III.

BÍLÁ MÍSTA KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY

Dnem 1. ledna 2015 nabyl účinnosti zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Národní bezpečnostní úřad začal plnit svou roli při určování kritické informační infrastruktury a dále při identifikaci významných informačních systémů ve veřejné správě.

Cílovým stavem implementace zákona o kybernetické bezpečnosti je zajištění bezpečného fungování české informační společnosti, tj. zajištění bezpečné realizace základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací. S tím nedílně souvisí ochrana nedistributivních práv státu, tj. zejména zajištění veřejného zájmu na bezpečném provozu kritické informační infrastruktury a všech významných informačních systémů. Z dosavadních zkušeností Národního bezpečnostního úřadu při implementaci zákona o kybernetické bezpečnosti do praxe vyplynuly poznatky o možných nesouladech současného systému zajištění kybernetické bezpečnosti v České republice s cílovým stavem, tedy o nedostatcích, které by mohly vést k narušení kybernetické bezpečnosti v České republice a tím ohrožení výše uvedeného cíle.

V tomto dokumentu Národní bezpečnostní úřad poukazuje na dosud zjištěná „bílá místa“ v oblasti kybernetické bezpečnosti a předkládá možné návrhy řešení jednotlivých problémů.

1. Důležité sektory mimo soustavu kritické informační infrastruktury

Mimo soustavu kritické informační infrastruktury bez ohledu na splnění průřezových kritérií stanovených nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (dále jen „nařízení“) jsou v současnosti chemický průmysl, zdravotnická zařízení a plynárenství. Skupinu informačních a komunikačních systémů z těchto sektorů nelze určit ani zařadit mezi prvky kritické informační infrastruktury a to z těchto důvodů: chemický průmysl, s výjimkou petrochemického průmyslu, není uveden mezi odvětvovými kritérii v nařízení a není z tohoto důvodu uveden ani v odvětvových kritériích podle nařízení; u zdravotnických zařízení není v nařízení v oblasti stanovení odvětvových kritérií v části VI. Komunikační a informační systémy, odvětvové kritérium, které by umožnilo pokrytí některých informačních systémů ve zdravotnických zařízeních. Oblast plynárenství je v rámci odvětví energetika velmi kvalitně nařízením upravena, prvky jsou však určeny jako evropská kritická infrastruktura. Jako národní kritická infrastruktura nebyly identifikovány ani určeny žádné prvky.

Toto jsou důvody, pro které není možné výše uvedené sektory zahrnout do systému varování a zvládání kybernetických bezpečnostních incidentů a zavést vůči jejich relevantním systémům povinnost minimální úrovně zabezpečení, která je u kritické informační infrastruktury stanovena zákonem o kybernetické bezpečnosti a prováděcí vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Tento stav považujeme za nevyhovující, protože informační nebo komunikační systémy ze shora uvedených důležitých odvětví, mohou způsobit v kybernetickém i reálném prostoru vážné problémy při zajišťování zájmů České republiky.

Jedním z možných způsobů řešení by byla novelizace zákona č. 240/2000 Sb., krizový zákon, a nařízení, což by umožnilo zahrnutí důležitých sektorů mezi prvky kritické infrastruktury. Primárně tak NBÚ tímto materiálem nenavrhuje v současné době přímou novelizaci krizového zákona, zejména proto, že v souvislosti s transpozicí Směrnice Evropského parlamentu a Rady (EU) o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS) do českého právního řádu, která se připravuje, lze novelizací zákona o kybernetické bezpečnosti najít řešení, které umožní přímé určení správců informačních a komunikačních systémů z uvedených oblastí, aniž by tyto osoby byly podřazeny pod krizový zákon.

Na zvážení je i zařazení vodního hospodářství a velkých dopravních staveb (např. velké tunely a řízení rozsáhlých dopravních systémů) do systému varování a zvládání kybernetických bezpečnostních incidentů.

2. Nedostatečná úprava vztahů mezi správci kritické informační infrastruktury či významných informačních systémů a dodavateli informačních a komunikačních technologií a služeb (ICT služeb)

Ze své dosavadní praxe, zejména při výkonu státního dozoru v oblasti kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti Národní bezpečnostní úřad zjistil, že mnozí správci kritické informační infrastruktury a významných informačních ve veřejné správě využívají outsourcing ICT služeb. V této souvislosti je nutno ještě upozornit na to, že v minulosti nebyly stanoveny žádné technické či organizačně bezpečnostní standardy pro zadávání veřejných zakázek v oblasti ICT. V současné době spadá do působnosti zákona o kybernetické bezpečnosti řada systémů a sítí, jejichž správci nemají nad těmito systémy a sítěmi technickou kontrolu. Výsledkem tohoto stavu je, že tito správci nemají technickou nebo právní možnost dostát základním požadavkům zákona o kybernetické bezpečnosti na zabezpečení jimi spravovaných systémů.

Problematickou se jeví zejména úprava přístupu k datům. Zároveň správcům kritické informační infrastruktury a významných informačních systémů chybí institut, kterým by bylo zajištěno dodržení bezpečnostních požadavků ze strany dodavatelů. Tyto problémy již v několika případech zapříčinily ohrožení fungování systémů, kdy např. ukončení dodavatelské smlouvy automaticky neznamenalo předání dat nutných pro provozování daného systému.

K řešení tohoto problému navrhl Národní bezpečnostní úřad, v rámci meziresortního připomínkového řízení k návrhu zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, předkládaný nyní Ministerstvem vnitra (MV-165721/LG-2015) k dalšímu legislativnímu procesu do Legislativní rady vlády, změnu v této oblasti a současně navrhl i související změnu zákona o kybernetické bezpečnosti. Oba zákony přitom obdobným způsobem řeší problematiku vztahu správce a provozovatele, včetně povinnosti provozovatele k předání dat, provozních údajů a dalších informací správci systému.

3. Nedostatek kvalifikovaných pracovníků v oboru kybernetické bezpečnosti

Z kontrolní činnosti Národního bezpečnostního úřadu dále vyplynul poznatek, že v současné době existuje značný nedostatek odborníků z oblasti kybernetické bezpečnosti, a to v zásadě ve všech potřebných oborech (informatika, řízení bezpečnosti informací, právo apod.). V případě veřejné správy je tento problém zesílen tou skutečností, že veřejná správa nemůže potřebné odborníky řádně

ohodnotit. Většina odborníků, kteří ukončili vysokoškolská studia v tomto oboru, přechází do soukromé sféry, která je schopna jim nabídnout vyšší finanční ohodnocení, případně jiné benefity. Nedostatek odborníků a z toho vyplývající zaměstnávání málo kvalifikovaného personálu pak může být považováno za kybernetickou bezpečnostní hrozbu sui generis, kdy neodborné řízení nebo neodborné zásahy do systémů spadajících pod kritickou informační infrastrukturu nebo významné informační systémy může způsobit jejich selhání.

Národní bezpečnostní úřad se sám podílí na vzdělávání osob v této oblasti, a to formou spolupráce s vysokými školami a jejich odbornými pracovišti. Na základě svých zkušeností považuje proto za jeden ze způsobů řešení výše popsaného problému potřebu vypracovat opatření ke zvýšení počtu odborníků na kybernetickou bezpečnost v České republice. Toto opatření by mělo být doplněno zlepšením odměňování klíčových pracovníků v oblasti kybernetické bezpečnosti ve veřejné správě a nastavením takových pracovních podmínek, aby byla schopna vzbudit zájem u uchazečů o takovou odbornou práci a následně byla schopna si takové odborníky i udržet. Nedostatek odborníků nutně povede k tomu, že veřejná správa a její informační systémy se stanou nepřiměřeně závislí na soukromých firmách v oblasti ICT služeb, což může vést ke zvyšování finanční náročnosti jejich správy a tedy ke zvyšování zátěže státního rozpočtu směrem k těmto dodavatelům.

Rada vlády pro informační společnost se zabývala otázkou možnosti odměňování zaměstnanců v oblasti ICT služeb a projednala analýzu porovnání platů v podnikatelské a nepodnikatelské sféře. Analýza vycházela z údajů „Informačního systému o průměrném výdělku“ a „Informačního systému o platu“. Mzda na pracovních místech např. systémového analytika respektive systémového administrátora a správce počítačových sítí za období od r. 2011 do r. 2015 byla v podnikatelské sféře v průměru 1,7krát respektive 1,49krát vyšší než v nepodnikatelské sféře. Rada vlády pro informační společnost ovšem konstatovala, že obdobné rozdíly lze najít i u dalších profesí (právníci, mzdové účetní atd.) a že nelze vytrhovat pouze některé obory služby ze systému a ty zvýhodňovat vůči ostatním, a proto nedoporučila vládě separátní řešení navýšení platů na úseku informačních a komunikačních technologií.

Národní bezpečnostní úřad se však domnívá, že by bylo vhodné toto stanovisko přehodnotit právě s ohledem na eliminaci rizik a zajištění bezpečnosti provozu informačních a komunikačních systémů ve veřejné správě, se zaměřením na oblast kybernetické bezpečnosti.

4. Bezpečnostní rizika vyplývající z některých právních předpisů

Samotnou kybernetickou bezpečnost České republiky může ohrozit i rigidní aplikace zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a to i přes výjimku v ustanovení § 11 odst. 4 písm. f) tohoto zákona, která se týká neposkytování údajů z evidence incidentů podle zákona o kybernetické bezpečnosti. Konkrétně totiž zákon o svobodném přístupu k informacím umožňuje požadovat na povinných osobách všechny ostatní informace v oblasti kybernetické bezpečnosti, a to včetně informací o zabezpečení kritické informační infrastruktury nebo informací o komunikaci mezi Národním bezpečnostním úřadem a příslušnými subjekty, při níž se řeší i aspekty mající dopad na bezpečnost informačních a komunikačních systémů kritické informační infrastruktury. Zpřístupnění takových informací veřejnosti by z bezpečnostních důvodů nemělo být možné už ze samotné podstaty cíle, který se zákonnou regulací v oblasti kybernetické bezpečnosti sleduje.

Jedním z možných řešení by bylo novelizovat zákon č. 106/1999 Sb., ale tento postup nepovažuje Národní bezpečnostní úřad v této době za aktuální. Možným řešením je rozšířit povinnost zachovávat mlčenlivost upravenou zákonem o kybernetické bezpečnosti o vybrané aspekty bezpečnostních opatření, stanovit povinnost mlčenlivosti i správcům a provozovatelům informačních systémů a sítí, kteří plní úkoly podle zákona o kybernetické bezpečnosti (nyní se mlčenlivost týká jen zaměstnanců Národního bezpečnostního úřadu podílejících se na řešení kybernetického útoku a to o údajích z evidence incidentů). Tím by bylo dosaženo efektu vynětí bezpečnostně exponovaných informací z rozsahu zákona č. 106/1999 Sb., aniž by bylo třeba přistoupit k jeho novelizaci.

Rovněž zákon č. 137/2006 Sb., o veřejných zakázkách a ani nově připravovaný zákon o zadávání veřejných zakázek plně nereflektuje požadavky kybernetické bezpečnosti a naopak mohou tyto zákony implicitně vytvářet či posilovat kybernetická bezpečnostní rizika. Příkladem budiž případ, ve kterém měl správně subjekt v rámci zadávacího řízení podle rozhodnutí Úřadu pro ochranu hospodářské soutěže zveřejnit provozní dokumentaci informačního systému, ve které se nachází ty nejcitlivější údaje o zabezpečení informačního systému, přičemž důvodem k tomuto postupu pak mělo být pouze poskytnutí informace o skutečném rozsahu veřejné zakázky uchazečům. Zpřístupnění této dokumentace třetím osobám je však vážným bezpečnostním rizikem pro daný systém. Zákon o veřejných zakázkách také v některých specifických případech neumožňuje vyloučit uchazeče z důvodu existence bezpečnostních rizik na jeho straně.

Zadávací řízení na dodávky ICT nelze z působnosti zákona o veřejných zakázkách vyjmout a priori. Je však nutné legislativně upravit situace, kdy by měla být kybernetická bezpečnost systémů kritické informační infrastruktury nebo významných informačních systémů nadřazena co nejotevřenější hospodářské soutěži tak, aby měli správci kritické informační infrastruktury a významných informačních systémů možnost řídit rizika tak, jak jim přikazuje zákon o kybernetické bezpečnosti. Je také vhodné najít shodu s Ministerstvem pro místní rozvoj a Úřadem pro ochranu hospodářské soutěže, jakým způsobem zajistit požadavky vyplývající ze zákona o kybernetické bezpečnosti při co nejotevřenější hospodářské soutěži.

Další bezpečnostní rizika mohou plynout z aplikace zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Tento zákon nabývá účinnosti dnem 1. července 2016 s výjimkou ustanovení § 6 a 7, které nabývají účinnosti dnem 1. července 2017. V uveřejňovaných smlouvách mohou být uvedeny detaily o použitých technologiích a o způsobu zabezpečení informačních systémů, které mohou potencionálním útočníkům poskytnout informace využitelné k útokům.