Rada
Európskej únie

V Bruseli 16. septembra 2022
(OR. en)

12429/22
ADD 6

Medziinštitucionálny spis:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	15. septembra 2022
Komu:	Generálny sekretariát Rady
Č. dok. Kom.:	SWD(2022) 283 final
Predmet:	PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU aktu o kybernetickej odolnosti Sprievodný dokument k NÁVRHU NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami a zmene nariadenia (EÚ) 2019/1020

Delegáciám v prílohe zasielame dokument SWD(2022) 283 final.

Príloha: SWD(2022) 283 final

EURÓPSKA
KOMISIA

V Bruseli 15. 9. 2022
SWD(2022) 283 final

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU

aktu o kybernetickej odolnosti

Sprievodný dokument

NÁVRHU NARIADENIA EURÓPSKEHO PARLAMENTU A RADY

o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami a zmene nariadenia (EÚ) 2019/1020

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

Súhrnný prehľad (max. 2 strany)

Posúdenie vplyvu aktu o kybernetickej odolnosti

A. Potreba konať

V čom spočíva problém a prečo ide o problém na úrovni EÚ?

Hardvérové a softvérové produkty sú často vystavené úspešným kybernetickým útokom, ktoré v roku 2021 viedli k odhadovaným celosvetovým ročným nákladom spôsobeným počítačovou kriminalitou vo výške 5,5 bilióna EUR. Tieto produkty majú dva hlavné problémy, ktoré zvyšujú náklady používateľov a spoločnosti: 1. nízku úroveň kybernetickej bezpečnosti, ktorá sa prejavuje rozšíreným výskytom zraniteľností a nedostatočným a nekonzistentným poskytovaním bezpečnostných aktualizácií na ich odstránenie, a 2. nedostatočné chápanie používateľov a ich prístup k informáciám, čo im bráni vyberať si produkty s vhodnými vlastnosťami kybernetickej bezpečnosti alebo používať ich bezpečným spôsobom.

Kybernetická bezpečnosť produktov s digitálnymi prvkami má výrazný cezhraničný rozmer, keďže produkty vyrobené v jednej krajine sa často používajú na celom vnútornom trhu. Navyše incidenty, ktoré spočiatku ovplyvňujú jeden subjekt alebo jeden členský štát, sa často v priebehu minút rozšíria na celý vnútorný trh.

Hoci sa existujúce právne predpisy o vnútornom trhu uplatňujú na určité produkty s digitálnymi prvkami, na väčšinu hardvérových a softvérových produktov sa v súčasnosti nevzťahujú žiadne právne predpisy EÚ, ktoré by upravovali ich kybernetickú bezpečnosť. V súčasnom právnom rámci EÚ sa nerieši najmä kybernetická bezpečnosť nezabudovaného softvéru, a to ani vtedy, keď útoky na kybernetickú bezpečnosť sú čoraz častejšie zamerané na zraniteľnosti týchto produktov a spôsobujú značné spoločenské a hospodárske náklady. Nedávnymi príkladmi sú spyware Pegasus, ktorý využil zraniteľnosti v mobilných telefónoch, alebo ransomvérový červ WannaCry, ktorý využil zraniteľnosť systému Windows a zasiahol počítače na celom svete.

Čo by sa malo dosiahnuť?

V snahe zaistiť riadne fungovanie vnútorného trhu boli identifikované dva hlavné ciele: 1. vytvoriť podmienky pre vývoj bezpečných produktov s digitálnymi prvkami a to tým, že sa zabezpečí, aby sa na trh uvádzali hardvérové a softvérové produkty s menším počtom zraniteľností a aby výrobcovia brali bezpečnosť vážne počas celého životného cyklu produktu; a 2. vytvoriť podmienky, ktoré umožnia používateľom zohľadniť kybernetickú bezpečnosť pri výbere a používaní produktov s digitálnymi prvkami. Boli stanovené štyri špecifické ciele: i) zaistiť, aby výrobcovia zlepšili bezpečnosť produktov s digitálnymi prvkami od fázy návrhu a vývoja aj počas celého životného cyklu; ii) zaistiť koherentný rámec pre kybernetickú bezpečnosť, ktorý uľahčí výrobcom hardvéru a softvéru dodržiavať predpisy; iii) zlepšiť transparentnosť bezpečnostných vlastností produktov s digitálnymi prvkami a iv) umožniť podnikom a spotrebiteľom bezpečné používanie produktov s digitálnymi prvkami.

Aká je pridaná hodnota opatrení na úrovni EÚ (subsidiarita)?

Zo silného cezhraničného charakteru kybernetickej bezpečnosti a rastúceho počtu incidentov s účinkami, ktoré presahujú hranice, odvetvia a produkty, vyplýva, že ciele nemožno účinne dosiahnuť len na úrovni členských štátov. Vzhľadom na globálny charakter trhov s produktmi s digitálnymi prvkami čelia členské štáty na svojom území v prípade rovnakého produktu s digitálnymi prvkami rovnakým rizikám. Vznikajúci rôznorodý rámec potenciálne odlišných vnútroštátnych pravidiel takisto prináša riziká, ktoré narúšajú otvorený a konkurencieschopný jednotný trh s produktmi s digitálnymi prvkami. Potrebné je preto spoločné opatrenie na úrovni EÚ, aby sa zvýšila úroveň dôvery medzi používateľmi a atraktívnosť

produktov s digitálnymi prvkami uvádzanými na trh EÚ. Aj vnútornému trhu by prospelo, keby sa zabezpečila právna istota a dosiahli rovnaké podmienky pre predajcov produktov s digitálnymi prvkami.

B. Riešenia

Aké sú rôzne možnosti na dosiahnutie týchto cieľov? Je niektorá z možností uprednostňovaná? Ak nie, prečo?

Analyzovali sa štyri možnosti politiky a súvisiace čiastkové možnosti idúce nad rámec súčasného stavu: 1. tzv. soft law prístup a dobrovoľné opatrenia; 2. *ad hoc* regulačný zásah pre konkrétny produkt v oblasti kybernetickej bezpečnosti hmotných produktov s digitálnymi prvkami a príslušného zabudovaného softvéru; 3. kombinovaný prístup vrátane horizontálnych kogentných právnych noriem pre kybernetickú bezpečnosť hmotných produktov s digitálnymi prvkami a príslušného zabudovaného softvéru a dve čiastkové možnosti posudzovania zhody, a 4. horizontálny regulačný zásah, ktorým sa zavádzajú požiadavky kybernetickej bezpečnosti pre širokú škálu produktov s digitálnymi prvkami vrátane nezabudovaného softvéru, s čiastkovými možnosťami týkajúcimi sa rozsahu a posudzovania zhody.

Z posúdenia vplyvu vyplynul záver, že **uprednostňovanou možnosťou** je možnosť 4, ktorá sa vzťahuje na všetky produkty s digitálnymi prvkami a v ktorej sa predpokladá povinné posúdenie kritických produktov treťou stranou na základe posúdenia účinnosti vzhľadom na špecifické ciele, efektívnosti nákladov v porovnaní s prínosmi a konzistentnosti.

Aké sú názory jednotlivých zainteresovaných strán? Kto podporuje ktorú možnosť?

Pri požiadavke na hodnotenie účinnosti politických zásahov sa respondenti v rámci verejnej konzultácie zhodli na tom, že možnosť 4 by bola najúčinnejším opatrením (4,08 na stupnici od 1 do 5). Patria k nim spotrebiteľské organizácie (5,00), respondenti, ktorí sa identifikovali ako používatelia (4,22), notifikované osoby (4,17), orgány dohľadu nad trhom (5,00) a výrobcovia produktov s digitálnymi prvkami (3,85) vrátane malých a stredných výrobcov (4,05).

C. Vplyvy uprednostňovanej možnosti

Aké sú výhody uprednostňovanej možnosti (prípadne hlavných možností, ak sa žiadna konkrétna možnosť neuprednostňuje)?

Uprednostňovaná možnosť by priniesla značné výhody rôznym zainteresovaným stranám. V prípade podnikov by sa zabránilo rozdielnym bezpečnostným pravidlám pre produkty s digitálnymi prvkami a znížili by sa náklady na dodržiavanie príslušných právnych predpisov v oblasti kybernetickej bezpečnosti. Znížil by sa počet kybernetickobezpečnostných incidentov, náklady na ich riešenie a poškodenie dobrého mena. V prípade celej EÚ sa odhaduje, že iniciatíva by mohla viesť k zníženiu nákladov z incidentov ovplyvňujúcich podniky približne o 180 až 290 miliárd EUR ročne. Výsledkom iniciatívy by bol ďalej zvýšený obrat vďaka rastúcemu využívaniu produktov s digitálnymi prvkami. Zlepšila by sa aj celosvetová reputácia spoločností, čo by podnietilo zvýšenie dopytu z krajín mimo EÚ. Uprednostňovaná možnosť by pre koncových používateľov zvýšila transparentnosť bezpečnostných vlastností a uľahčila používanie produktov s digitálnymi prvkami. Spotrebitelia a občania by profitovali aj z lepšej ochrany svojich práv, ako je ochrana súkromia a ochrana osobných údajov.

Aké sú náklady na uprednostňovanú možnosť (prípadne na hlavné možnosti, ak sa žiadna konkrétna možnosť neuprednostňuje)?

Uprednostňovanou možnosťou by sa zvýšili náklady na dodržiavanie a presadzovanie predpisov pre podniky, notifikované osoby a subjekty verejného sektora vrátane notifikujúcich orgánov, akreditačných

orgánov a orgánov dohľadu nad trhom. V prípade vývojárov softvéru a výrobcov hardvéru sa zvýšia priame náklady na dodržiavanie predpisov vzhľadom na nové požiadavky kybernetickej bezpečnosti, posudzovanie zhody, dokumentáciu a oznamovacie povinnosti, čo bude viesť k súhrnným nákladom na dodržiavanie predpisov až do výšky približne 29 miliárd EUR pri odhadovanej trhovej hodnote obratu z produktov s digitálnymi prvkami vo výške 1 485 miliárd EUR. Koncoví používatelia, vrátane podnikových koncových používateľov, spotrebitelia a občania môžu čeliť vyšším cenám produktov s digitálnymi prvkami. Tieto by sa však mali chápať v kontexte už opísaných značných prínosov. V prípade notifikovaných osôb sa predpokladá, že dodatočné náklady budú kompenzované zvýšením obratu.
Aký je vplyv na MSP a konkurencieschopnosť?
MSP budú ovplyvnené novými požiadavkami ako výrobcovia aj ako koncoví používatelia. Pokiaľ ide o náklady na dodržiavanie predpisov, v zásade by boli MSP ovplyvnené viac ako veľké spoločnosti, ktoré majú obvykle lepšie úspory z rozsahu a väčšie povedomie o kybernetickej bezpečnosti. MSP by však mali veľký prínos z iniciatívy, keďže kybernetická bezpečnosť začlenená v produktoch s digitálnymi prvkami by pre MSP ako používateľov predstavovala výraznú úsporu nákladov. Ako výrobcovia by mali MSP prínos z väčšej dôvery koncových používateľov a z nových spotrebiteľov. Bezproblémový prístup na vnútorný trh a zníženie fragmentácie trhu môže byť ešte výhodnejšie pre MSP, ktoré sú menej vybavené na zvládnutie rôznych regulačných požiadaviek. MSP pri zdôraznení potreby proporcionálneho prístupu a podporných opatrení vo všeobecnosti podporovali rovnaké podmienky medzi všetkými spoločnosťami a nedomnievali sa, že by boli znevýhodnené v porovnaní s väčšími spoločnosťami v prípade horizontálnych povinných požiadaviek.
Očakáva sa významný vplyv na štátne rozpočty a verejnú správu?
Iniciatíva bude mať vplyv na vnútroštátne orgány, ako sú vnútroštátne notifikujúce orgány, akreditačné orgány a orgány dohľadu nad trhom, ktoré sú zodpovedné za monitorovanie a presadzovanie navrhovaných opatrení. Tieto orgány budú znášať dodatočné náklady na úpravu (napr. školenie a ľudské zdroje) a presadzovanie predpisov s cieľom zohľadniť nové požiadavky. Zdroje vynaložené akreditačnými orgánmi sa však kompenzujú a do veľkej miery ich znášajú orgány posudzovania zhody prostredníctvom nákupu akreditačných služieb.
Očakávajú sa iné významné vplyvy?
Neočakávajú sa žiadne ďalšie významné negatívne vplyvy. Uprednostňovaná možnosť politiky by pomohla znížiť počet a závažnosť incidentov vrátane porušení ochrany osobných údajov a mala by pozitívne sociálne vplyvy, ako je zníženie počítačovej kriminality. Dopyt po odborníkoch na bezpečnosť bude pravdepodobne rásť a nevyváženosť, pokiaľ ide o informácie o kybernetickej bezpečnosti, by sa znížila.
Proporcionalita?
Uprednostňovaná možnosť neprekračuje rámec nevyhnutný na uspokojivé plnenie špecifických cieľov. Zásahom by sa zaistilo, že produkty s digitálnymi prvkami budú zabezpečené počas celého svojho životného cyklu a úmerne k rizikám, ktorým čelia.
D. Nadväzné opatrenia
Kedy sa táto politika preskúma?

Do [36 mesiacov] odo dňa začiatku uplatňovania tejto iniciatívy, a potom každé štyri roky predloží Komisia Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tejto iniciatívy.