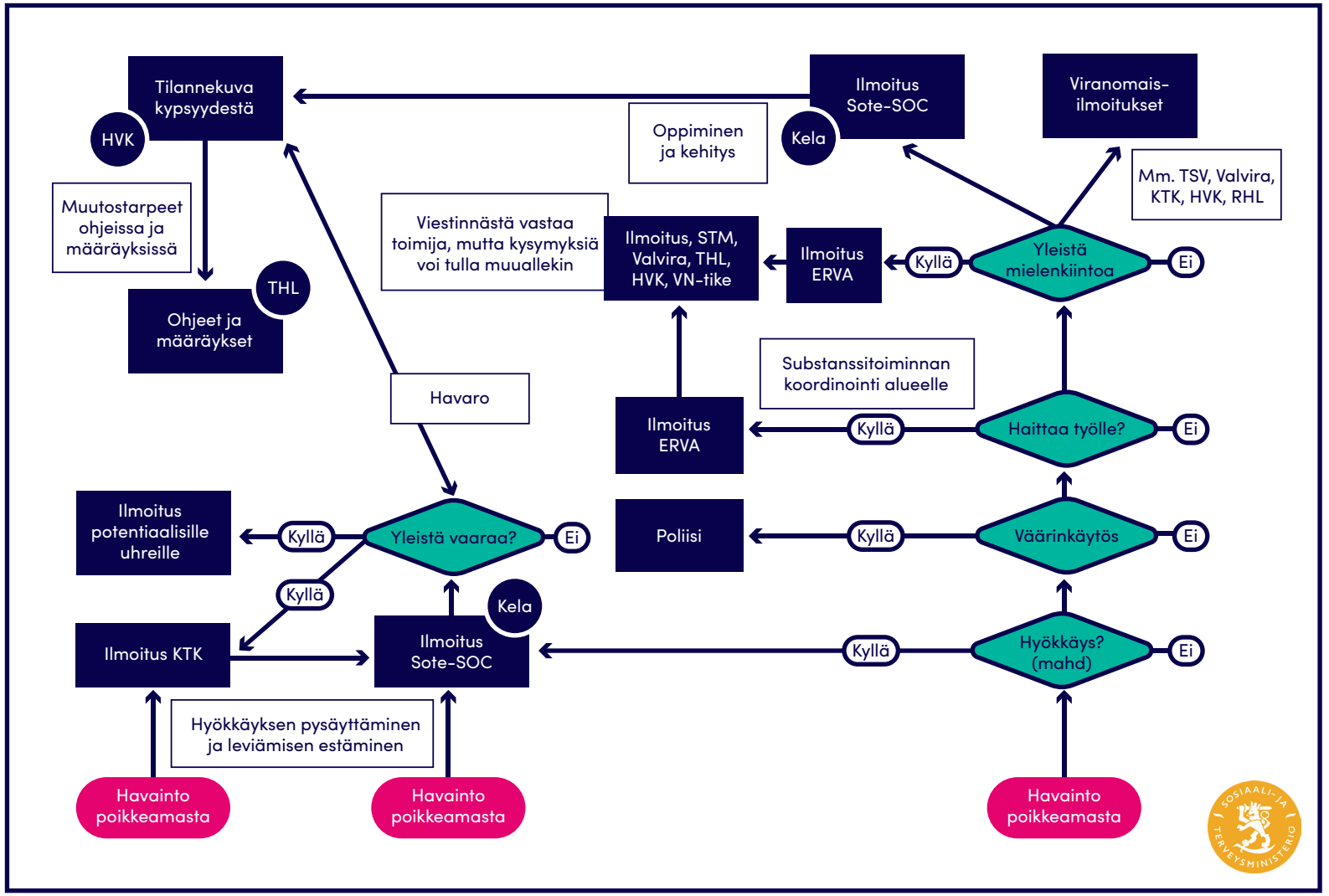
VALTIOVARAINMINISTERIÖ (VM)
| https://vm.fi/julkisen-hallinnon-ict

VALTORI
| https://valtori.fi/etusivu

Tiedonkulku ja toiminta toimijoiden välillä

STM:n julkaisussa **Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille** (STM:n julkaisuja 2019:14, Liite1) [3] on hyvä tiivis esittely suurimmasta osasta edellä mainituista toimijoista ja niiden roolista sosiaali- ja terveydenhuollossa. Toimijoiden roolien ymmärtämisen lisäksi on tärkeää tietää mihin toimijaan missäkin poikkeama/-häiriötilanteen vaiheessa tulee olla yhteydessä, tämä auttaa muun muassa tilannekuvan muodostamisessa.

Ohessa on sosiaali- ja terveysministeriön Teemupekka Virtasen tekemä kuva, jossa on havainnollistettu sosiaali- ja terveysalan kyberpoikkeaman/-häiriön osalta tiedonkulkua ja toimintaa. Oheinen kuva on luonnos, joten sen sisältämät tiedot voivat päivittyä. Vastaavantyyppisen kuvan tekeminen voi helpottaa terveydenhuollon organisaatiota kyberhäiriönhallinnassa.



KYS ERVA Kyber Road Show, STM:n Teemupekka Virtasen esitys "SoTe-sektorin kyberturvallisuuden tilannekuva", Teemupekka, 2020 (alkuperäisen kuvan visuaalista ilmettä on muokattu tekijän luvalla)

Kokemuksia koronakriisin ajalta

Koronakriisin aikana ympäri maailmaa, myös Suomessa, on nähty kohdennettujen kiristyshaittaohjelmien ja tietojenkalastelun raju kasvu. Näissä yritetään hyötyä kriisin tuottamasta epävarmuudesta ja kiireestä.

Kriisin aikaisia kyberhäiriöitä

Heti kriisin alkuvaiheessa COVID-19-aiheisia sähköposteja alkoi ilmaantua nopeaa tahtia, ja erään tutkimuksen mukaan niiden määrässä nähtiin jopa yli 600-prosenttinen kasvu vuoden 2020 helmi-maaliskuun aikana [8]. Tällaiset kalastelusähköpostit sisältävät linkkejä ja liitteitä, joista väitetään löytyvän tietoa tutkimuksista tai rokotteista koronavirukseen liittyen. Viestien uskottavuutta lisää se, että ne saatetaan naamioida virallisten tahojen, kuten WHO, ja oikeiden tutkimusten alle. Tosiasiassa linkkien ja liitteiden avaaminen saastuttaa tietokoneen tai älylaitteen haittaohjelmalla, joka avaa hyökkääjälle pääsyn laitteeseen ja sitä kautta organisaation verkkoympäristöön. Näin hyökkääjälle avautuu mahdollisuus tietojen varastamiseen tai salaamiseen rahallisen hyödyn saamiseksi. Virallisiksi koronatietoa välittäviksi tahoiksi naamioituja, haittaohjelmia levittäviä internetsivuja, on noussut kriisin aikana kovaa tahtia. NTT 2020 Global Threat Reportin mukaan uusia haitallisia sivuja on ilmaantunut pahimmillaan jopa 2000 sivun päivävauhtia [9].

Terveydenhuoltoon on tehty myös tietojenkalasteluyrityksiä puhelinsoitoilla, joissa on esiinnytty muun muassa IT-tuen nimissä. Näitä ”teknisen tuen” puheluita, ja Office 365 -tunnusten kalastelua on havaittu pitkin vuotta 2020. Uutena uhkana ovat nousseet kokouskutsut, jotka ovat kalastelulinkkejä. [10] Olemattomien hengityssuojainten ja testauspakkausten kaupittelukin on kuulunut koronakriisiä hyödyntävien ilmiöiden joukkoon [11]. Myös koronarokotteiden ja koronatestien eteen työskenteleviin yrityksiin on tehty hyökkäyksiä käyttäen sekä kohdennettua tietojenkalastelua että brute force -tekniikoita. Hyökkäysten kohteina on ollut useita johtavia lääkealan yrityksiä useissa maissa. [12]

Kiristyshaittaohjelmahyökkäyksiä, joiden päämääränä on ottaa haltuun ja salata tärkeitä tietojärjestelmiä, on kohdennettu kriisin kannalta kriittiseen infrastruktuuriin ja terveydenhuoltoon [13]. Tietojärjestelmät luvataan palauttaa käyttöön lunnaita vastaan, mutta lupauksia ei useinkaan täytetä. Syyskuussa 2020 tällainen hyökkäys, jossa sairaalan tietojärjestelmät suljettiin, aiheutti tiettävästi maailman ensimmäisen kyberrikollisuuteen liittyvän kuolemantapauksen [14]. Vuoden 2020 loppupuolella varoitettiin erityisesti Yhdysvaltojen terveydenhuollon toimijoihin kohdistuneista kiristyshaittaohjelmahyökkäyksistä, joissa hyödynnettiin mm. Conti, Trickbot, Ryuk ja BazarLoader -nimisiä haittaohjelmia [15].

Suomessa koettiin syksyllä 2020 tietomurto, jossa vietiin kymmenien tuhansien asiakkaiden henkilötietoja ja potilaskertomuksia. Tietojärjestelmiä ei otettu haltuun hyökkääjän toimesta, mutta anastetuilla asiakastiedoilla yritettiin kiristää ensin murron kohteeksi joutuneelta organisaatiolta lähes puolen miljoonan euron lunnaita, ja sen jälkeen kiristykset kohdistettiin suoraan asiakkaisiin. Ainakin 300 ihmisen tiedot julkaistiinkin Tor-verkossa. [16]

[8] 667% spike in email phishing attacks due to coronavirus fears, TechRepublic 2020
[9] A View of COVID-19's First Wave of Cybersecurity, info security GROUP, 2020
[10] Kybersää Lokakuu 2020, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
[11] Kybersää Maaliskuu 2020, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
[12] Cyberattacks targeting health care must stop, Microsoft 2020
[13] INTERPOL report shows alarming rate of cyberattacks during COVID-19, INTERPOL 2020
[14] Cyberattack On A Hospital Leads To The First Ransomware-Linked Death, Forbes 2020
[15] Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector, CISA 2020
[16] Yksi heistä on kiristäjä, YLE 2020

Lisääntyneen etätyön vaikutukset

Myös terveydenhuollossa siirryttiin entistä enemmän etätyöhön. On mahdollista, että tämä nopeassa aikataulussa tehty ”digiloikka” on jättänyt joissakin organisaatioissa tietoturva-aukkoja etäyhteyksiin ja pilvipalveluihin. Nopealla tahdilla käyttöönotetut palvelut ja laitteet vaatinevat myös jatkossa enemmän ylläpitotoimia kuin jos niiden rakenne ja toteutus olisi ehditty suunnitella huolellisesti. Kysymyksiä herättää myös lisääntyneen etätyön kuormittava vaikutus terveydenhuollon organisaatioiden tietoliikenneverkkoon ja pilvipalveluihin.

”Kotiverkko itsessään ei välttämättä ole tietoturvan kannalta yhtä hyvä kuin organisaation verkko.”

Organisaation kyberhäiriöihin varautumiseen vaikuttaa myös se, sallitaanko etätyössä omien laitteiden käyttö, ja mitä sovelluksia omaan tai työnantajan laitteeseen saa asentaa työtehtäviä varten. Kotiverkko itsessään ei välttämättä ole tietoturvan kannalta yhtä hyvä kuin organisaation verkko. Myös työtehtäviin liittyvän tiedon käsittely kotona asettaa omat haasteensa. Esimerkiksi potilastietoja saatetaan välittää sähköpostin kautta, ja tietoja voi kertyä sähköpostitilille pidemmän ajan kuluessa enemmänkin. Myös sillä, onko sähköpostitili oma vai työnantajan kautta saatu, ja käytetäänkö julkista internetiä vai salattua etäyhteyttä, on merkitystä. Henkilökunnan käyttöön tarkoitettuja kirjautumistietojakin saatetaan välittää eteenpäin liian huolettomasti. Salassa pidettävää tietoa saatetaan kotona myös tulostaa, mutta paperien säilyttämiseen ei ehkä ole lukittavaa kaappia. [17] Tulostimen ja tietokoneen välillä voi olla myös salaamaton langaton yhteys.

Kahden päällekkäisen kriisin uhka

Viimeistään koronakriisi on nostanut esiin kahden päällekkäisen kriisin uhkan. Maailmalla on nähty tilanteita, joissa ruuhkautunut ja paineen alla työskentelevä terveydenhuolto-organisaatio on joutunut kyberhyökkäyksen uhriksi. Yhtenä esimerkkinä voidaan mainita tšekkiläinen yliopistosairaala, johon kohdistui kyberhyökkäys maaliskuussa 2020. Sairaalan tekniset tietojärjestelmät jouduttiin sulkemaan, kiireellisiä leikkauksia siirtämään ja potilaita ohjaamaan toiseen sairaalaan. Hyökkäyksen vakavuutta lisäsi se, että kyseinen sairaala oli maan suurin COVID-19-testauslaboratorio. [18]

Terveydenhuoltoon kohdistetun kyberhyökkäyksen seuraukset voivat olla erittäin vakavia, mutta hyökkäyksiä yleisempiä ovat muut tietojärjestelmien häiriöt. Myös näiden kahden tunnistaminen toisistaan voi olla vaikeaa. Esimerkiksi syksyllä 2017 tapahtui yhdessä Suomen sairaanhoitopiirissä häiriö, joka onnettomuustutkintakeskuksen raportin mukaan sai alkunsa kahdeksan vuotta yhtäjaksoisesti päällä olleiden runkokytkimien vikaantumisesta. Häiriön vaikutukset olivat laaja-alaisia. Potilastietojärjestelmän toimimattomuus oli keskeisin ongelma. Potilaiden esitietoja ei pystytty lukemaan, lääkityksistä ja allergioista ei ollut varmaa tietoa, päivystyksessä oli vaikeuksia tietää, keitä potilaita oli sisällä ja joskus potilas unohtui ja hoito hidastui. Myös leikkaustoiminta häiriintyi merkittävästi esitietojen puuttumisen vuoksi, ja osassa leikkauksia tiedot hävisivät äkillisesti. Kirjaukset ja lähetteet mm. röntgeniin ja laboratoriokokeisiin jouduttiin tekemään paperilla. Tätä vaikeutti se, että kaikissa toimipisteissä ei ollut jatkuvuussuunnitelman mukaisesti valmiina kopioituja paperiversioita lähetteistä ja hoitosuunnitelmista. Ongelmia oli myös muun muassa valvontamonitorien yhteyksissä, ovien sähkölukoissa ja elvytyshälytysjärjestelmissä. Vakavasti sairaiden potilaiden hoito vaarantui näiden häiriöiden seurauksena. [19]

Tilanne, jossa tietojärjestelmien häiriöt iskisivät hetkellä, jolloin potilaiden hoito on kriisiytynyt, voisi olla pahimmillaan katastrofaalinen. Tämän vuoksi kyberhyökkäyksiin ja muihin häiriöihin varautuminen on erittäin tärkeä osa potilasturvallisuutta.

[17] Cybersecurity and Covid-19: Experiences from the frontline, PANACEA Research 2020
[18] Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, ZDNet 2020
[19] Helsingin ja Uudenmaan sairaanhoitopiirin tietojärjestelmähäiriöt 7.–8.11.2017, Onnettomuustutkintakeskus 2017

Kyberhyökkäystavat koronakriisi huomioiden

Ohessa on lueteltuna yleisiä terveydenhuoltoon kohdistuvia uhkia, joihin sisältyvät kriisin aikana nousseet uhkat.

Pilvipalvelut (potilas- ja asiakastietojärjestelmät, Kanta-palvelu ym.)

- Väärät järjestelmä- tai käyttöoikeusasetukset
- Palvelunestohyökkäykset
  - → Palvelut eivät toimi tai ovat hitaita
  - → Sairaalan henkilökunta ei pääse käsittelemään tarvittavia tietoja

Ohjelmistot

- Järjestelmään kirjautuvan henkilöllisyyttä ei todenneta
- Tietoturvaa huomioimaton ohjelmointi, haavoittuvuudet
- Käyttäjätunnukset hyökkääjän löydettävissä ohjelmiston käyttöohjeesta [20]

Tietojärjestelmät

- Tietojenkalastelu
  - → Kalastelusähköpostit, aiheina mm. koronatutkimus tai koronarokote
  - → Huijauspuhelut, esim. teknisen tuen nimissä
  - → Office 365 -kalastelut
- Haittaohjelmat
  - → Mm. korona-teemaiset sähköpostitse levitettävät haittaohjelmat, esim. Emotet
    - ↳ Hyökkääjällä pääsy potilastietoihin, valvontajärjestelmiin ja implantoituihin potilaslaitteisiin
    - ↳ Järjestelmien hidastuminen tai toimintahäiriöt
  - → Kiristyshaittaohjelmat
    - ↳ Järjestelmiä ei pystytä käyttämään, koska tiedot on salattu
    - ↳ Epävarmuus potilastietojen oikeellisuudesta sen jälkeen, kun tietojärjestelmät on palautettu toimintaan hyökkäyksen jälkeen
- Tietomurrot
  - → Henkilötietojen, potilaskertomuksien ym. myyminen eteenpäin
  - → Tietojen julkaisulla kiristäminen
- Palvelunestohyökkäykset
- Palvelunestohyökkäyksillä uhkailu ja lunnaiden vaatiminen

Langaton lähiverkko (WLAN)

- Tietoliikenneyhteys salaamaton tai heikosti salattu, joka edesauttaa hyökkääjän pääsyä:
  - → Potilaiden elintoimintojen tarkkailuun / salakuunteluun [21]
  - → Vääristämään, häiritsemään tai estämään tiedonsiirtoa [21]
  - → IoT-laitteiden ja muiden anturiteknologiaa käyttävien laitteiden häirintään [21]

Lääkintälaitteet

- Tunnistetietoja ei ole muutettu tehdasasetuksesta [22]
- Viivästyneet tai tekemättä jätetyt päivitykset, vanhojen laitemallien haavoittuvuudet
  - → Pääsy potilas- ym. tietoihin
  - → Äänisaaste: käyttäjien hämmentäminen tai häiritseminen laitteen paikallistamisäänellä [20]
- Haavoittuvuudet mm. infuusiopumpuissa
  - → Pääsy annostelun määrään [23]
- Lääkinnälliset laitteet valmistajien etävalvonnassa (ei sairaalan hallittavissa)

⚠ Etätyö

- Nopea digiloikka etätyöhön siirryttäessä kriisin aikana, uudet tekniikat, pilvipalvelut ym.
  → Tietoturva/tietosuoja voinut jäädä vajaaksi
- Kodista tullut sairaalan jatke
  → Hyökkäyspinta-alan kasvu etäyhteyksien lisääntyessä
- Kotiverkko ei ole välttämättä turvallinen
- Ylläpidon työtaakka kasvanut
- Työasemien riittävyys kaikelle henkilöstölle
- Etätyössä tietoja voi jäädä kotikoneelle, jota käyttävät muutkin perheenjäsenet
- Tulosteiden säilytykseen ei ole lukollisia kaappeja
- Tulostin liitetty tietokoneeseen salaamattomalla langattomalla yhteydellä

⚠ Fyysinen toimintaympäristö

- Toimitilojen avoimuus vaikeuttaa kybertoimintaympäristön fyysistä suojaamista
- Laitteen saastuminen muistitikun tai muistikortin avulla
- Etä- tai lähitunnistesirujen kopiointi (esim. kulkutunnisteissa) [24]
- Tiedon tai laitteen hukkaaminen tai varkaus
  → Laitteessa salasana, mutta kovalevy voi olla salaamaton
- Prosesseja tai vastuita ei ole määritelty
- Koti- ja etähoidon suojaaminen ja hallinta ei ole aina hoitavan organisaation käsissä
- Laitteiden saatavuusongelmat laajassa/pitkittyneessä kriisitilanteessa

⚠ Henkilökunta

- Kierretään suojausmekanismeja, jos laitteen tai ohjelmiston käytettävyys on huono
  → Estetään aikalukitus
  → Toisen käyttäjän tunnuksien käyttö
- Kiire vaikeuttaa tietoturvaohjeiden noudattamista
- Potilastiedon kerääntyminen sähköpostiin
- Ihmisten tekemät virheet (konfigurointivirheet, hoitohenkilökunnan virheet ym.)
- Kontrolloimaton salasanojen jakaminen, heikot salasanat, yhteiskäyttösalasanat
- Henkilökunta tarkoituksella tai vahingossa paljastaa tietoja
- Salasanalla suojattu ohjelmisto, johon erityishenkilöstö (hallinto/huoltohenkilökunta) ei tiedä tunnuksia [20]
  → Tekninen tuki ei pääse nopeasti korjaamaan ongelmaa tarpeen tullen
- Petokset ja huijaukset
  → Väärennetyt laskut
  → Tilataan kiireessä lisää suojainvarusteita, mutta tilaukset jäävät saamatta [17]

[20] Kyberturvallisuus sairaalajärjestelmissä: Osa 1, JYU 2017
[21] E-health systems in digital environments, JYU 2019
[22] Securing Wireless Infusion Pumps in Healthcare Delivery Organizations, NIST 2018
[23] Baxter, B.Braun infusion pumps among millions of devices implivated in Rip-ple20 cyber alert, Medtechdrive 2020
[24] Cyber security and resilience for Smart Hospitals, ENISA 2016

Hyvät käytännöt kyberhäiriöiden hallinnassa koronakriisin aikana

Henkilöstö

- Terveydenhuoltohenkilöstön tietoisuuden lisäämiskampanjat koronakriisin aikana: henkilöstö osaa ilmoittaa epäilyttävistä sähköposteista sekä toimia poikkeamatilanteessa ripeästi [25].
- Henkilöstön aktiivinen kyberturvallisuusaiheinen kouluttaminen.
- Aktiivinen tiedottaminen henkilöstölle kyberhäiriöistä.
- Henkilöstön kouluttaminen luotettavan internet-sivun osoitteenlaajennuspalvelun käyttöön, jos sähköposti sisältää lyhennetyn linkin [26].
- Tietojenkalastelun kohteeksi joutuneen henkilöstön kouluttaminen [26].
- Henkilöstön jäsenen saatua epäilyttävän tai oudon sähköpostiviestin tutulta lähettäjältä, ohjeistetaan häntä ottamaan yhteyttä lähettäjään muutoin kuin vastaamalla viestiin (esim. puhelimitse) [26].

Työasemat/tietojärjestelmät

- Järjestelmän vaarantuessa pysäytetään järjestelmän toiminnot (mikäli se on mahdollista). Irrotetaan haittaohjelmatartunnan saaneet koneet tietoliikenneverkosta ja ulkoisista asemista tai lääkinnällisistä laitteista. [25]

- Tietojenkalastelun torjuntaratkaisut käyttöön sähköpostiliikenteessä (esim. mustat listat, käyttäytymis-, sisältö- ja asiayhteyspohjaiset analysaattorit). Lisäksi tulee harkita liitetiedostojen, kuten suoritettavien tiedostojen, asennustiedostojen, komentorivitiedostojen, arkistotiedostojen jne. estämistä. [26]

Liiketoiminta

- Liiketoiminnan jatkuvuuden varmistaminen tehokkailla varmuuskopiointi- ja palautusmenettelyillä. Liiketoiminnan jatkuvuussuunnitelmat olisi laadittava aina, kun järjestelmän vika voi häiritä sairaalan ydinpalveluita. Palvelu- ja laitetoimittajan rooli on määriteltävä tarkasti tällaisissa tapauksissa. [25]

Lääkinnälliset laitteet

- Vaaratilanteisiin reagointi koordinoidaan laitteen valmistajan kanssa. Tehdään yhteistyötä toimittajien kanssa lääkinnällisten laitteiden tai kliinisten tietojärjestelmien häiriötapausten varalta. [25]

- Varaudutaan, että lääkinnällinen laite toimii myös ilman tietojärjestelmää.

- Lääkinnälliset laitteet segmentoidaan erilliseksi tietoliikenneverkon osaksi, johon hyökkääminen voidaan tehdä vaikeaksi.

- Prosesseissa ja ohjeissa on kuvattu, miten toimitaan ilman kriittisiä potilastietojärjestelmiä ja toimintaa on harjoiteltu.

Tietoverkot

- Aliverkkojen avulla tietoliikenne voidaan eristää ja/tai suodattaa, jolloin pääsyä verkon osasta toiseen voidaan rajoittaa tai se voidaan estää [25].

Etätyö

- Organisaatio ohjeistaa ja valvoo mitä työvälineitä ja laitteita kotona työskentelevät työntekijät käyttävät [27].

- Organisaatio huolehtii, että tietojärjestelmien ja sovellusten käyttövaltuudet myönnetään työntekijöille asianmukaisesti ja oikeaksi ajanjaksoksi [27].

- Organisaatio huolehtii, että tarpeettomiksi käyneet käyttövaltuudet poistetaan viipymättä [27].

- Organisaatiot tuntevat työntekijänsä, urakoitsijansa ja vapaaehtoistyöntekijänsä ja sen, kenelle on myönnetty pääsy mihin ja milloin [27].

[25] Cybersecurity in the healthcare sector during COVID-19 pandemic, Enisa 2020
[26] Phishing in Healthcare: How Not to Be a Victim Checklist, HIMSS 2020
[27] Healthcare Cybersecurity During COVID-19 and How to Pivot, HIMSS 2020

Kyberhäiriöihin varautuminen

"By failing to prepare, you are preparing to fail".

-Benjamin Franklin

Organisaation kyberturvallisuuteen liittyy mahdollisuus tapahtumiin, joita ei voi ennustaa ja niiden vaikutukset ovat ennakkoon tuntemattomia. Kyberturvallisuuden tilaan ja toiminnan jatkuvuuden varmistamiseen liittyy epämääräisyyttä ja epävarmuutta. Toiminnan jatkuvuuden varmistamiseen on laadittava varautumisen prosesseja, joilla toiminnan palautumiskykyä voidaan parantaa. Toimenpiteillä edistetään prosessien jatkuvuuden varmistamista toimintaympäristön häiriötilanteissa koko kriittisen infrastruktuurin alueella. [28]

Suomen kyberturvallisuusstrategiassa 2019 yhdeksi kolmesta strategisesta linjauksesta on nostettu kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio. [2]

[28] Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu, JYU 2020

Kyberturvallisuuden johtaminen

Valtioneuvosto nimitti vuoden 2020 helmikuussa valtion kyberturvallisuusjohtajaksi Rauli Paanasen. Rauli Paananen on Suomen historian ensimmäinen valtion kyberturvallisuusjohtaja. Kyberturvallisuusjohtajan tehtävä perustuu valtioneuvoston vuonna 2019 hyväksymään Suomen kyberturvallisuusstrategiaan, jonka mukaan kyberturvallisuusjohtajan tehtävänä on sovittaa yhteen kyberturvallisuuden kehittämistä, suunnittelua ja varautumista. Kyberturvallisuusjohtajan päätyönä on saada aikaiseksi kyberturvallisuuden kehittämisohjelma, joka selkeyttää hankkeiden ja tutkimuksen kokonaiskuvaa sekä konkretisoi kansallisia linjauksia. [29]

Kansallisen tason johtamisen lisäksi tarvitaan organisaatiotasoista kyberturvallisuuden järjestelmällistä johtamista. Organisaation kybertoimintaympäristön turvallisuutta ja luottamusta lisäävien toimenpiteiden aikaansaaminen on ensisijaisesti organisaation ylimmän johdon vastuulla. Yhdistämällä tarvittavat toimenpiteet ajatukseen toimintojen ja liiketoiminnan turvaamisesta kasvattaa niiden merkittävyyttä ja hyötyjä parantuneiden toimintaprosessien kautta koko organisaatiolle, sidosryhmille ja yhteiskunnalle. [28]

Kyberturvallisuuden johtamisessa yksi erittäin tärkeä tekijä on yhteinen ymmärrys johdon ja kyber- ja tietoturvallisuudesta vastaavien teknisten asiantuntijoiden välillä. On puhuttava samaa kieltä ja tähän ratkaisuna on muun muassa kyberturvallisuusasioiden esittely organisaation johdolle kertomalla ajankohtaisista riskeistä ja tilannekuvasta. Mitä enemmän kyberturvallisuuteen liittyvistä asioista puhutaan sitä tutumpia ne johdolle ovat.

Osana Digiturvaviikon (26.-30.10.2020) tukimateriaaleja julkaistiin asiankirja: **Digiturvan hyvät käytännöt johdolle ja ICT:n sekä digiturvan asiantuntijoille — tarkistuslista (VAHTI)**. Tarkistuslista sisältää asioita, joiden tulisi olla osa organisaation toiminnan arkea. Lisäksi asiakirjan loppuun on koottu linkkejä aihepiiriin liittyviin viranomaisohjeisiin.

Riskienhallinta

Riskienhallinnan avulla pyritään tunnistamaan, arvioimaan ja hallitsemaan organisaation tavoitteiden saavuttamista uhkaavia tekijöitä [30]. Tämä on keskeistä kyberhäiriöihin ennalta varautumisessa ja toiminnan jatkuvuuden varmistamisessa normaaliolojen häiriö- ja erityistilanteissa sekä poikkeusoloissa. Kyberuhkat voivat olla laadultaan joko tahallisia, tahattomia tai ympäristöstä johtuvia [31]. Tahalliset kyberuhkat voidaan jakaa kohdistettuihin ja kohdistamattomiin hyökkäyksiin sen mukaan, onko organisaatio valikoitunut rikoksen kohteeksi tarkoituksella vai sattumalta.

Rikosten tilannetorjunnalla voidaan vaikeuttaa rikostilaisuuksia ja pyrkiä näin välttämään organisaation joutumista kyberhyökkäyksen kohteeksi. Tilannetorjunnan taustalla vaikuttaa kolme teoriaa, rationaalisen valinnan teoria, esiintymisrakenteen teoria ja rutiinitoimintojen teoria. Rationaalisen valinnan teoria olettaa rikoksentekijän arvioivan teon hyötyjä ja riskejä sekä sen vaatimia ponnistuksia. Esiintymisrakenteen teoria näkee rikosten kasautuvan ajallisesti ja paikallisesti. Rutiinitoimintojen teoria puolestaan korostaa rikokseen tarvittavan kolme asiaa, jotka ovat motivoitunut tekijä, otollinen kohde ja riittämätön valvonta. [32]

Kyberuhkien tunnistamisessa ja näihin liittyvien rikostilaisuuksien arvioimisessa voidaan hyödyntää erilaisia riskienarviointitekniikoita, joissa lähestymistapa voi olla joko laadullinen tai määrällinen [31]. Käytettävistä riskienarviointitekniikoista annetaan esimerkkejä kansainvälisessä riskienhallintajärjestelmästandardissa SFS-EN IEC 31010 ja tietoturvallisuuden riskienhallintajärjestelmästandardissa SFS-ISO/IEC 27005 sekä valtionhallinnon ohjeessa riskienhallintaan Vahti-ohje 22/2017. Ohjeeseen sisältyy Excel-pohjainen **riskienhallintatyökalu**. VAHTI-ohjeen liitteistä löytyy myös hyviä esimerkkejä riskien luokittelusta, riskimatriiseista ja vaikutuksen arvioinnista. [33]

Riskien tunnistaminen				Riskianalyysi		Riskin merkityksen arviointi		Riskin käsittely	
Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua toteutuessa):	Todennäköisyys	Vaikutus	Riskin suuruus (T x V)	Toimenpide-tarpeet riskin käsittelylle (vakavuus/ sietokyky)	Toimenpide-ehdotukset riskin käsittelylle	Toimenpiteid vapaamuotoi (sanallinen) kuvaus
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	0 Ei arvioitu	

Ote VAHTI-ohjeen riskienhallintatyökalusta

[29] Valtion kyberturvallisuusjohtaja on nimitetty, valtioneuvosto 2020
[30] SFS-ISO 31000:2018 Riskienhallinta. Ohjeet, Suomen standardisoimisliitto SFS 2018 (2.painos)
[31] SFS-ISO/IEC 27005:2018 Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta, Suomen standardisoimisliitto SFS 2018 (3.painos)
[32] Tilannetorjunta ja rationaalisen valinnan teorian järki, Jukka-Pekka Takala, Haaste 4/2011
[33] VAHTI 22/2017 Ohje riskienhallintaan, Valtiovarainministeriö 2017

Suositukset nostavat tekniikkoina muun ohella esiin yhteiset aivoriihet ja esilaaditut tarkistusluettelot sekä arviointia ohjaavat vikapuu-, tapahtumapuu- ja rusettianalyysit. Johdettuun keskusteluun perustuvat aivoriihet ja eri tarkoituksiin tuotetut valmiit tarkistusluettelot voivat auttaa tunnistamaan yleisten uhkatekijöiden joukosta omaan toimintaan liittyviä haitallisia tapahtumia. Aivoriihessä tarkoituksena on, että keskustelun osapuolet ajatuksia ja tietoa vaihtamalla rakentavat yhteistä käsitystä organisaation uhkaympäristöstä. Tarkistusluettelot pyrkivät toimimaan keskustelun ja ajatusten herättelijöinä nostamalla esiin varautumiseen tai sen tasoon liittyviä seikkoja. [34]

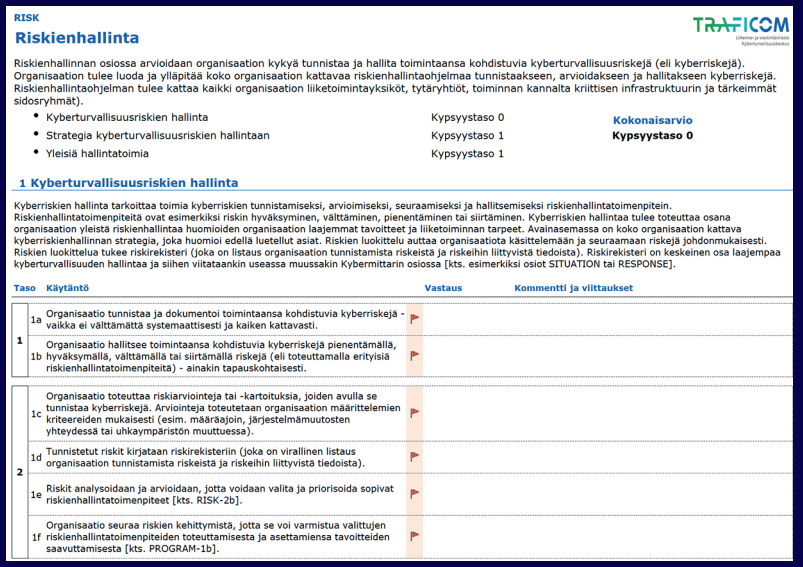
Haitallisten tapahtumien kehityskulkuun vaikuttavia syitä on mahdollista kartoittaa vikapuuanalyysein. Vikapuuanalyysissä tarkastellaan, mitkä kaikki tekijät voivat johtaa haitallisen tapahtuman toteutumiseen ja edellyttävätkö ne toteutuakseen useamman tekijän yhtäaikaista olemassaoloa. Tapahtumapuuanalyysi keskittyy vikapuuanalyysistä poiketen tunnistamaan haitallisesta tapahtumasta koituvia seurauksia. Tapahtumapuuanalyysi ei ota kantaa haitallista tapahtumaa edeltäviin tekijöihin. [34]

Riskienarviointitekniikoista rusettianalyysi sitoo vika- ja tapahtumapuuanalyysin yhteen kuvaten sekä haitalliseen tapahtumaan johtavat syyt että tästä aiheutuvat seuraukset. Rusettianalyysi tunnistaa edellä mainittujen tekniikoiden lisäksi kyberuhkien torjumiseksi, havaitsemiseksi ja rajoittamiseksi tehtyjä toimenpiteitä. Rusettianalyysiin koostettuja tuloksia on mahdollista jatkokäsitellä seuraus-todennäköisyysmatriisilla. Matriisi tuo käsittelyyn mukaan riskin todennäköisyyden ja vaikutusten suuruuden merkityksen kyberuhkan riskitasoon. [34]

Pontta riskien arvioimiseen ja niiden käsittelyyn luo sekä terveydenhuollon toimijoihin kohdistuvat lakisääteiset velvoitteet että toiminnanosallisten kyberturvallisuudelle asettamat vaatimukset ja odotukset. Terveydenhuollon toimijoiden edellytetään esimerkiksi tiedonhallintalain nojalla selvittävän olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittavan tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti [35]. Tieturvallisuustoimenpiteiden on oltava riittävät suojattavan kohteen arvoon ja tunnistetun uhkan suuruuteen nähden.

Riskien käsittelyä tunnistettujen riskien varalle toteutettavista hallintakeinoista ohjaa käsitteet riskinottohalusta ja riskinkantokyvystä. Riskinottohalu kuvaa, minkä verran organisaatio on valmis ottamaan riskiä tavoitteisiinsa pyrkiessään, kun taas riskinkantokyky kertoo, kuinka paljon organisaatio pystyy sietämään epävarmuutta menettämättä toimintakykyään. Riskien hallintakeinot voidaan yleisesti jakaa riskin muokkaamiseen, säilyttämiseen, välttämiseen ja jakamiseen [31]. Riskin käsittely voi aiheuttaa uusia riskejä. Jäljelle jäävistä riskeistä käytetään nimitystä jäännösriski.

Kyberturvallisuuskeskuksen kehittämä Kybermittari, on kansallinen kyberturvallisuuden riskienhallinnan arviointikehys. Sitä voidaan hyödyntää niin yhteiskunnalle kriittisten toimintojen kuin liiketoiminnankin jatkuvuuden arviointiin. Kybermittariin kuuluu itsearviointityökalu, joka kattaa kyberturvallisuuden riskienhallinnan yleisimmät osa-alueet, ja jonka tuloksena syntyy raportteja organisaation kypsyystasosta. Työkalu sopii organisaation toiminnan säännölliseen seuraamiseen ja kehittämiseen.



RISK

Riskienhallinta

TRAFICOM

Riskienhallinnan osiossa arvioidaan organisaation kykyä tunnistaa ja hallita toimintaansa kohdistuvia kyberturvallisuusriskejä (eli kyberriskejä). Organisaation tulee luoda ja ylläpitää koko organisaation kattavaa riskienhallintaohjelmaa tunnistaakseen, arvioidakseen ja hallitakseen kyberriskejä. Riskienhallintaohjelman tulee kattaa kaikki organisaation liiketoimintayksiköt, tytäryhtiöt, toiminnan kannalta kriittisen infrastruktuurin ja tärkeimmät sidosryhmät).

- Kyberturvallisuusriskien hallinta — Kypsyystaso 0
- Strategia kyberturvallisuusriskien hallintaan — Kypsyystaso 1
- Yleisiä hallintatoimia — Kypsyystaso 1

Kokonaisarvio
Kypsyystaso 0

1 Kyberturvallisuusriskien hallinta

Kyberriskien hallinta tarkoittaa toimia kyberriskien tunnistamiseksi, arvioimiseksi, seuraamiseksi ja hallitsemiseksi riskienhallintatoimenpitein. Riskienhallintatoimenpiteitä ovat esimerkiksi riskin hyväksyminen, välttäminen, pienentäminen tai siirtäminen. Kyberriskien hallintaa tulee toteuttaa osana organisaation yleistä riskienhallintaa huomioiden organisaation laajemmat tavoitteet ja liiketoiminnan tarpeet. Avainasemassa on koko organisaation kattava kyberriskienhallinnan strategia, joka huomioi edellä luetellut asiat. Riskien luokittelu auttaa organisaatiota käsittelemään ja seuraamaan riskejä johdonmukaisesti. Riskien luokittelua tukee riskirekisteri (joka on listaus organisaation tunnistamista riskeistä ja riskeihin liittyvistä tiedoista). Riskirekisteri on keskeinen osa laajempaa kyberturvallisuuden hallintaa ja siihen viitataankin useassa muussakin Kybermittarin osiossa [kts. esimerkiksi osiot SITUATION tai RESPONSE].

Taso	Käytäntö	Vastaus	Kommentti ja viittaukset
1	1a Organisaatio tunnistaa ja dokumentoi toimintaansa kohdistuvia kyberriskejä - vaikka ei välttämättä systemaattisesti ja kaiken kattavasti.		
	1b Organisaatio hallitsee toimintaansa kohdistuvia kyberriskejä pienentämällä, hyväksymällä, välttämällä tai siirtämällä riskejä (eli toteuttamalla erityisiä riskienhallintatoimenpiteitä) - ainakin tapauskohtaisesti.		
2	1c Organisaatio toteuttaa riskiarviointeja tai -kartoituksia, joiden avulla se tunnistaa kyberriskejä. Arviointeja toteutetaan organisaation määrittelemien kriteereiden mukaisesti (esim. määräajoin, järjestelmämuutosten yhteydessä tai uhkaympäristön muuttuessa).		
	1d Tunnistetut riskit kirjataan riskirekisteriin (joka on virallinen listaus organisaation tunnistamista riskeistä ja riskeihin liittyvistä tiedoista).		
	1e Riskit analysoidaan ja arvioidaan, jotta voidaan valita ja priorisoida sopivat riskienhallintatoimenpiteet [kts. RISK-2b].		
	1f Organisaatio seuraa riskien kehittymistä, jotta se voi varmistua valittujen riskienhallintatoimenpiteiden toteuttamisesta ja asettamiensa tavoitteiden saavuttamisesta [kts. PROGRAM-1b].		

Ote Kybermittarin itsearviointityökalusta

[34] SFS-EN IEC 31010:2019 Riskienhallinta. Riskien arviointimenetelmät, Suomen standardisoimisliitto SFS 2019 (2.painos)
[35] Laki julkisen hallinnon tiedonhallinnasta, Finlex 2019

Kyberturvallisuuskeskuksen laatiman ohjeen mukaan Kybermittarin käytön hyötyjä ovat [36]:

- Kriittisten palveluiden ja riskien tunnistaminen
- Organisaation ja toimialan tilannekuvan muodostaminen
- Vertailu toimialatuloksiin ja parhaisiin käytäntöihin
- Kehitysalueiden tunnistaminen ja toimien kohdistaminen.

Laajamittaisesti käytettynä mittari tukee kansallisella tasolla tilannekuvan muodostumista, viranomaistoimintaa ja resurssien oikeaa kohdentamista sekä kansallista kyberturvallisuusstrategiaa [37].

Kybermittari ja sen käyttöohjeet löytyvät osoitteesta www.kyberturvallisuuskeskus.fi/fi/kybermittari

Vuoden 2020 syyskuussa julkaistu **valtiovarainministeriön Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltumisesta** antaa hyviä ohjeita tietoaineistojen ja tietojärjestelmien turvaamiseen.

Riskienhallinnan yleisiä vaatimuksia kuvaillaan oppaassa näin [38]:

- Onko viranomainen tunnistanut ja dokumentoinut kaiken tiedon ja kaikki tietojärjestelmät, joista se on vastuussa?
- Onko näitä ylläpitävät ja käyttävät avainhenkilöt tunnistettu?
- Onko tietoihin, tietojärjestelmiin ja avainhenkilöihin mahdollisesti kohdistuvat uhkatekijät tunnistettu?
- Onko tiedoille ja tietojärjestelmille laadittu vaikutusanalyysi, jonka perusteella on mahdollista arvioida riskienhallintatoimenpiteiden oikeasuhtaisuus?
- Ovatko riskienhallintatoimenpiteet oikeasuhtaiset riskin realisoitumisen vaikutukseen ja todennäköisyyteen nähden?
- Ylläpidetäänkö riskirekisteriä ja arvioidaanko riskienhallintatoimenpiteiden toimivuutta säännöllisesti?

Myös **Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille** auttaa arvioimaan organisaation kykyä suojata salassa pidettävää tietoa. Ohje sisältää turvallisuusjohtamisen, fyysisen turvallisuuden ja teknisen tietoturvallisuuden osa-alueet. [39]

[36] Kybermittari, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020
[37] Kybermittari. Kansallinen kyberturvallisuuden arviointimalli. Käyttöohje, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020
[38] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, valtioneuvosto 2020
[39] Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille, puolustusministeriö

Jatkuvuudenhallinta

Tietoturva, varautuminen ja jatkuvuudenhallinta ovat asioita, jotka olisi syytä ottaa kiinteäksi osaksi organisaation toimintaa, prosesseja ja palveluja [3]. VAHTI-ohjeen 2/2016 Toiminnan jatkuvuuden hallinta, mukaan jatkuvuussuunnittelu käsittää toimia, joiden tarkoitus on toimintaa haittaavien tapahtumien vaikutuksen ja keston minimoiminen. Häiriötilanteissa toimimista ja toipumista parannetaan suunnitelman mukaisin toimenpitein ja varajärjestelyin. ”Jatkuvuussuunnittelu sisältää myös suunnitelmat, joissa kuvataan johtaminen, vastuut ja toimenpiteet, joiden mukaan toimintoja voidaan jatkaa erilaisissa häiriötilanteissa.” Tämä suunnittelu on tehtävä kaikissa kriittisissä toiminnoissa. Myös palveluntuottajien jatkuvuus- ja toipumissuunnitelmien on oltava linjassa oman jatkuvuussuunnittelun kanssa häiriötilanteista toipumisen varmistamiseksi. [40] Jatkuvuus on pystyttävä turvaamaan myös sellaisissa tilanteissa, kun sopimuskumppani ei selviydy sovituista velvoitteista [41].

Riippuvuus tietojärjestelmistä kasvaa terveydenhuollonkin ympäristöissä edelleen. Tästä huolimatta poikkeustilanteessa on pystyttävä toimimaan myös ilman niitä. Erityisesti potilasturvallisuuden kannalta kriittisillä osastoilla on oltava **jatkuvuussuunnitelma**, joka ottaa huomioon tietojärjestelmien häiriöt ja katkokset. Suunnitelmassa pitäisi huomioida esimerkiksi henkilöresurssien käyttö tiedon siirtoon tarpeen vaatiessa, työvuoromuutoksiin varautuminen, toimintojen priorisointi sekä valmius korvaavien laitteiden, järjestelmien ja papereiden käyttöön. [19] Oheisessa taulukossa otteita jatkuvuussuunnitelmista.

Potilastietojärjestelmä käyttökatkon tapahtuessa	Tietoliikenne- ja viestintätekniikkapalvelut
Tietohallinto tiedottaa katkoksesta sähköpostilla, puhelimitse ja/tai intranetin kautta.	Verkkoa valvotaan palveluna hankitulla valvontajärjestelmällä.
Hoitohenkilöstö odottaa n.15 minuuttia, jonka jälkeen toimitaan osaston oman jatkuvuussuunnitelman mukaan.	Erityisen kriittiset toiminnot: • leikkaukset, tehohoito, päivystys • kuvantaminen ja laboratoriotoiminnot • elvytyshälytykset, lääkitystiedot.
Potilaiden henkilö-, ilmoittautumis-, poistumis- ja käyntitiedot kirjataan tarkoitusta varten tehdyille paperilomakkeille.	Palveluntoimittajan huoltopalvelusopimukset yksittäisen komponentin vikaantumisen varalla.
Potilaskertomukset voidaan kirjoittaa työaseman tekstinkäsittelyohjelmaan.	Verkon keskeiset komponentit kahdennettu.
Vuodeosastolla määräykset, hoitokertomustiedot ym. käsin hoitosuunnitelmalomakkeelle.	Tietohallinnon ja kliinisten yksiköiden valmiussuunnitelmien välillä ei relaatiota, yksiköt päättävät toiminnastaan.
Digisanelu ei mahdollista katkon aikana. Katkon ylittäessä 2 tuntia siirrytään kasettisaneluihin.	
Jatkuvuussuunnitelman liitteessä suorat osoitteet laboratorio- ja kuvantamispalveluiden järjestelmään. Näitä voidaan käyttää, jos vika rajoittuu esim. potilastietojärjestelmään.	
Katkon jälkeen tiedot siirretään tietojärjestelmään.	

Otteita jatkuvuussuunnitelmista [19]

Organisaatioissa tulisi varmistaa, että jatkuvuussuunnitelma on tehty, se kattaa koko ICT:n eikä esimerkiksi vain terveydenhuollon laitteita, että se on otettu käyttöön ja että suunnitelman mukaisia toimia myös harjoitellaan. Suunnittelussa olisi syytä ottaa huomioon kyberhyökkäykset, myös koronakriisin tai vastaavien kriisien varjolla tehdyt, ja että häiriöt voivat olla pitkäkestoisia. Jatkuvuussuunnitelmaa on päivitettävä määrätietoisesti, koska tieto saattaa vanhentua nopeastikin.

Kuntaliiton ja Huoltovarmuuskeskuksen KUJA-projekteissa on ollut tavoitteena kunnallisen varautumisen ja jatkuvuudenhallinnan tukeminen ja kehittäminen. Projektin työkaluista löytyy muun muassa toimintakorttimalli häiriötilanteisiin, varautuminen tilannejohtamiseen, ja arviointimalli. **KUJA-arviointimalli** on hyvä apuväline organisaation varautumisen ja jatkuvuudenhallinnan kypsyyden kartoittamiseen ja systemaattisen kehittämisen rakentamiseen. Kypsyyden kartoitus on nopea ja helppo aloittaa KUJA-pikatestillä. [42]

Nro.	Arviointikysymys	Arvio nykytilasta: Kunnossa	Osittain kunnossa / selvitettävä	Ei kunnossa
1.	Varautumisen ja jatkuvuudenhallinnan perusteet ja vaatimukset on tunnistettu (esim. lainsäädäntö, sidosryhmävaatimukset). Varautumisen ja jatkuvuudenhallinnan toimintamalli on kuvattu sekä ohjeistettu. Varautumiseen liittyvät vastuut ja roolit on määritelty kirjallisesti.			
2.	Varautumisen ohjaamiseen ja kehittämiseen on varattu riittävästi resursseja. Minimissään organisaatiotason varautumisen koordinaattori (vast.) on nimetty, koulutettu sekä työaikaa on osoitettu koordinoimisen toteuttamiseksi.			
3.	Varautumisen ja jatkuvuudenhallinnan kaikki keskeiset suunnitelmat ja toimintakortit on laadittu/päivitetty kolmen vuoden sisällä ja organisaation ylin johto on ne hyväksynyt.			
4.	Käytettävissä on selkeä toimintamalli vakavissa häiriötilanteissa avainhenkilöiden hälyttämiseksi, toiminnan johtamiseksi sekä kriisiviestintään.			
5.	Toimintamallit ja suunnitelmat ovat helposti saatavilla ja henkilöstö on perehtynyt niihin. Toiminnan kannalta keskeiset henkilöt kaikilla tasoilla on perehdytetty toimintamallien ja suunnitelmien keskeisiin kohtiin.			
6.	Kaikissa tilanteissa ylläpidettävät kriittiset toiminnot ja tehtävät on tunnistettu. Myös näiden ylläpitämiseen liittyvät kriittiset järjestelmät, toiminnot ja tehtävät on tunnistettu ja määritetty riittävät hallintakeinot.			
7.	Koulutus ja harjoittelu on suunnitelmallista sekä säännöllistä. Koulutuksia ja harjoituksia järjestetään organisaation kaikilla tasoilla huomioiden henkilöiden roolit sekä tehtävät osana organisaation varautumista. Koulutuksien ja harjoituksien toteutumista seurataan.			
8.	Riskienhallinnan perusteet on määritelty ja riskienhallinnassa on [illegible]			

Ote KUJA-pikatestistä

Hyviä vinkkejä jatkuvuudenhallintaan ja jatkuvuussuunnitelman runko löytyvät VAHTI-ohjeesta 2/2016; Toiminnan jatkuvuuden hallinta. [40] Myös SOPIVA-hankkeen suosituksia voi käyttää toiminnan jatkuvuuden hallinnan tarkistuslistana [43].

[40] Toiminnan jatkuvuuden hallinta, valtioneuvosto 2016
[41] Sopimusperusteinen varautuminen: Ohje sosiaali- ja terveydenhuollon toimijoille, STM 2019
[42] Kuntien jatkuvuudenhallintaprojektit KUJA 1 ja 2, Kuntaliitto 2018
[43] Toiminnan on aina jatkuttava, SOPIVA-hanke Huoltovarmuuskeskus

Vastuumatriisi

Tärkeä osa varautumista on vastuiden jakaminen omassa organisaatiossa sekä sidosryhmien ja yhteistyökumppanien kanssa. Häiriötilanteiden päätöksentekoon ja toimintaan liittyvät vastuut on tärkeää sopia selkeästi niin, että häiriötilanteen käsittelyssä on mukana riittävästi asiantuntemusta. Olisi hyvä nimetä myös varahenkilöt häiriötilanteita varten sekä mahdollisesti päivystys- ja varallaolohenkilöstöä, ja sopia miten tarpeen tullen heidät saadaan kutsuttua paikalle. [44] On myös huomioitava henkilöstön jaksaminen häiriötilanteen pitkittyessä [42]. Häiriötilanteen sattuessa normaalin työajan ulkopuolella voidaan keinona varautumiseen luoda yhden vastuuhenkilön sijaan useita henkilöitä käsittävä rinki, josta tavoitella asianomaisia. Myös ulkoistettu tietoturvavalvomopalvelu voidaan tällaisten tilanteiden varalta valtuuttaa tekemään itsenäisiä päätöksiä, ellei organisaation omia vastuuhenkilöitä tavoiteta.

Vastuunjaon yksiselitteiseen dokumentointiin voidaan käyttää **vastuumatriisia**, esimerkiksi RACI-matriisin muodossa. Vastuumatriisissa on tärkeää olla huomioituna henkilökunnan osaaminen, resurssit, välineet ja laitteet. Pohjana voidaan käyttää Kuntaliiton AKUSTI-foorumin tuotoksena syntynyttä Excel-pohjaa SOTE-ICT-skenaarioiden RACI-matriisi vastuualueiden määrittelyyn [45], jossa on valmiiksi listattuna tietohallintomallin mukaisia yleisiä tehtäviä, ja esimerkinomaisia vastuurooleja.

	Tietohallintojohtaja	Työntekijä	Kokonaisarkkitehti	ICT-palvelujen vastuuhenkilö	IT-hankintapäällikkö	IT-laatupäällikkö	Tietoturvapäällikkö	Palvelutuottajan edustaja	
Toiminta häiriötilanteissa									
Varautumisen kustannukset	**A**		**I**		**R**		**C**		
Poikkeamailmoitusten vastaanotto		**I**		**A, R**			**I**	**C**	
Häiriöihin varautuminen									
Häiriöiden luokittelu									
Kutsuu yli- /hätätyöntekijät									
Viestintä									
Organisaation toiminnan rajaus									
Toipumis- ja varamenettelyt									
Lokitietojen hallinta									
Tutkintapyyntö									

Taulukossa poikkeamanhallinnan RACI-matriisihahmotelma, jossa muutamia rooleja ja vastuita esimerkkeinä. Matriisi on luotu poimien rooleja AKUSTI-foorumin Sote-ICT-skenaarioiden RACI-matriisi vastuualueiden määrittely -taulukosta [45], sekä Valtionvarainministeriön julkaisuja 8/2017: Tietoturvapoikkeamatilanteiden hallinta -ohjeen käsittelyvastuista [44].

Tietoturvapoikkeaman käsittelykyvyn muodostamisesta, ja mm. käsittelyvastuista, on tietoa Valtionvarainministeriön julkaisu 8/2017: Tietoturvapoikkeamatilanteiden hallinta -ohjeessa [44]. Ohessa oleva RACI-matriisin esimerkkihahmotelma häiriötilanteita varten on luotu yhdistellen edellä mainittuja dokumentteja.

RACI-matriisi muodostuu seuraavista käsitteistä [46]:

- **R**, vastuullinen, joka suorittaa tehtävän itse tai osana tiimiä
- **A**, vastaava, tekee päätöksen ja valvoo tehtävän valmistumista
- **C**, asiantuntija tai neuvoja
- **I**, tiedotettava

R-henkilöitä on oltava kutakin tehtävää kohti ainakin yksi, A-henkilöitä tasan yksi, ja C- ja I-henkilöitä valinnainen määrä.

	Rehtori	Hallintojohtaja	Henkilöstöpäällikkö	Opintohallinnon päällikkö	Tietohallintojohtaja	Asiakirjahallinnosta vastaava	Tilahallintopäällikkö	Johtava lakimies	Talouspäällikkö	Viestintäpäällikkö	Kehityspäällikkö	Turvallisuuspäällikkö	Tietoturvapäällikkö	Yksikön johtaja	Yksikön tietoturvavastaava	Tietotekninen asiantuntija	Palvelun/järjestelmän/tied on omistaja
Tietoturvalinjaukset																	
Tietoturvapolitiikan valmistelu		A			S								R				
Tietoturvatavoitteet ja niitä vastaavat mittarit		A			S								R				
Tietoturvallisuuden ohjaaminen																	
Yleiset tietoturvasäännöt ja -ohjeet		A			C								R		I		
Palvelukohtaiset tietoturvasäännöt ja -ohjeet					A								S				R
Henkilöstöä koskevat tietoturvallisuuteen liittyvät määräykset		A	R					C					S	I			
Tietoturvallisuuden yleinen organisointi		A			C								R		I		
Tietoriskienhallinnan organisointi		A			C							C	R		I		I
Vaatimustenmukaisuuden varmistaminen																	
Lainsäädännön seuranta		A						C					R				

Esimerkki tietoturvatehtävien vastuunjaosta löytyy myös FUSEC-työryhmän Ohje tietoturvavastuudokumentin laatimiseen-dokumentista [47].

[44] Tietoturvapoikkeamatilanteiden hallinta, valtioneuvosto 2017
[45] Sote-ICT-skenaarioiden RACI-matriisi vastuualueiden määrittelyyn, Liite 2, Excel, Kuntaliitto 2019
[46] Responsibility assignment matrix, Wikipedia
[47] Ohje tietoturvavastuudokumentin laatimiseen, FUCEC 2012

Kriisiviestintä

Viestintää tarvitaan aina tavanomaista enemmän häiriötilanteessa. Pitää olla valmius vastata nopeasti eri tahojen tiedontarpeisiin ja viestinnän pitää lisäksi olla avointa, ymmärrettävää ja luotettavaa. Viranomaisten ja viestinnän koordinoinnin tärkeys korostuu moniviranomaistilanteissa. Sitä suuremmat vaatimukset kohdistuvat viestintään, mitä vakavammasta väestön turvallisuutta tai terveyttä uhkaavasta häiriöstä on kysymys. Viestinnän on oltava hyvin selkeää ja yhdenmukaista. [48]

Viestintä on aina osa häiriötilanteen johtamista. Viestinnän henkilöstömitoitus tulisi suunnitella riittäväksi myös mahdolliseen ympärivuorokautiseen tarpeeseen. Viestinnässä on otettava huomioon sekä sisäinen, että ulkoinen viestintä. Häiriötilanteiden viestintään pitää varautua etukäteen. Organisaatiossa on oltava viestintäsuunnitelma häiriötilanteita varten. Siinä kuvataan sekä sisäisen että ulkoisen viestinnän organisointi ja vastuut organisaatiossa sekä yhteistyötoimintamalli tärkeimpien sidosryhmien sekä median kanssa. Häiriötilanteiden viestintäsuunnitelmaan kirjataan myös viestinnän kanavat häiriötilanteissa. Riippuen häiriötilanteesta myös viestinnän kohderyhmiä on syytä pohtia etukäteen erilaisten skenaarioiden avulla, kuten pandemia. Viestintäsuunnitelman liitteenä voi olla esimerkiksi käytännönläheisiä ohjeita, toimintakortteja, tarkistuslistoja, valmiita mallipohjia ja yhteystietoja. [48]

Kriisiviestinnän suunnitelman toimivuutta voi testata käytännössä esimerkiksi osana toiminnallista kyberturvallisuusharjoitusta.

[48] Valmius- ja jatkuvuudenhallintasuunnitelma: Ohje sosiaali- ja terveydenhuollon toimijoille, STM 2019
[49] Vesihuoltolaitoksen häiriötilanne- ja kriisiviestintäohje, huoltovarmuusorganisaatio vesihuoltopooli 2019

Kriisiviestintäsuunnitelman tarkistuslista

SKENAARIOT

- Millaisia kriisejä terveydenhuollon organisaatio voi kohdata?
  → Esim. potilastietojen joutuminen vääriin käsiin, potilasturvallisuuden vaarantuminen, mainekohu, toiminnan hidastuminen
- Miten tieto tapahtuneesta saadaan eri skenaarioissa?

TYÖNJAKO

- Kuka on vastuussa toiminnasta ja viestinnästä eri skenaarioissa?
- Kuka on viestimille annettavien tiedotteiden nimetty vastuuhenkilö?
- Ketkä ovat vastuullisten varahenkilöt?
- Miten vastuulliset ja varahenkilöt tavoitetaan: missä yhteystietoja säilytetään?
- Keneen otetaan yhteys työ- ja virka-ajan ulkopuolella? Mikä on hälytysjärjestys?

SIDOSRYHMÄT

- Ketkä ovat tärkeimmät terveydenhuollon organisaation ulkopuoliset toimijat eri tilanteissa?
- Miten heihin otetaan yhteyttä?
- Mikä on työnjako eri osapuolten välillä?

KANAVAT

- Mikä on avainhenkilöiden hälytyskanava
  → Esim. ennalta sovittu pikaviestipalvelu, tekstiviestiryhmä
- Mitkä ovat tiedonjakokanavat organisaation sisällä?
- Mitkä ovat kanavat ulkoisessa viestinnässä?
  → Esim. organisaation omat verkkosivut, tekstiviestipalvelut
- Kenellä on kanavien käyttötaidot ja -oikeudet?

POHJAT

- Tiedotepohjat valmiiksi eri skenaarioita varten.
- Valmiit yhteystietolistat eri skenaarioita varten.

JÄLKIHOITO

- Miten eri skenaariot päättyvät viestinnän näkökulmasta?
- Mitkä toiminnot lopettavat aktiivivaiheen? [49]

Hankintojen tietoturva

Uuden tietojärjestelmän liittäminen osaksi organisaation toimintaa luo uusia mahdollisuuksia, mutta myös uhkia. Siksi jo järjestelmien ja palveluiden vaatimusmäärittelyvaiheessa on tunnistettava niiden tietoturvallisuuden kannalta keskeiset asiat, määriteltävä kriittisyys ja arvioitava riskit. Riskiarvio tehdään käyttötarkoituksen ja toimintaympäristön pohjalta. Toimintaympäristöön vaikuttavat mm. lainsäädäntö, käyttäjät, ulkoiset vaatimukset, käsiteltävät tietoaineistot sekä liittymät, riippuvuudet ja tietovirrat muihin järjestelmiin. Riskiarvion, kriittisyyden ja edellytetyn tietoturvan tason perusteella tunnistetaan tietoturvavaatimukset koko elinkaaren ajalle. Vähimmäisvaatimukset tietoturvalle on asetettu tiedonhallintalaissa. [38]

Hankintoja tehdessä kannattaa harkita vain sellaisten valmistajien ratkaisuja, jotka ottavat kyberturvallisuuden huomioon [50]. Valmistajalta voi vaatia voimassa olevaa ISO 27001 sertifiointia. Tietoturva- ja tietosuojavaatimukset on syytä mainita myös sopimusehdoissa, niin että ne kattavat koko kohteen elinkaaren hankinnasta poistoon [3]. Sopimuksissa tulisi varsinaisten sopimuskumppaneiden lisäksi myös niiden alihankintayrityksiltä, ja muilta verkostokumppaneilta, edellyttää jatkuvuuden hallinnan suositusten noudattamista [43]. On myös tärkeää sopia kustannuksista, joita suositusten noudattamisen todentamisesta aiheutuu. Huoltovarmuuskeskuksen SOPIVA-suosituksia ja mallilausekkeita voi käyttää apuna sopimusten laatimisessa. Alihankintaketjut voivat usein olla mutkikkaita, ja esimerkiksi tietovarantojen fyysinen sijainti saattaa tulla myöhemmin esiin yllätyksenä. Nämä olisi syytä selvittää jo ennen sopimusten laatimista. Sopimuksessa olisi myös hyvä ottaa huomioon, kuinka toimitaan järjestelmän toimittajan tai palveluntuottajan mahdollisessa konkurssitilanteessa.

Myös palvelun tai tietojärjestelmän käytöstä tallentuva tietosisältö on selvitettävä ennen hankintaa, jotta tietoturva- ja tietosuojavaatimukset saadaan määriteltyä oikein [51]. Hankintavaiheen tietoturvavaatimuksilla voi olla myös merkittävä vaikutus elinkaaren aikaisiin kustannuksiin. Huoltovarmuuskeskuksen Kyber-terveys-hankkeessa luotu hankintojen tietoturvavaatimustaulukko, Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset [52], on hyvä riskienhallintatyökalu terveydenhuollon hankintoihin. Tietoturvavaatimukset edellyttävät, että organisaation muidenkin rakenteiden on oltava kunnossa. Näitä ovat muun muassa hankinnan kohteen vastuiden määrittely, vaatimusten sovittamisen edellyttämä tietoturvapalvelu, muutoshallintamenettelyt ja projektimalli, jossa tietoturva on mukana hankinnassa alusta alkaen. [51]

ID	Kategoria	Vaatimus	Vaihe	Vastuu V=Vendor C=Customer	Toteutusesimerkki	Pakollinen = M
5002	Käyttäjätunnukset & todentaminen	Toimittajan järjestelmässä on oltava mahdollisuus kehottaa käyttäjää muuttamaan salasana ajoissa ennen sen voimassaolon päättymistä. Koskee paikallisia käyttäjätilejä.	Koko elinkaari	V	Esimerkiksi kehotus ennen voimassaolon päättymistä ylläpitäjän määritteleminä päivinä	M
5003	Käyttäjätunnukset & todentaminen	Toimittajan tulee varmistaa, että paikallisille tunnuksille ei käytetä oletussalasanoja.	Koko elinkaari	V	Esimerkiksi tämä voidaan mainita kovennusohjeessa.	M
5004	Käyttäjätunnukset & todentaminen	Asiakkaan on varmistettava, että loppukäyttäjillä on yksilölliset identiteetit. Toimittajan on varmistettava, että yksilöllisyys säilyy järjestelmässä.	Koko elinkaari	C+V	Esimerkiksi käyttäjän identiteetti ei voi perustua vain sähköpostiosoitteeseen.	M
5005	Käyttäjätunnukset & todentaminen	Toimittajan on varmistettava, että Asiakkaan tunnistamat käyttäjäryhmät ja käyttäjien roolit toteutetaan järjestelmässä yksikäsitteisesti. Toimittajan täytyy varmistaa, että yksikäsitteisyys säilyy.	Koko elinkaari	V		M
5006	Käyttäjätunnukset & todentaminen	Toimittajan järjestelmän tulee rajoittaa yhteiskäyttöisten käyttäjä- tai palvelutunnusten käyttöä. Yhteiskäyttöisiä tunnuksia voidaan käyttää vain Asiakkaan hyväksymissä tapauksissa.	Koko elinkaari	V+C		M
5007	Käyttäjätunnukset & todentaminen	Toimittajan järjestelmässä on mahdollisuus käyttää ja vaatia vahvoja salasanoja nykyisten standardien mukaisesti. Järjestelmän on kyettävä sopeutumaan tulevaisuuden muutoksiin ja päivityksiin standardeissa. Koskee paikallisia käyttäjätunnuksia.	Koko elinkaari	V		M

Sisäiset ohjeet | OHJEET | Elinkaari | Organisaatio | Poisto | Määritelmät | Esimerkki tietovuokaaviosta | Elinkaari, esimerkki tuesta

Ote Soten hankintojen tietoturva- ja tietosuojavaatimukset -työkalusta. [52]

[50] How to secure your medical devices, SecurityMetrics
[51] VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohjeen uusi tukimateriaali - 12 liite 5. Tietoturvallisuuden ja jatkuvuudenhallinnan huomioiminen hankittaessa ulkoistettuja ICT-palveluita, Valtiovarainministeriö 2011
[52] Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020

Toteutusvaiheessa riskiarviointi tarkastellaan uudelleen, ja tehdään tarvittavat tarkennukset. Käyttöönoton yhteydessä laaditaan käyttöönottosuunnitelma, ja suoritetaan tietojärjestelmän hyväksyntätestaus, jolla varmistetaan, että aiemmin kuvatut vaatimukset toteutuvat. Ylläpitovaiheessa tietojärjestelmää ylläpidetään suunnitelmien mukaan, arvioidaan säännöllisesti riskit ja päivitetään suunnitelmia koko elinkaaren ajan. Ympäristössä ja vaatimuksissa tapahtuvat muutokset on syytä tunnistaa muutoshallintamenettelyn avulla, ja korjata dokumentaatiot muutosten mukaisesti. [38]

Vaikka yksittäiset laitteet täyttäisivät asetetut vaatimukset, kannattaa kiinnittää huomiota siihen, että koko laitejärjestelmän vaatimuksenmukaisuus voidaan varmistaa [53].

Myös käytöstä poistoa varten on tehtävä riskiarviointi, ja suunnitelma, jossa huomioidaan muun muassa säilytettävän tiedon migraatio, tuhottavien laitteiden ja muistivälineiden sanitointi sekä käytöstä poistuvan tietojärjestelmän osien tuhoaminen. Tuhoamisen sijaan tietojärjestelmien sisältö voidaan myös tarvittaessa arkistoida. On hyvä muistaa, että tietoaineisto voi sijaita useassa eri kohteessa, ja sillä voi olla oma elinkaarensa, joka on yleensä pidempi kuin yksittäisellä tietojärjestelmällä. [38] Tietojärjestelmän vanhenemisesta voi seurata myös se, että tietoaineiston tarkasteluun ei enää löydy välineitä. Poistoon liittyvät yksityiskohdat kannattaa kirjata tarkasti sopimusehtoihin. Poistamisen kustannukset saattavat nousta yllättävän suuriksi, ellei esimerkiksi tietojen siirrosta tai arkistoinnista ole sovittu etukäteen.

Opinnäytetyön Information Security Requirements in Public IT Procurements liitteistä löytyy avustavia kysymyksiä hankintojen tietoturvallisuustarpeiden pohtimiseen sekä malli tietoturvallisuusvaatimuksista. Ohjelmistojen vaatimuksiin voidaan sisällyttää esimerkiksi OWASP tietoturvakäytänteet, sekä manuaaliset että automatisoidut tietoturvallisuustestaukset ja suorituskykytestaus. [54]

Tietosuoja

Terveydenhuollossa tietoa tallentuu eri muodoissa, mm. tekstinä, röntgenkuvina, mittaustuloksina ja lääkemääräyksinä. Henkilö- ja terveystietojen lisäksi syntyy myös muuta henkilöön tai hoitoon liittyvää tietoa, joista henkilöllisyys tai terveystiedot voidaan saada selville. [55] Palveluntuottaja on myös potilastiedon rekisterinpitäjä [56]. Henkilötietojen käsittelyn elinkaaren alusta loppuun on noudatettava tietosuojaperiaatteita. Rekisterinpitäjän täytyy pystyä myös osoittamaan näiden periaatteiden tehokas toteutuminen. [57] Henkilötietojen käsittelyyn on oltava aina hyväksytyt perusteet, ja nämä perusteet on oltava kaikilla tiedossa. Henkilötietoja saa käsitellä vain sellaisessa tilassa ja tilanteessa, jossa tiedot eivät voi paljastua sivullisille. [58] Henkilötietojen käsittelyä on kaikki henkilötietoihin kohdistuvat toimenpiteet. Tietosuoja.fi kuvaa tietosuojaperiaatteiden mukaista henkilötietoihin suhtautumista näin [57]:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten,
- ja vain tarpeellinen määrä tarkoitukseen nähden
- päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot poistettava tai oikaistava viipymättä
- ainoastaan niin kauan kuin on tarpeen tarkoituksen toteuttamista varten, tiedot säilytetään muodossa, josta rekisteröity tunnistettavissa
- käsiteltävä luottamuksellisesti ja turvallisesti.

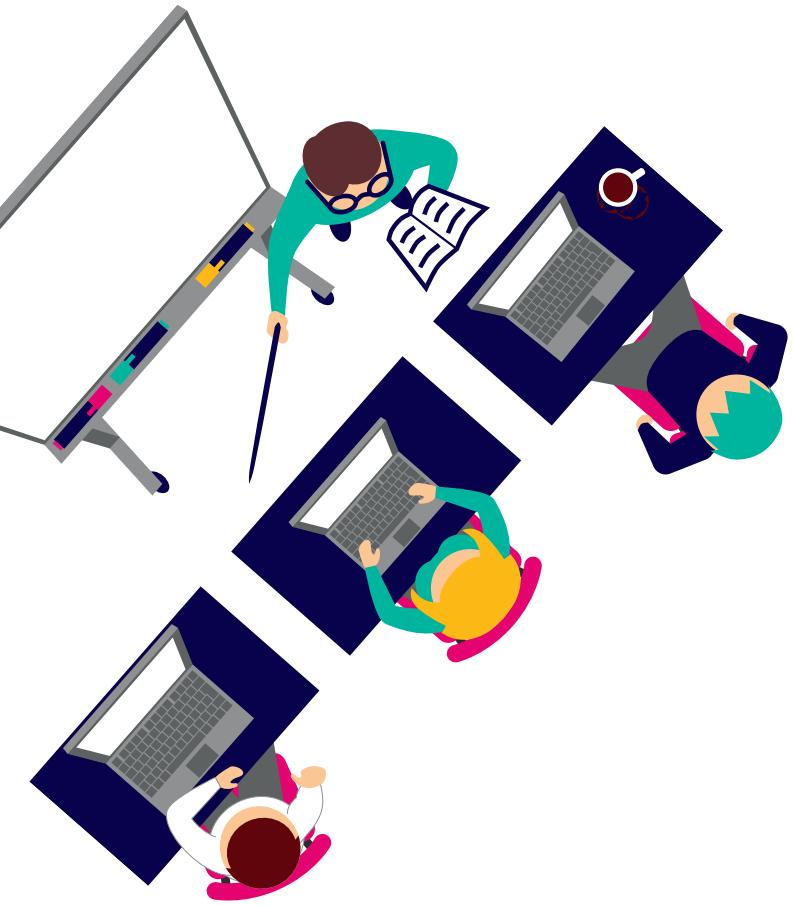
[53] Terveydenhuollon laadunhallinta - Lääkintälaitejärjestelmien turvallisuus, Lääkelaitos 2004
[54] Information Security Requirements in Public IT Procurements: Effect of Act on Information Management in Public Administration on Requirements, Aaltonen R. 2020
[55] Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt, STAKES 2005
[56] Tietosuoja sosiaali- ja terveydenhuollossa, Hyvinvointiala HALI ry
[57] Tietosuojaperiaatteet, tietosuojavaltuutetun toimisto
[58] Terveydenhuoltoalan kyberuhkia, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus

Keväästä 2018 lähtien on kaikissa EU-maissa ollut voimassa **yleinen tietosuoja-asetus, GDPR**. GDPR edellyttää tietosuojavastaavan nimeämistä julkishallinnon toimijoilta, ja muutenkin, kun arkaluontoista tietoa kerätään tai ihmisiä seurataan laajamittaisesti. Henkilötietojen käsittelyn perusteina voi olla rekisteröidyn suostumus, sopimus, lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleinen etu ja julkinen valta, tai rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu. Arkaluonteisen tiedon käsittely on sallittua vain poikkeustapauksissa. [59] Lisätietoja löytyy osoitteesta tietosuoja.fi/GDPR.

Terveyden ja hyvinvoinnin laitoksen sivuille on koottu tiedonhallinnan koulutusmateriaalia mm. tietosuojaan ja tietoturvallisuuteen liittyen. Pienten sosiaali- ja terveydenhuollon palveluntuottajien tueksi on julkaistu myös tietoturvan ja tietosuojan omavalvontasuunnitelman malli, joka auttaa tunnistamaan ja suunnittelemaan tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön olennaisia asioita [60]. Omavalvontasuunnitelmalla voidaan mm. varmistaa henkilöstön riittävät tietoturva- ja tietosuojataidot, sekä arkaluonteisen tiedon salassapidon merkitys. Tärkeä osa suunnitelmaa on selventää rooleja ja vastuita. [61] On hyvä muistaa, että ”kun kunta ostaa palvelun yksityiseltä palveluntuottajalta, asiakirjat ovat viranomaisen asiakirjoja ja niiden käsittelyyn sovelletaan myös lakia viranomaisten toiminnan julkisuudesta (621/1999)” [56].

Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille sopii myös organisaation kyvyn arvioimiseen salassa pidettävän tiedon suojaamisessa. Ohje sisältää turvallisuusjohtamisen, fyysisen turvallisuuden ja teknisen tietoturvallisuuden osa-alueet. [39]

[59] EU:n tietosuoja-asetus, tietosuojavaltuutetun toimisto
[60] Tietoturvan ja tietosuojan omavalvontasuunnitelman malli tukee pieniä sosiaali- ja terveydenhuollon palveluntuottajia, THL 2020
[61] Tietosuojan ja tietoturvallisuuden omavalvonta: Suunnitelma ja toteuttaminen, THL 2020



Kyberturvallisuusosaamisen kehittäminen

Huoltovarmuuskeskus yhteistyössä Digipoolin ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kanssa on tehnyt tiivistelmän (2020) kyberturvallisuuden nykytilakartoituksesta eri toimialoilla. Kartoituksen toteutti Digipoolin toimeksiannosta KPMG. Tiivistelmästä selviää, että henkilöstön kyberturvallisuusosaamista olisi syytä lisätä etenkin toimialoilla, joissa se ei kuulu ydinosaamiseen tai henkilöstön vaihtuvuus on suurta. Tiivistelmässä painotetaan lisäksi, että on hyvä kiinnittää huomiota erikoisosaamista vaativien alojen henkilöstön kyberturvallisuusosaamiseen. Nämä kuvaukset sopivat hyvin terveydenhuoltoon. [62]

> *Henkilöstön kyberturvallisuusosaamista olisi syytä lisätä etenkin toimialoilla, joissa se ei kuulu ydinosaamiseen tai henkilöstön vaihtuvuus on suurta.* [62]

Kyberturvallisuuskoulutukset

Oman organisaation järjestämien koulutusten lisäksi terveydenhuollon henkilöstön kyberturvallisuusosaamista voi kehittää esimerkiksi Oppiportin sosiaali- ja terveydenhuollon tietoturvakoulutuksilla. Duodecim Oppiportti on terveydenhuollon ammattilaisten täydennyskoulutuspalvelu. Koulutukset on tehty yhteistyössä Huoltovarmuuskeskuksen Kyber-Terveys-hankkeeseen osallistuvien sairaanhoitopiirien kanssa. Tarjolla on Tietoturva sosiaali- ja terveydenhuollossa -verkkokurssi, joka on tarkoitettu kaikille sosiaali- ja terveydenhuollon työntekijöille sekä Johdon ja esimiesten tietoturvakoulutus -koulutus, joka on tarkoitettu sosiaali- ja terveydenhuollon johtamiseen ja kehittämiseen osallistuville henkilöille. [63] Näitä tiiviitä (30min.) koulutuksia voidaan hyödyntää esimerkiksi osana uuden työntekijän perehdytystä. Myös Digi- ja väestöviraston Digiturvallinen elämä koulutukset sopivat alasta riippumatta organisaatioiden johdolle, asiantuntijoille ja henkilöstölle. Koulutusten avulla oppii toimimaan turvallisesti digitaalisen maailman uhkatilanteissa. Ilmaisten ja kaikille avointen verkkokoulutuksen kesto on 30–60 minuuttia. Tarjolla on myös Digiturvallinen elämä -peli, jonka avulla oppii digiturvataitoja helposti pelillisin keinoin. Pelin ensimmäisessä osassa keskitytään työelämässä tarvittaviin digiturvataitoihin. [64]

[62] KYBERTURVALLISUUDEN NYKYTILA ERI TOIMIALOILLA – KARTOITUKSEN KESKEISET HAVAINNOT, Huoltovarmuuskeskus 2020
[63] Duodecim Oppiportti, 2020
[64] Digiturvallinen elämä, Digi- ja väestötietovirasto

Kybertietoisuuden lisääminen

Ihmisiä pyritään manipuloimaan ja huijaamaan. Kyberrikolliset käyttävät ihmisiä tiedonhankinnan kanavana ja lähteenä luottamuksellisen tiedon ääreen. Kybertietoisuuden lisääminen organisaation sisällä on tärkeää, jotta kyberturvallisuusteemat pysyvät mielessä ja henkilöstö tietää miten toimia arkisissakin tilanteissa, vahvana lenkkinä teknologioiden ja prosessien rinnalla. Tietoisuuskampanjoiden toteuttaminen organisaation sisällä tulee olla säännöllistä. Mikäli organisaatiolla ei ole omaa materiaalia tietoisuuden lisäämisen tueksi, on mahdollista käyttää esimerkiksi seuraavia suomenkielisiä ajankohtaisia tietoverkkohuijauksia koskevia aineistoja tietoisuuden lisäämiseen.

CYBERDI-HANKKEEN TIETOPANKKI

| https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/tietopankki/

CYBERDI-projektissa yhtenä tavoitteena on kasvattaa käyttäjälähtöisesti yleistä tietoisuutta digitaalisen maailman uhkista ja rikollisuudesta. Projektin toteuttavat: Jyväskylän ammattikorkeakoulu (JAMK) ja Poliisiammattikorkeakoulu (POLAMK) ja rahoittajana toimii Opetus- ja kulttuuriministeriö.

TURVALISTIT

| https://turvalistit.fi/

Turvalistit on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen tuottama kampanja-aineisto. Turvalistit jakaa tietoturvan ilosanomaa, jotta kenenkään ei tarvitsisi oppia kantapään kautta. Tarjolla on videoita ja vinkkejä. Turvalisteja voi seurata myös Facebookin ja Instagramin välityksellä.

HUIJAUSINFO

| www.huijausinfo.fi

Kuluttajaliitolla on tarjolla Huijarit kuriin! -hankkeen puitteissa kuluttajille maksutonta neuvontaa ja koulutusta netissä tapahtuvista erilaisista huijauksista. Hankkeen aikana järjestetään myös vertaistukitoimintaa huijausten uhreille ja heidän läheisilleen. Hanketta rahoittaa STEA (Sosiaali- ja terveysjärjestöjen avustuskeskus).

Kyberturvallisuusharjoitukset

Kyberharjoitus on harjoitustapahtuma, jossa organisaatio mallintaa ja testaa varautumistaan erilaisiin kyberhäiriöihin. Harjoituksella tarkoitetaan organisaatiota kohtaavan tilanteen kuvitteellista mallintamista tarkoitukseen parhaiten soveltuvalla tavalla.

Kyberharjoituksen avulla kyberhäiriöitä simuloidaan eli mallinnetaan. Näin luodaan kuvitteelliset olosuhteet, joissa häiriön vaikutuksia ja niistä toipumista voidaan testata. [65]

Kyberharjoittelun hyötyjä ovat mm.

- organisaation kriisinsietokyvyn parantuminen
- tietojärjestelmäriippuvuuksista parempi ymmärtäminen
- parantunut ymmärrys häiriötilanteiden laajoista vaikutuksista
- sisäisen ja ulkoisen viestinnän kehittyminen
- parempi häiriötilanteiden johtaminen
- sisäisten prosessien kehittyminen (harjoituksen tulosten analyysin kautta)
- parantunut yhteisymmärrys palveluntuottajien ja asiakkaiden kanssa
- vastuualueiden selkiytyminen
- luottamuksen kasvu epävarmuudesta selviämiseen. [65]

Harjoitustyypit

Harjoitustyyppejä on erilaisia ja se minkälaista osaamista halutaan kehittää, määrittelee minkälaisen harjoituksen avulla kehitystyötä kannattaa tehdä. Perinteisesti tekniset harjoitukset ovat asiantuntijoiden ja teknisen ylläpidon osaamisen tukena, kun taas johdolle järjestetään johtamis- ja liiketoimintaharjoituksia. Yhteistoimintaharjoitus taas koskee kaikkia ja kehittää koko henkilöstön ja sidosryhmien osaamista. [65] Harjoitus voi myös olla eri harjoitustyyppien yhdistelmä, esimerkiksi teknistoiminnallinen harjoitus.

Laajemmat kuvaukset eri harjoitustyypeistä löytyy tuotoksesta: Kyberharjoitusohje Käsikirja harjoituksen järjestäjälle (Traficomin julkaisuja 26/2019) [66]

Yleisimmät harjoitustyypit ovat:

Työpöytäharjoitus sopii kyberhäiriöiden hallintaan, johtamiseen, prosessien läpikäyntiin ja arviointiin.

Juurisyyharjoitus (pre-mortem) sopii ongelmien ennakointiin ja riskienhallinnan suuntaamiseen.

Toiminnallinen harjoitus sopii kriisijohtamiseen, kriisiviestinnän harjoitteluun ja yhteistoimintaharjoitteluun.

Tekninen harjoitus sopii teknisten valmiuksien korottamiseen, järjestelmiin perehtymiseen ja palautumistesteihin.

Capture The Flag (CTF) harjoitus sopii teknisen osaamisen kehittämiseen ja järjestelmiin tutustumiseen.

Suuret yhteisharjoitukset sopivat verkostojen luomiseen, yhteistoiminnan vahvistamiseen ja tilannekuvan muodostamiseen. [66]

Häiriönkäsittelyharjoitus harjoittaa organisaation teknistä ja/tai hallinnollista kykyä selvittää organisaatioon kohdistuneen kyberhyökkäyksen vaikutukset ja varmistaa mahdollisimman tehokas palautuminen sekä oppi tapahtuneesta.

Terveydenhuollon kannalta keskeiset kyberturvallisuusharjoitukset

Kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC (Jyväskylä Security Technology) on Jyväskylän ammattikorkeakoulun IT-instituutin liiketoimintayksikkö, joka toteuttaa ja kehittää kansallisia kyberturvallisuusharjoituksia, **KYHA-harjoituksia**, osana turvallisuusstrategian toimeenpano-ohjelmia ja kehittämissuunnitelmia. JYVSECTEC järjestää vuosittain toteutettavia teknistoiminnallisia kansallisia kyberharjoituksia, jotka toteutetaan JYVSECTEC:in RGCE-kybertoimintaympäristössä (Realistic Global Cyber Environment). KYHA-harjoituksissa kehitetään viranomaistoimijoiden kyberturvallisuuden suorituskykyjä realistisessa teknisessä toimintaympäristössä. Johtavana ajatuksena on testata ja kehittää osallistujaorganisaatioiden kybersuorituskykyä ja yhteistoimintaa vakavissa kyberturvallisuuden häiriötilanteissa. Jyväskylän ammattikorkeakoulun päätoteuttamassa **Healthcare Cyber Range** -hankkeessa JYVSECTECin RGCE-ympäristöä laajennetaan terveydenhuoltopalveluiden viitekehykseen keskittyen terveydenhuollon järjestelmien ja prosessien mallintamiseen. Tämä mahdollistaa ensimmäisen terveydenhuollon suuren yhteisharjoituksen järjestämisen Healthcare Cyber Range -hankkeen pilottiharjoituksena vuoden 2021 syyskuussa. Pilottiharjoituksen jälkeen terveydenhuollon ympäristön kehittäminen jatkuu, jotta terveydenhuollon kansallisten teknistoiminnallisten KYHA-harjoitusten järjestäminen mahdollistuu tulevaisuudessa.

TIETO-harjoitus on järjestetty eri muodoissa säännöllisesti joka toinen vuosi 1980-luvun lopusta asti. Harjoituksen organisoinnista vastaa huoltovarmuusorganisaation Digipooli yhteistyössä Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen kanssa. Harjoituksen järjestämisestä vastaa Huoltovarmuuskeskus. [67]

[65] Opas digitaalisen turvallisuuden harjoitusohjelman ja -toiminnan suunnitteluun. Digi- ja väestötietovirasto
[66] Kyberharjoitusohje. Käsikirja harjoituksen järjestäjälle. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2019
[67] TIETO20-harjoitus testaa yhteistoimintaa laajassa kyberhäiriötilanteessa. Huoltovarmuuskeskus 2020

Vuoden 2018 TIETO-harjoituksessa oli vahvasti mukana terveydenhuolto sekä energia-ala, logistiikka ja liikenne, teollisuus, vesihuolto ja media-ala sekä toimialojen keskeiset ICT-palveluntuottajat. Harjoitus oli skenaariopohjainen strategisen tason harjoitus, joka järjestettiin kolmiosaisena ja huipentui syksyllä pidettyyn intensiivivaiheeseen. Harjoituksen tavoitteena oli parantaa yhteiskunnan kykyä ehkäistä laajoja kyberturvallisuushäiriöitä ja selvitä niistä. Harjoitus suunnattiin erityisesti huoltovarmuuskriittisille yrityksille. Yhteiskunnan elintärkeiden toimintojen kannalta kriittisten organisaatioiden yhteistoimintaa kehitettiin laajoihin kyberhäiriötilanteisiin liittyvässä harjoituksessa. Tarkastelun kohteena oli myös tietoturvayritysten ja viranomaisten välinen yhteistoiminta. [68]

Digi- ja väestötietovirasto (DVV) toteuttaa vuosittain **TAISTO-harjoituksen**, ensimmäinen toteutettiin vuonna 2018. TAISTO-harjoituksessa harjoitellaan organisaation toimintakykyä erilaisissa tietoturva- ja tietosuojaloukkaustilanteissa. Harjoituksen suunnittelu tehdään yhteistyössä muun muassa keskusrikospoliisin, Kyberturvallisuuskeskuksen, tietosuojavaltuutetun toimiston, Valtorin ja Turvallisuuskomitean kanssa. Harjoituspäivä rakentuu tapahtumista ja niihin liittyvistä syötteistä. TAISTO-harjoitukset ovat avoimia ja maksuttomia kaikille julkisen hallinnon organisaatioille ja niiden sidosryhmille. Vuonna 2020 organisaatio pystyi valitsemaan harjoituksen kestoksi joko puolen päivän tai koko päivän harjoituksen ja se toteutettiin Trasim-harjoitusalustalla. [69] Vuonna 2018 TAISTO-harjoitukseen osallistui 9 sairaanhoitopiiriä ja vuonna 2019 5 sairaanhoitopiiriä [70].

Kyberturvallisuussertifikaatit

Terveydenhuollon toimijoiden varautumista kyberhäiriötilanteiden varalle tukee erilaiset vaatimustenmukaisuuden arviointiin liittyvät tietoturvasertifioinnit ja muut hyväksynnät. Sertifioinnin kohteena voi olla joko organisaation johtamisjärjestelmä, konkreettinen tuote, noudatettava toimintaprosessi tai henkilöstön ammatillinen pätevyys. Sertifioinnin yhteydessä tarkasteltavat vaatimukset perustuvat useimmiten johonkin standardiin eli kirjalliseen julkaisuun yhteisesti sovituista suosituksista. [71]

Tieturvastandardoinnin ja -sertifioinnin tilaa Suomessa on kartoitettu viimeksi Kyberturvallisuuskeskuksen julkaisemassa selvityksessä ”Luottamuksen lähteillä – Näkökulmia tietoturvan standardointiin ja sertifiointiin” vuodelta 2019. Selvitys nostaa esille sertifiointien käytön merkityksen luottamuksen rakentamisessa ja vaatimusten toteutumisen valvonnassa. Suomessa tietoturvastandardeja ja niihin liittyviä hyväksyntöjä käytetään yleisesti organisaation oman tietoturvakyvykkyyden nostamisessa, lainsäädännön vaatimusten täyttämisessä ja liiketoimintaedun saavuttamisessa. [72]

Terveydenhuollon toimialalla tietoturvastandardit ja –sertifioinnit ovat kiinteä osa arjen työtehtäviä ja –välineitä, joita asiakas- ja potilastyössä käsitellään tai suoritetaan. Ne koskevat muun muassa tiedonhallinnan järjestämistä toiminnalta edellytetyn hyvän tiedonhallintatavan mukaisesti. Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettujen tietojärjestelmien on esimerkiksi ennen niiden käyttöönottoa täytettävä niille asetetut tekniset ja toiminnalliset vaatimukset. Lisäksi vaatimustenmukaisuus on kyettävä riittävällä tavalla osoittamaan. [73]

Potilastietojen käsittelyssä käytettävät potilastietojärjestelmät jaetaan voimassa olevien säädösten mukaisesti kahteen luokkaan A ja B. Tietojärjestelmäkohtainen luokitus määräytyy sen mukaan, onko tietojärjestelmä tarkoitus liittää Kansaneläkelaitoksen ylläpitämiin Kanta-palveluihin osaksi valtakunnallista tietojärjestelmäpalvelua vai ei. Kanta-palveluihin liitettävät tietojärjestelmät kuuluvat luokkaan A ja muut Kanta-palveluista erillään toimivat potilastietojärjestelmät luokkaan B. Tietojärjestelmään sovellettava luokitus asettaa ehtoja vaatimustenmukaisuuden osoittamiselle. [73]

Luokkaan A kuuluvat potilastietojärjestelmät saa ottaa käyttöön vasta, kun tietoturvallisuuden arviointilaitos on antanut sitä koskevan vaatimustenmukaisuustodistuksen. Luokkaan B kuuluvan tietojärjestelmän käyttöönotto on sallittua jo silloin, kun järjestelmän valmistaja on ilmoittanut tietojärjestelmästä Sosiaali- ja terveysalan lupa ja valvontavirasto Valviralle ja antanut vaatimustenmukaisuutta koskevan kirjallisen selvityksen. Toisin sanoen luokkaan B kuuluva tietojärjestelmä ei edellytä erillistä vaatimustenmukaisuuden todentamista vaan käyttöönottoon riittää valmistajan vakuutus tietojärjestelmälle asetettujen ehtojen täyttymisestä. [73]

[68] Tieto 2018 -kyberturvallisuusharjoitus käynnissä – Verkostona kyberuhkia vastaan, Huoltovarmuuskeskus 2018
[69] TAISTO-harjoitus, Digi- ja väestötietovirasto 2020
[70] TAISTO19-harjoitusraportti ja yhteenveto, Digi- ja väestötietovirasto 2019
[71] Sertifiointiorganisaatiot, Finas 2020
[72] Luottamuksen lähteillä: Näkökulmia tietoturvan standardointiin ja sertifiointiin, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2019
[73] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, Finlex 2007

Luokkaan A kuuluvien potilastietojärjestelmien hyväksyntämenettely nostaa esiin käsitteen kansallisesta akkreditointijärjestelmästä. Kansallisella akkreditointijärjestelmällä tarkoitetaan pätevyyden toteamisjärjestelmää, jolla varmistetaan muun ohella sertifiointien ja tarkastusten sekä vastaavien vaatimustenmukaisuudenarviointipalvelujen luotettavuus ja kansainvälinen hyväksyttävyys. Suomessa akkreditointijärjestelmään liittyvistä tehtävistä huolehtii kansallisena akkreditointielimenä Turvallisuus- ja kemikaalivirasto akkreditointiyksikkö nimeltä FINAS-akkreditointipalvelu. [74]

FINAS-akkreditointipalvelun tehtäviin kuuluu potilastietojärjestelmien tarkastuksista vastaavien tietoturvallisuuden arviointilaitosten pätevyyden toteaminen. Edellytyksenä pätevyyden toteamiselle on, että tietoturvallisuuden arviointilaitos täyttää akkreditointiin sovellettavat, ISO 27001 ja ISO 27006 standardeissa määritellyt yhdenmukaiset kansainväliset ja eurooppalaiset arviointiperusteet. Lisäksi tietoturvallisuuden arviointilaitoksen on ennen vaatimustenmukaisuuden arviointipalvelujen tarjoamista saatava Kyberturvallisuuskeskuksen hyväksyntä toiminnalleen. [75]

ISO 27001 on tällä hetkellä tunnetuin kansainvälinen tietoturvastandardi, joka käsittelee tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevia vaatimuksia. ISO 27001 –sertifikaatti osoittaa, että organisaation tietoturvajohtamisjärjestelmä on sertifioitu parhaiden käytäntöjen mukaisesti täyttäen standardin asettamat vaatimukset. Lisätietoja standardista https://www.iso.org/isoiec-27001-information-security.html

Kansallisiin ja kansainvälisiin standardeihin perustuvien virallisten tietoturvasertifiointien rinnalle on tuotu kustannustehokkaita tietoturvallisuuden arviointimalleja. Yksi tällaisista organisaation kyberturvallisuustason kartoittamiseen tarkoitetuista arviointimalleista on Jyväskylän ammattikorkeakoulun kehittämä ja hallinnoima FINCSC –kyberturvallisuussertifikaatti. FINCSC on osa Suomen kansallista varautumista. Vuoden 2017-2020 kyberturvallisuusstrategian toimeenpano-riskiohjelmaan yhtenä avaintoimenpiteenä kuuluva FINCSC-kyberturvallisuussertifikaatti koostaa yhteen organisaatioille asetettavat vähimmäisvaatimukset kyberturvallisuuden hallintaan. [76]

[74] Laki Turvallisuus- ja kemikaalivirastosta, Finlex 2010
[75] Laki tietoturvallisuuden arviointilaitoksista, Finlex 2011
[76] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, Turvallisuuskomitea 2017

Kyberturvallisuuteen liittyvän tilannetiedon jakaminen

Yksi merkittävimmistä tavoista parantaa organisaation sietokykyä kyberturvahyökkäyksiä vastaan on saada tarkka ja oikea-aikainen tilannetieto. Tilannetietojen tehokas tuottaminen ja hyödyntäminen saavutetaan jakamalla tietoa muiden tiedonjakeluverkon toimijoiden kanssa nopeasti ja luotettavasti vaarantamatta oman organisaation luottamuksellisia tietoja. Tässä kappaleessa esiteltävät tilannetiedon jakamisen mallit ja menetelmät soveltuvat hyvin organisaatioihin, jotka käsittelevät ja jakavat luottamuksellista kyberturvallisuuteen liittyvää tietoa eri organisaatioiden välillä, kuten esimerkiksi terveydenhuollon organisaatiot.

Yksittäisen toimijan antama tieto hyökkäyksestä ja puolustusmenetelmistä tarjoaa muille toimijoille tehokkaan tavan puolustautua kyberhyökkäyksiltä. Tietojen jakamisen keskeinen edellytys on kuitenkin se, kuinka toimijat voivat jakaa tietoa nopeasti, tarkasti ja vaarantamatta omaa toimintaansa paljastamalla tietoja hyökkäyksistä.

Kyberturvallisuustietojen jakamisessa tietojen luokittelulla on tärkeä rooli. Luokittelua edellyttävät kyberturvallisuustiedot sisältävät mm. tiedot tietoturvaloukkauksista, kohteena olevista tietojärjestelmistä tai puolustustoimista. Luokittelu tarjoaa mekanismin luottamuksellisten tietojen jakamisen hallitsemiseksi. Tällaisten tietojen jakamiseen liittyy aina riski. Tietojen jakaminen vaatii toimijoiden välisen luottamuksellisen suhteen, jotta tiedot voidaan siirtää turvallisesti organisaation ulkopuolelle. Tämä voidaan saavuttaa monin eri tavoin. [77]

Tiedonjaon ongelma on se, että tietoja tunkeutumisista ja haavoittuvuuksista ei yleensä voida välittää kaikille toimijoille tai tietoja joudutaan odottamaan liian kauan. Toisaalta välitetyt tiedot voivat olla liian yleisiä hyödynnettäväksi puolustustoimenpiteissä. Tässä tapauksessa on usein liian myöhäistä estää tai lieventää hyökkäysten vaikutuksia ennen vakavien vahinkojen syntymistä. [78]

Ongelmakenttä voidaan tiivistää seuraaviin havaintoihin. Arkaluonteisten tietojen välittämiseen toimijoiden välillä on oltava luottamuksellinen suhde. Tietojen välittämisen on oltava tehokasta. Tietojen on oltava riittävän yksityiskohtaisia, jotta vastaanotettu organisaatio voi käyttää niitä. Tarpeettomia tietoja olisi vältettävä toimijoiden välisessä tiedonsiirrossa, jotta vältetään tiedon tulva asiaankuuluvan tiedon havaitsemiseksi. Organisaatioiden on oltava halukkaita jakamaan arkaluonteisia tietoja. Halukkuus tiedon jakamiseen vaihtelee suuresti toimijoiden välillä [79].

Ensimmäiset askeleet kyberturvallisuustiedon jakamisongelman ratkaisemiseksi ottivat Yhdysvaltain viranomaiset vuonna 1998 julkaisemalla direktiivin kyberdatan jakamisen helpottamiseksi [80]. Direktiivissä kuvataan lähestymistapa teollisuuden tietojen analysointiin ja jakamiseen luottamuksellisten tiedonjakoverkostojen (ISAC, Information Sharing and Analysis Center) kautta [81]. Viimeisten viidentoista vuoden aikana on perustettu useita erillisiä ISAC-verkostoja [82]. Euroopan unionin alueella ENISA (European Union Agency for Cybersecurity) kannustaa ja tukee uusien ISAC-verkostojen perustamista mm. tarjoamalla erillisiä työkaluja niiden perustamiseen [83,84]. Katso lisää ISAC-keskusten perustamisesta: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit

[77] Cyber Threat Information Sharing: Perceived Benefits and Barriers, Zibak A.; Simpson A. 2019 doi: 10.1145/3339252.3340528, 2019
[78] A framework for cybersecurity information sharing and risk reduction, Microsoft, 2015
[79] Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (slna), Colicchia C., Creazza A., Noè C., Strozzi F. Supply Chain Management: An International Journal, Volume 24, Number 1, 2019
[80] Strategic Aspects of Cyber Risk Information Sharing, Laube S.; Böhme R. ACM Computing Surveys (CSUR), Volume 50(5), doi:10.1145/3124398, 2017
[81] The impact of information sharing on cybersecurity underinvestment: A real options perspective. Gordon L. A., Loeb M. P., Lucyshyn W., Zhou L. Journal of Accounting and Public Policy, Volume 34, Number 5, 2015
[82] Perspectives on cybersecurity information sharing among multiple stakeholders using a decisiontheoretic approach, He M.; Devine L.; Zhuang J. Risk Analysis, Volume 38, number 2, 2018
[83] Information Sharing and Analysis Centers (ISACs), Enisa
[84 ISAC in a box, Enisa

STIX uhkatiedon kuvauskieli

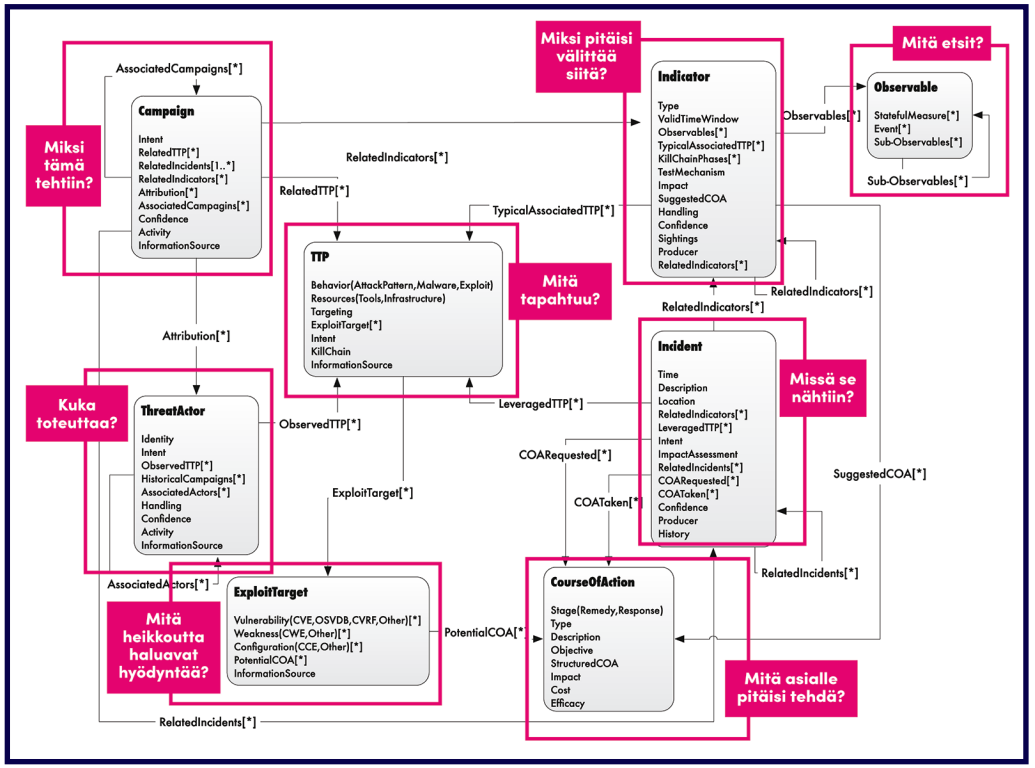
Seuraavat kappaleet (STIX uhkatiedon kuvauskieli, Uhkatiedon käsittely ja Uhkatiedon jakomallit ja alustat) on suunnattu erityisesti kyber- ja digiturvallisuuden parissa työskenteleville asiantuntijoille sekä teknisen tilannetiedon jakamisesta kiinnostuneille.

Mitre Corporation on julkaissut aikanaan seuraavat standardit tiedon esittämiseen (Structured Threat Information eXpression, STIX ™ v2.1) [85], tiedon välittämiseen (Trusted Automated eXchange of Indicator Information, TAXII ™ v.2.1) [86] ja havaintojen kuvaamiseen (Cyber Observable Expression, CyBOX ™ v.2.1.1) [87]. Nykyään tiedonjaon standardien ylläpidosta ja kehittämisestä vastaa OASIS ™ Cyber Threat Intelligence (CTI) työryhmänsä (technical committee) kautta [88].

STIX-kielen ja kuvantamismuodon on ottanut käyttöön laaja joukko kyberuhkia käsitteleviä organisaatioita ja yhteisöjä ympäri maailmaa. STIX on formaatti, joka auttaa tuottamaan jäsenneltyä uhkatietoa ja tukee seuraavia kyberuhkien hallinnan käyttötapauksia: kyberuhkien analysointi, uhkatietotunnisteiden määrittäminen, reagointitoimintojen hallinta ja kyberuhkien tietojen jakaminen. Kyseessä ei ole erillinen tiedonjako-ohjelma tai –työkalu, vaan formaatin tarkoituksena on auttaa ymmärtämään ja luomaan jäsenneltyjä, johdonmukaisia kyberuhkatietojen kuvauksia. Yleisimmin käytetty kuvauskieli on XML, mutta STIX tukee myös muita toteutusvaihtoehtoja (kuten semanttinen WEB). Esimerkki STIX-kuvauksesta toteutettuna XML-kuvauskielellä: https://raw.githubusercontent.com/STIXProject/schemas/version_1.0.1/samples/STIX_Domain_Watchlist.xml

STIX tarjoaa yhteisen, jäsennellyn mekanismin strukturoidun kyberuhkatiedon käsittelemiseksi, mikä parantaa johdonmukaisuutta, tehokkuutta, yhteentoimivuutta ja yleistä tilannetietoisuutta. STIX arkkitehtuuri tarjoaa mallin, kuinka erilaiset kyberuhkatiedot voidaan yhdistää joko paikallisesti organisaation sisällä tai jakamisyhteisön kautta.

Oheisessa STIX-arkkitehtuurissa (kuva) on kahdeksan rakennetta, jotka kaikki on luotu XML-skeemalla. Rakenteet ovat Observable, Indicator, Incident, TTP (Tactics, Techniques, and Procedures), ExploitTarget, CourseOfAction, Campaign ja ThreatActor [85].



STIX-arkkitehtuuri, alkuperäistä lähteen kuvaa muokattu (Kuvan lähde: Inference and Ontologies, ResearchGate 2014)

[85] Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™), White paper: STIX project Github 2014
[86] The Trusted Automated eXchange of Indicator Information (TAXII™), White paper: TAXII project Github 2014
[87] Cyber Observable eXpression (CybOX™) Archive Website, CybOX project Github
[88] Sharing threat intelligence just got a lot easier!, OASIS Open Github

Mitä etsit?

Kyberturvallisuuteen liittyvät havainnot (Observable) ovat ensisijaisia tietoja, joilla yhdistetään eri toimijoiden havainnot yhteiseksi kokonaisuudeksi esimerkiksi luomalla niille yhteinen tunniste, lähettävä IP-osoite tai sähköpostiosoite. Nämä havainnot mahdollistavat tehokkaan häiriötilanteiden etsinnän omista järjestelmistä.

Miksi pitäisi välittää siitä?

Tunnistetietoja (Indicator) voidaan käyttää epäilyttävän tai haitallisen verkkotoiminnan havaitsemiseen. Esimerkiksi tunnistetietoja voidaan käyttää kuvaamaan haitallisten verkkotunnusten joukkoa. Tunnistetietojen avulla organisaatio voi tehdä päätelmiä, koskeeko kyseinen tapahtuma heitä.

Missä se nähtiin?

Tapahtuma (Incident) koostuu organisaatioon vaikuttavista tietoturvatapahtumista, tapahtuman käsittelyyn osallistuvista henkilöistä ja tapahtuman käsittelyn aikatiedoista sekä muista merkityksellisistä tiedoista tai tehdyistä päätöksistä. Tapahtumatiedot vastaavat erityisesti kysymykseen, missä tapahtuma havaittiin, milloin ja kenen toimesta.

Mitä tapahtuu?

Hyökkääjän taktiikan, tekniikan ja menettelytapojen (TTP) tunnistamisella on keskeinen rooli kyberuhkatiedoissa ja kyberuhkien tutkinnassa. TTP-tiedot koostuvat erityisestä hyökkääjän käyttäytymisen tunnistamisesta (hyökkäysmallit, haittaohjelmat, hyväksikäytöt), hyödynnetyistä resursseista (työkalut, infrastruktuuri, persoonat), tiedoista kohteena olevista uhreista (kuka, mitä tai missä), kohdennetuista kohteista ja suunnitelluista vaikutuksista. TTP-kuvauksilla pyritään vastaamaan kysymykseen, mitä on tapahtumassa.

Mitä heikkoutta haluavat hyödyntää?

Hyödyntämiskohteen (Exploit Target) kuvauksella pyritään välittämään tietoa ohjelmistoissa, järjestelmissä, verkoissa tai kokoonpanoissa olevista haavoittuvuuksista tai heikkouksista, sekä niihin liittyvistä korjaustoimenpiteistä.

Miksi tämä tehtiin?

Kyberhyökkäyskampanjakuvauksella (Campaign) kuvataan joukkoa haitallisia toimintoja tai hyökkäyksiä, jotka tapahtuvat tietyn ajanjakson ajan tiettyjä kohteita vastaan. Kampanjakuvauksilla pyritään ymmärtämään, mitä hyökkääjä tai hyökkääjäjoukko tavoittelee.

Kuka toteuttaa?

Uhkatoimijat (Threat Actors) ovat todellisia henkilöitä, ryhmiä tai organisaatioita, joiden uskotaan toimivan kohdeorganisaatiota vastaan haitallisella tarkoituksella. Uhkatoimija voi ajan mittaan saada tukea tai olla sidoksissa erilaisiin tunkeutumista toteuttaviin ryhmiin tai organisaatioihin. Uhkatoimijat käyttävät resurssejaan ja mahdollisesti muiden toimijoiden resursseja hyökkäysten suorittamiseen ja kampanjoiden toteuttamiseen tavoitteidensa mukaisesti. Uhkatoimijoista voidaan kuvata STIXin avulla motiivit, kyvyt, tavoitteet, hyökkäyksen vaativuus, aiemmat toimet, resurssit (joihin heillä on pääsy) sekä heidän roolinsa organisaatiossa.

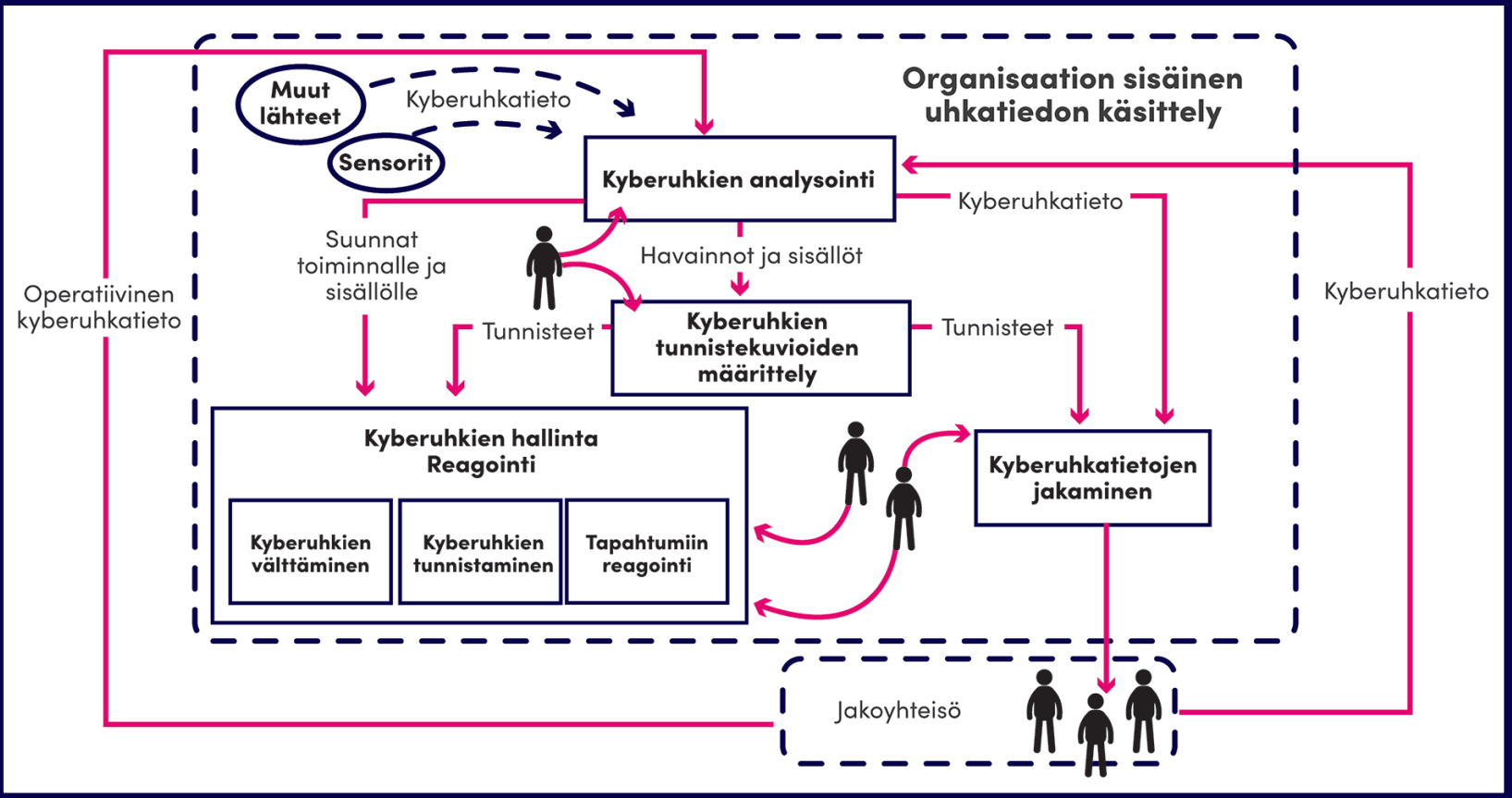
Mitä asialle pitäisi tehdä?

Toimintatapakuvauksessa (Course of Action) esitetään ne toiminnot, joilla pyritään estämään hyökkäys tai vastaamaan käynnissä olevaan hyökkäykseen. Se voi kuvata teknisiä, automatisoituja toimenpiteitä (korjaustiedostojen asentaminen, palomuurien uudelleenmääritys), mutta se voi myös kuvata korkeamman tason toimia, kuten työntekijöiden koulutusta tai käytäntöön tehtäviä muutoksia. Esimerkiksi kuvaus toimintatavasta, jolla haavoittuvuutta lievennetään, voisi olla tietyn korjaustiedoston käyttäminen.

Uhkatiedon käsittely

Kyberuhkatieto voidaan saada tiedonjakoverkostosta, omien seurantajärjestelmien ja muiden lähteiden, kuten CERT:in (Computer Emergency Response Team) tai laitevalmistajien kautta. Uhkatietoa analysoidaan organisaation sisällä ja määritellään uhalle ominaiset tunnisteet. Analysoinnin tulosten ja saatujen tunnisteiden perusteella organisaatiossa toteutetaan toimenpiteet uhkien välttämiseksi, tarkempien tunnisteiden saamiseksi ja reagoidaan mahdollisiin uhkiin. Saadut tiedot jaetaan tiedonjakoverkoston kautta muille organisaatioille. Toimintaa havainnollistetaan alla olevassa kuvassa.

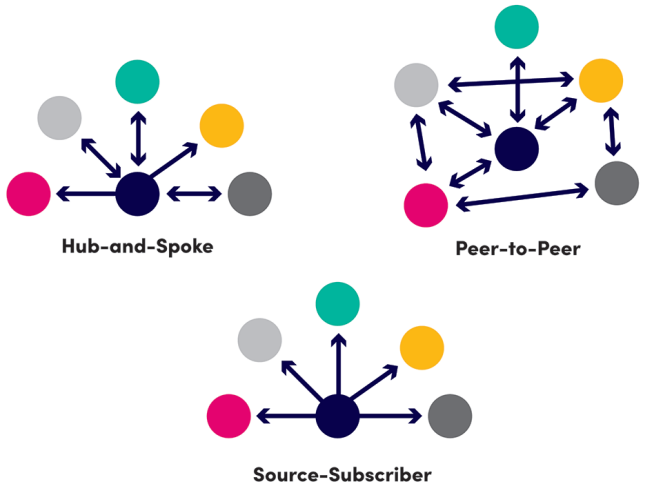
Tiedonjakoverkostossa toimijat analysoivat kyberuhkatietoja. Analysoinnin avulla saatujen havaintojen ja uhkien sisältöjen perusteella muodostetaan kuva tapahtumasta. Tapahtuman tunnisteet talletetaan yhteisesti sovitulla tavalla esimerkiksi STIX-formaattiin ja jaetaan tiedonjakoverkoston käyttöön. Kyberuhkien analysointi antaa myös suuntaviivat ja sisällöt, kuinka havaittua kyberuhkaa hallitaan ja kuinka siihen reagoidaan organisaatiossa. Tehtävän tarkoituksena on tunnistaa kyberuhan mahdolliset vaikutukset ja estää sen aiheuttamat mahdolliset häiriöt organisaation toiminnassa.



Kyberuhkatietojen käsittely tiedonjakoverkostossa

Uhkatiedon jakomallit ja alustat

Palvelut ja viestien vaihto organisaatioiden välillä on määritelty TAXII-protokollassa. TAXII tukee kolmea erilaista uhkatietojen jakamismallia: ”HUB-and-Spoke,”Peer-to-Peer” ja ”Source-Subscriber”. ”HUB-and-Spoke” jakamismallissa yksi toimija (HUB) toimii tiedon jakajana ja mahdollisesti myös tiedon vastaanottajana verkoston muilta jäseniltä (Spoke). ”Peer-to-Peer” jakamismallissa kukin verkoston toimija on sekä tiedon jakaja että tiedon vastaanottaja. ”Source-Subscriber” jakamismallissa taas yksi toimija (Source) välittää tietoja muille verkoston jäsenille (Subscriber).



Kyberuhkatiedon tiedonjakomallit havainnollistettuna

TAXII-palvelussa on kaksi erilaista ratkaisua, TAXII-palvelin ja TAXII-asiakas. Palvelin ja asiakas vaihtavat tietoja pyyntö-vastaus-mallin mukaisesti. TAXII mahdollistaa monimutkaisten tiedonjakorakenteiden toteuttamisen useiden toimijoiden välillä. Ratkaisussa kyberuhkatiedot voidaan jakaa tehokkaasti STIX-tietorakenteiden avulla. [86]

Toinen vaihtoehtoinen ja suosittu standardi kyberturvallisuustietojen jakamiselle on haittaohjelmien tiedonjakoalusta MISP (MISP - Malware Information Sharing Project - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing) [89]. Nimi on hieman harhaanjohtava, koska MISPiä voidaan käyttää myös uhkatiedustelualustana kohdennettujen hyökkäysten, uhkatiedon ja haavoittuvuustietojen jakamiseen, tallentamiseen ja korrelointiin.

MISP:n päätavoite on halu jakaa tietoa helposti ja automaattisesti päällekkäisen työn välttämiseksi [90]. MISP: llä on useita ominaisuuksia, kuten haitallisen toiminnan tunnistetietojen välittäminen (IoC, Indicators of Compromise), ryhmien jakaminen, automaattinen korrelaatio, vapaiden tekstien tuonti, tapahtumien jakelu ja yhteistyö. Se tukee useita tiedon esitysmuotoja, kuten esimerkiksi STIX-standardia. Kyseessä on ns. open source –ohjelmisto, joka mahdollistaa organisaatioihin tai ihmisiin kohdistuvien hyökkäysten, petosten tai uhkien havaitsemisen ja estämisen. Euroopan Unioni rahoittaa MISP-kehitystyötä.

[89] MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing, MISP-project
[90] Incidents Information Sharing Platform for Distributed Attack Detection, Fotiadou K., Velivassaki T., Voulkidis A., Railis K., Trakadas P., Zahariadis T. IEEE Open Journal of the Communications Society, Volume 1, 2020, doi: 10.1109/OJCOMS.2020.2989925

Terveydenhuollon tietojärjestelmät

Terveyden ja hyvinvoinnin laitoksen (THL) julkaisun, Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen kansallinen kokonaisarkkitehtuuri, mukaan tietojärjestelmäarkkitehtuuri kuvaa organisaation tai toimialan keskeisiä tietojärjestelmiä, keskinäisiä suhteita ja ominaisuustietoja. Tietojärjestelmäarkkitehtuuria suunnitellaan niin, että järjestelmäkokonaisuus tukee toiminnalle asetettuja tavoitteita mahdollisimman hyvin. [91] Terveydenhuollossa käytettyjä tietojärjestelmiä ovat sairaalan, perusterveydenhuollon, laboratorion, radiologian ja muiden erillisyksikköjen tietojärjestelmien lisäksi mm. talous- ja henkilöstöhallinnon sekä asianhallinnan järjestelmät, viestintäjärjestelmät sekä toiminnanohjaus- ja turvallisuusjärjestelmät. Potilastietojärjestelmät, joissa käsitellään potilaan hoitokokonaisuuden tietoja, ovat terveydenhuollon keskeisimpiä tietojärjestelmiä. Niiden ydinjärjestelmiä, kuten lähetteiden käsittely-, ajanvaraus- ja hoitotietojen kirjausjärjestelmät, käytetään melkein kaikkialla sairaalan yksiköissä. [20] Tietojärjestelmiä voi olla sekä organisaation omissa tiloissa, että kolmansien osapuolien palvelimilla. Ohessa joitakin sairaalan kriittisiä järjestelmiä. [92]

POTILASTIETOJÄRJESTELMÄT
- Uranus-Miranda desktop
- Oberon
- Ariel
- Alue-Pegasos

LABORATORIOJÄRJESTELMÄT
- KYS-ML
- Laboratorio-OVT

KUVANTAMISEN JÄRJESTELMÄT
- RIS
- PACS
- FORTE KOVIS KIBI
- NeaLink

VERITILAUSJÄRJESTELMÄT
- Verkis

ANESTESIATIETOJÄRJESTELMÄT
- Centricity Anaesthesia

TEHOHOIDON JÄRJESTELMÄT
- Critical Care Clinisoft

SYNNYTYSKERTOMUS
- Haikara / Pikkuhaikara

PATOLOGIAN JÄRJESTELMÄT
- Qpati

LEIKKAUSTOIMINNAN OHJAUS
- Orbit

TURVALLISUUSJÄRJESTELMÄT
- Kameravalvonta
- äänievakuointi
- Escraft
- ESMIKKO
- Tunstall

KESKUSVALVONTAJÄRJESTELMÄT
- Carescape
- Philips

MUUT KRIITTISET JÄRJESTELMÄT
- SYKe
- Citrix
- SCCM
- Direct Access
- DHCP
- Active Directory

HOITAJAKUTSUJÄRJESTELMÄT
- Miratel Aurora / Innova, Scharck

TIEDONVÄLITYSRAJAPINTA
- Ensemble

VIESTINTÄRATKAISUT
- Puhelinvaihde
- Oscar
- Exchange

TOIMINNANOHJAUSJÄRJESTELMÄT
- Codea

Sairaalan kriittisiä järjestelmiä

[91] Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen kansallinen kokonaisarkkitehtuuri v 2.1, Kanta 2019
[92] Kyberturvallisuus sairaaloiden eri toimialoilla, KYS 2016

Sairaaloissa on useita digitaalisia **automaatiojärjestelmiä**, kuten potilaiden elintoimintoja mittaavat laitteet ja lääkinnästä huolehtivat lääkepumput [58]. Lisäksi kiinteistöautomaatiolla voi olla vaikutus potilaan terveyteen. Useat automaatiojärjestelmät ovat valitettavan herkkiä häiriöille. Tietoturvakin on usein heikosti toteutettu; komentojen laillisuutta ei tarkisteta, käyttäjän tunnistusta ei ole, tai järjestelmä on yhdistetty suojauksitta julkiseen internetiin. Automaatiolaitteen suojausten puuttuminen voi avata hyökkääjälle reitin myös muualle verkkoon. [92] Kyberturvallisuuskeskuksen kartoituksen mukaan Suomessa on runsaasti suojaamattomia, julkiseen internetiin näkyviä, automaatiolaitteita, mm. lämmityksen ja ilmastoinnin ohjausjärjestelmiä, aurinkosähköjärjestelmien vaihtosuuntaajia ja kiinteistöjen lukitusjärjestelmiä. Mahdollisen hyökkäysreitin lisäksi verkkorikollinen voi hyödyntää kyseisiä laitteita osana palvelunestohyökkäystä, tai roskapostin lähettäjänä. Vinkkejä automaatiojärjestelmien turvaamiseen löytyy Kyberturvallisuuskeskuksen sivuilta. [93]

Useimpia terveydenhuollon järjestelmiä tarvitaan ympäri vuorokauden, ja monet niistä ovat toisiinsa sidoksissa. Tämä vaikeuttaa häiriötilanteessa laitteiden ja järjestelmien eristämistä, ja esimerkiksi uudelleenkäynnistämistä. [94] Elämää ylläpitävää laitetta ei voida suoraan sammuttaa, vaikka se olisi hakkeroitu. Hätätilassa henkilökunnan on pystyttävä käyttämään laitteita käytönhallintajärjestelmän sitä estämättä. [95] Verkkojen segmentointi niin, että eri järjestelmät ovat rinnakkaisissa ja sisäkkäisissä turvavyöhykkeissä, ja potilaisiin suoraan yhteydessä olevat järjestelmät näistä sisimpänä, auttaa suojaamaan kriittisimpiä kohteita [92].

Sosiaali- ja terveydenhuollossa tietojärjestelmät jaetaan A- ja B-luokkiin sen mukaan, onko ne liitetty Kanta-palveluun. Hallituksen uusi lakiesitys, jonka suunnitellaan astuvan voimaan 1.4.2021 terveydenhuollon osalta, sisältää velvoitteen liittää Kanta-palveluihin kaikki palvelunantajat, joilla on asiakas- tai potilastietojärjestelmä. Nämä järjestelmät on myös sertifioitava ja niiden yhteen toimivuus Kanta-palveluiden ja muiden Kantaan liitettyjen tietojärjestelmien kanssa on testattava. Asiakastietolakiin suunnitellaan myös Kelalle oikeutta valvoa palveluiden ja säilytettävien tietojen käyttöä tietoturvan lisäämiseksi. Asiakastietolaissa THL:llä on määräyksenantovaltuuksia, joihin kuuluvat mm. valtuudet ulottaa tietoturvavaatimukset koskemaan myös B-luokan järjestelmiä, ja esimerkiksi teknisen tietoturvatestauksen sisällyttäminen vaatimuksenmukaisuuden todentamiseen. [96] Terveyden ja hyvinvoinnin laitoksen tiedonhallinnan koulutusmateriaaleista löytyy tietoa terveydenhuollon tietojärjestelmien vaatimuksista ja sertifioinnista.

Myös **tietojen salaus** on järjestelmäarkkitehtuurin suunnittelussa otettava huomioon. Organisaation on syytä hyödyntää ja kehittää salausta suunnitelmallisesti osana arkkitehtuurin kehitystä. Salauksen tarve vaihtelee riippuen siitä, millaisissa tietojärjestelmissä tietoa käsitellään ja miten. Keskeistä on, että salaaminen on toteutettu oikein tietoaineiston koko elinkaaren ajan, tietojenkäsittelyn kaikissa vaiheissa. Vahti-ohjeesta 2/2015, Ohje salauskäytännöistä, löytyy hyviä käytännöllisiä ja teknisiä ohjeita salaukseen organisaation sisä- ja ulkopuolella, sekä tiedon salauksen **tarkistuslistat.** [97]

Tietojärjestelmät ja tilannetietoisuus

Organisaation tietojärjestelmistä, niiden kriittisyydestä, ja järjestelmien välisistä riippuvuussuhteista on syytä pitää kirjaa ja arvioida, mitkä ovat kunkin järjestelmän riskit, miten järjestelmät vaikuttavat toisiinsa ja mitä tapahtuu, jos jokin näistä ei enää toimi. On tärkeää tietää mitä tuotteita, ja millä laite- ja käyttöjärjestelmäversiolla, verkkoon on liitetty ja säännöllisesti tarkistaa, että uusimmat päivitykset ja paikkaukset on asennettu. Toimistoympäristö on yleisesti ottaen huomioitu organisaatioissa hyvin, mutta esimerkiksi lääkintä- ja kiinteistöautomaation laitteita ei välttämättä ole kattavasti kartoitettu.

Häiriötilanteiden vaikutuksista järjestelmien kesken on muodostettava riittävä ymmärrys. Poikkeamanhallinnan prosessien ja toimintaohjeiden kannalta on tärkeää ymmärtää kybertoimintaympäristö kokonaisuudessaan, jotta päätöksiä ei tehdä liian vähäisillä taustatiedoilla. Tietojärjestelmien inventointi ja tilannetietoisuuden ylläpitäminen onkin jatkuva prosessi.

Tietojärjestelmien turvallisuuden tasoa voi selvittää esimerkiksi penetraatiotestauksella. Penetraatiotestauksessa testataan järjestelmää tietoturvariskien osalta. Testauksessa suoritetaan samoja toimenpiteitä kuin aidoissa hyökkäyksissä, kuitenkin aiheuttamatta kohteelle vaaraa. Tietojärjestelmien säännöllinen testaus parantaa tilannetietoisuutta.

[93] Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2019
[94] Procurement Guidelines for Cybersecurity in Hospitals, ENISA 2020
[95] Miten lääkinnällisistä laitteista tehdään digiturvallisia?, Huld 2020
[96] Tiedotustilaisuus Vastaamo-tietomurron jatkotoimenpiteistä. 12.11.2020 klo 13.30, valtioneuvosto
[97] Ohje salauskäytännöistä. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 2/2015, valtiovarainministeriö

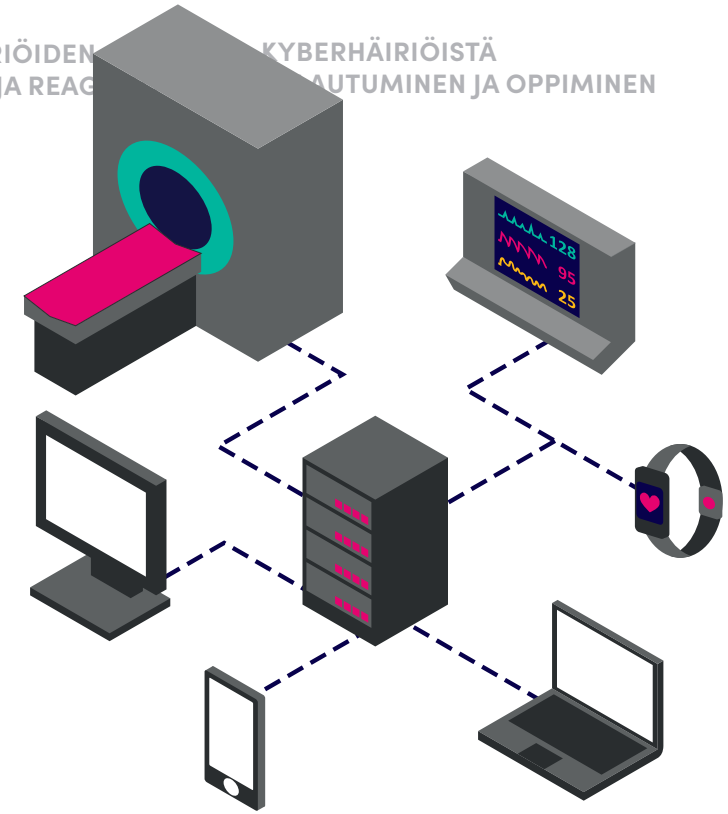
Tietojärjestelmien kriittisyysluokittelu

Tietojärjestelmät voidaan luokitella esimerkiksi erittäin kriittiseen, kriittiseen, erittäin tärkeään ja tärkeään. Erittäin kriittiseksi määritellyn järjestelmän on oltava suojattu kriisitilanteita varten erityisen hyvin. Esimerkiksi, että varajärjestelmä on kytketty eri virtalähteeseen kuin ensisijainen järjestelmä ja siten häiriötapauksessa virransaanti on varmistettu. Kriittiseksi luokitellulle tietojärjestelmälle on oltava tiedossa myös toipumisaika (RTO, Recovery Time Objective) eli pisin toiminnan sietämä käyttökatko sekä toipumispiste (RPO, Recovery Point Objective), joka kertoo, kuinka pitkältä ajalta saatetaan tietoa menettää sekä tietojärjestelmän vastuuhenkilö [40]. Jos järjestelmä on riippuvainen ulkopuolisesta palvelusta, on otettava huomioon palvelutuottajan palautumistavoitteet oman järjestelmän lisäksi. On hyvä muistaa, että pienikin palvelu voi olla kriittinen ja varmistaa, että sen olemassaolo on otettu huomioon. Ongelmia luokittelussa voi tuottaa se, että jotkin sairaalan järjestelmät ovat vanhoja, jopa 80-luvulta peräisin. Eri sairaanhoitopiirien kesken on myös suuria eroja. Järjestelmämäärä voi vaihdella 300–1000 välillä ja jokin yksittäinen järjestelmä voi olla toisessa organisaatiossa kriittinen ja toisessa ei. Tietojärjestelmien kriittisyysluokittelu on jatkuvaa työtä, jota arvioidaan uudelleen hankinto- ja tehdessä tai ympäristön muulla tavoin muuttuessa. Organisaation on myös nimettävä vastuuhenkilö varmistamaan luokittelun ajantasaisuus.

Kriittisyysluokittelun tukena voi käyttää VAHTI-ohjeista löytyvää BIA-vaikutusarviotyökalua. Työkalu on Excel-pohjainen taulukko, jonka avulla voidaan mm. luokitella tietojen ja kohteiden tietoturva- ja ICT-varautumista, tietoturvallisuuden tärkeyttä ja palvelutasotavoitteita, häiriöiden vaikutuksia sekä keskeisiä riippuvuuksia. [98]

Kriittisyysluokittelussa on arvioitava, kuinka nopeasti potilasturvallisuus vaarantuu järjestelmän vikaantuessa, minkälaiset varajärjestelyt auttaisivat kriisitilanteessa ja kuinka hyvin tällä hetkellä häiriöihin on varauduttu [99]. Potilasturvallisuuden lisäksi on hyvä miettiä, miten tietyn järjestelmän häiriö vaikuttaisi organisaation maineeseen, ja kuinka suuret kustannukset siitä voisi aiheutua [55]. Esimerkki potilasturvallisuuden kriittisyysluokista: [99]

1. Potilasturvallisuus voi vaarantua välittömästi, jos järjestelmä ei ole käytössä ja toimintaprosessi katkeaa häiriön takia.
2. Potilasturvallisuus voi vaarantua erittäin pian, jos järjestelmä ei ole käytössä ja toimintaprosessi katkeaa häiriön takia.
3. Potilasturvallisuus vaarantuu, jos järjestelmä ei ole käytössä kohtuullisen ajan kuluessa.



4. Odottamattoman käyttökatkoksen, tietojen menetyksen ja vanhenemisen vaikutukset

Arvioinnissa valinnoissa käytettävät vaihtoehdot 0-5:					
5	Sietämättömät	3	Merkittävät	1	Ei vaikutusta
4	Kohtuuttomat	2	Jonkin verran	0	Ei arvioitu

Odottamattoman katkoksen vaikutukset arviointialueille (1-5):	Painotus	oma	Omalle organisaatiolle	Kumppaneille tai alihankintatahoille	Asiakkaille tai loppukäyttäjille	Muulle osapuolelle… Yhteiskunnalle
Terveyden tai hengen vaara	1,20	1,20	1 Ei vaikutuksia	1 Ei vaikutuksia	4 Kohtuuttomat	1 Ei vaikutuksia
Lakisääteiset tehtävät	0,80	0,80	3 Merkittävät	3 Merkittävät	2 Jonkin verran	1 Ei vaikutuksia
Taloudelliset vahingot	1,00	1,00	3 Merkittävät	4 Kohtuuttomat	1 Ei vaikutuksia	3 Merkittävät
Mainevaikutukset	1,00	1,00	5 Sietämättömät	5 Sietämättömät	1 Ei vaikutuksia	2 Jonkin verran
Tärkeysindeksi:		3,50				
Tärkeysluokka:		Tärkeä				

Ote VAHTI-ohjeiden BIA-vaikutusarviotyökalusta, jolla voidaan arvioida yksittäisen järjestelmän kriittisyyttä [98]

[98] BIA-vaikutusarviotyökalu, Valtiovarainministeriö 2016
[99] Miten varmennan ICT:n kriittisessä toimintaympäristössä?, Tommi Tervo, Istekki Oy 2018

Tekninen jäljitettävyys

Lokit ovat organisaation järjestelmistä kerättäviä tapahtumatietoja, joista nähdään esimerkiksi, milloin ja kuka on kirjautunut tietojärjestelmään ja mitä tietoja on muutettu. Lokeja voidaan käyttää häiriötilanteiden selvittämisessä. Niiden seuranta auttaa tilanteen ymmärtämisessä, mutta myös korjaustoimenpiteissä ja häiriötilanteista palautumisessa. Tiedonhallintalaki myös velvoittaa viranomaisia huolehtimaan tarpeellisten lokitietojen keräämisestä. [38] Kyberturvallisuuden nykytila eri toimialoilla -kartoituksen mukaan parhaisiin käytäntöihin perustuva lokituspolitiikka on perusperiaate hyvälle ja ajantasaiselle tilannekuvan muodostamiselle. Kartoituksen mukaan useilla toimijoilla on kuitenkin tässä kehittämisen varaa. [62] Myös Kyberturvallisuuskeskus pitää puutteellista lokitietojen keruuta, seuraamista ja säilyttämistä yhtenä merkittävimpänä pidemmän aikavälin kyberuhkana suomalaisissa organisaatioissa [100].

Lokitietojen tallennuksessa luottamuksellisuus on tärkeää. Luvaton käsittely on estettävä ja varmuuskopiointi tehtävä säännöllisesti [44]. Hyvä käytäntö on välittää lokitiedot reaaliaikaisesti keskitettyyn lokienhallintajärjestelmään, jossa niiden eheys pystytään varmistamaan. Tämä vähentää myös lokitietojen menettämisen riskiä tilanteessa, jossa häiriön takia tietojärjestelmiä joudutaan uudelleenkäynnistämään tai asentamaan. [54] Keskitetyn lokienhallinnan lisäksi on hyvä olla käytössä SIEM-järjestelmä, joka auttaa reaaliaikaisen lokitiedon analysoinnissa ja tilannekuvan muodostamisessa [101]. On olennaista määritellä tarkasti mitkä tiedot tapahtumista tallennetaan, keillä on pääsy lokitietoihin ja miten kauan tietoja säilytetään. Esimerkiksi tietomurto voi tulla ilmi vasta kuukausien, jopa vuosien, jälkeen. Jos häiriön aikaiset lokit ovat tallessa, niistä voi olla suuri hyöty. Lokien kerääminen ja analysointi voi auttaa myös jo häiriön aikana tilannekuvan muodostamisessa ja toipumisen suunnittelussa.

Turvallisuustapahtumat	Verkkolokit	Sovellukset ja laitteet	IT-infrastruktuuri
Palomuurit, virustorjunta, haittaohjelmientorjunta, tunkeutumisen havaitsemisjärjestelmä (IDS), tietojen menetyksen estämispalvelu (DLP), VPN-keskittimet, web-suodattimet, hunajapurkit	Reitittimet, kytkimet, DNS-palvelimet, langattomat tukiasemat, WAN, virtuaalinen yksityinen pilvipalvelu (VPC)	Sovelluspalvelimet, tietokannat, intranet-sovellukset, web-sovellukset, SaaS-sovellukset, pilvipalvelut, työntekijöiden tietokoneet, mobiililaitteet	Konfiguraatio, sijainnit, omistajat, verkkokartat, haavoittuvuusraportit, ohjelmistoluettelot

Erilaisia lokilähteitä [103]

Kun jokainen käyttäjä kirjautuu järjestelmiin omilla tunnuksillaan, lokitieto toimii ikään kuin kyseisen henkilön allekirjoituksena. Organisaatiossa onkin syytä korostaa, että omia tunnuksia ei anneta muiden käyttöön.

Lokitietojen määrittely ja saatavuus on tärkeää määritellä myös ulkoistettujen palvelujen hankintavaiheessa. Palveluntarjoajan voi olla usein vaikea eritellä yhden tietyn asiakkaan lokeja muiden asiakkaiden lokitiedoista. Kriittisten palveluiden kohdalla on sopimuksissa syytä määritellä, miten ja millä aikataululla lokien on oltava saatavilla. Myös lainsäädäntö ja vaatimukset koskien tietojen käsittelyä ja tallennusta, on tunnistettava. Erityisesti, jos kyseessä on tietosuojan alainen tieto, kuten henkilötiedot. [102]

Sosiaali- ja terveydenhuollon asiakastietolaki edellyttää muun muassa, että palvelunantaja kerää lokitiedot kaikesta asiakastietojen käytöstä ja asiakastietojen luovutuksesta [73]. Hallituksen uudessa lakiesityksessä (HE 212/2020 vp, asiakastietolaki) edellytetään käyttölokitietojen tallentamista myös Kanta-palveluihin sekä mahdollisuutta näyttää näitä tietoja Omakanta-palvelussa. [96]

Ohjeita organisaation lokituksen järjestämiseen:

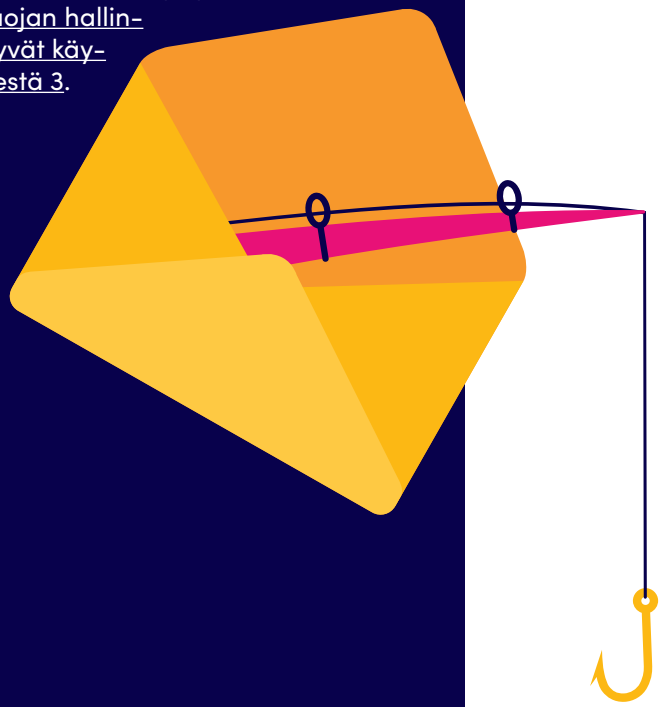
- Lokien keräys ja käyttö - Ohje lokitietojen tallentamiseen ja hyödyntämiseen [104]
- Näin keräät ja käytät lokitietoja [105]
- Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, Lokitietojen kerääminen (TiHL 17§) [38]
- Vahti 3/2009 Lokiohje [106]

[100] Kybersää Syyskuu 2020, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus
[101] Tietoturvapoikkeaman havaitseminen suuressa organisaatiossa, Ollikainen T. 2018
[102] Kyberhäiriötilanteet – Varautuminen ja toiminta, Huoltovarmuusorganisaatio 2019
[103] Tilannetietoisuuden kasvattaminen organisaation kybertoiminta-ympäristössä, Sara Sallinen Opinnäytetyö JAMK 2019
[104] Lokien keräys ja käyttö – Ohje lokitietojen tallentamiseen ja hyödyntämiseen, Viestintävirasto 2016
[105] Näin keräät ja käytät lokitietoja, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020
[106] Lokiohje, Valtionvarainministeriö 2009

Kyberhäiriöihin varautumisen tarkistuslista

Häiriöihin varautumisessa on syytä miettiä, mitkä ovat ne asiat, joita mahdollinen hyökkääjä saattaisi omasta organisaatiosta yrittää tavoitella. Kyberuhkat ja hyökkäystavat tulisi analysoida käyttäen samoja tekniikoita, taktiikoita ja menettelytapoja kuin mahdollinen hyökkääjä [107]. Tähän tarkistuslistaan on koottu keinoja ennakoida terveydenhuoltoon kohdistuvia, erityisesti kriisiaikana esiin nousseita yleisimpiä häiriöitä ja uhkia.

Yksi laajahko tarkistuslista toimenpiteistä organisaation tietoturvallisuuden ylläpitoon löytyy myös Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt -ohjeen liitteestä 3.



Tietojenkalastelu

Tietojenkalastelussa hyökkääjän tavoitteena on saada haltuunsa työntekijän käyttäjätunnus ja salasana. Jos käsittelet sähköpostilla potilas- ja asiakastietoja, saa sähköpostiisi murtautuja nekin tiedot haltuunsa viestihistoriasta. Asiakastietojen käsittely sähköpostilla saattaa olla kielletty työpaikallasi ja tämä on yksi syy siihen.

- Sähköpostin liitetiedostojen suorittava sisältö estetty
- Makrojen suorittaminen estetty Office-sovelluksissa [108]
  → Vaihtoehtoisesti vain organisaation allekirjoittamat/luotetun tahon allekirjoittamat makrot sallittu
- PowerShell-komentojen ajaminen työasemilla estetty [108]
  → Tai vähintään PowerShellin kutsuminen makrojen välityksellä estetty
- Sähköpostien autentikointi käytössä
  → SPF / DKIM ja DMARC [109]
- Henkilökunta koulutettu
  → Tunnistamaan sähköpostihuijaus [110]
  ↳ viesti tullut tutulta henkilöltä, mutta aihe epätyypillinen
  ↳ lähettäjä tai osoite tuntematon/epäilyttävä
  ↳ viestissä on kirjoitusvirheitä ja viesti tuntuu epäilyttävältä
  ↳ viesti on lähetetty poikkeavana ajankohtana, esim. yöllä
  ↳ viesti sisältää linkin tai liitteen, joka vaikuttaa epäilyttävältä
  ↳ viestissä kehotetaan tarkistamaan omat tiedot linkin kautta tai liitteestä
  ↳ jos viesti epäilyttää, varmistetaan aitous lähettäjältä puhelimitse tai kasvokkain
  ↳ salattuja zip-liitetiedostoja ei avata [108]
  → Tunnistamaan kalastelusivusto [110]
  ↳ Ei avata epäilyttäviä linkkejä
  ↳ luetaan tarkkaan ruudulle ilmestyvät ilmoitukset ja ikkunat, harkitaan ennen niihin reagoimista
  ↳ selataan ja ladataan sisältöä, kuvia ja tekstejä vain luotettavista lähteistä
  → Tietoturvalliseen käyttäytymiseen [110]
  ↳ säilytetään salasanat ja koodit niin, etteivät ne voi joutua vieraan käsiin
  ↳ ei jätetä tietokonetta auki omilla tunnuksilla edes hetkeksi
  ↳ ei anneta tunnuksia muille
  ↳ ollaan tarkkana, mihin palveluun syötetään henkilökohtaisia tietoja
  ↳ silputaan tai laitetaan tietosuojajätteeseen potilas-, käyttäjätunnus-, salasana- ja henkilötietoja sisältävät paperit
  ↳ ei kytketä laitteisiin tuntematonta muistitikkua tai -korttia [50]
  ↳ kiinnitetään huomiota ulkopuolisiin henkilöihin, tarkistetaan kulkukortit [50]
  ↳ käytetään kulkukorttia [50].

[107] Prepare, hunt and respond, JYVSECTEC
[108] Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020
[109] SPF, DKIM and DMARC brief explanation and best practices, End Point 2014
[110] Vältä kyberkömmähdyksiä, Tehy-lehti 9/2020

Kiristyshaittaohjelmat

Kiristyshaittaohjelmahyökkäyksessä tietojärjestelmät otetaan haltuun ja salataan niin, että tietoja ei enää pääse käsittelemään. Tietojärjestelmät luvataan palauttaa käyttöön maksua vastaan, mutta lupauksen toteutumisesta ei ole mitään takeita. Kiristäjä saattaa uhata myös kaapattujen tietojen paljastamisella. Lunnaita ei kuitenkaan missään tapauksessa pidä maksaa.

- Varmuuskopiot luotu 3–2–1 säännön mukaan (3 kopiota, 2:lla eri tallennusvälineellä, 1 niistä eri sijainnissa)
- Kopioilta palauttaminen testattu ja harjoiteltu
- Myös taustajärjestelmät ja alustat (Active Directory käyttäjätietokanta/hakemistopalvelu ym.) varmuuskopioitu
- Toimintamallit ja päätöksenteko sovittu kriisin varalle
  → Mukaan lukien alihankkijat ja sopimuskumppanit
- Kirjautumiseen vahvennetut säännöt
  → Vahvat salasanat
  → Monivaiheinen tunnistautuminen internetin kautta kirjautuessa
- Käytössä vain tarpeelliset palvelut, tarpeettomat poistettu
- Ohjelmistojen haavoittuvuuksia minimoidaan säännöllisellä ja ripeällä päivittämisellä
- Lokien kattava kerääminen suunniteltu ja toteutettu [105].

Huijaus/petos

Koronakriisi on nostanut esiin olemattomien suojainvarusteiden kaupittelun. Myös esimerkiksi tekaistujen laskujen lähettäminen organisaatioille siinä toivossa, ettei laskun aiheellisuutta tarkisteta, on yleistä.

- Henkilöstö koulutettu huijausyritysten tunnistamiseksi
- Henkilöstön jatkuva kouluttaminen ja tiedottaminen ajankohtaisista uhkista
- Laskujen käsittelyyn laadittu toimintatavat laskutushuijausten havaitsemiseen
- Ohjeet ja käytännöt laadittu poikkeamien ilmoittamiseen.

Ohjelmistohaavoittuvuudet

Kyberhyökkäyksissä hyödynnetään usein ohjelmistojen haavoittuvuuksia eli niihin jääneitä ohjelmointivirheitä.

- Lääkintälaitteiden ja tieto- ja viestintäteknisten laitteiden ja järjestelmien inventaario ajan tasalla
- Ylläpidon prioriteetti määritelty
- Korjauspäivitysten hallintaprosessit käytössä
- Valmistajien tietoturvatiedotteita seurataan
- Tarpeettomat palvelut ja toiminnot poistettu
- Verkot segmentoitu käyttötarkoituksen mukaan.

Etätyö

Organisaation täytyy huomioida huomattavassa määrin ja nopeassa tahdissa lisääntyneen etätyön vaikutukset tietoturvallisuudelle. Se miten etätyössä toimitaan, mitä tietoja ja millä välineillä saa käsitellä, on tärkeää määritellä selkeästi.

- Kapasiteetin riittävyys etätyölle varmistettu
  → Yhtenä apukeinona VPN split -tunnelointi [111]

- Etätyön tietoturvaohjeet laadittu, ja henkilöstö koulutettu toimimaan niiden mukaisesti
  → Sovittu, mitä tietoja etänä voidaan käsitellä
  → Sovittu, mitä laitteita työssä käytetään
  → Laitteiden ja ohjelmistojen päivityksistä ja suojauksista huolehditaan tietohallinnon ohjeiden mukaisesti
  → Lähiverkossa käytössä suojattu yhteys ja salasana
  → Huijausyrityksistä ja muista mahdollisista häiriöistä ilmoitetaan välittömästi tekniseen tukeen

- Verkonvalvonnalla/SOC:lla kyky tunnistaa sallitut ja luvattomat etäyhteydet [3]

- Työvälineiden riittävä salaus, kaksivaiheinen tunnistautuminen ja pääsyrajaukset [112]
  → Erityisesti huomioitu organisaation verkon ulkopuolelta kirjautumisessa

- Selvitetty työvälineiden ja pilvipalveluiden oikeudet ja tietojen luovuttaminen kolmansille osapuolille [112]
  → Pilvipalvelujen turvallinen käyttö varmistettu esim. Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) avulla

- Järjestelmien toimittajat sitoutettu organisaation toimintamalliin jo sopimusta tehtäessä (etäyhteyksien tekniset vaatimukset ja käyttötavat) [3]

- Etätyössä käytetyissä työvälineissä näkyy selkeästi ero sisäisen ja ulkoisen tiedonvälityksen välillä [112].

Automaatiojärjestelmät ja esineiden internet (IoT)

Sairaaloissa on käytössä erilaisia lääkinnällisiä automaatiojärjestelmiä, mutta myös kiinteistöautomaatiota, kuten mm. lukitusjärjestelmät ja lämmityksen ja ilmastoinnin ohjaus. Kaikki laitteet on syytä kartoittaa ja suojata asianmukaisesti.

- Laitekanta kartoitettu
- Laitteet suojattu verkon segmentoinnilla
- Laitteet fyysisesti suojattu

- Palomuuri [93]
  → Laitteessa tai laitteen ja internetin välissä
  → Vain tietyistä IP-osoitteista ja tiettyyn porttiin liikenne sallittu

- Poistettu käytöstä tarpeettomat ja turvattomat palvelut (esim. Telnet-yhteysprotokolla) [93].

- Mobiililiittymillä yhdistetyt laitteet myös suojattu, ja poistettu liittymistä mahdollisuus maksullisiin palveluihin [93]

[111] VPN-yhteyksien kapasiteetin varmistaminen, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020
[112] Ohjeita turvallisten etätyövälineiden valintaan, Huoltovarmuusorganisaatio 2020

Kyberhäiriöiden käsittely ja reagointi

Kyberhäiriöön varautuminen ei välttämättä riitä estämään kaikkia mahdollisia poikkeamatilanteita, jos sairaalaan tai terveydenhuollon organisaatioon kohdistetaan hyökkäys kyvykkään uhkatoimijan toimesta. Kyberhäiriöön reagointi muodostuu tällöin merkittäväksi. Reagointi kuten varautuminenkin tulee suunnitella, valmistella ja harjoitella ennen kuin tilanteeseen joudutaan. Kyberhäiriötilanteen hallinta (cyber incident management) ja vaste-/reagointitoiminta (incident response) ovat määritettyjä prosesseja poikkeamien tutkintaan, analysointiin ja ratkaisemiseen sekä palautumiseen. Kyberhäiriö on toteutunut kyberuhka, joka haittaa liiketoimintaa tai järjestelmien toimintaa. Käsitteistöä on avattu laajemmin sivulla 10, kappaleessa Kriisin aikaisia kyberhäiriöitä. Kyberhäiriötilanteiden käsittely voidaan jakaa eri osa-alueisiin, joita ovat valmistautuminen, vaste ja ensiarvio (engl. triage), eristäminen ja palautuminen sekä jälkianalyysi.

> *Reagointi kuten varautuminenkin tulee suunnitella, valmistella ja harjoitella ennen kuin tilanteeseen joudutaan.*

Kyberturvallisuuspoikkeamissa keskeisessä roolissa on ensiarvion (cyber triage) tekeminen, jossa selvitetään mistä hälytyksessä/havainnossa/epäilyssä on oikeasti kyse. Triage-vaiheessa on tärkeää selvittää mitä on tapahtunut, koska on tapahtunut ja mikä on vaikuttavuus liiketoimintaan. Jokaisesta hälytyksestä/havainnosta ei välttämättä muodostu häiriötä, mutta ne on tärkeää käsitellä Triage-prosessin mukaisesti, jotta ei virheellisesti sivuuteta todellista kyberhyökkäystä.

Kyberhäiriötilanteen käsittelyn ajallinen pituus riippuu paljon tapahtuman vakavuudesta ja monimutkaisuudesta. Yksinkertaisimpien poikkeamien käsittely tapahtuu nopeasti muutamissa minuuteissa, mutta monimutkaisempien tapauksien tutkinta ja käsittely sekä palautuminen voi viedä aikaa viikkoja.

Kyberhäiriötilanteen ja -poikkeaman käsittelyssä on tärkeää huomioida kokonaistilanteen hallinta sekä varmistua kattavasta selvitystyöstä ja oppien sekä kehityskohteiden keräämisestä. Tämä mahdollistaa organisaation jatkuvan kehittymisen myös tulevien hyökkäyksien estämiseen ja tutkintaan.

Tilannekuva tapahtumasta

Kyberhäiriötilanteen reagoinnissa merkittävässä roolissa on jatkuvan tilannekuvan ylläpitäminen ja sen hyödyntäminen. Tilannekuvassa oleellista on huomioida mm. rajallisten resurssien järkevä hyödyntäminen, kyberhyökkäyksen vaikutus organisaation toiminteisiin ja viestintä. Tilannekuvaa on myös tärkeä päivittää selvitystyön edetessä. Kyberhäiriötilanteeseen reagoinnissa on oleellista toimenpiteiden suunnitelmallisuus, toimenpiteiden kirjaaminen sekä kokonaiskuvan ymmärtäminen. Näitä varten organisaation on suunniteltava tapa koostaa tilannekuvaa varten tietoa sekä johtaa tilannetta sekä operatiivisella (käytännön toimenpiteitä tekevällä tasolla) että strategisella tasolla (ylemmällä johdolla).

Vastetoiminnan ja reagoinnin prosessi

Kyberpoikkeamien ja kyberhäiriötilanteiden käsittelyprosessi, myöhemmin IR (Incident Response) -prosessi, on osa organisaation tietoturvanhallinnan kokonaisprosessia. IR-prosessin tarkoituksena on kuvata tarkemmalla tasolla, miten havaintojen ja häiriöiden käsittely tehdään operatiivisella tasolla. Operatiivisella tasolla tarkoitetaan tässä IR-prosessin käytännön työhön osallistuvia tahoja (esimerkiksi: tekniset asiantuntijat, järjestelmien pääkäyttäjät, tietoturvapäällikkö, tietosuojavastaava, viestintä). Nämä tahot tulee olla määritettynä ennakkoon ja tarvittaessa IR-prosessiin voidaan ottaa lisähenkilöitä käsittelemään kyberhäiriötilannetta tarpeen vaatiessa. IR-prosessin tulee sisältää koko häiriön elinkaareen liittyvän toimintamallin kuvauksen. Esimerkkiviitekehyksiä IR-prosesseihin ovat julkaisseet mm. ISO (27035:2016), SANS, NIST ja JYVSECTEC. Lisäksi Sosiaali- ja Terveysministeriön julkaisussa (Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille, kohta Kyberhäiriötilanteen hallinta) on yleiskuvaus kyberhäiriötilanteeseen liittyvästä valtakunnallisesta hallintamallista pohjautuen terveydenhuollon rakenteeseen. Jos ensiarvion perusteella kyseessä epäillään olevan kyberhäiriö, on tietojärjestelmän omistajan käynnistettävä useita toimenpiteitä. Nämä toimenpiteet ja niiden järjestys häiriön vakavuuteen ja vaikutuksiin pohjautuen on esitetty hallintamallissa. [3]

Organisaation tulee soveltaa ohjeistuksia oman toimintansa mahdollistamiseksi. IR-prosessi perustuu systemaattiseen työhön eri vaiheissa häiriön-/ poikkeamankäsittelyä. Tavoitteena IR-prosessissa on tehokas ja selkeä operatiivinen käsittely häiriöille/poikkeamille sekä jatkuvan kehittämisen malli tapahtuneiden tilanteiden oppien ja kokemuksien kautta. Kantavana teemana on kattavat jälkianalyysit ja sieltä tulevat kehityskohteet operatiiviseen toimintaan kaikissa edellä mainituissa esimerkkiviitekehyksissä.

Huomioita ja suosituksia IR-prosessiin

IR-prosessia suunniteltaessa tai kehitettäessä tulee huomioida, että on olemassa selkeä kuvaus, miten kyberhäiriöiden ja -poikkeamien luokittelu tehdään. Esimerkiksi luokittelua voi tehdä häiriötyypin, vakavuuden, vaikuttavuuden, uhkatapahtuman tai palautumisen kannalta. Lisäksi on tärkeää suunnitella sekä määrittää IR-prosessin toteuttamiseen roolit ja niille nimetyt vastuuhenkilöt sekä varahenkilöt. Mikäli kyberhäiriö/-poikkeamatilanne tapahtuu, tulee organisaatiolla olla selkeä malli tilanteen seurantaan sekä dokumentointiin.

Esimerkki dokumentoinnin kohteista: ▶▶▶

Case ID: ID-numero

Havaintoajankohta: Päivämäärä ja kellonaika ensimmäiselle havainnolle

Vaikuttavuus organisaation toimintaan:

Nimi: Kuvaava nimi

Luokittelu: Häiriötyyppi, vakavuusaste, vaikuttavuus, uhkatapahtuma tai palautuminen

Kuvaus: Lyhyt kuvaus mistä häiriössä on kyse

Kohdeympäristö: Missä ympäristössä kyberhäiriötilanne ilmenee

Laajuus: Kuinka monta järjestelmää/asiakasta/käyttäjää häiriö koskee

Toimenpiteet: Kuvaus tehdyistä tutkinnallisista toimenpiteistä (kuvaus ja kellonaika)

Tarkistuslistat: Mitä tarkistuslistoja on käyty läpi?

IoCt: Mitä tunnistetietoja on löydetty kyberhäiriön tutkinnan aikana?

Vastatoimet: Mitä vastatoimia on tehty (kontrollit, muurisäännöt yms.), tekijä, ajankohta, järjestelmä?

Juurisyy: Miksi häiriö on tapahtunut?

Muistiinpanot: Häiriöön liittyvien muistiinpanojen kirjaaminen

Sulkemisajankohta: Päivämäärä ja kellonaika kun häiriö suljettiin

Tarkistuslistat kyberhäiriön tekniseen käsittelyyn

Seuraavat tarkistuslistat on suunnattu erityisesti kyber- ja digiturvallisuuden parissa työskenteleville asiantuntijoille sekä kyberhäiriön teknisestä käsittelystä kiinnostuneille.

Yleinen tapahtumien kulku kyberhäiriön/-poikkeaman teknisessä käsittelyssä

Poikkeaman havaitseminen

1. Varmistetaan, että kyseessä on oikeasti poikkeama/häiriötilanne
2. Ilmoitetaan poikkeamasta organisaation prosessien mukaisesti vastuulliselle taholle
3. IR-prosessia johtava henkilö määrittää toimenpiteet henkilöille ensiarvion (triage) suorittamiseksi
4. Toteutetaan ensiarvio erillisten ohjeiden perusteella, ks. Ensiarvio-vaiheen (triage) tekninen tarkistuslista
5. Aloitetaan dokumentoimaan havaitut/löydetyt tapahtumat ja suoritetut toimenpiteet aikajanalle
6. Suoritetaan tarkempi analyysi tapahtuneesta, dokumentoidaan ja suunnitellaan vastatoimet, ks. Tarkemman analyysin tarkistuslista
7. Suoritetaan vastatoimet ja dokumentoidaan ne
8. Varmistetaan vastatoimien onnistuminen ja dokumentointi
9. Järjestetään poikkeaman jälkianalyysi ja raportoidaan poikkeama raportointiohjeiden mukaisesti

Poikkeaman sulkeminen

Ensiarvio-vaiheen (triage) tekninen tarkistuslista

- Selvitä milloin poikkeama ensimmäisen kerran havaittiin
  - → Mistä havainto tuli?
  - → Varmista havainnon paikkansapitävyys

- Selvitä onko joku jo tutkinut poikkeamaa
  - → Onko organisaatiossa joku käsitellyt samaa asiaa?
  - → Onko julkisista lähteistä saatavilla olevista tiedoista nähtävissä vastaavaa?

- Selvitä mikä vaikutus poikkeamalla on organisaation kriittisiin palveluihin
  - → Mihin organisaation kriittisiin palveluihin poikkeamalla on vaikutus?
    - ↳ Onko poikkeamalla vaikutusta potilashoitoon?
  - → Kuinka moneen asiakkaaseen/käyttäjään poikkeama vaikuttaa?
  - → Onko poikkeamalla selkeitä vaikutuksia potilasturvallisuuteen?

- Selvitä mihin järjestelmiin poikkeama vaikuttaa
  - → Mitkä järjestelmät ovat kohteena?
  - → Mihin järjestelmiin kohteena olevista järjestelmistä on pääsy?
  - → Mihin järjestelmiin kohteena olevat järjestelmät vaikuttavat?
  - → Onko hallintaympäristön järjestelmät kohteena?

- Selvitä mihin tietoihin poikkeama vaikuttaa
  - → Onko henkilötietoihin päästy luvattomasti käsiksi?
  - → Onko organisaation luottamukselliseen tietoon päästy käsiksi?
  - → Onko organisaation potilastietoihin tai laitteistoihin päästy käsiksi?

Tarkemman analyysin tarkistuslista

Triage-analyysin perusteella valittujen järjestelmien tarkempi analyysi tehdään, jotta saadaan selkeämpi tieto siitä, miten poikkeama tapahtui ja miten se voidaan parhaalla mahdollisella tavalla mitigoida sekä miten kyberhäiriöstä/-poikkeamasta pystytään parhaiten palautumaan normaalitilanteeseen.

- Listaa järjestelmät ja niiden riippuvuudet muista järjestelmistä

- Varmista turvallinen pääsy kohdejärjestelmiin
  → Hyökkääjällä voi esimerkiksi olla järjestelmätason oikeudet kohdejärjestelmään, jolloin kirjautumalla järjestelmään voit menettää tunnuksesi hyökkääjälle

- Kerää paikalliset lokit järjestelmästä talteen analysointia varten

- Selvitä havainnon/hyökkäyksen alkuajankohta
  → Tämä voi olla haastavaa, mutta on tärkeää löytää ns. ensimmäinen jalansija
  → Ensimmäinen jalansija ei välttämättä ole siinä järjestelmässä mistä ensimmäinen havainto tuli

- Tutki järjestelmiin liittyvät palomuurit
  → Tarkista kohdejärjestelmään liittyvät palomuurin lokit
  → Tarkista palomuurin hälytykset
  → Tarkista avoimet istunnot (sessio), jotka liittyvät kohdejärjestelmiin

- Tutki järjestelmiin liittyvä Netflow-data
  → Selvitä mihin järjestelmästä on otettu yhteyksiä
  → Selvitä mistä järjestelmään on otettu yhteyksiä

- Tutki järjestelmiin liittyvät lokit
  → Selvitä lokeista kirjautumiset järjestelmään
  → Selvitä lokeista kirjautumiset järjestelmästä muualle

- Pyri selvittämään hyökkäyksen juurisyy (eli miten, milloin ja mitä hyödyntäen hyökkääjä on pystynyt hyökkäyksen tekemään)
  → Dokumentoi löydökset, IoC:t, toimenpiteet ja niiden ajankohdat sekä muistiinpanot

- Tee suunnitelma hyökkäyksen vaikutuksien minimoimiseen tai hyökkäyksen poistamiseen järjestelmistä

- Tee suunnitelma, miten palautuminen tästä hyökkäyksestä on järkevintä toimintaympäristössä tehdä. Huomioi aiheuttaako palautuminen potilashoitoa haittaavia vaikutuksia. Varmista palautuminen potilasturvallisuus huomioiden.

Tarkistuslistat uhkatapahtumittain

Tiedustelu, kalastelu ja käyttäjän manipulointi

Mikäli kyberhäiriö/-poikkeamatilanne koskettaa organisaation toiminnan teknistä tiedustelua on selvitettävä, liittyykö se johonkin menneeseen tai menossa olevaan kyberhäiriöön/-poikkeamaan. Muutoin teknisen tiedustelun tutkinta voi olla turhaa resurssien käyttöä varsinkin julkisten palveluiden osalta, koska niihin kohdistuu jatkuvasti erilaista skannausta ja tiedustelua. Teknisestä tiedustelusta on toisinaan toki hyödyllistäkin kerätä analyysitietoa, jotta voidaan todeta, onko ko. toiminta kasvanut merkittävästi. **Teknisestä tiedustelusta on tärkeää analysoida ja dokumentoida:**

- Tiedustelun ajankohta
- Kohdejärjestelmä(t)
- Tiedustelun menetelmä (porttiskannaus, käyttöjärjestelmän tunnistaminen yms.)
  - → Palomuurien lokitiedot
  - → Järjestelmän omat lokitiedot
  - → Netflow-data
- Käytetty protokolla ja portti
- Lähde IP-osoitteet ja maat

Kalasteluviestien osalta on tärkeää selvittää, onko kyse kohdennetusta kalastelusta (spear phishing) vai massatuotetusta kalastelusta. Kohdennetussa kalastelussa on tärkeää analysoida ja dokumentoida:

- Viestin saapumisajankohta
- Mistä kalasteluviesti on tullut?
- Onko vastaavaa kalasteluviestiä käytetty muualla maailmassa (onko julkisissa lähteissä tietoa asiasta)?
- Onko viestiä lähetetty muille organisaatiossa?
- Jos viestissä pyritään ohjaamaan käyttäjä huijaussivustolle
  - → Missä huijaussivustoa ylläpidetään?
  - → Onko mahdollista pyytää palveluntarjoajaa ottamaan sivusto pois verkosta?
  - → Onko mahdollista estää ko. sivuston käyttö organisaation verkosta?
- Palomuurien ja välityspalvelimien lokeista tulee selvittää, onko organisaatiosta liikennöity kyseiselle sivustolle
- Jos viestissä on liitetiedosto
  - → Onko sitä mahdollista analysoida organisaation sisäisillä työvälineillä?
  - → Onko liitetiedoston perusteella analysoitavissa mitä sovellusta se käyttää ja yrittääkö liitetiedosto hyväksikäyttää jotain haavoittuvuutta
- Millä menetelmällä käyttäjää on yritetty huijata aktivoimaan haitallinen koodi työasemassa?
- Valmistele kalasteluun liittyen ilmoituspohja organisaation viestinnän käyttöön

Massatuotetuissa kalasteluviesteissä on tärkeää analysoida ja dokumentoida:

- Mistä kalasteluviesti on tullut?
- Onko viesti lähetetty kaikille?
- Voidaanko viestistä löytää tunnusmerkkejä, joiden perusteella ne voidaan estää jo sähköpostipalvelimella?
- Valmistele kalasteluun liittyen ilmoituspohja organisaation viestinnän käyttöön

Käyttäjän manipuloinnissa (engl. social engineering) kyse voi olla fyysisesti tapahtuvasta tiedonkeräämisestä tai pääsyn saamisesta järjestelmiin ja fyysisiin tiloihin. Tällaisessa tilanteessa on tärkeää analysoida ja dokumentoida:

- Koska tilanne on ensimmäisen kerran tapahtunut?
- Missä tilanteessa käyttäjään otettiin yhteyttä?
- Millä välineellä käyttäjään oltiin yhteydessä?
- Mitä tietoa käyttäjä antoi yhteydenottajalle?
- Saiko hyökkääjä pääsyä suojattuihin tiloihin?
  - → Jos kyllä, onko tiloissa ylimääräisiä laitteita?
    - ↳ Jos kyllä, onko laite kiinni organisaation laitteessa/ympäristössä?
      - ↳ Jos kyllä, mihin laitetta käytetään ja mihin sillä on pääsy?
    - ↳ Jos kyllä, onko laite kytketty organisaation verkkoon?
      - ↳ Jos kyllä, mihin laitteesta on kommunikoitu organisaation verkossa?
    - ↳ Jos kyllä, onko laitteessa ulkoisia verkkoyhteyksiä (esim. 3G/4G/5G tai muut langattomat yhteydet)?

Palvelunestohyökkäys

Palvelunestohyökkäyksissä tilanne on usein kriittinen heti havainnosta lähtien. Tästä syystä on tärkeää selvittää palvelunestohyökkäyksen ominaispiirteet tarkasti, jotta mitigaatio on mahdollisimman tehokas. Palvelunestohyökkäyksestä on tärkeää analysoida ja dokumentoida:

- Kohdejärjestelmä ja palvelu, johon hyökkäys kohdistuu
- Alkamisajankohta
- Onko kyseessä volumetrinen (suuret liikenne-/käyttäjämäärät) hyökkäys?
  - → Jos kyllä, on tärkeää selvittää minkä tyyppistä liikenne on
    - ↳ Onko liikenne samankaltaista (protokolla, sovellus yms.) kuin palvelun normaali liikenne?
  - → Jos kyllä, on tärkeää tunnistaa liikenneprofiili, joka eroaa palvelun normaalista liikenteestä
    - ↳ Protokolla, portti, sovelluskohtaiset erityispiirteet (esim. DNS otsikkotiedot, HTTP otsikkotiedot)
    - ↳ Hyökkäysliikenteen volyymi: bitteinä sekunnissa ja paketteina sekunnissa
    - ↳ Muut mahdolliset eroavaisuudet normaalista liikenteestä
- Onko kyseessä muu palvelunestohyökkäys?
  - → Jos kyllä, onko kyse tietyn tyyppisestä liikenteestä palveluun?
  - → Jos kyllä, onko palveluun julkisesti tiedossa olevaa haavoittuvuutta, joka mahdollistaa palvelunestotilan?
    - ↳ Jos kyllä, onko julkisesti tiedossa, miten tehdä vastatoimia ko. haavoittuvuutta vastaan?
  - → Jos kyllä, käyttääkö hyökkäys HTTP(s) liikennettä?
    - ↳ Jos kyllä, onko HTTP menetelmä POST?
      - ↳ Jos kyllä, onko sivustolla lomaketta, jota hyökkäys hyödyntää?
    - ↳ Jos kyllä, onko HTTP menetelmä GET?
    - ↳ Jos kyllä, onko HTTP menetelmä joku muu kuin GET tai POST?

Työasemasaastuminen

Työasemien saastumisessa kyse voi olla usean asian yhteenliittymästä. Tämän vuoksi työasemien saastumisen tutkinta on tärkeää tehdä kattavasti ennen korjaustoimenpiteitä. Nykypäivän hyökkäykset kohdistuvat usein käyttäjien työasemiin, minkä vuoksi ne ovat myös monivaiheisia ensimmäisestä saastumisesta jalansijan lujittamiseen, hyökkääjän työkalujen asentamiseen ja toimenpiteiden suorittamiseen. Monet saastumisen vaiheista ovat hyökkääjän toimesta automatisoituja, joten usein ne tapahtuvat lyhyessä ajassa. **Työasemien saastumisessa on tärkeää analysoida ja dokumentoida:**

- Ensimmäisen havainnon ajankohta

- Mitä työasemalla on tehty ennen havaintoa?
  - → Sähköpostiviestit
  - → Uudet tiedostot
  - → Web-selaus ja lataukset
  - → Suoritetut ohjelmat

- Onko kyseessä kiristyshaittaohjelma?
  - → Jos kyllä, onko käyttäjän tiedostot salattu?
    - ↳ Jos kyllä, mitkä tiedostot ja mistä tiedostopolusta?
  - → Jos kyllä, onko käyttäjä tai organisaatio saanut kiristysviestin?
    - ↳ Jos kyllä, mitä kautta kiristysviesti tuli?
    - ↳ Jos kyllä, mitkä ovat vaatimukset?
    - ↳ Dokumentoi mahdolliset löydökset

- Tarkista työasemaan liittyvät mahdolliset hälytykset palomuurin lokeista tai keskitetystä lokienhallinnasta / SIEM:sta

- Tarkista löytyykö Netflow-datasta viitteitä epänormaalista liikenteestä
  - → Mitä uusia yhteyksiä on avattu havainnon jälkeen?

- Tarkista onko muissa työasemissa vastaavia havaintoja

- Tarkista löytyykö automaattisesti käynnistyviä sovelluksia työasemasta

- Tarkista löytyykö ajastettuja toimintoja

- Löytyykö työasemasta uusia prosesseja tai sovelluksia?
  - → Jos kyllä, onko prosessi tunnistettavissa jonkin ei-hyväksytyn sovelluksen/binäärin prosessiksi?
    - ↳ Jos kyllä, mitä verkkoyhteyksiä prosessilla on?
    - ↳ Jos kyllä, mitä tiedostoja prosessi käyttää?
    - ↳ Jos kyllä, millä käyttöoikeuksilla prosessia suoritetaan?
    - ↳ Jos kyllä, mistä tiedostopolusta sovelluksen/binäärin prosessi on käynnistetty?
  - → Jos ei, onko olemassa olevilla prosesseilla avoimia verkkoyhteyksiä Internetiin?
    - ↳ Jos kyllä, mitkä ovat yhteyksien tunnistetiedot (IP, TCP/UDP, portti)?
  - → Jos ei, onko olemassa olevilla prosesseilla avoimia verkkoyhteyksiä sisäverkon palveluihin?
    - ↳ Jos kyllä, mikä on normaalia verkkoliikennettä?
    - ↳ Jos kyllä, mikä on epänormaalia verkkoliikennettä?

- Tarkista löytyykö työaseman rekisteristä jotain poikkeavaa

- Onko työaseman ylläpitotyökaluja (Powershell yms.) käytetty työasemalla?
  - → Jos kyllä, onko nämä hyväksyttyjä ylläpidon toimenpiteitä?
    - ↳ Jos ei, mitä työkalua on käytetty ja mitä sillä on tehty?

- Käy läpi keskitetystä lokienhallinnasta/SIEM:stä löytyykö muista toimintaympäristöjen työasemista havaittuja tietoja verkkoyhteyksistä yms. löydöksistä

Tietomurto

Tietomurrolla tarkoitetaan tässä tapauksessa järjestelmään tai palveluun kohdistuvaa hyökkäystä, jossa käyttäjä/hyökkääjä on saanut pääsyn tietoon ja toimintaan, joihin hyökkääjällä ei ole oikeutta. Tietomurto voi tapahtua olemassa olevia käyttöoikeuksia käyttäen tai haavoittuvuutta hyväksi käyttäen. **Tietomurrossa on tärkeää analysoida ja dokumentoida:**

- Havainnon ajankohta
- Kohdejärjestelmä
- Onko kyseessä käyttöoikeuksien luvaton käyttö?
  - → Jos kyllä, minkä tason käyttöoikeuksista on kyse?
  - → Jos kyllä, onko hallintaympäristön ja/tai ylläpitäjän käyttäjätunnuksia käytetty?
- Onko kyseessä haavoittuvuuden hyväksikäyttö?
  - → Jos kyllä, millä menetelmällä järjestelmään on murtauduttu?
  - → Jos kyllä, onko haavoittuvuus julkisesti tiedossa?
    - ↳ Jos ei, valmistelkaa tietoaineisto haavoittuvuudesta ja ottakaa yhteyttä CERT-FI:hin (Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus) haavoittuvuuden koordinoimisesta
    - ↳ Jos kyllä, onko haavoittuvuudelle tarkempaa kuvausta hyväksikäyttömenetelmästä?
    - ↳ Jos kyllä, onko haavoittuvuudelle mitigaatiomenetelmää?
  - → Jos kyllä, onko organisaatiossa käytössä muita järjestelmiä samalla ohjelmistoversiolla
- Onko muissa järjestelmissä havaintoja vastaavista poikkeavuuksista?
- Mihin tietoon hyökkääjällä/käyttäjällä on järjestelmän kautta ollut pääsy?
  - → Onko tieto luokiteltua?
    - ↳ Jos kyllä, onko kyseessä organisaation salassa pidettävää tietoa?
    - ↳ Jos kyllä, onko kyseessä organisaation asiakkaiden salassa pidettävää tietoa?
  - → Onko järjestelmässä henkilötietoa?
    - ↳ Jos kyllä, ota yhteyttä tietosuojavastaavaan
    - ↳ Jos kyllä, onko tietoon päästy käsiksi?
      - ↳ Jos kyllä, selvitä kenen kaikkien tiedot ovat olleet hyökkääjän/käyttäjän nähtävissä/saatavissa
  - → Onko järjestelmässä potilastietoa?
    - ↳ Jos kyllä, onko tietoon päästy käsiksi?
      - ↳ Jos kyllä, selvitä kenen kaikkien tiedot ovat olleet hyökkääjän/käyttäjän nähtävissä/saatavissa
- Selvitä mitä tietoa on vuotanut hyökkääjälle
- Mistä lähde-IP-osoitteesta tietomurto on tehty?
- Mitä menetelmää hyökkääjä/käyttäjä on käyttänyt?
- Pystyikö hyökkääjä/käyttäjä suorittamaan haitallista koodia järjestelmässä?
  - → Jos kyllä, mikä prosessi tai sovellus on hyökkääjän/käyttäjän lisäämä?
  - → Jos kyllä, missä haitallinen koodi järjestelmässä sijaitsee?
  - → Jos kyllä, avaako haitallinen koodi hyökkääjälle komentokanavan järjestelmään?
    - ↳ Jos kyllä, millä kommunikaatiokanavalla järjestelmä ja hyökkääjän palvelin keskustelevat?
    - ↳ Jos kyllä, mikä on komentokanavan kohde-IP-osoite?
    - ↳ Jos kyllä, selvitä onko vastaavaa komentokanavaa käytetty muualla toimintaympäristössä?

Laajamittainen hyökkäys

Laajamittainen hyökkäys ei välttämättä ilmene välittömästi yksittäisestä havainnosta, vaan saattaa verhoutua eri tapahtumien kautta isommaksi kokonaisuudeksi. Laajamittaisella hyökkäyksellä tarkoitetaan hyökkäystä, jonka tavoitteena on lamauttaa organisaation operatiivinen toiminta osio kerrallaan tai vahingoittaa organisaation toimintakykyä laajamittaisesti. Laajavaikutteisessa hyökkäyksessä, kuten muissakin poikkeamissa, on tärkeää selvittää rauhassa mistä kaikesta on kyse ennen rajallisten resurssien kohdentamista eri tehtävien suorittamiseen. Kohdennetuissa hyökkäyksissä saatetaan käyttää myös selkeästi näkyviä hyökkäyksiä savuverhona, joilla resurssit pyritään kiinnittämään näkyvien hyökkäyksien tutkintaan ja selvittämiseen.

- Selvitä ensimmäisen havainnon alkuperä

- Tutki onko eri tietoturvakontrolleissa muuta epäilyttävää
  - → Tutki palomuurin lokit ja hälytykset
  - → Tutki päätelaitteiden tietoturvahälytykset
  - → Tutki sähköpostipalvelun hälytykset
  - → Dokumentoi mahdolliset löydökset

- Selvitä löytyykö muita viitteitä poikkeavuuksista

- Selvitä onko järjestelmistä avoimia hallintayhteyksiä muihin järjestelmiin

- Selvitä onko järjestelmistä avoimia C&C (komentopalvelin) yhteyksiä Internetiin
  - → Mitä protokollaa, IP-osoitetta, applikaatiota, palvelua käytetään
  - → Selvitä onko vastaavaa C&C-kanavaa auki muista järjestelmistä
  - → Dokumentoi IoC-tiedot C&C-yhteyksistä

- Selvitä toipumissuunnitelmasta kriittisimpien järjestelmien prioriteetti
  - → Tietoturvaryhmän tulee tehdä lopullinen päätös tutkintajärjestyksestä

- Analysoi vaikuttavuus eri järjestelmiin ja kokoa kokonaiskuva
  - → Dokumentoi missä kaikkialla on häiriöitä
  - → Dokumentoi mihin järjestelmiin ei ole hallintayhteyksiä enää
  - → Dokumentoi minkä järjestelmien luotettavuus on menetetty

- Tutki hyökkäyksen alkuperä eri järjestelmien löydöksien perusteella

- Kokoa aikajana hyökkäyksestä
  - → Mistä järjestelmistä löytyy IoC-tietoja (aikaleimat milloin ne ovat järjestelmiin päätyneet ensimmäisen kerran)

- Tietoturvaryhmän ja kriisiryhmän tulee tehdä päätös vastatoimista ja toipumisesta

Kyberhäiriöistä palautuminen ja oppiminen

Alustava toipuminen on aloitettava jo silloin, kun havaittua häiriötä epäillään kyberhäiriöksi. Tämä saattaa tarkoittaa esimerkiksi varajärjestelmän ottamista käyttöön. [3] Lähtökohtana on turvata toiminnan jatkuvuus, sekä tietojen luottamuksellisuus ja eheys.

Toipumisvaiheeseen voidaan siirtyä, kun havaitaan, että korjaustoimenpiteet ovat tehonneet. VAHTI-ohjeen, Tietoturvapoikkeamatilanteiden hallinta, mukaan toipumisvaiheen toimenpiteitä voivat olla mm. tietojen palauttaminen varmuuskopioista, haavoittuvuuksien korjaaminen, päivittäminen ja uudelleen asentaminen sekä laitteiden uusiminen. Toipumisvaiheessa toiminnot palautetaan normaalitilaan.

Häiriön päättymisestä on hyvä tiedottaa kohderyhmille, kullekin ryhmälle sopivaksi räätälöidyllä viestinnällä. Tiedote voi sisältää esimerkiksi kuvauksen tapahtuneesta, häiriön syyn yleisesti ja mihin tulokseen häiriön käsittelyssä päädyttiin. Tässä vaiheessa tiedotetaan myös mahdollisista toimenpidesuosituksista ja annetaan ohjeet normaaliin toimintaan palaamiseksi. [44] Häiriöstä ja sen vaikutuksista on hyvä järjestää jälkikäteen myös yhteinen tilaisuus, jossa havaitut puutteet ja onnistumiset käsitellään [3].

Dokumentointi

On tärkeää dokumentoida tarkasti häiriön rajaamisen ja palautumisen vaiheet, kuten myös kaikki siihen liittyvä todistusaineisto ja vaarantumisindikaattorit. Tämä auttaa ymmärtämään tapahtunutta, ja estämään vastaavanlaisten tilanteiden syntyminen tulevaisuudessa. [107] Usein voi olla haastavaa tosiaikaisesti tehdä dokumentointia muiden toipumistoimenpiteiden ohella, mutta tuleviin häiriöihin varautumisen ja mahdollisten uhkien toteutumisen estämisen kannalta on tärkeää tehdä riittävästi muistiinpanoja. Mitä lyhyemmän ajan kuluttua toipumisesta dokumentaatiota tehdään, sitä varmemmin saadaan tallennettua tarkka kuva tapahtumista. [113]

Myös toipumiskykyyn tehdyt parannukset pitäisi dokumentoida analysoimalla nykyistä tilannetta sekä aiempien häiriöiden toipumisvaiheita ja tunnistaa tärkeimmät tekijät, kuten merkittäviä viivästyksiä aiheuttaneet ongelmat tai pienet, mutta usein toistuvat ongelmat. [113]

[113] Guide for Cybersecurity Event Recovery, NIST 2016

Toipumissuunnitelma

Järjestelmillä ja prosesseilla tulisi olla omat toipumissuunnitelmansa, joita päivitetään säännöllisesti ja pidetään helposti saatavilla. Toipumissuunnitelmissa kuvataan mm. toimenpiteet, roolit ja vastuut normaalitilaan palaamiseksi sekä häiriötilanteessa viestiminen. Jatkuvuussuunnittelussa on otettava huomioon yksittäisten järjestelmien ja prosessien toipuminen sekä toipuminen organisaatiotasolla. Laajamittaisen häiriön varalta on järjestelmien kriittisyys ja niiden toipumisen tärkeysjärjestys oltava määriteltynä. [40] Tärkeää on huomioida järjestelmien ja mahdollisten alijärjestelmien keskinäiset vaikutukset.

Myös palveluntuottajilta ja alihankkijoilta on vaadittava palveluita koskevat toipumissuunnitelmat. [40] Toipumissuunnitelmia on jatkuvasti kehitettävä havaittujen puutteiden mukaan ja määriteltävä myös aikataulut ja vastuuhenkilöt korjausten toteuttamiseen. Ulkoistettujen palvelujen puutteet on syytä käsitellä ja korjata palveluntuottajien kanssa. Myös reklamointi voi tulla kyseeseen, jos selvästi nähdään, että palveluntuottaja on toiminut sopimusten tai käytäntöjen vastaisesti. [44]

VAHTI-ohjeesta, Toiminnan jatkuvuuden hallinta, löytyy vinkkejä toipumissuunnitelman laatimiseen ja esimerkki sisällysluettelosta.

Jälkianalyysi

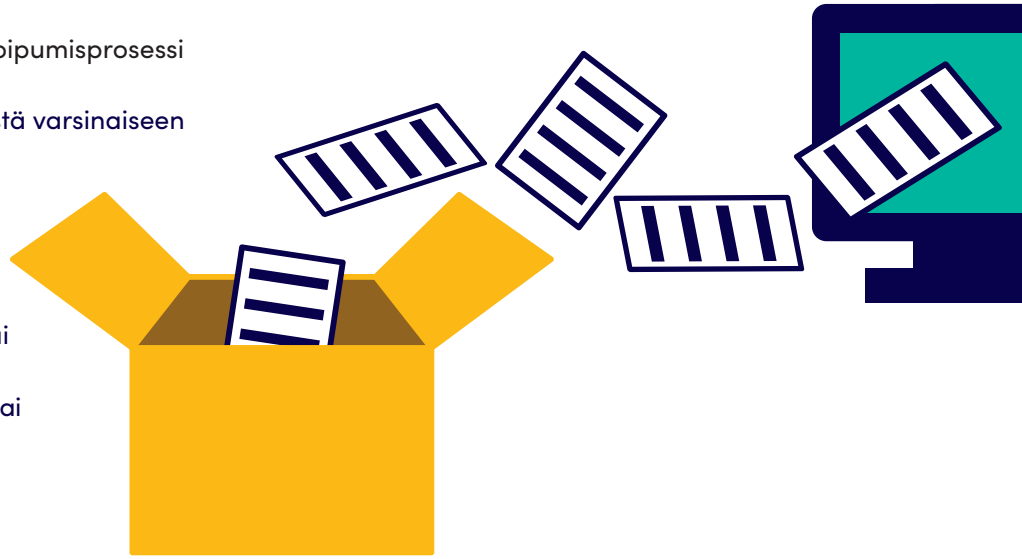
Kyberhäiriö/-poikkeamatilanteesta on tärkeää käydä läpi jälkianalyysi ja siihen liittyvä raportointi. Jälkianalyysissa käydään häiriön vaiheet läpi seikkaperäisesti ja pyritään tunnistamaan, miten poikkeamankäsittelyssä onnistuttiin, mitä asioita voitaisiin parantaa tulevaisuudessa ja mitä ympäristön kehittämiseksi pitää tehdä, että vastaavaa ei tapahdu uudestaan tai miten sen havaitseminen ja käsittely on tehokkaampaa.

Jälkianalyysiä käytetään organisaation kyvykkyyden kehittämiseen ja mahdollisten aukkojen ja haavoittuvuuksien korjaamiseen. Myös henkilöstön lisäkouluttaminen voidaan siinä nähdä tarpeellisena. [107] Ohjeisiin ja suunnitelmiin tehdään korjauksia analyysissä havaittujen puutteiden mukaisesti. Tämä on tärkeä osa organisaation toipumis-, oppimis- ja kehittymisprosessia. Opitut asiat kannattaa jakaa myös Kyberturvallisuuskeskukselle tiedon eteenpäin levittämistä ja palautteen saamista varten. [3] Jälkianalyysissa on tärkeää tunnistaa, mitä osa-alueita tulisi kehittää tai muuttaa häiriön perusteella esimerkiksi tietoturvakontrolleissa, käytänteissä, ohjeistuksissa tai politiikoissa.

Tarkistuslista häiriöstä palautumiseen

✓ Toipuminen

- Suunnitelman mukainen toipumisprosessi käynnistetty, tarvittaessa:
  - → Tiedot varajärjestelmästä varsinaiseen järjestelmään [3]
  - → Tietojen palautus varmuuskopioista [44]
  - → Haavoittuvuuksien korjaus [44]
  - → Järjestelmien päivitys tai uudelleen asennus [44]
  - → Laitteiden hankkiminen tai korvaaminen [44]



- Toipumistoimenpiteiden etenemisen valvonta [40]
- Normaali toiminta palautettu mahdollisimman nopeasti ja kustannustehokkaasti [40]
  - → Päätös normaaliin toimintaan siirtymisestä tehty toipumissuunnitelmien mukaisten toimenpiteiden jälkeen [44]
  - → Tehostettu ympäristön seuranta, kunnes varmistettu ettei poikkeaman uusiutuminen ole todennäköistä [44]
- Keskeytyksen vaikutukset organisaation toimintaan, talouteen ja maineeseen minimoitu [40].

Viestintä

- Tiedotettu sidosryhmiä poikkeamatilanteen päättymisestä [3]
- Järjestetty yhteinen tilaisuus, jossa käyty läpi tilanne, sen vaikutukset, ja havaitut puutteet [3]
- Lehdistötiedote tarvittaessa [44]
- Tilanteesta opitut asiat jaettu Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle [3].

Raportointi ja jälkianalyysi

- Todistusaineisto ja vaarantumisindikaattorit dokumentoitu [107]
- Häiriötilanteen toimenpiteiden ja päätösten raportointi ja jälkianalysointi
  - → Kuvaus, kuinka häiriö havaittiin
  - → Kuvaus tietojärjestelmistä ja datasta, johon häiriö vaikutti
  - → Tieto, kuka on vastuullinen järjestelmästä ja datasta
  - → Mikä aiheutti häiriön
  - → Oliko havaittu häiriö riskienhallinnassa tunnistettu riski
  - → Kuvaus, miten häiriö käsiteltiin ja miten siinä onnistuttiin
  - → Toimittiinko tilanteessa ohjeiden ja harjoiteltujen tapojen mukaisesti [114]
  - → Reagoitiinko häiriöilmoitukseen riittävän nopeasti [114]
  - → Oliko häiriön kartoituksen nopeus ja tehokkuus riittävää [114]
  - → Suositukset ja toimenpiteet, miten estää vastaavat häiriöt tulevaisuudessa
  - → Mitä seuraavalla kerralla voidaan tehdä paremmin
  - → Mitä kannattaa harjoitella
  - → Mihin tarvitaan lisäkoulutusta tai ulkopuolista apua
  - → Tietoturvaparannustarpeiden tunnistaminen
  - → Läpikäynnin pohjalta nousseet opit; miten häiriönkäsittelyä voidaan parantaa tulevia tilanteita varten
  - → Aikajana tapahtumista ja toimenpiteistä havainnosta häiriön sulkemiseen
  - → Viestinnän tehokkuuden arviointi (sisäinen ja ulkoinen) [114]
- Mukana jälkianalysoinnissa poikkeaman hallintaan osallistuneet, järjestelmien ja tiedon omistajat, johdon edustajat sekä tahot, joista häiriötilanteessa olisi ollut apua [44]
- Olemassa olevat jatkuvuus- ja toipumissuunnitelmat ym. ohjeet tarkastettu, ja korjattu havaittujen puutteiden osalta [44]
- Tarvittaessa toimintatapojen päivitys ja henkilöstön kouluttaminen [44]
- Reklamointi, jos selvää, että palveluntarjoaja on toiminut sopimuksen tai käytäntöjen vastaisesti [44].

[114] Effective Practices for Cyber Incident Response and Recovery, FSB 2020

Lähteet

[1] Varoitus: kyberhyökkäyksistä sairaaloihin tulossa globaali trendi, kasvu Euroopassa ”hälyttävää”, Tekniikka & Talous 2020 https://www.tekniikkatalous.fi/uutiset/tt/f3d302d3-8fff-43ee-80f8-cda61a1eaf34

[2] Suomen kyberturvallisuusstrategia 2019 https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

[3] Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille, STM 2019 http://urn.fi/URN:ISBN:978-952-00-4085-7

[4] Kyberturvallisuus sosiaali- ja terveydenhuollossa, JYU 2019 https://jyx.jyu.fi/bitstream/handle/123456789/63325/Kyberturvallisuus_Vol2FINAL.pdf

[5] The state of research on cyberattacks against hospitals and available best prac-tice recommendations: A scoping review, BMC Medical Informatics and Decision Makin 2019 https://doi.org/10.1186/s12911-018-0724-5

[6] A Lifeline: Patient Safety & Cybersecurity, Public-Private Analytic Exchange Pro-gram 2019 https://www.himss.org/sites/hde/files/media/file/2019/12/09/a-life-line-patient-safety-cybersecurity.pdf

[7] Data Breaches: In the Healthcare Sector, CIS Center for Internet Security 2020 https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/

[8] 667% spike in email phishing attacks due to coronavirus fears, TechRepublic 2020 https://www.techrepublic.com/article/667-spike-in-email-phishing-attacks-due-to-coronavirus-fears/

[9] A View of COVID-19’s First Wave of Cybersecurity, info security GROUP, 2020 https://www.infosecurity-magazine.com/blogs/view-covid19-first-wave/

[10] Kybersää Lokakuu 2020, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4_lokakuu_2020_TLP__WHITE_0.pdf

[11] Kybersää Maaliskuu 2020, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kybers%C3%A4%C3%A4_maaliskuu_2020.pdf

[12] Cyberattacks targeting health care must stop, Microsoft 2020 https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

[13] INTERPOL report shows alarming rate of cyberattacks during COVID-19, INTERPOL 2020 https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[14] Cyberattack On A Hospital Leads To The First Ransomware-Linked Death, Forbes 2020 https://www.forbes.com/sites/leemathews/2020/09/17/ransomware-attack-hospital-leads-to-death/?sh=55222ab33f05

[15] Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector, CISA 2020 https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[16] Yksi heistä on kiristäjä, YLE 2020 https://yle.fi/uutiset/3-11616210

[17] Cybersecurity and Covid-19: Experiences from the frontline, PANACEA Research 2020 https://www.panacearesearch.eu/webinars/panacea-webinar-cybersecurity-and-covid-19-experiences-frontline-23rd-june-2020-1100-cest

[18] Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, ZDNet 2020, https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

[19] Helsingin ja Uudenmaan sairaanhoitopiirin tietojärjestelmähäiriöt 7.–8.11.2017, Onnettomuustutkintakeskus 2017 https://www.turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/OZnac1oRj/Y2018-02_HUS.pdf

[20] Kyberturvallisuus sairaalajärjestelmissä: Osa 1, JYU 2017 https://www.jyu.fi/it/fi/tutkimus/julkaisut/tekes-raportteja/kyberturvallisuus-sairaalassa_-14-8-17.pdf

[21] E-health systems in digital environments, JYU 2019 https://jyx.jyu.fi/handle/123456789/67096

[22] Securing Wireless Infusion Pumps in Healthcare Delivery Organizations, NIST 2018 https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf

[23] Baxter, B.Braun infusion pumps among millions of devices implivated in Ripple20 cyber alert, Medtechdrive 2020 https://www.medtechdive.com/news/baxter-b-braun-infusion-pumps-among-millions-of-devices-implicated-in-rip/580429/

[24] Cyber security and resilience for Smart Hospitals, ENISA 2016 https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

[25] Cybersecurity in the healthcare sector during COVID-19 pandemic, Enisa 2020 https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

[26] Phishing in Healthcare: How Not to Be a Victim Checklist, HIMSS 2020 https://www.himss.org/resources/phishing-healthcare-how-not-be-victim-checklist

[27] Healthcare Cybersecurity During COVID-19 and How to Pivot, HIMSS 2020 https://www.himss.org/resources/healthcare-cybersecurity-during-covid-19-and-how-pivot

[28] Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu, JYU 2020 https://jyx.jyu.fi/handle/123456789/71395

[29] Valtion kyberturvallisuusjohtaja on nimitetty, valtioneuvosto 2020 https://valtioneuvosto.fi/-/valtion-kyberturvallisuusjohtaja-on-nimitetty

[30] SFS-ISO 31000:2018 Riskienhallinta. Ohjeet, Suomen standardisoimisliitto SFS 2018 (2.painos)

[31] SFS-ISO/IEC 27005:2018 Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta, Suomen standardisoimisliitto SFS 2018 (3.painos)

[32] Tilannetorjunta ja rationaalisen valinnan teorian järki, Jukka-Pekka Takala, Haaste 4/2011 https://www.haaste.om.fi/fi/index/lehtiarkisto/haaste42011/tilannetorjuntajarationaalisenvalinnanteorianjarki.html

[33] VAHTI 22/2017 Ohje riskienhallintaan, Valtiovarainministeriö 2017 https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-222017-ohje-riskienhallintaan

[34] SFS-EN IEC 31010:2019 Riskienhallinta. Riskien arviointimenetelmät, Suomen standardisoimisliitto SFS 2019 (2.painos)

[35] Laki julkisen hallinnon tiedonhallinnasta, Finlex 2019 https://www.finlex.fi/fi/laki/ajantasa/2019/20190906

[36] Kybermittari, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_esittely_20200407.pdf

[37] Kybermittari. Kansallinen kyberturvallisuuden arviointimalli. Käyttöohje, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_K%C3%A4ytt%C3%B6ohje_V1.pdf

[38] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, valtioneuvosto 2020 http://urn.fi/URN:ISBN:978-952-367-295-6

[39] Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille, puolustusministeriö https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

[40] Toiminnan jatkuvuuden hallinta, valtioneuvosto 2016 http://urn.fi/URN:ISBN:978-952-251-779-1

[41] Sopimusperusteinen varautuminen : Ohje sosiaali- ja terveydenhuollon toimijoille, STM 2019 http://urn.fi/URN:ISBN:978-952-00-4068-0

[42] Kuntien jatkuvuudenhallintaprojektit KUJA 1 ja 2, Kuntaliitto 2018 https://www.kuntaliitto.fi/yhdyskunnat-ja-ymparisto/turvallisuus-ja-varautuminen/varautuminen-ja-jatkuvuudenhallinta/kuja-jatkuvuudenhallintaprojektit

[43] Toiminnan on aina jatkuttava, SOPIVA-hanke Huoltovarmuuskeskus https://cdn.huoltovarmuuskeskus.fi/app/uploads/2016/08/31144121/SOPIVA_esite.pdf

[44] Tietoturvapoikkeamatilanteiden hallinta, valtioneuvosto 2017 http://urn.fi/URN:ISBN:%20978-952-251-930-6

[45] Sote-ICT-skenaarioiden RACI-matriisi vastuualueiden määrittelyyn, Liite 2, Excel, Kuntaliitto 2019 https://www.kuntaliitto.fi/sosiaali-ja-terveysasiat/tiedonhallinta/alueiden-ja-kuntien-sosiaali-ja-terveydenhuollon/akusti-foorumin-projektien-tuotoksia

[46] Responsibility assignment matrix, Wikipedia https://en.wikipedia.org/wiki/Responsibility_assignment_matrix

[47] Ohje tietoturvavastuudokumentin laatimiseen, FUSEC 2012 https://tt.eduuni.fi/sites/kity/Julkaistut%20dokumentit/FUSEC_FI/_FUSEC_Ohje_tietoturvavastuudokumentin_laatimiseen.docx

[48] Valmius- ja jatkuvuudenhallintasuunnitelma: Ohje sosiaali- ja terveydenhuollon toimijoille, STM 2019 http://urn.fi/URN:ISBN:978-952-00-4046-8

[49] Vesihuoltolaitoksen häiriötilanne- ja kriisiviestintäohje, huoltovarmuusorganisaatio vesihuoltopooli 2019 https://cdn.huoltovarmuuskeskus.fi/app/uploads/2019/05/23133452/Vesilaitosyhdistys-kriisiviestinta%CC%88ohje-sa%CC%88hko%CC%88inen.pdf

[50] How to secure your medical devices, SecurityMetrics https://www.securitymetrics.com/learn/how-to-secure-your-medical-devices

[51] VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohjeen uusi tukimateriaali - 12 liite 5. Tietoturvallisuuden ja jatkuvuudenhallinnan huomioiminen hankittaessa ulkoistettuja ICT-palveluita, Valtiovarainministeriö 2011 https://www.suomidigi.fi/vahti-32011-valtion-ict-hankintojen-tietoturvaohjeen-uusi-tukimateriaali-12-liite-5-tietoturvallisuuden-ja-jatkuvuudenhallinnan-huomioiminen-hankittaessa

[52] Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja

[53] Terveydenhuollon laadunhallinta - Lääkintälaitejärjestelmien turvallisuus, Lääkelaitos 2004 https://www.valvira.fi/documents/14444/50159/LH-2004-1_laakintalaitejarjestelmat.pdf

[54] Information Security Requirements in Public IT Procurements: Effect of Act on Information Management in Public Administration on Requirements, Aaltonen R. 2020 http://urn.fi/URN:NBN:fi:amk-2020060517391

[55] Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt, STAKES 2005 http://urn.fi/URN:NBN:fi-fe201204194082

[56] Tietosuoja sosiaali- ja terveydenhuollossa, Hyvinvointiala HALI ry https://www.hyvinvointiala.fi/tietoa-meista/toimintaymparisto/tietosuoja/

[57] Tietosuojaperiaatteet, tietosuojavaltuutetun toimisto https://tietosuoja.fi/tietosuojaperiaatteet

[58] Terveydenhuoltoalan kyberuhkia, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf

[59] EU:n tietosuoja-asetus, tietosuojavaltuutetun toimisto https://tietosuoja.fi/GDPR

[60] Tietoturvan ja tietosuojan omavalvontasuunnitelman malli tukee pieniä sosiaali- ja terveydenhuollon palveluntuottajia, THL 2020 https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/-/tietoturvan-ja-tietosuojan-omavalvontasuunnitelman-malli-tukee-pienia-sosiaali-ja-terveydenhuollon-palveluntuottajia-1

[61] Tietosuojan ja tietoturvallisuuden omavalvonta: Suunnitelma ja toteuttaminen, THL 2020 https://thl.fi/documents/920442/3022844/20201203_Tietosuojan_ja_tietoturvallisuuden_omavalvonta__suunnitelma_ja_toteuttaminen_mykkanen.pdf

[62] KYBERTURVALLISUUDEN NYKYTILA ERI TOIMIALOILLA – KARTOITUKSEN KESKEISET HAVAINNOT, Huoltovarmuuskeskus 2020 https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/05091400/Kyberturvallisuuden-nykytila-eri-toimialoilla.pdf

[63] Duodecim Oppiportti, 2020 https://www.oppiportti.fi/

[64] Digiturvallinen elämä, Digi- ja väestötietovirasto https://dvv.fi/digiturvallinen-elama

[65] Opas digitaalisen turvallisuuden harjoitusohjelman ja -toiminnan suunnitteluun, Digi- ja väestötietovirasto https://dvv.fi/documents/16079645/17634906/Opas+digitaalisen+turvallisuuden+harjoitusohjelman+ja+-toiminnan+suunnitteluun.pdf

[66] Kyberharjoitusohje. Käsikirja harjoituksen järjestäjälle, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2019 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

[67] TIETO20-harjoitus testaa yhteistoimintaa laajassa kyberhäiriötilanteessa, Huoltovarmuuskeskus 2020 https://www.huoltovarmuuskeskus.fi/tieto20-harjoitus/

[68] Tieto 2018 -kyberturvallisuusharjoitus käynnissä – Verkostona kyberuhkia vastaan, Huoltovarmuuskeskus 2018 https://www.huoltovarmuuskeskus.fi/tieto-2018-kyberturvallisuusharjoitus-kaynnissa-verkostona-kyberuhkia-vastaan/

[69] TAISTO-harjoitus, Digi- ja väestötietovirasto 2020 https://dvv.fi/taisto

[70] TAISTO19-harjoitusraportti ja yhteenveto, Digi- ja väestötietovirasto 2019 https://dvv.fi/documents/16079645/17634906/6-2020+TAISTO19+raportti.pdf/

[71] Sertifiointiorganisaatiot, Finas 2020 https://www.finas.fi/akkreditointi/Akkreditointialueet/Sivut/Sertifiointiorganisaatiot.aspx

[72] Luottamuksen lähteillä: Näkökulmia tietoturvan standardointiin ja sertifiointiin, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2019 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

[73] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, Finlex 2007 https://www.finlex.fi/fi/laki/ajantasa/2007/20070159

[74] Laki Turvallisuus- ja kemikaalivirastosta, Finlex 2010 https://www.finlex.fi/fi/laki/ajantasa/2010/20101261

[75] Laki tietoturvallisuuden arviointilaitoksista, Finlex 2011 https://www.finlex.fi/fi/laki/ajantasa/2011/20111405

[76] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020, Turvallisuuskomitea 2017 https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

[77] Cyber Threat Information Sharing: Perceived Benefits and Barriers, Zibak A.; Simpson A. 2019 doi: 10.1145/3339252.3340528, 2019

[78] A framework for cybersecurity information sharing and risk reduction, Microsoft, 2015, https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf

[79] Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (slna), Colicchia C., Creazza A., Noè C., Strozzi F. Supply Chain Management: An International Journal, Volume 24, Number 1, 2019

[80] Strategic Aspects of Cyber Risk Information Sharing, Laube S.; Böhme R. ACM Computing Surveys (CSUR), Volume 50(5), doi:10.1145/3124398, 2017

[81] The impact of information sharing on cybersecurity underinvestment: A real options perspective. Gordon L. A., Loeb M. P., Lucyshyn W., Zhou L. Journal of Accounting and Public Policy, Volume 34, Number 5, 2015

[82] Perspectives on cybersecurity information sharing among multiple stakeholders using a decisiontheoretic approach, He M.; Devine L.; Zhuang J. Risk Analysis, Volume 38, number 2, 2018

[83] Information Sharing and Analysis Centers (ISACs), Enisa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[84 ISAC in a box, Enisa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit

[85] Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™), White paper: STIX project Github 2014 http://stixproject.github.io/getting-started/whitepaper/

[86] The Trusted Automated eXchange of Indicator Information (TAXII™), White paper: TAXII project Github 2014 http://taxiiproject.github.io/getting-started/whitepaper/

[87]Cyber Observable eXpression (CybOX™) Archive Website, CybOX project Github https://cyboxproject.github.io/

[88] Sharing threat intelligence just got a lot easier!, OASIS Open Github https://oasis-open.github.io/cti-documentation/

[89] MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing, MISP-project https://www.misp-project.org/index.html

[90] Incidents Information Sharing Platform for Distributed Attack Detection, Fotiadou K., Velivassaki T., Voulkidis A., Railis K., Trakadas P., Zahariadis T. IEEE Open Journal of the Communications Society, Volume 1, 2020, doi: 10.1109/OJCOMS.2020.2989925

[91] Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen kansallinen kokonaisarkkitehtuuri v 2.1, Kanta 2019 https://yhteistyotilat.fi/wiki08/pages/viewpage.action?pageId=55770028#

[92] Kyberturvallisuus sairaaloiden eri toimialoilla, KYS 2016 https://ssty.fi/download/valmiusseminaari19102016/Pekkarinen_kybertuvallisuus_sairaalan_eri_toimialoilla.pdf

[93] Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2019 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa

[94] Procurement Guidelines for Cybersecurity in Hospitals, ENISA 2020 https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[95] Miten lääkinnällisistä laitteista tehdään digiturvallisia?, Huld 2020 https://huld.io/fi/nakemyksia/miten-laakinnallisista-laitteista-tehdaan-digiturvallisia/

[96] Tiedotustilaisuus Vastaamo-tietomurron jatkotoimenpiteistä. 12.11.2020 klo 13.30, valtioneuvosto https://valtioneuvosto.fi/documents/10616/20764066/Tiedotustilaisuus+Vastaamo-tietomurron+jatkotoimenpiteist%C3%A4+12.11.2020.pdf

[97] Ohje salauskäytännöistä. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 2/2015, valtiovarainministeriö https://www.suomidigi.fi/sites/default/files/2020-06/Vahti_2_2015_pdf.pdf

[98] BIA-vaikutusarviotyökalu, Valtiovarainministeriö 2016 https://www.suomidigi.fi/bia-vaikutusarviotyokalu

[99] Miten varmennan ICT:n kriittisessä toimintaympäristössä?, Tommi Tervo, Istekki Oy 2018 https://ssty.fi/wp-content/uploads/2018/02/MitenVarmennanICTVerkon_Tommi_Tervo.pdf

[100] Kybersää Syyskuu 2020, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4-syyskuu2020.pdf

[101] Tietoturvapoikkeaman havaitseminen suuressa organisaatiossa, Ollikainen T. 2018 http://urn.fi/URN:NBN:fi:amk-2018121020669

[102] Kyberhäiriötilanteet – Varautuminen ja toiminta, Huoltovarmuusorganisaatio 2019 https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/01/24095937/HVK-suosituksia-kyberh%C3%A4iri%C3%B6tilanteessa.pdf

[103] Tilannetietoisuuden kasvattaminen organisaation kybertoiminta-ympäristössä, Sara Sallinen Opinnäytetyö JAMK 2019 https://www.theseus.fi/bitstream/handle/10024/333061/Opinnaytetyo_SaraSallinen.pdf

[104] Lokien keräys ja käyttö – Ohje lokitietojen tallentamiseen ja hyödyntämiseen, Viestintävirasto 2016 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

[105] Näin keräät ja käytät lokitietoja, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

[106] Lokiohje, Valtionvarainministeriö 2009 https://www.suomidigi.fi/sites/default/files/2020-06/pdf_3_2009.pdf

[107] Prepare, hunt and respond, JYVSECTEC https://phr.jyvsectec.fi/

[108] Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020 https://www.kyberturvallisuuskeskus.fi/fi/emotet-haittaohjelmaa-levitetaan-aktiivisesti-suomessa

[109] SPF, DKIM and DMARC brief explanation and best practices, End Point 2014 https://www.endpoint.com/blog/2014/04/15/spf-dkim-and-dmarc-brief-explanation

[110] Vältä kyberkömmähdyksiä, Tehy-lehti 9/2020 https://www.tehylehtiarkisto.fi/lehti/20200902/#browse/32

[111] VPN-yhteyksien kapasiteetin varmistaminen, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vpn-yhteyksien-kapasiteetin-varmistaminen

[112] Ohjeita turvallisten etätyövälineiden valintaan, Huoltovarmuusorganisaatio 2020 https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/07/03140734/Ohjeita-turvallisten-et%C3%A4ty%C3%B6v%C3%A4lineiden-valintaan.pdfz

[113] Guide for Cybersecurity Event Recovery, NIST 2016 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

[114] Effective Practices for Cyber Incident Response and Recovery, FSB 2020 https://www.fsb.org/wp-content/uploads/P191020-1.pdf

Kyberhäiriöiden hallinta

KÄSIKIRJA TERVEYDENHUOLLON TOIMIJOILLE

BUSINESS FINLAND

HUOLTOVARMUUSKESKUS

thl

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

JYVSECTEC by jamk