Komise pro hodnocení dopadů regulace
Legislativní rada vlády České republiky

V Praze dne 7. července 2013
Č.j.: 753/13

Stanovisko
komise pro hodnocení dopadů regulace
k návrhu
zákona o kybernetické bezpečnosti

I. Úvod

Základním cílem návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů je nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity řešení kybernetických bezpečnostních incidentů a zavést do praxe soubor oprávnění a povinností s cílem zvýšit bezpečnost kybernetického prostoru.

Nastavením předvídatelného transparentního postupu pro subjekty, které budou zatíženy zákonnou regulací, se zajistí detailnější přehled o hrozbách a rizicích, jež se vyskytují v kybernetickém prostoru a umožní se v rychlém sledu reagovat na hrozby, které ohrožují bezpečnost informací v informačních systémech nebo bezpečnost služeb a sítí elektronických komunikací.

Pro subjekty, na něž dopadá regulace, jsou v návrhu zákona stanoveny konkrétní povinnosti, prostřednictvím kterých dojde ke zvýšení ochrany jejich informačních systémů, resp. sítí, které provozují. Tyto povinnosti lze vnímat jako v zásadě minimalistické, avšak dostatečně zajišťující dosažení předpokládaného cíle. Pro tzv. běžné uživatele budou vydávána doporučení a bude přistupováno k formulování závěrů nejlepší praxe.

II. Připomínky a návrhy změn

Jak potvrzuje vývoj v mezinárodních ekonomických vztazích, bezpečnost kybernetického prostoru každé země se stává hodnotícím kritériem pro investory

a významně ovlivňuje konkurenceschopnost země. Kvalita a bezpečnost síťových komunikačních služeb určuje kvalitu procesů výroby, distribuce i prodeje na světových trzích. Je pochopitelné, že i Evropská unie reflektuje narůstající potřebu zajištění ochrany kybernetického prostoru. Za tímto účelem byla vypracována Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Současně s tímto dokumentem Evropská komise předložila návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. Návrh směrnice vyžaduje, aby každý členský stát přijal národní strategii pro bezpečnost sítí a informací, jmenoval vnitrostátní orgán odpovědný za bezpečnost sítí a informačních systémů a zřídil skupinu pro reakci na počítačové hrozby, tzv. CERT (Computer emergency response team). Návrh dále požaduje, aby odpovědné vnitrostátní orgány spolupracovaly v rámci sítě umožňující bezpečnou a efektivní spolupráci včetně koordinované výměny informací, odhalování incidentů a reakcí na úrovni EU.

V hodnocení současného stavu je nutno konstatovat, že v České republice se ochrana kybernetického prostoru řeší především prostřednictvím osob v rámci soukromého práva bez regulace, prostřednictvím partikulárních pracovišť. K řešení situace bylo zřízeno Vládou Národní centrum kybernetické bezpečnosti jako součást NBÚ. Předmětné usnesení vlády uložilo řediteli NBÚ vybudovat do konce roku 2015 nejen plně funkční Národní centrum kybernetické bezpečnosti, ale i vládní koordinační místo pro okamžitou reakci na počítačové incidenty, tzv. vládní CERT, který bude součástí Národního centra kybernetické bezpečnosti, tj. součástí NBÚ.

Potřebu efektivní spolupráce mezi vládním CERT, soukromoprávními pracovišti řešící kybernetické útoky a postiženými subjekty potvrdily kybernetické útoky z počátku března letošního roku (4. – 7. 3. 2013). Předmětem těchto útoků byly zpravodajské servery, bankovní a finanční instituce, včetně České národní banky a Pražské burzy cenných papírů a internetové stránky některých mobilních operátů. Útoky směřovaly převážně na osoby soukromého práva, které pravděpodobně nebudou primárně podléhat regulaci návrhu zákona, a dále na informační systémy, z nichž pouze některé budou prvky kritické informační infrastruktury. Rozdílnými informacemi potřebnými k řešení kybernetického bezpečnostního incidentu disponovalo několik různých subjektů. Pro jeho řešení je přitom nezbytná rychlá a efektivní spolupráce, jakož i možnost sdílení potřebných údajů mezi NBÚ, soukromoprávními pracovišti řešícími kybernetické subjekty, subjekty postiženými kybernetickým útokem a poskytovateli služeb elektronických komunikací a subjektů zajišťující sítě elektronických komunikací.

Je zřejmé, že pravidla a vymezení této spolupráce pak musí být s ohledem na postavení NBÚ a charakter údajů předávaných mezi zainteresovanými subjekty upraveny zákonnou normou, která však může být vytvořena v různých variantách.

Hodnocení RIA se zabývá především dopady jednotlivých variant regulatorních opatření. Při zpracování Zákona o kybernetické bezpečnosti bylo uvažováno 5 variant:

V1 - Nulová varianta (bez specifické právní regulace)
V2 - Varianta ochrany informačních systémů nakládajících s utajovanými informacemi
V3 - Varianta ochrany veřejných informačních systémů
V4 - Varianta obecné působnosti a spolupráce s osobami soukromého práva

V5 - Varianta obecné působnosti a přímé regulace

Předkladatel jednotlivé varianty podrobně analyzoval a připravil jejich hodnocení v potřebné šíři. Závěr podrobných rozborů tvoří přehledná tabulka benefitů jednotlivých variant. Po multikriteriálním hodnocení je možno souhlasit s předkladatelem, že nejvýhodnější variantou je varianta 4., založená na působnosti ve spolupráci s osobami soukromého práva. Této variantě věnuje předkladatel i rozsáhlou analýzu administrativních i ekonomických dopadů, včetně dopadů do státního rozpočtu. U ostatních variant je analýza nákladů jen velmi stručně a vágně hodnocena. Navrhujeme, aby RIA k tomuto zákonu byla o upřesnění nákladů alternativních variant doplněna.

III. Závěr

Hodnocení dopadů je v důvodové zprávě k zákonu o kybernetické bezpečnosti velmi precizně a podrobně zpracováno, včetně souvislostí s legislativou EU a nejlepší praxí v EU a ve světě. Po doplnění stručných odhadů nákladů v případě dalších variant doporučujeme předložený návrh postoupit k dalšímu jednání ve Vládě ČR.

Vypracoval: Prof. Ing Petr Moos, CSc.

Prof. Ing. Michal Mejstřík, CSc.
předseda komise