Legislativa v České republice

Úvod

Právo chápe kybernetickou bezpečnost v mnohem užším významu, než jak ji musí vnímat podniková praxe. Z hlediska platného práva je totiž nutno odlišovat ochranu kybernetické bezpečnosti státu od dalších forem individuální informační bezpečnosti, tj. od ochrany dat včetně osobních údajů, ochrany obchodního tajemství, ochrany před běžnou trestnou činností zaměřenou k informacím (informační kriminalitou) apod. Bezpečnostní manažer tedy musí pracovat vedle legislativy týkající se přímo kybernetické bezpečnosti též s rozsáhlou trestní, správní a civilní legislativou upravující právní povinnosti, které souvisejí s nejrůznějšími formami získávání, zpracovávání, ukládání a komunikace informací.

Kybernetickou bezpečnost tedy právo vnímá jako ochranu národního kyberprostoru před bezpečnostními hrozbami. Jednotlivé bezpečnostní incidenty samozřejmě mohou dosáhnout takové intenzity, že se negativně projeví v národním měřítku, tj. dojde například k výpadku páteřní sítě. Většina běžně se vyskytujících incidentů však nedosahuje takové závažnosti, aby bylo nutno se jimi na úrovni národní kybernetické bezpečnosti zabývat – s takovými jevy se pak právo vypořádává za užití standardních ochranných institutů trestního, správního a civilního práva. Typickým příkladem může být únik osobních údajů nebo průnik do firemního informačního systému.

Ve vztahu ke kybernetické bezpečnosti v užším smyslu slova (tj., jak ji vnímá platné právo) je nutno v podnikové praxi řešit především problematiku ochrany podnikové informační infrastruktury před útoky zvenčí včetně náležité detekce takových útoků. Stejně důležité pak je z právního hlediska i zamezení tomu, aby podniková informační infrastruktura nebyla zneužita k útoku mimo ni. Za současné právní úpravy lze jen obtížně postihnout podnik za to, že nepoužívá ve vlastní síti náležitá bezpečnostní opatření (jedinou výjimkou je v tomto směru úprava povinností vzhledem k utajovaným informacím). Může však v konkrétních případech dojít k tomu, že bude podnik právně odpovědný za škody, které budou způsobeny jeho zaměstnancům, zákazníkům nebo třetím osobám z důvodu nedostatečného zabezpečení jeho informační infrastruktury. V České republice se podobně jako v ostatních euroatlantických zemích v současné době intenzivně pracuje na specifické právní úpravě národní kybernetické bezpečnosti. Tato úprava bude zahrnovat především nové povinnosti provozovatelů služeb elektronických komunikací aplikovat do jejich sítí certifikované bezpečnostní technologie. Současně dojde v gesci Národního bezpečnostního úřadu k vytvoření vládního dohledového pracoviště, které bude fungovat jako středisko ochrany státní a kritické komunikační infrastruktury a rovněž jako orgán krizového řízení pro případ masivního útoku s celostátním dopadem. Dále bude též upravena činnost národního dohledového pracoviště, jehož úkolem je vyhodnocovat informace o bezpečnostních incidentech ze soukromoprávní informační infrastruktury a koordinovat ochranná opatření s provozovateli konkrétních sítí (národní pracoviště již nyní provizorně funguje, a to na základě memoranda uzavřeného mezi CZ.NIC a Ministerstvem vnitra ČR).

JUDr. Radim POLČÁK, Ph.D.

(vedoucí ústavu práva a technologií při Masarykově univerzitě v Brně)

Ústavní pořádek

2/1993 Sb., Listina základních práv a svobod

110/1998 Sb., o bezpečnosti české republiky

Zákony

240/2000 Sb., o krizovém řízení a změně některých zákonů

365/2000 Sb., o informačních systémech veřejné správy

480/2004 Sb., o některých službách informační společnosti

127/2005 Sb., o elektronických komunikacích

412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Usnesení vlády

677/2007, Akční plán plnění opatření Národní strategie bezpečnosti České republiky

564/2011, o Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015

781/2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast

Vyhlášky

523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor

524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací

525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací

526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), ve znění vyhlášky č. 11/2008 Sb.

527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti)

528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.