EVROPSKÝ ÚČETNÍ DVŮR

CS

Tisková zpráva

Lucemburk 19. března 2019

V oblasti kybernetické bezpečnosti EU existuje nemálo výzev, varují auditoři

Podle nového informačního dokumentu Evropského účetního dvora je pro zvýšení kybernetické bezpečnosti v EU i přes učiněný pokrok stále nutné překonat řadu výzev. Vzhledem k narůstajícímu riziku, že se staneme obětí kyberkriminality nebo kybernetického útoku, je zcela zásadní budovat odolnost posílením správy, zvyšováním znalostí a informovanosti a zlepšením koordinace, říkají auditoři. Zdůrazňují také význam smysluplného vyvozování odpovědnosti a hodnocení, aby EU mohla dosáhnout svého cíle stát se nejbezpečnějším digitálním prostředím na světě.

Cílem tohoto informačního dokumentu je poskytnout přehled o situaci v oblasti politiky kybernetické bezpečnosti v EU, kterou autoři označují za složitou a nevyrovnanou, a určit hlavní výzvy z hlediska účinného provádění této politiky.

„*S ohledem na současné problémy spojené s kybernetickými útoky je právě nyní rozhodující doba na to, aby EU posílila svou kybernetickou bezpečnost a digitální nezávislost. Zároveň je třeba soustavně zachovávat základní hodnoty EU*," **uvedl Baudilio Tomé Muguruza, člen Evropského účetního dvora odpovědný za informační dokument**.

Auditoři rozdělili výzvy v oblasti kybernetické bezpečnosti do čtyř okruhů: politika a legislativní rámec, financování a výdaje, budování kybernetické odolnosti a účinná reakce na kybernetické bezpečnostní incidenty.

Politika a legislativní rámec: kybernetický ekosystém EU je složitý a mnohovrstevný. Snaha o propojení všech jeho vyvíjejících se součástí v jeden komplexní, strategický, soudržný a koordinovaný celek představuje velmi náročný úkol. Vypracovat opatření, která jsou v souladu se strategií v oblasti kybernetické bezpečnosti EU, je vzhledem k absenci měřitelných cílů a nedostatku spolehlivých údajů obtížné. Výstupy se málokdy měří a hodnoceno je jen málo oblastí, včetně stavu kybernetické bezpečnosti a připravenosti EU. Je tedy třeba zajistit posun směrem ke kultuře založené na výkonnosti se zabudovanými mechanismy hodnocení.

Účelem této tiskové zprávy je informovat o hlavních bodech informačního dokumentu Evropského účetního dvora.
Plné znění tohoto dokumentu je k dispozici na internetové stránce www.eca.europa.eu.

ECA Press

Mark Rogerson – tiskový mluvčí **T: (+352) 4398 47063** **M: (+352) 691 55 30 63**
Damijan Fišer – pracovník tiskového oddělení **T: (+352) 4398 45410** **M: (+352) 621 55 22 24**
12, rue Alcide De Gasperi - L-1615 Luxembourg
E: press@eca.europa.eu **@EUAuditors** **eca.europa.eu**

Financování a výdaje: výdaje na kybernetickou bezpečnost v EU jsou podle informačního dokumentu nízké a roztříštěné. EU a její členské státy musí vědět, jaké částky se investují kolektivně, aby určily, které nedostatky odstranit, avšak získat o tom jasný přehled je obtížné. Neexistuje žádný zvláštní rozpočet EU na financování strategie kybernetické bezpečnosti a chybí jasná představa o tom, kam které finanční prostředky směřují.

Komise se snaží překonat roztříštěnost v oblasti výzkumu kybernetické bezpečnosti, ale v současnosti výsledky investic do výzkumu často nejsou dostatečně patentovány, obchodně využity nebo šířeny, což omezuje odolnost, konkurenceschopnost a nezávislost EU.

Budování kybernetické odolnosti: absence jednotného mezinárodního rámce pro řízení kybernetické bezpečnosti narušuje schopnost mezinárodního společenství reagovat na kybernetické útoky a předcházet jim. Ve veřejném i soukromém sektoru v celé EU se často vyskytují nedostatky v řízení kybernetické bezpečnosti. Je proto obtížné dosáhnout jednotného přístupu ke kybernetické bezpečnosti na úrovni celé EU. Vzhledem k rostoucímu globálnímu nedostatku znalostí v oblasti kybernetické bezpečnosti má také zásadní význam zvyšování dovedností a informovanosti ve všech odvětvích a oblastech společnosti.

Účinná reakce na kybernetické bezpečnostní incidenty: digitální systémy jsou dnes natolik složité, že zabránit všem útokům je nemožné. Je proto třeba zajistit rychlou detekci a reakci. Kybernetická bezpečnost ještě není plně začleněna do stávajících mechanismů koordinace reakcí na krizi na úrovni EU, což potenciálně omezuje schopnost EU reagovat na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty. Závažným problémem je také případné zasahování do volebních procesů a dezinformační kampaně, zejména s ohledem na volby do Evropského parlamentu v květnu 2019.

Poznámky pro redaktory

Informační dokument je popisný a analytický dokument týkající se určité oblasti politiky. Neobsahuje auditní zjištění. Analýza v tomto dokumentu vychází z dokumentárního přezkumu informací, které jsou veřejně dostupné v oficiálních dokumentech, písemných stanoviscích a studiích třetích stran. Práce přímo na místě proběhla od dubna do září 2018 a zohledněn byl vývoj do prosince 2018. Auditoři v rámci své práce provedli také průzkum mezi národními kontrolními úřady členských států a pohovory s hlavními zainteresovanými stranami z institucí EU a zástupci soukromého sektoru.

Informační dokument EÚD „Výzvy týkající se účinné politiky EU v oblasti kybernetické bezpečnosti“ je k dispozici na internetové stránce EÚD (eca.europa.eu) ve 23 jazycích.