Euroopa Liidu
Nõukogu

Brüssel, 14. september 2017
(OR. en)

Institutsioonidevaheline dokument:
2017/0225 (COD)

12183/17
ADD 2

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Jordi AYET PUIGARNAU, direktor
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	SWD(2017) 501 final
Teema:	KOMISJONI TALITUSTE TÖÖDOKUMENT MÕJUHINNANGU KOMMENTEERITUD KOKKUVÕTE *Lisatud dokumendile:* Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“)

Käesolevaga edastatakse delegatsioonidele dokument SWD(2017) 501 final.

Lisatud.: SWD(2017) 501 final

EUROOPA
KOMISJON

Brüssel, 13.9.2017
SWD(2017) 501 final

KOMISJONI TALITUSTE TÖÖDOKUMENT

MÕJUHINNANGU KOMMENTEERITUD KOKKUVÕTE

Lisatud dokumendile:

Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. VAJADUS MEETMETE JÄRELE

Mis on lahendamist vajav probleem ja miks see on probleem?

Digitaaltehnoloogia ja internet on ELi majanduse ja ühiskonna alustalad. Sellised elutähtsad majandussektorid nagu transport, energeetika, tervishoid ja rahandus on oma põhitegevuses hakanud üha enam sõltuma võrgu- ja infosüsteemidest. Asjade internet ühendab sidevõrkude abil esemeid ja inimesi. See uus olukord tekitab enneolematuid võimalusi, aga ka nõrkusi. Küberturvalisuse intsidente esineb tõepoolest väga sagedasti. Nende keerukus, sagedus ja mõju ulatus – alates elutähtsatele teenustele juurdepääsu saamisest kuni demokraatlike protsesside mõjutamiseni – suureneb kindlasti veelgi.

Selles kontekstis on kindlaks tehtud järgmised omavahel seotud probleemid.

- Liikmesriikide killustatud tegevuspõhimõtted ja lähenemisviisid küberturvalisuse valdkonnas.
- ELi institutsioonide, organite ja asutuste poolt küberturvalisuse jaoks eraldatavate ressursside ja kasutatavate lähenemisviiside hajusus.
- Kodanikud ja ettevõtjad ei ole küberohtudest piisavalt teadlikud ning neil ei ole piisavalt teavet ostetud IKT toodete ja teenuste turvaomaduste kohta, samal ajal võetakse kasutusele üha enam riiklikke ja valdkondlikke sertifitseerimiskavasid.

Need probleemid mõjutavad ELi üldist kübervastupidavusvõimet ja siseturu tulemuslikku toimimist.

Mis tuleks saavutada?

Algatuse konkreetsed poliitikaeesmärgid on järgmised.

1. Suurendada liikmesriikide ja ettevõtjate suutlikkust ja valmisolekut, eelkõige elutähtsa taristu puhul.
2. Parandada koostööd ja koordineerimist liikmesriikides ning ELi institutsioonides, organites ja asutustes.
3. Suurendada ELi tasandil suutlikkust täiendada liikmesriikide võetavaid meetmeid, eelkõige piirüleste küberkriiside puhul.
4. Suurendada kodanike ja ettevõtjate teadlikkust küberturvalisusega seotud küsimustest.
5. Suurendada IKT toodete ja teenuste küberturvalisuse alase usaldusväärsuse üldist läbipaistvust, et suurendada usaldust digitaalse ühtse turu ja digitaalse uuendustegevuse vastu.
6. Vältida sertifitseerimiskavade killustatust ELis ning nendega seotud turvanõuete ja hindamiskriteeriumide killustatust liikmesriikides ja sektorites.

Milline on ELi tasandi meetmete lisaväärtus?

Kuna majanduse ja ühiskonna digiteerimisel ning omavahelisel ühendamisel on ülemaailmne ulatus, ületab probleemide mõõde kaugelt ühe liikmesriigi territooriumi. Seetõttu on vaja

sekkuda liidu tasandil. Praeguses kontekstis ja tulevikustsenaariume arvesse võttes näib, et liikmesriikide endi võetavad meetmed ja killustatud lähenemisviis küberturvalisusele ei saa eelkõige selle märkimisväärse piiriülese mõõtme tõttu suurendada ühist kübervastupidavusvõimet liidus.

B. LAHENDUSED

Millised on eri võimalused eesmärkide saavutamiseks? Kas on olemas eelistatud variant?

Selles mõjuhinnangus käsitletakse konkreetset poliitikameetmete komplekti, mis hõlmab Euroopa Liidu Võrgu- ja Infoturbeameti (edaspidi „ENISA“) läbivaatamist ning IKT turvalisuse sertifitseerimist.

ENISA läbivaatamine

Variant 0 – **lähtestsenaarium**. Selle variandi puhul säilitataks praegust olukorda. ENISA mandaati pikendataks ning ameti eesmärgid ja ülesanded jääksid üldjoontes muutumatuks, võttes arvesse ENISA-le edasiste ELi õigusaktidega (näiteks võrgu- ja infoturbe direktiiv) antavaid ülesandeid.

Variant 1 – **ENISA mandaadi lõpetamine** (ENISA tegevuse lõpetamine). Selle variandi puhul lõpetataks ENISA tegevus ameti mandaadi lõpus (2020. aasta juunis) ning võimalik, et selle pädevused/tegevusvaldkonnad jaotataks ümber ELi ja/või riiklikul tasandil.

Variant 2 – **reformitud ENISA**. Selle variandi puhul tuginetaks ENISA praegusele mandaadile, et teha valikulised muudatused, mille puhul võetaks arvesse küberturvalisuse keskkonna muutumist. Amet saaks alalise mandaadi, mis tugineks järgmistele peamistele alustele: toetus ELi poliitika kujundamisele ja rakendamisele, suutlikkuse arendamine, teadmised ja teave, turuga seotud ülesanded, teadusuuringud ja innovatsioon ning operatiivkoostöö ja kriisiohjamine.

Variant 3 – **täieliku tegevusvõimega ELi küberturvalisuse amet**. Selle variandi puhul reformitaks ENISA nii, et see hakkaks täitma kolme peamist ülesannet: 1. poliitikakujundamise/nõustamise ülesanne, 2. teabe- ja eksperdikeskus ning 3. infoturbeintsidentidega tegelev rühm (CERT). Selle variandi puhul muudetaks mandaadi ulatust üldjoontes samal moel kui variandi 2 puhul. Samas antaks ametile intsidentidele reageerimise ja kriisiohje valdkonnas lisaülesandeid, mille tulemusena hõlmaks amet kogu küberturvalisuse olelusringi ning tegeleks küberturvalisuse intsidentide ärahoidmise, avastamise ja neile reageerimisega.

Sertifitseerimine

Variant 0 – lähtestsenaarium (midagi ei tehta). Selle variandi puhul säilitaks komisjon hetkeolukorra ja ei võtaks mingeid poliitika- ega seadusandlikke meetmeid.

Variant 1 – **muud kui seadusandlikud (pehme õiguse) meetmed**. Selle variandi alusel kasutaks komisjon pehme õiguse poliitikameetmeid (näiteks tõlgendavad teadaanded, toetus ELi-ülestele eneseregulеerimise algatustele ja standardimine), et suurendada läbipaistvust ja vähendada killustatust.

<u>Variant 2</u> – ELi õigusakt, millega laiendatakse korralduskomitee kõrgemate ametnike infosüsteemide turbe rühma (edaspidi „SOG-IS“) kokkulepet kõikidele liikmesriikidele. Selle poliitikavariandi alusel teeks komisjon seadusandliku akti ettepaneku, et õiguslikult laiendada liikmesust kõikidele liikmesriikidele.

<u>Variant 3</u> – ELi üldine IKT turvalisuse sertifitseerimise raamistik. Selle variandi puhul loodaks Euroopa IKT turvalisuse sertifitseerimise raamistik (sealhulgas riigi ametiasutustest koosnev eksperdirühm), tuginedes võimalikult suurel määral olemasolevatele IKT turvalisuse sertifitseerimise kavadele. Raamistik võimaldaks sisuliselt luua ELi sertifitseerimiskavad, mida tunnustataks kõikides liikmesriikides.

Eelistatud variant on kombinatsioon ENISA puhul variandi 2 ja sertifitseerimise puhul variandi 3 kasutamisest.

Millised on erinevad sidusrühmad? Kes millist varianti toetab?

Valdav enamik sidusrühmadest kõikides konsultatsioonis osalenud kategooriates (liikmesriigid, tööstus, ELi institutsioonid, teaduskogukond) näivad toetavat eelistatud varianti, kuna nad pooldavad ENISA tugevdamist ja Euroopa IKT turvalisuse sertifitseerimise raamistiku loomist.

Eelkõige ollakse üksmeelel, et on vaja (vähemalt) alalise mandaadiga hästi toimivat ELi ametit, millel on piisavad ressursid ja volitused, et tulla toime praeguste ja tulevaste väljakutsetega küberturvalisuse valdkonnas. Sidusrühmad on ka laialdaselt nõus, et tuleb luua vabatahtlik ja kohandatava ulatusega Euroopa raamistik.

Tööstusvaldkonnas toetavad seda sertifitseerimise lahendust ettevõtjad, kelle suhtes juba kohaldatakse sertifitseerimisnõudeid ja kes saaksid kasu sertifikaatide vastastikusel tunnustamisel põhinevast ELi-ülesest mehhanismist. Seda toetavad ka VKEd, kes kannatavad kõige rohkem, kui nad on juba pidanud või peaksid hankima erinevates liikmesriikides erinevad sertifikaadid. Teatavad liikmesriigid ja eelkõige need, kellel on vähem ressursse, ning teatavad tööstusvaldkonna ja ELi institutsioonide esindajad andsid positiivse hinnangu ka ENISA puhul variandi 3 kasutamisele.

C. ELISTATUD POLIITIKAVARIANDI MÕJU

Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel juhul peamiste poliitikavariantide) eelised?

Eelistatud variandi alusel oleks ELil amet, mis keskendub liikmesriikide, ELi institutsioonide ja ettevõtjate toetamisele valdkondades, kus see annab kõige rohkem lisaväärtust. Need valdkonnad on järgmised: toetus võrgu- ja infoturbe direktiivi rakendamisele, poliitika kujundamine ja rakendamine, teave, teadmised ja teadlikkus, teadusuuringud, operatiivkoostöö ja kriisiohjamine ning turg. Eelkõige toetaks ENISA ELi poliitikat IKT turvalisuse sertifitseerimise valdkonnas, tagades Euroopa IKT turvalisuse sertifitseerimise raamistiku haldusliku käigushoidmise ja tehnilise juhtimise. Selle raamistikuga kehtestatakse tulemuslikult ELis IKT turvalisuse sertifitseerimist reguleerivate õigusnormide komplekt, millega edendatakse liikmesriikide väljastatud sertifikaatide vastastikuse tunnustamise süsteemi. Ollakse seisukohal, et ELi jaoks on kõige tõhusam need variandid kombineerida, et

saavutada järgmised kindlaks määratud eesmärgid: suurem suutlikkus küberturvalisuse valdkonnas, valmisolek, koostöö, teadlikkus, läbipaistvus ning turu killustatuse vältimine. See variant on ka kõige paremini kooskõlas poliitiliste prioriteetidega, kuna see lähtub küberjulgeoleku strateegiast ja sellega seotud poliitikast (näiteks võrgu- ja infoturbe direktiiv) ning digitaalse ühtse turu strateegiast. Lisaks sellele võimaldaks see variant saavutada eesmärgid ressursse mõistlikult kasutades.

Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) kulud?

Uutest ülesannetest hoolimata jääks reformitud ENISA paindlikuks organisatsiooniks. ELi eelarvest antav rahaline panus oleks praegusest suurem, aga siiski märkimisväärselt väiksem teiste elutähtsates valdkondades tegutsevate ametite omast.

Euroopa IKT turvalisuse sertifitseerimise raamistiku loomine ei tähendaks täiendavate algkulude tekkimist tööstusvaldkonnale (sealhulgas VKEdele). See võimaldaks hoopis märkimisväärset säästu neile ettevõtjatele, kes on oma tooted juba sertifitseerinud või on valmis turvalisuse sertifikaadi hankima, ning avaldaks kasulikku mõju nende konkurentsivõimele kõikjal maailmas. Teisest küljest tekiksid teatavad eelarvelised kulukohustused, et tagada raamistiku käigushoidmine, mis toimuks tehniliste ja sekretariaadi ülesannete puhul eelkõige reformitud ENISA mudeli alusel.

Kas on ette näha märkimisväärset mõju riigieelarvetele ja ametiasutustele?

Ei. ENISA tugevdamisest tekkivad kulud kaetaks peamiselt ELi eelarvest ning liikmesriigid saaksid ka edaspidi vabatahtlikult ametit rahastada. Sertifitseerimise puhul tuleneb peamine mõju liikmesriikide eelarvetele ja ametiasutustele vajaduse korral sertifitseerimisasutuse loomisest.

Kas on oodata muud olulist mõju?

Ei.

Proportsionaalsus?

Eelistatud variant sisaldab tasakaalustatud meetmeid, mida kõiki peetakse seatud eesmärgi saavutamiseks vajalikuks, ilma et sellest tuleneks liigne koormus asjaomastele sidusrühmadele. Seda arvesse võttes vastab algatus proportsionaalsuse põhimõttele.

D. JÄRELMEETMED

Millal poliitika läbi vaadatakse?

Tehakse ettepanek, et esimene hindamine toimub viis aastat pärast õigusakti jõustumist. Komisjon esitab seejärel Euroopa Parlamendile ja nõukogule hindamise kohta aruande, lisades sellele vajaduse korral läbivaatamise ettepaneku. Edasised hindamised toimuvad iga viie aasta tagant.