MĚŘENÍ EFEKTIVNOSTI SYSTÉMU ŘÍZENÍ BEZPEČNOSTI IS/ICT[1]

Doucek Petr, Nedomová Lea
Katedra systémové analýzy, Fakulta informatiky a statistiky, VŠE v Praze

Abstrakt: *V současné době se stalo velmi aktuální oblastí činnosti všech podnikových informatik řízení svých nákladů. Nasazování do praxe metodik typu COBIT a ITIL, představuje zásadní obrat v řízení podnikové informatiky. Koncepce nasazení referenčních modelů je jejich prostřednictvím dovedena do stádia, kdy jsou přesně popsány jednotlivé procesy podnikové informatiky a kdy už jenom zbývá efektivně měřit jejich výkonnost. Úzkou oblastí měření bezpečnosti podnikových informačních systémů se zabývá tento příspěvek. Poskytuje návrh metrik, jak měřit některé vybrané oblasti bezpečnosti podnikových informačních systémů.*

Abstract: *Today's very actual question seems to be Security assurance of IS/ICT in an organization. Improvement of various methodologies as COBIT and ITIL represents absolutely different approach to informatics management in an organization. General concept of reference models used for IS/ICT management opens new area for investigation of effectiveness and efficiency measurement of any information system and its management. The part of IS/ICT security management also belongs to this general streaming and starting attempts how to measure it at first and then on the base of these measurements to manage it. There are presented several proposals for metrics and their use for effective and efficient IS/ICT security management system.*

Klíčová slova: *bezpečnost IS/ICT, měření, měření efektivnosti systému řízení bezpečnosti IS/ICT*

Key words: *IS/ICT Security, metrics, effectiveness metrics for ISMS (Integrated Security Management System)*

Úvod

V současné době, kdy se prakticky všechny národy světa vydávají na cestu k znalostní společnosti a kdy probíhají změny v ekonomice, které si vynutily změnu názvu ekonomiky na „novou ekonomiku" (Kelly, 2000) nebo také „znalostní ekonomiku" (Drucker, 1968), se neustále větší a větší pozornost obrací k informačním a komunikačním technologiím (IS/ICT). Mezi základní pilíře korektního fungování znalostní společnosti řadíme (materiály WB, 2006):

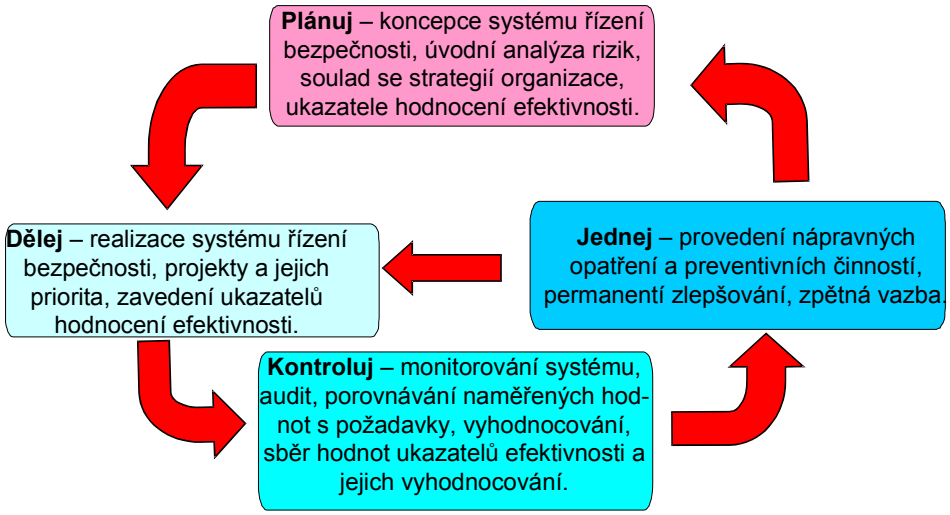
- legislativu, legislativní pravidla,
- profesní a kvalifikační předpoklady lidí – jejich vzdělávání,
- informační a komunikační technologie,
- inovace.

Legislativa je nezbytná, aby vyřešila problémy spojené se zrovnoprávněním dokumentů a dat uložených v IS/ICT s daty v klasické papírové formě. Všechny ostatní oblasti se de facto týkají IS/ICT. Cílem získání profesních a kvalifikačních předpokladů lidí pro práci se znalostmi je minimálně je naučit plnit s IS/ICT efektivně své pracovní i mimopracovní úkoly (např. vztahy se státem – elektronická administrativa, elektronické obchodování, elektronické bankovní služby). Samotné inovace pak představují širokou platformu pro rychlé progresivní změny v ekonomice založené zejména na schopnosti využívat IS/ICT. IS/ICT se tak stávají

[1] Příspěvek byl zpracován za přispění GAČR při řešení úkolu GAČR 201/06/0175 a v rámci projektu česko-slovenské vědeckotechické spolupráce „Informační management – efektivnost/výkonnost podnikových procesů."

kritickým faktorem úspěšnosti ekonomiky nejen firem, ale i celých států a prakticky i celého lidstva.

Zamyslíme-li se nad těmito fakty do důsledků jako někteří filozofové (Pstružina, 2000), (Fukuyama, 1992), dojdeme k závěru, že celá naše ekonomika a společnost je založena na důvěře. Ne ovšem na důvěře v dobré konání lidí, ve vlastní schopnosti, dovednosti a znalosti, ale na důvěře v IS/ICT. IS/ICT se tak pomalu z dobrého sluhy stávají vrtošivým a nevyzpytatelným pánem, který stále víc a víc ovlivňuje naše konání, rozhodování a ve finále určuje i hranici mezi úspěchem a neúspěchem. Aby IS/ICT nebyly oním zmíněným zlým pánem, je nutné je permanentně kontrolovat a starat se o tom aby plnily svůj základní úkol – poskytovaly služby. Aby IS/ICT poskytovaly požadované služby a tím i uspokojovaly požadavky, které na ně uživatelé kladou, je nutné zajistit jejich bezproblémový chod. Pro zajištění chodu IS/ICT je nutné splnit celou řadu požadavků. Jedním z nich je i požadavek na bezpečnost provozovaného IS/ICT. **Základním úkolem a cílem bezpečnosti IS/ICT organizace je zabezpečit a ochránit její aktiva v oblasti IS/ICT – tedy investice, které byly vynaloženy**, aby organizace mohla vykonávat svoje činnosti spojené s hlavními procesy a tím se realizovat na trhu. Z tohoto pohledu je zcela jedno, jestli se jedná o organizaci soukromou, státní, o instituci státní nebo veřejné správy nebo o nadaci. Pro projekty návrhu, zavedení a rozvoje systému řízení bezpečnosti IS/ICT se v současnosti využívá koncept Demingova modelu řízení. (ISO 17799:2005), který je znázorněn na následujícím obrázku Obr. 1.



Obr1.: Aplikace Demingova konceptu na model řízení bezpečnosti IS/ICT

Plánuj - Vymezení a definice systému řízení bezpečnosti a jeho rozsahu, zejména globální bezpečnostní politiky (případně systémových nebo problémově orientovaných bezpečnostních politik), plánů, cílů, jichž chce organizace v řízení bezpečnosti dosáhnout, a jejich přizpůsobení a soulad s celkovými cíli organizace vyjádřenými zejména v podnikatelské a informační strategii. Východiskem je úvodní analýza rizik organizace, z níž vycházejí další kroky. Na základě výsledků analýzy rizik se při návrhu systému řízení bezpečnosti rozhodne, jaká aktiva budou chráněna jakými konkrétními procesy, bezpečnostními funkcemi a mechanismy, tak aby tyto podporovaly realizaci strategických záměrů specifikovaných

bezpečnostní politikou (politikami), plány a cíli organizace. Součástí analýzy je i akceptování rizika vrcholovým vedením organizace. V této etapě životního cyklu se také stanovují metriky, podle nichž bude celková účinnost i účelnost systému řízení bezpečnosti hodnocena.

Dělej - V úvodu této etapy vzniká plán realizace systému řízení bezpečnosti IS/ICT, v němž jsou stanoveny příslušné kroky k realizaci. Jeho součástí je i tzv. plán bezpečnostních projektů, které jsou seřazeny, na základě analýzy rizik, podle priorit a určují způsob realizace požadované úrovně bezpečnosti v organizaci. Realizací jednotlivých projektů se zvyšuje úroveň bezpečnosti IS/ICT až do výše stanovené v etapě „Plánuj". Součástí této etapy je i zavedení mechanizmů pro vyhodnocování účelnosti a účinnosti podnikového informačního systému. V návaznosti na požadavky na bezpečnost se sestavuje potřebná dokumentace, rozdělují se role, odpovědnosti a pravomoci.

Kontroluj - Kontrolní část životního cyklu představuje zejména monitorování provozovaného systému řízení bezpečnosti (např. formou pravidelného sledování, auditu nebo náhodnými kontrolami), dále obsahuje stanovení prvních hodnot sledovaných ukazatelů (nastavení metrik pro řízení systému řízení bezpečnosti), porovnávání zjištěných hodnot s hodnotami požadovanými, vyhodnocování a zpracovávání výsledků, posuzování zjištěných výsledků ve vztahu k záměrům organizace vyjádřeným v bezpečnostní politice, plánům a cílům. Výsledky a zjištění získaná během kontrolní etapy životního cyklu řízení bezpečnosti IS/ICT se stávají podkladem pro poslední etapu životního cyklu – Zlepšování stavu systému řízení bezpečnosti.

Jednej - Zlepšování - provedení nápravných opatření a preventivních činností, založených na základě vyhodnocení výsledků zjištěných v předchozí etapě. Cílem je permanentní zlepšování systému řízení bezpečnosti a zároveň i možnost jeho rychlé inovace v případě potřeby, kdy se např. objeví dříve neočekávané hrozby nebo je nutné chránit jiný druh aktiv (např. organizace začne pracovat s tajnými daty). V etapě „Zlepšování" také probíhá vyhodnocování a měření vlastních dříve stanovených metrik systému řízení bezpečnosti. Zjišťuje se, jsou-li správně nastaveny a jaká je jejich vypovídací schopnost pro řízení systému řízení bezpečnosti.

Struktura měření efektivnosti bezpečnosti IS/ICT

U systému řízení bezpečnosti IS/ICT je nutné stejně jako u všech ostatních systémů řízení měřit jakých výsledků jeho nasazením, provozem a rozvojem dosahujeme. Z tohoto důvodu je nutné při jeho vymezení a definici stanovit ukazatele (metriky), podle nichž budeme tento systém řízení vyhodnocovat. Ukazatele můžeme rozdělit do následujících základních skupin:

- finanční
- personální,
- technické.

Celkový návrh potom vychází z možnosti provázání jednotlivých ukazatelů s mezinárodní normou ČSN ISO/IEC 17799:2005.

Návrh ukazatelů a možnosti měření

Následující tabulka (Tab.1) ukazuje možnosti a návrhy některých vybraných ukazatelů pro měření efektivnosti systému řízení bezpečnosti v organizaci. Tyto ukazatele mohou být pro praktické nasazení v organizaci rozšířeny dle konkrétní potřeby organizace. Rozšíření by se týkalo zejména ukazatelů v oblasti finanční a personální.

Tab. 1: Návrh ukazatelů pro měření efektivnosti systému řízení bezpečnosti.

Finanční		
Finanční náklady na bezpečnost IS/ICT/Finanční náklady na IS/ICT * 100	Procento rozpočtu IS/ICT	Sleduje se v procentech finančního ukazatele
Personální		
Pracovníci pracující v bezpečnosti IS/ICT/Pracovníci v IS/ICT * 100	Procento času vynaložené na IT	Sleduje se v procentech člověkohodin práce
Technické		
Celková dostupnost=min(ARIS(1),…,ARIS(i),..,ARIS(n)) ARIS(i)=(celkový dostupný čas(i)-celkový nedostupný čas(i)/celkový čas(i) ARIS(i): procento dostupnosti i-té části informačního systému	Měří dostupnost služeb IS/ICT v organizaci	Procento času, kdy je celý systém nebo některá ze služeb poskytovaných informatikou organizace nedostupná.
Počet bezpečnostních incidentů způsobených nedostatečným školením/ Počet všech bezpečnostních incidentů * 100	Měří efektivnost bezpečnostních školení.	Sleduje se procentech zjištěných incidentů
Počet subsystémů chráněných před malwarem/počet všech ohrožených subsystémů * 100	Měří ochranu před malwarem.	Sleduje se v procentech ochráněných subsystémů
Počet pracovních stanic s ochranou firewallem/ Počet všech pracovních stanic * 100	Měří rozsah implementace firewallu v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou firewallem/ Počet všech serverů * 100	Měří rozsah implementace firewallu v organizaci.	Sleduje se v procentech ochráněných serverů.
Počet pracovních stanic s ochranou proti spamu/ Počet všech pracovních stanic * 100	Měří rozsah ochrany proti spamu v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou proti spamu/ Počet všech serverů * 100	Měří rozsah ochrany proti spamu v organizaci.	Sleduje se v procentech ochráněných serverů.
Počet pracovních stanic s ochranou proti spywaru/ Počet všech pracovních stanic * 100	Měří rozsah ochrany proti spywaru v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou proti spywaru/ Počet všech serverů * 100	Měří rozsah ochrany proti spywaru v organizaci.	Sleduje se v procentech ochráněných serverů.
Počet pracovních stanic s ochranou proti nežádoucí útokům/ Počet všech pracovních stanic * 100	Měří rozsah ochrany proti nežádoucí útokům v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou proti nežádoucí útokům / Počet všech serverů * 100	Měří rozsah ochrany proti nežádoucí útokům v organizaci.	Sleduje se v procentech ochráněných serverů.
Počet bezpečnostních incidentů v určité oblasti.	Měří počet incidentů v určité oblasti informatiky nebo organizační jednotce.	Udává počet bezpečnostních incidentů v určité oblasti
Počet bezpečnostních incidentů/Počet uživatelů v oblasti	Měří počet bezpečnostních incidentů na jednoho uživatele v oblasti nebo organizační jednotce.	Udává počet bezpečnostních incidentů na jednoho uživatele v určité oblasti
Počet částí informačního systému (subsystémů) s plány na obnovu a se scénáři nouzového provozu/Počet všech subsystémů * 100	Měří zajištění organizace pro případ nenadálého výpadku systému	Sleduje v procentech části systému, které mají scénáře pro nouzový provoz a svoji obnovu
Počet subsystémů podléhajících archivaci /Počet všech subsystémů * 100	Měří zajištění organizace pro případ zničení dat a programového vybavení.	Sleduje v procentech části systému, které jsou v organizaci archivovány.

Závěr

Měření efektivnosti systému řízení bezpečnosti IS/ICT není v naší současné praxi IS/ICT absolutní prioritou, ale lze předpokládat, že ve velmi krátké době, zejména díky nasazování metodik pro snižování nákladů na IS/ICT jako jsou COBIT a ITIL, dojde na obvyklé otázky managementu společností i v oblasti bezpečnosti IS/ICT – Co nám tato oblast přináší? Kolik bezpečnost stojí? Nelze dosáhnout stejného efektu levněji? V tomto textu jsou uvedeny návrhy na některé možnosti měření efektivnosti a účelnosti systému řízení bezpečnosti IS/ICT v organizaci.

Převažují metriky technické – de facto provozní - které byly navrženy pro reálný provoz IS/ICT v organizacích a byly v něm i ověřeny. Metriky finanční a personální jsou zatím ve stavu zrodu a v současné době se jejich rozsáhlejší struktura formuluje. Významnou slabinou všech finančních metrik, je skutečnost, že je velmi obtížné odlišit finance, které jsou použity na bezpečnost IS/ICT nebo které byly použity na vlastní provoz. Proto i vypovídací schopnost finančních metrik je velmi omezená a jejich správnost závisí na odpovědnosti pracovníků, kteří je vykazují. Obdobný problém je i při vyčíslování ztrát způsobených bezpečnostními incidenty. Velmi často jsou vykazovány pouze přímé ztráty např. zničená data a náklady na jejich opětovné pořízení, málokdy ovšem jsou do nákladů bezpečnostního incidentu zahrnuty i náklady na práci bezpečnostních techniků a ostatních pracovníků, kteří za svoji práci dostanou mzdu, ale nikdo ji ani doprovodné náklady již nerozúčtuje k odpovídajícímu bezpečnostnímu incidentu a tedy i do režie konečného spotřebitele.

Literatura

[1] ČSN/ISO/IEC 17799:2005, Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Specifikace s návodem použití.

[2] Doucek, P., Nedomová, L., Klas, J.: Integrated Management System in Information Society. Organizacija, 2006, roč. 39, č. 1, s. 16–27. ISSN 1318-5454

[3] Fukuyama, R.: The Trust: The social Virtuos and the Creation of Prosperity, Hamish Hamiloton Ltd, 1992, London, ISBN 0-241-13376-9

[4] Kelly, K.: New Rules for the New Economy, Ten Radical Strategies for the Connected World. Penguin Group, New York USA, 1998. ISBN 067088111-2

[5] Novotný, O., Doucek, P.: Standardy řízení podnikové informatiky. IT systems, 2006, roč. 8, č. 4, s. 20–21. ISSN 1212-4567

[6] Novotný, O., Doucek, P.: Standardy řízení podnikové informatiky – bezpečnost, IT systems, 2006, roč. 8, č. 6, s. 48–50. ISSN 1212-4567

[7] Pstružina, K: Faust and the Problems in e-economics. Zadov 19.09.2001 – 21.09.2001. In: Hofer, Christian, Chroust, Gerhard (ed.). IDIMT-2001. Linz : Universitätsverlag Rudolf Trauner, 2001, s. 293–300. ISBN 3-85487-272-0.

[8] Vajda, V. Delina, R: Manažment rizika v elektronickom obchode. In: Ekonomie a Management. 1212-3609 : VIII., 2005. s. 127 - 133.

Kontaktní adresa:

Doc. Ing. Petr Doucek, CSc.
Mgr. Lea Nedomová
Katedra systémové analýzy
Fakulta informatiky a statistiky
Vysoká škola ekonomická v Praze
Nám. W. Churchilla 4
130 67 Praha 3
e-mail: Doucek@vse.cz, Nedomova@vse.cz