EVROPSKÁ
KOMISE

V Bruselu dne 15.9.2022
SWD(2022) 283 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN ZPRÁVY O POSOUZENÍ DOPADŮ

Akt o kybernetické odolnosti

Průvodní dokument k

návrhu
NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Souhrnný přehled (max. dvě strany)

Posouzení dopadů aktu o kybernetické odolnosti

A. Potřeba opatření

V čem spočívá problém a proč se jedná o problém na úrovni EU?

Hardwarové a softwarové produkty se stále častěji stávají předmětem úspěšných kybernetických útoků, což do roku 2021 povede k odhadovaným celosvětovým ročním nákladům spojeným s kybernetickou kriminalitou ve výši 5,5 bilionu EUR. Tyto produkty trpí dvěma hlavními problémy, které zvyšují náklady pro uživatele a společnost: 1) nízká úroveň kybernetické bezpečnosti, která se odráží v rozšířené zranitelnosti a nedostatečném a nekonzistentním poskytování bezpečnostních aktualizací k jejímu řešení, a 2) nedostatečné chápání informací a přístup k informacím ze strany uživatelů, což jim znemožňuje vybrat si produkty s patřičnými kybernetickými bezpečnostními vlastnostmi nebo je používat bezpečným způsobem.

Kybernetická bezpečnost produktů s digitálními prvky má silný přeshraniční rozměr, neboť produkty vyrobené v jedné zemi se často používají na celém vnitřním trhu. Kromě toho incidenty, které se zpočátku dotýkají jednoho subjektu nebo jednoho členského státu, se často během několika minut rozšíří po celém vnitřním trhu.

Zatímco stávající právní předpisy pro vnitřní trh se na některé produkty s digitálními prvky vztahují, většina hardwarových a softwarových produktů není v současné době upravena žádným právním předpisem EU, který by se zabýval jejich kybernetickou bezpečností. Stávající právní rámec EU se zejména nezabývá kybernetickou bezpečností nevestavěného softwaru, a to ani v případě, že se kybernetické útoky stále více zaměřují na zranitelnosti těchto produktů, což způsobuje značné společenské a hospodářské náklady. Mezi nedávné příklady patří spyware Pegasus, který zneužil zranitelnost mobilních telefonů, nebo ransomwarový červ WannaCry, který zneužil zranitelnost systému Windows a postihl počítače po celém světě.

Čeho by mělo být dosaženo?

Byly stanoveny dva hlavní cíle za účelem zajištění řádného fungování vnitřního trhu: 1) vytvořit podmínky pro vývoj bezpečných produktů s digitálními prvky tím, že bude zajištěno, aby hardwarové a softwarové produkty byly uváděny na trh s méně zranitelnostmi a aby výrobci brali vážně bezpečnost v průběhu celého životního cyklu produktu, a 2) vytvořit podmínky umožňující uživatelům, aby při výběru a používání produktů s digitálními prvky zohlednili kybernetickou bezpečnost. Byly stanoveny čtyři konkrétní cíle: i) zajistit, aby výrobci zlepšili bezpečnost produktů digitálními prvky od fáze návrhu a vývoje a během celého životního cyklu; ii) zajistit soudržný rámec kybernetické bezpečnosti, který výrobcům hardwaru a softwaru usnadní dodržování předpisů; iii) zvýšit transparentnost bezpečnostních vlastností produktů s digitálními prvky a iv) umožnit podnikům a spotřebitelům bezpečné používání produktů s digitálními prvky.

Jakou přidanou hodnotu budou mít tato opatření na úrovni EU (subsidiarita)?

Silná přeshraniční povaha kybernetické bezpečnosti a rostoucí počet incidentů, které se přelévají přes hranice a mezi odvětvími a produkty znamená, že těchto cílů nemohou členské státy účinně dosáhnout samy. Vzhledem ke globální povaze trhů s produkty s digitálními prvky čelí členské státy stejným rizikům u téhož produktu s digitálními prvky na svém území. Vznikající nejednotný rámec potenciálně odlišných vnitrostátních pravidel může také narušit otevřený a konkurenceschopný jednotný trh produktů s digitálními prvky. Pro zvýšení důvěry mezi uživateli a přitažlivosti produktů EU s digitálními prvky

uváděných na trh EU je proto nezbytná společná akce na úrovni EU. Prospěla by rovněž vnitřnímu trhu tím, že by výrobcům produktů s digitálními prvky poskytla právní jistotu a zajistila rovné podmínky.

B. Řešení

Prostřednictvím kterých možností lze cílů dosáhnout? Je některá možnost upřednostňována? Pokud ne, proč?

Byly analyzovány čtyři možnosti politiky a související dílčí možnosti, které jdou nad rámec současného stavu: 1) přístup založený na právně nevynutitelných předpisech a dobrovolná opatření; 2) regulační zásah *ad hoc* zaměřený na konkrétní produkt za účelem kybernetické bezpečnosti hmotných produktů s digitálními prvky a příslušného vestavěného softwaru; 3) smíšený přístup, včetně horizontálních závazných pravidel pro kybernetickou bezpečnost hmotných produktů s digitálními prvky a příslušným vestavěným softwarem a odstupňovaný přístup k nevestavěnému softwaru se dvěma dílčími možnostmi posuzování shody, a 4) horizontální regulační zásah zavádějící požadavky na kybernetickou bezpečnost pro širokou škálu produktů s digitálními prvky, včetně nevestavěného softwaru, s dílčími možnostmi týkajícími se oblasti působnosti a posuzování shody.

Posouzení dopadů dospělo k závěru, že **upřednostňovanou možností** je možnost 4, která se vztahuje na všechny produkty s digitálními prvky a předpokládá povinné posouzení kritických produktů třetí stranou na základě posouzení účinnosti ve vztahu ke konkrétním cílům, efektivnosti nákladů a přínosů a soudržnosti.

Jaké jsou názory jednotlivých zúčastněných stran? Kdo podporuje kterou možnost?

Respondenti, kteří byli požádáni, aby zhodnotili účinnost politických zásahů, souhlasili s tím, že nejúčinnějším opatřením bude možnost 4 (4,08 na stupnici od 1 do 5). Patří sem spotřebitelské organizace (5,00), respondenti, kteří se označují za uživatele (4,22), oznámené subjekty (4,17), orgány dozoru nad trhem (5,00) a výrobci produktů s digitálními prvky (3,85), včetně malých a středních (4,05).

C. Dopady upřednostňované možnosti

Jaké jsou výhody upřednostňované možnosti (je-li nějaká doporučena, jinak uveďte výhody hlavních možností)?

Upřednostňovaná možnost by měla významné výhody pro různé zúčastněné strany. V případě podniků by zabránila rozdílným bezpečnostním pravidlům pro produkty s digitálními prvky a snížila by náklady na dodržování příslušných právních předpisů v oblasti kybernetické bezpečnosti. Došlo by ke snížení počtu kybernetických incidentů, nákladů na řešení incidentů a újmy na dobré pověsti. Odhaduje se, že v celé EU by tato iniciativa mohla vést ke snížení nákladů v důsledku incidentů postihujících podniky o přibližně 180 až 290 miliard EUR ročně. Dále by tato iniciativa vedla ke zvýšení obratu v důsledku rostoucího využívání produktů s digitálními prvky. Zlepšila by se tak rovněž celosvětová pověst společností, což by vedlo k nárůstu poptávky mimo EU. Pro koncové uživatele by upřednostňovaná možnost zvýšila transparentnost bezpečnostních vlastností a usnadnila by využívání produktů s digitálními prvky. Spotřebitelé a občané by rovněž těžili z lepší ochrany svých základních práv, například ochrany soukromí a údajů.

Jaké jsou náklady na upřednostňovanou možnost (je-li nějaká doporučena, jinak uveďte náklady na hlavní možnosti)?

Upřednostňovaná možnost by zároveň zvýšila náklady na dodržování předpisů a vymáhání pro podniky, oznámené subjekty a veřejné orgány, včetně oznamujících orgánů, akreditačních orgánů a orgánů dozoru

nad trhem. Pro vývojáře softwaru a výrobce hardwaru se zvýší přímé náklady na dodržování nových požadavků na kybernetickou bezpečnost, povinností posuzování shody, dokumentace a podávání zpráv, což povede k souhrnným nákladům na dodržování předpisů ve výši přibližně 29 miliard EUR při odhadované tržní hodnotě obratu produktů s digitálními prvky ve výši až 1 485 miliard EUR. Koncoví uživatelé, včetně podnikatelských koncových uživatelů, spotřebitelů a občanů, mohou čelit vyšším cenám produktů s digitálními prvky. Je však třeba na ně nahlížet v kontextu výše popsaných významných přínosů. U oznámených subjektů se očekává, že dodatečné náklady budou kompenzovány zvýšením obratu.

Jaké budou dopady na malé a střední podniky a na konkurenceschopnost?

Nové požadavky budou mít dopad na malé a střední podniky, a to jak v roli výrobce, tak koncového uživatele. Pokud jde o náklady na dodržování předpisů, malé a střední podniky by byly v zásadě zasaženy více než velké společnosti, které mají obvykle vyšší úspory z rozsahu a větší povědomí o kybernetické bezpečnosti. Malé a střední podniky by však z této iniciativy měly velký prospěch, neboť kybernetická bezpečnost začleněná do produktů s digitálními prvky by malým a středním podnikům jakožto uživatelům přinesla značnou úsporu nákladů. Jako výrobci by malé a střední podniky měly prospěch z větší důvěry koncových uživatelů a nových zákazníků. Bezproblémový přístup na vnitřní trh a snížení roztříštěnosti trhu mohou přinášet ještě větší prospěch malým a středním podnikům, neboť jsou hůře vybaveny k tomu, aby se vypořádaly s různými regulačními požadavky. I když malé a střední podniky zdůraznily potřebu přiměřeného přístupu a podpůrných opatření, obecně podporovaly rovné podmínky pro všechny společnosti a nedomnívaly se, že by byly ve scénáři horizontálních závazných požadavků znevýhodněny ve srovnání s většími společnostmi.

Očekávají se významné dopady na vnitrostátní rozpočty a správní orgány?

Iniciativa bude mít dopad na vnitrostátní orgány, například vnitrostátní oznamující orgány, akreditační orgány a orgány dozoru nad trhem, které mají odpovědnost za monitorování a prosazování navrhovaných opatření. Tyto orgány ponesou dodatečné náklady na přizpůsobení (např. odbornou přípravu a lidské zdroje) a na prosazování, aby byly zohledněny nové požadavky. Prostředky vynaložené akreditačními orgány jsou však kompenzovány a z velké části hrazeny subjekty posuzování shody prostřednictvím nákupu akreditačních služeb.

Očekávají se jiné významné dopady?

Neočekávají se žádné jiné významné negativní dopady. Upřednostňovaná možnost politiky by pomohla snížit počet a závažnost incidentů, včetně případů porušení zabezpečení osobních údajů, a měla by pozitivní společenské dopady, například snížení kybernetické kriminality. Poptávka po odbornících v oblasti bezpečnosti pravděpodobně poroste a asymetrie v oblasti informací o kybernetické bezpečnosti by se snížily.

Proporcionalita?

Upřednostňovaná možnost nepřekračuje rámec toho, co je nezbytné pro uspokojivé splnění konkrétních cílů. Zásah by zajistil, že produkty s digitálními prvky budou zabezpečeny během celého jejich životního cyklu a úměrně rizikům, kterým čelí.

D. Návazná opatření

Kdy bude tato politika přezkoumána?

Do [36 měsíců ode dne použitelnosti této iniciativy] a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu této iniciativy.