Rada
Európskej únie

V Bruseli 22. marca 2022
(OR. en)

7474/22
ADD 3

Medziinštitucionálny spis:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	22. marca 2022
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	SWD(2022) 68 final
Predmet:	PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE ZHRNUTIE ANALÝZY VPLYVU Sprievodný dokument k návrhu NARIADENIA EURÓPSKEHO PARLAMENTU A RADY, ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

Delegáciám v prílohe zasielame dokument SWD(2022) 68 final.

Príloha: SWD(2022) 68 final

EURÓPSKA
KOMISIA

V Bruseli 22. 3. 2022
SWD(2022) 68 final

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE ANALÝZY VPLYVU

Sprievodný dokument

k návrhu NARIADENIA EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

{COM(2022) 122 final} - {SWD(2022) 67 final}

1. Úvod

V roku 2020 sa prudko zvýšil počet významných incidentov ovplyvňujúcich inštitúcie, orgány a agentúry Únie, ktorých pôvodcami boli aktéri označovaní ako pokročilé pretrvávajúce hrozby (advanced persistent threat, APT). To sa prejavuje aj v počte forenzných obrázkov, ktoré CERT-EU analyzovalo v roku 2020, ktorý sa v porovnaní s rokom 2019 viac než strojnásobil, zatiaľ čo počet významných incidentov od roku 2018 vzrástol viac než desaťnásobne.

Schopnosti v oblasti kybernetickej bezpečnosti a výdavky na bezpečnosť IT sú však v niektorých prípadoch v inštitúciách, orgánoch a agentúrach Únie pozoruhodne rozdielne, čo má za následok širokú škálu úrovní vyspelosti v oblasti kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie. Z analýzy panorámy hrozieb a zo štatistík incidentov v rámci bezpečnosti IT však vyplýva, že kybernetická expozícia inštitúcií, orgánov a agentúr Únie sa bude len zintenzívňovať.

2. Ciele

Identifikované nedostatky v konečnom dôsledku vedú k nedostatočnej úrovni kybernetickej odolnosti v inštitúciách, orgánoch a agentúrach Únie, rozdrobenému zabezpečovaniu zdrojov v oblasti bezpečnosti IT a k nevyrovnanému stavu bezpečnosti IT.

Cieľom legislatívneho aktu by bolo stanovenie opatrení na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie. Tým by sa podporilo a zabezpečilo, aby vyspelosť v oblasti kybernetickej bezpečnosti držala krok so zrýchľujúcou sa digitalizáciou inštitúcií, orgánov a agentúr Únie.

3. Medziinštitucionálna rada pre kybernetickú bezpečnosť a rámec kybernetickej bezpečnosti

Návrhom Medziinštitucionálnej rady pre kybernetickú bezpečnosť a rámca kybernetickej bezpečnosti sa zavedú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie, ktoré umožnia zosúladenie do rámca, ktorým sa riešia kybernetickobezpečnostné hrozby vo všetkých inštitúciách, orgánoch a agentúrach Únie, a Medziinštitucionálnej rade pre kybernetickú bezpečnosť sa stanovia povinnosti monitorovania a predkladania správ.

Návrhom sa modernizuje poslanie a úlohy CERT-EU a berie sa do úvahy zmenená a zvýšená digitalizácia v inštitúciách, orgánoch a agentúrach Únie v posledných rokoch, ako aj vyvíjajúca sa panoráma kybernetickobezpečnostných hrozieb.

Návrh nemá žiadny priamy vplyv ani rozpočtové dôsledky pre členské štáty ani občanov EÚ.

Právnym základom nariadenia je článok 298 Zmluvy o fungovaní Európskej únie, v ktorom sa stanovuje, že pri vykonávaní svojich poslaní sú inštitúcie, orgány, úrady a agentúry Únie podporované otvorenou, efektívnou a nezávislou európskou administratívou.

Tento návrh vychádza zo Stratégie EÚ pre bezpečnostnú úniu [COM(2020) 605 final] a zo stratégie kybernetickej bezpečnosti EÚ v digitálnej dekáde [JOIN(2020) 18 final].

4. Záver

Prostredníctvom Medziinštitucionálnej rady pre kybernetickú bezpečnosť a rámca kybernetickej bezpečnosti sa dosahuje väčšina plánovaných cieľov pomerne účinne, efektívne a súdržne s ostatnými politikami Únie s najširšou podporou zainteresovaných strán.

Zvolené riešenie je najživotaschopnejšou možnosťou vzhľadom na prevládajúce právne hranice, v rámci ktorých konáme. Prístup jedného riešenia, ktoré by vyhovovalo všetkým, by navyše nezodpovedal súčasnej rozličnej vyspelosti inštitúcií, orgánov a agentúr Únie a rozdielom v technologickom riziku a zložitosti, ktorým čelia.