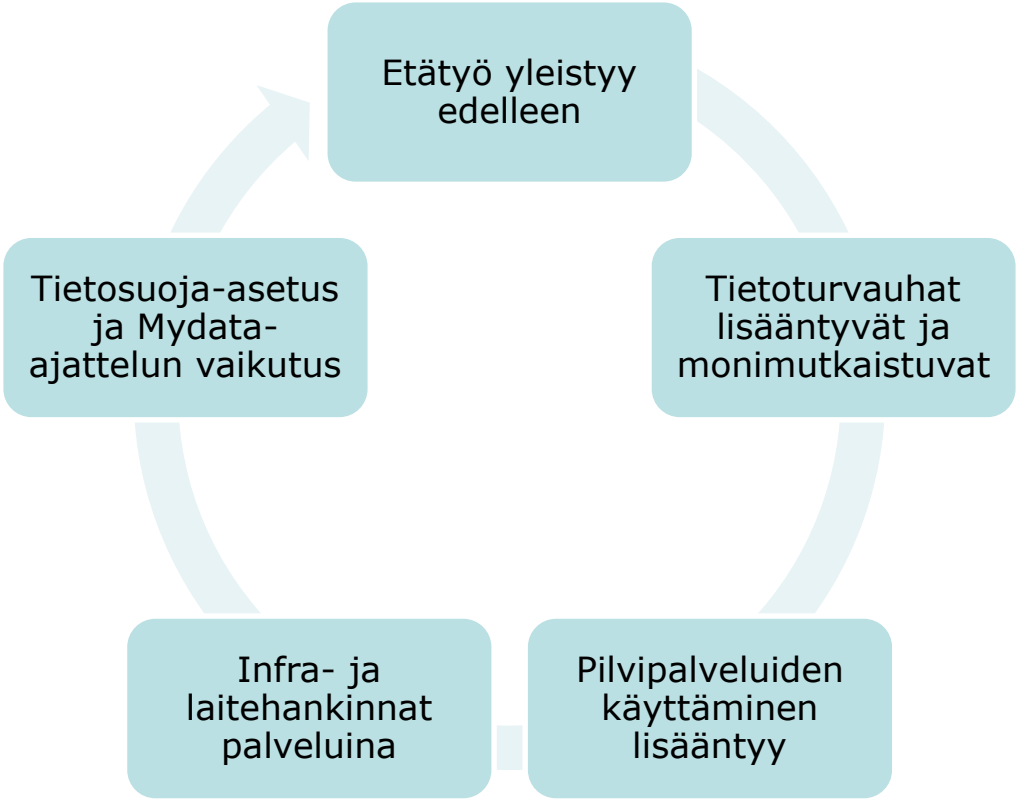
Tietohallinnon ja tietoturvan trendit sekä resurssit

12.11.2020

Tietohallintopäällikkö Ari Apilo

Toimintaympäristön muutostrendejä



Tietohallinnon suunnitellut menot 2021-2024

Toimintamenot

Henkilöstömenot ja –määrä ollut ennallaan (vajaat 2 Me/vuosi)

Ostopalvelujen määrän ennakoidaan kasvavan n. 7% eli n. 700.000 euroa (2021: 9,0 Me, 2024: 9,7 Me)

- Uusia palveluja mm. hallinnon asianhallinta
- Pilvipalvelusiirtymän vaikutus: investoinnit muuttuvat toimintamenoiksi
- Kustannustason nousu

Investointimenot

Investointitaso ollut jo pitkään sama 4,0 Me/vuosi (3 v siirtomääräraha)

25 käynnissä olevaa hanketta

Tietohallinnon hankesalkun menot vuodelle 2021 ovat yhteensä 6 400 000 euroa. Jo käynnissä olevien hankkeiden osuus on 4 500 000 euroa.

1 900 000 euroa on puolestaan varattu hankkeisiin, joiden on suunniteltu käynnistyvän loppuvuoden 2020 tai vuoden 2021 aikana.

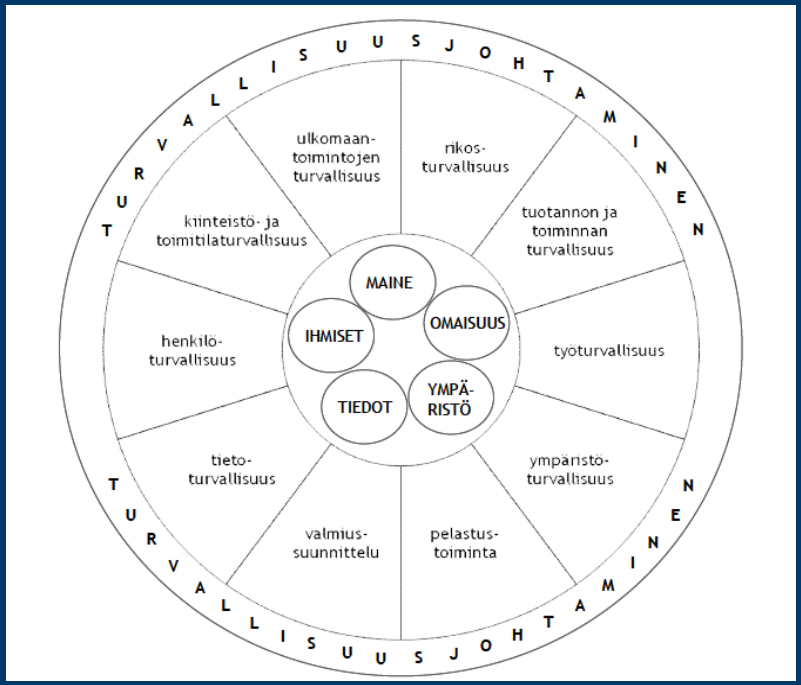
Hankekohtaiset arviot ovat kuitenkin vain suuntaa antavia ja tietohallintotoimisto ennakoi määrärahojen kokonaisuudessaan riittävän.

Tietoturvan resurssit

- THT:ssä tällä hetkellä yksi vain tietoturvaan erikoistunut erityisasiantuntija (Outi Juntura)
- Tietoturvatiimissä lisäksi TH-päällikkö ja kaksi asiantuntijaa
- Yksi erityisasiantuntijan virka tarvittaisiin 2021, jotta sisäiset resurssit riittävät (käynnissä oleva ma. erityisasiantuntijan rekrytointi ei onnistunut)
- Yhteensä tietoturvan toimintamenot n. 600-900 te vuosittain – alle 10% toimintamenoista – onko taso oikea?

Tietoturvakatsaus

Tietoturvavastaava Outi Juntura
12.11.2020



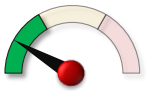
Tietoturvan hallintajärjestelmän auditointi

- Tietoturvan hallintajärjestelmä auditointiin eduskunnan tilintarkastajien toimesta ja yleisarvosanaksi saatiin B =Toimiva. Kehittämiskohteet ovat:

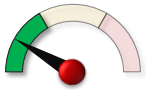
Kehittämiskohde	Toimenpide
Tietoturvariskien hallinta ja strateginen suunnittelu	Riskien hallinnan uudistaminen ja yhtenäistäminen eduskunnan kansliassa yhteistyössä turvallisuusosaston kanssa
Tietoturvan organisointi	**Tietoturvan ohjausryhmän perustaminen** **- Raportoidaan puolivuosittain kanslian johtoryhmään**.
Omaisuuden tietoturva	**O365 palveluiden uudelleen arviointi henkilötietojen käsittelyssä ja jäännösriskin hyväksyminen omistajan Tietohallintopäällikön toimesta**
Alihankkijoiden tietoturva	Päätoimittajan auditointi kolmen vuoden välein - Aloitetaan 2021
Tietoturvapoikkeamien hallinta	**Jäännösriskien ja kehittämistoimenpiteiden huomiointi johdon raportoinnissa. Kehitetään johdon raportointia osana puolivuosikatsausta**
Liiketoiminnan jatkuvuus	Hallinnollisen toiminnan jatkuvuussuunnitelmat. Kriittisten tietojärjestelmien testaukset toipumissuunnitelmien mukaisesti osana puolivuosittaista päivitystä.
Poikkeustilanteisiin varautuminen	Palvelutoimittajien resurssien riittävyys myös poikkeusoloissa realisoitunut. - **Huomioidaan uusissa kilpailutuksissa/sopimuksissa**.
Vaatimuksenmukaisuus	Riskien hallinta järjestelmien elinkaaren aikaisten riskien tunnistamiseen ja hallintaan osana palvelun ohjaamista.

- Toimenpiteiden käynnistämiset osittain odottavat eduskunnan normaalin toimintaan siirtymistä.

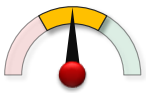
Tilannekuva tammi-lokakuu 2020



Tietovuodot ja tietomurrot
- Edustajan facebook tili kaapattu ja väärinkäytetty maksutietoja.



Verkkohyökkäykset ja julkiset palvelut
- Suojaukset toimineet ja suodatteneet “kohinan”
- Ei havaittuja verkkohyökkäyksiä, jotka olisivat aiheuttaneet toimenpiteitä.



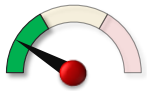
Uhkat (haittaohjelmat, botnetit…)
- Muutamia suojauksesta läpi päässeitä haittaohjelmia.
- Työasemissa havaittu haitallisia ohjelmia ja poistettu prosessin mukaisesti.
- Koneellinen kohdistettu hyökkäys WhatsAppilla.



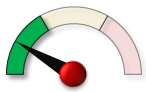
Haavoittuvuudet
- IOS Mail sähköpostihaavoittuvuudesta ei nähtävästi hyödynnetty.
- Poikkeama kriittisessä palvelussa, muutoin kriittiset haavoittuvuudet hoidettu prosessin mukaisesti.
- Haavoittuvuudet, jotka edellyttävät pääsyä verkkoon tai hallintaliittymään on viivästetty poikkeusolojen takia.



Kalastelu, tiedonhankinta ja vakoilu
- Useita havaintoja väärinkäyttöyrityksistä ja erilaisista urkintatoimenpiteistä, Koronaan liittyviä kalasteluviestejä.
- Pääsihteerin nimissä lähetetty rahankeräys IPEX-yhteisössä.
- Valtiollisten toimijoiden aktiivisuus lisääntynyt



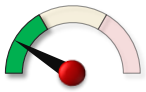
Tietoturvaperiaatteiden vastainen käyttö
- Useampi Teams/Skype kokous yhtäaikaisesti valiokuntatyössä muiden toimijoiden kanssa.



Verkkojen ja palveluiden toimivuus
- Ei havaittuja poikkeamia verkkojen toimimattomuuksia.



Talotekniikka- ja turvaverkot
- Näkyvyyttä pitää parantaa.



Pilvipalvelut
- Näkyvyys ja hälytykset käytössä toimistopilvipalveluun
- 0365 palveluun yritetty kirjaantua Yhdysvalloista, Kiinasta, Singaporesta TOR-verkosta.



Tietosuojaloukkaukset
- Yksittäinen tietosuojaloukkaus Skypen yhteissähköpostitilin käytössä.
- EU-tuomioistuimen Schrems II päätös aiheuttanee riskiä pilvipalveluiden käytössä. Privacy Shield järjestely mitätöity.

2020 vuoden auditoinnit

- Valiokuntien asianhallintajärjestelmä
- Julkinen verkkopalvelu
- Tietosuoja aineiston hävittäminen
- Salin puhelin äänestys
- Salin etä-äänestys
- Salijärjestelmän laajennettu käyttö
- Potilastietojärjestelmä
- Työterveyskysely