Legislativní rada vlády České republiky
Komise pro hodnocení dopadů regulace (RIA)

V Praze dne 13. dubna 2012
Č.j.: 328/12

Stanovisko komise pro hodnocení dopadů regulace

k návrhu
věcného záměru zákona o kybernetické bezpečnosti

I. Úvod:

Základním cílem zákona o kybernetické bezpečnosti je zvýšit bezpečnost kybernetického prostoru, nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity při řešení kybernetických bezpečnostních událostí a v této souvislosti zavést do praxe soubor oprávnění a povinností. Nastavením předvídatelného transparentního postupu pro subjekty, které budou zatíženy regulací, spočívajícího v postupných krocích, které mají zajistit detailnější přehled o hrozbách a rizicích, která se vyskytují v kybernetickém prostoru, se zajistí možnost v rychlém sledu reagovat na nové hrozby, které v budoucnu nastanou.

Věcný záměr zákona o kybernetické bezpečnosti navazuje na Bezpečnostní strategii České republiky a definuje záměry České republiky v oblasti informačního prostředí ČR. Navrhovatelé legislativního opatření sledují především ochranu před hrozbami, kterými jsou informační a komunikační systémy vystaveny, a snížení potenciálních škod způsobených v případě útoků na tyto informační a komunikační systémy.

II. Připomínky a návrhy změn:

Na proceduru RIA u předloženého věcného návrhu musíme nahlížet zejména s pohledu efektivity opatření vedoucích k bezpečnosti informačního prostředí instalovaného v rámci ICT. Dopady do ekonomiky i do administrativy z pohledu RIA budou dány především vývojem techniky a nelze je předem přesně specifikovat. Předkladatel vedl potřebné konzultace jak s uživateli, tak s operátory ICT. Závěry těchto konzultací předkladatel zohlednil v textu Věcného záměru. V textu jsou

respektovány připomínky z předběžných konzultací s komisí pro hodnocení dopadů regulace.

Text Věcného záměru zákona o kybernetické bezpečnosti je koncipován převážně jako právní dokument a případné technologické analýzy stávajícího stavu, které by zahrnovaly i problematiku bezpečnostních incidentů ponechává na případná vládní nařízení a směrnice reagující na konkrétní vývoj jednak techniky, ale i charakterů jejího potenciálního zneužití.

Ve věcném záměru je patrná snaha postihnout procesní stránku věci, bez souběžné prezentace předpokládaných hrozeb a orientačního popisu technologické oblasti, která má být chráněna. Za dané situace se jako optimální jeví, aby zákon o kybernetické bezpečnosti upravoval převážně obecný rámec, definoval základní pojmy a aby byla detailnější pozornost věnována úpravám rámce činností národního dohledového pracoviště a charakterizaci jeho činnosti a pravomoci vůči státním sítím a informačním systémům, případně vůči sítím a systémům náležejícím do kritické informační infrastruktury. Otázka kybernetické bezpečnosti se bude řešit postupně a v případě potřeby se záběr regulace bude rozšiřovat, pokud by se regulace ukázala jako nedostatečná.

Předkladatel si je evidentně vědom skutečnosti, že ochrana kybernetického prostoru není nic nového a pro Českou republiku bude výhodné ve větší míře využít zkušeností, mechanismů a postupů, které byly v oblasti kybernetické bezpečnosti nasbírány doma i v zahraničí a které se v praxi osvědčily. Zahraniční zkušenosti ukazují, že je vhodnější, když státní regulace doplňuje existující postupy pouze tam, kde soukromoprávní či akademické působení nedává smysl nebo vůbec není možné. V tomto smyslu lze souhlasit s předkladatelem, že činnost Národního CERT týmu a odpovídajících „nestátních“ subjektů typu CERT bude podléhat regulaci NBÚ jen v omezené a přesně definované míře. Lze souhlasit s tím, že bude založena na spolupráci a na vzájemných formálních i neformálních dohodách, tak jak je obvyklé a osvědčuje se v dnešní praxi a jak je doporučováno mezinárodními organizacemi, působícími na poli ochrany bezpečnosti informačního prostředí.

Předkladatelé, v souladu s požadavky RIA, diskutují i varianty regulace, včetně varianty nulové. Za nulovou variantu je možno považovat pokračování současného stavu, tj. neexistenci specifické zákonné úpravy a absenci centrálního institucionálního zajištění kybernetické bezpečnosti určeným orgánem veřejné moci.

Varianta ochrany informačních systémů nakládajících s utajovanými informacemi je postavena na předpokladu, že právní regulace dopadne pouze na systémy a sítě, které nakládající s utajovanými informacemi. Variantu řešení kybernetické bezpečnosti pouze v rámci regulace orgánů veřejné správy nelze realizovat. Varianta přímé regulace je založena na předpokladu, že stát prostřednictvím svých orgánů přímo kontroluje a reguluje fungování služeb informační společnosti. Ekonomické vyhodnocení uvedených variant je však značně obtížné s ohledem na variace technologií i na procesní stránku administrace součinnosti spolupracujících složek. Předkladatel však předpokládá zvýšené administrativní nároky i na ČTÚ včetně počtu pracovníků, kteří se budou agendou

kybernetické bezpečnosti zabývat. Bude nezbytné vyslovit podmínku, aby plnění funkcí agendy kybernetické bezpečnosti nevedlo na ČTÚ k navýšení počtu pracovníků.

Vybraný postup pro finální návrh představuje odpovědný kompromis v úrovni regulace kyberprostoru v ČR.

III. Závěr:

Předkladatel respektoval připomínky a doporučení z přípravných jednání i z mezirezortního připomínkového řízení. Komise pro hodnocení dopadů regulace **doporučuje Závěrečnou zprávu z hodnocení dopadů regulace schválit a současně navrhuje uložit předkladateli povinnost zpracovat RIA i pro paragrafové znění zákona.** Pozornost je třeba věnovat zejména dopadům týkajících se administrativní náročnosti a nákladům spojených s navýšením počtu administrativních a technických pracovníků pro zajištění agendy.

Vypracoval:
Prof. Ing. Petr Moos, CSc.

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