Euroopa Liidu
Nõukogu

Brüssel, 18. detsember 2020
(OR. en)

Institutsioonidevaheline dokument:
2020/0359(COD)

14150/20
ADD 3

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	16. detsember 2020
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	SWD(2020) 344 final
Teema:	KOMISJONI TALITUSTE TÖÖDOKUMENT MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE Lisatud dokumendile: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv 2016/1148

Käesolevaga edastatakse delegatsioonidele dokument SWD(2020) 344 final.

Lisatud: SWD(2020) 344 final

EUROOPA
KOMISJON

Brüssel, 16.12.2020
SWD(2020) 344 final

KOMISJONI TALITUSTE TÖÖDOKUMENT

MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE

Lisatud dokumendile:

Ettepanek:
EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV,

mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Kommenteeritud kokkuvõte

Mõjuhinnang *6. juuli 2016. aasta direktiivi (EL) 2016/1148 (mis käsitleb meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) läbivaatamise* kohta

A. Vajadus meetmete järele

Milles probleem seisneb ja miks see on ELi tasandi probleem?

Küberturvalisuse direktiiv, mis sillutas paljudes liikmesriikides teed olulisele mõtteviisi muutusele ning pani aluse institutsioonilise ja regulatiivse lähenemisviisi kujunemisele küberturvalisuse valdkonnas, on andnud küll märkimisväärseid tulemusi, kuid selle võimalused on osutunud piiratuks. Ühiskonna digiüleminek (mida võimendas COVID-19 kriis) on ohumaastikku laiendanud ning toonud kaasa uusi probleeme, mis nõuavad kohandatud ja uuenduslikke lahendusi. Küberrünnete arv kasvab endiselt, need on üha keerukamad ning pärinevad paljudest eri allikatest nii ELis kui ka mujal.

Tuginedes küberturvalisuse direktiivi toimivuse hindamisele, tuvastati mõjuhinnanguga järgmised probleemid: ELis tegutsevate ettevõtjate kübervastupidavusvõime madal tase ; ebaühtlane vastupidavusvõime tase liikmesriikide ja sektorite tasandil ning ühise olukorrateadlikkuse madal tase ja ühistegevuse puudulikkus kriisidele reageerimisel. Näiteks on mõne nimetatud probleemi ja teguri tõttu olukord selline, et mõne liikmesriigi teatavad suurhaiglad ei kuulu küberturvalisuse direktiivi kohaldamisalasse ega ole seega kohustatud sellest tulenevaid turvameetmeid rakendama, samas kui mõnes teises liikmesriigis kohaldatakse küberturvalisuse direktiivi nõudeid peaaegu igas haiglas.

Mis tuleks saavutada?

Küberturvalisuse direktiivi läbivaatamise kolm üldeesmärki on järgmised:

1. **Suurendada Euroopa Liidus kõigis asjaomastes sektorites tegutsevate ettevõtjate (ulatusliku kogumi) kübervastupidavusvõimet,** kehtestades eeskirjad, millega tagatakse, et kõik siseturul tegutsevad avaliku ja erasektori üksused, kes täidavad majanduse ja ühiskonna kui terviku jaoks olulisi ülesandeid, peavad võtma asjakohaseid küberturvalisuse meetmeid.
2. **Vähendada vastupidavusvõime taseme ebaühtlust siseturul direktiiviga juba hõlmatud sektorites,** ühtlustades täiendavalt 1) tegelikku kohaldamisala, 2) turvanõudeid ja intsidentidest teatamise nõudeid, 3) riiklikku järelevalvet ja täitmise tagamist reguleerivaid sätteid ning 4) liikmesriikide pädevate asutuste suutlikkust.
3. **Tõsta ühise olukorrateadlikkuse taset ning suurendada ühist valmisolekut ja reageerimissuutlikkust,** võttes meetmeid usalduse suurendamiseks pädevate asutuste vahel, jagades rohkem teavet ning kehtestades eeskirjad ja menetluskorra ulatuslike intsidentide või kriisi korral tegutsemiseks.

Milline on ELi tasandil meetmete lisaväärtus (subsidiaarsus)?

Kübervastupidavusvõime ei saa olla kogu liidus ühtlaselt tõhus, kui seda käsitletakse eri lähenemisviise rakendades ja riiklikult või piirkondlikult kapseldudes. Küberturvalisuse direktiiviga püüti seda puudust kõrvaldada, kehtestades võrgu- ja infosüsteemide turvalisuse raamistiku riikide ja liidu tasandil. Direktiivi ülevõtmisel ja kohaldamisel ilmnesid siiski ka teatavate sätete või lähenemisviiside olemuslikud puudused, näiteks küberturvalisuse direktiivi kohaldamisala ebaselge piiritletus. Lisaks on Euroopa majanduse sõltuvus võrgu- ja infosüsteemidest COVID-19 kriisi tekkimisest alates suurenenud ning sektorid ja teenused on omavahel üha rohkem seotud. Küberturvalisuse direktiivi esimene korrapärane läbivaatamine lõi seega võimaluse töötada välja täiendavad ELi meetmed. ELi sekkumine suuremas

ulatuses, kui küberturvalisuse direktiivi praegused meetmed ette näevad, on põhjendatav peamiselt järgmisega: i) probleemi piiriülene olemus; ii) ELi meetmete potentsiaal edendada ja hõlbustada tõhusat riiklikku poliitikat; iii) kooskõlastatud ja koostööl põhinevate küberturvalisuse alaste poliitikameetmete panus andmekaitse ja eraelu puutumatuse tõhusasse kaitsesse.

B. Lahendused

Millised on eri võimalused eesmärkide saavutamiseks? Kas on olemas eelistatud variant? Kui ei, siis miks?

Mõjuhinnangu tegemisel analüüsiti nelja poliitikavarianti: 0) praeguse olukorra säilitamine; 1) muude kui seadusandlike meetmete võtmine, et ülevõtmist ühtlustada; 2) küberturvalisuse direktiivi piiratud ulatuses muutmine täiendavaks ühtlustamiseks; 3) küberturvalisuse direktiivis süsteemsete ja struktuuriliste muudatuste tegemine. Poliitikavariant 1 jäeti kõrvale varases etapis, kuna see praegust olukorda märkimisväärselt ei muudaks. Mõjuhinnanguga jõutakse järeldusele, et **eelistatud poliitikavariant** on variant 3 (**küberturvalisuse direktiivis süsteemsete ja struktuuriliste muudatuste tegemine**), kuna sellega nähakse ette põhimõttelisem lähenemisviisi nihe laiema majandussegmendi hõlmamiseks kogu liidus ning seejuures sihipärasem järelevalve, mis on suunatud proportsionaalselt suurtele ja peamistele ettevõtjatele, ning kohaldamisala selge piiritlemine. Samuti optimeeritaks ja ühtlustataks sellega ettevõtjatele pandud turbekohustusi, loodaks tegevuslike aspektide jaoks tõhusam raamistik, antaks asjaomastele osapooltele selge lähtekoht vastutuse ja aruandluskohustuse jagamiseks ning soodustataks teabevahetust.

Millised on eri sidusrühmade seisukohad? Kes millist varianti toetab?

Enamik pädevaid asutusi ja ettevõtjaid toetas küberturvalisuse direktiivi läbivaatamist. Mitme konsultatsiooni käigus täheldasid nad, et läbivaadatud küberturvalisuse direktiiv peaks hõlmama lisa(all)sektoreid ning ühtlustama või optimeerima täiendavalt turvameetmeid ja aruandluskohustusi. Sidusrühmad avaldasid toetust ka uutele kontseptsioonidele või poliitilistele meetmetele, mis on vaid osa eelistatud poliitikavariandist (nt tarneahela turvalisuse põhimõtted, ELi operatiivse kriisiohjamise raamistiku institutsionaliseerimine).

C. Eelistatud poliitikavariandi mõju

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

Eelistatud poliitikavariant tooks märkimisväärset kasu: hinnangute kohaselt, mis põhinevad küberturvalisuse direktiivi läbivaatamise toetuseks korraldatud uuringu raames välja töötatud majandusmudelil, võib eelistatud poliitikavariant vähendada küberturvalisuse intsidentidega seotud kulusid 11,3 miljardi euro võrra.

Küberturvalisuse raamistikuga laiendataks sektoripõhist kohaldamisala märkimisväärselt, kuid lisaks mainitud eelistele kaasneb küberturvalisuse nõuetega koormus (eelkõige järelevalve aspektist), mida tasakaalustataks nii uute hõlmatud üksuste kui ka pädevate asutuste jaoks. Seda tänu asjaolule, et uue küberturvalisuse raamistikuga kasutataks kahetasandilist lähenemisviisi, keskendudes suurtele ja peamistele üksustele ning rakendades diferentseeritud järelevalvekorda, mis võimaldab suure hulga üksuste, nimelt olulisena (mitte elutähtsana) käsitatavate üksuste suhtes kohaldada järelevalve järelkontrollimeetmeid (nn *ex-post*-järelevalve, mis tähendab reageerivat lähenemist ega hõlma üldist kohustust nõuetele vastavust süstemaatiliselt dokumenteerida).

Kokkuvõttes saavutataks selle poliitikavariandiga soodsad kompromissid ja tõhusad sünergiad ning sellel

oleks kõigist analüüsitud poliitikavariantidest suurim potentsiaal tagada, et kogu liidu ulatuses saavutatakse võtmetähtsusega üksuste kübervastupidavusvõime kõrgem ja ühtlasem tase, mis lõppkokkuvõttes tähendaks nii ettevõtjate kui ka ühiskonna jaoks kulude kokkuhoidu.
Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) kulud?
Eelistatud poliitikavariandi rakendamine tähendaks asjaomaste liikmesriikide ametiasutustele teatavaid nõuete järgimise ja täitmise tagamisega seotud kulusid (hinnanguliselt suureneb ressursivajadus kokku ligikaudu 20–30 %). Samas tooks uus raamistik märkimisväärset kasu ka selle kaudu, et tagaks olulistest ettevõtjatest parema ülevaate ja nendega tõhusama suhtlemise, tulemuslikuma piiriülese operatiivkoostöö ning vastastikuse abistamise ja vastastikuse hindamise mehhanismid. Selle tulemusena tõuseks liikmesriikide küberturvalisuse alase suutlikkuse üldine tase. Küberturvalisuse raamistiku kohaldamisalasse hõlmatavad ettevõtjad peaksid esimestel aastatel pärast küberturvalisuse raamistiku jõustumist suurendama oma IKT-turbega seotud kulutusi maksimaalselt 22 % võrra (need ettevõtjad, kes juba kuuluvad praegu kehtiva küberturvalisuse direktiivi kohaldamisalasse, 12 % võrra). IKT-turbega seotud kulutuste keskmine suurenemine tooks samas kaasa proportsionaalse investeeringukasu, eelkõige tänu küberturvalisuse intsidentidega seotud kulude märkimisväärsele vähenemisele (hinnanguliselt kuni 11,3 miljardit eurot kümne aasta jooksul).
Milline on mõju VKEdele ja konkurentsivõimele?
Väike- ja mikroettevõtted jäetaks eelistatud poliitikavariandi puhul küberturvalisuse raamistiku kohaldamisalast välja. Keskmise suurusega ettevõtjate IKT-turbega seotud kulutused esimestel aastatel pärast uue küberturvalisuse raamistiku kasutuselevõttu eelduste kohaselt suurenevad. Samas soodustaks nende üksuste turvanõuete taseme tõstmine ka nende küberturvalisuse alase suutlikkuse suurenemist ja aitaks tõhustada nende IKT-alast riskijuhtimist.
Kas on ette näha märkimisväärset mõju riigieelarvetele ja ametiasutustele?
Oodatav mõju liikmesriikide eelarvetele ja haldusasutustele: lühikese ja keskpika perspektiivi prognoosi kohaselt suureneb ressursivajadus hinnanguliselt ligikaudu 20–30 %.
Kas on oodata muud olulist mõju?
Muud olulist negatiivset mõju ei ole ette näha. Eelistatud poliitikavariandi rakendamisega peaks saavutatama suurem küberturvalisuse alane suutlikkus ning seeläbi peaks oluliselt vähenema intsidentide, sealhulgas andmetega seotud rikkumiste arv ja raskusaste. Samuti avaldab see tõenäoliselt positiivset mõju kõikide küberturvalisuse raamistiku kohaldamisalasse kuuluvate üksuste jaoks võrdsete tingimuste tagamisele kõigi liikmesriikide ulatuses ning vähendab küberturvalisuse alase teabega seotud ebaühtlust.
Proportsionaalsus
Eelistatud variandiga ei mindaks kaugemale sellest, mis on vajalik erieesmärkide rahuldavaks saavutamiseks. Kavandatav julgeolekumeetmete ja aruandluskohustuste vastavusse viimine ja optimeerimine lähtub liikmesriikide ja ettevõtjate taotlusest praegust raamistikku parandada.

D. Järelmeetmed
Millal poliitika läbi vaadatakse?
Esimene läbivaatamine toimuks 54 kuud pärast õigusakti jõustumist. Komisjon esitaks Euroopa Parlamendile ja nõukogule läbivaatamise kohta aruande. Läbivaatamine valmistataks ette ENISA ja koostöörühma toetusel.