Evropský Parlament schválil nové zákony, posilující kybernetickou bezpečnost Evropské Unie v klíčových sektorech

Autor: Evropský Parlament (10. listopadu 2022)

Zdroj: Tisková zpráva a Návrh směrnice

Souhrn

S rychle se rozšiřující digitalizací každodenního života, dále urychlenou pandemií Covid-19, se ochrana před kybernetickými hrozbami stala nezbytnou pro správné fungování společnosti. Kybernetické útoky mohou být velmi nákladné. Podle Evropské komise se odhaduje, že roční náklady na kyberkriminalitu pro globální ekonomiku do konce roku 2020 dosáhly 5,5 bilionu EUR.

Dne 10. listopadu 2022 Evropský Parlament aktualizoval právní předpisy Evropské Unie (dále jen „EU"), aby posílil investice do silné kybernetické bezpečnosti základních služeb a kritických infrastrukturu a posílit pravidla pro celou EU.

1) Směrnice o bezpečnosti sítí a informací (NIS2)

Směrnice zavádí nová pravidla pro dosažení vysoké společné úrovně kybernetické bezpečnosti v celé EU – jak pro společnosti, tak pro země. Posiluje také požadavky na kybernetickou bezpečnost pro středně velké a velké subjekty, které působí a poskytují služby v klíčových odvětvích. Aktualizace směrnice NIS z roku 2016 má za cíl zlepšit srozumitelnost

a provádění a také řešit rychlý vývoj v této oblasti. Pokrývá více odvětví a činností než dříve, zjednodušuje oznamovací povinnosti a řeší bezpečnost dodavatelského řetězce. Po schválení parlamentem 10. listopadu jej budou muset schválit také země EU v Radě, poté budou mít členské státy 21 měsíců na jeho zavedení.

Nový zákon rozšiřuje okruh odvětví a činností, které jsou zásadní pro ekonomiku a společnost, včetně energetiky, dopravy, bankovnictví, zdravotnictví, digitální infrastruktury, veřejné správy a vesmíru. Nezahrnuje však národní a veřejnou bezpečnost, vymáhání práva nebo soudnictví. Zákon se vztahuje na veřejnou správu na centrální a regionální úrovni, nikoli však na parlamenty a centrální banky.

Vyžaduje, aby více subjektů a sektorů přijalo opatření k řízení rizik v oblasti kybernetické bezpečnosti, včetně poskytovatelů veřejných služeb elektronických komunikací, provozovatelů sociálních médií, výrobců kritických produktů (včetně zdravotnických prostředků) a poštovních a kurýrních služeb.

Zákon stanovuje pro země EU přísnější povinnosti v oblasti kybernetické bezpečnosti, pokud jde o dohled. Zlepšuje prosazování těchto povinností, včetně harmonizace sankcí mezi členskými státy. Jejím cílem je také zlepšit spolupráci mezi zeměmi EU, a to i v případě rozsáhlých incidentů, pod záštitou Agentury EU pro kybernetickou bezpečnost (Enisa).

2) Zákon o digitální operační odolnosti (Dora)

Vzhledem k tomu, že finanční sektor je stále více závislý na softwaru a digitálních procesech, potřebuje také zvýšenou ochranu. Zákon o digitální operační odolnosti (Dora) zajistí, že finanční sektor EU bude odolnější vůči vážným provozním poruchám a kybernetickým útokům. Parlament definitivně schválil právní předpis, který byl dříve dohodnut s Radou, dne 10. listopadu 2022.

Zákon zavádí a harmonizuje požadavky na digitální provozní odolnost pro sektor finančních služeb EU a zavazuje společnosti, aby zajistily, že budou schopny odolat všem typům narušení a hrozeb souvisejících s informačními a komunikačními technologiemi (ICT), reagovat na ně a zotavit se z nich.

Nová pravidla se vztahují na všechny společnosti poskytující finanční služby – jako jsou banky, poskytovatelé plateb, poskytovatelé elektronických peněz, investiční firmy, poskytovatelé služeb kryptoaktiv a také na kritické poskytovatele služeb v oblasti ICT třetích stran. Vnitrostátní orgány budou na provádění dohlížet a prosazovat jej.