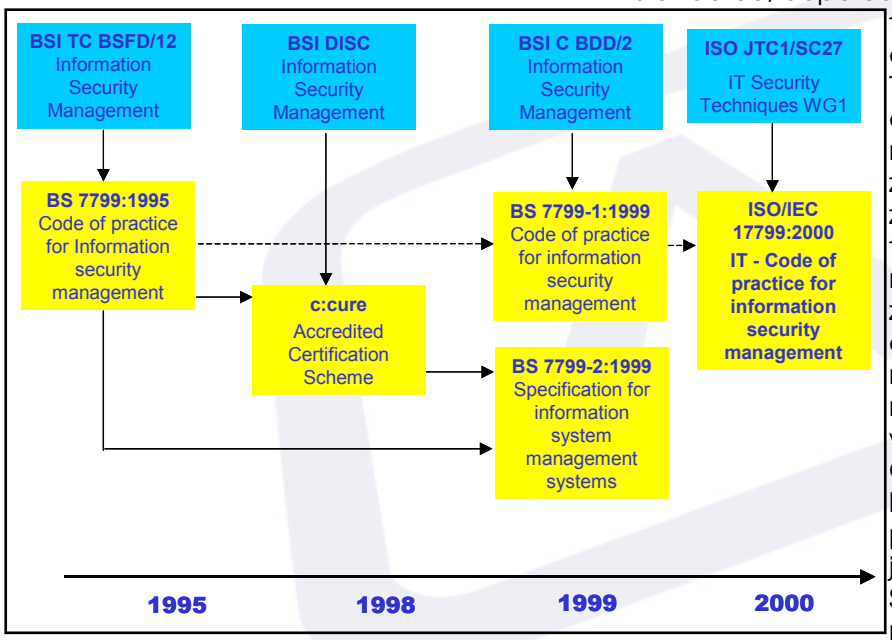
ISO 17799
standard třetího tisíciletí

Ing. Michal Žipaj, vedoucí konzultant společnosti Risk Analysis Consultants, spol. s r. o.

Jedním ze standardů, který zakončil svou cestu mezinárodním uznáním jako normy ISO pod označením ISO/IEC 17799, je britský standard BS 7799 pro řízení bezpečnosti informací (Information Security Management). ISO/IEC 17799:2000 nevznikal jako standard teoretický, ale vyvolala jej praktická potřeba řešit problematiku bezpečnosti informací v organizacích. Jaký má vliv na dění v České republice, jaké může mít přínosy a na jaké problémy mohou narazit organizace při jeho zavádění?

Pojmy a terminologie

Při praktické aplikaci pojmů a terminologie v podmínkách České republiky narážejí organizace na dva aspekty, které před ně stavějí dilema rozhodování.



obr. 1 Vznik a vývoj BS 7799

První aspekt je spojen se způsobem zafixování jednotlivého pojmu v obecné praxi. Jsou možné dvě cesty, kterými se pojem stane prakticky využívaným. První a obecně správná cesta (de jure), je určení pojmu v rámci tvorby nebo přebírání (harmonizace) norem platných v rámci České republiky odpovědnými institucemi. V případě České republiky je to především Český normalizační institut (ČSNI).

Druhý aspekt je spojen s praktickým odborným využitím řady mezinárodně uznávaných zdrojů, standardů, norem a doporučení, které neprošly harmonizací v ČSNI, ale jsou uznávány profesními sdruženími nebo odborníky v dané oblasti (de facto) jako platné.

Oba aspekty spojuje jeden společný faktor. V oblasti bezpečnosti informačních systémů a technologií jsou prakticky všechny pojmy a jejich výklady ve své podstatě překlady a interpretace anglických originálů různých standardů, doporučení, praktik a odborných textů v této oblasti do českého jazyka. Takže základní dilema organizací v České republice jsou spojena zpravidla se zvažováním, zda je určitý pojem nebo termín součástí platné normy; pokud není, tak zda je uznáván odbornou veřejností; když není uznáván, tak zda je možné ho použít podle vlastních zvyklostí atd. Organizace nemá ulehčené rozhodování ani v případě, že určitý pojem je součástí české normy. Stává se totiž, že takový pojem není odbornou veřejností akceptován.

Nedílnou součástí standardu ISO/IEC 17799:2000 je také určitá specifická terminologie, která zahrnuje řadu pojmů v různých zdrojích uváděných různě. Jako příklad

takového pojmu je možno uvést pojem risk analysis, který můžeme nalézt jak v překladu riziková analýza, tak jako analýza rizik. V jednotlivých organizacích, zvláště malých, zpravidla nejsou odborníci na bezpečnostní terminologii a velké organizace, jako například finanční instituce a banky v České republice, často používají svoji vlastní terminologii. Proto je z pohledu organizací výhodné praktické využití standardu ISO/IEC 17799:2000. Z hlediska pojmů a terminologie je možné postupovat následujícími způsoby:

a) využití harmonizovaného překladu ČSNI. Z praktického hlediska je tato varianta vázána na plán harmonizace ČSNI, který je značně nabitý. Na druhé straně není zatím znám způsob harmonizace pro ISO 17799:2000, který může být realizován jak překladem, tak převzetím originálu, což by problematiku pojmů a terminologie přímo neřešilo;

Obr. 2 Struktura BS 7799 - 1

b) využití existujících překladů blízkých standardu.

Řada organizací si již pro různé účely připravila překlady normy BS 7799-1:1999. Výhodou těchto překladů je, že mohou být rychle dostupné, na druhé straně budou obsahovat pojmy a terminologii, jejichž kvalita závisí na tvůrci tohoto překladu;

c) vlastní překlad. Tato varianta přichází v úvahu pro organizace, které nechtějí čekat na ČSNI a z různých důvodů jim nevyhovují dostupné překlady, například proto, že používají vlastní terminologii. Tyto organizace mohou pro zavedení pojmů a terminologie využít například již vydané normy ČSNI nebo podporu specializovaných slovníků.

Protože praktické využití standardu je ovlivněno i takovými aspekty, jako je terminologie, organizace by jí proto měly věnovat adekvátní pozornost.

Bezpečnostní politika a systém řízení bezpečnosti informací

Základem pro řešení bezpečnosti informací organizace je bezpečnostní politika informací(pojem bezpečnostní politika informací koresponduje s pojmem informační bezpečnostní politika), kterou organizace deklaruje svůj vztah k dosahování svých podnikatelských cílů ve vztahu k bezpečnosti zpracování a uchování informací.

Bezpečnostní politika informací podle ISO/IEC 17799:2000 je naprosto klíčový dokument, který je východiskem pro všechny oblasti, které organizace ve vztahu k bezpečnosti informací řeší. U organizací v České republice existují různé pohledy jak na bezpečnostní politiku organizace, tak i na bezpečnostní politiku informací. Je to dáno různými zdroji, které jednotlivé organizace pro jejich tvorbu a zavedení využily. Proto se liší jak strukturou, tak i obsahem.

Skutečně pro všechny organizace

Standard ISO/IEC 17799:2000 při řešení této problematiky mohou využít všechny organizace, bez ohledu na velikost nebo zaměření,

tj. státní instituce a úřady stejně jako komerční podniky; bankovní instituce stejně jako distribuční společnosti. V řadě organizací vzhledem k jejich velikosti a zaměření má bezpečnostní politika víceúrovňovou strukturu, od všeobecné, až po technickou a prováděcí. Standard je možné chápat do značné míry jako technologicky nezávislý, tj. bez vazeb na konkrétní produkty a systémy, ale definující požadavky, které se mají tyto technologie z hlediska bezpečnosti naplnit. Může být použit jako zdroj pro vyšší úrovně (high level) bezpečnostní politiky organizace.

Požadavky na zavedení systému

Při praktickém využití standardu mají organizace rozdílnou výchozí pozici. Řada organizací zatím neřešila problematiku bezpečnosti informací vůbec a nemá proto vytvořeny žádné předpoklady. Na druhé straně existuje řada organizací, jako jsou například finanční instituce (především banky), které již tuto problematiku řeší. Mají bezpečnostní politiku i rámec, ve kterém řízení bezpečnosti informací probíhá. Tato obecná východiska zpravidla vedou k několika variantám využití standardu ISO/IEC 17799:2000, které mohou být v závislosti na stavu organizace postupně využity. Tyto varianty se do určité míry shodují s kroky určenými v BS 7799-2, který definuje po-žadavky na zavedení systému řízení bezpečnosti informaci v organizaci:

a) Organizace nemá zaveden systém řízení bezpečnosti informací a neexistuje žádný schválený dokument pro řešení této problematiky. V tomto případě může organizace využít standardu pro vytvoření dokumentu (řádově 1 až 2 strany), kterým se vedení organizace přihlásí k řešení problematiky bezpečnosti informací, určí cíle a odpovědnosti za řešení této problematiky. Vypracování takového dokumentu vzhledem k jeho rozsahu a obsahu mohou provést přímo pracovníci organizace s případnou konzultační podporou některého z dodavatelů, který je na tuto problematiku orientován. Tím vznikne základní rámec pro další práce v této oblasti.

b) Organizace má představu a řeší určitým způsobem problematiku bezpečnosti informací. V takovém případě může využít standard ke zjištění souladu s obecně doporučovanými praktikami v této oblasti. Posoudit to mohou pracovníci organizace, kteří se seznámili se standardem hlavně pro získání přehledu, které oblasti má organizace vyřešeny a kde je problém. Dobrým vodítkem pro takové posouzení jsou jednotlivé cíle skupin doporučovaných praktik standardu (celkem 36), které obsahují jak vlastní cíl, tak i vysvětlení účelu dané oblasti. Zde může být využita konzultační podpora některého z dodavatelů nebo je možné využít nástrojů, které pomáhají vlastní práci efektivně zvládnout.

c) Organizace má již zaveden vlastní systém řízení bezpečnosti a chce ho uvést do souladu se standardem (např. pro účely certifikace nebo z obchodních důvodů). Tato varianta vyžaduje ze strany organizace znalé pracovníky (odborně erudované a odborně zvládající aplikaci standardu) a neobejde se bez podpory některého z dodavatelů služeb v této oblasti (pro konzultační podporu nebo přímo pro provedení některých činností, jako je např. audit). Důležité je, že pro dosažení výše uvedeného cíle je vhodné dodržet doporučení pro zavádění systému řízení bezpečnosti informací do organizace, protože poskytuje metodické vedení všemi důležitými prováděnými kroky (určení bezpečnostní politiky, rozsahu systému řízení bezpečnosti informací, analýzy rizik, výběru opatření a vytvoření postupu jejich zavedení), čímž zajistí jak efektivnost, tak i kvalitu (a tím i záruky) za prováděné činnosti.

Tyto varianty nejsou vyčerpávající a jejich výčet je ve velké míře závislý hlavně na organizaci a jejím vedení. Důležité je, že standard může pomoci organizacím v České republice prakticky řešit bezpečnost informací bez ohledu na to, v jakém stavu se nacházejí a kam chtějí v této oblasti dospět.

Risk Analysis Consultants s. r. o.
Národní 9, 110 00 Praha 1, CZ
tel: +420 2 2207 5340
fax: +420 2 2422 8273
rac@rac.cz, www.rac.cz