Rada
Európskej únie

V Bruseli 14. septembra 2017
(OR. en)

12183/17
ADD 2

Medziinštitucionálny spis:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

SPRIEVODNÁ POZNÁMKA

Od:	Jordi AYET PUIGARNAU, riaditeľ, v zastúpení generálneho tajomníka Európskej komisie
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	SWD(2017) 501 final
Predmet:	PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE ZHRNUTIE POSÚDENIA VPLYVU Sprievodný dokument Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“)

Delegáciám v prílohe zasielame dokument SWD(2017) 501 final.

Príloha: SWD(2017) 501 final

EURÓPSKA
KOMISIA

V Bruseli 13. 9. 2017
SWD(2017) 501 final

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE POSÚDENIA VPLYVU

Sprievodný dokument

Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY

o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“)

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A) POTREBA KONAŤ

V čom spočíva problém a prečo je to problém?

Digitálne technológie a internet sú opornými piliermi hospodárstva a spoločnosti EÚ. Kľúčové odvetvia hospodárstva ako doprava, energetika, zdravotníctvo či finančníctvo sú pri výkone svojich hlavných činností čoraz závislejšie od sieťových a informačných systémov. Ľudia a predmety sa stretávajú na internete vecí, ktorý využíva komunikačné siete. Táto nová realita prináša nevídané príležitosti, ale odhaľuje aj zraniteľné miesta. Kybernetické incidenty sa už rozmáhajú a ich komplexnosť, frekvencia a miera ich účinku – od prístupu k základným službám až po demokratické procesy – bude ďalej rásť.

V tomto kontexte sa identifikovali nasledujúce vzájomne previazané problémy:

- fragmentácia politík a prístupov ku kybernetickej bezpečnosti v jednotlivých členských štátoch,
- rozptýlené zdroje, ale aj prístupy ku kybernetickej bezpečnosti v rámci inštitúcií, agentúr a orgánov EÚ,
- nedostatočné povedomie občanov a firiem o kybernetických hrozbách, nedostatočné informácie o bezpečnostných vlastnostiach produktov a služieb IKT, ktoré si kupujú, ako aj čoraz častejšia prax prelínajúcich sa certifikačných systémov jednotlivých členských štátov a odvetví.

Tieto problémy vplývajú na celkovú kybernetickú odolnosť EÚ a efektívne fungovanie vnútorného trhu.

Čo by sa malo dosiahnuť?

Iniciatíva má tieto osobitné politické ciele:

1. posilniť spôsobilosti a pripravenosť členských štátov a podnikov, najmä z hľadiska kritických infraštruktúr;
2. zlepšiť spoluprácu a koordináciu medzi členskými štátmi, inštitúciami, agentúrami a orgánmi EÚ;
3. posilniť spôsobilosti na úrovni EÚ na doplnenie činností členských štátov, a to najmä v prípade cezhraničných kybernetických kríz;
4. zvýšiť informovanosť občanov a podnikov o otázkach kybernetickej bezpečnosti;
5. zvýšiť celkovú transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti produktov a služieb IKT, čím sa posilní dôvera v digitálny jednotný trh a v digitálnu inováciu;
6. zabrániť roztrieštenosti systémov certifikácie v EÚ a súvisiacich bezpečnostných požiadaviek a hodnotiacich kritérií v jednotlivých členských štátoch a odvetviach.

Aká je pridaná hodnota opatrení na úrovni EÚ?

Keďže digitalizácia a prepojenosť hospodárstva a spoločnosti má globálny dosah, rozmer týchto problémov výrazne presahuje hranice jedného členského štátu. Je preto potrebné konať na úrovni Únie. V súčasnom kontexte a berúc do úvahy budúce scenáre sa javí, že individuálne kroky členských štátov a nejednotný prístup ku kybernetickej bezpečnosti nedokážu, najmä vzhľadom na silný cezhraničný rozmer, zvýšiť spoločnú kybernetickú odolnosť Únie.

B) RIEŠENIA

Aké sú jednotlivé možnosti na dosiahnutie týchto cieľov? Uprednostňuje sa niektorá možnosť?

Toto posúdenie vplyvu sa zameriava na konkrétny súbor možností politiky zahŕňajúci revíziu agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), ako aj bezpečnostnú certifikáciu v odvetví IKT.

Revízia ENISA

Možnosť 0 – **východiskový scenár** – Pri tejto možnosti by sa zachoval *status quo*. Mandát agentúry ENISA by sa predĺžil, pričom ciele a úlohy agentúry by zostali z veľkej časti nezmenené, pri zohľadnení úloh, ktoré agentúre ENISA ukladajú neskoršie právne predpisy EÚ (napr. smernica NIS).

Možnosť 1 – **ukončenie mandátu agentúry ENISA** (a jej zrušenie). Táto možnosť by znamenala zrušenie agentúry ENISA na konci jej mandátu (jún 2020) a prípadne prerozdelenie jej kompetencií/činností na úrovni EÚ a/alebo členských štátov.

Možnosť 2 – **„reformovaná agentúra ENISA“**. Táto možnosť by nadviazala na súčasný mandát agentúry ENISA s cieľom prijať selektívne zmeny, ktoré zohľadňujú vývoj v kyberneticko-bezpečnostnej sfére. Agentúra by dostala trvalý mandát, stavajúc na týchto kľúčových prvkoch: podpora tvorby a vykonávania politík EÚ, budovanie kapacít, znalosti a informácie, trhové úlohy, výskum a inovácia, operačná spolupráca a krízové riadenie.

Možnosť 3 – **Agentúra EÚ pre kybernetickú bezpečnosť s plnými operačnými spôsobilosťami**. Táto možnosť znamená reformovanie agentúry ENISA sústredením troch hlavných funkcií: 1. politická/poradná funkcia; 2. stredisko informácií a odborných poznatkov a 3. tím reakcie na núdzové počítačové situácie (CERT). Táto možnosť by do značnej miery znamenala rovnakú zmenu rozsahu mandátu ako možnosť 2. Pridali by sa však dodatočné úlohy v oblasti reakcie na incidenty a krízového riadenia, takže agentúra by spravovala celý životný cyklus kybernetickej bezpečnosti od prevencie cez odhaľovanie až po reakciu na kybernetické incidenty.

Certifikácia

Možnosť 0 – východiskový scenár – žiadne kroky. Pri tejto možnosti by Komisia zachovala súčasný stav a nepodnikala žiadne politické ani legislatívne kroky.

Možnosť 1 – **nelegislatívne opatrenia („soft law“)**. Pri tejto možnosti by Komisia použila nezáväzné politické nástroje (napr. výkladové oznámenia, podporu celoúnijných

samoregulačných iniciatív a normalizačných činností) na zvýšenie transparentnosti a zmiernenie roztrieštenosti.

<u>Možnosť 2</u> – legislatívny akt na úrovni EÚ s cieľom rozšíriť dohodu SOG-IS na všetky členské štáty. Pri tejto možnosti politiky by Komisia navrhla legislatívny akt, ktorým by sa členstvo zákonne rozšírilo na všetky členské štáty.

<u>Možnosť 3</u> – všeobecný rámec bezpečnostnej certifikácie IKT v EÚ. Táto možnosť zahŕňa vytvorenie európskeho rámca bezpečnostnej certifikácie IKT (vrátane expertnej skupiny zloženej z vnútroštátnych orgánov), ktorý by čo najviac nadväzoval na existujúce systémy bezpečnostnej certifikácie IKT. Rámec by v zásade umožnil zriadenie certifikačných systémov EÚ, ktoré sa budú uznávať vo všetkých členských štátoch.

Uprednostňuje sa kombinácia možnosti 2 v prípade ENISA a možnosti 3 pri certifikácii.

Kto sú jednotlivé zainteresované strany? Kto podporuje ktorú možnosť?

Drvivá väčšina zainteresovaných strán vo všetkých kategóriách (teda členské štáty, odvetvie, inštitúcie EÚ, výskumná obec), ktoré sa zúčastnili na konzultáciách, podľa všetkého víta uprednostňovanú možnosť, keďže sú za posilnenie agentúry ENISA a vytvorenie európskeho rámca bezpečnostnej certifikácie IKT.

Zhodujú sa najmä na potrebe (minimálne) riadne fungujúcej agentúry EÚ s trvalým mandátom, ktorá bude mať primerané zdroje a mandát na riešenie súčasných i budúcich kyberneticko-bezpečnostných problémov. Medzi zainteresovanými stranami zároveň panuje všeobecná zhoda v otázke zriadenia dobrovoľného a rozšíriteľného európskeho rámca.

Na strane odvetvia toto riešenie certifikácie podporujú podniky, ktoré už certifikačným požiadavkám podliehajú a ktorým by prospel celoúnijný mechanizmus založený na vzájomnom uznávaní certifikátov. Podporujú ho aj MSP, ktoré najviac trpia tým, že musia alebo by museli absolvovať odlišné certifikačné postupy v rôznych členských štátoch. Niektoré členské štáty (najmä tie s obmedzenejšími zdrojmi), ako aj niektorí zástupcovia odvetvia a inštitúcií EÚ sa v otázke agentúry ENISA vyjadrili aj za možnosť 3.

C) VPLYVY UPREDNOSTŇOVANEJ MOŽNOSTI

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

Pri uprednostňovanej možnosti by EÚ mala agentúru zameranú na podporu členských štátov, inštitúcií EÚ a firiem v oblastiach, kde by priniesla najvyššiu pridanú hodnotu. Patrí sem: podpora vykonávania smernice NIS; príprava a vykonávanie politík; informácie, poznatky a zvyšovanie povedomia; výskum; operačná spolupráca a krízové riadenie; trh. Konkrétne by ENISA podporovala politiku EÚ v oblasti bezpečnostnej certifikácie IKT zabezpečovaním administratívnej údržby a technického riadenia európskeho rámca bezpečnostnej certifikácie IKT. Takýto rámec v praxi zavedie súbor pravidiel spravovania bezpečnostnej certifikácie IKT v EÚ, čím by sa podporil systém vzájomného uznávania certifikátov vydaných v rôznych členských štátoch. Riešenie kombinujúce tieto možnosti sa považuje za najúčinnejšie na dosiahnutie stanovených cieľov EÚ, ktorými sú posilnenie spôsobilostí v oblasti kybernetickej bezpečnosti, pripravenosť, spolupráca, povedomie, transparentnosť a

predchádzanie roztrieštenosti trhu. Zároveň je táto možnosť v najväčšom súlade s politickými prioritami, keďže je zakotvená v stratégii kybernetickej bezpečnosti a súvisiacich politikách (napr. smernica NIS), ako aj v stratégii digitálneho jednotného trhu. Okrem toho by sa pri tejto možnosti ciele dosiahli s rozumným vynaložením zdrojov.

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

„Reformovaná agentúra ENISA“ by si aj napriek novým úlohám zachovala svoju akcieschopnosť. Potrebný finančný príspevok z rozpočtu EÚ by bol vyšší než v súčasnosti, no stále výrazne pod úrovňou iných agentúr, ktoré tiež pôsobia v kľúčových oblastiach.

Vytvorenie európskeho rámca bezpečnostnej certifikácie IKT by pre odvetvie (vrátane MSP) neprinieslo žiadne počiatočné náklady navyše. Naopak, výraznú úsporu by zaznamenali tie firmy, ktoré už svoje produkty certifikujú alebo sú ochotné podstúpiť bezpečnostnú certifikáciu, pričom by sa zároveň zvýšila ich svetová konkurencieschopnosť. Na druhej strane táto možnosť zahŕňa určité rozpočtové záväzky na správu tohto rámca, ktorý by z hľadiska technických úloh a sekretariátu zabezpečoval model „reformovanej agentúry ENISA“.

Očakáva sa významný vplyv na štátne rozpočty a verejnú správu?

Nie. Náklady spojené s posilnením agentúry ENISA by z najväčšej časti pokrýval rozpočet EÚ, hoci členské štáty by mohli na činnosť agentúry dobrovoľne finančne prispievať. Pokiaľ ide o certifikáciu, hlavný dosah na štátne rozpočty a správy spočíva v náležitých prípadoch v zriadení certifikačného orgánu.

Očakávajú sa iné významné vplyvy?

Nie.

Proporcionalita?

Uprednostňovaná možnosť zavádza vyvážené opatrenia, ktoré sa všetky považujú za potrebné na dosiahnutie predmetných cieľov, pričom príslušné zainteresované strany nadmerne nezaťažujú. Preto sa táto iniciatíva považuje za vyhovujúcu zásade proporcionality.

D) NADVÄZUJÚCE OPATRENIA

Kedy sa táto politika preskúma?

Navrhuje sa, aby sa prvé hodnotenie vykonalo päť rokov po nadobudnutí účinnosti právneho nástroja. Komisia následne podá Európskemu parlamentu a Rade z hodnotenia správu, ktorú prípadne doplní návrhom na revíziu aktu. Ďalšie hodnotenia sa budú musieť vykonávať každých päť rokov.