Rada
Európskej únie

V Bruseli 17. októbra 2022
(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

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	17. októbra 2022
Komu:	Delegácie
Č. predch. dok.:	12930/22
Predmet:	Závery Rady o bezpečnosti dodávateľského reťazca IKT – závery Rady, ktoré Rada schválila na zasadnutí 17. októbra 2022

Delegáciám v prílohe zasielame závery Rady o bezpečnosti dodávateľského reťazca IKT, ktoré Rada schválila na svojom zasadnutí 17. októbra 2022.

PRÍLOHA

Závery Rady o bezpečnosti dodávateľského reťazca IKT

RADA EURÓPSKEJ ÚNIE,

PRIPOMÍNAJÚC svoje závery o

– spoločnom oznámení Európskemu parlamentu a Rade z 20. novembra 2017: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ,

– budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ,

– význame 5G pre európske hospodárstvo a potrebe zmierniť bezpečnostné riziká spojené s 5G,

– formovaní digitálnej budúcnosti Európy,

– obnove, ktorá urýchľuje prechod na dynamickejší, odolnejší a konkurencieschopnejší európsky priemysel,

– kybernetickej bezpečnosti pripojených zariadení,

– stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu,

– vývoji prístupu Európskej únie ku kybernetickej bezpečnosti ,

– o osobitnej správe Európskeho dvora audítorov č. 03/2022 s názvom „Zavádzanie sietí 5G v EÚ: oneskorenie v zavádzaní sietí, pričom bezpečnostné otázky zostávajú nevyriešené“,

PRIPOMÍNAJÚC závery Európskej rady na témy:

– COVID-19, jednotný trh, priemyselná politika, digitálne a vonkajšie vzťahy z 1. – 2. októbra 2020,

– vojenská agresia Ruska voči Ukrajine, bezpečnosť a obrana, energetika, hospodárske otázky, COVID-19 a vonkajšie vzťahy z 24. – 25. marca 2022,

– Ukrajina, potravinová bezpečnosť, bezpečnosť a obrana a energetika z 30. – 31. mája 2022,

1. Vzhľadom na rastúci význam geopolitiky pre kybernetickú bezpečnosť ZDÔRAZŇUJE, že Európska únia a jej členské štáty musia pristupovať ku kybernetickej bezpečnosti komplexným a strategickým spôsobom. Ruská vojenská agresia voči Ukrajine významne zmenila strategické a bezpečnostné prostredie Európskej únie a poukázala na potrebu silnejšej a schopnejšej Európskej únie v oblasti bezpečnosti a obrany. Podčiarkla, že je mimoriadne dôležité náležite zohľadniť geopolitické prostredie nielen pri reakcii na škodlivé kybernetické činnosti, ale aj pri budovaní a udržiavaní odolnosti informačných a komunikačných technológií (IKT). To má osobitný význam pre dodávateľské reťazce produktov a služieb IKT (dodávateľské reťazce IKT), ktoré môžu byť ohrozené geopolitickou rivalitou, ako to dokazuje útok SolarWinds, a súčasne na ne má vplyv geopolitické napätie a nestabilita, čo dokazuje hrozba súvisiaca so závislosťou od ruských predajcov IKT v čase vojenskej agresie Ruska voči Ukrajine.

2. KONŠTATUJE, že charakter rizík spojených s dodávateľským reťazcom IKT, ktorý pozostáva z prepojeného súboru zdrojov a procesov medzi hospodárskymi subjektmi (ako sú vymedzené v nariadení (EÚ) 2019/1020), ktorý sa začína získavaním surovín a zahŕňa výrobu a spracovanie produktov a služieb IKT, manipuláciu s nimi a ich dodávanie vrátane poskytovania podpory počas životného cyklu produktov a služieb IKT, prináša jedinečné výzvy a potenciálne ďalekosiahle dôsledky. Okrem rizík súvisiacich s nedostupnosťou produktov IKT, napríklad z dôvodu nedostatku kritických surovín a polovodičov potrebných na ich výrobu, sú dodávateľské reťazce produktov a služieb IKT vystavené aj iným hrozbám. Môžu byť najmä objektom rafinovaných a často utajených cielených útokov alebo zneužívania zo strany škodlivých aktérov, čo má vplyv na dôvernosť, integritu a dostupnosť prenášaných a uchovávaných citlivých údajov.

3. Uznávajúc, že pri zabezpečovaní aktív IKT je potrebný prístup zohľadňujúci všetky riziká, POTVRDZUJE význam návrhu smernice o odolnosti kritických subjektov s cieľom zlepšiť fyzickú bezpečnosť kritických subjektov a ZDÔRAZŇUJE, že okrem zvýšenia odolnosti proti útokom na dodávateľské reťazce, ku ktorým dochádza prostredníctvom kybernetických prostriedkov, je rovnako dôležité posilniť celkovú odolnosť a bezpečnosť dodávateľských reťazcov IKT voči celej škále hrozieb, ako sú prírodné udalosti, systémové zlyhania, vnútorné hrozby alebo ľudské chyby. V tomto zmysle UZNÁVA, že bezpečnosť dodávateľského reťazca IKT zahŕňa zaistenie ochrany produktov a služieb IKT, ktoré sa vyrábajú, dodávajú, obstarávajú a používajú v dodávateľských reťazcoch IKT, a to aj prostredníctvom ochrany jednotlivých komponentov a prenášaných údajov.

4. Na základe ponaučení z dôsledkov strategických závislostí Európskej únie od ruských fosílnych palív, ako aj z vplyvov narušení dodávateľských reťazcov počas pandémie COVID-19, najmä v súvislosti s liekmi a polovodičmi, kde boli odhalené strategické závislosti EÚ, NABÁDA členské štáty, aby sa usilovali o zabránenie podobným situáciám neželaných strategických vonkajších závislostí v súvislosti s produktmi a službami IKT. Vzhľadom na rastúcu digitalizáciu spoločnosti a čoraz väčšie využívanie IKT v kritickej infraštruktúre by sa strategické vonkajšie závislosti súvisiace s produktmi a službami IKT a ich dodávateľskými reťazcami mali nepretržite posudzovať a v prípade potreby riešiť.

5. PRIPOMÍNA, že dosiahnutie strategickej autonómie pri súčasnom zachovaní otvoreného hospodárstva je kľúčovým cieľom Únie, ktorý zahŕňa identifikáciu a zníženie strategických závislostí a zvýšenie odolnosti v najcitlivejších priemyselných ekosystémoch a špecifických oblastiach vrátane digitálnej oblasti. To zahŕňa rozvoj a zavádzanie strategických digitálnych kapacít a infraštruktúry, ako aj posilnenie schopnosti prijímať autonómne technologické rozhodnutia a, ako jeden z hlavných pilierov, zabezpečenie odolných a bezpečných infraštruktúr, produktov a služieb na budovanie dôvery v digitálny jednotný trh a v rámci európskej spoločnosti, a to pri súčasnom zachovaní otvorenosti, globálnej spolupráce s podobne zmýšľajúcimi partnermi a hospodárskej súťaže, ako aj využitie ich potenciálnych prínosov. Základné hodnoty Európskej únie spočívajú najmä v zachovaní súkromia, bezpečnosti, rovnosti, ľudskej dôstojnosti, zásad právneho štátu a otvoreného internetu ako predpokladoch dosiahnutia spoločnosti, hospodárstva a priemyslu opierajúcich sa o digitálny rozvoj a zameraných na človeka.

6. KONŠTATUJE, že vzhľadom na vývoj panorámy kybernetických hrozieb, ktorý sa v posledných rokoch prejavuje trendom vysoko účinných a rafinovaných útokov na dodávateľské reťazce, ako sú útoky SolarWinds, Mimecast alebo Kaseya, ktoré sa objavujú spolu s outsourcingom základných služieb IKT a ktoré zintenzívňuje celková závislosť od produktov a služieb IKT vyrábaných, poskytovaných alebo servisovaných tretími stranami, je vysoko pravdepodobné, že k útokom na dodávateľské reťazce so značnými škodami pre hospodárstvo a spoločnosť bude dochádzať aj v budúcnosti. V tejto súvislosti ZDÔRAZŇUJE význam posilnenia bezpečnosti a odolnosti dodávateľských reťazcov IKT pre fungovanie jednotného trhu spolu s potrebou zaistiť dostupnosť, bezpečnosť a rozmanitosť produktov a služieb IKT na jednotnom trhu. Preto UZNÁVA potrebu maximalizovať a zefektívniť využívanie existujúcich nástrojov a prístupov EÚ na dosiahnutie týchto cieľov, ako aj potrebu neustále sa prispôsobovať meniacej sa panoráme kybernetických hrozieb zavedením ďalších vhodných opatrení a mechanizmov, a to aj vo vzťahu k možným bezpečnostným rizikám vznikajúcich a prelomových technológií. NABÁDA členské štáty, aby v tejto súvislosti uplatňovali prístup zohľadňujúci riziká s cieľom zaoberať sa novými vývojovými trendmi v oblasti technológií.

7. UZNÁVA, že na účinné zmiernenie rizík spojených s dodávateľskými reťazcami IKT je nevyhnutné pochopenie neustále sa vyvíjajúcej panorámy kybernetických hrozieb, ako aj zložitosti útokov na dodávateľské reťazce. V tejto súvislosti ZDÔRAZŇUJE, že je potrebné prispôsobiť sa novým hrozbám aktívnym a nepretržitým monitorovaním, analýzou a posudzovaním panorámy hrozieb v dodávateľskom reťazci, zvyšovať informovanosť a získavať poznatky o hrozbách a zraniteľných miestach a proaktívne upozorňovať jednotlivé príslušné subjekty spôsobom, ktorý je pre ne vhodný. VÍTA prácu Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) týkajúcu sa bezpečnosti dodávateľského reťazca IKT, najmä jej správu o panoráme hrozieb, pokiaľ ide o útoky na dodávateľské reťazce.

MEDZISEKTOROVÉ NÁSTROJE A PRÍSTUPY

8. Opätovne POTVRDZUJE, že je dôležité, aby členské štáty zvážili potrebu diverzifikácie dodávateľov kritických IKT s cieľom zabrániť vzniku veľkých závislostí od jednotlivých dodávateľov, a najmä vysokorizikových dodávateľov, alebo ho obmedziť, keďže sa tým zvyšuje vystavenie dôsledkom možných narušení. UZNÁVA, že vyhýbanie sa odkázanosti na určitého dodávateľa a diverzifikácia dodávateľov IKT sú jedným z dôležitých prvkov na zabezpečenie stability a bezpečnosti vnútorného trhu. ZDÔRAZŇUJE, že je potrebné podporovať a vykonávať vhodné stratégie uľahčujúce diverzifikáciu dodávateľov a hospodársku súťaž technologicky neutrálnym spôsobom. Okrem toho NABÁDA na začlenenie aspektov súvisiacich s predchádzaním odkázanosti na určitého dodávateľa do právnych predpisov EÚ. V tejto súvislosti BERIE NA VEDOMIE návrh nariadenia o harmonizovaných pravidlách týkajúcich sa spravodlivého prístupu k údajom a ich používania (akt o údajoch), ktorého cieľom je zvýšiť interoperabilitu služieb spracúvania údajov a odstrániť prekážky pri zmene poskytovateľa služieb spracúvania údajov.

9. UZNÁVA prepojenie bezpečnosti dodávateľského reťazca IKT s verejným obstarávaním. ZDÔRAZŇUJE, že je potrebné, aby sa v postupoch verejného obstarávania primerane zohľadňoval význam bezpečnosti dodávateľského reťazca IKT tým, že sa v nich v prípade potreby stanovia objektívne a na posúdení rizika založené výberové kritériá týkajúce sa schopnosti uchádzačov zaistiť vysokú úroveň bezpečnosti poskytovaných služieb. VYZÝVA na nájdenie správnej rovnováhy medzi verejným záujmom na čo najefektívnejšom a najspravodlivejšom využívaní verejných finančných prostriedkov na jednej strane a verejným záujmom na zaistení bezpečnosti informačných systémov a zabezpečení hladkého fungovania jednotného trhu na strane druhej. S cieľom uľahčiť vykonávanie príslušných pravidiel verejného obstarávania pri zvyšovaní kybernetickej bezpečnosti VYZÝVA Komisiu, aby do tretieho štvrťroka 2023 vypracovala metodické usmernenia s cieľom povzbudiť verejných obstarávateľov, aby sa primerane zamerali na postupy uchádzačov a ich subdodávateľov v oblasti kybernetickej bezpečnosti a aby posúdili a v prípade potreby predložili návrhy na revíziu alebo doplnenie príslušných právnych predpisov v oblasti verejného obstarávania.

10. UZNÁVA, že priame zahraničné investície súvisiace s produktmi a službami IKT síce poskytujú hospodárske a sociálne výhody členským štátom, podnikom a občanom, ale by mohli zahŕňať riziká pre bezpečnosť a verejný poriadok, a KONŠTATUJE, že mechanizmus EÚ na preverovanie priamych zahraničných investícií spolu s príslušnými vnútroštátnymi systémami preverovania, ktoré poskytujú prostriedky na riešenie takýchto rizík, by sa tiež mohli používať ako užitočný nástroj na zaistenie bezpečnosti a odolnosti dodávateľského reťazca IKT tým, že prispejú k odstráneniu vysokorizikových investícií, ktoré môžu mať na bezpečnosť a odolnosť vplyv. UZNÁVA, že informácie vymieňané a zdieľané prostredníctvom tohto mechanizmu môžu pomôcť členským štátom lepšie posúdiť prípadné hrozby pre bezpečnosť dodávateľských reťazcov IKT a zodpovedajúcim spôsobom podniknúť potrebné kroky. VYZÝVA príslušných vnútroštátnych aktérov, aby v prípade potreby zohľadnili aj tento rozmer mechanizmu preverovania.

11. Pokiaľ ide o obranu, OPÄTOVNE POTVRDZUJE svoju výzvu adresovanú Komisii, aby v roku 2023 spolu s členskými štátmi posúdila riziká pre dodávateľské reťazce kritickej infraštruktúry v rôznych oblastiach vrátane digitálnej oblasti, ktoré súvisia s bezpečnostnými a obrannými záujmami EÚ, a aby preskúmala možnosti zvýšenia kybernetickej bezpečnosti v celom dodávateľskom reťazci obrannej technologickej a priemyselnej základne EÚ. Okrem toho VYZÝVA členské štáty a Komisiu, aby pri plnení záväzkov a opatrení Strategického kompasu zohľadňovali aspekt bezpečnosti dodávateľského reťazca IKT.

12. Uznávajúc význam kritických surovín, ako aj všetkých druhov polovodičov ako základných stavebných prvkov pre produkty IKT, NABÁDA na konštruktívne rokovania o návrhu nariadenia, ktorým sa zriaďuje rámec opatrení na posilnenie ekosystému polovodičov v Európe (akt o čipoch), a o návrhu nariadenia Rady, ktorým sa mení nariadenie (EÚ) 2021/2085, ktorým sa zriaďujú spoločné podniky v rámci programu Horizont Európa, pokiaľ ide o spoločný podnik pre čipy.

NÁSTROJE ŠPECIFICKÉ PRE KYBERNETICKÚ BEZPEČNOSŤ

13. Osobitne pokiaľ ide o telekomunikačnú infraštruktúru, UZNÁVA úspechy dosiahnuté na úrovni Únie pri zlepšovaní bezpečnosti dodávateľského reťazca sietí 5G, najmä prostredníctvom súboru nástrojov EÚ pre bezpečnosť 5G (súbor nástrojov EÚ pre 5G). VYZÝVA členské štáty, aby si ďalej vymieňali informácie o najlepších postupoch a metodikách, pokiaľ ide o vykonávanie opatrení odporúčaných v súbore nástrojov EÚ pre 5G, a najmä aby uplatňovali príslušné obmedzenia vysokorizikových dodávateľov kľúčových aktív, ktoré sú v koordinovaných posúdeniach rizík EÚ vymedzené ako kritické a citlivé. ZDÔRAZŇUJE, že súbor nástrojov EÚ pre 5G predstavuje agilný nástroj založený na posudzovaní rizika na riešenie identifikovaných bezpečnostných výziev, ktorý umožňuje včasné a efektívne riešenie aspektov kybernetickej bezpečnosti 5G pri súčasnom rešpektovaní právomocí členských štátov, a POZNAMENÁVA, že je cenným nástrojom na ďalšie koordinované posilnenie bezpečnosti dodávateľského reťazca telekomunikačných sietí v podmienkach úplnej transparentnosti, ktorý by mohol slúžiť ako inšpirácia pre nástroje posudzovania a zmierňovania rizík súvisiace s inými dôležitými odvetviami. PRIPOMÍNA výzvu adresovanú príslušným orgánom, aby na základe posúdení rizík vypracúvali odporúčania pre členské štáty a Komisiu s cieľom posilniť odolnosť komunikačných sietí a infraštruktúr v Európskej únii vrátane pokračujúceho vykonávania súboru nástrojov EÚ pre 5G.

14. POUKAZUJE na význam interoperabilných prístupov, ktoré môžu riešiť odkázanosť na určitého dodávateľa a znížiť riziko koncentrácie a zároveň zvýšiť bezpečnosť dodávateľského reťazca v celom spektre infraštruktúry a služieb IKT. Najmä vo vzťahu k sieťam 5G UZNÁVA potenciálne prínosy koncepcie Open RAN v tejto súvislosti, pričom zároveň PRIPOMÍNA správu o kybernetickej bezpečnosti Open RAN, ktorú uverejnila skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, pričom poznamenáva, že táto koncepcia sa stále vyvíja a jej bezpečnosť, transparentnosť a normalizácia sú v počiatočnej fáze zrelosti, a ZDÔRAZŇUJE, že pred akýmkoľvek prechodom na nové normy alebo architektúry je dôležité vykonávať posudzovanie rizík.

15. ZDÔRAZŇUJE význam existujúcich a budúcich horizontálnych legislatívnych nástrojov v oblasti kybernetickej bezpečnosti pre zvýšenie bezpečnosti dodávateľského reťazca IKT, najmä nariadenia o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (akt o kybernetickej bezpečnosti), pripravovanej smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2), návrhu nariadenia, ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie, ako aj návrhu nariadenia o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami (akt o kybernetickej odolnosti). Okrem toho BERIE NA VEDOMIE významný vývoj odvetvových predpisov v oblasti kybernetickej bezpečnosti, najmä budúceho nariadenia o digitálnej prevádzkovej odolnosti finančného sektora (DORA), ktoré zahŕňa rámec dohľadu nad externými poskytovateľmi IKT služieb, ktoré sú kritické pre finančné subjekty. Týmito nariadeniami sa zavádzajú všeobecné povinnosti týkajúce sa bezpečnosti dodávateľského reťazca, ako aj podrobné a osobitné požiadavky relevantné pre dotknuté odvetvie. Zároveň ZDÔRAZŇUJE, že dodávatelia často dodávajú svoje produkty a služby do rôznych odvetví, a nie len do jedného odvetvia. Preto je veľmi dôležité zabezpečiť, aby boli požiadavky na bezpečnosť dodávateľského reťazca v čo najväčšej miere zosúladené vo všetkých príslušných odvetviach, najmä v tých, na ktoré sa bude vzťahovať budúca smernica NIS 2, s cieľom zabrániť nezrovnalostiam medzi povinnosťami uloženými dodávateľom, ako aj znížiť zaťaženie prevádzkovateľov kritických odvetví pri posudzovaní dodržiavania týchto povinností zo strany dodávateľov, pričom sa zohľadnia osobitosti jednotlivých odvetví.

16. VÍTA návrh aktu o kybernetickej odolnosti ako dôležitý legislatívny nástroj na dosiahnutie pokroku v bezpečnom vývoji produktov s digitálnymi prvkami a na zabezpečenie zohľadnenia kybernetickej bezpečnosti v celom životnom cykle produktov s digitálnymi prvkami. KONŠTATUJE, že návrh aktu o kybernetickej odolnosti má potenciál významne prispieť k posilneniu bezpečnosti dodávateľského reťazca IKT. PODPORUJE konštruktívne rokovania a včasné prijatie tohto aktu.

17. V tomto kontexte BERIE NA VEDOMIE prebiehajúcu prácu pod vedením agentúry ENISA spolu s členskými štátmi a inými stranami s cieľom poskytnúť EÚ systémy certifikácie produktov, služieb a procesov IKT, ktoré budú v súlade s aktom o kybernetickej bezpečnosti a ktoré by mali prispieť k zvýšeniu celkovej úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. NABÁDA všetky zainteresované strany, aby sa zapojili do prípravných prác na jednotlivých európskych systémoch certifikácie s cieľom vybudovať dôveru v bezpečné produkty, procesy a služby IKT a zvýšiť ich odolnosť, a VYZÝVA Komisiu, aby po dokončení prípravných prác urýchlene pripravila vykonávacie akty týkajúce sa európskych systémov certifikácie, najmä európskeho systému certifikácie kybernetickej bezpečnosti (EUCC) založeného na spoločných kritériách. KONŠTATUJE, že európske systémy certifikácie by mali v prípade potreby zahŕňať požiadavky na bezpečnosť dodávateľského reťazca vrátane vzťahov s dodávateľmi.

18. ZDÔRAZŇUJE potrebu dôkladného vykonávania všetkých pripravovaných ustanovení NIS 2 týkajúcich sa bezpečnosti dodávateľského reťazca IKT. V tejto súvislosti ZDÔRAZŇUJE význam koordinovaných posúdení rizík EÚ týkajúcich sa kritických dodávateľských reťazcov (koordinované posúdenia rizika pre dodávateľský reťazec), vnútroštátnych politík v oblasti bezpečnosti dodávateľského reťazca a bezpečnostných opatrení súvisiacich s dodávateľským reťazcom. KONŠTATUJE, že pokiaľ ide o riziká pre bezpečnosť primárneho dodávateľa alebo koncového zákazníka, pozornosť by sa mala venovať nielen primárnym dodávateľom, ale aj príslušným subdodávateľom. S cieľom uľahčiť vykonávanie opatrení manažmentu rizík pre dodávateľský reťazec NABÁDA agentúru ENISA, aby s pomocou skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zhodnotila najlepšie postupy, ktoré sú k dispozícii na manažment rizík pre dodávateľský reťazec, a aby ich zoskupila do metodických usmernení. NABÁDA ju takisto, aby monitorovala investície do bezpečnosti dodávateľského reťazca IKT zo strany subjektov regulovaných podľa nadchádzajúcej smernice NIS 2.

19. ZDÔRAZŇUJE tiež prínosy a riziká, ktoré v kontexte bezpečnosti dodávateľského reťazca vyplývajú z využívania poskytovateľov riadených služieb (MSP) a poskytovateľov riadených bezpečnostných služieb (MSSP). Hoci využívanie týchto poskytovateľov môže výrazne zlepšiť bezpečnosť v rámci organizácií a viesť k vyššej úrovni kybernetickej bezpečnosti, diaľkové riadenie systémov a služieb IKT v kombinácii s privilegovaným prístupom k IKT prostrediu zákazníkov, ktorý by MSP a MSSP mohli potrebovať, môže v prípade kompromitovaných MSP alebo MSSP viesť k značným kaskádovým účinkom na veľký počet zákazníkov. Je preto mimoriadne dôležité, aby si MSP a MSSP zachovali vysokú úroveň vlastnej vnútornej bezpečnosti a bezpečnosti služieb, ktoré poskytujú, a aby k svojim zákazníkom vo vzťahu k týmto službám zaujali transparentný prístup. V tejto súvislosti VÍTA ich budúce začlenenie do rozsahu pôsobnosti pripravovanej smernice NIS 2.

20. Pokiaľ ide o vykonávanie mechanizmu koordinovaného posudzovania rizík dodávateľského reťazca podľa pripravovanej smernice NIS 2, v tejto súvislosti BERIE NA VEDOMIE význam netechnických rizikových faktorov, ako je neprimeraný vplyv tretích štátov na dodávateľov a poskytovateľov služieb, a v tomto kontexte UZNÁVA faktory, ktoré možno použiť na posúdenie rizikového profilu, ako sa uvádza v koordinovanom posúdení rizika kybernetickej bezpečnosti sietí 5G na úrovni EÚ. VYZÝVA Komisiu, aby do druhého štvrťroka 2023 po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a agentúrou ENISA určila konkrétne služby, systémy alebo produkty IKT, ktoré by mohli byť prioritne predmetom koordinovaného posúdenia rizík pre dodávateľský reťazec.

21. KONŠTATUJE, že závislosť od vysokorizikových dodávateľov produktov a služieb IKT používaných na prevádzku kritických sietí a systémov predstavuje strategickú hrozbu, ktorú je potrebné zmierniť prostredníctvom vhodných politík na vnútroštátnej úrovni aj na úrovni EÚ, ako aj prostredníctvom spolupráce medzi členskými štátmi a s podobne zmýšľajúcimi medzinárodnými partnermi. S cieľom uľahčiť zmiernenie tohto strategického rizika a podporiť koordinované posúdenia rizík pre dodávateľský reťazec VYZÝVA skupinu pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, aby v spolupráci s Komisiou a agentúrou ENISA vypracovala súbor opatrení na zníženie rizík pre dodávateľský reťazec kritických IKT (súbor nástrojov pre dodávateľský reťazec IKT). Súbor nástrojov pre dodávateľský reťazec IKT by mal vychádzať zo scenárov strategických hrozieb určených pre dodávateľské reťazce IKT a mal by poskytovať opatrenia na reakciu na tieto scenáre využitím skúseností zo súboru nástrojov pre 5G a zo skúseností získaných na vnútroštátnej úrovni. Mal by transparentným spôsobom dopĺňať koordinované posúdenia rizika pre dodávateľský reťazec v prípade konkrétnych služieb, systémov alebo produktov IKT podľa pripravovanej smernice NIS 2 tým, že ponúkne všeobecné opatrenia na zníženie rizík, ktoré možno upraviť pre konkrétne služby, systémy alebo produkty IKT škálovateľným spôsobom na základe rizík identifikovaných v jednotlivých koordinovaných posúdeniach rizík pre dodávateľský reťazec.

22. ZDÔRAZŇUJE dôležitú úlohu výskumu, inovácií, investícií a podnikateľských činností v digitálnej oblasti a v oblasti kybernetickej bezpečnosti, ako aj financovania takýchto činností, pokiaľ ide o predchádzanie možným budúcim neželaným formám strategickej závislosti a posilnenie celkovej odolnosti dodávateľských reťazcov IKT. V tejto súvislosti ZDÔRAZŇUJE úlohu a význam strategických aj implementačných úloh Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier (ECCC) pre prispievanie k maximalizácii účinkov investícií na posilnenie vedúceho postavenia a otvorenej strategickej autonómie Únie v oblasti kybernetickej bezpečnosti a podporných technologických kapacít a zručností Únie a na zvýšenie globálnej konkurencieschopnosti Únie. V tejto súvislosti VYZÝVA na rýchle sfunkčnenie ECCC. VYZÝVA ECCC, aby vo svojom strategickom programe zohľadnilo aspekty bezpečnosti dodávateľského reťazca IKT vrátane napríklad bezpečného vývoja softvéru a zároveň zabezpečilo konzistentnosť a komplementárnosť a zabránilo zdvojovaniu úsilia. PODPORUJE posilnenie európskej konkurencieschopnosti v oblasti kybernetickej bezpečnosti prostredníctvom programov financovania, ako je program Horizont Európa pre výskum a inovácie, ako aj program Digitálna Európa na posilnenie, budovanie a získavanie základných kapacít pre digitálne hospodárstvo, spoločnosť a demokraciu EÚ.

PODPORNÉ MECHANIZMY

23. NABÁDA na posilnenie stimulov finančnej podpory súvisiacich s opatreniami zameranými na posilnenie bezpečnosti dodávateľského reťazca IKT. VYZÝVA ECCC, Komisiu a príslušné zainteresované strany, aby prioritne preskúmali možnosti začlenenia aspektov bezpečnosti dodávateľského reťazca IKT do nadchádzajúcich výziev v rámci pracovných programov programu Digitálna Európa a programu Horizont Európa v oblasti kybernetickej bezpečnosti alebo do akýchkoľvek iných relevantných možností financovania, a to aj so zreteľom na nadchádzajúce vykonávanie smernice NIS 2. Tieto možnosti financovania by mali byť okrem iného zamerané na to, aby sa organizáciám umožnilo podporovať zachovanie vysokej úrovne kybernetickej bezpečnosti, pokiaľ ide o obstarávanie produktov a služieb IKT v celom dodávateľskom reťazci, najmä pokiaľ ide o nahradenie konkrétnych kritických služieb, systémov alebo produktov IKT uznaných za vysokorizikové v súlade s budúcimi koordinovanými posúdeniami rizík pre dodávateľský reťazec.

24. UZNÁVA, že globalizácia a špecializácia služieb IKT a zvýšená závislosť od produktov a služieb tretích strán prinášajú potrebu úzkej spolupráce v EÚ a na medzinárodnej úrovni pri výmene poznatkov a odborných znalostí medzi príslušnými zainteresovanými stranami, a NABÁDA ich, aby dosiahli silnú a koordinovanú pozíciu, ktorá zabezpečí bezpečnosť dodávateľského reťazca IKT komplexným spôsobom. UZNÁVA tiež potrebu ďalej skúmať relevantné najmodernejšie prístupy a techniky, pokiaľ ide o vhodnú základnú kybernetickú hygienu a dlhodobé riešenia na dosiahnutie bezpečných a odolných dodávateľských reťazcov IKT, ako aj najvhodnejšie spôsoby ich podpory a potenciálneho začlenenia do politík alebo iných iniciatív. V tejto súvislosti UZNÁVA, že osobitná pozornosť by sa mala venovať preskúmaniu prínosov a nevýhod systematických riešení, ako sú zásady nulovej dôvery, softvérový zoznam materiálov a podobné dlhodobé riešenia. ODPORÚČA, aby sa na tento účel využila skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

25. Berie NA VEDOMIE prínosy monitorovania a účinného zdieľania informácií o kybernetických incidentoch a hrozbách pre prevenciu, odhaľovanie a zmierňovanie účinkov útokov na dodávateľský reťazec. ZDÔRAZŇUJE, že je potrebné pokračovať v budovaní dôvery medzi členskými štátmi, pokiaľ ide o účinné zdieľanie takýchto informácií. V tejto súvislosti PRIPOMÍNA návrh Komisie na podporu členských štátov pri zriaďovaní a posilňovaní centier bezpečnostných operácií s cieľom vybudovať ich sieť v celej EÚ a ďalej monitorovať a predvídať signály možnosti útokov na siete. PRIPOMÍNA potrebu komplementárnosti a koordinácie v rámci existujúcich sietí a mechanizmov a v tejto súvislosti ZDÔRAZŇUJE najmä úlohu siete jednotiek CSIRT a potrebu ďalšieho preskúmania potenciálu týchto sietí na podporu efektívnej, bezpečnej a spoľahlivej kultúry zdieľania informácií. PRIPOMÍNA úsilie členských štátov zriadiť s podporou EÚ sektorové, celoštátne a regionálne jednotky CSIRT a národné alebo európske strediská pre výmenu a analýzu informácií ako súčasť efektívnej siete partnerstiev v oblasti kybernetickej bezpečnosti v Únii.

26. Vzhľadom na prepojenú a globálnu povahu hrozieb pre dodávateľský reťazec IKT ZDÔRAZŇUJE, že je dôležité venovať sa bezpečnosti dodávateľského reťazca IKT a zvyšovať ju na celosvetovej úrovni. Vzhľadom na to ODPORÚČA využívanie digitálnych partnerstiev, kybernetických dialógov a iných relevantných iniciatív EÚ vrátane prípadných dohôd o voľnom obchode na podporu hodnotení dodávateľov produktov IKT a poskytovateľov služieb IKT založených na posúdení rizika, využívanie dôveryhodných dodávateľov a využívanie bezpečného a inovatívneho digitálneho ekosystému založeného na otvorených, interoperabilných a transparentných normách. Okrem toho OPÄTOVNE ZDÔRAZŇUJE víziu partnerstiev Global Gateway, ako aj Rady EÚ – USA pre obchod a technológie a činnosti v rámci jej pracovných skupín s cieľom podporovať využívanie dôveryhodných/nízkorizikových dodávateľov a vytvoriť mechanizmus financovania na podporu projektov bezpečnejšej, odolnejšej a dôveryhodnejšej infraštruktúry a služieb IKT v tretích štátoch, a to aj tým, že sa zdržia financovania nákupov od nedôveryhodných/vysokorizikových dodávateľov technologicky neutrálnym spôsobom.

27. Opätovne POTVRDZUJE svoj záväzok prispievať k otvorenému, slobodnému, globálnemu, stabilnému a bezpečnému kybernetickému priestoru a podporovať ho a dodržiavať normy, pravidlá a zásady zodpovedného správania štátov v kybernetickom priestore stanovené v rámci OSN. Najmä v súvislosti s bezpečnosťou dodávateľského reťazca IKT PRIPOMÍNA normu schválenú skupinou vládnych expertov OSN a otvorenou pracovnou skupinou OEWG, v ktorej sa štáty nabádajú, aby podnikli primerané kroky na zabezpečenie integrity dodávateľského reťazca, a to aj prostredníctvom vypracovania objektívnych opatrení spolupráce, aby koncoví používatelia mohli dôverovať bezpečnosti produktov IKT, a snažili sa zabrániť šíreniu škodlivých nástrojov a techník IKT a využívaniu škodlivých skrytých funkcií, a ZASADZUJE SA za jej rozsiahle vykonávanie.