Rada
Evropské unie

Brusel 17. října 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

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	17. října 2022
Příjemce:	Delegace
Č. předchozího dokumentu:	12930/22
Předmět:	Závěry Rady o bezpečnosti dodavatelského řetězce IKT – závěry Rady, které Rada schválila na zasedání konaném dne 17. října 2022

Delegace naleznou v příloze závěry Rady o bezpečnostní dodavatelského řetězce IKT ve znění schváleném Radou na jejím zasedání konaném dne 17. října 2022.

PŘÍLOHA

Závěry Rady o bezpečnosti dodavatelského řetězce IKT

RADA EVROPSKÉ UNIE,

PŘIPOMÍNAJÍC své závěry o:

– společném sdělení Evropskému parlamentu a Radě ze dne 20. listopadu 2017: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU,

– budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU,

– významu 5G pro evropské hospodářství a potřebě zmírnit bezpečnostní rizika spojená s 5G,

– utváření digitální budoucnosti Evropy,

– oživení urychlujícím přechod k dynamičtějšímu, odolnějšímu a konkurenceschopnějšímu evropskému průmyslu,

– kybernetické bezpečnosti zařízení připojených k internetu,

– strategii kybernetické bezpečnosti EU pro digitální dekádu,

– rozvoji kybernetické pozice Evropské unie,

– zvláštní zprávě Evropského účetního dvora č. 03/2022 nazvané „Spouštění sítí 5G v EU: při zavádění sítí dochází ke zpoždění a bezpečnostní problémy zůstávají nevyřešeny“,

PŘIPOMÍNAJÍC závěry Evropské rady o:

– COVID-19, jednotném trhu, průmyslové politice, digitálních aspektech a vnějších vztazích přijaté na zasedání ve dnech 1. a 2. října 2020,

– vojenské agresi Ruska vůči Ukrajině, o bezpečnosti a obraně, energetice, hospodářských otázkách, pandemii COVID-19 a vnějších vztazích přijaté na zasedání ve dnech 24. a 25. března 2022,

– Ukrajině, potravinovém zabezpečení, bezpečnosti a obraně, jakož i energetice přijaté na zasedání ve dnech 30. a 31. května 2022,

1. vzhledem k rostoucímu významu geopolitiky pro kybernetickou bezpečnost ZDŮRAZŇUJE, že Evropská unie a její členské státy musí ke kybernetické bezpečnosti přistupovat komplexním a strategickým způsobem. Ruská vojenská agrese vůči Ukrajině značně změnila strategické a bezpečnostní prostředí Evropské unie a ukázala potřebu silnější a schopnější Evropské unie v oblasti bezpečnosti a obrany. Tato agrese výrazně upozornila na to, že je nanejvýš důležité náležitě zohlednit geopolitické prostředí nejen při reakci na nepřátelské činnosti v kyberprostoru, ale také při budování a udržování odolnosti informačních a komunikačních technologií (IKT). To má zvláštní význam pro dodavatelské řetězce produktů a služeb IKT (dodavatelské řetězce IKT), které by mohly být ohroženy na základě geopolitického soupeření, jak dokládá útok SolarWinds, a zasaženy geopolitickým napětím a nestabilitou, jak ukazuje hrozba související se závislostí na ruských prodejcích IKT v době vojenské agrese Ruska vůči Ukrajině;

2. BERE NA VĚDOMÍ, že povaha rizik spojených s dodavatelským řetězcem IKT, který se skládá z propojeného souboru zdrojů a procesů mezi hospodářskými subjekty (jak jsou definovány v nařízení (EU) 2019/1020) a který začíná získáváním surovin a zahrnuje výrobu a zpracování produktů a služeb IKT, manipulaci s nimi a jejich dodávání, včetně poskytování podpory během životního cyklu produktů a služeb IKT, přináší jedinečné výzvy a potenciálně dalekosáhlé důsledky. Kromě rizik spojených s nedostupností produktů IKT, například kvůli nedostatku kritických surovin a polovodičů potřebných pro jejich výrobu, jsou dodavatelské řetězce produktů a služeb IKT vystaveny dalším hrozbám. Zejména mohou být terčem nepřátelských subjektů nebo mohou být těmito subjekty zneužívány, a to sofistikovanými a často skrytými způsoby, které mají dopad na důvěrnost, integritu a dostupnost předávaných a uchovávaných citlivých dat;

3. uznávajíc, že při zajišťování aktiv v oblasti IKT je nutný přístup zohledňující všechna rizika, POTVRZUJE význam návrhu směrnice o odolnosti kritických subjektů pro zlepšení fyzické bezpečnosti kritických subjektů a ZDŮRAZŇUJE, že kromě posílení odolnosti vůči útokům na dodavatelské řetězce prováděným kybernetickými prostředky je stejně důležité posílit celkovou odolnost a bezpečnost dodavatelských řetězců IKT vůči celé řadě hrozeb, jako jsou přírodní události, selhání systémů, vnitřní hrozby nebo lidské chyby. V tomto smyslu UZNÁVÁ, že bezpečnost dodavatelského řetězce IKT zahrnuje zajištění ochrany produktů a služeb IKT vyráběných, dodávaných, pořizovaných a používaných v dodavatelských řetězcích IKT, a to i prostřednictvím ochrany jednotlivých složek a předávaných dat;

4. na základě ponaučení vyplývajícího z důsledků strategických závislostí Evropské unie na ruských fosilních palivech, jakož i z dopadů narušení dodavatelských řetězců během pandemie COVID-19, zejména pokud jde o léčivé přípravky a polovodiče, u nichž byly strategické závislosti EU vystaveny zátěži, VYBÍZÍ členské státy, aby usilovaly o zamezení podobným situacím nežádoucí strategické vnější závislosti v souvislosti s produkty a službami IKT. Vzhledem k rostoucí digitalizaci společnosti a stále častějšímu využívání IKT v rámci kritické infrastruktury by měly být strategické vnější závislosti související s produkty a službami IKT a jejich dodavatelskými řetězci průběžně posuzovány a případně řešeny;

5. PŘIPOMÍNÁ, že dosažení strategické autonomie při současném zachování otevřené ekonomiky je klíčovým cílem Unie, který zahrnuje nalezení a omezení strategických závislostí a zvýšení odolnosti v nejcitlivějších průmyslových ekosystémech a konkrétních oblastech, včetně digitální oblasti. To zahrnuje rozvoj a zavádění strategických digitálních kapacit a infrastruktury, jakož i posílení schopnosti činit autonomní technologická rozhodnutí, a, jakožto jeden z hlavních pilířů, zajištění odolných a bezpečných infrastruktur, produktů a služeb pro budování důvěry v jednotný digitální trh a v rámci evropské společnosti při současném zachování otevřenosti, globální spolupráce s podobně smýšlejícími partnery a konkurenceschopnosti a využití jejich potenciálních přínosů. Základní hodnoty Evropské unie chrání především soukromí, bezpečnost, rovnost, lidskou důstojnost, právní stát a otevřený internet, což jsou nezbytné předpoklady pro vybudování společnosti, hospodářství a průmyslu, jež se budou opírat o digitální rozvoj a jež budou zaměřeny na člověka;

6. KONSTATUJE, že v důsledku vývoje v oblasti kybernetických hrozeb, který se v posledních letech projevuje trendem vysoce účinných a sofistikovaných útoků na dodavatelské řetězce, jako jsou útoky SolarWinds, Mimecast nebo Kaseya, jež se objevují společně s externím zajišťováním základních služeb IKT a zintenzivňují se celkovou závislostí na produktech a službách IKT vyráběných, poskytovaných nebo obsluhovaných třetími stranami, je velmi pravděpodobné, že k útokům na dodavatelské řetězce se značnými škodami pro hospodářství a společnost bude docházet i v budoucnosti. V této souvislosti ZDŮRAZŇUJE význam posílení bezpečnosti a odolnosti dodavatelských řetězců IKT pro fungování jednotného trhu spolu s potřebou zajistit na tomto trhu dostupnost, bezpečnost a rozmanitost produktů a služeb IKT. Proto UZNÁVÁ potřebu maximalizovat a zefektivnit využívání stávajících nástrojů a přístupů EU k dosažení těchto cílů, jakož i potřebu neustále se přizpůsobovat změnám v oblasti kybernetických hrozeb zavedením dalších vhodných opatření a mechanismů, a to i ve vztahu k možným bezpečnostním rizikům vznikajících a přelomových technologií. VYBÍZÍ členské státy, aby v tomto ohledu uplatňovaly přístup založený na posouzení rizik s cílem řešit otázky spojené s technologickým vývojem;

7. UZNÁVÁ, že pro účinné zmírňování rizik spojených s dodavatelskými řetězci IKT je zásadně důležité chápat neustále se vyvíjející problematiku kybernetických hrozeb, jakož i složitost útoků na dodavatelské řetězce. V tomto ohledu ZDŮRAZŇUJE, že je nezbytné přizpůsobovat se novým hrozbám aktivním a nepřetržitým monitorováním, analýzou a posuzováním situace ohledně hrozeb v dodavatelském řetězci, zvyšovat povědomí a získávat znalosti o hrozbách a zranitelných místech a odpovídajícím způsobem aktivně upozorňovat příslušné subjekty. VÍTÁ práci Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) ohledně bezpečnosti dodavatelského řetězce IKT, zejména její zprávu o typech ohrožení v souvislosti s útoky na dodavatelské řetězce;

MEZIODVĚTVOVÉ NÁSTROJE A PŘÍSTUPY

8. ZNOVU POTVRZUJE, že je důležité, aby členské státy zvážily potřebu diverzifikovat dodavatele kritických IKT, aby se tak zabránilo vytváření významných závislostí na jednotlivých dodavatelích, nebo aby se vytváření těchto závislostí omezilo, a to zejména závislostí na vysoce rizikových dodavatelích, neboť se tím zvyšuje vystavení důsledkům možných narušení. UZNÁVÁ, že zamezení závislosti na prodejci a diverzifikace dodavatelů IKT jsou jednou z důležitých složek pro zajištění stability a bezpečnosti vnitřního trhu. ZDŮRAZŇUJE, že je třeba podporovat a provádět odpovídající strategie usnadňující diverzifikaci prodejců a konkurenceschopnost technologicky neutrálním způsobem. Dále VYBÍZÍ k začlenění aspektů souvisejících s předcházením závislosti na prodejci do právních předpisů EU. V tomto ohledu OCEŇUJE návrh nařízení o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (akt o datech), jehož cílem je zvýšit interoperabilitu služeb zpracování dat a odstranit překážky bránící změně poskytovatele služeb zpracování dat;

9. UZNÁVÁ souvislost mezi bezpečností dodavatelského řetězce IKT a zadáváním veřejných zakázek. ZDŮRAZŇUJE, že je třeba, aby byl v postupech zadávání veřejných zakázek náležitě zohledněn význam bezpečnosti dodavatelského řetězce IKT tím, že jsou ve vhodných případech stanovena objektivní výběrová kritéria založená na posouzení rizik týkající se schopnosti uchazečů zajistit vysokou úroveň bezpečnosti poskytovaných služeb. VYZÝVÁ k nalezení správné rovnováhy mezi veřejným zájmem co nejúčinněji a spravedlivě využívat veřejné prostředky na jedné straně a veřejným zájmem zabezpečit informační systémy a zajistit hladké fungování jednotného trhu na straně druhé. S cílem usnadnit provádění příslušných pravidel pro zadávání veřejných zakázek s ohledem na zvýšení kybernetické bezpečnosti VYZÝVÁ Komisi, aby do třetího čtvrtletí roku 2023 vypracovala metodické pokyny pro motivaci veřejných zadavatelů k tomu, aby se u uchazečů a jejich subdodavatelů náležitě zaměřili na postupy v oblasti kybernetické bezpečnosti a aby posoudili a v případě potřeby předložili návrhy na revizi nebo doplnění příslušných právních předpisů v oblasti zadávání veřejných zakázek;

10. UZNÁVÁ, že přímé zahraniční investice související s produkty a službami IKT sice mají hospodářské a sociální přínosy pro členské státy, podniky a občany, mohly by však zahrnovat rizika pro bezpečnost a veřejný pořádek, a KONSTATUJE, že mechanismus EU pro prověřování přímých zahraničních investic spolu s příslušnými vnitrostátními prověřovacími systémy, které poskytují prostředky k řešení těchto rizik, by mohly být rovněž použity jako užitečný nástroj pro zajištění bezpečnosti a odolnosti dodavatelského řetězce IKT tím, že přispějí k odstranění vysoce rizikových investic, které mohou tuto bezpečnost a odolnost ovlivnit. UZNÁVÁ, že informace vyměňované a sdílené prostřednictvím tohoto mechanismu mohou členským státům pomoci lépe posoudit možné hrozby pro bezpečnost dodavatelských řetězců IKT a odpovídajícím způsobem přijmout nezbytná opatření. VYZÝVÁ příslušné vnitrostátní aktéry, aby tento rozměr prověřovacího mechanismu ve vhodných případech zohledňovali;

11. pokud jde o obranu, ZNOVU POTVRZUJE svou výzvu, aby Komise v roce 2023 společně s členskými státy posoudila rizika pro dodavatelské řetězce kritické infrastruktury v různých oblastech, včetně digitální oblasti, související s bezpečnostními a obrannými zájmy EU a aby prozkoumala možnosti, jak zvýšit kybernetickou bezpečnost v celém dodavatelském řetězci technologické a průmyslové základny obrany EU. Dále VYZÝVÁ členské státy a Komisi, aby se zabývaly bezpečností dodavatelského řetězce IKT při provádění závazků a opatření Strategického kompasu;

12. uznávajíc význam kritických surovin, jakož i všech druhů polovodičů jako základních stavebních kamenů produktů IKT, VYBÍZÍ ke konstruktivním jednáním o návrhu nařízení, kterým se zřizuje rámec opatření pro posílení evropského ekosystému polovodičů (akt o čipech), a o návrhu nařízení Rady, kterým se mění nařízení (EU) 2021/2085, kterým se zřizují společné podniky v rámci programu Horizont Evropa, pokud jde o společný podnik pro čipy;

NÁSTROJE SPECIFICKÉ PRO KYBERNETICKOU BEZPEČNOST

13. Pokud se jedná konkrétně o telekomunikační infrastrukturu, UZNÁVÁ úspěchy dosažené na úrovni Unie ohledně zlepšení bezpečnosti dodavatelského řetězce sítí 5G, zejména prostřednictvím souboru opatření EU pro bezpečnost sítí 5G (soubor opatření EU pro sítě 5G). VYZÝVÁ členské státy, aby si i nadále vyměňovaly informace o osvědčených postupech a metodikách týkajících se provádění opatření doporučených v souboru opatření EU pro sítě 5G, a zejména aby pro klíčová aktiva definovaná jako kritická a citlivá v rámci koordinovaného posuzování rizik v EU uplatňovaly příslušná omezení ohledně vysoce rizikových dodavatelů. ZDŮRAZŇUJE, že soubor opatření EU pro sítě 5G představuje pružný nástroj založený na posouzení rizik pro řešení zjištěných bezpečnostních výzev, který umožňuje včas a účinně řešit aspekty kybernetické bezpečnosti sítí 5G při současném respektování pravomocí členských států, a UZNÁVÁ, že se jedná o cenný nástroj pro další a plně transparentní posílení bezpečnosti dodavatelského řetězce telekomunikačních sítí koordinovaným způsobem, který by mohl sloužit jako inspirace pro nástroje pro posuzování a zmírňování rizik ve vztahu k jiným životně důležitým odvětvím. PŘIPOMÍNÁ výzvu příslušných orgánů, aby byla na základě posouzení rizik formulována doporučení určená členským státům a Komisi, za účelem posílení odolnosti komunikačních sítí a infrastruktur v rámci Evropské unie, včetně pokračujícího provádění souboru opatření EU pro sítě 5G;

14. BERE NA VĚDOMÍ význam interoperabilních přístupů, které mohou řešit problém závislosti na prodejci, snížit riziko koncentrace a zlepšit bezpečnost dodavatelského řetězce v celém spektru infrastruktury a služeb IKT. Zejména pokud jde o sítě 5G, UZNÁVÁ v tomto ohledu potenciální přínosy koncepce Open RAN a zároveň PŘIPOMÍNÁ zprávu o kybernetické bezpečnosti Open RAN zveřejněnou skupinou pro spolupráci v oblasti bezpečnosti sítí a informací a konstatuje, že tato koncepce se stále vyvíjí a její bezpečnost, transparentnost a standardizace je v rané fázi vyspělosti, a ZDŮRAZŇUJE, že před jakýmkoliv přechodem na nové normy nebo architektury je důležité provést posouzení rizik;

15. ZDŮRAZŇUJE, že pro zvýšení bezpečnosti dodavatelského řetězce IKT jsou důležité stávající i připravované horizontální legislativní nástroje v oblasti kybernetické bezpečnosti, zejména nařízení o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti), připravovaná směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS 2), návrh nařízení, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie, jakož i návrh nařízení o horizontálních požadavcích na kybernetickou bezpečnost u produktů s digitálními prvky (akt o kybernetické odolnosti). Dále BERE NA VĚDOMÍ významný vývoj odvětvových předpisů v oblasti kybernetické bezpečnosti, zejména budoucího nařízení o digitální provozní odolnosti finančních služeb (DORA), které zahrnuje rámec dohledu nad poskytovateli služeb IKT z řad třetích stran, kteří mají pro finanční subjekty zásadní význam. Tyto předpisy ukládají obecné povinnosti týkající se bezpečnosti dodavatelského řetězce, jakož i podrobné a zvláštní požadavky týkající se dotčeného odvětví. Zároveň ZDŮRAZŇUJE, že dodavatelé své produkty a služby často dodávají do různých odvětví, nikoli jen do jednoho. Je proto velmi důležité zajistit, aby byly požadavky na bezpečnost dodavatelského řetězce v maximální možné míře sladěny ve všech příslušných odvětvích, zejména pak v odvětvích, na něž se vztahuje budoucí směrnice NIS 2, aby se tak zabránilo nesrovnalostem mezi povinnostmi uloženými dodavatelům a aby se snížila zátěž provozovatelů kritických odvětví při posuzování toho, zda dodavatelé tyto povinnosti dodržují, přičemž je třeba zohlednit specifika daného odvětví;

16. VÍTÁ návrh aktu o kybernetické odolnosti jakožto důležitého legislativního nástroje pro dosažení pokroku v bezpečném vývoji produktů s digitálními prvky a pro zajištění toho, aby kybernetická bezpečnost byla zohledněna během celého životního cyklu produktů s digitálními prvky. KONSTATUJE, že návrh aktu o kybernetické odolnosti může významně přispět k posílení bezpečnosti dodavatelského řetězce IKT. VYBÍZÍ ke konstruktivním jednáním a včasnému přijetí tohoto aktu;

17. v tomto ohledu OCEŇUJE probíhající práci pod vedením Agentury Evropské unie pro kybernetickou bezpečnost spolu s členskými státy a dalšími zúčastněnými stranami s cílem poskytnout Evropské unii systémy certifikace produktů, služeb a procesů IKT, které budou v souladu s aktem o kybernetické bezpečnosti a které by měly přispět ke zvýšení celkové úrovně kybernetické bezpečnosti v rámci jednotného digitálního trhu. VYBÍZÍ všechny zúčastněné strany, aby se zapojily do přípravných prací na jednotlivých evropských systémech certifikace s cílem vybudovat důvěru v bezpečné produkty, procesy a služby IKT a posílit jejich odolnost, a VYZÝVÁ Komisi, aby po dokončení přípravných prací urychleně připravila prováděcí akty týkající se evropských systémů certifikace, zejména evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích. BERE NA VĚDOMÍ, že evropské systémy certifikace by měly v případě potřeby zahrnovat požadavky na bezpečnost dodavatelského řetězce, včetně vztahů s dodavateli;

18. ZDŮRAZŇUJE, že je třeba důkladně provést všechna připravovaná ustanovení NIS 2 týkající se bezpečnosti dodavatelského řetězce IKT. V tomto ohledu VYZDVIHUJE význam koordinovaných posuzování rizik kritických dodavatelských řetězců na úrovni EU (koordinovaná posuzování rizik dodavatelského řetězce), vnitrostátních politik v oblasti bezpečnosti dodavatelského řetězce a bezpečnostních opatření souvisejících s dodavatelským řetězcem. BERE NA VĚDOMÍ, že pozornost je třeba věnovat nejen hlavním dodavatelům, ale také příslušným subdodavatelům, pokud jde o rizika pro bezpečnost hlavního dodavatele nebo koncového zákazníka. S cílem usnadnit provádění opatření pro řízení rizik v dodavatelském řetězci VYBÍZÍ agenturu ENISA, aby za pomoci skupiny pro spolupráci v oblasti bezpečnosti sítí a informací provedla hodnocení osvědčených postupů, jež jsou pro řízení rizik v dodavatelském řetězci k dispozici, a aby je začlenila do metodických pokynů. Dále VYBÍZÍ agenturu ENISA, aby sledovala investice do bezpečnosti dodavatelského řetězce IKT u subjektů, na něž se vztahuje připravovaná směrnice NIS 2;

19. ZDŮRAZŇUJE rovněž přínosy a rizika, které v souvislosti s bezpečností dodavatelského řetězce vyplývají z využívání poskytovatelů řízených služeb a poskytovatelů řízených bezpečnostních služeb. I když využívání těchto poskytovatelů může výrazně zlepšit bezpečnost v rámci organizací a vést k vyšší úrovni kybernetické bezpečnosti, může řízení systémů a služeb IKT na dálku v kombinaci s privilegovaným přístupem k prostředí IKT zákazníků, jež mohou poskytovatelé řízených služeb a poskytovatelé řízených bezpečnostních služeb potřebovat, vést v případě napadení těchto poskytovatelů ke kaskádovému efektu s významným dopadem na velký počet zákazníků. Je proto nanejvýš důležité, aby poskytovatelé řízených služeb a poskytovatelé řízených bezpečnostních služeb udržovali vysokou úroveň své vnitřní bezpečnosti a bezpečnosti služeb, které poskytují, a aby vůči svým zákazníkům, pokud jde o bezpečnost poskytovaných služeb, zaujali transparentní přístup. V tomto ohledu VÍTÁ jejich budoucí začlenění do oblasti působnosti připravované směrnice NIS 2;

20. pokud jde o provádění mechanismu koordinovaného posuzování rizik dodavatelského řetězce podle připravované směrnice NIS 2, BERE v této souvislosti NA VĚDOMÍ význam netechnických rizikových faktorů, jako je nepatřičný vliv třetího státu na dodavatele a poskytovatele služeb, a v této souvislosti UZNÁVÁ faktory, které lze použít k posouzení rizikového profilu, jak je uvedeno v koordinovaném posouzení rizik kybernetické bezpečnosti sítí 5G ze strany EU. VYZÝVÁ Komisi, aby do druhého čtvrtletí roku 2023 po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací a agenturou ENISA určila konkrétní služby, systémy nebo produkty IKT, které by mohly být přednostně podrobeny koordinovanému posouzení rizik v dodavatelském řetězci;

21. BERE NA VĚDOMÍ, že závislost na vysoce rizikových dodavatelích produktů a služeb IKT používaných pro provoz kritických sítí a systémů představuje strategickou hrozbu, kterou je třeba zmírnit prostřednictvím vhodných politik na vnitrostátní úrovni i na úrovni EU a prostřednictvím spolupráce mezi členskými státy a s podobně smýšlejícími mezinárodními partnery. S cílem usnadnit zmírnění tohoto strategického rizika a podpořit koordinovaná posouzení rizik dodavatelského řetězce VYZÝVÁ skupinu pro spolupráci v oblasti bezpečnosti sítí a informací, aby ve spolupráci s Komisí a agenturou ENISA vypracovala soubor opatření ke snížení rizik v dodavatelském řetězci kritických IKT (soubor opatření pro dodavatelský řetězec IKT). Soubor opatření pro dodavatelský řetězec IKT by měl vycházet ze scénářů strategických hrozeb zjištěných pro dodavatelské řetězce IKT a poskytovat opatření pro reakci na tyto scénáře s využitím zkušeností ze souboru opatření pro sítě 5G a ze zkušeností získaných na vnitrostátní úrovni. Měl by transparentním způsobem doplňovat koordinovaná posouzení rizik dodavatelského řetězce pro konkrétní služby, systémy nebo produkty IKT podle připravované směrnice NIS 2 tím, že nabídne obecná opatření ke snížení rizik, jež lze upravit pro konkrétní služby, systémy nebo produkty IKT rozšiřitelným způsobem na základě rizik zjištěných v jednotlivých koordinovaných posouzeních rizik dodavatelského řetězce;

22. ZDŮRAZŇUJE důležitou úlohu výzkumu, inovací, investic a podnikatelských činností v digitální oblasti a oblasti kybernetické bezpečnosti, jakož i financování těchto činností, pokud jde o zabránění případným nežádoucím strategickým závislostem v budoucnosti a posílení celkové odolnosti dodavatelských řetězců IKT. V této souvislosti ZDŮRAZŇUJE úlohu a význam strategických a prováděcích úkolů Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost (ECCC) a sítě národních koordinačních center s cílem přispívat k maximalizaci účinků investic na posílení vedoucího postavení a otevřené strategické autonomie Unie v oblasti kybernetické bezpečnosti a podpůrných technologických kapacit a dovedností Unie a na zvýšení její globální konkurenceschopnosti. V tomto ohledu VYZÝVÁ k urychlenému zprovoznění ECCC. VYZÝVÁ ECCC, aby ve své strategické agendě zohlednilo aspekty bezpečnosti dodavatelského řetězce IKT, včetně například vývoje bezpečného softwaru, a to při současném zajištění soudržnosti a doplňkovosti a předcházení zdvojování úsilí. PODPORUJE posílení evropské konkurenceschopnosti v oblasti kybernetické bezpečnosti prostřednictvím programů financování, jako je program pro výzkum a inovace Horizont Evropa a program Digitální Evropa pro posílení, budování a získávání základních kapacit pro digitální ekonomiku, společnost a demokracii EU;

PODPŮRNÉ MECHANISMY

23. VYBÍZÍ k posílení pobídek finanční podpory souvisejících s opatřeními zaměřenými na posílení bezpečnosti dodavatelského řetězce IKT. VYZÝVÁ ECCC, Komisi a příslušné zúčastněné strany, aby prioritně prozkoumaly možnosti zahrnutí aspektů bezpečnosti dodavatelského řetězce IKT do nadcházejících výzev obsažených v pracovních programech pro kybernetickou bezpečnost v rámci programu Digitální Evropa a programu Horizont Evropa nebo do jakýchkoli jiných relevantních možností financování, a to i s ohledem na nadcházející provádění směrnice NIS 2. Tyto možnosti financování by měly být mimo jiné zaměřeny na to, aby organizacím umožnily podporovat zachování vysoké úrovně kybernetické bezpečnosti, pokud jde o zadávání zakázek na produkty a služby IKT v celém dodavatelském řetězci, zejména pokud jde o nahrazení konkrétních kritických služeb, systémů nebo produktů IKT považovaných za vysoce rizikové v souladu s budoucími koordinovanými posouzeními rizik dodavatelského řetězce;

24. UZNÁVÁ, že globalizace a specializace služeb IKT a zvýšená závislost na produktech a službách třetích stran s sebou nesou potřebu úzké spolupráce v rámci EU i na mezinárodní úrovni při sdílení poznatků a odborných znalostí mezi příslušnými zúčastněnými stranami, a VYBÍZÍ je, aby nalezly silnou a koordinovanou pozici zajišťující komplexní bezpečnost dodavatelského řetězce IKT. UZNÁVÁ rovněž, že je třeba dále zkoumat příslušné nejmodernější přístupy a techniky, a to jak pro odpovídající základní kybernetickou hygienu, tak pro dlouhodobá řešení pro dosažení bezpečných a odolných dodavatelských řetězců IKT, jakož i nejvhodnější způsoby jejich podpory a jejich případné začlenění do politických nebo jiných iniciativ. UZNÁVÁ v tomto ohledu, že zvláštní pozornost by měla být věnována zkoumání přínosů a nevýhod systematických řešení, jako jsou zásady nulové důvěry, soupis prvků použitých v softwaru a podobná dlouhodobá řešení. DOPORUČUJE využívat za tímto účelem skupinu pro spolupráci v oblasti bezpečnosti sítí a informací;

25. BERE NA VĚDOMÍ přínosy monitorování a účinného sdílení informací o kybernetických incidentech a hrozbách pro prevenci, odhalování a zmírňování účinků útoků na dodavatelské řetězce. ZDŮRAZŇUJE, že v zájmu účinného sdílení těchto informací je třeba nadále budovat důvěru mezi členskými státy. PŘIPOMÍNÁ v tomto ohledu návrh Komise podpořit členské státy při zřizování a posilování bezpečnostních operačních středisek (SOC) s cílem vybudovat síť bezpečnostních operačních středisek v celé EU a dále sledovat a na základě signálů předvídat útoky na sítě. PŘIPOMÍNÁ potřebu doplňkovosti a koordinace v rámci stávajících sítí a mechanismů, zejména v této souvislosti ZDŮRAZŇUJE úlohu sítě skupin pro reakce na počítačové bezpečnostní incidenty (týmů CSIRT) a potřebu dalšího zkoumání potenciálu těchto sítí s cílem podpořit účinnou, bezpečnou a spolehlivou kulturu sdílení informací. PŘIPOMÍNÁ úsilí členských států zřídit za podpory EU odvětvové, vnitrostátní a regionální týmy CSIRT a vnitrostátní či evropská střediska pro sdílení a analýzu informací (ISAC) jako součást účinné unijní sítě partnerství pro kybernetickou bezpečnost;

26. vzhledem k propojené a globální povaze hrozeb pro dodavatelský řetězec IKT ZDŮRAZŇUJE, že je důležité se bezpečnosti dodavatelského řetězce IKT věnovat a posilovat ji na celosvětové úrovni. S ohledem na tuto skutečnost DOPORUČUJE využívání digitálních partnerství, kybernetických dialogů a dalších příslušných iniciativ EU, včetně případných dohod o volném obchodu, za účelem podpory hodnocení dodavatelů produktů IKT a poskytovatelů služeb IKT založených na posouzení rizik, využívání důvěryhodných dodavatelů a vytvoření bezpečného a inovativního digitálního ekosystému založeného na otevřených, interoperabilních a transparentních normách. Kromě toho ZNOVU OPAKUJE vizi partnerství „Global Gateway“ a Rady EU–USA pro obchod a technologie a činnosti v rámci jejích pracovních skupin s cílem podpořit využívání důvěryhodných a jiných než vysoce rizikových dodavatelů a vytvořit mechanismus financování umožňující projekty zaměřené na bezpečnější, odolnější a důvěryhodnější infrastrukturu a služby IKT ve třetích státech, mimo jiné tím, že se zdrží financování nákupů od nedůvěryhodných a vysoce rizikových dodavatelů technologicky neutrálním způsobem;

27. ZNOVU POTVRZUJE svůj závazek přispívat k otevřenému, svobodnému, globálnímu, stabilnímu a bezpečnému kyberprostoru a prosazovat jej a dodržovat normy, pravidla a zásady odpovědného chování států v kyberprostoru stanovené v rámci OSN. Zejména v souvislosti s bezpečností dodavatelského řetězce IKT PŘIPOMÍNÁ normu schválenou skupinou vládních expertů OSN a otevřenou pracovní skupinou, v níž se státy vyzývají, aby podnikly přiměřené kroky k zajištění integrity dodavatelského řetězce, a to i prostřednictvím vypracování objektivních opatření spolupráce, aby koncoví uživatelé mohli mít důvěru v bezpečnost produktů IKT, a aby se snažily zabránit šíření škodlivých nástrojů a technik IKT a používání škodlivých skrytých funkcí, a ZASAZUJE SE za její široké provádění;