Rada
Evropské unie

Brusel 22. března 2022
(OR. en)

Interinstitucionální spis:
2022/0085(COD)

7474/22
ADD 3

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

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) 68 final
Předmět:	PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE SOUHRN ANALÝZY DOPADŮ Průvodní dokument k návrhu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

Delegace naleznou v příloze dokument SWD(2022) 68 final.

Příloha: SWD(2022) 68 final

EVROPSKÁ
KOMISE

V Bruselu dne 22.3.2022
SWD(2022) 68 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN ANALÝZY DOPADŮ

Průvodní dokument k

návrhu NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

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

1. Úvod

V roce 2020 výrazně vzrostl počet významných incidentů postihujících orgány, instituce a jiné subjekty Unie, jejichž původci byli aktéři pokročilé trvalé hrozby (APT). To se rovněž odrazilo v počtu bitových kopií pro forenzní analýzu, které analyzoval tým CERT-EU v roce 2020; ve srovnání s rokem 2019 se jejich počet ztrojnásobil, přičemž počet významných incidentů se od roku 2018 zvýšil více než desetinásobně.

Schopnosti v oblasti kybernetické bezpečnosti a výdaje na bezpečnost informačních technologií v orgánech, institucích a jiných subjektech Unie jsou v některých případech nápadně nerovnoměrné, což vede k tomu, že je škála úrovní vyspělosti kybernetické bezpečnosti u orgánů, institucí a jiných subjektů Unie velmi rozsáhlá. Z analýzy prostředí hrozeb a ze statistiky o bezpečnostních incidentech v oblasti informačních technologií dále vyplývá, že kybernetická expozice orgánů, institucí a jiných subjektů kybernetickým hrozbám se bude jen zintenzivňovat.

2. Cíle

Zjištěné nedostatky v konečném důsledku vedou k nedostatečné úrovni kybernetické odolnosti orgánů, institucí a jiných subjektů Unie, k roztříštěnému vynakládání zdrojů na zajištění bezpečnosti informačních technologií a k nevyvážené situaci v oblasti zabezpečení informačních technologií.

Cílem legislativního aktu by bylo poskytnout opatření pro zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie. To by podpořilo a zajistilo, že vyspělost kybernetické bezpečnosti bude držet krok se zrychlující se digitalizací orgánů, institucí a jiných subjektů Unie.

3. Interinstitucionální výbor pro kybernetickou bezpečnost a rámec pro kybernetickou bezpečnost

Návrh na zřízení Interinstitucionálního výboru pro kybernetickou bezpečnost a rámce pro kybernetickou bezpečnost zavede opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a dalších subjektech Unie, jež umožní sbližování všech orgánů, institucí a jiných subjektů Unie kolem tohoto rámce za účelem řešení kybernetických bezpečnostních hrozeb, a zavede monitorování a podávání zpráv Interinstitucionálnímu výboru pro kybernetickou bezpečnost.

Návrh modernizuje poslání a úkoly centra CERT-EU s ohledem na změny a nárůst digitalizace orgánů, institucí a jiných subjektů Unie v posledních letech a vyvíjející se prostředí kybernetických bezpečnostních hrozeb.

Návrh nemá přímý dopad ani rozpočtové důsledky pro členské státy nebo občany EU.

Právním základem pro nařízení je článek 298 Smlouvy o fungování Evropské unie, který stanoví, že při plnění svých úkolů se orgány, instituce a jiné subjekty Unie opírají o otevřenou, efektivní a nezávislou evropskou správu.

Tento návrh navazuje na strategii bezpečnostní Unie EU (COM(2020) 605 final) a na strategii kybernetické bezpečnosti EU pro digitální dekádu (JOIN(2020) 18 final).

4. Závěr

Interinstitucionální výbor pro kybernetickou bezpečnost a rámec pro kybernetickou bezpečnost dosahují většiny zamýšlených cílů relativně účinným a efektivním způsobem,

soudržným s jinými politikami Unie s nejširší podporou zúčastněných stran. Toto řešení, jež bylo vybráno, je nejvíce životaschopnou možností s ohledem na přetrvávající právní hranice, ve kterých se pohybujeme, přičemž univerzální přístup „jednoho řešení vhodného pro všechny“ by zároveň neodpovídal dnešní heterogenní vyspělosti orgánů, institucí a jiných subjektů Unie a rozdílům v technologických rizicích a složitostem, s nimiž se potýkají.