Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

LAUSUNTO

Eduskunnan hallintovaliokunta
HaV@eduskunta.fi

Päiväys/Datum
26.4.2022
Dnro/Dnr
TRAFICOM/179066/03.03.01/2022
Viite/Referens
27.4.2022 klo 11.15 VNS 1/2022 vp

Liikenne- ja viestintäviraston lausunto koskien ajantasaisselontekoa turvallisuusympäristön muutoksesta

Liikenne- ja viestintävirasto, jäljempänä myös Traficom, kiittää mahdollisuudesta lausua asiassa. Traficom katsoo, että selonteko antaa hyvän ja laaja-alaisen kuvan nykyisestä turvallisuusympäristöstä sekä toimista kyberturvallisuuden parantamiseksi Suomessa. Virasto haluaa lisäksi korostaa myös liikenteen ja logistiikan, erityisesti Itämeren tavaraliikenteen roolia Suomen huoltovarmuudessa. Kyberturvallisuusuhkat ovat globaaleja ylittäen maiden rajat ja siten myös ulko- ja turvallisuuspoliittisen toimintaympäristön muuttuminen heijastuu myös kyberympäristöön Suomessa.

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. Liikenne- ja viestintävirastolla ja teleyrityksillä on pitkät perinteet toimivasta yhteistyöstä varautumisen ja tietoturvallisuuden saralla. Kyberturvallisuuskeskus tukee myös muiden kriittisten toimialojen kyberturvallisuustyötä.

Varautuminen kyberhyökkäyksiä ja muita kyberturvallisuuden vaarantavia uhkia vastaan vaatii pitkäjänteistä kehittämistä ja resurssien määrätietoista kohdistamista kehittämistoimenpiteisiin. Monia keskeisiä kehittämistoimenpiteitä onkin jo suunniteltu ja käynnistetty. Muutokset ulko- ja turvallisuuspoliittisessa turvallisuusympäristössä antavat aiheen nopeuttaa näitä kehittämistoimenpiteitä ja tehdä hyvin kohdennettuja kyberturvallisuutta parantavia toimenpiteitä nopeutetulla aikataululla. Suurelta osin tarvittavat kehitystoimenpiteet ovat jo kartoitettu eri kyberturvallisuutta käsittelevissä valtioneuvoston periaatepäätöksissä, kuten periaatepäätöksessä kyberturvallisuuden kehittämisohjelmasta ja periaatepäätöksessä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. Monelta osin nämä selonteossakin mainitut kehitystoimenpiteet ja -hankkeet ovat myös käynnissä. Kaikilta osin näitä toimenpiteitä ei kuitenkaan ole saatu käynnistettyä ja toimeenpantua johtuen riittämättömistä resursseista toteuttaa niitä. Traficom pitääkin ensiarvoisen tärkeänä, että selonteossakin esille tuodut toimet kyberturvallisuuden parantamiseksi toteutetaan.

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. 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.

Yhteiskunnan kriittisiä toimintoja turvaavan osaamisen ja resursoinnin pitäisi mahdollistaa myös vastaaminen yllättäviin kriisitilanteisiin, joissa resurssien tarve on kasvanut. Yhteistyö kansallisesti ja kansainvälisesti on keskeisessä roolissa varautumisessa kyberturvallisuusuhkiin ja kyberturvallisuuden varmistamisessa. Muuttunut ulko- ja turvallisuuspoliittinen ympäristö vaatii yhteistyön tiivistämistä ja tätä yhteistyötä muun muassa Traficom ja Traficomiin sijoitettu Kyberturvallisuuskeskus on rakentanut jo kaksi vuosikymmentä. Yhteistyö on keskeisessä roolissa kyberturvallisuuden yhdistetyn tilannekuvan luomisessa ja tiedon jakamisessa. Saadulla tiedolla voidaan parhaimmillaan ennaltaehkäistä kyberhyökkäys tai rajoittaa sen vaikutuksia Suomeen. On myös tärkeää, että Suomi ja EU vaikuttavat kansainvälisten kybernormien ja standardien kehittämiseen sekä riittävän omavaraisuuden luomiseen kyberturvallisuuden kannalta keskeisten palvelujen ja tuotteiden osalta. Yhteistyö ja kansainvälinen vaikuttaminen vaativat lisäresursseja niin Suomelta kuin EU:lta.

Lisäksi Liikenne- ja viestintävirasto haluaa kiinnittää valiokunnan huomion liikennepalveluiden ja - verkkojen toiminnan varmistamisen merkitykseen. Yhteiskunnan toiminnan kannalta kriittisiä liikennepalveluita ovat muun muassa väestön toimeentulolle ja elinkeinoelämälle kriittiset kuljetukset, työssäkäyntiliikenne, sosiaali- ja terveyspalvelujen kuljetukset, koulukuljetukset sekä yhteiskunnan tuottamat kuljetuspalvelut. Kriittisiä liikenneverkkoja ovat muun muassa liikennejärjestelmän keskeiset solmukohdat, kuten satamat, terminaalit, lentokentät sekä kriittinen väylästö. Palveluiden ja verkkojen toiminnan häiriintymisellä tai estymisellä olisi välitön ja erittäin merkittävä vaikutus koko yhteiskunnan toimintaan. Kriittisten liikennepalvelujen käytettävyys ja saatavuus varmistetaan häiriötilanteissa ja myös poikkeusoloissa riskinarvioinnilla, etukäteisvalmisteluin ja varautumisella. Varautumistoimintaa riittävä resursointi on keskeistä.

Sauli Pahlman
ylijohtaja

Tämä asiakirja on allekirjoitettu sähköisesti. Liikenne- ja viestintävirasto (Traficom) 26.4.2022. Allekirjoituksen oikeellisuuden voi todentaa sähköisiä allekirjoituksia tukevalla lukijaohjelmalla tai Traficomin kirjaamosta.