Europos Sąjungos
Taryba

Briuselis, 2020 m. gruodžio 18 d.
(OR. en)

14150/20
ADD 3

Tarpinstitucinė byla:
2020/0359(COD)

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

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2020 m. gruodžio 16 d.
kam:	Europos Sąjungos Tarybos generaliniam sekretoriui Jeppe TRANHOLMUI-MIKKELSENUI
Komisijos dok. Nr.:	SWD(2020) 344 final
Dalykas:	KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS „POVEIKIO VERTINIMO ATASKAITOS SANTRAUKA“, pridedamas prie pasiūlymo dėl Europos Parlamento ir Tarybos Direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148

Delegacijoms pridedamas dokumentas SWD(2020) 344 final.

Pridedama: SWD(2020) 344 final

EUROPOS
KOMISIJA

Briuselis, 2020 12 16
SWD(2020) 344 final

KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS

POVEIKIO VERTINIMO ATASKAITOS SANTRAUKA

pridedamas prie

Pasiūlymo dėl Europos Parlamento ir Tarybos Direktyvos

dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148

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

Santraukos lentelė

Poveikio vertinimas dėl *2016 m. liepos 6 d. Direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (toliau –TIS direktyva) peržiūros*

A. Būtinybė imtis veiksmų

Kokia tai problema ir kodėl ji yra ES masto?

Nepaisant reikšmingų laimėjimų, jau paaiškėjo, kad TIS direktyva, kuri sudarė sąlygas gerokai pakeisti mąstyseną, institucinį ir reguliavimo požiūrį į kibernetinį saugumą daugumoje valstybių narių, turi trūkumų. Vykstant skaitmeninei visuomenės transformacijai (kurią dar labiau paskatino COVID-19 krizė), padidėjo grėsmių įvairovė ir atsirado naujų problemų, kurioms spręsti reikalingos pritaikytos ir novatoriškos reagavimo priemonės. Kibernetinių išpuolių toliau daugėja, o įvairūs ES vidaus ir užsienio subjektai vykdo vis sudėtingesnius kibernetinius išpuolius.

Remiantis TIS direktyvos taikymo vertinimu, poveikio vertinime nustatytos šios problemos: žemas ES veikiančių įmonių kibernetinio atsparumo lygis; nevienodas atsparumas valstybėse narėse ir sektoriuose ir žemas bendro informuotumo apie padėtį lygis, taip pat bendro reagavimo į krizę nebuvimas. Pavyzdžiui, dėl kai kurių iš šių problemų ir paskatų susidarė situacijų, kai pagrindinės ligoninės valstybėse narėse nepatenka į TIS direktyvos taikymo sritį, todėl jos neprivalo įgyvendinti atitinkamų saugumo priemonių, o kitoje valstybėje narėje TIS saugumo reikalavimai taikomi beveik kiekvienai šalies ligoninei.

Ką reikėtų pasiekti?

Atliekant TIS peržiūrą numatyti trys bendrieji tikslai:

1. **Didinti visų Europos Sąjungoje visuose atitinkamuose sektoriuose veikiančių įmonių kibernetinio atsparumo lygį**, nustatant taisykles, kuriomis užtikrinama, kad visi viešieji ir privatieji subjektai visoje vidaus rinkoje, atliekantys svarbias funkcijas ekonomikai ir visai visuomenei, imtųsi tinkamų kibernetinio saugumo priemonių.
2. Toliau derinant 1) *de facto* taikymo sritį, 2) saugumo ir pranešimo apie incidentus reikalavimus, 3) nacionalinę priežiūrą ir vykdymo užtikrinimą reglamentuojančias nuostatas ir 4) valstybių narių kompetentingų institucijų pajėgumus, **mažinti atsparumo skirtumus vidaus rinkoje ir tai daryti sektoriuose, kuriems jau taikoma direktyva**.
3. **Gerinti bendro informuotumo apie padėtį lygį ir kolektyvinius gebėjimus pasirengti ir reaguoti**, imantis priemonių kompetentingų institucijų tarpusavio pasitikėjimui didinti, dažniau dalijantis informacija ir nustatant taisykles bei procedūras didelio masto incidento ar krizės atveju.

Kokia būtų papildoma ES lygmens veiksmų nauda (subsidiarumas)?

Kibernetinis atsparumas Sąjungoje negali būti veiksmingas, jeigu bus laikomasi nevienodo nacionaliniu ar regioniniu lygmeniu izoliuoto požiūrio. TIS direktyva šis trūkumas buvo iš dalies išspręstas nacionaliniu ir Sąjungos lygmenimis nustatant tinklų ir informacinių sistemų saugumo sistemą. Tačiau jos perkėlimas į nacionalinę teisę ir įgyvendinimas taip pat atskleidė tam tikrų nuostatų ar požiūrių trūkumų, pavyzdžiui, neaiškios TIS direktyvos taikymo srities ribos. Be to, nuo COVID-19 krizės pradžios Europos ekonomika kaip niekad anksčiau tapo dar labiau priklausoma nuo tinklų ir informacinių sistemų, o sektoriai ir paslaugos tarpusavyje vis labiau sujungiami. Todėl pirmoji periodinė TIS direktyvos peržiūra suteikė galimybę ES imtis tolesnių veiksmų. ES intervencija, apimanti daugiau nei dabartines TIS direktyvos priemones, iš esmės yra pateisinama dėl: i) tarpvalstybinio problemos pobūdžio; ii) ES veiksmų siekiant pagerinti ir palengvinti veiksmingą nacionalinę politiką potencialo; iii) suderintų ir bendradarbiavimu

grindžiamų TIS politikos priemonių indėlio veiksmingai užtikrinant duomenų apsaugą ir privatumą.

B. Sprendimai

Kokiais būdais galima pasiekti tikslus? Ar viena iš politikos galimybių pasirinkta kaip tinkamiausia? Jei ne, kodėl?

Poveikio vertinime išnagrinėtos keturios politikos galimybės: 0) išlaikyti *status quo*; 1) ne teisėkūros priemonės, kuriomis siekiama suderinti perkėlimą į nacionalinę teisę; 2) nedideli TIS direktyvos pakeitimai siekiant tolesnio derinimo; 3) sisteminiai ir struktūriniai TIS direktyvos pakeitimai. 1 galimybė atmesta ankstyvame etape, nes iš esmės nenukrypsta nuo *status quo*. Poveikio vertinime daroma išvada, kad **tinkamiausia galimybė** yra 3 galimybė (t. y. **sisteminiai ir struktūriniai TIS sistemos pakeitimai**), nes pagal ją būtų iš esmės pakeistas požiūrį, į taikymo sritį įtraukiant platesnį Sąjungos ekonomikos segmentą, taip pat tikslingiau vykdyti priežiūrą, kuri būtų taikoma proporcingai didelėms ir pagrindinėms bendrovėms, kartu aiškiai nustatant taikymo sritį. Be to, taip būtų supaprastintos ir dar labiau suderintos su saugumu susijusios įmonių pareigos, sukurta veiksmingesnė veiklos aspektų nustatymo sistema, taip pat nustatytas aiškus pagrindas bendrai atitinkamų subjektų atsakomybei ir atskaitomybei ir skatinamas keitimasis informacija.

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

Dauguma kompetentingų institucijų ir įmonių pritarė TIS direktyvos peržiūrai. Per kelias konsultacijas jos nurodė, kad peržiūrėta TIS direktyva turėtų apimti papildomus (pa)sektorius, suderinti arba supaprastinti papildomas saugumo priemones ir pareigas pranešti. Suinteresuotosios šalys taip pat pritarė naujoms koncepcijoms ar su politika susijusioms priemonėms, kurios yra tik tinkamiausios galimybės dalis (pvz., tiekimo grandinės saugumo politikai, veikiančios ES krizių valdymo sistemos institucionalizavimui).

C. Tinkamiausios galimybės poveikis

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

Tinkamiausia galimybė duotų didelės naudos: iš skaičiavimų, atliktų remiantis ekonominiu modeliavimu, kuris buvo parengtas pasitelkiant pagalbinį tyrimą, skirtą TIS peržiūrai, matyti, kad pasirinkus tinkamiausią galimybę kibernetinio saugumo incidentų kaina gali sumažėti 11,3 mlrd. EUR.

Taikymo sritis sektoriuose būtų gerokai išplėsta pagal TIS sistemą, tačiau, palyginti su minėtais privalumais, našta, kuri gali atsirasti dėl TIS reikalavimų, visų pirma dėl priežiūros, taip pat būtų suderinta tiek naujų subjektų, kurie bus įtraukti į taikymo sritį, tiek kompetentingų institucijų atžvilgiu. Taip yra todėl, kad pagal naująją TIS sistemą būtų nustatytas dviejų lygmenų metodas, daugiausia dėmesio skiriant dideliems ir pagrindiniams subjektams ir diferencijuotai priežiūros tvarkai, kuri leistų vykdyti tik daugelio jų *ex post* priežiūrą (t. y. reaktyvi priežiūra netaikant bendros pareigos sistemiškai dokumentuoti reikalavimų laikymąsi), visų pirma tų, kurie laikomi „svarbiais“, tačiau nėra „esminiai“.

Apskritai tinkamiausia galimybė duotų abipusę naudą ir sinergiją, be to, tinkamiausia galimybė iš visų analizuotų politikos galimybių turi didžiausią potencialą užtikrinti didesnį ir nuoseklesnį pagrindinių subjektų visoje Sąjungoje kibernetinio atsparumo lygį, kuris galiausiai padėtų įmonėms ir visuomenei sutaupyti.

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

Taikydamos tinkamiausią galimybę atitinkamos valstybių narių institucijos patirtų tam tikrų atitikties ir vykdymo užtikrinimo išlaidų (apskaičiuota, kad ištekliai iš viso padidės maždaug 20–30 proc.). Tačiau

naujoji sistema taip pat būtų labai naudinga dėl geresnės pagrindinių įmonių apžvalgos ir sąveikos su jomis, tvirtesnio tarpvalstybinio operatyvinio bendradarbiavimo, taip pat savitarpio pagalbos ir tarpusavio vertinimo mechanizmų. Dėl to valstybėse narėse iš esmės padidėtų kibernetinio saugumo pajėgumai.

Apskaičiuota, kad įmonėms, kurios pateks į TIS sistemos taikymo sritį, keliais pirmaisiais metais po naujos TIS sistemos įdiegimo reikėtų ne daugiau kaip 22 proc. padidinti dabartines IRT saugumo išlaidas (įmonių, kurioms jau taikoma dabartinė TIS direktyva, atveju tai būtų 12 proc.). Tačiau toks vidutinis IRT saugumo išlaidų padidėjimas suteiktų proporcingą naudą iš tokių investicijų, visų pirma dėl gerokai sumažėjusių kibernetinio saugumo incidentų išlaidų (numatoma, kad per dešimt metų ji sieks 11,3 mlrd. EUR).

Koks bus poveikis MVĮ ir konkurencingumui?

Pagal tinkamiausią galimybę mažosios ir labai mažos įmonės nebūtų įtrauktos į TIS sistemos taikymo sritį. Galima tikėtis, kad vidutinės įmonės pirmaisiais metais nuo naujos tinklų ir informacijos saugumo sistemos įdiegimo padidins IRT saugumo išlaidas. Kartu padidinus saugumo reikalavimų šiems subjektams lygį taip pat būtų skatinami jų kibernetinio saugumo pajėgumai ir padedama gerinti IRT rizikos valdymą.

Ar tai turės didelį poveikį nacionaliniams biudžetams ir administravimo subjektams?

Poveikis būtų daromas nacionaliniams biudžetams ir administravimo subjektams: numatoma, kad trumpuoju ir vidutinės trukmės laikotarpiu ištekliai padidės maždaug 20–30 proc.

Ar bus dar koks nors didelis poveikis?

Jokio kito reikšmingo neigiamo poveikio nenumatoma. Tikėtina, kad tinkamiausia politikos galimybe bus užtikrinti patikimesni kibernetinio saugumo pajėgumai ir atitinkamai sumažės incidentų, įskaitant duomenų saugumo pažeidimus, skaičius ir sunkumas. Be to, tikėtina, kad tai turės teigiamą poveikį užtikrinant vienodas sąlygas visose valstybėse narėse visiems subjektams, patenkantiems į TIS taikymo sritį, ir sumažins kibernetinio saugumo informacijos asimetriją.

Koks poveikis proporcingumo principui?

Tinkamiausia galimybe neviršijama to, kas yra būtina tam, kad būtų patenkinamai pasiekti konkretūs tikslai. Numatomas saugumo priemonių ir įpareigojimų teikti ataskaitas suderinimas ir supaprastinimas yra susiję su valstybių narių ir įmonių prašymais gerinti dabartinę sistemą.

D. Tolesni veiksmai

Kada politika bus persvarstoma?

Pirmoji peržiūra būtų atliekama praėjus 54 mėnesiams po teisinės priemonės įsigaliojimo. Komisija Europos Parlamentui ir Tarybai pateiktų peržiūros ataskaitą. Peržiūra būtų parengta padedant ENISA ir Bendradarbiavimo grupei.