TRAFICOM
Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

LAUSUNTO

Eduskunnan puolustusvaliokunta
puv@eduskunta.fi

Päiväys/Datum
2.5.2022
Dnro/Dnr
TRAFICOM/189969/03.03.01/2022
Viite/Referens
Puolustusvaliokunta tiistai 03.05.2022 klo 10.00
lausuntopyyntö, VNS 1/2022 vp

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen lausunto koskien ajankohtaisselontekoa

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

Suomessa on syytä varautua aikaisempaa tehokkaammin kyberhyökkäyksiin ja kyberhäiriöihin.

Kyberturvallisuuskeskus pitää ajankohtaisselontekoa hyvänä kuvauksena turvallisuusympäristömme tilasta kyberturvallisuuden osalta. Kyberturvallisuusuhkat ja -häiriöt tulevat nykyään aiempaa konkreettisimmin esille - samalla tavoin kuin fyysisessä maailmassa kohtaamamme turvallisuusuhkat ja muut häiriöt. Yhteiskunnan eri palveluiden digitalisoituessa kyberturvallisuusuhat eivät ole enää erillisen virtuaalimaailman vitsaus, vaan organisaatioiden ja ihmisten 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 ja myös

Tilannekuva ja julkisen sektorin kyky varautua ovat yhä tärkeämpiä

Turvallisuusympäristömme on pysyvästi muuttunut eikä kyberriskejä voida enää arvioida irrallaan muista turvallisuusriskeistä. Uusien riskien tunnistaminen ja niihin vastaaminen edellyttää poikkihallinnollista seurantaa, analyysiä ja vastetta. Turvallisuuden kokonaistilannekuvalla on kasvanut tarve huoltovarmuuskriittisillä sektoreilla ja valtiojohdossa. Samoin kokonaistilannekuvan tarvetta on arvioitava aiempaa laajemmasta viitekehyksestä. Siihen liittyvät kyberturvallisuutta koskeva tilannekuva, kansallisesti kriittisten toimijoiden kybervarautuminen sekä myös julkisen sektorin kyky varautua kyberhäiriöihin. Kansainvälisellä ja kansallisella tiedonvaihdolla on keskeinen osa siinä, miten lyhyen ja pitkän aikavälin kyberriskeihin tulee varautua. Tässä tiedonvaihdossa Kyberturvallisuuskeskuksella on pitkät perinteet.

Siviiliyhteiskunnan rooli kriittisten toimialojen kyberturvallisuuden varmistamisessa on keskeinen

Kyberhyökkäykset ovat paitsi osa arkipäivää, niin myös erilaisia konflikteja. Suomen tulee suojata kansallinen päätöksenteko, turvallisuusviranomaisten toiminta ja kriittisten palveluiden sekä kriittisen infrastruktuurin toimivuus niin kyberhyökkäyksiä kuin myös muita kyberturvallisuuden vaarantavia uhkia vastaan.

Varautumisella on Suomessa pitkät perinteet, mutta panostuksia vaaditaan lisää eikä ote saa herpaantua. Poikkeusoloissakin siviiliyhteiskunnan rooli kriittisten toimialojen kyberturvallisuuden varmistamisessa on keskeinen. Kyberturvallisuuskeskuksella on pitkät perinteet teleyritysten kanssa tehtävästä varautumis- ja tietoturvatyöstä. Kyberturvallisuuskeskus tukee myös muita toimialoja kyberturvallisuuden edistämisessä.

Suomalainen päätöksentekokyky tulee turvata

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 sekä yrityksiin kohdistuneet kiristyshaittaohjelmat ja tietovuodot. Eikä myöskään sovi unohtaa, että suomalainen päätöksenteko on ollut uhattuna, kun Suojelupoliisi esti eduskuntaan kohdistuneen kybervakoiluoperaation.

Keskeisiä kehittämistoimia turvallisuusympäristön muutokseen vastaamiseksi on jo tunnistettu. Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamisesta kriittisillä toimialoilla tulee parantamaan tilannetta muun muassa kriittisten toimialojen osalta, mikäli periaatepäätöksen toteuttamiseen sitoudutaan riittävällä rahoituksella jatkossakin. Samoin oleva EU:n verkko- ja tietoturvadirektiivin päivitys (ns. NISD2) tulee asettamaan entistä tiukempia varautumis- ja viranomaisvalvontavaatimuksia keskeisille toimialoille. Tulevaisuudessa yhä useammat yhteiskunnan kriittiset sektorit ovat velvoitettuja huolehtimaan kyberturvallisuudesta nykyistä vahvemmin. Muun muassa näiden toimien toteutus ja toimien osoittaminen kokonaan uusille sektoreille ovat keskeisessä roolissa siviiliyhteiskunnan toimintojen kybersuojauksen parantamisessa.

Kyberturvallisuuskeskus tuottaa kansallista yhdistettyä kyberturvallisuuden tilannekuvaa

Kriisitilanteessa kyberturvallisuuden tilannekuva ja viranomaisyhteistyöprosessit ovat ensiarvoisen keskeisessä roolissa kriittisten toimialojen suojelemisessa, kyberturvallisuusriskien realisoitumisen ennakoinnissa ja näihin liittyvän päätöksentekokyvyn mahdollistamisessa.

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. Samoin kriittinen infrastruktuuri ja toimialojen kriittisyys on määriteltävä yhteiskunnassa entistä tarkemmin.

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.

Suomen oltava uskottava kybervarautumisessa

Yhteiskunnan kyberkyvykkyydet, luotettavat verkot ja digitaaliset palvelut sekä

viranomaisten kyky palvella elinkeinoelämää ovat jatkossa korostetussa määrin kilpailutekijä Suomelle. Mikäli Suomi ei kykene ylläpitämään uskottavaa kybervarautumistasoa, Suomen maariski voidaan katsoa liian korkeaksi kansainvälisiä investointeja suunniteltaessa. Suomalaisen ja Suomessa toimivan kyberteollisuuden kilpailukyvyn edellytyksenä ovat muun muassa EU:n kyberturvallisuusasetuksen mukaiset sertifiointi- ja akkreditointitehtävät.

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 viime vuosina leikattu, jonka seurauksena toimenpiteet toteutetaan vaillinaisesti ja jätetään osin kokonaan toteuttamatta. Myös panostukset kyberosaamisen kehittämiseen Suomessa ovat arviomme mukaan olleet puutteellisia.

Kyberturvallisuuskeskuksen jo olemassa olevien tehtävien kasvanut resursointitarve on huomioitava pysyvästi jatkossa

Toimintaympäristön muutoksesta johtuva Kyberturvallisuuskeskuksen jo olemassa olevien tehtävien kasvanut resursointitarve on huomioitava pysyvästi jatkossa. Kyberturvallisuusongelmissa ja vallitsevassa maailman tilanteessa Kyberturvallisuuskeskuksen apua tai palveluita tarvitsevia kansalaisia, viranomaisia ja yhteiskunnan kriittisten toimialojen toimijoita on joka vuosi entistä enemmän. Mikäli 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