EVROPSKÁ KOMISE

Brusel 25.10.2023
C(2023) 7405 final

Vážený pane předsedo,

rádi bychom poděkovali Senátu za jeho stanovisko k těmto dokumentům:

- *sdělení Komise Evropskému parlamentu a Radě – Řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU („Akademie dovedností v oblasti kybernetické bezpečnosti“) (COM(2023) 207 final),*
- *návrh nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně (COM(2023) 209 final) a*
- *návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby (COM(2023) 208 final).*

S ohledem na současný geopolitický kontext je nezbytné, aby Evropa postupovala společně v duchu jednoty, solidarity a rozhodnosti. „Balíček opatření v oblasti kybernetické bezpečnosti“ přijatý dne 18. dubna 2023 by vytvořil mechanismy, které jsou v souvislosti s rostoucími kybernetickými hrozbami potřebné k zajištění kybernetické bezpečnosti a posílení spolupráce na úrovni Unie.

Vítáme, že Senát podporuje cíle sdělení o Akademii dovedností v oblasti kybernetické bezpečnosti. Snahou Komise je řešit nedostatek dovedností v oblasti kybernetické bezpečnosti a odstranění nedostatků na trhu práce za účelem posílení konkurenceschopnosti, růstu a odolnosti Evropské unie.

Současná bezpečnostní situace vyžaduje posílenou solidaritu na úrovni Unie, aby bylo možné lépe odhalovat kybernetické hrozby a incidenty a připravit se a reagovat na ně, což je cíl nového návrhu aktu o kybernetické solidaritě.

Pokud jde o obavy Senátu týkající se sdílení informací v souvislosti s novým návrhem aktu o kybernetické solidaritě, jakož i možné duplikace navrhovaného evropského kybernetického štítu se stávající sítí CSIRT, je třeba poznamenat, že navrhovaná opatření nemají vliv na odpovědnost členských států v oblasti národní bezpečnosti, veřejné bezpečnosti a prevence, vyšetřování, odhalování a stíhání trestných činů. Sdílení informací mezi účastníky evropského kybernetického štítu by kromě toho muselo být v souladu se stávajícími právními požadavky, zejména s právními předpisy Unie a vnitrostátními právními předpisy v oblasti ochrany údajů, jakož i s pravidly Unie pro hospodářskou soutěž, jimiž se řídí výměna informací. Členské státy, které by se evropského kybernetického štítu účastnily, by podle návrhu musely zajistit vysokou úroveň bezpečnosti údajů

Pan Miloš Vystrčil
Předseda Senátu
Valdštejnské náměstí 17/4
CZ – 118 26 PRAHA 1

a fyzické bezpečnosti infrastruktury evropského kybernetického štítu. Dále, pokud jde o sdílení informací se subjekty ze třetích zemí, musel by být zajištěn soulad s bezpečnostními zájmy Unie.

Bezpečnostní operační střediska tvořící evropský kybernetický štít a zřizovaná na dobrovolném základě a s využitím finančních prostředků Unie by nevedla k duplikaci se strukturami pro výměnu informací a spolupráci podle revidované směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS 2)[1], jako je síť bezpečnostních týmů typu CSIRT. Evropský kybernetický štít má zlepšit situační povědomí v EU tím, že bude národní a přeshraniční bezpečnostní operační střediska vybízet, aby s pomocí interoperabilních nástrojů a infrastruktur operativním způsobem shromažďovala údaje a sdílela zpravodajské informace o kybernetických hrozbách. To znamená, že evropský kybernetický štít by činnost vykonávanou sítí bezpečnostních týmů typu CSIRT doplňoval.

Je třeba rovněž poznamenat, že členské státy mohou jako národní bezpečnostní operační středisko určit některý ze stávajících subjektů, například svůj vnitrostátní bezpečnostní tým typu CSIRT, je-li to subjekt veřejný. Stejně tak by členské státy, které se chtějí evropského kybernetického štítu účastnit, měly možnost určit i jiný subjekt než svůj vnitrostátní bezpečnostní tým typu CSIRT. Rozhodnutí je ponecháno zcela na nich.

Pokud jde o podnět Senátu posilovat již fungující formy spolupráce v rámci kybernetické bezpečnosti, je třeba poznamenat, že navrhovaným aktem o kybernetické solidaritě se stávající systém správy programu Digitální Evropa nemění, ale tento akt jej spíše rozvíjí a posiluje. Navrhovaným nařízením se stávající evropské kapacity doplňují, a to na jedné straně s cílem budovat a posilovat společné schopnosti bezpečnostních operačních středisek v oblasti odhalování a situačního povědomí a na straně druhé za účelem rozvoje připravenosti a schopnosti reakce na významné a rozsáhlé kybernetické bezpečnostní incidenty.

Pokud jde o připomínky týkající se chybějícího posouzení dopadů, navrhovaný akt o kybernetické solidaritě vychází z opatření, která již byla zahájena a která jsou již podporována v rámci programu Digitální Evropa. Patří k nim výzva ke zřizování národních a přeshraničních bezpečnostních operačních středisek v rámci programu Digitální Evropa a krátkodobý podpůrný program poskytovaný Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) na opatření na podporu kybernetické bezpečnosti pro připravenost a reakci na incidenty. Navrhovaný akt o kybernetické solidaritě by umožnil dlouhodobou podporu těchto opatření, a posílil tak solidaritu a lepší koordinaci na úrovni EU.

Opatření navrhovaná v tomto nařízení by byla podporována programem Digitální Evropa a jsou v souladu se správou a rozpočtem stanovenými v nařízení o programu Digitální Evropa. Návrh neukládá povinnosti jednotlivcům ani společnostem. Nebude mít žádné významné administrativní dopady ani dopady na životní prostředí nad rámec těch, které již byly posouzeny v posouzení dopadů nařízení o programu Digitální Evropa. Jeho cílem není harmonizace ani stanovení nových regulačních povinností, nýbrž nasměrování finančních prostředků EU vyhrazených na kybernetickou bezpečnost do opatření s velkým dopadem a posílení naší kolektivní schopnosti bránit se stále vážnějším kybernetickým hrozbám.

---

[1] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (Úř. věst. L 333, 27.12.2022, s. 80).

Navrhované nařízení by tedy rovněž změnilo nařízení o programu Digitální Evropa[2] tak, aby zahrnovalo další činnosti v rámci specifického cíle č. 3, aniž by se odchýlilo od původního rámce programu Digitální Evropa a stávajících pracovních programů. Je třeba rovněž poznamenat, že hlavní navrhovaná opatření jsou dobrovolné povahy, což znamená, že si členské státy mohou zvolit, zda se chtějí účastnit akcí souvisejících s posilováním schopností odhalovat hrozby či zda budou využívat navrhované podpory připravenosti a reakce na incidenty.

Závěrem je třeba připomenout, že tento návrh byl přijat v souvislosti s agresí Ruska vůči Ukrajině, kterou doprovázejí strategie nepřátelských kybernetických operací, což změnilo vnímání a hodnocení připravenosti EU na kolektivní řešení krizí v oblasti kybernetické bezpečnosti. V závěrech Rady ze dne 23. května 2022 o rozvoji kybernetické pozice Evropské unie byla Komise vyzvána, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

V souladu s pokyny Komise pro zdokonalení tvorby právních předpisů tedy již existuje dostatek podkladů, jež umožňují provedení těchto omezených změn v programu Digitální Evropa i bez vypracování posouzení dopadů.

Doufáme, že jsme uvedenými vysvětleními dostatečně reagovali na připomínky Senátu, a těšíme se na další pokračování vzájemného politického dialogu.

S úctou

Maroš Šefčovič
výkonný místopředseda

Thierry Breton
člen Komise

ÚŘEDNĚ OVĚŘENÝ OPIS
Za generální tajemnici

Martine DEPREZ
Ředitel
Rozhodování a jednání ve sboru
EVROPSKÁ KOMISE

[2] Nařízení Evropského parlamentu a Rady (EU) 2021/694 ze dne 29. dubna 2021, kterým se zavádí program Digitální Evropa a zrušuje rozhodnutí (EU) 2015/2240 (Úř. věst. L 166, 11.5.2021, s. 1).