Finnish Information Security Cluster (FISC) – Kyberala ry

Lausunto

09.09.2024

Asia: VN/12457/2021

Lausuntopyyntö luonnoksesta Yhteiskunnan turvallisuusstrategiaksi 2024 (YTS2024)

Luku 1. Johdanto

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

Kannatamme, että kokonaisturvallisuuden toimintamallissa yhteiskunnan elintärkeät toiminnot pyritään turvaamaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistoiminnalla kaikissa olosuhteissa ja kaikilla tasoilla. Tämä tulisi kuitenkin ilmetä myös käytännössä aitona kumppanuutena ja yhteistyönä elinkeinoelämän kanssa viranomaisten yksipuolisen toiminnan sijaan. Tällöin olennainen kysymys on, mitä viranomaiset voivat omalta osaltaan tehdä, jotta elinkeinoelämä voisi osallistua ja huolehtia omista riskeistään ja jatkuvuutensa varmistamisesta. Toisin sanoen viranomaistoimintaan liittyvää valmistelua tulisi suunnata aiempaan selvemmin siihen, miten julkinen sektori voi tukea Suomessa sijaitsevia organisaatioita turvallisuuden riskienhallintakeinojen toimeenpanossa.

Lisäksi on tarpeen huomioida, ettei yhteiskunnan elintärkeiden toimintojen turvaaminen ole kaksijakoinen (turvaaminen / turvaamattomuus), vaan laadullinen seikka. Toimintojen turvaaminen tarkoittaa korkeaa tuotannon jatkuvuutta. Tälle ns. pavelutasolle onkin kyettävä asettamaan perusteltuja ja yritysten hallinnollisen taakan ja kustannusten osalta järkeviä ja toteuttamiskelpoisia tavoitteita. Varautuminen on resurssi-intensiivistä. Varautumisen ytimessä on ajatus, että henkilötyötä ohjataan pohtimaan ja toteuttamaan järjestelyjä etukäteen sen suhteen, mikä voi mennä pieleen, miten häiriötä estetään syntymästä, miten tilanteesta voitaisiin palautua ja etenkin, mitä investointeja mahdollisesti tarvitaan toimintakyvyn turvaamiseksi. Siksi varautumisen kehittämisen tulisi keskittyä resurssienkäytön optimointimahdollisuuksiin. Ko. työtä ei voi tehdä ilman kyseisten toimijoiden merkittävää osallistumista. Yritykset ovat jo nyt lähes hallitsemattoman uuden (EU-)sääntelytaakan edessä, josta syystä kansallisia vaatimuksia sisältää sääntelyä ei tule antaa.

Luku 2. Yhteiskunnan elintärkeät toiminnot

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

PIA ry:n lausuntoon myös viitaten, ehdotamme seuraavan kappaleen lisäystä luvun 2 Yhteiskunnan elintärkeät toiminnot; 2.3. Puolustuskyky loppuun:

Kyberturvallisuusteollisuuden (vastaavasti kuin puolustusteollisuuden) rooli ja sen tuotantokyky korostuvat muuttuneessa turvallisuustilanteessa. Kilpailukykyinen kotimainen alan teollisuus ja sen kansainvälinen verkottuminen ovat keskeisessä asemassa kokonaisturvallisuuden ylläpitämisessä sekä uusien ratkaisujen kehittämisessä. Yhteiskunnan kriittisestä infrastruktuurista yhä suurempi osa on yksityisten yritysten hallinnassa ja niiden suojaamiseksi sekä toimivuuden varmistamiseksi tarvitaan yritysten tuottamaa teknologiaosaamista ja palveluja. Ekosysteemin ylläpito ja kehittäminen edellyttävät laajaa kansallista osaamispohjaa teollisuudessa.

Luku 3. Yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

On selvää, että vahinkovaikutuksiltaan mittaamattomiin, vaikka todennäköisyyksiltään pieniin uhkiin kuten sotilaalliseen konfliktiin tai muuhun aseelliseen uhkaan, tulee edelleen varautua riittävällä tasolla. Tätä tehtävää varten yhteiskunnassa on nimenomaisia ja nimettyjä viranomaisia sekä muita toimijoita. Samalla on kuitenkin syytä huomioida, että uhkien käsittelyn ei tule typistyä, eikä perustua kapea-alaisesti sotilaallisiin uhkiin. Uhkamalleista riippumatta huoltovarmuuden, elinkeinoelämän ja kansalaisyhteiskunnan toimintaedellytyksistä huolehtimisen tulee perustua (taloudellisen) hyvinvoinnin lähtökohtiin, sillä vahva talous on ratkaisevan tärkeä riskienhallinnan lähtökohta.

Luku 4. Yhteiskunnan elintärkeiden toimintojen turvaaminen

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

Taloudellisten toimijoiden ja hallinnon, mukaan lukien yhteiskunnan elintärkeitä toimintoja ylläpitävät organisaatiot, on tuottavuutta kasvattaakseen panostettava digitalisaatioon, mikä edellyttää digitaalisten riskien hallintaa. Julkiset panostukset digitalisaation ja digitaalisten riskien hallintaan yhdessä ja yhtäaikaisesti ovat siksi välttämättömiä. Digitaalinen valmius (preparedness) ja resilienssi synnytetään siellä, missä tieto ja tietojärjestelmät ovat. Ylivoimainen osa tiedosta sekä tieto- ja viestintäjärjestelmistä on yritysten hallussa – esim. Suomessa on 78 000 työnantajayritystä. Jokainen näistä on osa yhteiskunnan toiminnan ja taloudellisen toimeentulon jatkuvuutta, tuottaen n. 60% bruttokansantuotteesta. Uhkiin vastaamiseksi varautumismallin tulisikin kannustaa soveltuvien riskienhallintakeinojen käyttöönottamiseen.

Tietoturvaloukkausten ennalta ehkäisemisestä, niiden selvittämisestä ja vaikutusten poistamisesta vastaavat valtaosin tiedon ja tietojärjestelmien haltijat. Viranomaisilla on rooleja edellä mainituissa (kuten rikosten syyteharkintaan saattaminen, uhkatunnistetietojen välittäminen sekä hallinnollisten vaatimusten valvonta). Jatkuvuuden varmistamisen ja tieto-omaisuuden suojaamisen näkökulmasta nämä tehtävät ovat vaikuttavuudeltaan ja tuloksellisuudeltaan kuitenkin toissijaisia.

Yritysten edellytyksiä huolehtia kyberturvallisuudesta on perusteltua tukea politiikkatoimin. Keskeinen ehdotus on modernien tietoturvaratkaisujen käyttöönoton tuki, osittain EU-rahalla toteutettuna (edistyneitä kyberturvallisuus- eli tietoturvaratkaisuja on laajasti saatavilla markkinoilta ja parhaita käytänteitä on tunnistettu kattavasti, mutta ne eivät ole riittävän laajasti eri toimijoiden käytössä). Esimerkiksi Suomessa oli käytössä 2023 tietoturvaseteli huoltovarmuuskriittisten yritysten tietoturvan vahvistamiseen, jonka 6 M€ määräraha varattiin moninkertaisesti loppuun alle kahdessa viikossa.

Luku 5. Kokonaisturvallisuuden toimijat

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

Yritykset ovat yhteiskunnan toiminnan kannalta ja myös oikeudellisesta näkökulmasta keskeisimpiä toimijoita kokonaisturvallisuuden malliin suhteutetun kyberturvallisuuden varmistamisessa. Suomen n. 450 000 yrityksestä 20 suurimman yhteenlaskettu liikevaihto ylittää yksinään 160 mrd€ (lähes kaksi kertaa valtion 2024 budjetti) ja esim. teknologia-alan 6000 yritystä muodostavat noin kolmanneksen Suomen bruttokansantuotteesta. Tässä valossa on syytä painottaa, että yhteistyörakenteissa, joissa ei ole elinkeinoelämän kattavaa edustusta on ilmeinen vaara, että vaikuttavuus jää heikoksi kyberturvallisuuden kehittämisen, suunnittelun, varautumisen ja kriittisen tieto- ja viestintäteknisen infrastruktuurin varautumisen koordinaation ja yhteensovittamisen osalta.

Vastaavasti PIA ry:n lausuntoon viitaten elinkeinoelämä on entistä vahvemmin kokonaisturvallisuuden ja maanpuolustuksen kyvykkyyksien toimittaja. On myös tarpeen jatkaa keskustelua ja työtä sen eteen, että yhteiskunnassa toimittaisiin entistä selkeämmin siitä lähtökohdasta, että yritykset ovat ”toimittajaroolin” lisäksi kumppaneita erilaisten turvallisuuteen liittyviä toimintojen ylläpitämisessä markkinatalouden säännöin ja periaattein. Tämä tarkoittaa myös harkintaa, miltä osin julkisten tai julkisomisteisien toimijoiden on perusteltua harjoittaa toimintaa kilpailluilla ja toimivilla markkinoilla.

Yhteistyötä elinkeinoelämän kanssa tulisi tehostaa siirtymällä toimintamalliin, jossa yritykset kytketään läpinäkyvämmin ja alusta lähtien virkamiesvalmisteluihin mukaan. Suomessa toimivan elinkeinoelämän keskeistä asemaa osana huoltovarmuuttamme tulee kehittää kotimaisen teollisuuden tuotantokapasiteettia vahvistamalla. Samalla vahvistuu kyky reagoida muuttuneeseen turvallisuustilanteeseen. Suomella on oltava riittävä teollinen ja teknologinen osaaminen kriittisten järjestelmien itsenäisen käytön takaamiseksi. Pitkäsikaisriskien hallinnan kannalta on olennaista, että kriittisten teknologioiden aloilla toimivat suomalaisyritykset kykenevät ylläpitämään osaamistasoaan. Mm. kansallisen osaamisen huoltovarmuus erityisesti digitalisaation, kyberturvallisuuden, tekoälyn, analytiikan ja autonomian osalta ovat merkitykseltään kasvavia alueita. Tässä liittyen myös Huoltovarmuuskeskuksen ja huoltovarmuuspoolien roolia tulisi kirkastaa ja jatkossa, NIS2-direktiivin toimialoja mukaillen, tuoda näkyväksi kaikilla relevanteilla toimialoilla (poolit ovat toimijoita, jotka yhteensovittavat viranomaisten ja elinkeinoelämän varautumisen tarpeita).

Luku 6. Kokonaisturvallisuuden tulevaisuus

Kirjoita yksilöity palautteesi tähän. Merkitse alaluku tai sivunumero.

Kyberturvallisuus on keskeinen elementti, jonka avulla varmistetaan osaltaan kansallisen turvallisuuden, maanpuolustuksen, huoltovarmuuden, elinkeinoelämän ja kansalaisyhteiskunnan toimintaedellytykset. Suomen (taloudellista) hyvinvointia ei tule kuitenkin perustaa kapeaan ajatukseen varautumisesta aseelliseen uhkaan tai poikkeusoloihin. Digitaalisen resilienssin tärkein elementti on päivittäinen jatkuvuus eli yhteiskunnan toimijoiden käyttämien viestintä- ja tietojärjestelmien (ml. data) ylläpitämien tietovirtojen ja palveluiden luottamuksellisuus, eheys ja saatavuus. Jokaisella, joka hallitsee edellä mainittuja, on oma vastuunsa ja roolinsa toteuttaa soveltuvia riskienhallintatoimia (esim. vahva osapuolten tunnistautuminen ja tarkka pääsynvalvonta sekä kvanttiturvallisen salauksen käyttöönotto).

OSA 2: Strategiset tehtävät

Kirjoita yksilöity palautteesi tähän. Merkitse strategisen tehtävän numero ja nimi sekä nimeä osio (Päämäärä ja tavoitteet; Toiminta-ajatus; Toimijat).

Osa 2: Strategiset tehtävät

Strategialuonnoksessa mainitun kyberturvallisuuden kansallisen yhteistoimintamallin (s. 111) osalta viranomaisten intressien hahmottamisessa olisi perusteltua ottaa jo lähtökohdaksi se, millaiset politiikkatoimet olisivat Suomen pitkäaikaisen kokonaisedun mukaisia. Yhdeksi toiminnan periaatteeksi tulisi kirjata myös, miten Suomi kehittyy, kilpailee ja pärjää suhteessa muihin valtioihin (välttäen hallinnonalojen omia, osaoptimoituja kehittämiskeinoja). On välttämätöntä, että Suomen asema avoimena sekä yritysten oikeuksia ja intressejä kunnioittavana markkinataloutena otetaan aiempaa selvemmin huomioon myös digitaalisen turvallisuuden toimissa. Julkisen ja yksityisen sektorin tiiviimpää yhteistyötä ja luottamusta vahvistavaa yhteistoimintamallia kehitettäessä tulisi strategiassa ottaa kantaa myös siihen, millaisilla rakenteilla tavoitetta kohdin edetään.

Esimerkiksi kohdassa Toiminta-ajatus todetaan (s. 112): ”Varautumisen perustana ovat lainsäädännöstä johtuvat toimijoiden velvoitteet, oikeudet ja tehtävät sekä hankinnat ja yhteistyösopimukset. Kyberhäiriötilanteissa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa.” Katsomme, että kirjaus on jo valtiosääntöoikeuden lähtökohdista virheellinen, sillä yksityinen omaisuus on perustuslailla turvattu. Näin ollen myös tietojärjestelmät, tieto ja data ovat turvatut, eikä tällöin viranomaiselle ole oikeutta ”johtaa” eli määrätä yksityisen omaisuuden käytöstä edes hyvää tarkoittaen. Toiminta-ajatukseen tulisikin kirjata, että ”Kyberhäiriötilanteiden välttämisen suhteen toimivaltaiset viranomaiset valvovat toiminnan harjoittajia sekä häiriötilanteen aikana tukevat niitä hallintatoimissa kukin tehtävänsä ja toimivaltansa puitteissa.”

Luonnoksessa kansalliseksi kyberturvallisuusstrategiaksi, joka on tähän strategialuonnokseen vahvasti kytköksissä, kehittäminen vaikuttaa kohdistuvan pääosin, ellei lähes kokonaan viranomaisten toiminnan ja yhteistyömuotojen kehittämiselle. Lisäksi yhteistyö vaikuttaa

kohdistuvan lähinnä kyberuhkia koskevaan tiedonvaihtoon eli häiriötilanteiden hallintaan, mikä edustaa vain yhtä, kapeahkoa yhteistoiminnan osa-aluetta yhteensä yhdeksästä jo aiemmin tunnistetusta alueesta (ohjaus, tutkimus, tilannekuva, regulaatio, osaaminen, jatkuvuus/varautuminen, hankinnat/hankkeet/palvelut, harjoittelu). Luottamusta vahvistavaa yhteistoimintamallia ei ole mahdollista saavuttaa yksistään kuvatuilla toimintalinjoilla tai ehdotetulla rakenteella puuttuu myös kokonaan pohdinta siitä, mitkä ovat yksityisen sektorin intressit ja mahdollisuudet tukea ja osallistua viranomaisten toimintaa kuvaaviin tavoitteisiin. Yhteistoiminnan luonnostelussa tulisi lähteä liikkeelle siitä, miten strategia mahdollistaa hallitusohjelmassakin vahvistetun tavoitteen, jossa poliittisen- ja hallintovallan tehtävä on tarjota puitteet vapaudelle ja (taloudellisille) mahdollisuuksille.

Sivun 113 neljännessä kappaleessa on virhe. Siinä todetaan: ”Yhteiskunnan keskeisten toimijoiden on EU:n kyberturvallisuusdirektiivin mukaisesti arvioitava riskejä, joita kohdistuu niiden käyttämien viestintäverkojen ja tietojärjestelmien turvallisuuteen.” Direktiivin mukaan velvoite koskee sekä keskeisiä että tärkeitä toimijoita, joten termi ”tärkeä” tulisi lisätä virkkeeseen.

PIA ry:n lausuntoon viitaten ehdotamme myös korjausta osaan 2, Talous, infrastruktuuri, huoltovarmuus, 44. Elintärkeän teollisuus- ja palvelutuotannon turvaaminen (toiminta-ajatus):

Sivun 128 ensimmäisessä kappaleessa on virhe. Siinä todetaan: ”Valmistavan teollisuuden yrityksillä ei ole yleistä lakiin perustuvaa velvoitetta. Niiden osalta varautuminen perustuu alan järjestöjen ja Huoltovarmuuskeskuksen välisiin sopimuksiin. Sopimusperusteista varautumista täydentää tiettyjen kriittisten hyödykkeiden (tavarat, materiaalit) lakisääteinen velvoitevarastointi.” Huomautamme, että Puolustusvoimilla ja yrityksillä on erityisiä sopimuksia kriisiaikoja ja niihin varautumista varten. Lisäksi valmistavan teollisuuden yritysten varautuminen perustuu ensisijaisesti niiden omaehtoiseen, liiketoimintalähtöiseen riskienhallintaan. Alan järjestöjen ja Huoltovarmuuskeskuksen välisillä sopimuksilla (tarkoitetaan oletettavasti poolisopimuksia) ei ole yksittäisiin valmistavan teollisuuden yrityksiin nähden velvoittavaa vaikutusta. Yksittäisten yritysten kiinnittyminen poolityöhön perustuu vapaaehtoisuuteen.

Huoltovarmuussopimusten sisältöä tulisi käsitellä strategiaehdotuksessa tarkemmin ainakin siltä kantilta, että voitaisiinko niissä sopia muustakin kuin vain varastoinnista, esimerkiksi osaamisen tuottamista tai ylläpidosta, palveluista, ohjelmistojen kehittämisestä tai ylläpidosta jne.

Lisäksi kuvaus on virheellinen siltä osin, että sekä edellä mainittu kyberturvallisuusdirektiivin sekä ns. CER-direktiivin osalta teollisuudella on riskien arviointivelvollisuuden lisäksi lukuisia nimenomaisia velvoitteita ottaa käyttöön konkreettisia riskienhallintatoimia, joiden avulla toimintojen ja tuotannon jatkuvuutta varmistetaan.

Esitämme, että kyseinen kappale muotoiltaisiin tarkemmin kuvaamaan nykytilannetta esimerkiksi seuraavasti:

Varautuminen sekä siihen liittyvä riskien hallinta perustuu lainsäädäntöön, sopimuksiin ja yritysten omaehtoiseen toimintaan. Valtion viranomaisilla ja liikelaitoksilla sekä kunnilla on lakisääteinen velvoite varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen normaaliolojen häiriötilanteissa ja poikkeusoloissa. Valmistavan teollisuuden yrityksillä ei ole yleistä lakiin perustuvaa velvoitetta, joskin keskeisillä sektoreilla EU-sääntely edellyttää runsaasti erilaisia turvallisuusriskien hallintatoimia. Muilta osin varautuminen perustuu ensisijaisesti yritysten omaehtoiseen riskienhallintaan. Tietyillä, mm. puolustusteollisuuden yrityksillä, on lisäksi erilaisia sopimusjärjestelyitä Puolustusvoimien kanssa. Sopimusperusteista varautumista täydentää tiettyjen kriittisten hyödykkeiden (tavarat, materiaalit) lakisääteinen velvoitevarastointi.

Yleiset kommentit strategialuonnokseen.

Kirjoita yleiset havaintosi strategialuonnoksesta.

Lausunto: luonnos Yhteiskunnan turvallisuusstrategiaksi 2024 (YTS2024)

Teknologiateollisuus ry sekä Kyberala (FISC) ry kiittävät mahdollisuudesta lausua asiasta. Lausunto on edellä mainittujen yhteinen.

Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka tekevät puolet Suomen viennistä ja tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Teknologiateollisuuden toimialayhdistys Finnish Information Security Cluster – Kyberala ry edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa.

Yhdymme Puolustus- ja ilmailuteollisuus PIA ry:n lausuntoon. Haluamme lisäksi kiinnittää huomiota muissa kohdissa mainittuihin seikkoihin.

Sund Peter
Finnish Information Security Cluster (FISC) – Kyberala ry -
Teknologiateollisuus ry:n ja Kyberala ry:n yhteinen lausunto