Komise pro hodnocení dopadů regulace
Legislativní rada vlády České republiky

V Praze dne 26. listopadu 2014
Č.j.: 15219/2014-LRV

Stanovisko
komise pro hodnocení dopadů regulace

k návrhu

vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

I. Úvod

Touto vyhláškou se stanoví obsah a struktura bezpečnostní dokumentace pro informační systém kritické informační infrastruktury. Vyhláška formuluje i formát pro komunikační systém kritické informační infrastruktury.

Vyhláška stanovuje obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.

Významnou součástí vyhlášky jsou náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor oznámení kontaktních údajů a jeho formu.

Neprovedení navrhované úpravy nové vyhlášky o kybernetické bezpečnosti by znamenalo nenaplnění zákonného zmocnění. Absence vymezení obsahu a rozsahu jednotlivých bezpečnostních opatření by znamenala nedostatečnou míru zabezpečení informačních a komunikačních systémů kritické informační infrastruktury a významných informačních systémů, což by vedlo ke zvýšené míře pravděpodobnosti výskytu kybernetických bezpečnostních incidentů v těchto systémech a s tím spjatým dalším negativním následkům materiální i nemateriální povahy.

II. Připomínky a návrhy změn

Analýza dopadů – RIA byla provedena velmi pozorně a důkladně. Vyhláška má důležitý význam systémový – stanovuje totiž principy vzniku kompetencí

a odpovědností, principy přidělování rolí v systémech zajišťujícím úroveň kybernetické bezpečnosti, proto je důležité, aby byla vyhláška zcela srozumitelná celému systému kybernetické ochrany a nikoliv pouze vybrané skupině právníků. Při čtení vyhlášky narážíme na velké množství prohřešků proti pravidlům jazyka českého a to zejména v oblasti větné stavby. RIA se zabývá věcnou stránkou vyhlášky a formální stránka zde hodnocena není.

Překážkou je stavba dlouhých souvětí. Například, předmět úpravy je formulován jednou větou rozvinutou na šesti řádcích. Vymezení pojmů už vůbec nectí pravidla stavby souvětí a čtenář musí číst pasáž mnohokrát, aby obsahu dobře porozuměl, protože je formulováno větou rozvinutou na jeden a půl stránky. Navíc je interpunkce této věty tak nejasná a špatná, že je tato věta téměř nesrozumitelná. Totéž možno říci o ostatních následujících částech.

Po věcné stránce se jeví vyhláška jako výborný a nezbytný dokument, upravující akční formát pravidel pro systémové přístupy a praktické postupy v oblasti kybernetické bezpečnosti. Nicméně charakteristika rizik a výběr opatření postrádá oporu v potřebném odstupňování rizik. Popis je v tomto ohledu ve vyhlášce poněkud vágní. Tento nedostatek je pak přímo patrný především v paragrafu, který se týká řízení rizik.

Dobře jsou naopak zpracovány scénáře pro řízení aktiv. Ty by pak měly být povinně rozpracovány jednotlivými institucemi státní správy a bezpečnostními složkami.

III. Závěr

Dokument má značný význam pro systémové řešení problémů v oblasti kybernetické bezpečnosti informačních systémů, komunikačních systémů a systémů sdílení a managementu znalostí, nejen ve státní správě. Věcně je vyhláška zpracována s dobrou znalostí problematiky a postihuje dobře řetězce kompetencí a odpovědností. Formátuje pravidla pro přidělování rolí v systému a uvádí základní obecné scénáře pro chování systému při výskytu bezpečnostních incidentů.

Vyhláška však je po jazykové stránce příliš komplikovaná a těžko srozumitelná. Proto Komise RIA doporučuje vyhlášku po formální – jazykové stránce dopracovat k větší srozumitelnosti a doplnit škálu (jednotlivé úrovně) rizik, které se při výskytu kybernetických bezpečnostních incidentů mohou vyskytnout.

Výše uvedené připomínky a doporučení jsou předkladateli sdělovány nad rámec vyjádření ke kvalitě předložené RIA, přesto vzhledem k tomu, že podmiňují samotnou funkčnost a efektivní implementaci vyhlášky v praxi, se jedná o skutečnosti, jejichž dopracování je předpokladem pro doporučení návrhu spolu se závěrečnou zprávou RIA ke schválení.

Vypracoval: Prof. Ing. Petr Moos, CSc.

Prof. Ing. Michal Mejstřík, CSc., v.r.
předseda komise