Hybrid CoE

1.3.2021

EUROOPAN HYBRIDIUHKIEN TORJUNNAN OSAAMISKESKUS
LAUSUNTO

EDUSKUNTA
LIIKENNE- JA VIESTINTÄVALIOKUNTA
EU /2020/0359
Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi kyberturvallisuuden korkean tason varmistamiseksi EU:n alueella ja direktiivin 2016/1148 kumoamisesta

Yleistä:

Komission yllämainittu direktiivi on tärkeä askel EU:n yhteisen kyberturvallisuuden vahvistamisessa. Se laajentaa ja syventää aiemman vuonna 2016 annetun NIS-direktiivin soveltamisalaa sekä unionin tasoisia toimenpiteitä. Direktiivi luo yhtenäisiä velvoitteita ja käytäntöjä jäsenmaiden kyberturvallisuustoimille ja pyrkii näin varmistamaan, ettei unionijärjestelmään synny haavoittuvuuksia ja heikomman valvonnan tasoja, joiden kautta olisi mahdollista haavoittaa koko unionin kyberinfrastruktuurin keskinäisriippuvaista järjestelmää.

Direktiivin sisältämiä muutoksia voi nykyistä kyberturvallisuusympäristön kehitystä silmälläpitäen pitää varsin perusteltuina. Direktiivin soveltamisalan laajennus vastaa nyky-yhteiskuntien kokonaisturvallisuuden tarpeita ja EU-tasoisten kyberturvallisuuskäytäntöjen (keskeisten toimijoiden tunnistaminen, kyberturvallisuusvalmiuksen ja yhteisen tilannekuvan kehittäminen sekä haavoittuvuuksien tunnistaminen ja häiriöihin varautuminen) lujittaminen puolestaan on vastaus sekä unionin sisäisten keskinäisriippuvuuksien että ulkoisen turvallisuusympäristön kehitykseen.

Seuraavaksi tehdään joitakin yksittäisiä huomioita direktiiviehdotukseen liittyen.

Euroopan hybridiuhkien torjunnan osaamiskeskus
Lintulahdenkatu 5 A
00530 Helsinki

Hybrid CoE

1.3.2021

Kyberturvallisuusinstrumentit osana hybridiuhkia

Hybridiosaamiskeskuksen toiminnassa on käynyt konkreettisesti ilmi, kuinka kyberturvallisuuteen liittyvät haavoittuvuudet ovat merkittävä uhka keskuksen osallistujamaille. Hybridivastustajat valmistautuvat käyttämään tietoverkkoja, tietojärjestelmiä ja digitaalisia ohjausjärjestelmiä hyväkseen eri tavoin. Havaintoja vihamielisestä valtioiden sponsoroimasta järjestelmiin soluttautumisesta julkistetaan jatkuvasti.

Tunkeutumisten ilmeisimpänä tavoitteena voi olla järjestelmistä saatavien tietojen varastaminen. Tämä uhka liittyy kaikkiin tiedustelukysymyksiin, mutta lisääntyvästi teollisuusvakoiluun, jossa on vaarana innovaatioihin ja liiketoimintakilpailuun liittyvän tiedon menettäminen. Tunkeutujat voivat myös luoda valmiuden vahingoittaa yhteiskunnan kriittisiä järjestelmiä. Mahdollisia toimintatapoja ovat tiedostojen manipulointi ja hävittäminen, järjestelmien toiminnan estäminen sekä digitaalisten ohjausjärjestelmien kaappaaminen virheellisten toimintojen aiheuttamiseksi. Näillä tavoilla voidaan saada aikaan merkittäviä häiriöitä, joilla on joko paikallisesti tuhoisa tai laaja-alainen vaikutus. Osana laajempaa hybridioperaatiota tai -sodankäyntiä niiden merkitys voi olla ratkaiseva.

Tietoverkkoihin ja -järjestelmiin kohdistuvien hybridiuhkien ennaltaehkäisemiseksi on hyödyllistä kohottaa järjestelmien ns. resilienssiä, tässä tapauksessa suojausta, häiriönsietoa ja palautumiskykyä. Sen lisäksi parantuva kyky havaita vihamielinen toiminta ja tunnistaa tekijät (attribuutio) kohottaa toiminnasta hyökkääjälle aiheutuvia riskejä. Näin on varsinkin silloin, kun hyökkäyksen kohteeksi joutunut yritys tai valtio saisi todennäköisesti tukea kumppaneiltaan. EU:lla on jo mahdollisuus käyttää pakotteita kyberhyökkäyksiin liittyen, millä pyritään aikaansaamaan pelotevaikutusta tällaisen toiminnan estämiseksi.

Lausuttavana oleva direktiiviluonnos sisältää merkittäviä parannusehdotuksia kybersektorin resilienssin, tunkeutumisten havaitsemiskyvyn, tekijöiden tunnistamisen ja unionin yhteisten kyberturvallisuusstandardien ja -menetelmien parantamiseksi.

Euroopan hybridiuhkien torjunnan osaamiskeskus
Lintulahdenkatu 5 A
00530 Helsinki

Kehitettäväksi esitetään monitasoista tiedonvaihtojärjestelmää. Esitetyllä koordinointiryhmällä olisi huomattavan monitahoinen tehtäväkenttä. Sitä täydentäisi kansallisten CSIRT-keskusten verkosto, EU-CyCLONe kyberkriisiverkosto ja ENISA:lta edellytettävä tilanneraportti. Tämä kokonaisuus olisi omiaan edistämään kaikkia yllä mainittuja hybridiuhkien torjunnan tavoitteita tuottaessaan yksittäiselle jäsenvaltiolle huomattavasti mahdollisuuksia saada tietoja varautumisen tueksi ja suoraa tukea ongelmatilanteissa.

Lisäksi direktiivin piiriin kuuluisi edellistä vaihetta enemmän erilaisia toimijoita jäsenvaltioissa. Tämä on myönteistä. Esimerkiksi sopii se, että vasta nyt järjestelmään liitetään sairaalat. Potilastietojen anastaminen, niiden manipulointi sekä sairaaloiden järjestelmien häirintä ovat mahdollisia rikoksen tai hybriditoiminnan keinoja, jollaisia ei tulisi jättää kattamatta. Esitetään, että direktiivin käsittelyn yhteydessä luonnosta analysoidaan tarkasti ja aktiivisesti sen estämiseksi, että merkittäviä yhteiskunnan toimintoja yhä jäisi soveltamisalueen ulkopuolelle. Lisäksi olisi toivottavaa, että syntyy riittävät vaatimukset epäiltyjen tapahtumien jälkikäteen tapahtuvaa todentamista varten ja niiden raportoimiseksi (attribuutio).

Asian tärkeyden huomioon ottaen on tarpeellista, että direktiivin kansallisen toimeenpanon valvonta luodaan tehokkaaksi. Direktiivin keskeisen tarkoituksen – kyberturvallisuuden korkean tason varmistaminen EU-alueella – edellyttää jäsenmaiden yhdenmukaista sitoutumista kyberturvallisuuskäytäntöjen ja siihen liittyvän seurannan ja kriisivalmiuden luomiseen.

Direktiivin tarkoittamat järjestelmät ja toimijat ovat siten verkottuneita, että säännökset on laadittava EU-tasolla (subsidiariteettiperiaate toteutuu). Jos tällainen hanke jäisi jäsenvaltioiden sääntelyn varaan, syntyisi haitallisessa määrin eri tasoisia ratkaisuja, millä olisi myös sisämarkkinoiden kilpailua vääristävää vaikutusta. Yritykset saattaisivat vältellä korkeaa turvallisuutta edellyttäviä jäsenmaita sijaintipaikkana ja joka tapauksessa kustannusten hinnoitteluvaikutukset olisivat epätasaisia.

Ehdotettu direktiivi vaikuttaisi luovan EU:sta yhdenmukaisesti toimivan ja kohtuudella suojatun kyberalueen, joka toimii yhdessä uhkilta suojautumisessa ja niihin vastaamisessa. Paitsi, että tätä tulee pitää EU:n ja sen jäsenvaltioiden kyberuhkien

Euroopan hybridiuhkien torjunnan osaamiskeskus
Lintulahdenkatu 5 A
00530 Helsinki

torjuntakapasiteettia merkittävästi kasvattavana aloitteena, myös hybridiuhkien suhteen tämä on erittäin kannatettava kehityssuunta.

Euroopan hybridiuhkien torjunnan osaamiskeskus
Lintulahdenkatu 5 A
00530 Helsinki