26.4.2022

Eduskunta
Valtiovarainvaliokunnan hallinto- ja turvallisuusjaosto

sanna.turpeinen@eduskunta.fi

Asiantuntijalausuntopyyntö 21.4.2023 – VNS 1/2022 vp

Ajankohtaisselonteko turvallisuusympäristön muutoksesta - kyberturvallisuus

Liikenne- ja viestintäministeriö kiittää valtiovarainvaliokunnan hallinto- ja turvallisuusjaostoa asiantuntijalausuntopyynnöstä. Liikenne- ja viestintäministeriö esittää lausunnossaan seuraavaa:

Kybertoimintaympäristön muutos

Kybertoimintaympäristö on muuttunut pysyvästi. Muutokseen ovat vaikuttaneet muuttunut geopoliittinen tilanne ja koronapandemia, jonka seurauksena koko digitaalinen toimintaympäristö ajautui murrokseen uusien teknologioiden käytön ja teknologisen kehityksen myötä.

Tapahtuneiden muutosten takia kybertoimintaympäristön uhkakenttä on laajentunut merkittävästi. On oletettavaa, että valtiollinen toiminta tulee pysyväksi toimintamuodoksi eri yhteiskuntien toimintakykyyn vaikuttamisessa. Digitaalinen murros tuo ja on jo tuonut käyttöön uusia teknologioita, jotka entisestään monimutkaistavat kybertoimintaympäristöä.

Kyberuhkiin varautuminen on noussut tärkeäksi osaksi Suomen ulko-, turvallisuus- ja puolustuspolitiikkaa. Kybertoiminta on jo ollut yksi voimankäytön muoto, jota on käytetty yhtenä hybridivaikuttamisen välineenä myös normaalioloissa, jolloin erityyppisten konfliktien rajapinta ja sitä kautta siviili- ja sotilaallisten uhkien ero on hämärtynyt.

Kyberhäiriötilanteita aiheutuu ja aiheutetaan monista syistä. Motiivina voi olla valtiollinen intressi, taloudellinen rikoshyöty, vahingonteko tai haavoittuvuuksien paljastaminen. Yritykset ja julkinen sektori joutuvat varautumaan näihin kaikkiin. Siviiliverkkoon kohdistuva hyökkäys voi lamaannuttaa yhteiskuntaa laajasti oli taustalla sotilaallinen tai muu motiivi.

Selonteko antaa ajantasaisen ja kattavan kokonaiskuvan toimintaympäristön muutoksesta sekä muuttuneessa toimintaympäristössä huomioon otettavista seikoista. Liikenne- ja viestintäministeriö on osallistunut aktiivisesti selonteon kyberturvallisuusosion laatimiseen.

Kyberturvallisuuden varautuminen

Kyberuhilta suojautuminen on osa kokonaisturvallisuutta, joka koskettaa laaja-alaisesti valtionhallintoa ja kaikkia hallinnonaloja. Selonteko antaa hyvän kokonaiskuvan kyberturvallisuuden varautumisesta ja toimijoista Suomessa.

Ministeriö korostaa, että Suomessa tieto- ja kyberturvallisuuden varautumisella on pitkät ja toimivat perinteet. Viranomaisten kesken työnjako on selvä, ja perustuu lainsäädäntöön. Operatiivista yhteistyötä tehdään päivittäisellä tasolla ja viranomaisilla on hyvin organisoidut koordinaatioryhmät.

Kyberturvallisuuden kehittämistä ovat ohjanneet kyberturvallisuusstrategiat vuosilta 2013 ja 2019 sekä vuonna 2021 julkaistu kyberturvallisuuden kehittämisohjelma, jossa vahvistetaan Suomen kyberkyvykkyyksiä ja osaamista rakennetaan julkisten ja yksityisten toimijoiden ekosysteemiä.

Aktiivisen kyberdiplomatian avulla pyritään vahvistamaan monitoimijapohjaista yhteistyötä ja yhteisiä pelisääntöjä sekä Suomen omaa kykyä vastata Suomeen kohdistuviin kybertoimiin.

Selonteossa todetusti kyberturvallisuusympäristön muutos korostaa tarvetta valtioneuvostotason tiiviille koordinaatiolle ja ajantasaiselle tilannekuvalle. Kybersuojauksesta vastaavien ministeriöiden ja kyberturvallisuusviranomaisten sisäistä ja keskinäistä yhteistyötä onkin tiivistetty entisestään. Kyberturvallisuus lisättiin myös digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministerityöryhmän tehtäviin maaliskuussa 2022.

Liikenne- ja viestintäministeriöllä on kyberturvallisuutta koordinoiva rooli. Kyberturvallisuuskeskus tukee yhteiskunnan kyberturvallisuuden varmistamista ja tuottaa kyberturvallisuuden tilannekuvaa. Liikenne- ja viestintäministeriöön sijoitettu valtioneuvoston kyberturvallisuusjohtaja huolehtii siitä, että kybertoimintaympäristöön kohdistuvien häiriötilanteiden johtamista ja yhteistyötä operatiivisella tasolla kehitetään kyberturvallisuustoimijoiden kesken. Kyberturvallisuushäiriötilanteessa kyberturvallisuusjohtaja yhdessä muiden toimijoiden kanssa tuottaa tilannekuvaa valtionjohdolle ja koordinoi tilannetta. Lisäksi liikenne- ja viestintäministeriö koordinoi tilannetta muiden ministeriöiden kesken horisontaalisesti.

Parhaillaan sisäministeriön ja puolustusministeriön johdolla tarkastellaan viranomaisten toimintaedellytyksiä kyberturvallisuuden varmistamisessa, kyberrikostorjunnassa ja kyberpuolustuksessa yhteistyössä eri toimijoiden kanssa.

Valtioneuvoston periaatepäätöksessä tietoturvan ja tietosuojan parantamisesta kriittisillä toimialoilla (2021) on linjattu useita tietoturvaa ja tietosuojaa parantavia toimenpiteitä. Osana periaatepäätöksen toimeenpanoa liikenne- ja viestintäministeriön johdolla selvitetään

viranomaisten tiedonvaihdon parantamista eri kyberhäiriötilanteissa ja siihen tarvittavia lainsäädäntömuutoksia.

Myös käynnissä oleva EU:n verkko- ja tietoturvadirektiivin päivittäminen ja laajentaminen vahvistavat kriittisten toimijoiden, kuten sähkö- ja vesihuollon toimijoiden, kyberturvallisuutta.

Julkisen talouden suunnitelmaa koskevissa neuvotteluissa lisättiin myös merkittävästi rahoitusta kyberturvallisuuden varautumisen parantamiseen. Kyberturvallisuuteen tulee jatkossakin ohjata riittävästi panostuksia niin, ettei kyberturvallisuuden korjausvelkaa pääse syntymään ja että kybersuojaus on ajantasaista. Ministeriö yhtyy myös selonteon huomioon julkisen hallinnon eri sektoreiden ja hallinnon tasojen kyvykkyyksien ja osaamisen varmistamisen tärkeydestä sekä korostaa tietojärjestelmien tietoturvallisuuden ja tietosuojan varmistamisen roolia osana kyberturvallisuutta.

Kriittinen verkkoinfrastruktuuri

Suomessa yritykset omistavat suurelta osin kriittisen infrastruktuurin ja hallinnoivat valtavaa tietomassaa. Yritysten rooli Suomen kybertoimintaympäristön turvaamisessa on olennainen. Datatalouden perusteita määriteltäessä on jo alusta asti kiinnitettävä huomiota tietoturvallisuuteen ja datan eheyden, luotettavuuden ja saatavuuden varmistamiseen. Yhä useampi yritys on myös teknologiayritys ja yhä useampi kuluttajatuote on kytketty internetiin.

Kyberturvallisuusympäristön muutos korostaa toimitusketjujen hallinnan merkityksen lisääntymistä myös erilaisten ohjelmistojen ja digitaalisten palveluiden osalta. On tärkeää lisätä ja parantaa kaikkien yritysten, organisaatioiden kuin myös kansalaisten digi- ja kyberturvallisuustaitoja sekä tehdä tiivistä yhteistyötä julkisen ja yksityisen sektorin toimijoiden kesken. Nämä seikat on tuotu hyvin ilmi selonteossa.

Suomi on edelläkävijä 5G-teknologiassa ja teollisen internetin sovellusten kehittäjänä. Verkkoteknologiassa toimitusketjujen ja laitteiden luotettavuuden ja turvallisuuden on oltava korkealla tasolla.

Jo entuudestaan vahvaa viestintäverkkojen turvallisuutta koskevaa sääntelyä täydennettiin vuonna 2021. Lähtökohtana on, että viestintäverkon kriittisissä osissa ei saa käyttää laitteita, jotka voivat vaarantaa kansallisen turvallisuuden tai maanpuolustuksen. Nykyinen tilanne korostaa ajantasaista osaamista ja kyvykkyyksiä uusimmista verkkoteknologioista ja niihin liittyviin uhkiin varautumisesta, sekä lainsäädäntötarpeiden jatkuvaa arvioimista. Myös kaapeliyhteydet ja niiden turvaaminen ovat osa kriittistä infrastruktuuria.

Satelliittipaikannusjärjestelmien tuottamasta sijainti- ja aikatiedosta on tullut keskeinen osa toimivaa yhteiskuntaa ja sen kriittisiä palveluita. Käytettävyyteen liittyvät häiriöt voivat vaikuttaa nopeasti ja laajasti yhteiskunnan perustoimintoihin. Maaliskuussa 2022 Suomessa havaittiin GPS-häiriöitä ja näillä häiriöillä oli vaikutuksia siviililentoihin, mutta

vaaratilanteilta vältyttiin. EU:n Galileo-satelliittipaikannusjärjestelmä ja sen yhteiskunnan kriittisille toimijoille tarkoitettu julkisesti säännelty palvelu on EU:n yksi merkittävimpiä kyberturvallisuushankkeita.

EU- ja kansainvälinen yhteistyö

Ministeriö yhtyy selonteossa esitettyyn näkemykseen, että kansainvälinen yhteistyö on keskeistä Suomen kyberturvallisuudelle ja -puolustukselle. Yhteistyötä tehdään tiiviisti myös ministeriön hallinnonalalla.

Rauli Paananen
Kyberturvallisuusjohtaja
Liikenne- ja viestintäministeriö

Nina Hyvärinen
Johtava asiantuntija
Tieto-osasto