Yrityslainsäädäntö
Markku Rajamäki

Eduskunnan puolustusvaliokunnalle
PuV@eduskunta.fi

Muistio 1 (5)

20.4.2026

Viite: Puolustusvaliokunta tiistai 21.04.2026 klo 10.30 / U 17/2026 vp / Asiantuntijapyyntö 15.4.2026

Elinkeinoelämän keskusliitto EK:n asiantuntijalausunto valtioneuvoston kirjelmästä U 17/2026 vp eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi

Kiitämme mahdollisuudesta tulla kuulluksi.

Pidämme Euroopan komission CSA2- ja NIS2-muutosehdotuksia tavoitteiltaan pääkohdiltaan kannatettavina samoin kuin Suomen U-kirjelmästä ilmenevää ehdotettua Suomen kantaa. On tärkeää, että muuttuneessa maailmantilanteessa huolehditaan yritysten toimintaedellytyksistä ja taloudellisesta turvallisuudesta. EU:n on vähennettävä ulkoisia riskejä turvaamalla samalla EU:n ja jäsenvaltioiden globaali kilpailukyky digitaalisessa siirtymässä ja vahvistamalla yhteiskuntien ja EU:n kriisinsietokykyä. Sääntelyn osalta on tärkeää, että se on selkeää ja mahdollistaa hyvän ennakoitavuuden kyberturvallisuuden valvontaan, sertifiointeihin sekä toimitusketjuriskien hallintaan liittyvissä kysymyksissä.

Kokonaisuuteen liittyy kuitenkin joitakin ehdotuksia, joihin toivomme jatkovalmistelussa kiinnitettävän erityistä huomiota ja että Suomi ajaa näitä näkemyksiä omassa vaikuttamistyössään:

ENISA:n uudet tehtävät ja resurssit

Euroopan unionin kyberturvallisuusvirasto ENISA:lle esitetään huomattavasti laajempia tehtäviä kuin sillä tällä hetkellä on, sekä näiden tehtävien suorittamiseksi merkittäviä rahoitus- ja henkilöresurssilisäyksiä. Huomioiden ENISA:n aiempi suoriutuminen ja mm. tehoton kyberturvallisuuden sertifiointikehyksen hyödyntäminen, pidämme erittäin tärkeänä, että toiminnan tuloksellisuus varmistetaan jatkossa aiempaa paremmin. Pelkkä resurssien lisäys ei sitä takaa.

ENISA:n kaikki tehtävät tulisi käydä läpi ja pyrkiä karsimaan niitä niin, että se voisi jatkossa keskittyä aidosti jäsenvaltioiden ja niissä toimivien yritysten toimintaa tukeviin ja jäsenvaltioiden tehtäviä täydentäviin

tehtäviin, joista jäsenvaltiot eivät selviä yksin tai joita ei ole järkevää hoitaa jäsenvaltioiden tasolla ja toimesta.

ENISA:n uusien tehtävien osalta keskeistä on operatiivisen yhteistyön ja tilannekuvaan liittyvien tehtävien priorisoiminen ja huolellinen muotoilu. Tärkeintä on kehittää ENISA:n valmiuksia hyödyntää kyvykkyyksiään sekä keräämäänsä tietoa kyberuhkien ehkäisyn, havaitsemisen ja datanhaltioiden torjuntatoimien tukemiseen liittyviä tehtäviä varten. Samalla tulee huomioida, että vaikka jäsenvaltioiden välinen tiedonvaihto on tarpeen tietoturvaloukkauksien ehkäisemisessä, selvittämisessä ja mahdollisesti jossain määrin myös torjumisessa, keskeisin työ tehdään datanhaltijoiden (ml. tieto- ja viestintäjärjestelmien haltijat) toimesta. Kyse on siis digitaaliseen tietoon ja -järjestelmiin liittyvästä toimintariskien hallintakyvystä ja ENISA voi parhaimmillaankin vain tukea ko. kyvykkyyksien ylläpitoa.

Viittaamme yksityiskohtien osalta jäsenliittomme Teknologiateollisuus ry:n toimialayhdistys Kyberala ry:n valiokunnalle antamaan lausuntoon.

EU:n kyberturvallisuussertifiointijärjestelmä

Kannatamme EU:n kyberturvallisuussertifiointijärjestelmän uudistamista ehdotuksen mukaisesti. Se on tervetullut ja tärkeä askel kohti selkeämpää, ketterämpää ja vaikuttavampaa eurooppalaista kyberturvallisuuden varmistamista. Ehdotus vahvistaa ENISA:n roolia sertifiointijärjestelmien laadinnassa, teknisessä ylläpidossa ja kehittämisessä, mikä parantaa järjestelmien ajantasaisuutta sekä varmistaa, että ne vastaavat nopeasti muuttuvaan uhkaympäristöön ja teknologiseen kehitykseen.

On tärkeää ja ehdottoman kannatettavaa, että sertifioinnit säilyvät jatkossakin vapaaehtoisina. Vapaaehtoisen järjestelmän hyväksyttävyyden kannalta on erityisen tärkeää, että sertifioinnin hankkimisen kustannukset säilyvät työn ja kustannusten osalta houkuttelevalla tasolla. Tällöin sertifioinnista muodostuu entistä hyödyllisempi väline yrityksille, jotka voivat sen avulla osoittaa vaatimustenmukaisuutensa useiden EU-säädösten alla yhdenmukaisesti ja pienemmällä hallinnollisella taakalla.

NIS2 -muutosdirektiiviehdotuksen mukaan jäsenvaltiot voisivat edellyttää toimijoita hankkimaan sertifioinnin vaatimustenmukaisuuden osoittamiseksi, jolloin sertifioinnin hankkineeseen toimijaan ei kohdistettaisi säännöllisiä turvallisuusauditointeja. Tätä tulisi selvittää jatkovalmistelussa tarkemmin. Lopputuloksena ei saa olla käytännössä pakollinen sertifiointi. Joissain tilanteissa ilman sertifikaattia toimija voisi altistua jatkuvalle valvonnalle, jonka kustannukset voisivat ylittää sertifioinnin hankkimisen kustannukset.

Lisäksi painotamme sitä, että sertifiointivaatimusten tulee olla aidosti riskiperustaisia. Vaaditun turvallisuuden tason toteutuminen on olennaista, mutta sen toteutumiseen johtavien turvallisuuskontrollien ja -toimien kokonaisuuden tulee lähtökohtaisesti aina jäädä toimijan itsensä päätettäväksi. Useimmissa tapauksissa vaadittu turvallisuuden taso voidaan saavuttaa useammanlaisella kontrollien ja toimien kokonaisuudella. Sen vuoksi keskeistä on sen arviointi, miten kontrollien ja toimien kokonaisuus vaikuttaa riskiin, eikä se, että valvottava käyttäisi tai soveltaisi juuri tiettyjä kontrolleja ja toimia.

Näiltä osin vaikutustenarviointiin on jatkovalmistelussa kiinnitettävä erityistä huomiota.

ICT-toimitusketjujen turvallisuuden hallinta

Pidämme ehdotettua EU-tasoista ICT-toimitusketjujen turvallisuuden hallinnan mekanismia sinällään tarpeellisena. Perusteet tälle on esityksessä mielestämme avattu kattavasti.

Painotamme sitä, että ICT-toimitusketjuja koskevien rajoitusten ja teknisten velvoitteiden on oltava riskiperusteisia, oikeasuhtaisia ja teknisesti toteuttamiskelpoisia. Järjestelmien ja laitteiden elinkaari sekä palvelujen kapasiteetti ja jatkuvuus on huomioitava, kun velvoitteita ja siirtymäaikoja asetetaan.

Komissio on arvioinut, että tiettyjen korkean riskin toimittajien osien vaihtamisesta aiheutuvat vuosittaiset kustannukset kolmen vuoden aikajänteellä olisivat 3,4–4,3 miljardin euron luokassa matkaviestinverkkojen operaattoreille. Samalla investoinnit luotettuihin toimittajiin kasvaisivat vuosittain enimmillään 2 miljardiin euroon vuodessa. Ehdotuksella saattaa olla vaikutusta jäsenvaltioiden mahdolliseen korvausvelvollisuuteen.

Sen sijaan komissio ei ole tarkemmin arvioinut mahdollisia kustannuksia muille NIS2-direktiivin toimialoille, joihin ICT-toimitusketjuja koskevat velvoitteet kohdistuisivat. Vaikutukset riippuvat myös siitä, milloin verkkolaitteiden käyttöä koskevat rajoituksen tulisivat voimaan. Näihin liittyvä vaikutustenarvioinnin riittämättömyys on merkittävä puute esityksessä.

Jatkovalmistelussa on kiinnitettävä erityistä huomiota riskiperusteisuuteen, oikeasuhtaisuus- ja suhteellisuusperiaatteisiin sekä vaikutustenarviointiin kokonaisuutena. Korvauskysymyksiä on ehdotuksessa tarkasteltu vielä täysin riittämättömästi, joten niitä tulee täsmentää ja täydentää merkittävästi.

Luovutettavien tietojen minimointi

Mitä tulee mahdolliseen kieltoon käyttää korkean riskin toimittajien ICT-komponentteja, valtioneuvosto on kattavasti arvioinut komission ehdotusta U-kirjelmässä ja on mm. todennut, että sen "voidaan arvioida olevan merkityksellinen perustuslain 12 §:n 2 momentin mukaisen julkisuusperiaatteen ja salassa pidettävien tietojen luovuttamisen kannalta. Asetuksen mukainen tietojen luovuttaminen saattaisi edellyttää salassa pidettävien tietojen luovuttamista ENISA:lle, EU:n komissiolle sekä muille jäsenmaille. Komissio ei ole tarkemmin arvioinut salassa pidettävien tietojen ja tiedonvaihdon merkitystä.".

CSA2-esitys laajentaa muutenkin merkittävästi tiedonluovutusvelvoitteita suhteessa ENISA:an, komissioon ja kansallisiin valvontaviranomaisiin.

On selvää, että salassapitoon ja tiedonvaihtoon liittyviä näkökohtia ja rajoitteita on välttämätöntä jatkovalmistelussa käsitellä ja täydentää. Kaikenlaisen tiedon luovuttamisen on perustuttava perusteltuun tarpeeseen ja luovutettavien tietojen riskit on arvioitava etukäteen. Erityisen tärkeää on varmistaa, ettei sääntelyn toimeenpano edellytä verkkoarkkitehtuurin tai vastaavan tyyppisten, kriittisten teknisiä yksityiskohtia sisältävien tietojen tarpeettoman yksityiskohtaista luovuttamista.

On myös huomioitava, että luovutettavien tietojen laajentaminen lisää soveltamisalaan kuuluvien yritysten hallinnollista taakkaa, mikä tulee huomioida vaikutustenarvioinneissa.

Komissiolle siirrettävä täytäntöönpanovalta

Puheena olevat ehdotukset lisäävät merkittävästi komissiolle siirrettävää säädösvaltaa. Valtioneuvosto toteaa, että komissiolle delegoitavien toimivaltuuksien tulisi olla tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja perusteltuja. Näkemystä olisi kuitenkin perusteltua täsmentää ja lausua asiasta yksityiskohtaisemmin.

NIS 2 -muutosdirektiivissä komissiolle ehdotetaan mahdollisuutta antaa riskienhallintatoimenpiteistä täysharmonisoivia täytäntöönpanosäädöksiä. Tämä poikkeaisi NIS 2 -direktiivin luonteesta vähimmäisharmonisoivana säädöksenä ja kaventaisi merkittävästi jäsenvaltioiden liikkumavaraa. Kirjelmässä tähän suhtaudutaan alustavan varauksellisesti.

Komissiolle esitetään merkittävää resurssilisäystä (50 henkilötyövuotta). Merkittävä osa lisäresursseista kohdistuu ICT-toimitusketjujen riskiarviointeihin ja sertifiointeihin, eli juuri niihin toimintoihin, joissa komissio käyttää teknistä säädösvaltaa. Tämä korostaa jäsenvaltioiden osallistumisen ja toimialojen asiantuntemuksen merkitystä.

Ehdotus sisältää lisäksi huomattavan määrän täytäntöönpanosäädöksiä, joita valmisteltaisiin komitologiamenettelyissä. Teknisten täytäntöönpanoasetusten markkinavaikutukset voivat olla välittömiä, minkä vuoksi valmistelun läpinäkyvyys, perustelut ja toimialojen kuuleminen ovat olennaisia. Esitämme, että valiokunta kiinnittää lausunnossaan huomiota siihen, että valtioneuvoston on neuvotteluissa suhtauduttava kriittisesti täysharmonisoiviin täytäntöönpanosäädöksiin riskienhallintatoimenpiteistä, varmistettava ENISA:n, jäsenvaltioiden ja toimialan asiantuntemuksen hyödyntäminen komission teknisten säädösten valmistelussa sekä huolehdittava siitä, että komissiolle siirrettävä täytäntöönpanovalta on tarkkarajaista ja komitologiamenettelyt läpinäkyviä.

Kyberturvallisuuskeskuksen resurssit

Lopuksi toteamme, että kyberturvallisuudessa suomalaisista viranomaisista erityisesti Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen rooli on aivan keskeinen. Sille on tullut viime vuosien lainsäädäntömuutosten myötä myös lisätehtäviä. Nyt esitetyt muutokset saattavat toteutuessaan osin vähentää, mutta esim. mahdollisten lisätiedonjakoa ja -raportointia ENISA:lle edellyttävien tehtävien osalta myös mahdollisesti lisätä Kyberturvallisuuskeskuksen tehtäviä nykyisestä. On erittäin tärkeää, että Kyberturvallisuuskeskuksen resurssoinnista huolehditaan niin, että se kykenee selviytymään kaikista lakisääteisistä tehtävistään. Niistä monet ovat suomalaisyrityksille erittäin tärkeitä.

Sama koskee myös muita, mm. NIS2-valvovia viranomaisia, joille esitysten toteutumisen myötä tulisi uusia valvonta- ja täytäntöönpanotehtäviä.