Euroopa Liidu
Nõukogu

Brüssel, 16. september 2022
(OR. en)

Institutsioonidevaheline dokument: 2022/0272(COD)

12429/22
ADD 6

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	15. september 2022
Saaja:	Nõukogu peasekretariaat
Komisjoni dok nr:	SWD(2022) 283 final
Teema:	KOMISJONI TALITUSTE TÖÖDOKUMENT MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE Kübervastupidavusvõime määrus Lisatud dokumendile: Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020

Käesolevaga edastatakse delegatsioonidele dokument SWD(2022) 283 final.

Lisatud: SWD(2022) 283 final

EUROOPA
KOMISJON

Brüssel, 15.9.2022
SWD(2022) 283 final

KOMISJONI TALITUSTE TÖÖDOKUMENT

MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE

Kübervastupidavusvõime määrus

Lisatud dokumendile:

Ettepanek: Euroopa Parlamendi ja nõukogu määrus,

mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Kommenteeritud kokkuvõte (kuni 2 lk)

Mõjuhinnang kübervastupidavusvõime määruse kohta

A. Vajadus meetmete järele

Mis on probleem ja miks on tegemist ELi tasandi probleemiga?

Riist- ja tarkvaratooteid tabavad sageli edukad küberründed; nende tõttu suurenes küberkuritegevuse hinnanguline ülemaailmne kulu 2021. aastaks 5,5 triljoni euroni aastas. Neid tooteid mõjutavad kaks põhiprobleemi, mis suurendavad kasutajate ja ühiskonna kulusid: 1) küberturvalisuse madal tase, mida kajastavad levinud nõrkused ning ebapiisavad ja ebajärjekindlad turvauuendused nende kõrvaldamiseks, ning 2) kasutajate ebapiisav arusaamine ja juurdepääs teabele, mis takistab neil valida nõuetekohaste küberturvalisuse omadustega tooteid või kasutada neid turvalisel viisil.

Digielemente sisaldavate toodete küberturvalisusel on tugev piiriülene mõõde, kuna ühes riigis toodetud tooteid kasutatakse sageli kogu siseturul. Lisaks levivad algselt üht üksust või liikmesriiki mõjutanud intsidendid sageli minutite jooksul üle kogu siseturu.

Kuigi teatavate digielemente sisaldavate toodete suhtes kohaldatakse kehtivaid siseturgu käsitlevaid õigusakte, ei ole enamik riist- ja tarkvaratooteid praegu hõlmatud ühegi ELi õigusaktiga, mis käsitleks nende küberturvalisust. Eelkõige ei käsitleta praeguses ELi õigusraamistikus sisseehitamata tarkvara küberturvalisust, vaatamata sellele, et küberrünnete sihtmärgiks võetakse üha enam just nende toodete nõrkused, põhjustades märkimisväärseid ühiskondlikke ja majanduslikke kulusid. Hiljutised näited on Pegasuse nuhkvara, mille puhul kasutati ära mobiiltelefonide nõrkusi, või WannaCry lunavara-uss, mille puhul kasutati ära Windowsi nõrkust ja mis mõjutas arvuteid kogu maailmas.

Mida tahetakse saavutada?

Siseturu nõuetekohase toimimise tagamiseks määrati kindlaks kaks põhieesmärki: 1) luua tingimused turvaliste digielemente sisaldavate toodete arendamiseks, tagades, et turule lastakse vähemate nõrkustega riist- ja tarkvaratooted ning et tootjad suhtuvad turvalisusesse tõsiselt toote kogu elutsükli jooksul, ning 2) luua tingimused, mis võimaldavad kasutajatel digielemente sisaldavate toodete valimisel ja kasutamisel küberturvalisust arvesse võtta. Seati neli erieesmärki**:** i) tagada, et tootjad parandavad digielemente sisaldavate toodete turvalisust alates projekteerimis- ja arendamisetapist ning kogu elutsükli jooksul; ii) tagada sidus küberturvalisuse raamistik, mis hõlbustab riist- ja tarkvaratootjatel nõuete täitmist; iii) suurendada digielemente sisaldavate toodete turvaomaduste läbipaistvust ning iv) võimaldada ettevõtjatel ja tarbijatel digielemente sisaldavaid tooteid turvaliselt kasutada.

Milline on ELi tasandi meetmete lisaväärtus (subsidiaarsus)?

Küberturvalisuse tugev piiriülene olemus ja selliste intsidentide kasvav arv, millel on piiriülene ning muudele sektoritele ja toodetele ülekanduv mõju, tähendavad, et liikmesriigid üksi ei suuda eesmärke tulemuslikult saavutada. Võttes arvesse digielemente sisaldavate toodete turgude ülemaailmset olemust, seistakse liikmesriikide territooriumil samade digielemente sisaldavate toodete puhul silmitsi samade riskidega. Kujunev ebaühtlane raamistik, mis koosneb potentsiaalselt lahknevatest siseriiklikest õigusnormidest, võib ka takistada digielemente sisaldavate toodete avatud ja konkurentsivõimelise ühtse turu toimimist. Seega on vaja ELi tasandi ühismeetmeid, et suurendada kasutajate usaldust ja ELi turule lastavate digielemente sisaldavate toodete populaarsust. Need tooksid kasu ka siseturule, tagades õiguskindluse ja luues võrdsed võimalused digielemente sisaldavate toodete tootjatele.

B. Lahendused

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

Analüüsiti nelja poliitikavarianti ja nende allvariante, mis lähevad praegusest olukorrast kaugemale: 1) pehme õiguse lähenemisviis ja vabatahtlikud meetmed; 2) tootepõhine sihipärane regulatiivne sekkumine digielemente sisaldavate materiaalsete toodete ja vastava sisseehitatud tarkvara küberturvalisuse valdkonnas; 3) kombineeritud lähenemisviis, mis hõlmab horisontaalseid kohustuslikke eeskirju digielemente sisaldavate materiaalsete toodete ja vastava sisseehitatud tarkvara küberturvalisuse kohta ning sisseehitamata tarkvara puhul järkjärgulist lähenemisviisi koos kahe alamvariandiga vastavushindamiseks, ning 4) horisontaalne regulatiivne sekkumine, millega kehtestatakse küberturvalisuse nõuded paljudele digielemente sisaldavatele toodetele, sealhulgas sisseehitamata tarkvarale, ning alamvariandid kohaldamisala ja vastavushindamise kohta.

Mõjuhinnangus jõuti järeldusele, et tuginedes tulemuslikkuse hindamisele erieesmärkide, kulutõhususe ning sidususe alusel, on **eelistatud variant** 4. variant, mis hõlmab kõiki digielemente sisaldavaid tooteid ja millega nähakse ette kriitilise tähtsusega toodete kohustuslik kolmanda isiku poolne hindamine.

Millised on eri sidusrühmade seisukohad? Kes millist varianti toetab?

Kui avalikul konsultatsioonil osalejatel paluti hinnata poliitikameetmete tõhusust, nõustusid nad, et kõige tõhusam meede oleks 4. variant (4,08 punkti skaalal 1–5). Osalejate hulka kuulusid tarbijaorganisatsioonid (5,00), end kasutajatena määratlenud osalejad (4,22), teavitatud asutused (4,17), turujärelevalveasutused (5,00) ja digielemente sisaldavate toodete tootjad (3,85), sealhulgas väikesed ja keskmise suurusega tootjad (4,05).

C. Eelistatud poliitikavariandi mõju

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

Eelistatud variant tooks eri sidusrühmadele märkimisväärset kasu. Ettevõtjate jaoks hoiaks see ära digielemente sisaldavate toodete suhtes kohaldatavate turvaeeskirjade lahknevuse ja vähendaks asjaomaste küberturvalisuse õigusaktide nõuete täitmisega seotud kulusid. See vähendaks küberintsidentide arvu, intsidentide käsitlemise kulusid ja mainekahju. Algatus võib kogu ELis vähendada ettevõtjaid mõjutavate intsidentidega seotud kulusid hinnanguliselt 180–290 miljardi euro võrra aastas. Lisaks tooks see kaasa käibe kasvu tänu digielemente sisaldavate toodete üha suuremale kasutuselevõtule. See parandaks ka ettevõtjate ülemaailmset mainet, mis tooks kaasa nõudluse suurenemise väljaspool ELi. Lõppkasutajate jaoks suurendaks eelistatud variant turvaomaduste läbipaistvust ja hõlbustaks digielemente sisaldavate toodete kasutamist. Tarbijad ja kodanikud saaksid kasu ka oma põhiõiguste (nagu eraelu puutumatus ja andmekaitse) paremast kaitsest.

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

Eelistatud variant suurendaks nõuete täitmise ja nende täitmise tagamisega seotud kulusid ettevõtjate, teavitatud asutuste ja avaliku sektori asutuste, sealhulgas teavitavate, akrediteerimis- ja turujärelevalveasutuste jaoks. Tarkvaraarendajate ja riistvaratootjate jaoks suurenevad otsesed nõuete täitmisega seotud kulud uute küberturvalisuse nõuete, vastavushindamise, dokumenteerimise ja aruandekohustuste tõttu, mille tulemusel nõuete täitmisega seotud kulud kokku on kuni ligikaudu 29 miljardit eurot, samal ajal kui digielemente sisaldavate toodete hinnanguline turuväärtus käibe alusel on kuni 1 485 miljardit eurot. Digielemente sisaldavate toodete hinnad võivad muutuda lõppkasutajate,

sealhulgas ärikasutajate, tarbijate ja kodanike jaoks kõrgemaks. Neid hindu vaadeldes tuleks siiski võtta arvesse eespool kirjeldatud märkimisväärset kasu. Teavitatud asutuste puhul peaks käibe suurenemine eeldatavasti lisakulud katma.
Milline on mõju VKEdele ja konkurentsivõimele?
Uued nõuded mõjutavad VKEsid nii tootjate kui ka lõppkasutajatena. Nõuete täitmisega seotud kulud mõjutaksid VKEsid põhimõtteliselt rohkem kui suurettevõtjaid, kellel on tavaliselt suurem mastaabisääst ja suurem küberturvalisusealane teadlikkus. VKEd saaksid algatusest siiski suurt kasu, sest digielemente sisaldavate toodete küberturvalisus tooks VKEdele kui kasutajatele kaasa märkimisväärse kulude kokkuhoiu. Tootjatena saaksid VKEd kasu lõppkasutajate suuremast usaldusest ja uutest klientidest. Sujuv juurdepääs siseturule ja turu killustatuse vähenemine võib olla VKEdele veelgi kasulikum, kuna neil on vähem võimalusi erinevate regulatiivsete nõuetega toimetulekuks. Rõhutades vajadust proportsionaalse lähenemisviisi ja toetusmeetmete järele, toetasid VKEd üldiselt kõigi ettevõtjate võrdseid võimalusi ja ei uskunud, et nad satuksid horisontaalsete kohustuslike nõuete stsenaariumi korral suuremate ettevõtjatega võrreldes ebasoodsamasse olukorda.
Kas on ette näha märkimisväärset mõju riigieelarvetele ja ametiasutustele?
Algatus mõjutab riikide ametiasutusi, näiteks riikide teavitavaid asutusi, akrediteerimisasutusi ja turujärelevalveasutusi, kes vastutavad kavandatud meetmete järelevalve ja nende rakendamise tagamise eest. Uute nõuetega arvestamiseks kannavad need asutused lisakulusid seoses kohandustega (nt koolitus ja inimressursid) ja nõuete täitmise tagamisega. Vastavushindamisasutused, kes ostavad akrediteerimisteenuseid, korvavad aga suures osas akrediteerimisasutuste kulutatavad vahendid.
Kas on oodata muud olulist mõju?
Muud olulist negatiivset mõju ei ole ette näha. Eelistatud poliitikavariant aitaks vähendada intsidentide, sealhulgas isikuandmetega seotud rikkumiste arvu ja raskusastet ning sellel oleks positiivne sotsiaalne mõju, näiteks küberkuritegevuse vähenemine. Nõudlus turbespetsialistide järele tõenäoliselt kasvaks ja küberturvalisusealase teabe ebaühtlus väheneks.
Proportsionaalsus?
Eelistatud variant ei lähe kaugemale sellest, mis on vajalik erieesmärkide rahuldavaks saavutamiseks. Sekkumine tagaks, et digielemente sisaldavad tooted on kaitstud kogu nende olelusringi jooksul ja proportsionaalselt riskidega.
D. Järelmeetmed
Millal poliitika läbi vaadatakse?
Hiljemalt [36 kuud] pärast algatuse kohaldamise alguskuupäeva ja seejärel iga nelja aasta tagant esitab komisjon Euroopa Parlamendile ja nõukogule aruande algatuse hindamise ja läbivaatamise kohta.