VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Digitaalisen turvallisuuden strateginen riskiarvio, haastattelujen yhteenveto

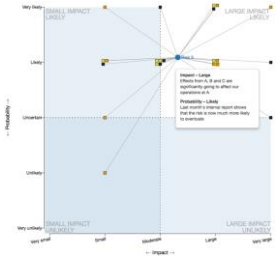
Tuija Kuusisto, tietohallintoneuvos
Niko Mäkilä, erityisasiantuntija
Miika Hätinen, korkeakouluharjoittelija
07.09.2020

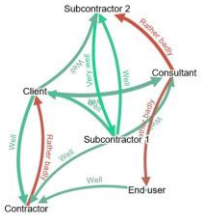
Digitaalisen turvallisuuden johtoryhmän jäsenten haastattelut

- Digitaalisen turvallisuuden strategisen johtoryhmän haastatteluilla selvitettiin
  - riskiarviomallin sisältöä,
  - digitaalisen turvallisuuden riskiarvioinnin nykytilaa sekä
  - merkittävimpiä digitaalisen turvallisuuden riskejä
- Haastattelujen tulosten yhteenveto on TLIV luokiteltu raportti
- Haastattelijat: Tuija Kuusisto, Miika Hätinen, Jani Pyrrö, VM

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskiarviomalli - vaiheistus

DVV & Tietokiri	DVV& Vahti	VM & DVV & Vahti	STR JORY	DVV & Vahti	STR JORY
Tiedon keräys	**Tiedon luokittelu**	**Tiedon analysointi**	**Tiedon verifiointi**	**Analyysin täydennys**	**Toimeenpano**
Digiturvanäkökulma: • Kansallinen riskiarvio • Julk hall riskienhallinta • TIKE, SUPO, Traficom, DVV/Vahti • JTS, TTS • Kv-riskidata: WEF, ISF, Enisa	Luokitellaan riskit (VM/riskienhallinta): • Strateginen, operatiivinen, taloudellinen sekä vahinkoriski Poimitaan digiturvan näkökulmasta vaikuttavat ja olennaiset riskit	Digiturvan näkökulmasta poimitut riskit käsitellään päätöksenteon pohjaksi riskikuvausmallin mukaisesti	Strateginen johtoryhmä käsittelee riskikartan Ylimmän johdon asiantuntija-arvio riskikuvausmallin mukaisesti	DVV ja Vahti-verkosto täydentävät riskienhallintatoimen-piteet sekä niihin liittyvät kustannukset. Arvioidaan riskien-hallinnan riippuvuussuhteita	Strateginen johtoryhmä käsittelee riskit & riippuvuussuhteet ja seuraa toimenpiteitä Strategisen johtoryhmän jäsenet sisällyttävät riskiarvion mukaiset toimenpiteet JTS ja TTS





VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Riskiarviomalli - riskien kuvausluonnos

Turvat-tava kohde	Riskin kuvaus	Todennä-köisyys	Arvioitu frekvenssi	Vaikutuk-set	Menetykset	Hallinta	Vastuu	Kustannus	Vaikuttavuus	Seuranta
Koh-teen nimi	Riskin kuvaus ja lähde	Riskin toteutumisen todennäköi-syys arvioidulla ajanjaksolla, esim. asteikolla 1-4	Riskin esiintyvyys arvioidulla ajanjak-solla	Riskin vaikutus; riskien kriittisyyden perusteella, esim. asteikolla 1-4	Arvioidut menetykset jos riski toteutuisi.	Valittavat suojaus-toimet	Riskin hallinnasta vastuulli-nen taho	Valittujen suojaustoimien kustannukset (I)	Digitaalisen turvallisuuden vaikuttavuus (T), menetysten pienentyminen (Z), T=Z-I	Suojaus-toimien vaikuttavuu-den seuranta

Digiturvariskien aiheuttamia potentiaalisia menetyksiä

- Immateriaalioikeudelliset menetykset
- Luottamuksellisen tiedon vuotamisesta aiheutuvat seuraukset
- Henkeen ja terveyteen kohdistuvat menetykset
- Toiminnan keskeytykset
- Korvallisuusvelvollisuudet kolmansille osapuolille
- Poikkeamien tutkimisen ja selvittämisen aiheuttamat menetykset
- Datan ja ohjelmistojen menetykset
- Vaikutukset maineeseen
- Kiristystapauksista ja petoksista aiheutuneet menetykset
- Fyysiseen omaisuuteen kohdistuvat menetykset

(Rokkas, Neokosmidis ja Xydias 2018, Systemic Analyzer in Network Threat (SAINT) – projekti)

Yhteenveto strategisen digiturvan joryn haastatteluista

- Keskeiset havainnot strategisesta riskiarviomallista
  - Haastatellut pitivät riskiarviomallia hyvänä
  - Pohdittava mihin ja millä tasolla riskiarvioinnilla tahdotaan vaikuttaa? Ja miten arvioinnin tulokset saadaan käyttöön?
    - Kattavuus koko julkinen hallinto ml liikelaitokset ja yhtiöt sekä yliopistot ja korkeakoulut
    - Vuosittainen fokusoituminen johonkin julkisen hallinnon alueeseen, osana kokonaisturvallisuuden hallintaa
  - Tiedon keräysvaihe on kriittinen, tietolähteet heterogeenisiä
  - Turvattavien kohteiden tunnistaminen ja riskien luokittelu on olennaista
  - Keskinäisriippuvuuksista johtuen yhteistoimintakartan laadinta on merkittävä osa mallia
  - Riskienhallintamalli on integroitava talouden vuosikelloon
- Julkisen hallinnon strategisen tason digitaalisen turvallisuuden tilannekuva on puutteellinen - Tarve säännölliselle koko julkisen hallinnon kattavalle riskiarvioinnille
  - Tarve tarkentaa strategista tilannekuvaa kuntien osalta

Strategisen digiturvan joryn haastattelujen perusteella toteutettiin kuntien ICT-yhtiöiden haastattelut elokuussa

- Kuntien ja kuntayhtymien ICT-yrityksien (7 kpl) haastattelu
  - Kuntien digitaalisen turvallisuuden ja riskiarvioinnin nykytila
  - Kuntien kannalta merkittävimpiä digitaalisen turvallisuuden riskejä
  - Haastatellut yritykset:
    - Kuntien Tiera Oy
    - Oulun Digi
    - 2M-IT Oy
    - Istekki Oy
    - Kymijoen ICT
    - Meidän IT ja talous Oy (MEITA)
    - LapIT Oy

Kuntien ICT-yhtiöiden haastattelujen johtopäätökset

- Kuntien keskeisten ICT-yhtiöiden näkemyksen mukaan kuntien riskienhallinnan tilanne on heterogeeninen ja vaihtelee kunnittain
  - Usein kunnissa ei selkeästi vastuutettu digitaalisen turvallisuuden riskienhallintaa, eikä kokonaisvaltaista, säännöllistä digitaalisen turvallisuuden riskienhallintaa tehdä
  - Kuntien digitaalinen turvallisuus monesti ulkoistettu ICT-yhtiön vastuulle
  - Kunnissa ei ole yhteisiä käytäntötapoja tai linjauksia joita noudattaa digiturvan osalta
  - Etenkin pienissä kunnissa ICT-osaamisen ja digiturvan taso usein huono
- Pääasiassa sosiaali- ja terveydenhuollon puolella kriittisimmät tietovarannot ja järjestelmät
  - Riskinä erityisten henkilötietojen/terveystietojen vuodot
- Kunnat, ja niiden ICT-yhtiöt raportoivat laajalti merkittävät tietoturvapoikkeamat Kyberturvallisuuskeskukselle

Seuraavat askeleet

- Strategisen riskiarviomallin pilotointi kuntasektorilla syksyn 2020 aikana
- Tunnistettujen riskien käsittely mallin mukaisesti
  - digiturvan strategisessa johtoryhmässä syyskuussa ja joulukuussa
  - Vahti-verkostossa ja VM:ssä loka-marraskuussa
- Riskiarvioinnin tulokset huomioidaan kun kuntien digiturvan kehittämisen toimenpiteitä tarkennetaan osana Haukka-hanketta, ja toteutetaan JUDO-hankkeen kanssa
- Pilotoinnin kokemusten perusteella strateginen riskiarviomalli tarkennetaan ja julkaistaan vuonna 2021
- Säännöllistä digiturvan strategisten riskien arviointia jatketaan

Liite 1: Digitaalisen turvallisuuden strategisen johtoryhmän haastattelujen tulokset

Haastatellut henkilöt

- Nerg Päivi, valtiovarainministeriö
- Kerkelä Janne, valtioneuvoston kanslia
- Puustinen Pekka, ulkoministeriö
- Aalto Jukka, sisäministeriö
- Knape Petri, sisäministeriö
- Jyväsjärvi Raimo, puolustusministeriö
- Karjalainen Anna-Maija, valtiovarainministeriö
- Mustonen Esko, valtiovarainministeriö
- Paananen Rauli , liikenne- ja viestintäministeriö
- Vilkkonen Laura, liikenne- ja viestintäministeriö
- Voipio-Pulkki Liisa-Maria, sosiaali- ja terveysministeriö
- Klemm Kari, työ- ja elinkeinoministeriö
- Valtonen Vesa, Turvallisuuskomitea
- Rousku Kimmo, digi- ja väestötietovirasto
- Viskari Janne, digi- ja väestötietovirasto
- Karttaavi Tommi, Kuntaliitto
- Ylikoski Jari, Kuntaliitto
- Inna Lauri, Salon kaupunki
- Viljanen Ritva, Vantaan kaupunki

Riskiarviomallista

- Haastateltavat kannattivat koko julkisen hallinnon kattavaa riskiarviota
  - Riskiarvio on fokusoitava aluksi/vuosittain
- Riskiarviomallissa huomioitava
  - Turvallisuuden kokonaiskuvan hahmottaminen ja ennakointityö
  - Mihin ja millä tasolla on tarkoitus vaikuttaa?
  - Tulosten on oltava tarpeeksi konkreettisia, ja johtajien ymmärrettävissä
- Ehdotettiin fokusointia aluksi kuntiin
  - Kuntien heterogeenisyys – epäselvä digiturvan tilannekuva
  - Suuri määrä tietovarantoja ja työntekijöitä
  - Vuoden 2019 tietoturvaloukkaustapaukset

Riskiarvioprosessista

- Haastateltavat pitivät alustavaa prosessikuvausta hyvänä
  - Tiedon keräysvaihe on kriittinen
    - Heterogeenisistä, laajoista tietolähteistä on vaikea tunnistaa olennaisia riskejä
    - Tämä haastaa riskiarvion luotettavuuden
    - Tiedonkeruun tulisi myös olla riittävästi automatisoitu
- Laajasta ja heterogeenisestä tietopohjasta johtuen turvattavien kohteiden tunnistaminen ja riskien luokittelu on olennaista
- Prosessi on integroitava talouden vuosikelloon, jotta voidaan ajoissa vaikuttaa talouden ja toiminnan suunnitteluun
- Keskinäisriippuvuuksista johtuen yhteistoimintakartan laadinta on merkittävä osa prosessia
- Pohdittava: Kuinka riskiarvion tulokset saadaan parhaalla mahdollisella tavalla hyödynnettäviksi julkisen hallinnon toimijoille?

Kustannusten arviointi osana riskiarviointia

- Haastatteluissa suhtauduttiin pääosin positiivisesti kustannusten arviointiin osana riskiarviointia
  - Resursointia mahdollistetaan tuomalla esiin digiturvan kustannuksia
  - Kustannusten jaottelu esimerkiksi NISTin kyberturvallisuuden arvioinnin viitekehyksellä
- Kustannusten arvioinnin haasteita
  - Julkisessa hallinnossa käytetään useita laadullisia mittareita
  - Nopeasti muuttuvasta toimintaympäristöstä johtuen riskien realisoitumisen kustannusten historiadatan käyttö on vaikeaa

Liite 2: Kuntien omistamien ICT-yhtiöiden haastattelujen tulokset

Kuntien ICT-yhtiöiden haastattelut elokuussa 2020

- Haastattelut suurimpien kuntien omistamien ICT-yhtiöiden kanssa
  - Kuntien digitaalisen turvallisuuden, ja riskiarvioinnin nykytila
  - Kuntien kannalta merkittävimpiä digitaalisen turvallisuuden riskejä
  - Haastatellut yritykset:
    - Kuntien Tiera Oy
    - Oulun Digi
    - 2M-IT Oy
    - Istekki Oy
    - Kymijoen ICT
    - Meidän IT ja talous Oy (MEITA)
    - LapIT Oy

Digitaalisen turvallisuuden riskienhallinnan tilanne kunnissa 1

- Kuntien keskeisten ICT-yhtiöiden näkemyksen mukaan kuntien riskienhallinnan tilanne on heterogeeninen ja vaihtelee kunnittain
  - Usein kunnissa ei selkeästi vastuutettu digitaalisen turvallisuuden riskienhallintaa, eikä kokonaisvaltaista, säännöllistä digitaalisen turvallisuuden riskienhallintaa tehdä
  - Tyypillisesti pienissä kunnissa
    - Riskienhallinta on pistemäistä ja reaktiivista
    - Vain osa hallinnollista prosessia, eikä kata operatiivisen toiminnan riskejä
    - Digitaalinen turvallisuus usein kunnanjohtajan vastuulla
  - Kaupungeissa
    - Riskienhallinta on osa operatiivista toimintaa
    - Riskejä pienentävät toimet ovat usein hiukan jäljessä
    - Tyypillisesti on erikseen nimettyjä digiturvan vastuuhenkilöitä

Digitaalisen turvallisuuden riskienhallinnan tilanne kunnissa 2

- Sairaanhoitopiireissä
  - Riskienhallinta on usein ulkoistettu ICT-yhtiöille, jotka pyrkivät aktiiviseen riskienhallintaan
  - Rahoittajakunnat keskittyvät kustannusten minimointiin, eikä innokkuutta rahoittaa esim. datan menetystilanteiden harjoittelua ole
- Kuntien ICT-yhtiöissä
  - Pitäisi harjoitella enemmän häiriötilanteista toipumisia
  - Keväällä 2020 tunnistettiin kohdennettuja hyökkäyksiä
- Kuntien ICT-yhtiöiden alihankkijat
  - Teleoperaattoreiden ja isojen ICT-toimijoiden osalta riskienhallinta hyvällä tasolla
  - Pienissä, yhtä ratkaisua tarjoavissa alihankkijoissa riskienhallinnan kyky heikko, ja ne usein nojautuvat kansainvälisiin pilvipalvelutarjoajiin

Digitaalisen turvallisuuden riskienhallinnan tilanne kunnissa 3

- Riskienhallinnassa keskitytään ulkoisiin uhkiin, ei huomioida sisäisiä riskejä
- Tietosuojan riskienhallinnasta vähän havaintoja
- Kuntien digitaalinen turvallisuus monesti täysin ulkoistettu ICT-yhtiön vastuulle
  - Ei mielletä että digiturvallisuus vaikuttaisi kovinkaan paljon omaan toimintaan, sen ollessa ulkoistettuna
- Digitaaliseen turvallisuuteen ei olla välttämättä valmiita panostamaan kovinkaan paljon resursseja
  - Minimiturvauksen taso katsotaan monesti riittäväksi
  - Sosiaali- ja terveydenhuollon tietoturvaan panostetaan usein eniten sen kriittisyyden vuoksi

Digitaalisen turvallisuuden riskienhallinnan tilanne kunnissa 4

- Kunnissa ei ole yhteisiä käytäntötapoja tai linjauksia joita noudattaa digitaalisen turvallisuuden osalta
  - Esimerkiksi voiko sote-tietoa säilyttää pilvessä?
- Varautumisen merkitys kasvaa mutta siihen ei panosteta riittävästi
- ICT-yhtiöt ovat pääosin saaneet osaavaa henkilökuntaa
- Kunnat eivät pysty kilpailemaan osaamisesta kaupallisten toimijoiden kanssa
  - Etenkin pienissä kunnissa ICT-osaamisen ja digitaalisen turvallisuuden taso usein huono

Mitä tietoa digitaalisista riskeistä tai niiden hallinnasta puuttuu?

- Kokonaisvaltaista kuvaa digitaalisista riskeistä ei ole
- Digitaaliset uhat kehittyvät jatkuvasti, mutta tunnistaminen ei
- ICT-yhtiöillä ei välttämättä ole tarkkaa kuvaa kuntien koko toiminnasta tai kaikista järjestelmistä, jotta ICT-yhtiössä osattaisiin arvioida riskien kaikkia vaikutuksia
- Kriittisiä toimintoja ja palveluita ei välttämättä arvioida, luokitella tai priorisoida
- Kuntien johtoa varten tarvittaisiin skenaarioita, joissa uhkia ja euromääräisiä menetyksiä olisi kuvattu selkeästi
- Kunnissa voisi olla tietoturva- ja tietosuoja-agentteja

Potentiaalisten realisoituvien riskien kustannusten arvioinnista

- Potentiaalisia euromääräisiä menetyksiä riskien realisoituessa ei juurikaan arvioida
  - Vaikea arvioida täsmällisesti.
  - Arviot eivät olisi välttämättä vertailukelpoisia
- Rahallisia arvioita esittämällä olisi helpompi perustella lisäresursointia digiturvallisuuteen
- Esimerkkitapausten ja erilaisten skenaarioiden hahmottamisen kautta riskien potentiaalisten vaikutusten arviointia ja esittelyä

Mikä on tilanne koskien tietoturvapoikkeamien ilmoittamista kyberturvallisuuskeskukselle?

- Kunnat, ja niiden ICT-yhtiöt raportoivat laajalti merkittävät tietoturvapoikkeamat kyberturvallisuuskeskukselle
- Yhteistyö kyberturvallisuuskeskuksen kanssa toimii hyvin
  - Yhteistyötä voisi jopa kasvattaa, esimerkiksi keskuksesta voisi hankkia asiantuntijapalveluita tarvittaessa
  - Kyberturvallisuuskeskus voisi tuottaa nykyistä tarkempaa tilannekuvaa ilmoitusten perusteella
- Kyberturvallisuuskeskus voisi tuottaa ajankohtaista, lähes reaaliaikaista tilannekatsausta riskeistä ja erilaisista kyberhyökkäyksistä
- Kyberturvallisuuskeskus: Kuntien kontaktihenkilöluettelo on puutteellinen

Muita näkökulmia

- Palvelutuotantoympäristöjen ja palveluiden tietoturvallisuuden tason luokittelu ja sertifiointi kuntien hankintoja ja sopimuksia varten
  - Palvelutuotannon turvallisuusluokittelu, esim. asteikolla 0-5, jossa esim. jos Amazonin pilvipalvelua käytetään perusmuotoisesti se olisi tason 0 palvelu
  - Palveluiden luokittelu sen mukaisesti minkä tietoturvallisuusluokan tietoja ko palvelussa saa käsitellä / mitkä ovat palvelun täyttämät tietoturvallisuustoimenpidevaatimukset
- Digitaalista turvallisuutta pitäisi edistää yhtenäisillä ratkaisuilla
  - Hyviä kokemuksia yhteisen resursoinnin ja kehittämisen kautta
- Digiturvan riskienhallintaa olisi syytä tehdä kokonaisvaltaisesti ja proaktiivisesti

Liite 3: Mitä VM:ssä Haukassa jo tapahtuu kuntien digiturvan edistämiseksi?

Kuntien haavoittuvuuksien skannaus, analysointi ja viestintä kunnille

- VM yhdessä DVV:n JUDO-hankkeen ja Traficomin kanssa on käynnistämässä kuntien haavoittuvuuksien skannausta, analysointia ja viestintää kunnille tämän syksyn aikana
- …?

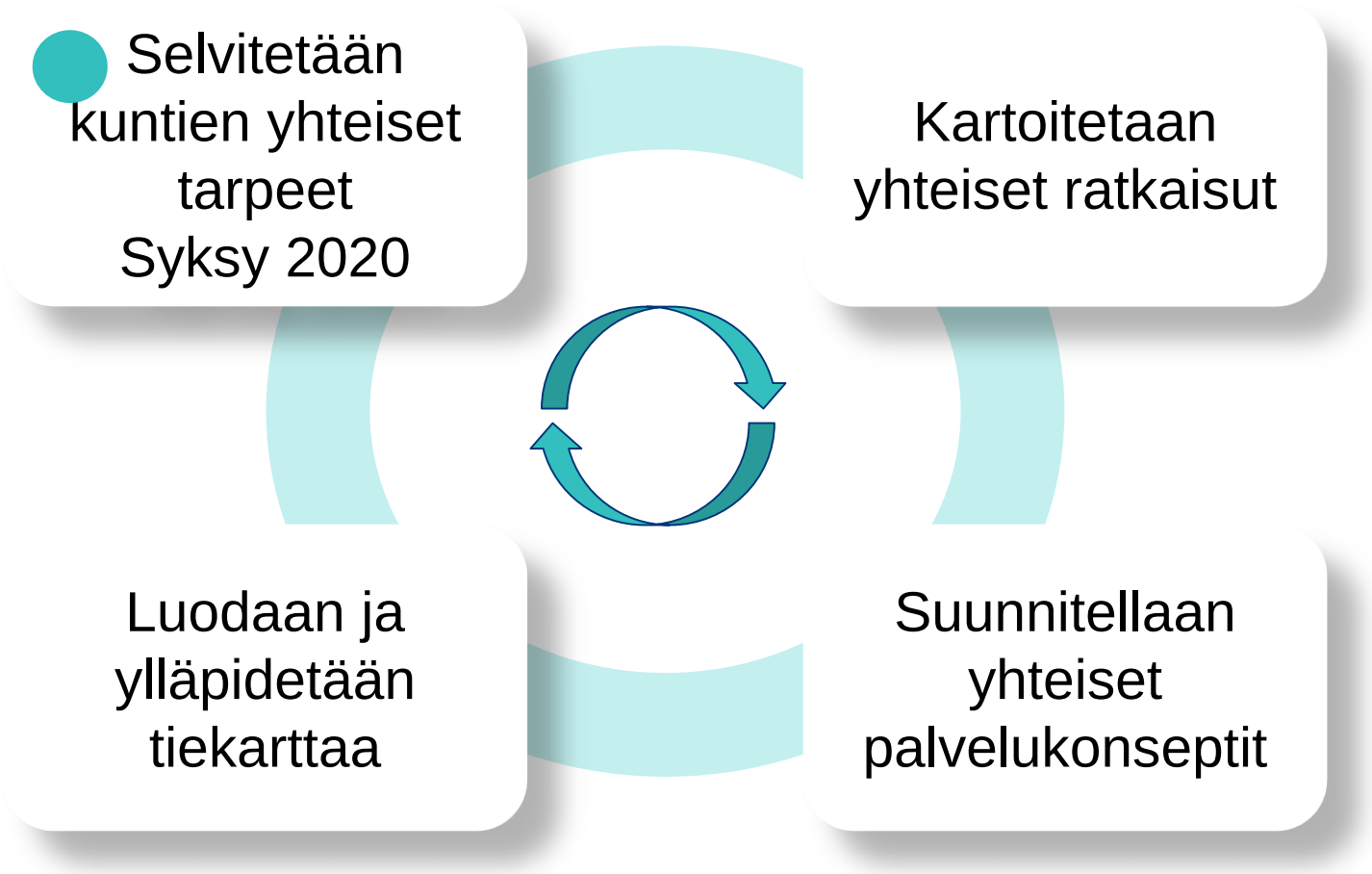
Liite 4: Mitä DVV:ssä jo tapahtuu Haukassa/JUDO-hankeessa kuntien digitaalisen turvallisuuden kehittämiseksi?

Haukka-hankkeesta tukea kuntien digitaaliseen turvallisuuteen

Kuntien tarpeiden selvitys käynnistyy

Kirsi Janhunen

DIGI- JA VÄESTÖTIETO-VIRASTO



Kuntien tarpeiden pohjalta luodaan jatkuvasti ylläpidettävä tiekartta digitaalisen turvallisuuden palveluista