TRAFICOM
Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

LAUSUNTO

Eduskunnan talousvaliokunta
TaV@eduskunta.fi

Päiväys/Datum
27.4.2022
Dnro/Dnr
TRAFICOM/182035/03.03.01/2022
Viite/Referens
talousvaliokunta torstai 28.04.2022 klo 12.00 VNS 1/2022 vp

Lausunto Eduskunnan talousvaliokunnalle koskien ajankohtaisselontekoa turvallisuusympäristön muutoksesta

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

Kyberturvallisuuskeskus pitää ajankohtaisselontekoa hyvänä kuvauksena turvallisuusympäristömme tilasta kyberturvallisuuden osalta. Kyberturvallisuusuhkat tulevat nykyään aiempaa konkreettisimmin esille - samalla tavoin kuin fyysisessä maailmassa kohtaamamme turvallisuusuhkat. 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 Suomessa on syytä varautua aikaisempaa tehokkaammin kyberhyökkäyksiin ja kyberhäiriöihin.

Kyberhyökkäykset ovat osa arkipäivää ja 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.

Turvallisuusympäristömme on pysyvästi muuttunut eikä kyberriskejä voida enää arvioida irrallaan muista turvallisuusriskeistä. Toimintaketjujen hallintaan, tavaraliikenteen toimintavarmuuteen ja kyberturvallisuuteen on syytä kiinnittää entistä suurempaa huomioita. Suomalainen yhteiskunta on riippuvainen viestintäverkoista (ml. kansainväliset tietoliikenneyhteydet), tietojärjestelmistä ja digitaalisista palveluista sekä näitä tarjoavista ja näissä käytettäviä laitteita tarjoavista toimijoista. 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.

Traficom korostaakin tarvetta määritellä Suomen kriittinen infrastruktuuri siten, että Suomessa muodostuu yhteinen näkemys yhteiskunnan kannalta kriittisestä infrastruktuurista ja sen merkityksestä julkishallinnon toimintojen ja palvelujen kuin yhteiskunnan elintärkeiden toimintojen kannalta. Kriittisen infrastruktuurin määrittely on varautumisen kannalta ensiarvoisen tärkeää, jotta toimenpiteet voidaan useita toimialoja kattavissa laajoissa häiriötilanteissa ja kriisitilanteessa kohdentaa oikein ja tehokkaasti (esim. polttoainejakelu). Kriittisen infrastruktuurin määrittelyssä tulee ottaa huomioon, että vahvasti verkottuneessa yhteiskunnassa kyberturvallisuusuhkat voivat keskinäisriippuvuuksien johdosta aiheuttaa entistä suurempia vahinkoja. Yhteiskunta on yhä riippuvaisempi digitaalisesta toimintaympäristöstä. Tämän vuoksi kyberturvallisuuden tulee olla sisäänrakennettuna kaikessa toiminnassa, prosesseissa ja järjestelmissä, joihin kohdistuu uhkatekijöitä. Kokonaisvaltaisesti yritysten kyberosaamisen tulee olla riittävää, jotta viranomaiset voivat auttaa kyberriskien realisoituessa.

Kyberturvallisuuskeskus tuottaa kansallista kyberturvallisuuden tilannekuvaa. Kriisitilanteessa kyberturvallisuuden tilannekuva 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, tulee kyberturvallisuutta koskevan tilannekuvan muodostamiseen osoittaa nykyistä enemmän resursseja.

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.

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 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. Myös panostukset kyberosaamisen kehittämiseen Suomessa ovat puutteellisia.

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.

Sauli Pahlman
ylijohtaja

Johanna Erkkilä
johtaja

Tämä asiakirja on allekirjoitettu sähköisesti. Liikenne- ja viestintävirasto (Traficom) 27.4.2022. Allekirjoituksen oikeellisuuden voi todentaa sähköisiä allekirjoituksia tukevalla lukijaohjelmalla tai Traficomin kirjaamosta.