Rada
Evropské unie

Brusel 22. ledna 2026
(OR. en)

Interinstitucionální spisy:
2026/0011 (COD)
2026/0012 (COD)

5611/26
ADD 2

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	21. ledna 2026
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	SWD(2026) 12 final
Předmět:	PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE SOUHRN ZPRÁVY O POSOUZENÍ DOPADŮ Průvodní dokument k návrhu nařízení Evropského parlamentu a Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2) a návrhu směrnice Evropského parlamentu a Rady, kterou se mění směrnice (EU) 2022/2555, pokud jde o zjednodušující opatření a sladění s [návrhem aktu o kybernetické bezpečnosti 2]

Delegace naleznou v příloze dokument SWD(2026) 12 final.

Příloha: SWD(2026) 12 final

EVROPSKÁ
KOMISE

Ve Štrasburku dne 20.1.2026
SWD(2026) 12 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN ZPRÁVY O POSOUZENÍ DOPADŮ

Průvodní dokument k

návrhu nařízení Evropského parlamentu a Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2)

a

návrhu směrnice Evropského parlamentu a Rady, kterou se mění směrnice (EU) 2022/2555, pokud jde o zjednodušující opatření a sladění s [návrhem aktu o kybernetické bezpečnosti 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Souhrn posouzení dopadů

Cíl

Hlavním cílem tohoto posouzení dopadů je zhodnotit přiměřenost stávajících předpisů při řešení vyvíjejících se kybernetických bezpečnostních hrozeb v celé EU. Navrhuje integrovaný soubor možností politiky zaměřených na posílení Agentury Evropské unie pro kybernetickou bezpečnost (ENISA), reformu evropského rámce pro certifikaci kybernetické bezpečnosti a zjednodušení dodržování stávajícího legislativního rámce v oblasti kybernetické bezpečnosti. Toto posouzení zdůrazňuje, že je důležité upravit správu v kybernetické oblasti tak, aby byla v souladu s technologickým pokrokem a požadavky trhu, a zároveň zajistit konkurenceschopnost a zohlednit dopady na životní prostředí.

Formulace problému

Navzdory dosavadnímu úsilí se prostředí kybernetické bezpečnosti v EU v kontextu stále složitějších hrozeb nadále potýká se značnými výzvami. Účinnému řízení kybernetické bezpečnosti brání nedostatečná koordinace mezi členskými státy a dalšími aktéry na úrovni EU, váznoucí provádění nástrojů politiky a regulační překážky a složitost. Tyto problémy mají za následek zvýšené náklady pro podniky a veřejné orgány, zvýšené riziko kybernetických incidentů a nejednotnou úroveň ochrany občanů.

Odůvodnění pro opatření EU

Kybernetické bezpečnostní hrozby překračují hranice států; proto důrazná reakce nezbytně vyžaduje jednotný přístup. Intervence na úrovni EU zajišťuje důslednou ochranu, zvyšuje konkurenceschopnost tím, že poskytuje rovné podmínky, a usnadňuje volný pohyb digitálních služeb a produktů v rámci jednotného trhu. Harmonizace na úrovni EU rovněž snižuje administrativní zátěž díky zjednodušení dodržování předpisů a zefektivnění postupů.

Možnosti politiky a upřednostňovaná možnost

Tato zpráva analyzuje čtyři oblasti intervence, z nichž každá obsahuje soubor možností politiky zvažovaných s ohledem na specifické cíle, jichž má být dosaženo: 1) mandát agentury ENISA (rovněž součást stávajícího aktu o kybernetické bezpečnosti); 2) evropský rámec pro certifikaci kybernetické bezpečnosti (rovněž součást současného aktu o kybernetické bezpečnosti) a 3) cílené změny směrnice NIS 2, jejichž cílem je zjednodušení a které jsou zároveň propojeny s mandátem agentury ENISA a evropským rámcem pro certifikaci kybernetické bezpečnosti. Každý z těchto souborů možností představuje samostatnou oblast intervence, která je zároveň vzájemně propojená s ostatními oblastmi a je pro ně relevantní.

Možnosti řešení nesouladu mezi rámcem politiky kybernetické bezpečnosti EU a potřebami zúčastněných stran ve stále nepřátelštějším prostředí

Možnost A.1: *Vyjasnění mandátu agentury ENISA a stanovení priorit* – tato možnost by zajistila jasný a stabilní rámec pro úkoly agentury ENISA začleněním úkolů stanovených v jiných právních předpisech.

Možnost A.2: *Reforma mandátu agentury ENISA* – tato možnost by zrušila a nahradila akt o kybernetické bezpečnosti a zcela přepracovala mandát agentury.

Možnost A.3: *Reforma mandátu agentury ENISA s výrazným zaměřením na operativní podporu* – tato možnost by navazovala na možnost A.2. Kromě toho by agentura ENISA vyvinula kapacity, které by na žádost členského státu přímo podporovaly subjekty podle směrnice NIS 2 při reakci na kybernetické bezpečnostní incidenty a obnově po takových incidentech.

Možnosti týkající se evropského rámce pro certifikaci kybernetické bezpečnosti

Možnost B.1: *Vyjasnění oblasti působnosti, prvků a cílů evropského rámce pro certifikaci kybernetické bezpečnosti a zavedení mechanismu udržování* – tato možnost stanoví nový mechanismus udržování schémat, který by po jejich přijetí prováděla agentura ENISA.

Možnost B.2: *Reforma evropského rámce pro certifikaci kybernetické bezpečnosti revizí jeho postupů a rozšířením oblasti působnosti s cílem usnadnit dodržování právních předpisů* – v rámci této možnosti by byl akt o kybernetické bezpečnosti zrušen a nahrazen novým nařízením. Vedle možnosti B.1 by byl také revidován postup týkající se žádostí, vývoje a přijímání schémat, aby se zlepšila odpovědnost a účinnost.

Možnost B.3: *Reforma evropského rámce pro certifikaci kybernetické bezpečnosti podle možnosti B.2 a zavedení povinné certifikace kybernetické pozice* – tato možnost by navazovala na možnost B.2, jejím cílem je však dále zvýšit dopad rámce zavedením povinné certifikace základních subjektů spadajících do oblasti působnosti směrnice NIS 2, a to s ohledem na konkrétní rizikové scénáře, namísto využívání pouze dobrovolné certifikace subjektů.

Možnosti týkající se zjednodušení

Možnost C.1: *Uplatnění přístupu založeného na „soft law" a nelegislativních nástrojích, včetně využití stávajících zmocnění (přijetí prováděcích aktů podle čl. 21 odst. 5 a čl. 23 odst. 11 směrnice NIS 2)* – tato možnost předpokládá přijetí prováděcích aktů s využitím stávajících zmocnění podle směrnice NIS 2 s cílem zajistit vyšší míru harmonizace opatření pro řízení rizik v oblasti kybernetické bezpečnosti, prahových hodnot pro hlášení incidentů, jakož i údajů, formátů a postupů podávání oznámení, spolu s přijetím souboru pokynů ke zvýšení právní jistoty a harmonizovaného provádění.

Možnost C.2: *Cílená intervence – další zjednodušení dodržování příslušného legislativního rámce Unie pro kybernetickou bezpečnost* – tato možnost zahrnuje omezenou intervenci prostřednictvím změn aktu o kybernetické bezpečnosti a směrnice NIS 2 s cílem zjednodušit konkrétní aspekty rámce kybernetické bezpečnosti, včetně úprav oblasti působnosti, maximální harmonizace prováděcích aktů, prokázání souladu prostřednictvím certifikace a přijetí souboru pokynů, jak se předpokládá v rámci možnosti C1.

Možnost C.3: *Harmonizace opatření souvisejících s kybernetickou bezpečností stanovených v právních předpisech Unie* – tato možnost by navazovala na možnost C.2 a odstranila by všechna opatření k řízení kybernetických bezpečnostních rizik nebo zmocnění související s těmito opatřeními obsažená v odvětvových právních předpisech. Namísto toho by byl ekosystém směrnice NIS 2 změněn tak, aby stanovil zjednodušené požadavky pro všechny druhy subjektů a zajistil tímto způsobem větší harmonizaci.

Možnosti pro zabezpečení dodavatelského řetězce IKT

Možnost D.1: *Přístup k řešení kybernetických bezpečnostních rizik v dodavatelských řetězcích IKT na základě „soft law“* – tato možnost by neumožňovala regulační intervenci na úrovni EU. Namísto toho by Komise zvýšila počet koordinovaných posouzení rizik a dobrovolných souborů nástrojů.

Možnost D.2: *Regulační intervence ad hoc kodifikující soubor opatření pro sítě 5G* – tato možnost by kodifikovala opatření obsažená v souboru opatření pro sítě 5G. Zavedla by povinnost členských států zajistit, aby v klíčových aktivech sítě nebyly používány komponenty od vysoce rizikových dodavatelů.

Možnost D.3: *Komplexní a horizontální rámec pro řešení kybernetických bezpečnostních rizik v dodavatelských řetězcích IKT* – tato možnost by zavedla horizontální, technologicky a odvětvově neutrální regulační rámec pro řešení netechnických kybernetických bezpečnostních rizik v dodavatelských řetězcích IKT.

Po rozsáhlých analýzách upřednostňovaný balíček politik zahrnuje: možnost A.2 – Reforma mandátu agentury ENISA; možnost B.2 – Reforma evropského rámce pro certifikaci kybernetické bezpečnosti revizí postupu a rozšířením oblasti působnosti s cílem usnadnit zjednodušení dodržování právních předpisů; možnost C.2 – Cílená intervence – další zjednodušení dodržování příslušného legislativního rámce Unie pro kybernetickou bezpečnost a možnost D.3 – Komplexní a horizontální rámec pro řešení kybernetických bezpečnostních rizik v dodavatelských řetězcích IKT.

Tato kombinace nabízí dobře vyváženou reakci na zjištěné politické výzvy a výrazně zvyšuje účinnost, efektivnost a soudržnost v celé EU.

Hlavní dopady

Analýza nákladů a přínosů: Přechod na navrhovaný regulační rámec přinese agentuře ENISA náklady na plnění jejích nových úkolů odhadované na částku 161,3 milionu EUR za pět let a veřejným orgánům v celé EU náklady na dohled ve výši až 80 milionů EUR za pět let (se zohledněním příslušných úspor nákladů). Pokud jde o podniky, během tříletého přechodného období by postupné vyřazování konkrétních vysoce rizikových zařízení mohlo vést k ročním nákladům ve výši 3,4 až 4,3 miliardy EUR pro provozovatele mobilních sítí, zatímco investice do důvěryhodných dodavatelů by mohly současně vzrůst až na 2 miliardy EUR ročně. Kromě toho se očekává, že zjednodušení a omezení povinností týkajících se dodržování předpisů povede pro podniky k úsporám nákladů ve výši až 14,6 miliardy EUR. Kromě toho by ze zlepšení celkové kybernetické pozice a technologické suverenity EU a z

podněcování inovací a konkurenceschopnosti plynuly značné přínosy pro občany, veřejné orgány a podniky, které by měly v dlouhodobém horizontu do značné míry kompenzovat počáteční výdaje.

Konkurenceschopnost: Upřednostňované možnosti snižují roztříštěnost trhu a harmonizují regulatorní požadavky, a tím zvyšují rovnost v hospodářské soutěži v celé EU a poskytují podnikům jasnější cesty k dodržování předpisů a inovacím.

Kontrola souladu s cíli v oblasti klimatu: Při posuzování se zvažoval potenciální dopad každé možnosti na životní prostředí. Zvláštní pozornost byla věnována energetické účinnosti, emisím souvisejícím s cestováním a konsolidaci infrastruktury. Upřednostňované možnosti A.2, B.2 a C.2 mají omezený dopad na životní prostředí, zatímco možnost D.3 zohledňuje environmentální neutralitu s ohledem na životní cyklus produktů a přechodná období pro náhradu klíčových aktiv. To je v souladu se závazkem EU k udržitelnosti.

Digitalizace jako standard: Důraz na zefektivnění digitálních procesů prokazuje závazek EU k přístupu upřednostňujícímu digitální řešení, který zajistí rychlejší a spolehlivější výměnu dat a rozhodování. Možnost D.3 by mohla mít rovněž velký dopad na digitalizaci, neboť by znamenala nahrazení komponent pocházejících od subjektů usazených ve třetích zemích nebo kontrolovaných subjekty z těchto zemí, které vzbuzují obavy z hlediska kybernetické bezpečnosti.

Zjednodušení a snížení zátěže: Upřednostňované možnosti přispívají ke zjednodušení, neboť zavádějí vyjasnění oblasti působnosti a opatření ke zjednodušení dodržování předpisů a dohledu, což snižuje administrativní zátěž. Je zohledněna zásada „jeden přijmout – jeden zrušit“, neboť je zajištěno, aby nové povinnosti byly vyváženy snížením požadavků v jiných oblastech.

Závěr

Toto posouzení dopadů představuje komplexní strategii pro zvýšení kybernetické bezpečnosti EU, řešení neefektivních prvků regulace a přípravu digitálního prostředí na budoucí výzvy. Doporučuje společný a soudržný přístup, ukotvuje politické reformy ve stávajících rámcích a zároveň se přizpůsobuje nové technologické realitě. Prostřednictvím těchto opatření hodlá EU zajistit odolnou, konkurenceschopnou a udržitelnou digitální ekonomiku.