TRAFICOM/116905/03.03.01/2022
21.3.2022

**Eduskunnan puolustusvaliokunta**
PuV@eduskunta.fi

# Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen asiantuntijalausunto Puolustusvaliokunnalle koskien kyberturvallisuutta ja -puolustusta Suomessa

*Teema:* millä keinoin Suomen kyberturvallisuutta ja -puolustusta voidaan kehittää lyhyellä, keskipitkällä ja pitkällä aikavälillä.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus kiittää Eduskunnan puolustusvaliokuntaa asiantuntijalausuntopyynnöstä.

Kyberturvallisuusuhkat tulevat entistä konkreettisimmin esille samalla tavoin kuin fyysisessä maailmassa kohtaamamme turvallisuusuhkat. Yhteiskunnan eri palveluiden digitalisoituessa kyberturvallisuusuhat eivät ole enää erillisen virtuaalimaailman vitsaus, vaan jokapäiväiseen elämään vaikuttava uhka. Monesti nämä uhkakuvat voivat kohdistua myös yhteiskunnan toiminnan kannalta kriittisiin toimintoihin. Muuttuva turvallisuusympäristö ja kyberturvallisuutta koskevat uhkakuvat voivat vaikuttaa yhä useammin myös kansalliseen turvallisuuteen. Käynnissä oleva kansainvälinen tilanne on osoittanut sen, että Euroopassa on syytä varautua aikaisempaa tehokkaammin kyberhyökkäyksiin, -häiriöihin ja -vaikuttamiseen. Tämän osalta on syytä muistaa, että kyberhyökkäysten, -häiriöiden ja -vaikuttamisen taustalla voi olla myös valtiolliset tekijät.

Turvallisuusympäristömme on pysyvästi muuttunut eikä kyberriskejä voida enää arvioida irrallaan muista turvallisuusriskeistä. Kansainvälisen tilanteen perusteella vaikuttaa siltä, että kyberhyökkäykset ja -vaikuttaminen voivat olla hyökkääjätaholle ensimmäinen aggressiota osoittava toimi. Kyberturvallisuuskeskus korostaa, että uusien riskien tunnistaminen ja niihin vastaaminen edellyttää poikkihallinnollista analyysiä ja toimia. Tästä syystä siviili- ja puolustusviranomaisten on toimittava saumattomasti yhteen kyberturvallisuuden ja -puolustuksen kehittämisessä. Vain tiiviillä viranomaisyhteistyöllä ja yhteistyöllä yksityisen sektorin kanssa voidaan kehittää koko yhteiskunnan kyberturvallisuutta koskevaa varautumista ja häiriönsietokykyä. Korkean tason kyberturvallisuus yhteiskunnan eri sektoreilla ja kehittynyt kyberpuolustus ovat myös tärkeä signaali niille tahoille, jotka toimivat aggressiivisesti kybertoimintaympäristössä.

Kyberturvallisuuden ja kyberpuolustuksen kehittämisessä on äärimmäisen keskeistä, että jo olemassa olevat kehityspolut mahdollistetaan resurssien näkökulmasta ja että niiden hyöty realisoituu täysimääräisenä. Näitä ovat muun muassa Kyberturvallisuuden kehittämisohjelma, jonka painopisteinä ovat muun muassa kansallinen osaaminen ja kyberomavaraisuuden parantaminen sekä monipuolisesti turvallisen viestinnän mahdollistava kansallinen salaustuoteperhe. Lisäksi Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla on kyberturvallisuuden kehittämisessä kriittisessä roolissa. Periaatepäätöksen toimenpiteillä asetettaisiin muun muassa kriittisille toimialoille nykyistä täsmällisempiä tietoturvallisuusvaatimuksia ja tuotettaisiin kartoituspalvelua suurimmille kunnille. Samoin käynnissä olevat LVM:n lainsäädäntö sekä SM:n ja PLM:n selvityshankkeet osaltaan tunnistavat parantamiskohteita, joiden toteuttamisen mahdollistaminen on keskeistä.

Kansallisten toimien ohella on tärkeää, että EU:n tasolla on käyty aktiivista keskustelua ja harjoiteltu jäsenvaltioiden keskinäistä avunantoa kyberhäiriö- ja kriisitilanteissa.

Seuraavassa Kyberturvallisuuskeskus esittää tarkempia ajatuksia kyberturvallisuuden kehittämiseksi eri aikajänteillä.

**Lyhyen aikavälin toimet**

Lyhyellä aikavälillä on mahdollista kehittää erityisesti kybertilannetietoisuuteen ja organisaatioiden tavoitettavuuteen, sekä kyberturvallisuuden viranomaisresursoinnin korjausvelan parantamiseen.

Turvallisuuden kokonaistilannekuvalla on kasvanut tarve huoltovarmuuskriittisillä sektoreilla ja valtiojohdossa. Kriisitilanteessa edellä mainittu tilannekuva ja sen tuottamiseksi sovitut selkeät roolit ja viranomaisyhteistyöprosessit ovat ensiarvoisen keskeisessä roolissa kriittisten toimialojen suojelemisessa, kyberturvallisuusriskien realisoitumisen ennakoinnissa ja näihin liittyvän päätöksentekokyvyn mahdollistamisessa. Jotta tarvittavaa tilannekuvaa voidaan tuottaa yhteiskunnan ja valtion kriittisten toimintojen tukemiseksi, turvallisuutta, ml. kyberturvallisuutta, koskevan tilannekuvan muodostamiseen tulee osoittaa nykyistä enemmän resursseja. Tilannekuvatoiminnon kehityksessä tulee huomioida myös tietojen jakaminen ja koostaminen kansainvälisten kumppaneiden kanssa.

Julkisen sektorin organisaatioiden ja huoltovarmuuskriittisten toimijoiden tavoitettavuus kyberhäiriötilanteissa on Kyberturvallisuuskeskuksessa tunnistettu ongelmalliseksi. Kaikilla edellä mainittuihin kategorioihin kuuluvilla organisaatioilla ei ole selkeää yhteyspistettä, joihin kyberturvallisuusongelmista voi viestiä. Nopea tavoitettavuus ja välittömät toimet hyökkäyksen tai häiriön torjumiseksi voivat olla kriittisiä koko yhteiskunnan turvallisuuden kannalta.

Toimintaympäristön muutoksesta johtuva Kyberturvallisuuskeskuksen jo olemassa olevien tehtävien kasvanut resursointitarve on huomioitava. Kyberturvallisuusongelmissa Kyberturvallisuuskeskuksen apua tarvitsevia kansalaisia, viranomaisia ja yhteiskunnan kriittisten toimialojen toimijoita on joka vuosi entistä enemmän. Kasvavaan tuen tarpeeseen vastaaminen edellyttää lisärahoitusta. Kyberturvallisuuskeskuksen toiminnan ja toimintojen kehittäminen välttämättömälle tasolle edellyttää useiden miljoonien eurojen lisärahoitusta. Mikäli nyt jäämme jälkeen Suomen kyberturvallisuuden perustan ja varautumisen rakentamisessa, tulevat tulevaisuuden kustannukset kyberturvallisuuden toimenpiteiden laiminlyönnistä olemaan moninkertaisesti suhteessa nyt esitettyihin panostuksiin. Kyse ei ole ainoastaan taloudellisista menetyksistä, vaan myös esimerkiksi henkisistä kärsimyksistä, joista Vastaamo-tapauksen seuraukset ovat vain yksi esimerkki. Haluamme osaltamme huolehtia siitä, että Suomen kyberturvallisuutta koskeva varautuminen ja häiriönsietokyky ovat riittävällä tasolla suhteessa vallitseviin uhkiin ja riskeihin.

**Keskipitkän aikavälin toimet**

Tilannekuvan muodostumisen parantaminen vaatii keskipitkällä aikavälillä viranomaisille ajantasaiset ja turvalliset työkalut turvaluokiteltuun viestintään viranomaisten välillä. Nykyisellään viranomaisten välinen ja kriittisen infrastruktuurin toimijoiden suuntaan tapahtuva yhteydenpito nojaa liiaksi siiloutuneisiin järjestelmiin tai sähköpostiin. Toimivien ja suojattujen tiedonvaihtokanavien puute voi johtaa siihen, että kansallinen päätöksentekojärjestelmä voi olla uhattuna kriisitilanteessa. Kansallisen

tiedonvaihdon lisäksi vahvemmin suojattujen tiedonvaihtokanavien tarve korostuu myös kansainvälisessä yhteistyössä.

Kyberturvallisuuden varmistaminen koostuu useista eri tasoilla toteutettavista toimenpiteistä. Viranomaistoimijat voivat omalla toiminnallaan edistää kansallista kyberturvallisuutta ja kyberpuolustusta. Vaikka viranomaiset voivat velvoittaa ja kannustaa eri tahoja kehittämään kyberturvallisuutta koskevaa varautumistaan, kyberturvallisuuden ja sitä koskevan varautumisen edistäminen edellyttää aktiivisia toimia yksityiseltä sektorilta. On syytä huomioida, että yksityisen sektorin toimijat vastaavat pääasiallisesti kriittisen infrastruktuurimme ylläpidosta ja suojaamisesta. Kriittisen infrastruktuurin aktiivinen suojaaminen muun muassa kyberhyökkäyksiltä on tärkeää yhteiskunnan kokonaisturvallisuuden näkökulmasta. Kriittisen infrastruktuurin suojaamisen osalta Kyberturvallisuuskeskus haluaa korostaa koko toimitusketjun turvaamisen merkitystä. Toimitusketjun suojaamisen lisäksi Kyberturvallisuuskeskus pitää tärkeänä, että tunnistetaan teknologiariippuvuuksien aiheuttamat riskit toimitusketjujen toimivuudelle ja huoltovarmuudelle. Kriittisen infrastruktuurin kyberturvallisuustoimenpiteiden toteutumista on tärkeää mitata säännöllisesti.

Kyberturvallisuuskeskus haluaa muistuttaa, että myös monet kriittisistä teknologioista, kuten esimerkiksi viestintäverkot, ovat kriittisiä niin siviiliyhteiskunnan kuin maanpuolustuksen näkökulmasta.

EU:n kilpailukyvyn ja kyberturvallisuutta koskevan omavaraisuuden vahvistaminen edellyttävät, että Euroopassa panostetaan kyberturvallisuutta koskevaan teollisuuden ja teknologian kehittämiseen sekä tutkimuksen resursointiin. Kyberturvallisuuskeskus haluaa tuoda esille komission puolustuspaketissakin mainitun Kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen (EU:n kompetenssikeskus) ja sen alle perustetun kansallisten koordinointikeskusten verkoston. Uusi Kyberturvallisuuden kompetenssikeskus ja kansallinen koordinointikeskus pystyvät tukemaan niin EU-tason kuin kansallisia kyberturvallisuustoimijoita. Suomessa Kyberturvallisuuskeskus toimii kansallisena koordinointikeskuksena.

**Pitkän aikavälin toimet**

Kyberturvallisuuskeskus pitää merkittävänä, että kyberturvallisuus on nostettu vahvemmin esille EU:n sääntelyhankkeissa ja harjoitustoiminnassa. Kyberturvallisuuskeskus pitää tärkeänä, että erityisesti yhteiskunnan kriittisten sektoreiden kyberturvallisuutta kehitetään EU-sääntelyn keinoin. Tästä hyvänä esimerkkinä on verkko- ja tietoturvadirektiivin (NIS-direktiivi) uudelleenarviointi, joka vahvistaa yhteiskunnan kriittisten sektoreiden kyberturvallisuutta. Kyberturvallisuuskeskus katsoo, että sääntelyn pitää kuitenkin olla oikeasuhtaista ja päällekkäistä työtä tulee pyrkiä välttämään eri säädöshankkeiden välillä.

Lisäksi kyberturvallisuusosaamiseen on panostettava jo peruskoulujärjestelmästä alkaen. Keskeisenä ongelmakohtana erityisesti laajoissa kyberhäiriöissä Kyberturvallisuuskeskus näkee kyberturvallisuusosaamisen ja sen kehittäminen on väistämättä yksi tärkeimmistä pitkän aikavälin toimenpiteistä. Suomessa ei ole tällä hetkellä siviilipuolen kyberturvallisuusosaamisen riittävää reserviä, jota voitaisiin ottaa käyttöön laajoissa ja vakavissa häiriötilanteissa. Osaamisen kehittäminen vaatii ennen kaikkea pitkäjänteistä sitoutumista ja resursoinnin jatkuvuutta.

Sauli Pahlman

Ylijohtaja