14.10.2018

Eduskunnan hallintovaliokunta
hav@eduskunta.fiu

O 106/2016 vp Valtiovarainministeriön selvitys julkisen hallinnon turvallisuusverkkotoiminnan toimeenpanosta (EV 245/2014 vp, HaVM 35/2014 vp, HE 54/2013 vp

Julkisen hallinnon turvallisuusverkkotoiminnan toimeenpano

Hallintovaliokunta on pyytänyt Valtion tieto- ja viestintätekniikkakeskus Valtorilta ja Valtorin TUVE-yksiköltä kirjallista asiantuntijalausuntoa julkisen hallinnon turvallisuusverkkotoiminnan toimeenpanosta.

Valtori kiittää mahdollisuudesta antaa kirjallinen lausunto asiasta ja lausuu seuraavaa.

Valtion tieto- ja viestintätekniikkakeskus Valtori toimii Hallinnon turvallisuusverkon tieto- ja viestintäteknisten sekä integraatiopalveluiden tuottajana siten kuin tehtävistä TUVE-laissa (10/2015) ja TUVE-asetuksessa (1109/2015) säädetään. TUVE-laissa säädettyjen tehtävien lisäksi Valtori vastaa valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottamisesta siten, kuin tehtävistä laissa (1226/2013) ja valtioneuvoston asetuksessa (132/2014) säädetään.

Lausunnossaan Valtori arvioi turvallisuusverkkotoiminnan toimeenpanoa omasta näkökulmastaan.

Toimintojen siirto

TUVE-palvelut siirtyivät Valtorin tuotettavaksi 1.6.2016. TUVE-lain mukaan palveluntuottajan on erotettava laissa tarkoitettu toiminta hallinnollisesti, toiminnallisesti ja taloudellisesti muusta toiminnastaan. TUVE-palveluiden suunnittelu ja tuotanto organisoitiin Valtorissa TUVE-yksikköön. Siirtoprojekti onnistui hyvin eikä palveluissa tapahtunut siirrosta johtuvia häiriöitä.

Turvallisuuden ja varautumisen vaatimusten toteutuminen

Hallinnon turvallisuusverkon varautumista ja tietoturvallisuutta koskevista vaatimuksista on säädetty Valtioneuvoston asetuksen (1109/2015) 8 ja 9 §:ssä. Varautumisen ja turvallisuuden arviointikriteereistä taas on säädetty asetuksen 10 §:ssä

Valtiovarainministeriö arvioi Valtorin kyvykkyyden ottaa vastaan TUVE-palvelut jo ennen ko. toimintojen siirtoa. Tällä varmistettiin, että Valtori täyttää riittävässä määrin korkean varautumisen, valmiuden ja turvallisuuden vaatimukset.

Valtorin TUVE-yksikön toiminta on todennetusti tietoturva-asetuksen mukaisella korotetulla tasolla. TUVE-yksikön tietoturvallisuutta hallitaan tietoturvallisuuden hallintajärjestelmällä, joka perustuu ISO 27001 standardiin. Tietoturvan hallintajärjestelmä kattaa koko yksikön toiminnan. Standardin mukaisesti sertifioituja palveluja ovat viestintäpalvelut ja päätelaitepalvelut sekä palvelunhallintajärjestelmän tukiprosessit.

Lisäksi Viestintäviraston NCSA-toiminto (National Communications Security Authority) on arvioinut Valtorin TUVE-yksikön turvallisuusjohtamista vuosina 2016 ja 2018. Näiden arvioiden mukaan TUVE-yksikön turvallisuusjohtaminen täyttää kansallisen salassa pidettävän tiedon suojausvaatimukset.

Valtorin TUVE-yksikön tuottamien palveluiden varautumisen ja turvallisuuden tasoa selvitettiin valtiovarainministeriön aloitteesta vuonna 2017. Selvityksessä todettiin, että sekä TUVE-palveluiden että TUVE-asiakkaiden omien tietojärjestelmien ja toimintatapojen tietoturvaa tulee kehittää edelleen. Valtiovarainministeriö antoi heinäkuussa 2018 määräyksen turvallisuusverkon turvallisuutta parantavista toimenpiteistä sekä käynnisti uuden turvallisuusverkkoarkkitehtuurin suunnittelun. Toimenpiteet jatkuvat määräyksen mukaisesti vuoteen 2020 asti ja uuden arkkitehtuurin mukaista toimintaa aletaan rakentaa vuoden 2020 jälkeen.

Turvallisuusverkon käyttäjille on myös laadittu ohjeistus turvallisuuden vähimmäisvaatimuksista ja periaatteista TUVE-palveluita käytettäessä. Tämä ohjeistus on tällä hetkellä TUVE-asiakkaiden kommentoitavana ja ohjeistus on tarkoitus ottaa käyttöön vielä tänä vuonna.

Palveluiden kustannukset ja rahoitus

Valtorin TUVE-palveluiden kustannukset katetaan käyttäjiltä perittävillä palvelumaksuilla. TUVE-palvelut ovat tuotteistettuja palveluita ja maksut perustuvat joko kapasiteetin käyttöön tai käyttäjämääriin. Palvelumaksut kattavat sekä palveluiden käyttö- ja ylläpitokustannukset että palveluiden kehittämiseen liittyvät kustannukset.

Palveluille asetettavat tietoturva- ja muut vaatimukset lisäävät palveluiden kokonaiskustannuksia koko ajan. Toisaalta käyttäjämäärän kasvu ja palveluiden käytön lisääntyminen ovat helpottaneet kustannusten noususta aiheutuvaa palveluiden yksikköhintojen korotuspainetta.

Tulevaisuus

Jatkuvasti kasvavat turvallisuusuhat, kyberhyökkäykset, hybridivaikuttaminen yms. vaikuttavat myös TUVE-palveluiden turvallisuuden varmistamiseen ja jatkuvaan kehittämiseen. TUVE-asiakaskunnan ja muidenkin valtionhallinnon toimijoiden rahoitustilanteen arvioidaan kiristyvän edelleen. TUVE-asiakkaat edellyttävät, että palveluiden hinnoissa ei tapahdu merkittäviä yksikköhintojen nousuja lähitulevaisuudessa.

Miten Valtori pystyy kehittämään ja ylläpitämään korkean varautumisen ja tietoturvan tasoa siten, että palveluiden turvallisuuden tasosta ei tingitä

tai kehityskohteita ei siirretä tulevaisuuteen? Riittävän varautumis- ja turvallisuustason rahoitusvaje tulisi jotenkin ratkaista.

Toisaalta digitalisaation myötä tietotekniikan nopea kehittyminen ja uudenlaiset palvelut vievät toimintaympäristöjämme entistä avoimempaan suuntaan. Viranomaisten välinen sekä viranomaisten ja muiden toimijoiden välinen yhteistyö ja sähköinen tiedonvaihto lisääntyvät koko ajan. Myös turvallisuusviranomaisten odotetaan tuottavan kansalaisille entistä enemmän helppokäyttöisiä ja millä tahansa päätelaitteella käytettävissä olevia palveluita. Näistä johtuen TUVE-asiakkaiden tarve muiden kuin TUVE-palveluiden käyttämiseen kasvaa jatkossa. Samoin kasvaa tarve sellaisille tietoteknisille työvälineille, joilla pystytään käyttämään eri turvallisuus- ja suojaustasoilla olevia palveluita ja tietoja.

Valtorille nämä vaatimukset tuovat uusia haasteita. Kuinka kehittää ja tuottaa palveluita, jotka käyttävät sujuvasti eri tietoturva- ja suojaustasoilla olevia tietoja ja samalla täyttävät niiden käsittelylle asetetut lakisääteiset tai muut vaatimukset.

Uusien teknisten ratkaisujen kehittämisen rinnalla tulisi tarkastaa ja saattaa digiaikaan myös tähän asiakokonaisuuteen liittyvä lainsäädäntö ja muu normisto.