29. 1. 2015

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Právní úprava informační bezpečnosti pro orgány veřejné moci

O informační bezpečnosti se v posledních měsících hovoří především v souvislosti s novým zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“). Přímými adresáty ZKB je poměrně úzký okruh tzv. povinných osob. Nicméně bezpečnost informací pořizovaných, uchovávaných, vytvářených a zpracovávaných nejen v počítačových systémech, ale v celém systému řízení, je aktuální prakticky pro každou organizaci. Pro orgány veřejné moci to platí dvojnásob.

Informační bezpečnost je obvykle definována na základě konceptu známého pod zkratkou CIA, která v tomto případě označuje anglická slova Confidentiality, Integrity a Availability. Jde o hodnoty důvěrnosti (ochrana informací před neoprávněným přístupem, tj. stanovení, kdo a za jakých podmínek má k dané informaci přístup), celistvosti či integrity (ochrana informace před neoprávněnou změnou nebo smazáním) a dostupnosti (zajištění trvalé, spolehlivé a bezpečné dostupnosti informace oprávněným osobám). Koncept CIA je obecně přijímaným vymezením obsahu informační bezpečnosti. Akceptuje jej i česká právní praxe a právní řád.

ZKB kybernetickou bezpečnost přímo nedefinuje. Z jeho kontextu však lze dovodit, že kybernetickou bezpečností se míní zajišťování bezpečnosti informací v systémech kybernetického prostoru. Používání obou pojmů, tedy kybernetické a informační bezpečnosti, někdy působí terminologický problém. Informační bezpečnost se obecně vztahuje k zajištění konkrétních informací uložených v konkrétním systému, který může být technické, netechnické nebo i smíšené povahy. Oproti tomu kybernetická bezpečnost obecně směřuje pouze k technickým systémům. Informační bezpečnost je v tomto smyslu pojmem širším.

Právní úprava informační bezpečnosti je vedle zákona o kybernetické bezpečnosti rozprostřena v řadě dalších předpisů. Můžeme uvést např. zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „ZISVS“), zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „ArchSS“) a jiné.

Právní povinnosti na úseku informační bezpečnosti závisí na postavení subjektu vůči danému informačnímu systému, na účelu informačního systému nebo na jeho začlenění do nadřazeného systému, případně na charakteru vazeb k jinému systému. Je nezbytné vždy vycházet z konkrétních faktických okolností. Jestliže daný systém je informačním systémem veřejné správy (§ 3 ZISVS), pak je třeba určit, zda je orgán veřejné moci vůči němu v postavení správce (§ 2 písm. c) ZISVS), resp.

provozovatele (§ 2 písm. d) ZISVS). Podle toho se jeho povinnosti na úseku informační bezpečnosti řídí § 5b ZISVS, resp. § 3 odst. 8 ZISVS. Jde nicméně o strohá ustanovení pouze obecně konstatující povinnost správce, resp. provozovatele informačního systému veřejné správy bezpečnost informací zajišťovat. Není v této souvislosti bez zajímavosti, že pojem bezpečnosti informací je v ZKB i ZISVS upraven v zásadě shodně.

V dalších předpisech je úprava informační bezpečnosti již zaměřena na daný výsek veřejné správy a nevztahuje se pouze k technickým systémům. Takto například ArchSS upravuje v § 68 odst. 4 parametry budovy, ve které je umístěna spisovna nebo správní archiv. Budova musí být chráněná před povodněmi, musí být zpracována požární dokumentace, prostory pro ukládání dokumentů musí být zabezpečeny proti škodlivému působení přírodních vlivů aj. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, upravuje mimo jiné komunikaci orgánů veřejné moci prostřednictvím datových schránek. Orgán veřejné moci je podle příslušných ustanovení § 8 a 9 tohoto zákona povinen řídit přístup k datovým schránkám tak, aby nedocházelo k narušování bezpečnosti informací v systému datových schránek. Obdobných příkladů speciální úpravy informační bezpečnosti bychom našli řadu.

Vzhledem k masivní informatizaci nejen orgánů veřejné moci, ale i celé společnosti, je řízení bezpečnosti informací pro většinu organizací nezbytností Z právního hlediska systém řízení bezpečnosti informací ovlivňuje řadu aspektů řízení, od interních předpisů, přes pracovní smlouvy až po dodavatelské právní vztahy. K řádnému fungování systému řízení bezpečnosti informací je proto vhodný systémový přístup s využitím některého z mezinárodně uznávaných standardů doprovázený právní podporou směřující nejen k naplňování právních povinností, ale také k zajištění právní pozice organizace pro případy narušení informační bezpečnosti.

Mgr. Ing. Robert Kotzian, Ph.D.,
advokátní koncipient

Strelička & Partners, advokátní kancelář, s.r.o.

Veselá 163/12
602 00 Brno

Tel.: +420 515 917 587
e-mail: info@strelicka.cz

Další články:

- Nepravomocné povolení stavby a změna územního plánu
- Letiště a letecké stavby
- Nejvyšší správní soud vymezuje nové hranice zneužití práva u běžných nákladů na reklamu
- Limity dohledu nad výkonem znalecké činnosti
- Stavebníci získávají od roku 2026 silnější pozici v soudních sporech o povolení stavby
- Novela zákona o spotřebitelském úvěru: zásadní regulatorní přelom, který změní finanční trh i praxi poskytovatelů spotřebitelských úvěrů
- Regulace cen taxislužby v roce 2026: co se mění a jaké mají obce možnosti?
- Jaké klíčové změny přináší návrh novely stavebního zákona?
- Nový zákon o zbraních a střelivu
- Novela zákona o pyrotechnice: likvidace profesionálů namísto zmírnění negativních vlivů
- Nový zákon o zbraních – hlavní a vedlejší držitelé a změny v posuzování zdravotní způsobilosti