Rada
Evropské unie

Brusel 29. března 2022
(OR. en)

Interinstitucionální spis:
2022/0084(COD)

7670/22
ADD 7

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	22. března 2022
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	SWD(2022) 65 final
Předmět:	PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE SOUHRN ZPRÁVY O ANALÝZE DOPADŮ Průvodní dokument k návrhu nařízení Evropského parlamentu a Rady o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie

Delegace naleznou v příloze dokument SWD(2022) 65 final.

Příloha: SWD(2022) 65 final

EVROPSKÁ
KOMISE

V Bruselu dne 22.3.2022
SWD(2022) 65 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN ZPRÁVY O ANALÝZE DOPADŮ

Průvodní dokument k

návrhu nařízení Evropského parlamentu a Rady

o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie

{COM(2022) 119 final} - {SWD(2022) 66 final}

Souhrnný přehled

Analýza dopadů na bezpečnost informací v orgánech, institucích a jiných subjektech Unie

A. Politické souvislosti

Strategická agenda Evropské rady na období 2019–2024 vyzývá orgány, aby chránily informační a komunikační sítě EU a její rozhodovací procesy před nepřátelskými činnostmi všeho druhu, včetně kybernetických a hybridních hrozeb. Rada pro obecné záležitosti proto v prosinci 2019 dospěla k závěru, že orgány a instituce EU by měly vypracovat a provést komplexní soubor opatření k zajištění bezpečnosti jejich informací.

V červenci 2020 přijala Komise strategii bezpečnostní unie EU, v níž se zavázala doplnit úsilí členských států v oblasti bezpečnosti. V rámci této strategie Komise navrhla vytvořit minimální soubor pravidel pro bezpečnost informací a kybernetickou bezpečnost ve všech orgánech a institucích Unie.

B. Jaký problém se řeší?

Hlavní problémy jsou tyto: i) významný rozdíl mezi úrovní bezpečnosti orgánů a institucí Unie v závislosti na jejich vnitřních pravidlech pro bezpečnost informací a ii) nedostatečná koordinace mezi orgány a institucemi Unie při plnění jejich bezpečnostních úkolů.

V současné době mají orgány a instituce Unie pro bezpečnost informací buď vlastní pravidla, nebo taková pravidla zatím vůbec nepřijaly. Roztříštěnost použitelného právního rámce vedla v různých oblastech k různým kategoriím neutajovaných informací, rozdílným označením a pokynů pro manipulaci. Pokud jde o utajované informace EU, interoperabilita příslušných systémů zůstává omezená, což brání bezproblémovému předávání informací mezi orgány a institucemi a s členskými státy.

Tato situace zvyšuje riziko, že útočníci způsobí narušení bezpečnosti na nejslabším článku a využijí je jako výchozí bod pro další útoky na jiné orgány nebo instituce.

C. Čeho by mělo být dosaženo?

Obecným cílem iniciativy je vytvořit pravidla pro bezpečnost informací pro všechny orgány a instituce Unie s cílem zajistit silnější a důslednou ochranu před vyvíjejícími se hrozbami pro jejich informace.

Obecný cíl se promítá do čtyř specifických cílů:

- zavést harmonizované a komplexní kategorie informací,
- identifikovat nedostatky v oblasti bezpečnosti a provést požadovaná opatření,
- zavést úzkou spolupráci v oblasti bezpečnosti informací mezi orgány a institucemi Unie,
- modernizovat politiky v oblasti bezpečnosti informací s ohledem na digitální transformaci a práci z domova.

D. Jaké jsou názory jednotlivých zúčastněných stran?

Konzultované zúčastněné strany (orgány a instituce Unie, vnitrostátní bezpečnostní orgány členských států a odborníci na výzkum ze Společného výzkumného střediska) se shodly na potřebě společných norem v

oblasti bezpečnosti informací pro všechny orgány a instituce Unie se zaměřením na tyto body:

- Měla by být zohledněna rozmanitost a odlišné podnikatelské prostředí každého orgánu a instituce a mělo se umožnit řešení na místní úrovni.
- Ačkoli většina orgánů a institucí je připravena spolupracovat se svými protějšky ve společných orgánech pro účely bezpečnosti informací, nejsou ochotny delegovat své rozhodovací pravomoci.
- Návrh nařízení by měl být vypracován s ohledem na mezivládní dohodu[1] členských států o ochraně utajovaných informací.

E. Jaký má návrh dopad?

Přínosy

Vytvořením základních pravidel pro bezpečnost informací ve všech orgánech a institucích Unie návrh nařízení zvýší celkovou úroveň bezpečnosti informací a zároveň sníží stávající nejednotnost. Měl by rovněž pomoci odstranit případná slabá místa a chránit informace sdílené v rámci evropské správy.

Z hlediska účinnosti by návrh nařízení měl vést k přínosům plynoucím z koordinovaného plnění společných úkolů v oblasti bezpečnosti informací (např. prověrky, akreditace komunikačních a informačních systémů) a vytvoření společných správních orgánů (např. interinstitucionální koordinační skupiny, technických podskupin).

Hospodářský dopad

U orgánů a institucí Unie se očekává, že úsilí potřebné k provedení nových právních předpisů bude kompenzováno zvýšením efektivity, přičemž dodatečné náklady lze zahrnout do stávajících programů na zlepšení bezpečnosti informací v každé organizaci. Z dlouhodobého hlediska budou těžit ze soudržného přístupu k řešení neustále se vyvíjejících hrozeb pro bezpečnost informací.

Evropská komise by měla zajistit stálý sekretariát interinstitucionální koordinační skupiny a přidělit na tento úkol lidské zdroje (jeden úředník AD a jeden úředník AST).

Na úrovni správních orgánů členských států a soukromého sektoru se neočekávají žádné hospodářské dopady.

F. Následná opatření

Kdy bude tato politika přezkoumána?

Úplné hodnocení s cílem posoudit dopady a provádění návrhu nařízení bude provedeno každých pět let po datu použitelnosti. Komise vypracuje zprávu obsahující její zjištění a předloží ji Evropskému parlamentu a Radě.

[1] Dohoda mezi členskými státy Evropské unie zasedajícími v Radě o ochraně utajovaných informací vyměňovaných v zájmu Evropské unie, 2011/C202/05.