LEGISLATÍVNE PODMIENKY PRE BEZPEČNOSŤ INFORMÁCIÍ

Pplk. Ing. Peter HOLEŠA
Ministerstvo obrany SR, Sekcia brannej politiky a rozvoja armády

Budovanie informačných systémov nastoľuje nielen otázky technického riešenia prenosu, spracúvania a využívania dát, ale aj ich potrebnej ochrany pred úmyselným alebo neúmyselným narušením. Príprava vstupných údajov býva časovo i finančne náročná a bolo by veľmi nezodpovedné ponechať všetky vytvorené podklady bez náležitého zabezpečenia. Rovnako i samotný proces spracúvania informácií a prípravy výstupov pre rozhodovanie nie je bez rizika prípadnej modifikácie alebo aj možného zneužitia dát.

Účinná ochrana informácií vyžaduje však, popri prijímaní technických opatrení, dobrú legislatívnu základňu. Rovnako ako v iných oblastiach právneho systému, musia byť aj v tejto sfére vymedzené určité pravidlá i s príslušnými sankciami za ich porušenie. Ako príklad, dotýkajúci sa každého občana, môžem uviesť problematiku ochrany osobných údajov, ktoré by sa dali zneužívať rôznymi spôsobmi. O citlivosti tejto otázky svedčí fakt, že hoci už v roku 1992 bol prijatý patričný zákon, začiatkom roku 1998 bolo prerokované a schválené nové znenie zákona NR SR č.52/1998 Z.z. o ochrane osobných údajov v informačných systémoch.

Jedným z rozhodujúcich legislatívnych opatrení každého štátu je prijatie zákona na ochranu utajovaných skutočností. Jeho význam vyplýva už zo samotného názvu, pričom je rozhodujúcim kritériom pre značnú časť spracovávaných informácií a to najmä tých, ktoré je v záujme štátu čo najprísnejšie strážiť. Základné princípy ochrany dát, vymedzené v takomto zákone, sa potom následne využívajú aj pre nižšie úrovne zabezpečenia, napríklad v podnikovej a súkromnej sfére na ochranu „firemného“ tajomstva, vo finančnej sfére apod. V našej republike bol k tejto problematike v roku 1996 prijatý zákon NR SR č.100/1996 Z.z. a v nasledujúcom roku jeho vykonávací predpis: Vyhláška MV SR č.129/1997 Z.z..

1. Zákon NR SR č.100/1996 Z.z.

Ako už bolo povedané, je základnou legislatívnou normou, ktorá definuje štátne a služobné tajomstvo, určuje spôsob jeho ochrany, zodpovednosť osôb, charakterizuje technické prostriedky a podmieňuje ich využívanie a napokon stanovuje sankcie za jeho nedodržiavanie. Z hľadiska bezpečnosti informácií sú dôležité nasledujúce zásady:

- utajované skutočnosti sa musia chrániť pred nepovolanými osobami a prístup k nim je redukovaný výberom osôb
- na ochranu informácií sa využívajú fyzické, mechanické, režimové, technické, programové a šifrové metódy (ich vhodná kombinácia)
- všetky technické prostriedky na vytváranie, spracúvanie, prenos a archivovanie informácií a vecí obsahujúcich utajované skutočnosti sa môžu používať iba tak, aby sa zabezpečila ochrana týchto informácií
- na používanie technických prostriedkov musí byť spracovaný a schválený bezpečnostný projekt.

Pozitívom prijatého zákona je, že vytvoril legislatívnu podstatu pre prácu s utajovanými skutočnosťami a tým aj východiskový rámec pre ochranu informácií. Jeho praktické využívanie prinieslo však niekoľko problémov a to najmä vo vzťahu k toľko diskutovanej aproximácii práva:

- dva stupne označovania utajenia (tajné a prísne tajné) nie sú kompatibilné s používanými štyrmi stupňami v štátoch EÚ a NATO
- podrobnejšie je potrebné vymedziť spôsob výberu osôb, ako aj ich oprávnení pre zoznamovanie sa s utajovanými skutočnosťami
- absencia centrálneho orgánu (bezpečnostného úradu) a jeho právomocí sťažuje výkon niektorých funkcií (certifikácia, štátny dozor, vydávanie potvrdení apod.)
- ukazuje sa nutnosť zavedenia funkcie bezpečnostného riaditeľa v orgánoch štátnej správy, ktorý by bol poverený výkonom povinností vyplývajúcich zo zákona.

2. Vyhláška MV SR č.129/1997 Z.z.

V nadväznosti na prijatý zákon o ochrane utajovaných skutočností bola vydaná vykonávacia vyhláška, ktorá podrobnejšie vymedzuje niektoré ustanovenia zákona a to najmä v oblasti:

- určovania oprávnených osôb
- manipulácie s písomnosťami (evidencia, rozmnožovanie, preprava, ukladanie a vyraďovanie)
- používania a ochrany technických prostriedkov.

Vo vzťahu k bezpečnosti informácií je najviac aktuálna tretia oblasť, ktorá detailnejšie definuje technické prostriedky a ich využívanie, ako aj základné bezpečnostné dokumenty: bezpečnostný zámer, bezpečnostný projekt a bezpečnostné smernice.

Prínosom vykonávacej vyhlášky je, že sa podrobnejšie zaoberá uvedenou problematikou a najmä, že komplexnejšie rieši ochranu informácií spracovávaných technickými prostriedkami. K tomu určuje tieto základné zásady:

- technické prostriedky je možné používať iba v súlade so schváleným bezpečnostným projektom
- ochrana musí byť zabezpečená po celú dobu spracovania informácií
- automatické vedenie kontrolného záznamu o aktivitách užívateľov
- využívanie schválených prostriedkov šifrovej ochrany informácií
- pravidelné vyhodnocovanie a kontrola bezpečnostných opatrení
- určenie zodpovednej osoby.

Rovnako, ako spomínaný zákon, ani vykonávacia vyhláška sa nevyhla určitým nedostatkom, medzi ktoré možno zaradiť:

- nejednoznačné vymedzenie niektorých pojmov (napríklad: „prenos technickými prostriedkami“ z hľadiska použitia prostriedkov šifrovej ochrany informácií)
- absenciu kritérií a požiadaviek na prostriedky tzv. fyzickej bezpečnosti (zámky, mreže, ochranné fólie, elektronické kontrolné a zabezpečovacie systémy, signalizácia apod.)
- protirečivosť analýzy rizík a vo vyhláške uvedenej analýzy kvalitatívneho zabezpečenia ochrany, resp. klasifikovania hlavných hrozieb
- neprepracovanosť opatrení v oblasti personálnej a administratívnej bezpečnosti, ako aj organizačných opatrení.

3. Porovnanie právnych noriem s legislatívou v ČR

V súvislosti s prípravou Českej republiky pre vstup do NATO bolo potrebné prijať celý rad právnych noriem, medzi ktorými boli aj normy z oblasti ochrany utajovaných skutočností. Základný zákon bol po dlhodobejšom procese prijatý až 11.6.1998, ale v krátkom časovom slede po ňom nasledovalo vydanie 8 súvisiacich predpisov:

- o podrobnostiach určovania a označovania stupňa utajenia a práci s utajovanými písomnosťami (vyhláška č.244/1998 Sb.)
- o osobnostnej spôsobilosti (vyhláška č.245/1998 Sb.)
- nariadenie vlády k stanoveniu zoznamov utajovaných skutočností (č.246/1998 Sb.)
- o objektovej bezpečnosti (vyhláška č.258/1998 Sb.)
- o spôsobe a postupe overovania bezpečnostnej spoľahlivosti organizácie (vyhláška č. 263/1998 Sb.)
- o zdravotnej spôsobilosti (vyhláška č.315/1998 Sb.)
- o zaistení technickej bezpečnosti a certifikácii technických prostriedkov (vyhláška č. 12/1999 Sb.)
- o zaistení bezpečnosti informačných systémov a ich certifikácii (vyhláška č.56/1999 Sb.).

Z uvedeného prehľadu je zrejmé, že legislatívne podmienky pre bezpečnosť informácií sú v Českej republike prepracovanejšie a komplexnejšie postihujú celú túto oblasť. Už samotný zákon o utajovaných skutočnostiach (č.148/1998 Sb.), ktorý je porovnateľný s obdobnými zákonmi v EÚ a NATO, vytvoril dobrú právnu základňu a zriadením Národného bezpečnostného úradu delegoval výkon súvisiacich funkcií na tento ústredný správny úrad. Väčšinu vykonávacích vyhlášok pripravil a vydal novozriadený úrad, ktorý má zodpovedajúce kompetencie aj na ich kontrolu a výkon príslušných právomocí.

Prakticky všetky nedostatky z našich právnych noriem, ktoré som uviedol v predchádzajúcej časti článku, sa v zákone a vyhláškach Českej republiky nevyskytujú. Oveľa podrobnejšie je napríklad riešená oblasť výberu osôb, kde je zavedený bezpečnostný dotazník, ktorého súčasťou sú posudok o zdravotnej spôsobilosti, posudok o osobnostnej spôsobilosti, čestné prehlásenie o bezúhonnosti atď. Rovnako v oblasti bezpečnosti informácií sa podrobnejšie definujú základné kritériá, zavádza sa proces certifikácie (v ktorom sa zisťuje zhoda technických prostriedkov, informačných systémov

a kryptografických prostriedkov s bezpečnostnými štandardmi) a bezpečnostnej spoľahlivosti organizácie.

Významným prvkom je taktiež kategorizácia prostredia, v ktorom technické prostriedky spracúvajúce utajované skutočnosti pracujú, čím sa zabezpečujú nielen samotné prostriedky, ale celé objekty a ochrana je komplexnejšia. Samostatná vyhláška rieši zaistenie bezpečnosti informačných systémov, čo je pri súčasnom rozvoji výpočtovej techniky a informatiky vôbec, veľkým prínosom z hľadiska ich ochrany. Táto právna norma detailne rozpracováva požiadavky na celé systémy i rôzne komponenty, bezpečnostné dokumenty, prevádzkové podmienky a certifikáciu informačných systémov.

4. Záver

Z uvedeného porovnania zreteľne vyplýva fakt, že v Českej republike sa venovala sústredenejšia pozornosť príprave legislatívy v oblasti ochrany utajovaných skutočností a bezpečnosti informácií. Ministerstvo vnútra SR, ktoré je ústredným orgánom štátnej správy na ochranu utajovaných skutočností a šifrovú ochranu informácií, si zrejme uvedomilo určité zaostávanie a v priebehu minulého roku pripravovalo novelizáciu zákona NR SR č.100/1996 Z.z. Táto novelizácia však nepredpokladala výraznú zmenu zákona a v podstate sa sústredila iba na zvýšenie počtu stupňov utajenia z dvoch na štyri.

Na rokovaní legislatívnej rady vlády SR v tomto roku bolo rozhodnuté, že pripravovaná novelizácia nepostačuje a je nevyhnutné navrhnúť nové znenie zákona. Príslušní legislatívni odborníci teraz pripravujú prvú pracovnú verziu a je otázkou, pre aké úpravy sa rozhodnú. Domnievam sa, že vhodné príklady nemusia hľadať ďaleko a právne normy Českej republiky v tejto oblasti môžu byť inšpirujúce.