Europos Sąjungos
Taryba

Briuselis, 2017 m. rugsėjo 14 d.
(OR. en)

12183/17
ADD 2

Tarpinstitucinė byla:
2017/0225 (COD)

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

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinio sekretoriaus, kurio vardu pasirašo direktorius Jordi AYET PUIGARNAU
kam:	Europos Sąjungos Tarybos generaliniam sekretoriui Jeppe TRANHOLMUI-MIKKELSENUI
Komisijos dok. Nr.:	SWD(2017) 501 final
Dalykas:	KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS „POVEIKIO VERTINIMO SANTRAUKA“, pridedamas prie Pasiūlymo dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO dėl ES kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas)

Delegacijoms pridedamas dokumentas SWD(2017) 501 final.

Pridedama: SWD(2017) 501 final

EUROPOS
KOMISIJA

Briuselis, 2017 09 13
SWD(2017) 501 final

KOMISIJOS TARNYBŲ DARBINIS DOKUMENTAS

POVEIKIO VERTINIMO SANTRAUKA

pridedamas prie

Pasiūlymo dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO

dėl ES kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas)

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

A. BŪTINYBĖ IMTIS VEIKSMŲ

Kokią problemą reikia spręsti ir kokios šios problemos priežastys?

Skaitmeninės technologijos ir internetas yra ES ekonomikos ir visuomenės stuburas. Ypatingos svarbos sektorių, kaip antai transporto, energetikos, sveikatos ar finansų, pagrindinės funkcijos vis labiau priklauso nuo tinklo ir informacinių sistemų. Daiktų internetas jungia objektus ir žmones ryšių tinklais. Ši nauja realybė suteikia precedento neturinčių galimybių, tačiau turi ir pažeidžiamų vietų. Kibernetinių incidentų vis daugėja. Jų sudėtingumas, dažnumas ir poveikio aprėptis – nuo prieigos prie esminių paslaugų iki demokratinių procesų – tik didės.

Šiomis aplinkybėmis įvardytos šios tarpusavyje susipynusios problemos:

- kibernetinio saugumo politikos ir požiūrio į kibernetinį saugumą valstybėse narėse nenuoseklumas;
- išskaidyti ištekliai ir nevienodas požiūris į kibernetinį saugumą ES institucijose, agentūrose ir įstaigose;
- menkos piliečių ir įmonių žinios apie kibernetines grėsmes, nepakankamas jų informavimas apie perkamų ar naudojamų IRT produktų ir paslaugų saugumo savybes, taip pat didėjanti nacionalinių ir sektorinių sertifikavimo schemų įvairovė.

Šios problemos mažina bendrą ES kibernetinį atsparumą ir trukdo veiksmingam vidaus rinkos veikimui.

Ką reikėtų pasiekti?

Konkretūs iniciatyvos politiniai tikslai.

1. Gerinti valstybių narių ir įmonių pajėgumus bei parengtį, visų pirma susijusius su ypatingos svarbos infrastruktūros objektais.
2. Gerinti valstybių narių ir ES institucijų, agentūrų bei įstaigų bendradarbiavimą ir veiklos koordinavimą.
3. Didinti ES lygmens galimybes papildyti valstybių narių veiksmus, ypač tarpvalstybinių kibernetinių krizių atveju.
4. Didinti piliečių ir įmonių informuotumą kibernetinio saugumo klausimais.
5. Didinti bendrą IRT produktų ir paslaugų kibernetinio saugumo užtikrinimo skaidrumą, siekiant stiprinti pasitikėjimą bendrąja skaitmenine rinka ir skaitmeninėmis inovacijomis.
6. Vengti nereikalingos sertifikavimo schemų ES ir susijusių reikalavimų bei vertinimo kriterijų visose valstybėse narėse ir sektoriuose gausos.

Kokia papildoma ES lygmens veiksmų nauda?

Kadangi ekonomikos ir visuomenės skaitmeninimo ir jungimo užmojis apima visą pasaulį, problemų mastas taip pat viršija vienos valstybės narės teritorijos ribas. Todėl reikalinga Sąjungos lygmens intervencija. Esant dabartinėms aplinkybėms ir žvelgiant į ateities

scenarijus, atrodo, kad, norint padidinti bendrą Sąjungos kibernetinį atsparumą, pavienių jos valstybių narių veiksmų ir skirtingų požiūrių į kibernetinį saugumą nepakaks, ypač dėl jo ryškaus tarpvalstybinio aspekto.

B. SPRENDIMAI

Kokiais būdais galima pasiekti tikslus? Ar viena iš politikos galimybių pasirinkta kaip tinkamiausia?

Šiame poveikio vertinime nagrinėjamos konkrečios politikos galimybės, apimančios Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) veiklos peržiūrą ir IRT saugumo sertifikavimą.

ENISA veiklos peržiūra

0 galimybė. Atskaitos scenarijus. Pasirinkus šią galimybę išlaikomas *status quo*. Agentūros ENISA įgaliojimai būtų pratęsti, o jos tikslai ir uždaviniai iš esmės nesikeistų, kartu būtų atsižvelgta į agentūrai pavestas užduotis pagal vėlesnius ES teisės aktus (pvz., TIS direktyvą).

1 galimybė. ENISA įgaliojimai nepratęsiami (ENISA nutraukia veiklą). Pasirinkus šią galimybę, ENISA veikla nutrūktų pasibaigus jos įgaliojimams (2020 m. birželio mėn.), o kompetencija ir veikla būtų perskirstyta ES ir (arba) nacionaliniu lygmeniu.

2 galimybė. Pertvarkyta ENISA. Ši galimybė būtų grindžiama dabartiniais ENISA įgaliojimais numatant priimti būtiniausius pakeitimus, kuriais būtų atsižvelgiama į kibernetinio saugumo padėties raidą. Agentūrai būtų suteikti nuolatiniai įgaliojimai, grindžiami šiais pamatiniais elementais: parama ES politikos formavimo ir įgyvendinimo veiklai, gebėjimų stiprinimu, žiniomis ir informacija, su rinka susijusiomis užduotimis, moksliniais tyrimais ir naujovėmis, operatyviniu bendradarbiavimu ir krizių valdymu.

3 galimybė. Visišku operaciniu pajėgumu veikianti ES kibernetinio saugumo agentūra. Ši galimybė numato reformuoti ENISA sujungiant tris pagrindines funkcijas: 1) politinę patariamąją funkciją, 2) informacijos ir ekspertizės centrą ir 3) Kompiuterinių incidentų tyrimo tarnybą (CERT). Ši galimybė iš esmės reikštų tokius pat įgaliojimų aprėpties pokyčius kaip ir 2 galimybė, tik būtų įtrauktos papildomos užduotys į reagavimo į incidentus ir krizių valdymo sritis, kad agentūros įgaliojimai apimtų visą kibernetinio saugumo grandinę, taigi kibernetinių incidentų prevenciją, aptikimą ir reagavimą į juos.

Sertifikavimas

0 galimybė. Atskaitos scenarijus. Nesiimti jokių veiksmų. Pasirinkusi šią galimybę, Komisija išlaikytų *status quo* ir nesiimtų jokių politinių ar teisėkūros veiksmų.

1 galimybė. Ne teisėkūros (privalomos teisinės galios neturinčios) priemonės. Pasirinkusi šią galimybę, Komisija imtųsi privalomos teisinės galios neturinčių politinių priemonių (pvz., skelbtų aiškinamuosius komunikatus, remtų ES masto savireguliavimo ir standartizavimo iniciatyvas), siekdama didinti skaidrumą ir mažinti susiskaidymą.

2 galimybė. ES teisės aktas dėl vyresniųjų pareigūnų grupės informacinių sistemų saugumo klausimais (SOG-IS) susitarimo taikymo visose valstybėse narėse. Pasirinkusi šią galimybę, Komisija pasiūlytų teisės aktą, kuriuo visos valstybės narės būtų teisiškai įpareigotos prisijungti prie susitarimo.

<u>3 galimybė.</u> ES bendra IRT kibernetinio saugumo sertifikavimo sistema. Pasirinkus šią galimybę, būtų sukurta europinė IRT saugumo sertifikavimo sistema (taip pat ekspertų grupė, kurią sudarytų nacionalinių valdžios institucijų atstovai), kuri būtų kuo labiau paremta esamomis IRT saugumo sertifikavimo schemomis. Iš esmės, taikant šią sistemą, būtų nustatomos ES sertifikavimo schemos, kurios būtų pripažįstamos visose valstybėse narėse.

Tinkamiausia politikos galimybė – ENISA reglamentavimo 2 galimybės ir sertifikavimo reglamentavimo 3 galimybės derinys.

Kokia įvairių suinteresuotųjų šalių nuomonė? Kas kuriai galimybei pritaria?

Atrodo, kad didžioji dauguma visų kategorijų suinteresuotųjų subjektų (valstybės narės, sektoriaus atstovai, ES institucijos, mokslo tyrimų bendruomenė) pritaria tinkamiausios galimybės pasirinkimui, nes pirmenybę teikia agentūros ENISA stiprinimui ir Europos IRT saugumo sertifikavimo sistemos sukūrimui.

Visų pirma, visuotinai sutariama dėl būtinybės turėti sklandžiai veikiančią ES agentūrą, turinčią nuolatinius įgaliojimus ir reikiamų išteklių, kuriai būtų pavedami dabartiniai ir būsimi kibernetinio saugumo uždaviniai. Suinteresuotieji subjektai taip pat pritaria savanoriškos ir lanksčios europinės sertifikavimo sistemos sukūrimui.

Tarp sektoriaus atstovų tokį sprendimą dėl sertifikavimo palaiko tos įmonės, kurios jau susiduria su sertifikavimo reikalavimų taikymu ir kurioms būtų naudingas ES masto mechanizmas, grindžiamas tarpusavyje pripažįstamais sertifikatais. Tam pritaria ir MVĮ – jos labiausiai nukentėtų, jei joms reikėtų savo produktus kiekvienoje valstybėje narėje sertifikuoti atskirai. Kai kurios valstybės narės (visų pirma tos, kurios turi mažiau išteklių), kai kurie sektoriaus atstovai ir ES institucijos taip pat teigiamai įvertimo ENISA reglamentavimo 3 galimybę.

C. TINKAMIAUSIOS GALIMYBĖS POVEIKIS

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

Pagal pasirinktą galimybę ES turėtų agentūrą, padedančią valstybėms narėms, ES institucijoms ir verslo įmonėms tose srityse, kuriose ji duotų didžiausią papildomą naudą. Ji padėtų: įgyvendinti TIS direktyvą; formuoti ir įgyvendinti politiką; plėsti žinias ir didinti informuotumą; vykdyti mokslinius tyrimus; vykdyti operatyvinį bendradarbiavimą įvykus krizei; stiprinti rinką. Visų pirma, ENISA turėtų remti ES politiką, susijusią su IRT saugumo sertifikavimu, užtikrinant administracinį ir techninį Europos IRT saugumo sertifikavimo sistemos valdymą. Turint tokią sistemą būtų veiksmingai taikomos IRT saugumo sertifikavimą Europos Sąjungoje reglamentuojančios taisyklės, o tai skatintų visose valstybėse narėse išduotų sertifikatų tarpusavio pripažinimą. Sprendimas suderinti šias galimybes buvo įvertintas kaip veiksmingiausias būdas ES pasiekti nustatytus tikslus: padidinti kibernetinio saugumo pajėgumus, užtikrinti pasirengimą, bendradarbiavimą, informuotumą, skaidrumą ir išvengti rinkos susiskaidymo. Ši galimybė taip pat labiausiai atitinka ES kibernetinio saugumo strategijos bei susijusių politikos sričių (pvz., TIS direktyvos) ir bendrosios skaitmeninės rinkos strategijos politinius prioritetus. Be to, pasirinkus šią galimybę tikslai būtų pasiekti racionaliai panaudojant išteklius.

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

Nors pertvarkyta ENISA įgytų naujų funkcijų, ji išliktų veiksmingai veikianti organizacija. Finansinis įnašas iš ES biudžeto turėtų būti didesnis nei dabar, bet vis tiek jis būtų gerokai mažesnis, nei skiriama kitoms ypatingos svarbos srityse veikiančioms agentūroms.

Dėl Europos IRT saugumo sertifikavimo sistemos sukūrimo sektorius (įskaitant MVĮ) neturėtų papildomų išankstinių išlaidų. Priešingai – tos įmonės, kurios jau sertifikuoja savo produktus arba ketina tai daryti, sutaupytų daug lėšų, o tai turėtų teigiamos įtakos jų konkurencingumui visame pasaulyje. Kita vertus, reikėtų tam tikrų biudžetinių įsipareigojimų sistemos veikimui užtikrinti, iš esmės tai darytų pertvarkyta ENISA, atliekanti technines ir sekretoriato užduotis.

Ar tai turės didelį poveikį nacionaliniams biudžetams ir administravimo subjektams?

Ne, lėšos agentūrai ENISA stiprinti daugiausia bus skiriamos iš ES biudžeto, o iš valstybės narės galės jai skirti finansinį įnašą savanoriškai. Didžiausią poveikį nacionaliniams biudžetams ir administravimo subjektams, susijusį su sertifikavimu, turės sertifikavimo institucija sukūrimas, jei to reikės.

Ar bus dar koks nors didelis poveikis?

Ne.

Proporcingumo principas

Pagal tinkamiausią galimybę numatytos subalansuotos priemonės: laikoma, kad jos visos reikalingos tikslams pasiekti ir kad jos nebus pernelyg didelė našta atitinkamiems suinteresuotiesiems subjektams. Atsižvelgiant į tai, laikoma, kad ši iniciatyva atitinka proporcingumo principą.

D. TOLESNI VEIKSMAI

Kada politika bus peržiūrėta?

Šiuo metu siūloma pirmąkart vertinimą atlikti praėjus penkeriems metams nuo teisinės priemonės įsigaliojimo. Tada Komisija pateiks atlikto vertinimo ataskaitą Europos Parlamentui ir Tarybai ir, jei reikės, pasiūlymą peržiūrėti teisinę priemonę. Vėliau vertinimas būtų atliekamas kas penkerius metus.