Dokumentace, kontrola a audit bezpečnosti IS/CT
Jak bezpečnost kontrolovat? (2)

Plán realizace bezpečnosti – Jakou cestu zvolit?

Dokument Plán realizace bezpečnosti obsahuje návrh realizace strategických cílů specifikovaných v bezpečnostní politice IS/ICT. Na strategické úrovni představuje rozpracování cílů do posloupnosti kroků tzv. bezpečnostních projektů – tj. projektů, jejichž realizací se zlepší (nebo alespoň nezhorší) bezpečnostní situace organizace. Součástí plánu jsou nejen navrhované projekty, ale také určení priorit jejich realizace s přihlédnutím k zájmům vrcholového vedení organizace, kapacitním, finančním a jiným možnostem organizace. Materiál obsahuje, ve formě projektů, návrh postupu implementace základních funkcí bezpečnosti v organizaci. Celkově bývá materiál pojat tak, že představuje posloupnost jednotlivých kroků, které je nutné provést na všech organizačních úrovních k tomu, aby byla při implementaci dosažena požadovaná úroveň bezpečnosti tak, jak ji vymezila bezpečnostní politika IS/ICT. Součástí plánu realizace bezpečnosti je i plánování reakcí organizace pro případ výjimečných nebo havarijních situací – tzv. zajištění výkonu procesů organizace při havárii nebo výpadku systému (Business Continuity Planning). Další oblastí, kterou musí každá organizace vyřešit, jsou scénáře obnovy zpracování dat při normalizaci činností organizace po havárii nebo výjimečné situaci – tzv. zajištění obnovy zpracování dat (Disaster Recovery Planning).

Dokument je nutné pravidelně aktualizovat a přizpůsobovat průběžně se měnícím podmínkám v organizaci. Obvykle se zhodnocení tohoto dokumentu provádí v pravidelných časových úsecích (obvykle jeden rok) a po přehodnocení a úpravách slouží jako:

- podklad pro úpravy v informační strategii organizace,
- podklad pro změny bezpečnostní politiky IS/ICT organizace,
- jeden z podkladů pro sestavování rozpočtu IS/ICT, resp. rozpočtu organizace,
- podklad pro plánování práce auditu IS/ICT.

S vlastním dokumentem pracují zejména pracovníci z oblasti informačního systému a informační technologie. Běžný pracovník včetně manažerů nepracujících v oblasti IS/ICT s dokumentem jako takovým do styku nepřijde. Zprostředkovaně se k němu dostává pouze v etapě plánování projektů, kdy může specifikovat svoje požadavky na bezpečnost, a potom až v etapě realizace příslušného projektu, kdy se na něm podílí jako řešitel [6].

Příručka bezpečnosti IS/ICT – Jak dosáhnout strategických cílů?

Dokument Příručka bezpečnosti IS/ICT představuje základ rutinního provozu v oblasti bezpečnosti IS/ICT. Zároveň je podrobnějším rozpracování obecných zásad bezpečnosti IS/ICT v organizaci, která je deklarována v bezpečnostní politice IS/ICT organizace. Obsahuje základní požadavky na formulaci bezpečnostních procedur, obsahuje i rámcové vymezení pravomocí a odpovědností mezi organizačními jednotkami resortu. Na tento materiál pak navazují věcně a procesně orientované dokumenty (konkrétní bezpečnostní mechanizmy, vzory, směrnice, dokumentace pro výkon rolí v organizaci apod.). Při zpracovávání Příručky bezpečnosti IS/ICT v organizaci se věnuje převážně pozornost následujícím oblastem:

- vymezení odpovědností a pravomocí,
- vymezení vztahů při zajištění fyzické bezpečnosti včetně vymezení tzv. režimových prostorů a stanovení režimů pro ně,
- vymezení vztahů při zajištění logické bezpečnosti,
- určení způsobu řízení bezpečnosti informační a komunikační technologie,
- zajištění bezpečnosti při provozu lokálních pracovních stanic,
- zajištění bezpečnosti při provozu počítačových sítí v organizaci včetně vzdáleného přístupu do informačního systému,
- zajištění nouzového provozu organizace v oblasti IS/ICT,
- vztahy k ostatním komponentám dokumentace IS/ICT a nejen IS/ICT v organizaci.

Příručka bezpečnosti IS/ICT je podobně jako bezpečností strategie dokument, který není možné sestavit jednou pro vždy. Je nutné s ním pravidelně pracovat, ověřovat jeho aktuálnost a zkoumat jeho relevantnost vzhledem k vývoji informačního systému organizace a vývoji informačních technologií ve světě.

Další dokumenty

Kromě významných strategických a taktických dokumentů, jež jsou v tomto článku stručně zmíněny, se v každé organizaci, která chce efektivně provozovat účinný systém řízení bezpečnosti, vypracovává celá řada dokumentů dalších. Z procesně orientovaných dokumentů jsou to např. popisy bezpečnostních mechanizmů, popisy nastavení parametrů, jak technických, tak i programových prostředků v organizaci, způsoby nastavení komunikace jak uvnitř organizace, tak i mimo organizaci, způsob práce s mobilní výpočetní technikou a její připojování do počítačové sítě organizace apod., z věcně orientovaných dokumentů např. dodatek pracovní smlouvy, kdy se pracovník zavazuje dodržovat zásady práce s výpočetní technikou, postup a procedury auditu IS/ICT apod., z dokumentace orientované na role pak např. příručky správců aplikací, příručka správce systému a v neposlední řadě příručka pro práci uživatele IS/ICT v organizaci. Jejich počet, struktury, působnost a zejména vzájemné vazby mezi nimi jsou natolik závislé od konkrétních podmínek určité organizace, že není prakticky možné je popisovat ad hoc. Pro celkovou složitost vztahů je vhodné na určení koncepce a struktury dokumentace bezpečnosti IS/ICT v podmínkách určité organizace vyhledat pomoc odborníků nebo specializovaných konzultačních firem. Významnou výhodou zde uvedeného modelu dokumentace bezpečnosti IS/ICT je skutečnost, že všechny dokumenty jsou mezi sebou propojeny vazbami, které jsou v praxi realizovány formou odkazů. Propojení dokumentů odstraňuje redundance popisů na různých místech organizace a vytváří tak důležitý předpoklad pro operativní a efektivní řízení systému bezpečnosti IS/ICT.

Literatura

(vybrané tituly)

[5] DOUCEK, P.: Bezpečnost informačních systémů a mezinárodní standardy, In: Pour, J.: Systems Integration 2004, VŠE Praha, 2004, ISBN 80-245-0701-3

[6] DOUCEK, P.: Řízení projektů informačních systémů, Professional Publishing, Praha 2004

Pokračovanie v budúcom čísle.

Petr Doucek

Vysoká škole ekonomická v Praze
Fakulta informatiky a statistiky
nám. W. Churchilla 4, 130 67 Praha 3, ČR
e-mail: doucek@vse.cz
http://fis.vse.cz