Valtori/2620/00 05 00/2025
Valtori/2619/00 05 00/2025

ICT-toiminnan tukipalvelut

16.10.2025

Asiantuntijalausunto Valtioneuvoston selontekoon sisäisestä turvallisuudesta liikenne- ja viestintävaliokunnalle sekä puolustusvaliokunnalle

Eduskunnan liikenne- ja viestintävaliokunta sekä puolustusvaliokunta ovat pyytäneet Valtion tieto- ja viestintätekniikkakeskus Valtorilta asiantuntijalausuntoa Valtioneuvoston selontekoon sisäisestä turvallisuudesta (VNS 6/2025).

Valtori kiittää mahdollisuudesta lausua asiassa ja katsoo tarkoituksenmukaiseksi lausua samansisältöisesti molempiin lausuntopyyntöihin.

Yleistä

Selonteko tarjoaa kattavan ja ajankohtaisen tilannekuvan sisäisen turvallisuuden toimintaympäristön muutoksista sekä viranomaisten roolista yhteiskunnan kriisinkestävyyden ja turvallisuuden ylläpitämisessä. Selonteon linjaukset tukevat vahvasti yhteiskunnan toimintojen jatkuvuutta, kyberturvallisuuden kehittämistä ja varautumista.

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 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.

Toimintaympäristön muutoksesta

Teknologian jatkuva kehittyminen (ml. tekoäly) sekä kyberturvallisuuden pysyvästi kohonnut uhkataso ovat muuttaneet toimintaympäristön uhkanäkymää. Näihin uhkiin vastaaminen edellyttää uusia ja tehokkaampia toimia, yhteistyötä laajasti viranomaiskentässä sekä havainnointi ja reagointikyvyn ympärivuorokautista ylläpitoa. Tiedonvaihto ja tilannekuvan ylläpitäminen viranomaisyhteistyössä ovat elintärkeitä suojaustoimintojen onnistumiselle. Voimassa oleva lainsäädäntö tietosuojanäkökulmasta rajoittaa tietyiltä osin käytettävissä olevien suojaus suorituskykyjen käyttöä.

Kyberturvallisuudessa on laajasti raportoitu kiristyshaittaohjelmahyökkäyksistä, valtiollisten toimijoiden kyberoperaatioista ja tekoälyllä automatisoidusti tuotetuista laajoista huijauskampanjoista. Digitaalisen toimintaympäristön haavoittuvuudet ovat korostaneet tarvetta kehittää turvallisuuskulttuuria suunnitelmallisesti ja kokonaisvaltaisesti. Tämän rinnalla tapahtuva teknologinen kehitys, kuten kvanttilaskenta ja AI/tekoäly, muuttavat jatkuvasti kyberturvallisuuden toimintaympäristöä sekä lisäävät uusia uhkamahdollisuuksia ja kyberriskejä. Kvanttiturvallisuuden varmistaminen valtiohallinnossa seuraavien vuosien aikana on merkittävässä roolissa tiedon luotettavuuden varmistamisessa.

Valtori korostaa lisäksi toimitusketjujen hallinnan merkitystä turvallisuuden varmistamisessa niin ICT- kuin muiden teknologiaa ja ohjelmistoja sisältävien laitteistojen osalta. Toimitusketjut on yleisesti tunnistettu myös yhdeksi potentiaaliseksi hybridivaikuttamisen kohteeksi.

Turvallisuusinvestointien kasvaessa haastaa kilpailu osaavasta työvoimasta toiminnan kehittämistä. Valtiohallinto ei voi toimia palkkajohtajana, joka johtaa siihen, että on välttämätöntä hyödyntää koulutus- ja akatemiaohjelmia riittävän osaamisen varmistamiseksi.

Valtori pitää hyvänä, että selonteossa on hyvin tuotu esiin informaatiovaikuttamisen merkitys ja sen eri muodot. Yhteisiin tieto- ja viestintäteknisiin palveluihin kohdistuu erityisesti palvelunestohyökkäyksiä, mutta myös kehittyneempiä pitkäkestoisia uhkia, joiden tavoitteena on tiedon kerääminen tai jalansijan luominen palveluiden jatkuvuutta uhkaaville toimenpiteille. Edellä mainituissa tapauksissa myös informaatiovaikuttaminen on yksi uhkavektori. Palvelunestohyökkäyksissä ns. rikos -palveluna (Crime-as-a-Service) on nouseva trendi ja tekoälyn käyttö on merkittävästi kehittänyt ns. kalasteluviestien laatua.

Turvallisuuskulttuuria ja -rakenteita sekä henkilöstön tietoisuutta tiedustelu-uhista on kehitettävä. Madaltamalla henkilöstön ilmoittamiskynnystä pienistäkin laittoman tiedustelun merkeistä, on mahdollista puuttua tilanteiden kehityskulkuun riittävän aikaisessa vaiheessa.

Valtori näkee tärkeänä, että selonteossa on otettu kantaa kyberturvallisuutta vakavasti vaarantavan tilanteen johtovastuiden sekä tilannekuvan muodostamisen selkeyttämiseen. Valtori näkee asiassa kehitettävää ja vaikutukseltaan laajojen kyberturvallisuutta vaarantavien, useaan viranomaiseen vaikuttavien johtamistilanteiden hoitamista, on syytä jatkossa harjoitella enemmän teknisluonteisten harjoitusten lisäksi.

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. Asiakaskohtaisista ratkaisuista luopuminen ja entistä laajempi yhteisten palvelujen käyttö kasvattaa turvallisuustasoa.

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.

Yhteenveto

Valtori näkee selonteossa esitetyt, toimialaansa liittyvät kyberturvallisuutta ja yhteisten tieto- ja viestintäteknisten palveluiden jatkuvuutta edistävät linjaukset kannatettavina.

Kyberulottuvuudessa tapahtuvien rikosten torjunnan lisäksi korostuvat ennakointi ja riittävien suojaustoimenpiteiden toteuttaminen.

Valtori kannattaa lisäksi esitettyä toimenpidettä turvallisuusselvityslain uudistamista henkilöturvallisuuden hallinnan kehittämiseksi.

Marja Rantala

Toimitusjohtaja

Hannu Naumanen

Ylijohtaja, ICT-toiminnan tukipalvelut

Asiakirjan sähköinen allekirjoitus
Elektronisk underskrift av document
Electronic signature of a document

Asia / Sak / Case

Valtori/2619/00 05 00/2025	Liikenne- ja viestintävaliokunta tiistai 21.10.2025 klo 12.30 / VNS 6/2025 vp / Asiantuntijapyyntö

Asiakirja / Dokument / Document

Valtori/2619/00 05 00/2025-4	Asiantuntijalausunto Valtioneuvoston selontekoon sisäisestä turvallisuudesta liikenne- ja viestintävaliokunnalle sekä puolustusvaliokunnalle

Allekirjoitukset / Underskrifter / Signatures

Signed By:Naumanen Hannu 91209798J
Signed at:2025-10-16 12:23:23 +03:00
Reason:I approve this document

Signed By:Rantala Marja 91294372R
Signed at:2025-10-16 12:24:49 +03:00
Reason:I approve this document