Dokumentace, kontrola a audit bezpečnosti IS/CT
Jak bezpečnost kontrolovat? (1)

Petr Doucek

Úvod

Nedílnou součástí vybudování kompletního systému řízení bezpečnosti informačního systému a informačních a komunikačních technologií (IS/ICT) v organizaci je vytvoření dokumentace celého systému. Bez kvalitní, dobře koncepčně navržené a aktuální dokumentace lze jen velmi obtížně celou bezpečnost IS/ICT kontrolovat a řídit. Nejedná se ale jen o vlastní úzce pojatý proces řízení bezpečnosti, ale jeho součástí se v širším slova smyslu stává i kontrola a dozor nad plněním přijatých bezpečnostních norem, pravidel a směrnic, návrh pracovních postupů, povinností a odpovědností a v neposlední řadě i logika a způsoby vedení auditu integrovaného systému řízení včetně auditu bezpečnosti IS/ICT. Dokumentace systému řízení musí splňovat několik základních pravidel, aby ji bylo možné efektivně využívat v praxi. Musí zejména:

- splňovat koncepci určenou bezpečnostní politikou organizace (resp. bezpečnostní politikou IS/ICT),
- být přehledná, jasná a srozumitelná,
- obsahovat všechny skutečnosti, které mají vztah k zajištění bezpečnosti IS/ICT v organizaci,
- být jednouše udržovatelná v aktuálním stavu, včetně možnosti jejího průběžného rozšiřování nebo jejích rychlých změn,
- být použitelná pro podporu výkonu konkrétních rolí v organizaci.

V tom je nezastupitelná úloha dokumentace v organizaci. Pokud budujeme v organizaci informační systém, má většina managerů představu svých očekávání od něj. V případě dokumentace systému řízení bezpečnosti IS/ICT, většina managerů takovou představu vůbec nemá, proto je výhodné pro případy dodávek takového systému nebo jeho dokumentace využít pomoc specializovaných konzultačních a poradenských firem. Vlastní problematika je velmi složitá a obtížně se v ní orientují i profesionálové, proto následující odstavce slouží zejména k základní orientaci v problematice dokumentace zajištění bezpečnosti IS/ICT. Nebudeme se také detailně zabývat jejími širšími souvislostmi a vazbami a to zejména na bezpečnostní politiku celé organizace, její interní legislativní rámec a platné legislativní úpravy na určitém teritoriu.

Dokumentace bezpečnosti – vše musí být někde zaznamenáno

Aby bylo možné efektivně využívat v organizaci nasazený systém bezpečnosti IS/ICT, je nutné všechny jeho složky podrobně zdokumentovat. Dokumentace bezpečnosti IS/ICT se skládá převážně z:

- příruček pro různé organizační jednotky a hierarchické úrovně řízení v organizaci,
- směrnic a nařízení jednotlivých úrovní managementu v organizaci,
- prováděcích předpisů ke směrnicím a nařízením,
- dokumentů obsahujících údaje o nastavení parametrů různých technických zařízení,
- dokumentů obsahujících údaje o nastavení parametrů a atributů základního i aplikačního programového vybavení.

Jednotlivé příručky, nařízení, směrnice a dokumenty, které jsou součástí dokumentace bezpečnosti IS/ICT, vyjadřují přesně na určité role směrované interpretace skutečností, mající vztah k bezpečnosti IS/ICT. Soustava dokumentů musí tvořit jednotný, organický celek, který není v rozporu s nadřízenými dokumenty, směrnicemi a zákony a co nejjednodušším způsobem postihuje celou problematiku bezpečnosti IS/ICT v organizaci. Tedy je na jednu stranu komplexní, ale na druhou stranu v něm buď vůbec nejsou, nebo jsou minimalizovány, redundance v popisech, doporučeních a příkazech. Takový systém dokumentů musí nezbytně mít předem danou strukturu a případně i plán realizace svých jednotlivých složek – dokumentů. Z pohledu zajištění integrity dokumentace a minimalizace redundancí je trochu problém s tím, že dokumentace vlastně vyjadřuje různé pohledy často na stejné jevy bezpečnosti – např. jinak je dokumentována bezpečná práce s aplikačním programovým vybavením pro uživatele, jinak pro jeho správce. Konceptuální schéma dokumentace bezpečnosti je znázorněné na obr. 1. Konceptuální schéma se stává východiskem pro vymezení skutečné struktury dokumentace bezpečnosti v konkrétní organizaci.

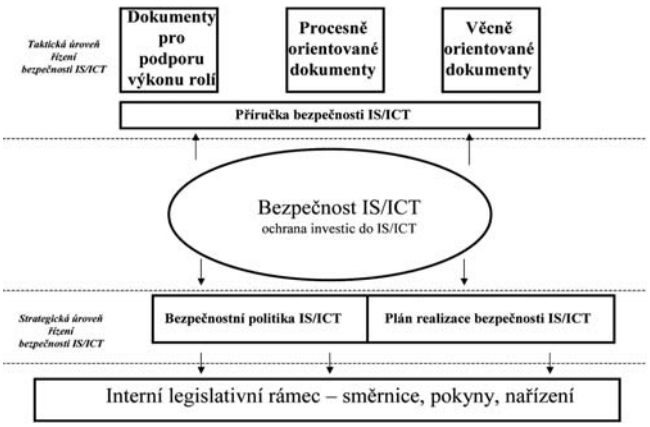
Struktura dokumentace bezpečnosti IS/ICT

Dokumentace bezpečnosti IS/ICT bývá z praktických důvodů obvykle strukturována dvěma způsoby. Prvním z nich je podpora určité hierarchické úrovně řízení. Takový pohled nazýváme pohledem manažerským, který vymezuje úroveň managementu, pro níž jsou určeny jednotlivé dokumenty a která úroveň managementu zodpovídá za jejich dodržování, aktualizaci, údržbu a aktuálnost. Z tohoto pohledu můžeme rozlišit:

- **strategickou úroveň** – Bezpečnostní politika IS/ICT – cíle, záměry a představy o zajištění bezpečnosti IS/ICT; Plán realizace bezpečnosti – stanovení postupu, jak dosáhnout cílů specifikovaných v bezpečnostní politice IS/ICT,
- **taktickou úroveň** – rozpracovaná Bezpečnostní politika IS/ICT do Příručky bezpečnosti IS/ICT; rozpracované popisy procedur a sdružené do ucelených příruček pro jednotlivé role v organizaci, věcně a procesně orientovaná dokumentace, směrnice, dodatky smluv, vzory postupů pro jednání se třetími stranami, vzory pro řešení bezpečnostních incidentů apod.,
- **provozní/operativní úroveň** – detailně rozpracované procedury a bezpečnostní mechanizmy pro jednotlivé konkrétní role, pracoviště nebo části informačního systému.

Začlenění manažerského pohledu do konceptuálního schématu dokumentace bezpečnosti IS/ICT je znázorněno na obr. 1.

Druhým způsobem členění dokumentace je její určení z pohledu podporovaných činností, rolí a cílů v rámci organizace. Toto členění patří zejména na taktickou manažerskou úroveň a je úzce spjato s praktickou realizací dokumentace bezpečnosti IS/ICT



Obr.1 Konceptuální schéma dokumentace bezpečnosti IS/ICT

v organizaci. Kromě strategických dokumentů (Bezpečnostní politika, Plán realizace bezpečnosti) je součástí dokumentace bezpečnosti IS/ICT i celá řada příkazů, směrnic, standardů, doporučení, zvyklostí, procedur a mechanizmů, které jsou určeny pro různé role nebo různá funkční místa v organizaci. Z hlediska, účelu – tj. komu jsou jednotlivé dokumenty určeny, je možné rozlišit jejich orientaci na:

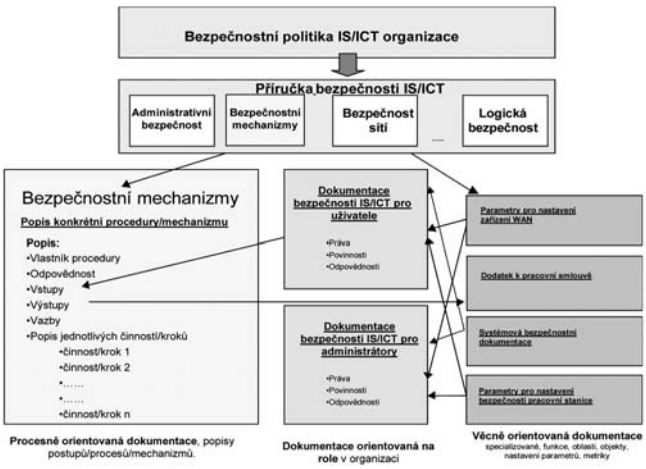
- **procesy** – procesně orientovanou dokumentaci – obsahuje popisy bezpečnostních mechanizmů a procedur v organizaci (např. jak nastavit technické parametry serveru, aby vyhovoval určitým předem stanoveným požadavkům na bezpečnost IS/ICT, jak nastavit parametry určitého základního programového vybavení – databází, operačních systémů apod. tak, aby splňovaly zásadu prokazatelnosti? apod.),
- **role a funkce** – dokumentaci orientovanou na výkon rolí v organizaci – obsahuje informace, které potřebuje znát zaměstnanec, vykonávající určitou roli v organizaci ve vztahu k bezpečnosti IS/ICT (např. příručka bezpečnosti pro uživatele osobního počítače, Příručka pro bezpečnou práci administrátora aplikace apod.),
- **řešení věcných problémů** – věcně orientovanou dokumentaci – obsahuje specializované funkce, oblasti, objekty (např. příručka nebo směrnice pro akceptaci nových částí informačního systému v organizaci, aby nebyla porušena bezpečnost informačního systému jako celku, postup při uzavírání pracovní smlouvy se zaměstnancem, tak aby byla zohledněna odpovědnost zaměstnance za dodržování zásad bezpečnosti IS/ICT – např. formou dodatku pracovní smlouvy o osobní odpovědnosti za využívání prostředků IS/ICT apod.).

Schéma začlenění účelově orientované dokumentace bezpečnosti IS/ICT do strategického rámce řízení a způsob jeho nasazení je uvedeno na obr. 2. Cílem tohto modelu je zajistit:

- jednotný komplexní pohled na bezpečnost IS/ICT – „aby se na něco nezapomnělo“,
- integritu všech dokumentů – pokud možno mít jednu skutečnost v systému dokumentace popsánu jen jednou a na jednom místě a vazby mezi dokumenty jsou řešeny pouze odkazy ne citacemi nebo přejímáním jejich částí do dokumentů jiných,
- jednoduchost údržby a změn – popsané skutečnosti jsou pouze v jednom místě systému, proto s jejich změnou se „změní“ i texty, z nichž byly na změněný text uvedeny odkazy.

Tyto dokumenty bezpečnosti IS/ICT musí tvořit jeden společný harmonický normativní rámec organizace, který navíc musí být v souladu:

- s ostatními interními normami organizace (příkazy, směrnice, vyhlášky, doporučení, návody),
- se standardy bezpečnosti IS/ICT(vnitřními, resortními, národními a mezinárodními),



Obr.2 Schéma dokumentace bezpečnosti IS/ICT – nasazení v praxi

- se zákonnými normami platnými na území příslušného státního útvaru (zákony, vyhláškami uvedenými ve věstnících ministerstev apod.).

Dokumenty

Dokumentace bezpečnosti IS/ICT se skládá z jednotlivých dokumentů, které jsou mezi sebou v rámci organizace propojeny. Základním strategickým dokumentem, z něhož vychází celá koncepce bezpečnosti IS/ICT v organizaci, je Bezpečnostní politika IS/ICT. Z Bezpečnostní politiky IS/ICT organizace pak vycházejí další dva hlavní dokumenty. V oblasti provozní to je Příručka bezpečnosti IS/ICT organizace. V oblasti realizační to je Plán realizace bezpečnosti IS/ICT.

Bezpečnostní politika IS/ICT organizace – strategie

Je základním dokumentem bezpečnosti IS/ICT v organizaci. Vyhlašuje ji vrcholové vedení organizace ve spolupráci s dalšími organizačními jednotkami [4]. Vychází z celkové bezpečnostní politiky organizace, koresponduje s ní, určuje a vymezuje cíle, jichž chce organizace v řízení bezpečnosti IS/ICT dosáhnout a specifikuje požadovanou úroveň bezpečnosti v organizaci. Zároveň představuje výchozí podklad pro zpracování priorit pro realizaci projektů bezpečnosti IS/ICT. Pro rozsáhlejší organizace se někdy navíc ještě vydávají tzv. problémově orientované bezpečnostní politiky. Tyto politiky vymezují cíle v dílčích oblastech bezpečnosti IS/ICT – např. v oblasti personální, administrativní, zajištění fyzické bezpečnosti apod. Dílčí bezpečnostní politiky jsou buď určeny odborným útvarům – např. personální politika útvaru personálnímu – nebo výkonným organizačním jednotkám – např. politika zajištění fyzické bezpečnosti oddělení příjmu zboží. Dílčí politiky se také mohou týkat určitých částí informačního systému. V takovém případě se jim říká systémové bezpečnostní politiky a mohou se týkat například té části informačního systému, která pracuje s daty vyhrazenými nebo důvěrnými dle zákona č. 148/1999 Sb. České republiky, o ochraně utajovaných skutečností.

U celého dokumentu bezpečnostní politiky je nutné pravidelně ověřovat jeho platnost a aktuálnost z pohledu podpory dosahování základních cílů organizace. Dalšími impulsy pro případnou korekci bezpečnostní politiky IS/ICT je vyhodnocení Plánu realizace bezpečnosti IS/ICT, závěry jednotlivých bezpečnostních projektů, zejména jestli se projektem podařilo dosáhnout kýženého cíle, a závěry auditů, a to jak závěry auditů majících vztah bezpečnosti IS/ICT nebo k informačnímu systému organizace, tak i závěry jiných auditů – např. auditu řízení kvality, environmentálního auditu, účetního auditu apod.

Literatura

(vybrané tituly)

[1] ČSN 36 9790 – ČSN/ISO/IEC 17799 – Informační technologie - Soubor postupů pro management bezpečnosti informací

[2] ČSN 36 9790 – ČSN/BS 7799-2 – Systém řízení bezpečnosti informací – Specifikace s návodem pro použití

[3] ČSN 36 9789 – ČSN/ISO/IEC 15408 1-3 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT

[4] DOUCEK, P.: Budování systému řízení bezpečnosti IS/ICT – Jak bezpečnost realizovat?, In: AT&P journal, 02/2005, ISSN 1335-2237

Pokračovanie v budúcom čísle.

Petr Doucek

Vysoká škola 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