Vladimír Smejkal

Jaké povinnosti vyplývají pro orgány veřejné moci ze zákona o kybernetické bezpečnosti?*)

Dnes Vám budu povídat o zákonu o kybernetické bezpečnosti. Jako obvykle, jak se tomu u nás stává, zákon o kybernetické bezpečnosti nabyl účinnosti 1. ledna 2015 a prováděcí předpisy k němu byly vydány někdy mezi Mikulášem a Štědrým dnem 2014, což nebylo úplně ideální. Některé záležitosti se řeší doposud, zejména určování tzv. významných informačních systémů.

Pravdou je, že tento zákon je reakcí na nové hrozby v kybernetickém prostoru, z čehož rovněž vznikají nové povinnosti a odpovědnosti, i v kontextu nabytí účinnosti nového občanského zákoníku. Máme zde totiž řadu konstrukcí, z nichž je generována například objektivní odpovědnost nebo povinnost k náhradě škody, je mezi nimi tedy patrné propojení.

Potřebujeme zákon o kybernetické bezpečnosti?

Zákon o kybernetické bezpečnosti má za cíl stanovit podmínky spolupráce mezi soukromým sektorem a veřejnou správou, těžištěm je ale obrana před kybernetickými bezpečnostními incidenty. Obrana však může být vybudována pouze tak, budou-li nastaveny nějaké povinnosti, oprávnění, a podle zákona se bude vyhlašovat také stav určitého nebezpečí. Je to asi již rok nebo dva, kdy útočníci zaútočili v ČR nejdříve na servery sdělovacích prostředků, potom bank a ve výsledku je přetížili natolik, že tyto servery spadly a lidé se pak nemohli dostat například do svého internetového bankovnictví. Právě proti takovýmto útokům by měly být vytvořeny organizační struktury či postupy, které umožní se ubránit.

Zeptejme se tedy: Potřebujeme takový zákon nebo je to pouze jeden z mnoha zákonů, kterými zejména levicové vlády „zaplevelují" prostor veřejný i soukromý v tomto státě? Zde musím objektivně říci, že ano, že jej potřebujeme. Na konferenci Právní prostor 2015 jsme uvedli hlavní původce kybernetické kriminality. Jedná se vcelku o čtyři zdroje: cizí státy, které organizují kybernetické útoky, teroristé, ale také vaši zaměstnanci a organizovaný zločin. Tyto čtyři okruhy osob mohou mít motivaci, a dnes i prostředky, k tomu, aby zaútočili na vaši organizaci, její informační systém, data, která tam máte uložena, případně na osoby, o jejichž údajích se právě z Vašeho informačního systému dozví.

*) Příspěvek je přepisem vystoupení autora na odborné konferenci Právo ve veřejné správě 2015 (*pozn. red.*).

Každý z těchto typických útočníků může mít jinou motivaci, někdo se bude chtít pomstít svému zaměstnavateli, někdo způsobit chaos, někdo za účelem následného vydírání. Podstatné ale je, že tyto hrozby nepochybně existují.

Oblasti ohrožení

V podstatě existují tři hlavní oblasti ohrožení: prvními jsou **technologické řídicí systémy**. Dnes se nebudeme příliš zabývat tím, když někdo shodí webovou stránku. Tyto útoky jsou poměrně běžné a ostatně při některých typech útoků jim ani nelze dopředu zabránit. Avšak v momentě, kdy útočník začne pacientům na jednotce intenzivní péče zavírat kyslík, je to přeci jen vážnější záležitost. Podobně jako zásah do řízení metra, řízení letového provozu atd.

Je tu i tzv. plíživé nebezpečí, o němž se v současné době velmi hovoří, v němž je možno vidět komerční, obchodní využití, a tím je heslo „**internet věcí**“. Každý přístroj, který máte doma nebo ve firmě, bude připojený k internetu, abyste ho mohli na dálku ovládat, modernizovat stažením nového softwaru apod. To zní sice krásně, ale ve skutečnosti se jedná o extrémní zdroj nebezpečí. Rozhodně netoužím po tom, mít doma špiony či čidla, neboť i lednička se při vhodném útoku může proměnit ve špiona, který bude monitorovat, co se odehrává ve vaší domácnosti. Netoužím po tom, aby mě někdo mohl monitorovat. Už Bradbury popisoval ve svých knihách budoucnost, tzv. chytrý dům, který Vás může jednoho dne zamknout a spustit požár, až tiše uhoříte ve svém zamčeném domě, pakliže jeho ovládání zneužije útočník. Nicméně tzv. internet věcí může spočívat i v tom, že někdo napadne vaše auto a na dálku jej bude ovládat, stejně jako jiné věci, které běžně užíváte.

Třetí oblastí ohrožení jsou **informační útoky**, velice často prováděné prostřednictvím sociálních sítí. I tam se situace mění ještě k horšímu, od informačních útoků, kdy o vás někdo napíše určitou informaci, až po podvody či případy, kdy se osoba prohlásí za vašeho přítele a následně vás požádá o dvacet korun, avšak ve skutečnosti vás, z vašeho vlastního bankovního účtu, okrade o dvě stě tisíc korun. Jelikož je kolem nás stále více a více vytvářena pavučina informační sítě, je možnost zaútočit na jakékoli slabiny každého z nás mnohem větší. Podobně tomu je v oblasti informačních systémů veřejné správy obsahujících citlivé údaje, které v mnoha případech slouží pro výkon veřejné správy v tak kritických oblastech, jež bychom bez informačních technologií nemohli ani vykonávat. To je hlavním důvodem, proč potřebujeme zákon o kybernetické bezpečnosti a mít bezpečné informační systémy. V souladu s tvrzením odborníků a prognostiků je nepochybné, že součástí budoucích válek budou i války kybernetické.

Cíle zákona a vymezení subjektů

Vedle samotného přijetí zákona je však důležité jej také naplnit. Zákon a prováděcí předpisy, společně s dalšími technickými předpisy, jež jsou součástí našeho právního řádu a vytvářejí dobrý podklad pro to, abychom se kybernetickému nebezpečí dokázali postavit. Zákon si klade tyto hlavní cíle: konstituce práv a povinností Národního bezpečnostního úřadu, tedy orgánu státu, jemuž je

svěřena konkrétní pravomoc v oblasti kybernetické bezpečnosti a v jehož rámci bylo vytvořeno tzv. Národní centrum kybernetické bezpečnosti. Národní bezpečnostní úřad tedy vykonává státní správu v oblasti kybernetické bezpečnosti. Zákon dále nastavil mechanismus přenosu informací, neboť vyskytne-li se určité riziko, tj. kybernetický útok, je potřeba tuto hrozbu analyzovat a co nejdříve o ní informovat ty, kdo jsou zařazeni například do kritické infrastruktury státu nebo provozují tzv. významné informační systémy, včetně podání informace o dalším postupu. Dalšími cíli zákona je vybudování systému včasného varování, prevence a osvěty, a dále zavádění opatření jednak preventivních, jednak reaktivních, tj. konkrétních opatření při hrozícím útoku. První část zákona tedy pojednává o prevenci, druhá část pak o případné reakci na kybernetickou hrozbu či útok. Zákon nastavuje způsoby řešení situací v momentě, kdy buď nějaký útok na prvky kritické informační infrastruktury hrozí, nebo již útok nastal.

Zákon rovněž vymezuje jednotlivé subjekty. Jsou jimi Národní bezpečnostní úřad, oblast nazvaná „řízení kybernetické bezpečnosti" a subjekty vyjmenované v § 3 ZKB[1)]. Toto ustanovení je naprosto klíčové, neboť subjekty v něm vyjmenované mají povinnost se tímto zákonem řídit a realizovat tak systém řízení bezpečnosti informací. Osoby neuvedené v § 3 ZKB sice na první pohled nemají povinnost se zákonem řídit, nicméně lze doporučit, aby každý, kdo provozuje určitý informační systém, měl systém řízení kybernetické bezpečnosti nastavený v souladu se zákonem, byť se jedná o záležitost dobrovolnou. Ust. § 3 vyjmenovává tyto osoby: poskytovatelé služeb a provozovatelé služeb elektronických komunikací, orgány nebo osoby zajišťující významné sítě, pokud nejsou správcem komunikačního systému, správce informačního nebo komunikačního systému kritické informační infrastruktury a správce významného informačního systému. Prozatím jsou většinou subjektů uvedených v § 3 písm. c), d) a e) organizační složky státu nebo státní podniky, kterým je tak uložena řada nových povinností.

Kritická infrastruktura

Pokud jde o pojem **kritická infrastruktura**, jedná se v podstatě o vše, co umožňuje, abychom tzv. žili svůj normální život, tj. aby se po zapnutí vypínače rozsvítilo světlo nebo abychom si každý den mohli nakoupit potraviny. V tomto směru považuji za zajímavé zmínit, že dnes se velmi hovoří i o právu na informační sebeurčení. Laicky řečeno to znamená, že pokud se připojím k internetu, můžu se spolehnout na jeho funkčnost. Avšak jednoho dne se může stát, že internet nebude fungovat, stejně jako jiné komunikační sítě, banky, výroba, zdravotnictví, vláda apod. Toto vše, společně se síťovými infrastrukturami, jako jsou elektřina, voda či plyn, vytváří kritickou infrastrukturu, bez které bychom dnes nemohli vůbec existovat.

Jaká je však definice kritické informační infrastruktury? Zde nám pomůže krizový zákon, který definuje jakési prvky kritické infrastruktury, jejichž naru-

[1)] Zákon o kybernetické bezpečnosti.

šení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Prvky kritické infrastruktury – kterými může být cokoliv, např. stavby, zařízení, veřejná infrastruktura – se určují podle průřezových a odvětvových kritérií. Přestože zákonná formulace není příliš jasná, můžeme si to ukázat na rozhodovacím schématu. Pokud platí alespoň jedno z průřezových kritérií, a pokud platí alespoň jedno z odvětvových kritérií, jedná se – bavíme-li se pouze o oblasti informačních a komunikačních technologií – o informační systém kritický. Jedná-li se o informační systém organizační složky státu, je zařazen do seznamu kritické infrastruktury, který schvaluje vláda. Pokud se nejedná o systém organizační složky státu, měla by o jeho určení, podle krizového zákona, rozhodnout jednotlivá ministerstva. V oblasti informačních technologií to však určuje opatřením obecné povahy Národní bezpečnostní úřad, což je speciální úprava oproti zákonu o krizovém řízení, uvedená právě v zákoně o kybernetické bezpečnosti. Pakliže výše uvedené podmínky nejsou splněny, nejedná se o informační systém patřící do kritické infrastruktury, avšak stále se může jednat o tzv. významný informační systém, v němž jsou povinnosti obdobné.

Průřezové kritérium pro učení prvků kritické infrastruktury vyplývá z nařízení vlády a je dáno těmito kritérii: může vést k více než 250 mrtvým, k více než 2,5 tisíci osob s dlouhodobou hospitalizací, jeho ekonomický dopad je vyšší než 0,5% HDP (což činí v současnosti 21 miliard korun), dopad na veřejnost s mezní hodnotou rozsáhlého omezení nezbytných služeb pro každodenní život postihující více než 125 tisíc osob. První dvě varianty zřejmě nemusí být příliš časté, například případ 125 tisíců osob se týká všech krajů, statutárních měst, v rámci Prahy i MČ Prahy 4. Poslední bod se týká konkrétních subjektů vytvářejících strukturu veřejné správy u nás.

Odvětvová kritéria se týkají všech možných oblastí, jakými jsou kupříkladu energetika či potravinářství. Nově sem byla zařazena i oblast kybernetické bezpečnosti. To však neznamená, že v ostatních oblastech se kybernetická bezpečnost neužije. Pokud tedy mám kybernetickou bezpečnost, ale potřebuji k ní elektrickou energii, pak samozřejmě i tato energie se stává součástí kritické infrastruktury. Je vidět, že v oblasti informačních technologií je zahrnuto v podstatě vše kolem nás – pevné sítě, mobilní sítě, rozhlasové a televizní vysílání, satelitní komunikace, poštovní služby, technologické prvky informačních systémů a zejména oblast kybernetické bezpečnosti. Definice posledně jmenované je poněkud odlišná – i kdyby nebyly splněny výše uvedené prvky, pak pokud není informační systém nahraditelný (popřípadě pouze za vynaložení nepřiměřených nákladů nebo za dobu delší než 8 hodin či se jedná o informační systém obsahující údaje o více než 300.000 osobách), hovoříme i v těchto případech o kritické infrastruktuře. Je-li tedy například stanovena povinnost, že určitý informační systém nesmí „vypadnout" na více než 8 hodin, lze snadno vypočítat, že tzv. dostupnost informačního systému (počet hodin za rok, ve kterých musí být informační systém k dispozici), musí být větší než 99,9 %.

Kritická infrastruktura státu

Jako informační systém obsahující osobní údaje lze označit drtivou většinu

informačních systémů veřejné správy, týká se to Prahy, Brna, Ostravy, všech krajů s výjimkou Karlovarského a všech celostátní informačních systémů, jako jsou evidence motorových vozidel, řidičských průkazů atd.

Pokud jde o komunikační infrastrukturu, zde platí to samé, ovšem s další podmínkou, kterou je připojení o kapacitě nejméně 1 GB za sekundu. I to se může týkat řady informačních systémů, i zde je požadavek 99,9 % dostupnosti.

Informační a komunikační systémy však nalezneme i v jiných oblastech kritické infrastruktury státu – integrovaný záchranný systém, radiační monitorování, vše, co souvisí s meteorologickou a hydrologickou situací, a oblast veřejné správy. Nařízení vlády v tomto směru přináší definici, podle níž sem spadá oblast veřejných financí, tj. Ministerstvo financí, Generální finanční ředitelství, Úřad pro zastupování státu ve věcech majetkových apod. Obrovským balíkem informačních systémů je sociální ochrana. Patří sem informační systémy a datové sítě pro sociální zabezpečení, státní sociální podporu a zaměstnanost, tedy vše, co stát provozuje prostřednictvím Úřadu práce. Dále je zde zařazena ostatní státní správa, tj. výkon činnosti ministerstev a jiných ústředních správních úřadů při zajišťování připravenosti na řešení krizových situací, a zpravodajské služby.

Nadto existuje tzv. evropská kritická infrastruktura, což je infrastruktura, jejíž narušení by mělo závažný dopad na další členský stát EU, nejspíš by se jednalo o ropovod, plynovod apod.

Otázkou je, jak vše doopravdy probíhá? Prvky kritické infrastruktury, které provozuje organizační složka státu, jsou určeny vládou. U těch, které nejsou provozovány organizační složkou státu, proběhne určitý proces a výsledek určí Národní bezpečností úřad. My však dnes nejsme schopni dohledat, co do prvků kritické infrastruktury vlastně patří. Vláda sice zveřejnila usnesení, ale odkazuje v něm na dokumenty veřejnosti nepřístupné. NBÚ rovněž neuveřejnil, která opatření obecné povahy vydal, někde ve Věstníku však uvádí, že jejich počet je 40 vyhlášených a 30 připravených. Poslední zmínka na celostátní úrovni je z 25. května, nikde však tyto informace nelze dohledat. Je zde vcelku 406 prvků kritické infrastruktury, určených velmi nejasným způsobem a o značném definičním rozpětí: od „Ministerstva financí“ až po „Celní úřad pro Zlínský kraj“, a přes „Datová infrastruktura Okresní správy sociálního zabezpečení Třebíč“, až po „Stanice Fifejdy HZS Moravskoslezského kraje“. Je to nutné - seznam takto atomizovat?

Do kategorie komunikační infrastruktury patří 45 položek – všechna ministerstva a ústřední správní úřady, Česká národní banka, Generální finanční ředitelství, Generální ředitelství cel, Policejní prezidium, Česká správa sociálního zabezpečení a Evropská agentura.

Významný informační systém

Nezapomínejme však na **významný informační systém**, tj. informační systém spravovaný orgánem veřejné moci, který není kritickou infrastrukturou, ale který při svém narušení může omezit nebo výrazně ohrozit výkon orgánu veřejné moci. Jsou to nejcitlivější místa zákona, neboť některé jsou v prováděcím předpise stanoveny výslovně, některé však přes určitá kritéria. V příloze k vy-

hlášce určující významné informační systémy nalezneme 92 systémů, které nejsou moc překvapivé. Patří sem základní registry, rejstřík trestů, Czech point atd. Překvapivě je zde ale například i aplikace pro testování nových řidičů a dopravců v rámci autoškol. Okruh významných informačních systémů tím ale nekončí. Jsou zde další kritéria, přičemž skutečnost, že určitý subjekt není v uvedeném seznamu, neznamená ještě závěr, že nemá významný informační systém, neboť správce informačního systému si tuto skutečnost musí posoudit sám. Tomu napomohou dopadová a oblastní určující kritéria, přičemž ve vyhlášce je výslovně stanoveno, že významným informačním systémem není informační systém, jehož správcem je obec a při výkonu působnosti obce Hlavní město Praha. Čili obce nikoli, kraje však ano, stejně jako všechny ostatní organizační složky státu. Dalo by se diskutovat o tom, zda je vůbec legální, aby takové ustanovení bylo napsáno ve vyhlášce, podle mého názoru je ústavnost tohoto vymezení velmi diskutabilní, neboť by mělo být vyhrazeno zákonu.

Opět platí jakési schéma, podle něhož můžeme určit provozovatele významného informačního systému. Orgány veřejné moci, s výjimkou obcí, jsou-li uvedeny v příloze, jsou významným informačním systémem. Ty, které v příloze uvedené nejsou, mohou být významným informačním systémem, naplní-li alespoň jedno dopadové oblastní kritérium. Provozovatel pak musí vydat interní správní akt, který určí, že systém je významným informačním systémem a musí tuto skutečnost oznámit Národnímu bezpečnostnímu úřadu.

Pokud jde o kritéria kategorie významného informačního systému, ta jsou kvantifikovaná – jedná se o negativní vliv na fungování orgánu veřejné moci, poskytování služeb veřejnosti, hospodaření nebo na provoz jiného informačního systému, dále bude-li to trvat déle než 3 pracovní dny nebo za vynaložení nepřiměřených nákladů. Posuzování posledně jmenovaného se může zdát dosti komplikované, neboť si lze představit situaci, kdy až po uplynutí několika let orgány činné v trestním řízení „vypočítají“, že určitý subjekt vynaložil náklady nepřiměřené a výsledkem bude obvinění z trestných činů. Proto bych v tomto ohledu všem doporučil vše dokumentovat, zadávat si odborné posudky, byť současně ale nelze říci, že by sám odborný posudek někoho mohl „vyvinit“.

Dalším je dopadové kritérium, dle kterého může narušení prvku kritické infrastruktury vést k obětem na životě a zdraví nebo způsobit ztráty ve výši větší než 5% rozpočtu toho kterého orgánu veřejné moci. Nutno tedy počítat s tím, že informační systém, v jehož rámci je provozován výkon veřejné správy, může být veřejným informačním systémem. Pod oblastní kritéria je ve vyhlášce zařazeno jednoduše všechno. Nalezneme zde oblast vedení správního řízení, ale například i databázi osobních údajů. Některé oblasti jsou bohužel definovány velice nepřesně, například vedení internetových stránek, mezirezortní spolupráce, atd. Totožné lze říci i o krajích, byť seznam je poněkud kratší. Nutno upozornit, že kraje v rámci přenesené působnosti budou muset zkoumat, zda splňují oblastní kritéria a zda splňují dopadová určující kritéria, neboť v takovém případě má jejich informační systém charakter významného informačního systému. Podle sdělení od NBÚ proběhly již dvě vlny určování významného informačního systému, kdy byly určeny např. následující významné informační systémy: ČEPRO, Česká spořitelna, Česká pojišťovna, Komerční banka, Řízení

letového provozu, Státní pokladna, Centrum sdílených služeb, Správa železniční dopravní cesty. Nyní probíhá další vlna, v níž by mělo dojít k určení Pražské plynárenské distribuce, UPC, T-Mobile, O2 a Vodafone. Stále však nejsou a nebyly posouzeny kraje nebo provozovatelé síťových služeb, kteří nemají celostátní dopad. Lze tedy počítat s tím, že tento proces bude stále probíhat.

Sítě elektronických komunikací

Dále jsou významné sítě elektronických komunikací, které nejsou žádným právním předpisem definovány. Podle sdělení NBÚ je odpovědností správce sítě elektronických komunikací zhodnotit, zda jeho síť definici naplňuje či nikoliv s tím, že zajišťuje-li subjekt přímé zahraniční propojení, měl by to daný subjekt vědět. Pakliže zajišťuje propojení kritické informační infrastruktury, čili například provozuje městskou datovou síť, na niž je připojeno něco, co patří do oblasti kritické infrastruktury, je třeba zahájit určitý proces. Dle NBÚ je v tomto případě důležité, aby subjekty kritické infrastruktury o určení informovaly subjekty, které jejich infrastrukturu připojují k jejich kybernetickému prostoru. Pokud tedy nějaký subjekt provozuje datovou síť, může snadno „spadnout" do definice významných sítí elektronických komunikací, protože je na něj připojen někdo, kdo je významným informačním systémem nebo kritickou infrastrukturou.

Stanovené povinnosti

Všechny subjekty podle § 3 ZKB mají stanoveny určité povinnosti. Subjekty vyjmenované v písm. c), d) a e) jsou povinny zavést a provádět bezpečností opatření pro informační systém, komunikační systém nebo významný informační systém a vést o nich bezpečnostní dokumentaci. Zákon zde ukládá povinnost těm, kteří provozují kritickou informační, kritickou komunikační infrastrukturu nebo významný informační systém, zavést a provozovat informační nebo komunikační systém jako bezpečný a mít o tom bezpečnostní dokumentaci. Zajímavostí je zde fakt – a domnívám se, že by se mohlo jednat o nepřímou novelu zákona o veřejných zakázkách – že **orgány a osoby jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro významné nebo kritické informační systémy.** Výslovně je zde napsáno, že zohlednění požadavků vyplývajících z bezpečnostních opatření, v míře nezbytné pro splnění povinnosti podle ZKB, nelze považovat za omezení hospodářské soutěže nebo neodůvodněnou překážku v hospodářské soutěži. Toto ustanovení významným způsobem mění podmínky pro některé veřejné zakázky. S odvoláním na toto ustanovení bude možné vybrat dodavatele, který zajistí spolehlivost funkčnosti informačního systému, utajení informací atd. Soutěže na tzv. nejnižší nabídkovou cenu tak již nadále nebudou možné. Pakliže bude přijat nový zákon o veřejných zakázkách, pak bez ohledu na jeho znění, ukládá ZKB přímo povinnost zohlednit požadavky vyplývající z bezpečnostních opatření. Všechny subjekty uvedené v § 3 písm. b), c), d) a e) ZKB jsou povinny detekovat bezpečnostní události, ohlásit je bezodkladně po jejich detekci, při-

čemž ty, které provozují významnou síť, ohlašují tuto skutečnost provozovateli Národního CERT[2)] (Centrum pro kybernetickou bezpečnost). Další povinností je provádět reaktivní opatření, která nařídí Národní bezpečností úřad, a ochranná opatření, mířící do prevence. Zatímco poskytovatelé sítí a služeb mají povinnost tato opatření provádět pouze v případě kybernetického nebezpečí nebo nouzového stavu, orgánů státu nebo provozovatelů kritické informační a komunikační infrastruktury a významných informačních systémů se to týká vždy, když úřad opatřením obecné povahy „něco" stanoví, například způsob zvýšení ochrany informačních systémů. Přeženu-li to hodně, může opatření obecné povahy znít ve smyslu povinnosti odpojit se jednoduše od internetu.

Osoby, které provozují kritickou infrastrukturu a významné informační systémy měly již dávno oznámit kontaktní údaje a zavést bezpečnostní opatření podle zákona. Tento krok je třeba učinit nejpozději do jednoho roku od okamžiku, kdy někdo řekne, že daný informační nebo komunikační systém je kritická infrastruktura nebo pokud je zařazen jako tzv. významný informační systém. Je zde potom tedy rok na vylepšení či dopracování systému jako systému bezpečného a zajištění veškeré bezpečnostní dokumentace.

Ustanovení § 5 ZKB uvádí, že bezpečností opatření sestávají z organizačních opatření a technických opatření. Prvně jmenované jsou, dalo by se říci, všechno možné. Lze mezi ně podřadit systém řízení bezpečnosti, provádění řízení rizik, definování bezpečnostní politiky, nastavení organizační bezpečnosti, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, zajišťování bezpečnosti lidských zdrojů atd. Každý bod má svůj zásadní význam. Kupříkladu řízení rizik je *alfou omegou* toho, jak vybudovat informační systém bez ohledu na to, jestli je nebo není kriticky významný. Každý správce informačního systému by měl začít řízením rizik, tzn. provést analýzu rizik, definovat případný dopad, následek, škodu, a na základě tohoto pak nastavit bezpečnostní opatření. Jinými slovy, je třeba vědět, proti čemu se má ten který systém bránit, obyčejný antivir v žádném případě není dostatečný.

Kromě organizačních opatření existují i technická opatření, i v tomto případě zákon uvádí v podstatě seznam, z nějž některá opatření jsou kategorií obrovskou, některá jsou nástroji, další jsou aplikační bezpečností, nalezneme zde ale třeba i kryptografické prostředky. Posledně uvedené jsou významnější než se zdá, neboť nikdy nemůžeme předem vědět, kdo a z jakého důvodu se bude zajímat o naše data. Mohou to být orgány činné v trestním řízení, zhrzení zaměstnanci atd. Pokud mohu doporučit, nikdy se nespoléhejte na hesla. Šifrujte, používejte dlouhá přístupová hesla, která nejsou slovem, nýbrž větou. Věta se dobře pamatuje, ale přitom její prolomení hrubou silou je nemožné.

Naštěstí zde máme prováděcí předpis, vyhlášku o kybernetické bezpečnosti, která stanoví, co výše uvedené jednotlivé položky ze ZKB znamenají. Sama o sobě však nestačí. Definuje rámec, který stanoví, co je třeba udělat, avšak je potřeba také zjistit, jak to udělat. To můžeme zjistit tak, že buď si na tuto službu najmeme příslušnou kvalifikovanou osobu, nebo budeme postupovat podle

---

[2)] Computer Emergency Response Team (*pozn. red.*).

technických norem, které stanoví nikoli závazné, ale pouze doporučené postupy. V některých případech se ale prováděcí předpis může výslovně dovolávat na konkrétní normu, pak je použití této normy povinné. Nejčastěji se tak lze setkat s normami ČSN ISO/IEC 27000. Takových norem je celkem pět nebo šest.

Závěrem

Na závěr bych rád doporučil literaturu. Základní tři knihy týkající se informačních systémů veřejné správy a jejich bezpečnosti jsem napsal já nebo jsem byl jejich spoluautorem. Jiné knihy pokrývající tuto problematiku bohužel ani neexistují. Jako první doporučuji knihu „E-government v České republice a jeho právní a technologické aspekty". Druhá kniha se týká řízení rizik organizace a řízení rizik informačního systému, jmenuje se „Řízení rizik ve firmách a jiných organizacích". Konečně třetí knihou je „Kybernetická kriminalita", která vyšla v letošním roce[3)] a zabývá se všemi aspekty zločinu v kybernetickém prostoru.

[3)] V roce 2015 (*pozn. red.*).