Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

Tulevaisuusvaliokunta
tuV@eduskunta.fi

Päiväys/Datum
29.9.2021
Dnro/Dnr
TRAFICOM/458764/03.03.01/2021
Viite/Referens
Asiantuntijapyyntö tulevaisuusvaliokunta perjantai 01.10.2021 klo 10.00 / VNS 4/2021 vp Asia: Valtioneuvoston selonteko sisäisestä turvallisuudesta

Liikenne- ja viestintäviraston lausunto valtioneuvoston sisäisen turvallisuuden selonteosta

Liikenne- ja viestintävirasto Traficom kiittää mahdollisuudesta lausua asiassa. Traficom pitää sisäisen turvallisuuden selontekoa (myöhemmin "selonteko") hyvin valmisteltuna ja jakaa suurelta osin siinä esitetyt johtopäätökset. Traficom pitää hyvänä, että selonteossa on huomioitu myös globaalit haasteet ja niiden vaikutukset sisäiseen turvallisuuteen, sillä nykyinen digitaalinen yhteiskunta ja siihen kohdistuvat turvallisuusuhkat eivät noudata valtioiden rajoja.

Traficom pitää tärkeänä, että sisäisen turvallisuuden selontekoa on valmisteltu aikaisempaa laaja-alaisemmin ja että valmistelussa on otettu huomioon myös ulko- ja turvallisuuspoliittinen selonteko sekä puolustusselonteko. Kyberturvallisuuden alalla sisäinen ja ulkoinen turvallisuus nivoutuvat voimakkaasti yhteen, minkä vuoksi kyberturvallisuushaasteisiin vastaaminen edellyttää toimeenpanovaiheessa yhä kokonaisvaltaista hallinnonalojen rajat ylittävää tarkastelua.

Kyberturvallisuus on olennainen osa sisäistä turvallisuutta

Selonteossa viranomaistoiminnassa tunnistettutuissa kehittämiskohteissa on tärkeää ottaa huomioon valtioneuvoston periaatepäätös kyberturvallisuuden kehittämisohjelmasta. Kyberturvallisuus on poikkihallinnollinen ja koko yhteiskuntaa läpileikkaava kivijalka, ja näkemyksemme mukaan sitä ei ole tällä hetkellä riittävällä tavalla huomioitu. Kyberturvallisuuden kehittämisohjelma on laadittu laaja-alaisessa yhteistyössä eri viranomaisten ja yritysten kesken ja sen tavoitteena on muun muassa parantaa digitaalisen yhteiskunnan kestävyyttä sekä sietokykyä kybertoimintaympäristön eri ilmiöitä vastaan. Kyberturvallisuuden kehittämisohjelmassa on määritelty tarvittavat toimenpiteet Suomen kyberturvallisuuden kehittämiseksi. Nämä toimenpiteet vaikuttavat olennaisella tavalla myös sisäisen turvallisuuden varmistamiseen, kehittämiseen ja yhteiskunnan kriisinsietokykyyn. Kyberturvallisuuden kehittämisohjelman toimenpiteille ei kuitenkaan ole osoitettu riittävää rahoitusta, jolloin vaarana on sisäisen turvallisuuden osalta Suomen kyberturvallisuuden tilan heikentyminen ja puutteellinen kyky vastata kyberturvallisuushaasteisiin.

Kyberrikollisten ja valtiollisten toimijoiden kyberkyvykkyydet kehittyvät uusien teknologioiden antamien mahdollisuuksien avulla ja lisäksi kyberhyökkäyksiä on voinut jo kauan ostaa palveluna avoimesta internetistä. Viime vuosina näkyvimpänä suomalaisena kyberherätyksenä olivat kuntasektoriimme kohdistuneet kyberhyökkäykset. Ne osoittivat yhteiskuntamme haavoittuvuuden ja haittasivat

muun muassa kansalaisten peruspalveluita ja arkea. Suomeen on myös rantautunut uusi merkittävä ilmiö, jossa rikolliset havittelevat suuria lunnaita kiristyshaittaohjelmahyökkäyksillä, joiden kohteina ovat suuret yritykset. Hyökkäykset ovat aiheuttaneet yrityksille vakavia toiminnan häiriöitä ja jopa toiminnan keskeytyksiä sekä mittavia taloudellisia tappioita. Tapaus Vastaamo oli Suomen historian yksi merkittävimmistä tietomurroista. Varastamillaan tiedoilla hyökkääjä kiristi niin Vastaamoa kuin kymmeniä tuhansia sen palveluita käyttäneitä kansalaisia. Myös suomalainen päätöksenteko on ollut uhattuna, kun Suojelupoliisi esti eduskuntaan kohdistuneen kybervakoiluoperaation, jossa yritettiin tunkeutua eduskunnan tietojärjestelmiin. Tämän lisäksi maailmalla ovat yleistyneet kyberturvallisuusuhkien vaikutukset suoraan fyysiseen maailmaan. Hakkerit lamauttivat Ruotsin johtavan kauppaketju Coopin kiristyshaittaohjelman avulla, ja uhreiksi joutuivat tuhannet yritykset ainakin 17 eri maassa.

Myös Traficomin Kyberturvallisuuskeskukseen tulevat ilmoitukset tietoturvaloukkauksista ovat kuluneen kahden vuoden aikana kolminkertaistuneet.

Kansallisen turvallisuuden uhkiin varautumisen ja vastaamisen toimenpiteissä tulisi ottaa huomioon myös valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla ja siinä esitetyt toimenpiteet. Sisäisen turvallisuuden varmistamiseksi tulisi kehittää kansallista osaamista, yhteistyötä ja kyvykkyyksiä.

Kriittinen infrastruktuuri tulee määritellä pikaisesti

Traficom pitää selonteossa esitettyjä toimenpiteitä kansallisen turvallisuuden uhkien tunnistamiseksi ja torjumiseksi perusteltuina ja erittäin tarpeellisina. Tärkeimpänä toimenpiteenä Traficom korostaa kriittisen infrastrultuurin määrittelyä siten, että Suomessa on yhteinen näkemys kriittisestä infrastruktuurista ja sen merkityksestä valtiohallinnon toimintojen ja palveluiden sekä 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.

Yhteistyö tulee määritellä perinteistä tapaa laajemmin

Selonteko huomioi hyvin tarpeen (turvallisuus-)viranomaisten väliselle yhteistyölle ja jo tehdyn työn sisäisen turvallisuuden varmistamiseksi. Asiaa on kuitenkin käsitelty varsin perinteisestä turvallisuusviranomaisen määritelmän näkökulmasta. Kyberturvallisuus koskettaa kaikkien hallinnonalojen viranomaistoimintaa ja on tärkeää, että selonteossa nousisi esiin tarve varautua digitaalisen yhteiskunnan kyberturvallisuusuhkiin turvallisuus- ja siviiliviranomaisten välisellä yhteistyöllä. Selonteossa ja sisäisestä turvallisuudesta käytävässä keskustelussa yleisemminkin tulisi katsoa asiaa laaja-alaisemmin myös perinteisten näkökulmien ulkopuolelta, missä muun muassa Traficomin Kyberturvallisuuskeskus kansallisena tietoturvallisuusviranomaisena on olennainen toimija perinteisten

turvallisuusviranomaisten rinnalla. Kyberturvallisuuskeskus palvelee kaikkia kriittisiä sektoreita ja tekee aktiivisesti yhteistyötä niitä ohjaavien ja valvovien viranomaisten kanssa mukaan lukien turvallisuusviranomaisten, kuten poliisin, kanssa tukien niitä kyberrikosten ennaltaehkäisemisessä ja selvittämisessä.
Kyberturvallisuuskeskuksella on myös keskeinen rooli kyberturvallisuuden kokonaistilannekuvan ylläpitämisessä ja jakamisessa ja vakavien tai laajavaikutteisten kyberuhkien ennaltaehkäisyssä. Hyvä kyberturvallisuuden taso voidaan saavuttaa vain, jos jokainen digitaaliseen yhteiskuntaan kytkeytynyt toimija kantaa oman vastuunsa kyberturvallisuuden toteutumisesta.

Toimintaympäristön muutosta analysoitaessa on tärkeää huomioida myös selonteon ulkopuolelle tällä hetkellä jäävistä asioista avaruus- ja satelliittiteknologia, suurvaltakilpailu, ulkomaiset toimijat ja jälkimmäiseen liittyen erityisesti viime vuosin korostunut trendi, missä kyberturvallisuuden kannalta keskeisiä toimijoita myydään ulkomaiseen omistukseen. Teknologisen kehityksen (mm. tekoäly, kvanttilaskenta, automaatio, toimialojen digitalisoituminen) ja sekä kyberilmiöiden seuraaminen ja ennakointi on keskeistä tulevaisuuden kyberuhkiin varautumisessa.

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