Ulkoministeriö

Lausunto

30.12.2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Ulkoministeriö kiittää liikenne- ja viestintäministeriötä laajalti kokoavasta työstä, jonka pohjalta työryhmän väliraportti on laadittu.

Ulkoministeriö on osallistunut työryhmän työhön ja tuonut työskentelyn kuluessa esiin, että vaikka työryhmän työssä on keskitytty tietoturvan ja tietosuojan parantamiseen sääntelyn keinoin, vähintään yhtä tärkeää on huomioida se laaja kansallinen ja kansainvälinen toimintaympäristö, jossa haavoittuvuuksia pyritään vähentämään. Kyberuhat eivät tunne rajoja ja toisaalta pelkkä tekninen järjestelmäturvallisuuteen ja sääntelyyn keskittyvä työ vastaa vain osittain tieto- ja kyberturvallisuuden vahvistamisen tarpeisiin. Teknisten ja sääntelyulottuvuuksien ohella on tarkasteltava toimintoja ja prosesseja, jotka mahdollistavat toimintaympäristön ennakoivan ymmärtämisen ja tämän ymmärryksen heijastamisen tietoturvan vahvistamiseen tarvittaviin toimiin. On myös huomattava, että ko. toiminnot ja prosessit eivät ole yksinomaan organisaatioiden sisäisiä, vaan ylittävät usein läpileikkaavina organisaatioiden väliset rajat.

Vihamielinen kybertoiminta on lisääntynyt merkittävästi viime vuosina. COVID19-pandemia on osaltaan korostanut tätä kehitystä, kun työnteko ja tiedonkulku on aiempaa merkittävämmin siirtynyt sähköisiin tietoverkkoihin. Tämän vuoksi vieraiden valtioiden tiedustelu- ja vaikuttamistoiminnassakin on painottunut aiempaa enemmän henkilötiedustelun sijaan verkkotiedustelu sekä kohdennettu vaikuttaminen. Niin yksityiset kuin valtiotoimijat etsivät jatkuvasti haavoittuvuuksia, joita voivat hyödyntää joko rahallisen hyödyn saamiseksi (erit. yksityiset toimijat) tai pahantahtoiseen vaikuttamiseen, ml. hybridivaikuttamiseen (erit. valtiotoimijat ja/tai bulvaanit). Valtiotason tai valtioihin kytköksissä olevat toimijat ovat viime vuosina toteuttaneet lukuisia vihamielisiä kyberiskuja, joiden ilmeisenä tavoitteena on ollut hyödyntää haavoittuvuuksia ja heikentää tai lamauttaa toisten valtioiden keskeisten instituutioiden tai kriittisen infrastruktuurin toimintaa tai tavoitella rahallista hyötyä. Ei ole poissuljettua, että tällainen kyberisku voisi kohdistua

myös Suomen valtiollisiin instituutioihin. Vihamieliseen kybertoimintaan on varauduttava ja valmistauduttava sekä kansallisin toimin että toimimalla aktiivisesti kansainvälisillä foorumeilla.

Kyberiskujen kynnyksen nostamiseksi EU on mm. kehittänyt kyberpakotejärjestelmän, jonka puitteissa rajoittavien toimien piiriin on heinäkuusta 2020 lähtien listattu vihamielisten kyberhyökkäysten toteuttajia Venäjältä, Kiinasta ja Pohjois-Koreasta. Suomen turvallisuuden kannalta on tärkeää kehittää EU-tason välineitä, joilla kyberiskuihin ja tietoturvallisuuteen kytkeytyviä haavoittuvuuksia hyödyntävään vihamieliseen toimintaan voidaan puuttua.

Ulkoministeriö pitää kansallisten tietoturvaa ja –suojaa vahvistavien toimien lisäksi keskeisenä kansainvälistä yhteistyötä sellaisten politiikkojen ja toimien muodostamiseksi, jotka ennaltaehkäisevät tietoturvahaavoittuvuuksia kriittisillä sektoreilla. Tämä näkyy mm. EU:n kyberturvallisuus- ja diplomatian välineiden kehittämisessä ja hyödyntämisessä kansallisella tasolla sekä hybridiuhkien torjumista koskevassa yhteistyössä ja resilienssin vahvistamissa. Resurssien turvaaminen kansainväliseen vaikuttamistyöhön ja kansallisten politiikkojen muodostamiseen on keskeistä.

Kansallisella tasolla on tärkeää työskennellä poikkisektoriaalisesti. Tämä näkemys heijastuukin työryhmän väliraportissa. Tietojen hallinnoinnissa toimijoiden väliset integraatiot ovat yhteentoimivuusvaateiden myötä kasvaneet. Esimerkiksi perustietovarantojen osalta hallinnon strategisena tavoitteena on jo pitkään ollut saada yksi tieto yhdestä paikasta kaikkien sitä tarvitsevien tahojen käyttöön (esim. väestötiedot, paikkatiedot). Näin ollen tietoympäristöjen välillä on kytköksiä ja riippuvuuksia, jotka on tunnistettava ja pyrittävä turvaamaan.

Toisaalta eri hallinnonalojen osalta uhkatekijät ja turvallisuusvaateet ovat osittain myös keskenään poikkeavia, eli jatkossakin on erityistä turvaamista edellyttäviä toimijoita ja toimintoja. Turvallisuusratkaisujen vakioinnissa on löydettävä nykyistä parempi tasapaino keskitettyjen ja sinänsä kustannustehokkaiden mallien ja toisaalta pisteratkaisujen välillä. Kun tietotekniikka- ja –turvapalvelut keskitetään niin etäisyys organisaatioihin, jotka varsinaisesti käyttävät tai tuottavat ao. tietoa (ja ylipäätään ymmärtävät ao. tiedon merkityksen) kasvaa ja samalla ohenee herkkyys esim. toimintaympäristön muutosten seurannan tärkeydelle. Tätä omistajalinkkiä olisi syytä vahvistaa erilaisilla yhteistyörakenteilla ja omistajan tai asiakkaan tarpeiden kuuntelulla ja ymmärtämisellä. Vastaavasti resursointipohdinnoissa on huomioitava toisaalta keskitettyjä palveluja tuottavien ja valvovien toimijoiden ja toisaalta sektorikohtaiset tarpeet.

Työryhmän väliraportissa, ”Nykytilan arviointi” –osiossa tuodaan hyvin esiin kansainvälisen yhteistyön merkitystä tietoturvallisuuden ja tietosuojan kehittämisessä, ml. Euroopan Unionia keskeisenä viitekehyksenä, sekä kansainvälisen kybertoimintaympäristön muutoksia. Osiossa todetaan, että Suomen kyberturvallisuutta, tietoturvallisuutta ja tietosuojaan liittyviin tekijöihin voidaan kansallisen ja kansainvälisen sääntelyn ohella vaikuttaa toimialojen toimintakulttuureja

kehittämällä, vapaaehtoisella yhteistyöllä viranomaisten ja palveluiden tarjoajien välillä sekä kehittämällä sekä hyödyntämällä EU-politiikkoja ja välineitä.

Näemme kuitenkin, että myös työryhmän raportin poliittisissa linjauksissa on selkeästi todettava kansainvälisen kybertoimintaympäristön kehitys sekä tarve kansainvälisen kybertoimintaympäristön kehitystä koskevan tilannekuvan muodostamiseen ja jakamiseen kansallisesti hallinnonalojen ja yksityissektorin välillä niin, että se huomioidaan Suomen kansallisen toimintaympäristön arvioinnissa ja Suomen toiminnassa, ml. resurssien osalta.

Väliraportin muut osat, kommentit:

Joitakin huomioita väliraportista seuraavassa:

* Toimenpideohjelman laajuus ja monialaisuus; onko vaarana toimeenpiteiden pirstaloituminen? Mitkä asiat on saatava kokonaiskoordinaation alle, mitkä toisaalta ovat selkeästi toimialariippuvaisia? Kysymys on toki laaja, mutta olisi löydettävä vastauksia siihen, miten ja millä tasoilla tieto- ja kyberturvallisuutta aidosti johdetaan. Esimerkiksi Traficomin Kyberturvallisuuskeskukselle on asetettu runsaasti vaateita ja eri tasoille (Traficomin ohellakin) on varmistettava riittävä resursointi.

* Toiminnalliset tavoitteet on luotava realistisiksi ja annettaville suosituksille tulee olla olemassa myös seurantamenettely. On siis määritettävä, miten linjauksilla asetettuja tavoitteita mitataan ja mihin johtopäätökset tuloksista johtavat. Seurantamenettelyihin tai vastaaviin ei luonnoksessa ole toistaiseksi otettu kantaa.

Dokumentissa suojattavaa kohdetta on yleensä lähestytty melko teknisestä näkökulmasta. Sana tietojärjestelmä esiintyy 26 kertaa, tieto 13 kertaa, joissa se terminä pääosassa toimi etuliitteenä, kuten ”tieto- ja viestintätekniikka….”, mutta kertaakaan tietoa ei mainittu suojattavana kohteena itsessään. Tavallaan ajattelun keskiössä esityksessä on tietojärjestelmä, mutta ei niiden sisältämä tieto. Tiedon kuitenkin olla lähtökohtaisesti kohde, jota suojataan. Tiedon turvaaminen on suojauksen ydintä, jotta, tarkastelussa ei unohdu hallinnallinen kokonaisuus; tietojärjestelmän suojauksen lisäksi järjestelmää tai tietoa käyttävät ihmiset, asiaan liittyvät toimintaprosessit eli tiedon koko elinkaari.

Uusikartano Ari
Ulkoministeriö