Zákon o kritické infrastruktuře: východiska a aktuální stav

kpt. Ing. David Patrman, Ph.D., *MV-GŘ HZS ČR, david.patrman@hzscr.cz*

Souhrn

Příspěvek se zabývá aktuální podobou věcného záměru zákona o odolnosti subjektů kritické infrastruktury (zákon o kritické infrastruktuře), kterým je do národní legislativy transponována směrnice Evropského parlamentu a Rady (EU) 2022/2557 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (tzv. směrnice CER). Obsahem příspěvku je popis východisek připravovaného zákona, včetně přiblížení změn oproti současnému pojetí systému ochrany kritické infrastruktury, postupu při identifikování subjektů kritické infrastruktury nebo gescí za jednotlivá odvětví a pododvětví. Současně jsou představeny vybrané zamýšlené nástroje, jako je dokumentace, opatření k zajištění odolnosti, hlášení incidentů nebo ověřování spolehlivosti. V kontextu zmiňovaného zákona shrnuje také podstatu souvisejících prováděcích právních předpisů.

Klíčová slova: *kritická infrastruktura, subjekt kritické infrastruktury, odolnost, směrnice CER, základní služba*

Úvod

Připravovaný zákon o odolnosti subjektů kritické infrastruktury (zákon o kritické infrastruktuře) je reakcí na transpozici směrnice Evropského parlamentu a Rady (EU) 2022/2557 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (tzv. směrnice CER), která nabyla účinnosti dne 16. ledna 2023, do právního řádu České republiky. Jak již její název napovídá, tato směrnice mimo jiné zcela nahrazuje směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Souvisejícím dokumentem se směrnicí CER je poté nařízení Komise v přenesené pravomoci (EU) 2023/2450, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2022/2557 stanovením seznamu základních služeb.

Změny oproti současnému systému

S novým pojetím systémy ochrany kritické infrastruktury se pojí určité změny oproti současnému systému, který vychází z krizového zákona č. 240/2000 Sb. Nejzásadnější změnou je celková změna filozofie při identifikaci samotné kritické infrastruktury. Dosud se pozornost zaměřovala na jednotlivé prvky, které se v případě naplnění prahových hodnot kritérií staly prvky kritické infrastruktury. Nově budou identifikovány subjekty kritické infrastruktury, které si poté na základě vlastního uvážení identifikují takovou svou infrastrukturu, která je pro jejich poskytování konkrétní základní služby nezbytná. Chráněným zájmem se tak nově stane kontinuální poskytování základní služby. Základní služby budou rozděleny do odvětví, případně pododvětví, přičemž každé z nich bude mít stanoveného gestora. Při identifikaci subjektů kritické infrastruktury již nebudou používána průřezová a odvětvová kritéria, ale pouze specifické kritérium nebo kritéria pro každou základní službu, která budou definována takovým způsobem, aby nevznikal prostor pro pochybnosti, zdali je daný subjekt naplňuje či nikoliv. Zcela novými nástroji pak budou hlášení incidentů, cvičení či ověřování spolehlivosti.

Proces identifikování subjektů kritické infrastruktury

Úvodním krokem při identifikaci subjektů kritické infrastruktury bude vstup samotného zákona a nařízení vlády o základních službách a kritérií významnosti v platnost. Potenciální subjekt kritické infrastruktury poté posoudí, zdali naplňuje kritérium významnosti u poskytované základní služby a v případě kladného posouzení splní svou povinnost tím, že požadované informace vloží do informačního systému Portál kritické infrastruktury. Gestor tyto informace posoudí z hlediska relevance a v případě kladného posouzení doporučí Ministerstvu vnitra zapsat dotčený subjekt na seznam subjektů kritické infrastruktury. Po tomto zapsání gestor (případně Ministerstvo vnitra) vyrozumí dotyčný subjekt o tom, že

se stává subjektem kritické infrastruktury. Poté co subjekt obdrží vyrozumění mu začínají plynout lhůty pro plnění povinností subjektu kritické infrastruktury podle zákona.

Nástroje zákona o kritické infrastruktuře

Zákon přináší různé nástroje pro jeho naplňování. Některé z nich jsou obdobné těm, co již existují ve stávajícím systému ochrany kritické infrastruktury, zatímco jiné jsou zcela nové. Mezi ty stěžejní lze zařadit dokumentaci, opatření k zajištění odolnosti, ověřování spolehlivosti, Portál kritické infrastruktury a hlášení incidentů.

Dokumentace

Dokumentaci lze rozdělit na dvě úrovně, a to národní dokumentace a dokumentace subjektu kritické infrastruktury. Na národní úrovni bude vypracována *Strategie pro posílení odolnosti subjektů kritické infrastruktury* (dále jen „Strategie“) a *Posouzení rizik České republiky* (dále je „Posouzení rizik“). Strategie představí systém zvyšování odolnosti subjektů kritické infrastruktury a strategické cíle v této oblasti. Dále stanoví opatření pro zvýšení odolnosti na národní úrovni. Posouzení rizik poté bude definovat významné hrozby pro kritickou infrastrukturu na území České republiky. Jeho součástí bude mimo jiné i analýza meziodvětvových a přeshraničních dopadů. Dokumentace subjektu kritické infrastruktury zahrnuje *Plán odolnosti kritické infrastruktury*, ve kterém budou mimo jiné stanovena opatření k zajištění odolnosti dotyčného subjektu a principy kontinuity podnikání. Současně bude zpracováno *Posouzení rizik subjektu kritické infrastruktury*, ve kterém dotyčný subjekt identifikuje hrozby pro jeho infrastruktury zajišťující poskytování základní služby.

Opatření k zajištění odolnosti

Subjekty kritické infrastruktury budou za účelem zajištění své odolnosti povinny přijímat technická, bezpečnostní a organizační opatření. Jedná se o opatření sloužící k řízení rizik, pro zajištění kontinuity činností, odezvu na incidenty, fyzickou bezpečnost, k řízení bezpečnosti pracovníků a dodavatelského řetězce.

Ověřování spolehlivosti

Ověřování spolehlivosti bude aplikováno pro vybraný okruh pracovníků a lze jej rozdělit na dvě úrovně. První úrovní je ověření totožnosti a potvrzení trestně právní bezúhonnosti. To bude probíhat standardním systémem výpisu z rejstříku trestů a bude se týkat pracovníků podílejících se na poskytování základní služby, vstupujících do citlivých prostor nebo nakládajících s citlivými informacemi či přistupujících do kontrolních systémů. Ověřování spolehlivosti těchto pracovníků bude oprávněním (nikoliv povinností) subjektu kritické infrastruktury. Druhou úrovní je poté ověřování spolehlivosti v souvislosti s výkonem citlivé činnosti. To se bude týkat manažera kritické infrastruktury, který bude muset být držitelem dokladu o bezpečnostní způsobilosti vydaným Národním bezpečnostním úřadem, případně držitelem osvědčení na stupeň utajení Důvěrné a vyšší. V tomto případě se bude jednat o povinnost subjektu kritické infrastruktury.

Portál kritické infrastruktury

Portál kritické infrastruktury bude novým informačním systémem vyhotoveným pro úkony spojené s aplikací zákona o kritické infrastruktuře. Bude komponentou nově vznikajícího Informačního systému krizového řízení (ISKŘ) a jeho používáním bude docíleno zjednodušení a zefektivnění procesu identifikace subjektů kritické infrastruktury, stejně jako výkonu pravomocí Ministerstva vnitra, věcně příslušných ústředních správních úřadů a České národní banky. V rámci této platformy bude možné sdílet vybrané informace mezi jednotlivými aktéry, tj. gestory a subjekty kritické infrastruktury, stejně jako mezi subjekty kritické infrastruktury nebo gestory navzájem. Mimo to bude Portál kritické infrastruktury sloužit také k hlášení incidentů.

Hlášení incidentů

Za incident bude považována událost, která může významně narušit nebo která významně naruší poskytování základní služby. V případě jeho vzniku zasílá subjekt kritické infrastruktury hlášení s obsahem dle směrnice CER. Pokud není schopen zaslat hlášení ihned, tak předá *prvotní hlášení* (nejpozději do 24 hodin od vzniku incidentu) a následně *závěrečnou zprávu* (nejpozději do jednoho

měsíce od vzniku incidentu). V případě, že incident trvá i po uplynutí lhůty jednoho měsíce, předá subjekt kritické infrastruktury po jejím uplynutí *zprávu o pokroku* a následně po ukončení incidentu *závěrečnou zprávu*. Hlášení bude předáváno skrze Portál kritické infrastruktury, v případě jeho nefunkčnosti náhradním způsobem, a to skrze Národní operační a informační středisko (NOPIS) Ministerstva vnitra – generálního ředitelství Hasičského záchranného sboru České republiky. Informace o incidentu Ministerstvo vnitra neprodleně postupuje konkrétnímu gestorovi odvětví nebo pododvětví základních služeb.

Závěr

Připravovaný zákon reaguje na evropskou směrnici CER, která v systému ochrany kritické infrastruktury reflektuje aktuální bezpečnostní hrozby a celkové bezpečnostní prostředí. V rámci nového pojetí ochrany kritické infrastruktury dojde mimo jiné ke vzniku nových povinností a pravomocí subjektů kritické infrastruktury, jejichž cílem je zvýšit odolnost těchto subjektů vůči stěžejním hrozbám a zajistit tak poskytování zájmových základních služeb, které jsou ze své podstaty nezbytné pro zachování základních funkcí státu, hospodářských činností, bezpečnosti, veřejného zdraví nebo životního prostředí.