Asiantuntijalausunto Valtioneuvoston selontekoon sisäisestä turvallisuudesta liikenne- ja viestintävaliokunnalle sekä puolustusvaliokunnalle – tiivistetty esitys

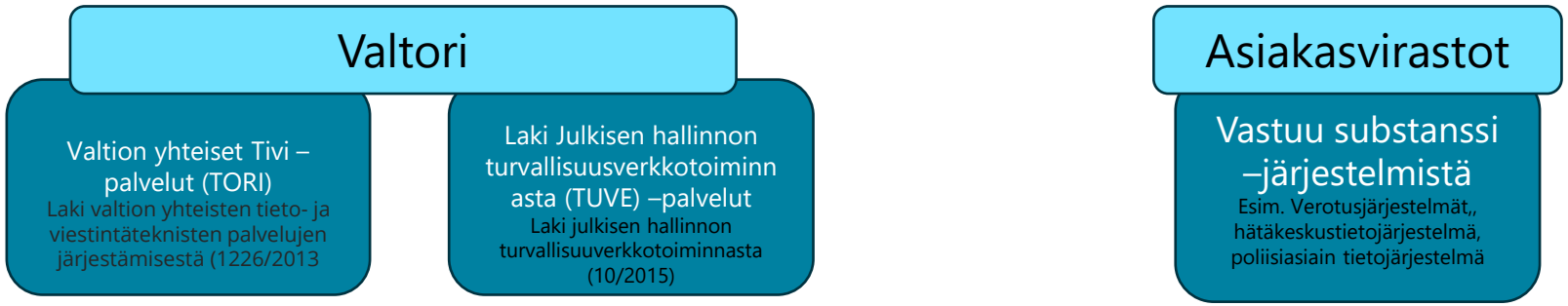
Valtion tieto- ja viestintätekniikkakeskus, Valtori

Ylijohtaja Hannu Naumanen

Valtori

Teema 1: Lainsäädäntö ja roolit

- Valtori tuottaa lakisääteisesti valtionhallinnon toimialariippumattomat (TORI) ICT-palvelut sekä korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintäteknisiä palveluja ja integraatiopalveluja.
- Valtori toimii palvelutuottajana laki julkisenhallinnon turvallisuusverkkotoiminnasta (10/2015) mukaisesti. Turvallisuusverkkotoimintaan liittyvä käyttöoikeus ja toiminta on erikseen säädeltyä suhteessa muuhun Valtorin toimintaan. Turvallisuusverkkotoiminnan (TUVE) asiakkaat (pääosa sisäisen turvallisuuden toimijoista) voivat käyttää myös muita Valtorin palveluita, mutta turvallisuusverkkotoiminnan palveluiden käyttö on mahdollista vain laissa luetelluille sekä valtiovarainministeriön erikseen hyväksymille käyttäjäryhmille.
- Asiakkaat ml. sisäisen turvallisuuden toimijat vastaavat substanssiin liittyvien toimialasidonnaisten (TOSI) tietojärjestelmien kehittämisestä.



- Valtiovarainministeriön johdolla on käynnistetty lainsäädännön kehittämishanke, jonka tavoitteena on ajantasaistaa säädöspohja vastaamaan toimintaympäristön muutoksia. Valtori näkee tärkeänä, että lainsäädännön uudistamishanke etenee, jotta jatkossa voidaan vastata myös sisäisestä turvallisuudesta vastaavien viranomaisten palvelutarpeisiin paremmin sekä samalla varmistaen käytettävien palveluiden turvallisuus
- **Esimerkki:** Valtori voi tarjota tehokkaammin käyttötarpeisiin vastaavia (ml. kumppaneiden tuottamia) palveluita koko asiakaskunnalle

Valtori

Teema 2: Uhkatilanne ja uhkavektorit

*(Yleisyys/vaikuttavuus), Valtorin arvio

- Kyberturvallisuuteen liittyviä uhkavektoreita:
  - Kiristyshaittaohjelmat (+++/+)*
  - Palvelunestohyökkäykset (+++/+)
  - Uhkatoimijoiden kyberoperaatiot (ml. valtiolliset toimijat) (+/+++)
  - tekoälyllä automatisoidusti toteutetut laajat huijauskampanjat. (+++/+)
  - Toimitusketjut, myös hybridivaikuttamisessa (+/++)
- Toimintaympäristön muutostekijöitä:
  - Kvanttilaskenta / Kvanttisalaus
  - AI/tekoäly
  - Informaatiovaikuttaminen
  - Crime as-a-service - menetelmä
    - Erityisesti palvelunestohyökkäyksissä

Digitaalisen toimintaympäristön haavoittuvuudet ovat korostaneet tarvetta kehittää turvallisuuskulttuuria suunnitelmallisesti ja kokonaisvaltaisesti.

Valtori

Teema 3: Tiedonvaihto ja johtaminen

- Tiedonvaihto ja tilannekuvan ylläpitäminen viranomaisyhteistyössä ovat elintärkeitä suojaustoimintojen onnistumiselle.
- Pääosa tiedonvaihtofoorumeista on toimivia sekä yhteistä päämäärää edistäviä.
- **Esimerkki:** Voimassa oleva lainsäädäntö (tietosuojanäkökulma) rajoittaa tietyiltä osin viranomaisilla käytettävissä olevien suojaus- ja havainnointi suorituskykyjen käyttöä.

- Valtori näkee tärkeänä, että selonteossa on otettu kantaa kyberturvallisuutta vakavasti vaarantavan tilanteen johtovastuiden sekä tilannekuvan muodostamisen selkeyttämiseen. Valtori näkee asiassa kehitettävää ja selkeytettävää.
- Vaikutukseltaan laajojen kyberturvallisuutta vaarantavien ja useaan viranomaiseen vaikuttavien johtamistilanteiden harjoitteluun on syytä panostaa enemmän teknisluonteisten harjoitusten lisäksi.

Valtori

Teema 4: Rahoitus ja korjausvelan hallinta - pilviteknologiat

- Julkisen hallinnon kireästä taloudellisesta tilanteesta huolimatta on tärkeätä huolehtia kyberturvallisuuden ja ICT-palvelujen varautumiseen (ml. esimerkiksi suoja- ja väistotilat), liittyvän rahoituksen riittävästä varmistamisesta, ettei tietojärjestelmiin liittyvä korjausvelka kasva liian suureksi.
    - **Esimerkki:** Yhteisessä palveluympäristössä Teeman 1 mukaisesti ylläpitovastuut hajautuvat laajalle joukolle

- Asiakaskohtaisista ratkaisuista luopuminen ja entistä laajempi yhteisten palvelujen käyttö kasvattaa turvallisuustasoa.
    - **Esimerkki:** Valtionhallinnossa on käytössä yli kaksikymmentä erillistä työasemavakiota

- Uusien teknologioiden hallittu käyttöönotto ja mahdollistaminen, erityisesti pilvipalveluiden osalta, tuo mahdollisuuksia hallita korjausvelkaa tehostaen samalla tuottavuutta. Pilvipalveluiden hallittu korkeintaan turvallisuusluokka IV tiedon käsittelyn mahdollistaminen on arvioitu edistävän pilvisiirtymää merkittävästi.

Valtori