Dnro TRAFICOM/97701/03.03.01/2022
8.3.2022

Valtiovarainvaliokunnan liikennejaosto

kaisa.iso-sipila@eduskunta.fi

Liikenne- ja viestintäviraston asiantuntijalausunto valtiovarainvaliokunnan liikennejaostolle kyberturvallisuus-teemasta

Teema: Kyberturvallisuuden resursointi sekä organisaatiorakenteen toimivuus ja sen mahdolliset kehittämistarpeet

Liikenne- ja viestintävirasto kiittää Eduskunnan valtiovarainvaliokunnan liikennejaostoa asiantuntijalausuntopyynnöstä. Liikenne- ja viestintävirasto ja sen osana toimiva Kyberturvallisuuskeskus esittää lausunnossaan seuraavaa:

Kyberturvallisuusuhkat tulevat entistä konkreettisimmin esille samalla tavoin kuin fyysisessä maailmassa kohtaamamme turvallisuusuhkat. Yhteiskunnan eri palveluiden digitalisoituessa kyberturvallisuusuhat eivät ole enää erillisen virtuaalimaailman vitsaus, vaan jokapäiväiseen elämään vaikuttava uhka. Monesti nämä uhkakuvat voivat kohdistua myös yhteiskunnan toiminnan kannalta kriittisiin toimintoihin. Myös käynnissä oleva kansainvälinen tilanne on osoittanut sen, että Euroopassa on syytä varautua aikaisempaa tehokkaammin kyberhyökkäyksiin, -häiriöihin ja -vaikuttamiseen.

Turvallisuusympäristömme on pysyvästi muuttunut eikä kyberriskejä voida enää arvioida irrallaan muista turvallisuusriskeistä. Uusien riskien tunnistaminen ja niihin vastaaminen edellyttää poikkihallinnollista analyysiä. Turvallisuuden kokonaistilannekuvalla on kasvanut tarve huoltovarmuuskriittisillä sektoreilla ja valtiojohdossa. Kriisitilanteessa edellä mainittu tilannekuva ja sen tuottamiseksi sovitut selkeät roolit ja viranomaisyhteistyöprosessit ovat ensiarvoisen keskeisessä roolissa kriittisten toimialojen suojelemisessa, kyberturvallisuusriskien realisoitumisen ennakoinnissa ja näihin liittyvän päätöksentekokyvyn mahdollistamisessa. Jotta tarvittavaa tilannekuvaa voidaan tuottaa yhteiskunnan ja valtion kriittisten toimintojen tukemiseksi, turvallisuutta, ml. Kyberturvallisuutta, koskevan tilannekuvan muodostamiseen tulee osoittaa nykyistä enemmän resursseja. Viranomaisverkostossa tarvitaan myös entistä enemmän toimialakohtaista vahvaa erikoistumista ja osaamista, jotta arvoketjuihin liittyviä keskinäisriippuvuuksia voidaan analysoida, riskejä ennakoida ja mahdollistaa se, että digitaalisesta yhteiskunnasta ei tulisi entistä haavoittuvampi.

Tilannekuvan muodostuminen vaatii puolestaan viranomaisille ajantasaiset ja turvalliset työkalut turvaluokiteltuun viestintään viranomaisten välillä. Nykyisellään viranomaisten välinen ja kriittisen infrastruktuurin toimijoiden suuntaan tapahtuva yhteydenpito nojaa liiaksi siiloutuneisiin järjestelmiin tai sähköpostiin. Toimivien ja suojattujen tiedonvaihtokanavien puute voi johtaa siihen, että kansallinen päätöksentekojärjestelmä voi olla uhattuna kriisitilanteessa.

Kyberrikollisten ja muiden kybertoimijoiden kyvykkyydet ja erilaiset kyberturvallisuutta koskevat häiriöt sekä hyökkäykset kehittyvät alati kehittyvän teknologian ohella. Yhteiskunnalla tulee olla valmius vastata näihin uhkiin. Viime vuosina näkyvimpinä kyberturvallisuutta koskevina häiriöinä ovat Suomessa olleet kuntasektoriin kohdistuneet kyberhyökkäykset, yrityksiin kohdistuneet

kiristyshaittaohjelmat sekä Psykoterapiakeskus Vastaamoon kohdistunut laaja tietomurto. Eikä myöskään sovi unohtaa, että suomalainen päätöksenteko on ollut uhattuna, kun Suojelupoliisi esti eduskuntaan kohdistuneen kybervakoiluoperaation.

Yhteiskunnan kyberkyvykkyydet, luotettavat verkot ja digitaaliset palvelut sekä viranomaisten kyky palvella elinkeinoelämää ovat jatkossa korostetussa määrin kilpailutekijä Suomelle. Suomalaisen ja Suomessa toimivan teollisuuden kilpailukyvyn edellytyksenä ovat muun muassa EU:n kyberturvallisuusasetuksen mukaiset sertifiointi- ja akkreditointitehtävät. Muussa tapauksessa suomalaiset valmistajat ja arviointilaitokset joutuisivat hakemaan viranomaishyväksyntää toisen maan EU viranomaiselta. Sertifointien tulevasta kysynnästä ja kilpailutilanteesta johtuen on erittäin epätodennäköistä, että tarvittava hyväksyntä saataisiin toisen maan viranomaiselta.

Kyberympäristön muutoksista huolimatta Suomen panostukset kyberturvallisuuteen ovat viimeisen vuosikymmenen ajan jääneet merkittävästi jälkeen uhkien kehittymisestä. Suomen kyberturvallisuuden kehittämisen toimenpiteille asiantuntijoiden arvioimia ja määrittämiä rahoitustarpeita on leikattu, jonka seurauksena toimenpiteet toteutetaan vaillinaisesti ja jätetään osin kokonaan toteuttamatta. Kyberturvallisuuskeskuksella on lukuisia lakisääteisiä tehtäviä ja tällä hetkellä edes kaikkiin lakiperusteisiin tehtäviin ei ole myönnetty resursseja.

Toimintaympäristön muutoksesta johtuva Kyberturvallisuuskeskuksen jo olemassa olevien tehtävien kasvanut resursointitarve on huomioitava. Kyberturvallisuusongelmissa Kyberturvallisuuskeskuksen apua tarvitsevia kansalaisia, viranomaisia ja yhteiskunnan kriittisten toimialojen toimijoita on joka vuosi entistä enemmän. Kasvavaan tuen tarpeeseen vastaaminen edellyttää lisärahoitusta. Kyberturvallisuuskeskuksen toiminnan ja toimintojen kehittäminen välttämättömälle tasolle edellyttää useiden miljoonien eurojen lisärahoitusta. Mikäli nyt jäämme jälkeen Suomen kyberturvallisuuden perustan rakentamisessa, tulevat tulevaisuuden kustannukset kyberturvallisuuden toimenpiteiden laiminlyönnistä olemaan moninkertaisesti suhteessa nyt esitettyihin panostuksiin. Kyse ei ole ainoastaan taloudellisista menetyksistä, vaan myös esimerkiksi henkisistä kärsimyksistä, joista Vastaamo-tapauksen seuraukset ovat vain yksi esimerkki. Haluamme osaltamme huolehtia siitä, että Suomen kyberturvallisuutta koskeva varautuminen ja häiriönsietokyky ovat riittävällä tasolla suhteessa vallitseviin uhkiin ja riskeihin.

Kirsi Karlamaa

Pääjohtaja

Sauli Pahlman

Ylijohtaja