Europos Sąjungos
Taryba

Briuselis, 2022 m. rugsėjo 16 d.
(OR. en)

12429/22
ADD 6

Tarpinstitucinė byla:
2022/0272(COD)

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

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2022 m. rugsėjo 15 d.
kam:	Tarybos generaliniam sekretoriatui
Komisijos dok. Nr.:	SWD(2022) 283 final
Dalykas:	KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS „POVEIKIO VERTINIMO ATASKAITOS SANTRAUKA dėl Kibernetinio atsparumo akto“, pridedamas prie Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020

Delegacijoms pridedamas dokumentas SWD(2022) 283 final.

Pridedama: SWD(2022) 283 final

EUROPOS
KOMISIJA

Briuselis, 2022 09 15
SWD(2022) 283 final

KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS

POVEIKIO VERTINIMO ATASKAITOS SANTRAUKA

dėl Kibernetinio atsparumo akto

pridedamas prie

Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento

dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, kuriuo iš dalies keičiamas Reglamentas (ES) 2019/1020

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

Santraukos lentelė (ne daugiau kaip 2 psl.)

Kibernetinio atsparumo akto poveikio vertinimas

A. Būtinybė imtis veiksmų

Kokia tai problema ir kodėl ji yra ES masto?

Aparatinės ir programinės įrangos produktai dažnai nukenčia nuo sėkmingų kibernetinių atakų – apskaičiuota, kad 2021 m. metinė kibernetinių nusikaltimų žala pasaulyje siekė 5,5 trln. EUR. Šiems produktams būdingos dvi pagrindinės problemos, dėl kurių naudotojai ir visuomenė patiria papildomų išlaidų: 1) žemas kibernetinio saugumo lygis, kurį atspindi plačiai paplitę pažeidžiamumai ir nepakankamas bei nenuoseklus saugumo naujinių teikimas jiems spręsti, ir 2) nepakankamas naudotojų supratimas ir prieiga prie informacijos – todėl jie negali pasirinkti tinkamomis kibernetinio saugumo savybėmis pasižyminčių produktų ar saugiai juos naudoti.

Produktų su skaitmeniniais elementais kibernetiniam saugumui būdingas stiprus tarpvalstybinis aspektas, nes vienoje šalyje pagaminti produktai dažnai naudojami visoje vidaus rinkoje. Be to, incidentai, kurie iš pradžių paveikė vieną subjektą arba vieną valstybę narę, dažnai per kelias minutes išplinta visoje vidaus rinkoje.

Nors galiojantys vidaus rinkos teisės aktai taikomi tam tikriems produktams su skaitmeniniais elementais, daugumai aparatinės ir programinės įrangos produktų šiuo metu netaikomi jokie ES teisės aktai, kuriais būtų sprendžiamas jų kibernetinis saugumas. Visų pirma, dabartinėje ES teisinėje sistemoje nesprendžiamas neįtaisytosios programinės įrangos kibernetinis saugumas, nors kibernetinėse atakose vis dažniau siekiama pasinaudoti šių produktų pažeidžiamumais ir dėl to patiriama didelė socialinė ir ekonominė žala. Naujausi pavyzdžiai – šnipinėjimo programa „Pegasus“, išnaudojusi mobiliųjų telefonų pažeidžiamumus, arba išpirkos reikalaujanti programa „WannaCry“, išnaudojusi „Windows“ pažeidžiamumą ir turėjusi poveikį kompiuteriams visame pasaulyje.

Ką reikėtų pasiekti?

Nustatyti du pagrindiniai tikslai, kuriais siekiama užtikrinti tinkamą vidaus rinkos veikimą: 1) sudaryti sąlygas kurti saugius produktus su skaitmeniniais elementais užtikrinant, kad aparatinės ir programinės įrangos produktai būtų pateikiami rinkai su mažiau pažeidžiamumų ir kad gamintojai rimtai atsižvelgtų į saugumą per visą produkto gyvavimo ciklą; ir 2) sudaryti sąlygas, kad rinkdamiesi ir naudodami produktus su skaitmeniniais elementais naudotojai galėtų atsižvelgti į kibernetinį saugumą. Nustatyti keturi konkretūs tikslai**:** i) užtikrinti, kad gamintojai padidintų produktų su skaitmeniniais elementais saugumą nuo projektavimo ir kūrimo etapo ir per visą gyvavimo ciklą; ii) užtikrinti nuoseklią kibernetinio saugumo sistemą, palengvinančią aparatinės ir programinės įrangos gamintojų reikalavimų laikymąsi; iii) padidinti produktų su skaitmeniniais elementais saugumo savybių skaidrumą ir iv) sudaryti sąlygas įmonėms ir vartotojams saugiai naudoti produktus su skaitmeniniais elementais.

Kokia būtų papildoma ES lygmens veiksmų nauda (subsidiarumo principas)?

Dėl kibernetinio saugumo stipraus tarpvalstybinio pobūdžio ir daugėjančių incidentų, persiduodančių tarp skirtingų valstybių narių, sektorių ir produktų, pavienės valstybės narės negali veiksmingai pasiekti šių tikslų. Atsižvelgiant į pasaulinį produktų su skaitmeniniais elementais rinkų pobūdį, valstybės narės savo teritorijoje susiduria su ta pačia rizika dėl to paties produkto su skaitmeniniais elementais. Besiformuojanti netvarkinga galimai skirtingų nacionalinių taisyklių sistema taip pat gali trukdyti atvirai ir konkurencingai bendrai produktų su skaitmeniniais elementais rinkai. Todėl reikia imtis bendrų veiksmų ES lygmeniu siekiant padidinti naudotojų pasitikėjimą ES rinkai pateikiamais produktais su skaitmeniniais elementais

bei šių produktų patrauklumą. Tai taip pat būtų naudinga vidaus rinkai, nes suteiktų teisinio tikrumo ir sudarytų vienodas sąlygas produktų su skaitmeniniais elementais gamintojams.

B. Sprendimai

Kokių yra galimybių pasiekti šiuos tikslus? Ar viena iš galimybių pasirinkta kaip tinkamiausia? Jei ne, kodėl?

Išanalizuotos keturios politikos galimybės ir susijusios antrinės galimybės, viršijančios *status quo*: 1) neprivalomų teisės aktų ir savanoriškų priemonių metodas; 2) konkretiems produktams pritaikyta *ad hoc* reglamentavimo intervencija, skirta materialių produktų su skaitmeniniais elementais ir atitinkama įtaisytąja programine įranga kibernetiniam saugumui užtikrinti; 3) mišrus metodas, apimantis horizontaliąsias privalomas materialių produktų su skaitmeniniais elementais ir atitinkama įtaisytąja programine įranga kibernetinio saugumo taisykles ir paskirstytąjį metodą neįtaisytajai programinei įrangai su dviem antrinėmis atitikties vertinimo galimybėmis; ir 4) horizontaliojo reglamentavimo intervencija, pagal kurią kibernetinio saugumo reikalavimai nustatomi įvairiems produktams su skaitmeniniais elementais, įskaitant neįtaisytąją programinę įrangą, su antrinėmis taikymo srities galimybėmis ir atitikties vertinimu.

Poveikio vertinime padaryta išvada, kad **tinkamiausia** yra 4 galimybė, apimanti visus produktus su skaitmeniniais elementais ir numatanti privalomą trečiosios šalies atliekamą ypatingos svarbos produktų vertinimą, pagrįstą veiksmingumo vertinimu pagal konkrečius tikslus, sąnaudų ir naudos efektyvumu bei suderinamumu.

Kokios yra įvairių suinteresuotųjų subjektų nuomonės? Kas kuriai galimybei pritaria?

Paprašyti įvertinti politinių intervencijų veiksmingumą, viešų konsultacijų respondentai sutiko, kad 4 galimybė būtų veiksmingiausia priemonė (4,08 balo skalėje nuo 1 iki 5). Tai apima vartotojų organizacijas (5,00), vartotojais prisistatančius respondentus (4,22), notifikuotąsias įstaigas (4,17), rinkos priežiūros institucijas (5,00) ir produktų su skaitmeniniais elementais gamintojus (3,85), įskaitant mažo ir vidutinio dydžio įmones (4,05).

C. Tinkamiausios galimybės poveikis

Kokie būtų tinkamiausios galimybės (jei jos nėra – pagrindinių galimybių) pranašumai?

Tinkamiausia galimybė suteiktų daug naudos įvairiems suinteresuotiesiems subjektams. Įmonės išvengtų skirtingų produktams su skaitmeniniais elementais taikomų saugumo taisyklių, o tai sumažintų susijusių kibernetinio saugumo teisės aktų reikalavimų laikymosi išlaidas. Tai sumažintų kibernetinių incidentų skaičių, incidentų valdymo išlaidas ir žalą reputacijai. Apskaičiuota, kad visoje ES dėl šios iniciatyvos įmonių išlaidos dėl patiriamų incidentų gali sumažėti maždaug 180–290 mlrd. EUR per metus. Be to, dėl šios iniciatyvos padidėtų apyvarta dėl didėjančio produktų su skaitmeniniais elementais naudojimo. Ji taip pat gerintų įmonių reputaciją pasaulyje, dėl to išaugtų paklausa ES nepriklausančiose šalyse. Galutiniams naudotojams tinkamiausia galimybė padidintų saugumo savybių skaidrumą ir palengvintų produktų su skaitmeniniais elementais naudojimą. Be to, vartotojams ir piliečiams būtų naudinga geresnė jų pagrindinių teisių apsauga, pavyzdžiui, teisės į privatumą ir duomenų apsaugą.

Kokios būtų tinkamiausios galimybės (jei jos nėra – pagrindinių galimybių) įgyvendinimo išlaidos?

Dėl tinkamiausios galimybės atsirastų papildomų reikalavimų laikymosi ir vykdymo užtikrinimo išlaidų įmonėms, notifikuotosioms įstaigoms ir valdžios institucijoms, įskaitant notifikuojančiąsias, akreditavimo ir rinkos priežiūros institucijas. Programinės įrangos kūrėjams ir aparatinės įrangos gamintojams tai

padidins tiesiogines išlaidas, susijusias su naujų kibernetinio saugumo reikalavimų laikymusi, atitikties vertinimu, dokumentacijos ir ataskaitų teikimo pareigomis, dėl to bendros reikalavimų laikymosi išlaidos sieks maždaug 29 mlrd. EUR, o numatoma produktų su skaitmeniniais elementais rinkos vertė (vertinant apyvartą) bus iki 1 485 mlrd. EUR. Galutiniams naudotojams, įskaitant galutinius verslo naudotojus, vartotojus ir piliečius, gali padidėti produktų su skaitmeniniais elementais kainos. Tačiau tai turėtų būti vertinama atsižvelgiant į pirmiau aprašytą didelę naudą. Tikimasi, kad notifikuotosioms įstaigoms papildomas išlaidas kompensuos padidėjusi apyvarta.

Koks bus poveikis MVĮ ir konkurencingumui?

Nauji reikalavimai turės įtakos MVĮ, kurios yra gamintojai ir galutiniai naudotojai. Kalbant apie reikalavimų laikymosi išlaidas, iš esmės tai turėtų didesnį poveikį MVĮ nei didelėms įmonėms, kurios paprastai pasižymi geresne masto ekonomija ir geriau suvokia kibernetinį saugumą. Tačiau ši iniciatyva MVĮ būtų labai naudinga, nes į produktus su skaitmeniniais elementais integruotos kibernetinio saugumo priemonės ženkliai sumažintų MVĮ, kaip naudotojų, išlaidas. Gaminančioms MVĮ tai būtų naudinga dėl didesnio galutinių naudotojų pasitikėjimo ir naujų klientų. Dar naudingesnė MVĮ gali būti sklandi prieiga prie vidaus rinkos ir mažesnė rinkos fragmentacija, nes šios įmonės yra ne taip gerai pasirengusios vykdyti skirtingus reglamentavimo reikalavimus. Pabrėždamos proporcingumo ir paramos priemonių poreikį, MVĮ iš esmės palaikė vienodas sąlygas visoms įmonėms ir nemanė, kad horizontaliųjų privalomų reikalavimų scenarijus joms būtų mažiau palankus, palyginti su didesnėmis įmonėmis.

Ar tai turės didelį poveikį nacionaliniams biudžetams ir administravimo subjektams?

Ši iniciatyva turės poveikį nacionalinėms valdžios institucijoms, pavyzdžiui, nacionalinėms notifikuojančiosioms institucijoms, akreditavimo institucijoms ir rinkos priežiūros institucijoms, atsakingoms už siūlomų priemonių stebėseną ir vykdymo užtikrinimą. Šios institucijos patirs papildomų prisitaikymo (pvz., mokymo ir žmogiškųjų išteklių) ir vykdymo užtikrinimo išlaidų, kad atsižvelgtų į naujus reikalavimus. Tačiau akreditavimo įstaigų išnaudotus išteklius kompensuoja ir didžiąja dalimi padengia atitikties vertinimo įstaigos, pirkdamos akreditavimo paslaugas.

Ar bus dar koks nors didelis poveikis?

Jokio kito reikšmingo neigiamo poveikio nenumatoma. Tinkamiausia politikos galimybė padėtų sumažinti incidentų, įskaitant asmens duomenų pažeidimus, skaičių ir sunkumą ir turėtų teigiamą socialinį poveikį, pavyzdžiui, mažintų kibernetinių nusikaltimų. Tikėtina, kad saugumo specialistų poreikis augs ir kibernetinio saugumo informacijos asimetrija mažės.

Proporcingumo principas

Tinkamiausia galimybe neviršijama to, kas yra būtina tam, kad būtų patenkinamai pasiekti konkretūs tikslai. Šia intervencija būtų užtikrinta, kad produktai su skaitmeniniais elementais būtų apsaugoti per visą jų gyvavimo ciklą, proporcingai patiriamai rizikai.

D. Tolesni veiksmai

Kada politika bus persvarstoma?

Ne vėliau kaip praėjus 36 mėnesiams nuo iniciatyvos taikymo pradžios dienos, o vėliau kas ketverius metus Komisija teikia Europos Parlamentui ir Tarybai iniciatyvos vertinimo ir peržiūros ataskaitas.