Europos Sąjungos
Taryba

Briuselis, 2020 m. gruodžio 2 d.
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2020 m. gruodžio 2 d.
kam:	Delegacijoms
Dalykas:	Tarybos išvados dėl prijungtųjų įrenginių kibernetinio saugumo - Tarybos išvados, patvirtintos taikant rašytinę procedūrą

Delegacijoms pridedamos Tarybos išvados dėl prijungtųjų įrenginių kibernetinio saugumo, kurias 2020 m. gruodžio 2 d. Taryba patvirtino taikydama rašytinę procedūrą.

PRIEDAS

Tarybos išvados dėl prijungtųjų įrenginių kibernetinio saugumo

Europos Sąjungos Taryba,

PRIMINDAMA

- Tarybos išvadas dėl bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“,
- Tarybos išvadas dėl kibernetinio saugumo pajėgumų ir gebėjimų stiprinimo ES,
- Tarybos išvadas dėl 5G svarbos Europos ekonomikai ir poreikio mažinti su 5G susijusią saugumo riziką,
- Tarybos išvadas „Aukšto skaitmeninimo lygio Europos ateitis po 2020 m. Skaitmeninio ir ekonominio konkurencingumo visoje Sąjungoje ir skaitmeninės sanglaudos stiprinimas“,
- Tarybos išvadas dėl Europos skaitmeninės ateities kūrimo,
- Europos Vadovų Tarybos išvadas dėl COVID- 19, bendrosios rinkos, pramonės politikos, skaitmeninių klausimų ir išorės santykių,
- Europos Komisijos komunikatą dėl Europos skaitmeninės ateities formavimo,

1. PABRĖŽIA, kad Europos Sąjunga ir jos valstybės narės turi užtikrinti savo skaitmeninį suverenumą ir strateginį savarankiškumą, kartu išsaugodamos atvirą ekonomiką. Tai apima gebėjimo savarankiškai rinktis technologinius sprendimus stiprinimą ir, kaip vieną iš pagrindinių ramsčių, atsparią ir saugią infrastruktūrą, produktus bei paslaugas, padedančius didinti pasitikėjimą bendrąja skaitmenine rinka ir pasitikėjimą Europos visuomenėje. Europos Sąjungos pagrindinėmis vertybėmis visų pirma saugomas privatumas, saugumas, lygybė, žmogaus orumas, teisinė valstybė ir atvirasis internetas – būtinos sąlygos siekiant sukurti skaitmeninę į žmogų orientuotą visuomenę, ekonomiką ir pramonę.

2. PRIPAŽĮSTA didėjančią prijungtųjų įrenginių, įskaitant mašinas, jutiklius ir tinklus, kurie sudaro daiktų internetą, ir jų saugumo svarbą. Prijungtieji įrenginiai atliks esminį vaidmenį toliau formuojant Europos skaitmeninę ateitį pramonės ir verslo požiūriu, taip pat kasdieniame naujos kartos technologijų vartotojų gyvenime. Šalia 5G ryšio, dirbtinio intelekto, kvantinės kompiuterijos, našiosios kompiuterijos, debesijos kompiuterijos, paskirstytojo registro technologijų, t. y. blokų grandinės, ir kitų naujų prietaikų, galimybės siekiant tvaraus ekonomikos augimo ir didesnio mūsų visuomenės skaitmeninimo lygmens gali būti realizuotos tik naudojant kibernetiškai saugius prijungtuosius įrenginius.

3. PAŽYMI, kad dėl didėjančio prie interneto prijungtų vartotojams skirtų produktų ir pramonės įrenginių naudojimo kartu atsiras naujų pavojų privatumui, informaciniam ir kibernetiniam saugumui, įskaitant vis didesnį galimą poveikį produktų ir duomenų vientisumui ir prieinamumui – visa tai gali turėti tiesioginį poveikį saugai. Siekiant apsaugoti vartotojus, sustiprinti bendrą Europos kibernetinį atsparumą ir padidinti piliečių pasitikėjimą skaitmeniniais sprendimais ir technologijomis, itin svarbu kuo labiau sumažinti tokius pavojus. Tai kartu skatins tokių įrenginių Europos tiekėjų konkurencingumą ir inovacinį pajėgumą. Kibernetinis saugumas ir privatumas turėtų būti pripažinti esminiais reikalavimais produktų inovacijos, gamybos ir kūrimo procesuose, įskaitant projektavimo etapą (pritaikytasis saugumas), ir turėtų būti užtikrinami per visą produkto gyvavimo ciklą ir visoje jo tiekimo grandinėje.

4. PABRĖŽIA, kad, be prijungtųjų įrenginių aukšto saugumo lygio užtikrinimo, ne mažiau svarbu didinti vartotojų informuotumą apie galimą jų privatumo ir saugumo riziką. Tai padėtų sumažinti grėsmes, kylančias dėl intensyvesnio prijungtųjų įrenginių naudojimo, padidintų pasitikėjimą bendrąja skaitmenine rinka ir leistų maksimaliai pasinaudoti prijungtųjų įrenginių technologijų teikiama ekonomine ir visuomenine nauda.

5. PABRĖŽIA, kad viešosios investicijos į mokslinius tyrimus ir inovacijas, visų pirma pagal programas „Europos horizontas“ ir „Skaitmeninė Europa“, taip pat privačiosios investicijos galėtų sukurti vertingų paskatų didinti prijungtųjų įrenginių saugą bei saugumą ir tuo pačiu – pažangiųjų ryšių tinklų atsparumą. Taip pat turėtų būti paspartintos investicijos į būtiną skaitmeninę infrastruktūrą ir technologijas siekiant diegti naujausias prijungtųjų įrenginių technologijas, kad būtų pasiekta pramonės ir skaitmeninė lyderystė ir užtikrintas strateginis savarankiškumas, kartu išsaugant atvirą ekonomiką.

6. PABRĖŽIA, kad reikia užtikrinti IRT sistemų ir IRT komponentų, naudojamų daugelyje įvairių bendrosios skaitmeninės rinkos sektorių, saugumo funkcijų aukšto lygio papildomumą ir palyginamumą.

7. GERAI VERTINA dabartinius veiksmus Sąjungos lygmeniu siekiant padidinti prijungtųjų įrenginių kibernetinio saugumo lygį, visų pirma atsižvelgiant į naujausias Komisijos iniciatyvas, kuriomis siekiama trumpuoju laikotarpiu nagrinėti kibernetinio saugumo aspektus atitinkamuose teisės aktuose, pavyzdžiui, aktuose pagal naująją teisės aktų sistemą (NTAS), visų pirma Direktyvoje 2014/53/ES (Radijo įrenginių direktyvoje). PABRĖŽIA, kad svarbu įvertinti poreikį ilguoju laikotarpiu priimti horizontalųjį teisės aktą, kuriuo, be kita ko, būtų apibrėžtos būtinos pateikimo rinkai taisyklės, kad būtų atsižvelgta į visus atitinkamus prijungtųjų įrenginių kibernetinio saugumo aspektus, pavyzdžiui, prieinamumą, vientisumą ir konfidencialumą. Šiuo atžvilgiu PALANKIAI VERTINA diskusiją siekiant išnagrinėti tokio teisės akto taikymo sritį ir jo sąsajas su kibernetinio saugumo sertifikavimo sistema, kaip apibrėžta Kibernetinio saugumo akte (KSA), siekiant padidinti saugumo lygį bendrojoje skaitmeninėje rinkoje.

8. PABRĖŽIA, kad kibernetinio saugumo reikalavimai turėtų būti apibrėžti laikantis atitinkamų Sąjungos teisės aktų, įskaitant KSA, NTAS, Reglamentą dėl Europos standartizacijos ir galimo būsimo horizontaliojo teisės akto, kad būtų išvengta teisės aktų dviprasmiškumo ir susiskaidymo.

9. PRIPAŽĮSTA svarbų visų suinteresuotųjų subjektų, visų pirma gamintojų, vaidmenį siekiant padidinti prijungtųjų įrenginių kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje, todėl RAGINA koordinuoti veiksmus ir glaudžiai bendradarbiauti su visais viešaisiais ir privačiaisiais suinteresuotaisiais subjektais, be kita ko, atsižvelgiant į galimą būsimą horizontalųjį teisės aktą.

9a. PALANKIAI VERTINA vykdomą darbą, kuriam vadovauja ENISA, siekiant parengti pirmųjų ES kibernetinio saugumo sertifikavimo schemų, t. y. siūlomų Europos Sąjungos bendrų kriterijų ir siūlomų debesijos paslaugų schemų, projektus. Šios schemos sudarys svarbų prijungtųjų įrenginių sertifikavimo pagrindą.

10. PABRĖŽIA, kad visose papildomose prijungtųjų įrenginių ir susijusių paslaugų sertifikavimo schemose, kurios būtų nustatytos tęstinėje Sąjungos darbo programoje ir apibrėžtos pagal KSA, turėtų būti nurodyta, kaip turėtų būti laikomasi taikomų saugumo reikalavimų atitinkamu saugumo užtikrinimo lygmeniu remiantis konkrečiais Europos ir tarptautiniu mastu pripažintais standartais, nepriklausomai nuo sektoriaus, kuriame produktas bus naudojamas, ir kokios testavimo specifikacijos, sertifikatai ir t. t. turi būti taikomi.

11. PRIPAŽĮSTA, kad prijungtiesiems įrenginiams sertifikuoti reikėtų taikyti atitinkamas normas, standartus ar technines specifikacijas, susijusias su kibernetinio saugumo vertinimais pagal KSA. Todėl PABRĖŽIA, kad reikia nustatyti prijungtųjų įrenginių kibernetinio saugumo normas, standartus ar technines specifikacijas, ir REKOMENDUOJA stiprinti Europos standartizacijos organizacijų pastangas šioje srityje. Kartu PAŽYMI, kad vartotojams skirtų daiktų interneto įrenginių kibernetinio saugumo standartas ETSI EN 303 645 yra svarbus žingsnis šia kryptimi.

12. PRAŠO Komisijos apsvarstyti prašymą parengti potencialias prijungtųjų įrenginių ir susijusių paslaugų kibernetinio saugumo sertifikavimo schemas remiantis šiuo metu kuriama tęstine Sąjungos darbo programa, kuo labiau atsižvelgiant į šiuo metu kuriamas horizontaliąsias Europos kibernetinio saugumo sertifikavimo schemas. Taikoma savanorišku pagrindu, tokia schema suteiks galimybę tokių produktų gamintojams reklamuoti produktus, kurių saugumo užtikrinimo lygis yra įvertintas.

13. PRAŠO aptarti, kaip kibernetinio saugumo tikslą būtų galima įtvirtinti būsimame horizontaliajame teisės akte, apimančiame kibernetinio saugumo riziką, susijusią su prijungtaisiais įrenginiais, ir kartu PAŽYMI, kad, kai tikslinga, reikia apsvarstyti galimybę pritaikyti esminius atitinkamų NTAS priklausančių direktyvų reikalavimus.

14. RAGINA Komisiją prireikus taip pat įvertinti papildomus konkretiems sektoriams taikomus reglamentus, kuriuose turėtų būti nustatyta, kokio lygio kibernetinį saugumą turėtų atitikti prijungtasis įrenginys, siekiant užtikrinti, kad tokiems įrenginiams, kurių saugumo rizika yra didesnė, būtų nustatyti specialūs saugumo ir privatumo reikalavimai.

15. PABRĖŽIA, kad reikia gerinti Europos piliečių gyvenimo kokybę bei gerovę ir stiprinti pasitikėjimą bendrąja skaitmenine rinka. Mūsų visuomenės saugumas ir privatumas yra labai svarbūs veiksniai mūsų pagrindinėms Sąjungos vertybėms išsaugoti. Todėl PABRĖŽIA, jog reikia remtis KSA nustatyta sistema, atsižvelgiant į skirtingus saugumo užtikrinimo lygius, kad visuose NTAS sektoriuose būtų suderinti saugumo reikalavimai, kad būtų išvengta susiskaidymo ir identiškų reikalavimų daugkartinių patikrų ir kad visoje Europos Sąjungoje būtų sudarytos vienodos konkurencijos ir inovacijų sąlygos.

16. RAGINA Komisiją, ES kibernetinio saugumo agentūrą (ENISA), Telekomunikacijų atitikties vertinimo ir rinkos priežiūros komitetą ir Europos kibernetinio saugumo sertifikavimo grupę (EKSSG) aktyviai dalyvauti šioje iniciatyvoje, kuria siekiama stiprinti bendrąją skaitmeninę rinką ir didinti pasitikėjimą IRT produktais, paslaugomis ir procesais, skirtais prijungtiesiems įrenginiams, užtikrinant privatumą ir kibernetinį saugumą, ir sudaryti palankesnes sąlygas didesniam Sąjungos daiktų interneto pramonės konkurencingumui pasaulyje užtikrinant aukščiausius atsparumo, saugumo ir saugos standartus.

17. Šiame kontekste PABRĖŽIA, kad reikia remti MVĮ, kurios yra vienas iš esminių Europos kibernetinio saugumo ekosistemos elementų, ir RAGINA MVĮ dalyvauti visose pradėtose viešose konsultacijose ir standartizacijos veikloje, kad būtų atsižvelgta į jų vertingą ir svarbų indėlį siekiant, kad kibernetinis saugumas taptų pasiekiamu tikslu ir konkurenciniu pranašumu Europos rinkoje.

18. PAŽYMI, kad pareiga užtikrinti kibernetinį saugumą ir privatumą per visą produkto gyvavimo ciklą ir visoje jo tiekimo grandinėje galėtų turėti teigiamą poveikį technologijų sektoriaus aplinkosauginiam pėdsakui, nes gamintojai siektų pažangių ir tvarių kūrimo ir gamybos procesų ir taip sumažėtų elektroninės įrangos atliekų, susijusių su prijungtųjų įrenginių šalinimu, kiekis.