

Käytännön oppeja - kuinka toimia oikein tietomurto-tilanteessa?

Mikael Hitruhin

Kolme pääpointtia

1. Tietomurtoon tulee reagoida nopeasti, ei hätäisesti
2. Tietomurto koskettaa kaikkia organisaation työntekijöitä, ei ainoastaan ”tietoturvaehdettä”
3. Tietomurtoihin tulee varautua

Mitä tehdä kun tietomurto
tapahtuu?

Mitä kokonaisuuksia tietomurron hallinnassa tulee tunnistaa?

Tietoturva –
sähköinen infra

Tietosuoja

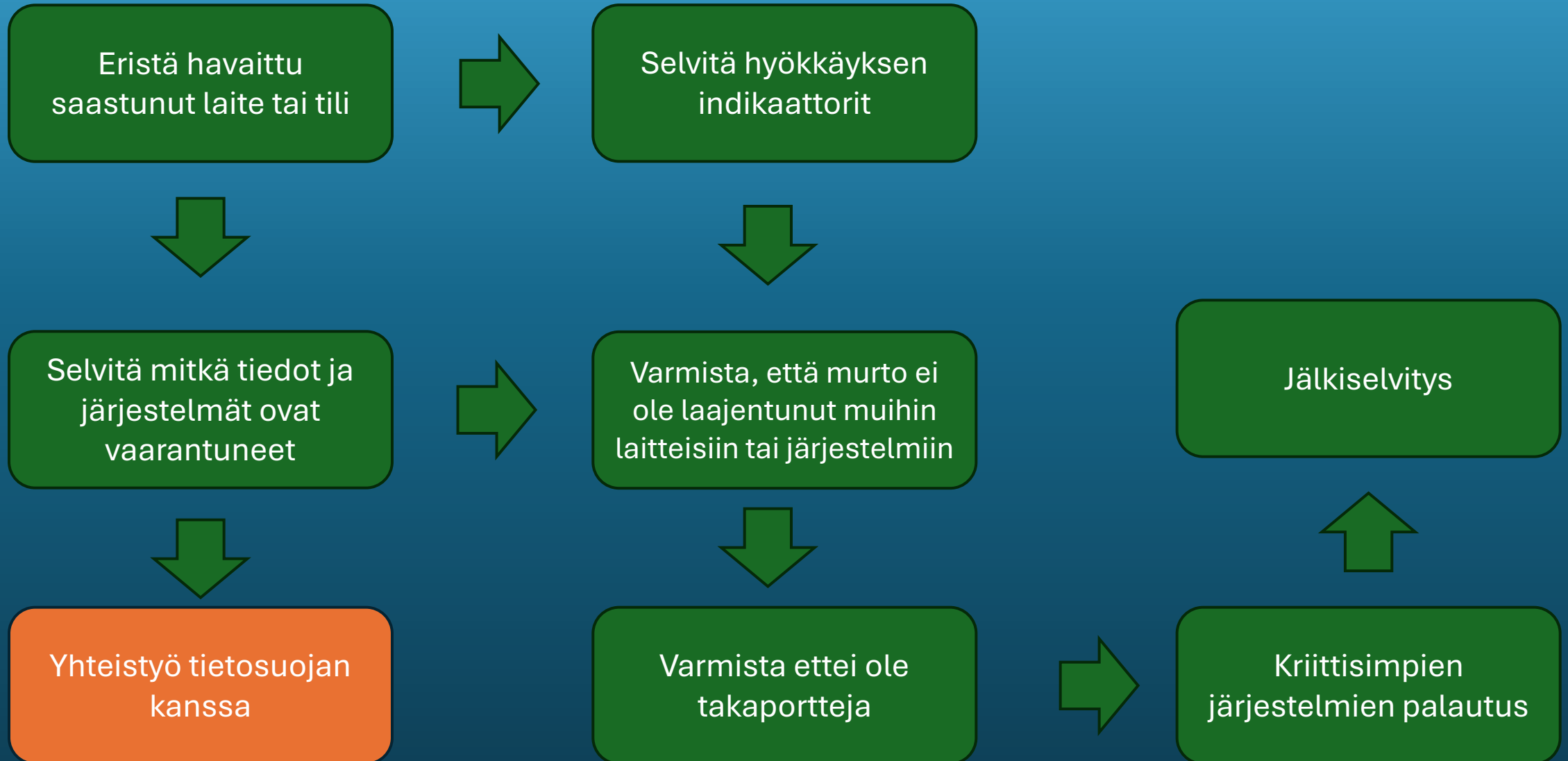
Henkilöstö

Viestintä

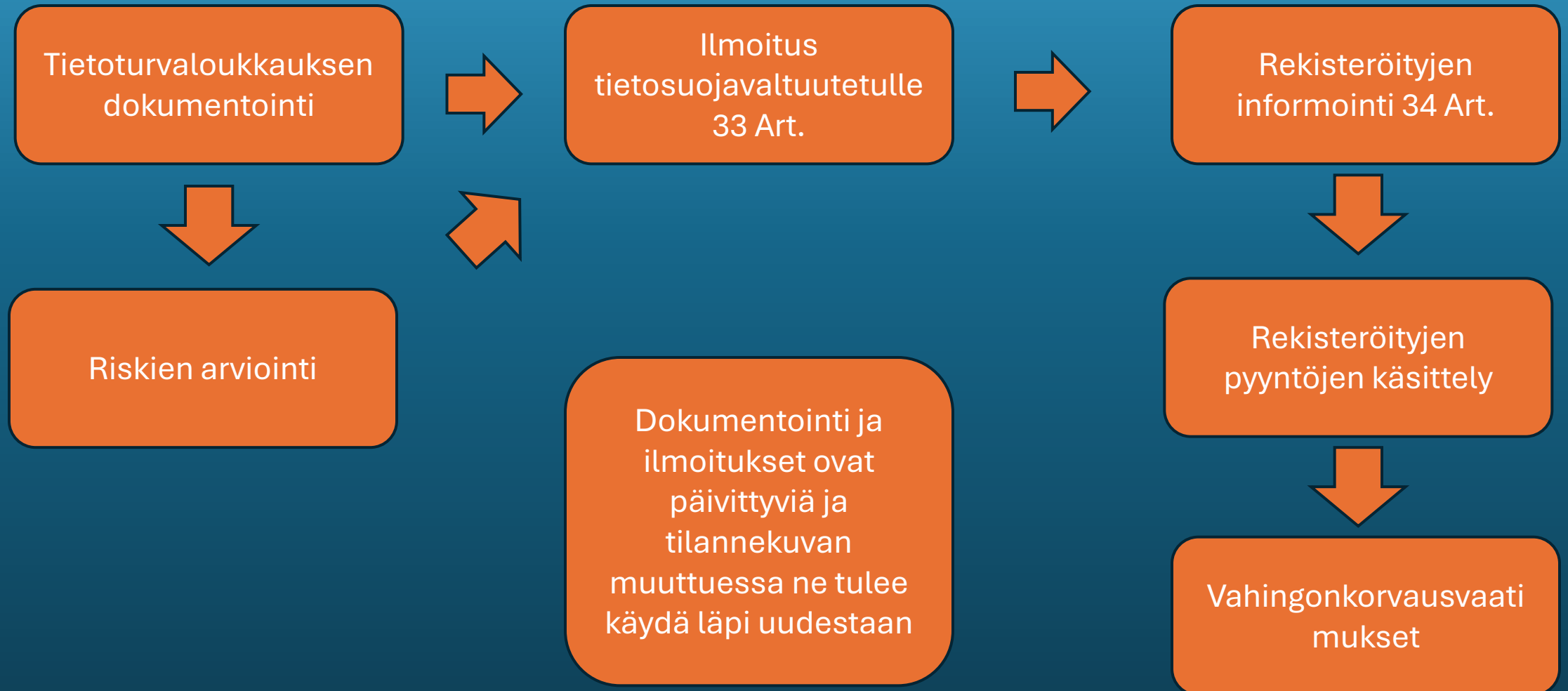
Koordinointi ja
tiedonkulku

Viranomaisyhteistyö

Tietoturva ja sähköinen infra



Tietosuoja



Viestintä

Sisäinen viestintä

- Tarkoitus informoida henkilökuntaa tietomurron vaikutuksista heidän työhön
- Jos henkilökunnan tietoja on murron kohteena, myös heitä on informoitava rekisteröityinä

Ulkoinen viestintä

- Tietomurron kohteita tulee informoida tietomurrosta
- Ulkoiseen viestintään kuuluu myös organisaation esim. verkkosivujen tiedotteet
 - Viestinnällisillä toimenpiteillä voi helpottaa esim. rekisteröityjen tietopyyntöjen tekemistä



Mediaviestintä

- Mediaan on hyvä tehdä itsenäisesti tiedotteet, jotta viesti mediassa on selkeä
- Uutisseurantaa kannattaa tehdä ja pyytää virheellisten uutisten oikaisua

Yhteistyö tietosuojan kanssa

Viranomaisyhteistyö

**Tutkivat viranomaiset ja
valvontaviranomaiset**

Tietosuoja-valtuutettu

Kyberturvallisuuskeskus

Poliisi

**Yhteistyökumppanit ja muut
tahot, joihin tietomurto vaikuttaa**

Muut tahot, jotka
käyttävät murron
kohteena olevia tietoja

Muut tunnistetut
kriittiset viranomaiset

Henkilöstö



Koordinointi ja tiedonkulku



Miten varautua ennalta?

Varautumisen toimenpiteet

- Varautumiskeinot voidaan karkeasti jakaa kahteen eri kategoriaan:
 - Ennaltaehkäisevät toimet, joilla vähennetään tietomurron toteutumisen riskiä
 - Vahinkoa rajaavat toimet, joilla vähennetään tietomurron vaikutusta rekisteröityihin ja organisaatioon

Ennaltaehkäisevät toimet

- Ylläpidetään työntekijöiden tietoturvaosaamista
- Suojataan eri järjestelmät säilytettävien tietojen arkaluonteisuuden tason mukaan
- Järjestelmien väliset integraatiot tunnetaan ja rajataan vain välttämättömiin
- Käyttäjillä on oikeat käyttöjätasot eri järjestelmissä

Vahinkoa rajaavat toimet

- Ylläpidetään työntekijöiden tietosuoja- ja tiedonhallintaosaamista
- Säilytetään tiedot oikeissa paikoissa säilytysaika huomioiden
- Tunnetaan talon sisäiset asiantuntijat sekä ulkopuoliset yhteistyökumppanit, joihin ollaan tietomurron tapahtuessa yhteydessä
- Laaditaan toimintamallit ja varautumissuunnitelmat

Tekniset-, organisatoriset- ja fyysiset tietoturvatimet

Tekniset toimet

- Palomuurit
- Salaustaso
- Varmuuskopiot
- Lokitus
- Verkkojen eriyttäminen
- Etäyhteyskäytännöt
- Järjestelmien väliset integraatiot

Organisatoriset toimet

- Tietoturvastrategia
- Henkilöstön kouluttaminen
- Tiedonhallinta
- Riskienhallinta
- Tietojen luokittelu
- Valvonta

Fyysiset toimet

- Työtilojen ja laitteiden suojaaminen

Tietoturvan ja tietosuojan kulttuuri

- Tärkein ennaltaehkäisyn keino on tietoturvan ja –suojan kulttuurin rakentaminen
- Ei riitä, että ymmärretään mitä ohjeistusta tulee noudattaa, vaan myös että miksi ohjeistusta tulee noudattaa – ja noudattamatta jättämisen mahdolliset seuraamukset
- Kulttuuri tulee rakentaa työyhteisön omalla kielellä ja toimintatapojen ympärille

Hyviä käytäntöjä
tietomurrosta selviämiseen

Kommunikointi ja viestintä

- Viestinnän tietomurrosta tulee olla avointa, jotta rekisteröidyt voivat reagoida ja varautua tietomurron vaikutuksiin.
- Luottamuksen voi menettää vain kerran – jos luottamus menetetään, ei tietomurrosta selviä ilman merkittävää mainehaittaa

Yhteydenpito viranomaisiin

- Informoi tarvittavia viranomaisia oma-aloitteisesti ja pidä heidät ajan tasalla. Noudata saamiasi viranomaisohjeistuksia, jos sellaista annetaan
 - Esim. Jos tietosuojavaltuutettu antaa ohjeistusta rekisteröityjen tiedottamisesta
- Dokumentoi tietomurron johdosta tehtävät toimenpiteet, jotta voit myöhemmin osoittaa toimineesi oikein. Huolellisella ja asianmukaisella suhtautumisella seuraamusmaksutkin vähenevät verrattuna välinpitämättömyyteen.

Yhteydenpito viranomaisiin

- Tietosuojavaltuutetulle lähetetyt tietoturvaloukkausilmoitukset ovat lähtökohtaisesti julkisia
 - Sisältö ei saa poiketa siitä, mitä sanotaan julkisesti
- Hyvä käytäntö on kirjoittaa tietoturvaloukkausilmoitus sekä vastaukset selvityspyyntöihin julkisiksi ja antaa kaikki salassapidettävä tieto erillisissä salassapidettävissä liitteissä.

Rekisteröidyn oikeudet

- Tietomurron seurauksena tulee varautua siihen, että rekisteröitydyt ovat aktiivisia omien oikeuksiensa toteuttamisen suhteen:
 - Tarkastuspyyntöjä tulee lisää
 - Poistopyyntöjä tulee lisää
- Rekisteröityjen pyyntöjä kannattaa keskittää tiettyihin kanaviin.
 - Tietosuoja-asetuksessa ei ole määrämuotoa rekisteröidyn oikeuksien käyttämiselle

Rekisteröidyn oikeudet ja vastausaika

- ”[..] jos rekisterinpitäjä saa tilapäisesti suuren määrän pyyntöjä esimerkiksi toimintaansa koskevan poikkeuksellisen julkisuuden vuoksi, tätä voidaan pitää perusteltuna syynä pidentää vastausaikaa.” (EDPB Ohjeet 1/2022 rekisteröityjen oikeuksista – oikeus tutustua tietoihin)

Asiakaspalvelu

- Asiakaspalvelussa tulee huomioida asiakkaiden tilanne. Ihmiset ovat tietomurron johdosta huolestuneita ja/tai ärtyneitä ja varmasti alttiimpia ilmoittaa väärinkäytöksistä ja virheistä tietosuojavaltuutetulle.
- Hyvä käytäntö on laatia selkeät verkkosivut tietomurrosta ja koota rekisteröidyille materiaali valmiiksi. Asiakaspalvelijoilla on oltava kyky opastaa tietomurron uhreja.
- Hyvä asiakaspalvelu ei eskaloi tilannetta.

Vahingonkorvausvaatimukset

- Tietomurto saattaa herättää rekisteröityjä tekemään myös vahingonkorvausvaatimuksia. Organisaatiossa on hyvä reagoida ennakoivasti tällaisten vaatimusten käsittelyyn.
- Joissakin tilanteissa myös pelko tietojen väärinkäytöstä voi olla peruste vahingonkorvauksella, jos siitä voidaan osoittaa syntyneen vahinkoa (Case C-340/21)

Mistä saan lisää tietoa?

- Traficomin Kyberturvallisuuskeskus
- DVV VAHTI-verkoston tapahtumat ja harjoitukset, Taisto
- Onnettomuustutkintakeskuksen tutkinnan tulokset (kesäkuussa 2025)

Kiitos

Mikael Hitruhin
Tietosuojaan vastuuhenkilö
Helsingin kaupunki
mikael.hitruhin@hel.fi