Europos Sąjungos
Taryba

Briuselis, 2022 m. spalio 17 d.
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2022 m. spalio 17 d.
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	12930/22
Dalykas:	Tarybos išvados dėl IRT tiekimo grandinių saugumo – Tarybos išvados, kurias Taryba patvirtino 2022 m. spalio 17 d. posėdyje

Delegacijoms priede pateikiamos 2022 m. spalio 17 d. posėdyje Tarybos patvirtintos Tarybos išvados dėl IRT tiekimo grandinių saugumo.

PRIEDAS

Tarybos išvados dėl IRT tiekimo grandinių saugumo

EUROPOS SĄJUNGOS TARYBA,

PRIMINDAMA išvadas dėl:

– bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ (2017 m. lapkričio 20 d.);

– kibernetinio saugumo pajėgumų ir gebėjimų stiprinimo ES;

– 5G svarbos Europos ekonomikai ir poreikio mažinti su 5G susijusią saugumo riziką;

– Europos skaitmeninės ateities formavimo;

– perėjimą prie dinamiškesnės, atsparesnės ir konkurencingesnės Europos pramonės spartinančio ekonomikos gaivinimo;

– prijungtųjų įrenginių kibernetinio saugumo;

– Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategijos

– Europos Sąjungos pozicijos kibernetiniais klausimais parengimo;

– Europos Audito Rūmų specialiosios ataskaitos Nr. 03/2022 „5G diegimas Europos Sąjungoje. Vėlavimas diegti tinklus, kurių saugumo klausimai vis dar neišspręsti“;

PRIMINDAMA Europos Vadovų Tarybos išvadas dėl:

– COVID-19, bendrosios rinkos, pramonės politikos, skaitmeninių klausimų ir išorės santykių (2020 m. spalio 1–2 d.);

– Rusijos karinės agresijos prieš Ukrainą, saugumo ir gynybos, energetikos, ekonominių klausimų, COVID-19 ir išorės santykių (2022 m. kovo 24–25 d.);

– Ukrainos, aprūpinimo maistu saugumo, saugumo ir gynybos ir energetikos (2022 m. gegužės 30–31 d.),

1. atsižvelgdama į didėjančią geopolitikos svarbą kibernetiniam saugumui, PABRĖŽIA, kad Europos Sąjunga ir jos valstybės narės turi laikytis išsamaus ir strateginio požiūrio dėl kibernetinio saugumo. Rusijos karinė agresija prieš Ukrainą sukėlė esminį Europos Sąjungos strateginės ir saugumo aplinkos pokytį ir parodė, kad Europos Sąjunga turi būti stipresnė ir pajėgesnė saugumo ir gynybos srityje. Ji iškėlė į šviesą tai, kad į geopolitines sąlygas itin svarbu deramai atsižvelgti ne vien reaguojant į kibernetinę kenkimo veiklą, bet ir stiprinant ir išlaikant informacinių ir ryšių technologijų (IRT) atsparumą. Tai ypač svarbu kalbant apie IRT produktų ir paslaugų tiekimo grandines (IRT tiekimo grandines), kurioms gali kilti pavojus dėl geopolitinių varžybų, kaip parodė išpuolis prieš *SolarWinds*, ir kurias gali paveikti geopolitinės įtampos ir nestabilumas, kaip parodė grėsmė, susijusi su priklausomybe nuo Rusijos IRT pardavėjų, Rusijos karinės agresijos prieš Ukrainą metu;

2. PAŽYMI, kad dėl rizikos, susijusios su IRT tiekimo grandine, kurią sudaro rinkinys tarpusavyje susijusių išteklių ir procesų tarp ekonominės veiklos vykdytojų (kaip apibrėžta Reglamente (ES) 2019/1020), pradedant nuo žaliavų gavimo ir baigiant IRT produktų ir paslaugų gamyba, apdorojimu, tvarkymu ir tiekimu, įskaitant paramos teikimą IRT produktų ir paslaugų gyvavimo ciklo metu, pobūdžio kyla unikalių iššūkių ir galimai toli siekiančių pasekmių. Be rizikos, susijusios su IRT produktų neprieinamumu, pavyzdžiui, dėl jų gamybai būtinų svarbiausiųjų žaliavų ir puslaidininkių trūkumų, IRT produktų ir paslaugų tiekimo grandinėms kyla ir kitų grėsmių. Visų pirma, į jas gali nusitaikyti arba jas gali netinkamai naudoti piktavališki subjektai, darydami tai sudėtingais, dažnai slaptais būdais, turinčiais poveikį perduodamų ir saugomų neskelbtinų duomenų konfidencialumui, vientisumui ir prieinamumui;

3. sutikdama su tuo, kad IRT turtui apsaugoti reikia laikytis visus pavojus apimančio požiūrio, PRIPAŽĮSTA pasiūlymo dėl Direktyvos dėl ypatingos svarbos subjektų atsparumo svarbą, siekiant didinti ypatingos svarbos subjektų fizinį saugumą, ir PABRĖŽIA, kad vienodai svarbu stiprinti ne tik atsparumą kibernetinėmis priemonėmis vykdomiems išpuoliams prieš tiekimo grandines, bet ir bendrą IRT tiekimo grandinių atsparumą ir saugumą, kad jos atsilaikytų prieš pačius įvairiausius grėsmių veiksnius, kaip antai gamtos reiškinius, vidaus subjektų keliamą grėsmę arba žmogaus klaidas. Šiuo atžvilgiu PRIPAŽĮSTA, kad IRT tiekimo grandinių saugumas reiškia ir pagamintų, pristatytų, įgytų ir IRT tiekimo grandinėse naudojamų IRT produktų ir paslaugų apsaugos užtikrinimą, be kita ko, apsaugant atskirus komponentus ir perduodamus duomenis;

4. remdamasi patirtimi, įgyta atsižvelgiant į strateginės Europos Sąjungos priklausomybės nuo Rusijos iškastinio kuro pasekmes ir į tiekimo grandinių sutrikimų per COVID-19 pandemiją poveikį, visų pirma susijusį su medicinos produktais ir puslaidininkiais, kai atsiskleidė ES strateginė priklausomybė, RAGINA valstybes nares dirbti, kad būtų išvengta panašių nepageidaujamo strateginės priklausomybės nuo išorės situacijų, kiek tai susiję su IRT produktais ir paslaugomis. Kadangi visuomenė vis labiau pereina prie skaitmeninių technologijų ir IRT vis daugiau naudojamos ypatingos svarbos infrastruktūroje, su IRT produktais ir paslaugomis bei jų tiekimo grandinėmis susijusi strateginė priklausomybė nuo išorės turėtų būti nuolat vertinama ir, kai tikslinga, mažinama;

5. PRIMENA, kad pasiekti strateginį savarankiškumą ir kartu išlaikyti atvirą ekonomiką yra vienas iš svarbiausių Sąjungos tikslų, kuris apima strateginės priklausomybės nustatymą bei mažinimą ir atsparumo didinimą jautriausiose pramonės ekosistemose bei konkrečiose srityse, įskaitant skaitmeninę sritį. Tai apima strateginių skaitmeninių pajėgumų ir infrastruktūros plėtojimą ir diegimą, taip pat gebėjimo savarankiškai rinktis technologinius sprendimus stiprinimą ir, kaip vieną iš pagrindinių ramsčių, atsparios ir saugios infrastruktūros, produktų bei paslaugų, padedančių didinti pasitikėjimą bendrąja skaitmenine rinka ir pasitikėjimą Europos visuomenėje, užtikrinimą, kartu išlaikant atvirumą, bendradarbiavimą pasaulyje su panašiai mąstančiais partneriais ir konkurencingumą ir naudojantis galimais viso to privalumais. 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;

6. PAŽYMI, kad dėl pokyčių kibernetinių grėsmių aplinkoje, kuriuos rodo itin paveikių ir sudėtingų išpuolių prieš tiekimo grandines (pvz., prieš *SolarWinds*, *Mimecast* ar *Kaseya*) pastarųjų metų tendencija ir kurie formuojasi tuo pačiu metu, kai pagrindinės IRT paslaugos užsakomos, ir suintensyvėja dėl bendro kliovimosi trečiųjų šalių pagamintais, teikiamais ar aptarnaujamais IRT produktais ir paslaugomis, labai tikėtina, kad ateityje bus vykdoma daugiau išpuolių prieš tiekimo grandines ir taip daroma didelė žala ekonomikai bei visuomenei. Atsižvelgdama į tai, PABRĖŽIA, kad, norint užtikrinti bendrosios rinkos veikimą, svarbu stiprinti IRT tiekimo grandinių saugumą ir atsparumą ir kartu bendrojoje rinkoje būtina užtikrinti IRT produktų ir paslaugų prieinamumą, saugumą ir įvairovę. Todėl PRIPAŽĮSTA, kad, norint pasiekti šiuos tikslus, reikia kuo daugiau naudoti esamas ES priemones ir metodus ir racionalizuoti jų naudojimą, taip pat nuolat taikytis prie kintančios kibernetinių grėsmių aplinkos, nustatant papildomas tinkamas priemones ir mechanizmus, be kita ko, susijusius su galima besiformuojančių perversminių technologijų saugumo rizika. šiuo atžvilgiu RAGINA valstybes nares naujos technologinės plėtros keliamus klausimus spręsti laikantis rizika grindžiamo požiūrio;

7. PRIPAŽĮSTA, kad siekiant veiksmingai sumažinti su IRT tiekimo grandinėmis susijusią riziką, būtina suprasti nuolat kintančią kibernetinių grėsmių aplinką ir išpuolių prieš tiekimo grandines sudėtingumą. Šiuo atžvilgiu AKCENTUOJA, kad reikia prie naujų grėsmių prisitaikyti aktyviai ir nuolat stebint, analizuojant ir vertinant tiekimo grandinėms kylančių grėsmių aplinką, didinti informuotumą ir kaupti žinias apie grėsmes bei pažeidžiamumą ir aktyviai, specialiai nustatytu būdu perspėti atitinkamus subjektus. PALANKIAI VERTINA Europos Sąjungos kibernetinio saugumo agentūros (ENISA) darbą, susijusį su IRT tiekimo grandinių saugumu, visų pirma jos ataskaitą dėl išpuolių prieš tiekimo grandines grėsmių aplinkos;

TARPSEKTORINĖS PRIEMONĖS IR METODAI

8. DAR KARTĄ PATVIRTINA, kad svarbu, jog valstybės narės apsvarstytų poreikį turėti įvairių ypatingos svarbos IRT tiekėjų, siekiant išvengti didelės priklausomybės nuo vieno tiekėjo, ypač didelės rizikos tiekėjo, susiformavimo arba apriboti šį procesą, nes tai didina galimų sutrikimų padarinių riziką. PRIPAŽĮSTA, kad vienas iš svarbių vidaus rinkos stabilumo ir saugumo užtikrinimo elementų yra susaistymo su pardavėju vengimas ir IRT tiekėjų įvairinimas. PABRĖŽIA, kad reikia skatinti ir įgyvendinti deramas strategijas, kuriomis technologijų atžvilgiu neutraliai sudaromos sąlygos pardavėjų įvairinimui ir konkurencingumui. Be to, RAGINA į ES teisės aktus integruoti aspektus, susijusius su susaistymo su pardavėju prevencija. Šiuo atžvilgius GERAI VERTINA pasiūlymą dėl Reglamento dėl suderintų sąžiningos prieigos prie duomenų ir jų naudojimo taisyklių (Duomenų akto), kuriuo siekiama didinti duomenų tvarkymo paslaugų sąveikumą ir šalinti kliūtis pakeisti duomenų tvarkymo paslaugų teikėją;

9. PRIPAŽĮSTA IRT tiekimo grandinių saugumo ir viešųjų pirkimų sąsają. PABRĖŽIA, kad viešųjų pirkimų procedūrose turi būti deramai atsižvelgiama į IRT tiekimo grandinių saugumo svarbą, nustatant, kai tikslinga, objektyvius ir rizika grindžiamus atrankos kriterijus, susijusius su konkurso dalyvių pajėgumu užtikrinti aukštą teikiamų paslaugų saugumo lygį. RAGINA rasti tinkamą pusiausvyrą tarp viešojo intereso kuo efektyviau ir sąžiningiau panaudoti viešąsias lėšas ir viešojo intereso apsaugoti informacines sistemas ir užtikrinti sklandų bendrosios rinkos veikimą. Siekiant sudaryti palankesnes sąlygas įgyvendinti atitinkamas viešųjų pirkimų taisykles atsižvelgiant į kibernetinio saugumo didinimą, PRAŠO Komisijos ne vėliau kaip 2023 m. trečiąjį ketvirtį parengti metodines gaires, siekiant paskatinti perkančiąsias organizacijas skirti tinkamą dėmesį konkurso dalyvių ir jų subrangovų kibernetinio saugumo praktikai, ir įvertinti atitinkamus viešųjų pirkimų teisės aktus, o prireikus pateikti pasiūlymų juos peržiūrėti ar papildyti;

10. PRIPAŽĮSTA, kad nors su IRT produktais ir paslaugomis susijusios tiesioginės užsienio investicijos ir teikia ekonominę ir socialinę naudą valstybėms narėms, įmonėms ir piliečiams, jos taip pat gali kelti riziką saugumui ir viešajai tvarkai, ir PAŽYMI, kad ES tiesioginių užsienio investicijų tikrinimo mechanizmas kartu su atitinkamomis nacionalinėmis tikrinimo sistemomis, kuriose nustatytos tokios rizikos mažinimo priemonės, galėtų būti taikomas ir kaip naudinga priemonė IRT tiekimo grandinių saugumui ir atsparumui apsaugoti ir padėti eliminuoti didelės rizikos investicijas, galinčias pakenkti tokiam saugumui ar atsparumui. PRIPAŽĮSTA, kad keičiantis ar dalijantis informacija pagal šį mechanizmą valstybėms narėms gali būti lengviau geriau įvertinti galimas grėsmės IRT teikimo grandinių saugumui ir atitinkamai imtis reikiamų veiksmų. RAGINA atitinkamus nacionalinius subjektus taip pat, kai tikslinga, atsižvelgti į šį tikrinimo mechanizmo aspektą;

11. kalbant apie gynybą, DAR KARTĄ PATVIRTINA, kad prašo Komisijos kartu su valstybėmis narėmis 2023 m. įvertinti ypatingos svarbos infrastruktūros tiekimo grandinių riziką įvairiose srityse, įskaitant skaitmeninę sritį, susijusiose su ES saugumo ir gynybos interesais, ir išnagrinėti galimybes didinti kibernetinį saugumą visoje ES gynybos technologinės ir pramoninės bazės tiekimo grandinėje. Be to, PRAŠO valstybių narių ir Komisijos apsvarstyti IRT tiekimo grandinių saugumo klausimą įgyvendinant Strateginio kelrodžio įsipareigojimus ir veiksmus;

12. pripažindama svarbiausiųjų žaliavų ir visų rūšių puslaidininkių, kaip pagrindinių IRT produktų sudedamųjų dalių, svarbą, RAGINA konstruktyviai derėtis dėl pasiūlymo dėl Reglamento, kuriuo nustatoma Europos puslaidininkių ekosistemos stiprinimo priemonių sistema (Lustų akto), ir dėl pasiūlymo dėl Tarybos reglamento, kuriuo keičiamos Reglamento (ES) 2021/2085, kuriuo pagal programą „Europos horizontas“ steigiamos bendrosios įmonės, nuostatos, susijusios su Lustų bendrąja įmone;

KIBERNETINEI SRIČIAI SKIRTOS PRIEMONĖS

13. konkrečiai kalbant apie telekomunikacijų infrastruktūrą, PRIPAŽĮSTA Sąjungos lygmens pasiekimus didinant 5G tinklų tiekimo grandinių saugumą, visų pirma pasitelkiant ES 5G saugumo priemonių rinkinį (ES 5G priemonių rinkinį). RAGINA valstybes nares toliau keistis informacija apie priemonių, rekomenduojamų ES 5G priemonių rinkinyje, įgyvendinimo geriausią praktiką bei metodiką ir visų pirma taikyti atitinkamus apribojimus pagrindinių objektų, kurie ES suderintame rizikos vertinime apibrėžiami kaip ypatingos svarbos ir pažeidžiamiausi objektai, didelės rizikos tiekėjams. AKCETUOJA, kad ES 5G priemonių rinkinys yra dinamiška rizika grindžiama priemonė, skirta nustatytiems saugumo iššūkiams įveikti, kuri sudaro sąlygas laiku ir veiksmingai spręsti su 5G kibernetinio saugumo aspektais susijusius klausimus, kartu atsižvelgiant į valstybių narių kompetenciją, ir PRIPAŽĮSTA, kad tai yra vertinga priemonė visiškai skaidriai ir koordinuotai toliau didinti telekomunikacijų tinklų tiekimo grandinių saugumą, kuria gali būti remiamasi rengiant rizikos vertinimo ir mažinimo priemones, susijusias su kitais itin svarbiais sektoriais. PRIMENA, kad atitinkamos institucijos raginamos parengti rizikos vertinimais grindžiamas rekomendacijas valstybėms narėms ir Komisijai, kad būtų stiprinami atsparumo ryšių tinklai ir infrastruktūra Europos Sąjungoje, įskaitant tolesnį ES 5G priemonių rinkinio įgyvendinimą;

14. PAŽYMI, kad svarbu taikyti sąveikius metodus, kuriais galima spręsti susaistymo su pardavėju klausimą ir sumažinti koncentracijos riziką, kartu gerinant tiekimo grandinių saugumą per visą IRT infrastruktūros ir paslaugų spektrą. Visų pirma kiek tai susiję su 5G tinklais, jų atžvilgiu PRIPAŽĮSTA galimą atvirųjų radijo prieigos tinklų (RAN) koncepcijos naudą ir kartu PRIMENA apie TIS bendradarbiavimo grupės paskelbtą Ataskaitą dėl atvirųjų RAN kibernetinio saugumo, kurioje pažymima, kad ši koncepcija vis dar plėtojama, o jų saugumas, skaidrumas ir standartizavimas yra ankstyvame užbaigtumo etape, ir PABRĖŽIA, kad svarbu įvertinti riziką prieš pereinant prie naujų standartų ar architektūros;

15. AKCETUOJA, kad siekiant didinti IRT tiekimo grandinių saugumą, svarbūs yra esami ir būsimi kibernetinio saugumo horizontalieji teisės aktai, visų pirma Reglamentas dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo (Kibernetinio saugumo aktas), būsima Direktyva dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2), pasiūlymas dėl Reglamento, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti, taip pat pasiūlymas dėl Reglamento dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams (Kibernetinio atsparumo aktas). Be to, ATKREIPIA DĖMESĮ į svarbius pokyčius, susijusius su konkretiems sektoriams skirtais kibernetinio saugumo reglamentais, visų pirma būsimu Reglamentu dėl skaitmeninės veiklos atsparumo finansų sektoriuje (SVAA), į kurį įtraukta IRT paslaugas teikiančių trečiųjų šalių, kurios yra ypatingos svarbos finansų sektoriaus subjektams, priežiūros sistema. Šiais reglamentais nustatomos bendrosios pareigos, susijusios su tiekimo grandinių saugumu, taip pat atitinkamam sektoriui aktualūs išsamūs ir konkretūs reikalavimai. Kartu PABRĖŽIA, kad tiekėjai dažnai tiekia savo produktus ir teikia paslaugas įvairiuose, o ne viename pramonės sektoriuje. Todėl labai svarbu užtikrinti, kad tiekimo grandinių saugumo reikalavimai, kiek įmanoma, būtų suderinti visuose atitinkamuose sektoriuose, ypač tuose, kuriems bus taikoma būsima TIS 2 direktyva, siekiant išvengti tiekėjams nustatytų pareigų neatitikimų ir palengvinti naštą, tenkančią ypatingos svarbos sektorių veiklos vykdytojams vertinant, kaip tiekėjai vykdo tas pareigas, kartu atsižvelgiant į sektoriaus ypatumus;

16. PALANKIAI VERTINA pasiūlymą dėl Kibernetinio atsparumo akto, kaip svarbią teisėkūros priemonę, kuria siekiama paspartinti saugų skaitmeninių elementų turinčių produktų kūrimą ir užtikrinti kibernetinį saugumą per visą skaitmeninių elementų turinčių produktų gyvavimo ciklą. PAŽYMI, kad pasiūlymas dėl Kibernetinio atsparumo akto gali reikšmingai prisidėti prie IRT tiekimo grandinių saugumo stiprinimo. RAGINA vesti konstruktyvias derybas ir laiku priimti šį aktą;

17. šiuo atžvilgiu PRIPAŽĮSTA darbą, kurį ENISA vykdo kartu su valstybėmis narėmis ir kitais suinteresuotaisiais subjektais ir kuriam vadovauja, siekiant ES parengti Kibernetinio saugumo aktą atitinkančias IRT produktų, paslaugų ir procesų sertifikavimo schemas, kurios turėtų padėti didinti bendrą kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. RAGINA visus suinteresuotuosius subjektus dalyvauti parengiamajame darbe dėl atskirų Europos sertifikavimo schemų, siekiant didinti pasitikėjimą saugiais IRT produktais, procesais bei paslaugomis ir stiprinti jų atsparumą, ir RAGINA Komisiją užbaigus parengiamąjį darbą skubiai parengti įgyvendinimo aktus dėl Europos sertifikavimo schemų, visų pirma dėl bendrais kriterijais grindžiamos Europos kibernetinio saugumo sertifikavimo schemos (EUCC). PAŽYMI, kad Europos sertifikavimo schemos prireikus turėtų apimti tiekimo grandinės saugumo reikalavimus, įskaitant santykius su tiekėjais;

18. AKCETUOJA, kad reikia visapusiškai įgyvendinti visas būsimas TIS 2 nuostatas, susijusias su IRT tiekimo grandinių saugumu. Šiuo atžvilgiu PABRĖŽIA, kad yra svarbūs ES suderinti ypatingos svarbos tiekimo grandinių rizikos vertinimai (suderinti tiekimo grandinių rizikos vertinimai), nacionalinė tiekimo grandinių saugumo politika ir su tiekimo grandinėmis susijusios saugumo priemonės. PAŽYMI, kad kalbant apie riziką pirminio tiekėjo ar galutinio vartotojo saugumui reikėtų atkreipti dėmesį ne tik į pirminius tiekėjus, bet ir į atitinkamus subrangovus. Kad būtų sudarytos palankesnės sąlygos įgyvendinti tiekimo grandinių rizikos valdymo priemones, RAGINA ENISA, padedant TIS bendradarbiavimo grupei, apibendrinti geriausią praktiką, susijusią su tiekimo grandinių rizikos valdymu, ir įtraukti ją į metodines gaires. Be to, RAGINA ENISA stebėti pagal būsimą TIS 2 direktyvą reglamentuojamų subjektų investicijas į IRT tiekimo grandinių saugumą;

19. taip pat ATKREIPIA DĖMESĮ į tiekimo grandinių saugumo kontekste gaunamą naudą ir riziką, kai pasitelkiami valdomų paslaugų teikėjai (VPT) ir valdomų saugumo paslaugų teikėjai (VSPT). Pasitelkus šiuos paslaugų teikėjus galima reikšmingai padidinti saugumą organizacijose ir pasiekti aukštesnį kibernetinio saugumo lygį, tačiau nuotolinis IRT sistemų ir paslaugų valdymas kartu su privilegijuota prieiga prie klientų IRT aplinkos, kurios gali prireikti VPT ir VSPT, gali (tuo atveju, jei kiltų pavojus VPT ir VSPT) turėti stiprų grandininį poveikį dideliam skaičiui klientų. Todėl itin svarbu, kad VPT ir VSPT išlaikytų aukštą savo pačių vidaus ir teikiamų paslaugų saugumo lygį ir laikytųsi skaidraus požiūrio į savo klientus, kiek tai susiję su teikiamų paslaugų saugumu. Šiuo atžvilgiu PALANKIAI VERTINA tai, kad ateityje jos bus įtrauktos į būsimos TIS 2 direktyvos taikymo sritį;

20. kalbant apie suderinto tiekimo grandinių rizikos vertinimo mechanizmo įgyvendinimą pagal būsimą TIS 2 direktyvą, PAŽYMI, kad šiame kontekste yra svarbūs netechniniai rizikos veiksniai, pavyzdžiui, nederama trečiosios valstybės įtaka tiekėjams ir paslaugų teikėjams, ir šiame kontekste PRIPAŽĮSTA veiksnius, kurie gali būti naudojami vertinant rizikos profilį, kaip nurodyta ES suderintame 5G tinklų kibernetinio saugumo rizikos vertinime. PRAŠO Komisijos, pasikonsultavus su TIS bendradarbiavimo grupe ir ENISA, ne vėliau kaip 2023 m. antrąjį ketvirtį nustatyti konkrečias IRT paslaugas, sistemas ar produktus, kuriems prioritetine tvarka galėtų būti taikomi suderinti tiekimo grandinių rizikos vertinimai;

21. PAŽYMI, kad priklausomybė nuo didelės rizikos tiekėjų, kurie tiekia IRT produktus ir teikia paslaugas, naudojamas eksploatuojant ypatingos svarbos tinklus ir sistemas, kelia strateginę grėsmę, kuri turi būti mažinama taikant tinkamą politiką tiek nacionaliniu, tiek ES lygmeniu, taip pat valstybėms narėms bendradarbiaujant tarpusavyje ir su panašiai mąstančiais tarptautiniais partneriais. Kad būtų sudarytos palankesnės sąlygos mažinti šią strateginę riziką ir remiami suderinti tiekimo grandinių rizikos vertinimai, PRAŠO TIS bendradarbiavimo grupės, bendradarbiaujant su Komisija ir ENISA, parengti ypatingos svarbos IRT tiekimo grandinių rizikos mažinimo priemonių rinkinį (IRT tiekimo grandinių priemonių rinkinį). IRT tiekimo grandinių priemonių rinkinys turėtų būti grindžiamas IRT tiekimo grandinėms nustatytais strateginiais grėsmių scenarijais ir jame turėtų būti numatytos reagavimo į šiuos scenarijus priemonės, remiantis su 5G priemonių rinkiniu susijusia ir nacionaliniu lygmeniu įgyta patirtimi. Jis turėtų skaidriai papildyti pagal būsimą TIS 2 direktyvą atliekamus konkrečių IRT paslaugų, sistemų ar produktų suderintus tiekimo grandinių rizikos vertinimus, pasiūlant bendrąsias rizikos mažinimo priemones, kurias įvairiu mastu galima pritaikyti konkrečioms IRT paslaugoms, sistemoms ar produktams, remiantis rizika, nustatyta atliekant individualius suderintus tiekimo grandinių rizikos vertinimus;

22. PABRĖŽIA svarbų mokslinių tyrimų, inovacijų, investicijų ir verslo veiklos vaidmenį skaitmeninėje ir kibernetinio saugumo srityje, taip pat tokios veiklos finansavimo vaidmenį siekiant išvengti galimos nepageidaujamos strateginės priklausomybės ateityje ir stiprinti bendrą IRT tiekimo grandinių atsparumą. Šiame kontekste PABRĖŽIA Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro ir Nacionalinių koordinavimo centrų tinklo (ECCC) strateginių ir įgyvendinimo užduočių vaidmenį ir svarbą siekiant prisidėti prie kuo didesnio investicijų poveikio, kad būtų stiprinama Sąjungos lyderystė ir atviras strateginis savarankiškumas kibernetinio saugumo srityje ir Sąjungos parama technologiniams pajėgumams bei įgūdžiams ir didinamas Sąjungos konkurencingumas pasaulyje. Šiuo atžvilgiu RAGINA užtikrinti, kad ECCC greitai pradėtų veikti. PRAŠO ECCC savo strateginėje darbotvarkėje atsižvelgti į IRT tiekimo grandinių saugumo aspektus, įskaitant, pavyzdžiui, saugios programinės įrangos kūrimą, kartu užtikrinant nuoseklumą bei papildomumą ir vengiant bet kokio pastangų dubliavimo. REMIA Europos konkurencingumo didinimą kibernetinio saugumo srityje pasitelkiant finansavimo programas, pavyzdžiui, mokslinių tyrimų ir inovacijų programą „Europos horizontas“, taip pat Skaitmeninės Europos programą, kuria siekiama stiprinti, kurti ir įgyti pagrindinius ES skaitmeninės ekonomikos, visuomenės ir demokratijos pajėgumams;

PARAMOS MECHANIZMAI

23. RAGINA didinti finansinės paramos paskatas, susijusias su priemonėmis, kuriomis siekiama stiprinti IRT tiekimo grandinių saugumą. RAGINA prioritetine tvarka, taip pat atsižvelgiant į būsimą TIS 2 direktyvos įgyvendinimą, ECCC, Komisiją ir atitinkamus suinteresuotuosius subjektus išnagrinėti galimybes įtraukti IRT tiekimo grandinės saugumo aspektus į būsimus kvietimus teikti pasiūlymus pagal Skaitmeninės Europos programos ir programos „Europos horizontas“ kibernetinio saugumo darbo programas arba bet kokias kitas aktualias finansavimo galimybes. Šiomis finansavimo galimybėmis, be kita ko, turėtų būti siekiama suteikti organizacijoms galimybę padėti išlaikyti aukštą kibernetinio saugumo lygį IRT produktų ir paslaugų viešųjų pirkimų visoje tiekimo grandinėje atžvilgiu, visų pirma kiek tai susiję su konkrečių ypatingos svarbos IRT paslaugų, sistemų ar produktų, kurie remiantis būsimais suderintais tiekimo grandinių rizikos vertinimais bus pripažinti esančiais didelės rizikos, pakeitimu;

24. PRIPAŽĮSTA, kad dėl globalizacijos ir IRT paslaugų specializacijos bei didesnės priklausomybės nuo trečiųjų šalių produktų ir paslaugų kyla poreikis glaudžiai bendradarbiauti ES ir tarptautiniu mastu atitinkamiems suinteresuotiesiems subjektams dalijantis žiniomis ir patirtimi, ir RAGINA juos rasti tvirtą ir suderintą poziciją, kuria būtų visapusiškai užtikrintas IRT tiekimo grandinių saugumas. Taip pat PRIPAŽĮSTA, kad reikia toliau nagrinėti atitinkamus pažangiausius metodus ir būdus, susijusius tiek su tinkama pagrindine kibernetine higiena, tiek su ilgalaikiais sprendimais saugioms ir atsparioms IRT tiekimo grandinėms užtikrinti, taip pat tinkamiausius jų propagavimo ir galimo įtraukimo į politiką ar kitas iniciatyvas būdus. Šiuo atžvilgiu PRIPAŽĮSTA, kad ypatingas dėmesys turėtų būti skiriamas sisteminių sprendimų, pavyzdžiui, nulinio pasitikėjimo principų, programinės įrangos komplektavimo specifikacijų ir panašių ilgalaikių sprendimų, naudos ir trūkumų nagrinėjimui. REKOMENDUOJA tuo tikslu pasitelkti TIS bendradarbiavimo grupę;

25. ATKREIPIA DĖMESĮ į stebėsenos ir veiksmingo keitimosi informacija apie kibernetinius incidentus ir grėsmes naudą siekiant užkirsti kelią išpuoliams prieš tiekimo grandines, juos aptikti ir sumažinti jų poveikį. PABRĖŽIA, kad reikia toliau stiprinti valstybių narių tarpusavio pasitikėjimą, kad būtų veiksmingai dalijamasi tokia informacija. Šiuo atžvilgiu PRIMENA apie Komisijos pasiūlymą padėti valstybėms narėms steigti ir stiprinti saugumo operacijų centrus (SOC) siekiant visoje ES sukurti SOC tinklą, kad būtų atidžiau stebimi išpuolių prieš tinklus signalai ir tam būtų iš anksto pasirengta. PRIMENA, kad reikia užtikrinti papildomumą ir koordinavimą esamuose tinkluose ir mechanizmuose, visų pirma šiuo atžvilgiu AKCENTUOJA CSIRT tinklo vaidmenį ir tai, kad reikia toliau nagrinėti šių tinklų potencialą siekiant propaguoti veiksmingą, saugią ir patikimą dalijimosi informacija kultūrą. PRIMENA, kad valstybės narės ėmėsi pastangų (remiamų ES) įsteigti sektorines, nacionalines ir regionines reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT) ir nacionalinius arba europinius keitimosi informacija ir jos analizės centrus (ISAC), kurie yra veiksmingo kibernetinio saugumo partneryščių tinklo Sąjungoje dalis;

26. kadangi IRT tiekimo grandinių grėsmės yra tarpusavyje susijusios ir pasaulinio pobūdžio, AKCENTUOJA, kad svarbu siekti IRT tiekimo grandinių saugumo ir jį didinti pasauliniu lygmeniu. Todėl REKOMENDUOJA naudotis skaitmeninėmis partnerystėmis, dialogais kibernetikos klausimais ir kitomis atitinkamomis ES iniciatyvomis, įskaitant, kai tinkama, laisvosios prekybos susitarimus, siekiant skatinti rizika grindžiamus IRT produktų tiekėjų ir IRT paslaugų teikėjų vertinimus, naudotis patikimų tiekėjų paslaugomis ir saugia ir novatoriška skaitmenine ekosistema, grindžiama atvirais, sąveikiais ir skaidriais standartais. Be to, PAKARTOJA „Global Gateway“ partneryščių, taip pat ES ir JAV prekybos ir technologijų tarybos viziją, taip pat jos darbo grupėse vykdomą veiklą, siekiant skatinti naudotis patikimų / ne didelės rizikos tiekėjų paslaugomis ir sukurti finansavimo mechanizmą, kuris sudarytų sąlygas vykdyti projektus, dėl kurių IRT infrastruktūra ir paslaugos trečiosiose valstybėse taptų saugesnės, atsparesnės ir patikimesnės, be kita ko, nefinansuojant pirkimų iš nepatikimų / didelės rizikos tiekėjų technologiniu požiūriu neutraliu būdu;

27. DAR KARTĄ PATVIRTINA savo įsipareigojimą prisidėti prie atviros, laisvos, pasaulinės, stabilios ir saugios kibernetinės erdvės ir ją propaguoti, taip pat laikytis JT sistemoje nustatytų atsakingo valstybių elgesio kibernetinėje erdvėje normų, taisyklių ir principų. Kalbant konkrečiai apie IRT tiekimo grandinės saugumą, PRIMENA JT Vyriausybių ekspertų grupės ir neribotos sudėties darbo grupės patvirtintą normą, pagal kurią valstybės raginamos imtis pagrįstų tiekimo grandinės vientisumo užtikrinimo veiksmų, be kita ko, rengiant objektyvias bendradarbiavimo priemones, kad galutiniai naudotojai galėtų pasitikėti IRT produktų saugumu, ir siekti užkirsti kelią kenkėjiškų IRT priemonių ir metodų plitimui ir žalingų paslėptų funkcijų naudojimui, ir PASISAKO už jos plataus masto įgyvendinimą.