FiCom ry | EU
25.4.2022

Hallintovaliokunnalle
Asia: VNS 1/2022 vp Ajankohtaisselonteko turvallisuusympäristön muutoksesta

# FiComin lausunto turvallisuusympäristön muutoksiin liittyvästä ajankohtaisselonteosta

Suomen vahvuutena on yksityisen ja julkisen sektorin luottamuksellinen yhteistyö. Viranomaisten rooli on koordinoida asioita eri hallinnonalojen välillä ja luoda yhteinen kuva kyberturvallisuuden tilanteesta. Yrityksillä taas on kyky suojata tietojärjestelmiä ja -infraa kyberhäiriöiltä ja -hyökkäyksiltä. Kybervarautumisen ytimenä tulee jatkossakin olla yksityisen ja julkisen sektorin yhteistyön vahvistaminen. Tiedon pitää kulkea molempiin suuntiin mutkattomasti. Yritysten pitää kertoa myös heikot signaalit ja havainnot viranomaisille. Lisäksi mitä varhaisemmassa vaiheessa yrityksillä on tieto mahdollisista uhkista sitä vahvemmin ne pystyvät siihen varautumaan. Tiedustelulait mahdollistavat tiedustelutiedon valikoidun jakamisen myös yrityksille.

Teleyrityksillä, kriittisen infran ylläpitäjinä, on mahdollisuus ja halukkuus tuoda oma osaaminen ja panos yhteiskunnan ylläpidon turvaamiseen. Myös ajankohtaisselonteossa privat/public-yhteistyö korostuu asianmukaisesti.

Toimivallan ja vastuiden selkiyttäminen ja viranomaistyön tiivistäminen mainitaan ajankohtaisselonteossa. Myös toimiala pitää näitä tarkennuksia tärkeinä. Esimerkiksi EU-pakotteiden toimeenpanon osalta oli harmillista toimivaltaepäselvyyttä.

Teleyrityksillä on vahvaksi muodostunut luottamus Traficomin kyberturvallisuuskeskuksen asiantuntevaan toimintaan. Toivottavaa on, että hyväksi ja toimivaksi todetut hallinnon rakenteet säilyvät. Ehjää ei kannata rikkoa. Kyberturvallisuuskeskuksen nykyinen, täysin keskeiseksi muodostunut rooli on säilytettävä.

Lainsäädäntö kyberturvallisuuden osalta on Suomessa ajantasaistettu viime vuosina; EU:sta on tulossa tarvittavaa lisäsääntelyä (NIS, CER). Näiden lisäksi tarvetta lisäregulaatiolle ei toimialan puolella tunnisteta. Tärkeämpää kuin laatia lisäsääntelyä on rakentaa yhteistyömallit toimiviksi.

Mahdollinen Nato-jäsenyys on toimialan näkökulmasta jatkumoa EU:n yhteiselle tiivistyvälle kyberpolitiikalle. Kyberturvallisuuden kehittämisessä EU:lla on selkeä rooli. Sen sijaan EU:n rooli kyberpuolustuksessa, kuten muillakin kansallisen turvallisuuden osa-alueilla on hyvin vähäinen. Nato-jäsenyys mahdollistaisi laajemman tuen ja yhteistoiminnan myös kyberpuolustukseen liittyvissä kysymyksissä.

Teleoperaattoreiden varautuminen erilaisiin kyberuhkiin on kokonaisvaltaista ja jatkuvaa. Turvallisuutta ei rakenneta hetkessä. Tämänhetkinen varautuminen rakentuu edellisten vuosien työlle. Riskien tunnistamisesta ja suojaamisesta huolimatta haavoittuvuuksia ja hyökkäyksiä havaitaan jatkuvan valvonnan, yhteistyön ja osaamisen avulla. Erilaisia varautumishankkeita, prosessien kehitystyötä on viime vuosina tehty paljon ja yritysten varautumiskyvykkyys on korkea. Valmista ja täysin riskitöntä tilannetta ei kuitenkaan koskaan saavuteta, vaan tehtävää riittää.

Siirtymäkausi jäsenyyshakemuksen jättämisen jälkeen on arvioiden mukaan kyberturvallisuutta haastava. Tiiviillä, luottamukseen perustuvalla yhteistyöllä ja tietojen aktiivisella jakamisella, myös viranomaisten suunnasta yrityksiin, pystytään hallitsemaan myös mahdolliset Suomeen ja suomalaisiin kohdistuvat vaikuttamisyritykset.

Elina Ussa
FiCom ry