Budování systému řízení bezpečnosti IS/ICT – Jak bezpečnost realizovat?

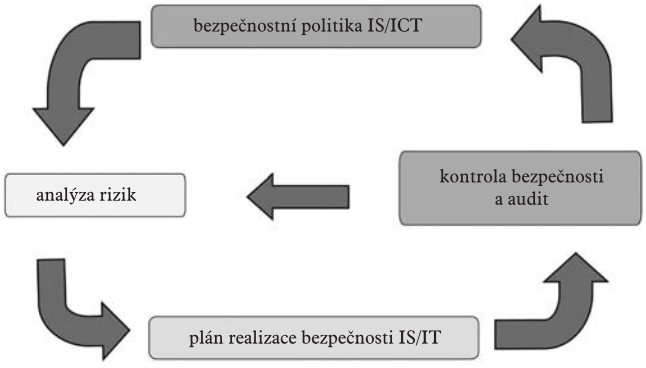
Petr Doucek

Úvod

V minulé části cyklu věnované bezpečnosti informačních systémů ve firmách a organizacích jsme se věnovali teoretickým východiskům pro specifikaci bezpečnosti IS/ICT jako problémové oblasti, vymezili jsme některé základní pojmy a kategorie. Tyto věci by měly být známy prakticky každému manažerovi organizace, bez ohledu na to, na které hierarchické úrovni řízení je sám zařazen nebo kterou věcnou oblast ve firmě řídí. Proč všichni a nejenom odborníci v informatice? Bezpečnost IS/ICT a její řízení je tak dobré nebo tak špatné, jak je dobrý nebo špatný její nejslabší článek. Proto se stala nezbytným prvkem budování jakéhokoli systému řízení bezpečnosti IS/ICT jeho propagace a osvěta. Aby se pracovníci mohli před nějakým nebezpečím nebo hrozbou chránit, musí si ji nejprve uvědomovat a chápat její závažnost. A to je důvod, proč bezpečnost informačního systému není jen otázkou pro několik specialistů informatiků. Bezpečnost, její specifikace, nasazení, integrace do systému řízení, její prosazování, kontrola a audit se musí stát nedílnou součástí mechanizmu řízení na všech úrovních řízení firmy. Za dodržování zásad bezpečnosti IS/ICT, stejně tak jako za dodržování všech ostatních zásad, norem a pravidel ve firmě je zodpovědný liniový vedoucí pracoviště. Z tohoto důvodu musí být se zásadami bezpečnosti sám velmi dobře obeznámen, obdobně jako s procesy, které je nutno dodržovat pro dosažení požadované úrovně bezpečnosti. Proto je nutné v každé organizaci vybudovat systém řízení bezpečnosti tak, aby zahrnoval všechny podstatné složky a aspekty, které mají na bezpečnosti IS/ICT vliv. Podívejme se nyní trochu podrobněji na tento ne příliš jednoduchý proces.

Jak začít?

Základním východiskem pro budování systému bezpečnosti IS/ICT a jejího řízení je podnikatelská strategie, která určuje hranice podnikatelské činnosti firmy. Pokud není organizace podnikatelským subjektem, nahrazuje podnikatelskou strategii účel existence organizace – např. organizace státní nebo veřejné správy, nadace, sdružení apod. Tato hlavní myšlenka účelu existence firmy nebo organizace musí být přenesena do oblasti informačních a komunikačních technologií ve formě informační strategie. Informační strategie obsahuje nebo by měla obsahovat všechny základní zásady budování informačního systému firmy včetně jeho dalšího rozvoje. Tedy její součástí musí být i zásady pro tvorbu, zavedení a realizaci bezpečnosti IS/ICT. Pro sestavení systému



Obr.1 Cyklus řízení bezpečnosti IS/ICT v organizaci

bezpečnosti je nutné provést několik úvodních kroků, jejichž cílem je stanovit výchozí podmínky pro celý systém bezpečnosti. Jsou to následující kroky:

- stanovit konkrétní požadovanou úroveň bezpečnosti v organizaci,
- vytvořit základní globální (firemní) bezpečnostní politiku organizace,
- na jejím základě provést výchozí analýzu rizik.

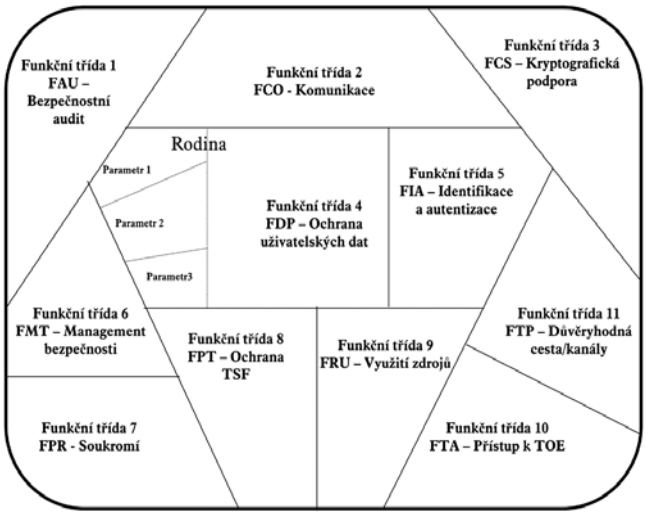
Tím se odstartuje spirálový proces, který je rámcově specifikován modelem PDCA. Proces vybudování a periodické obnovy systému bezpečnosti IS/ICT je znázorněn na obr. 1.

Podívejme se ovšem podrobněji na jednotlivé úvodní kroky budování systému bezpečnosti.

Stanovení konkrétní požadované úrovně bezpečnosti v organizaci – patří mezi nejdůležitější kroky. V něm se vedení firmy rozhoduje o důležitosti a významu konkrétních aktiv IS/ICT pro firmu. Pro stanovení požadované úrovně bezpečnosti je možné použít několik mezinárodně uznávaných zdrojů. V nedávné minulosti byly používány zejména dva:

- TCSEC (Trusted Computer System Evaluation Criteria), která vznikla ve Spojených státech v počátku osmdesátých let (1983) jako součást tzv. duhové série pro hodnocení bezpečnosti informačních systémů pro potřeby Ministerstva obrany USA. Někdy se také nazývá „Oranžová kniha“ (Orange book).
- ITSEC (Information Technology Security Evaluation Criteria), která, inspirována americkým vzorem, vznikla v Evropě na počátku devadesátých let (1992). Tato kritéria hodnocení bezpečnosti informačních systémů vycházejí ovšem i z dalších standardů jednotlivých evropských států – Velké Británie (CESG Memorandum Number 3 – určená pro státní správu a ministerstvo obchodu a průmyslu, DTIEC – určená pro bezpečnost komerčních informačních systémů), Německo – ZSIEC, Francie – SCSSI.

Celkové pojetí obou výše uvedených standardů je velmi podobné. Vychází ze stanovení tzv. bezpečnostních tříd. K tomu, aby mohl být informační systém zařazen do určité třídy bezpečnosti, musí jeho parametry dopovídat parametrům stanoveným standardy pro příslušnou vybranou třídu bezpečnosti. Shoda skutečných hodnot parametrů s hodnotami požadovanými je pak předmětem testování (certifikace) a následné akreditace informačního systému v konkrétních podmínkách. Hlavní nevýhodou celého uvedeného systému hodnocení je požadavek, že informační systém, pokud chce splňovat kritéria pro zařazení do nějaké vyšší třídy bezpečnosti, musí splňovat všechna kritéria tříd nižších. Celý takto inkrementálně (vrstevně) postavený systém řízení bezpečnosti je trochu těžkopádný a obtížně aplikovatelný zejména v organizacích, kde nemají jasnou konzistentní představu o předmětu ochrany a mají zájem význam některých aktiv IS/ICT podtrhnout, ale zároveň nemají dostatek finančních prostředků pro zajištění bezpečnosti všech aktiv rovnoměrně. Pojetí s aplikací tříd vyhovuje více řízení bezpečnosti v podmínkách státní správy nebo vojenských a polovojenských organizacích než nasazení v podnikatelské sféře. Z tohoto důvodu vznikl ke konci minulého století nový systém hodnocení bezpečnosti tzv. Common Criteria (ČSN ISO/IEC 15408 1-3). Tento systém je založen na zcela jiném



Obr.2 Schéma struktury hodnocení bezpečnosti IS/ICT dle ČSN ISO/IEC 15408 1-3

pojetí. Úroveň bezpečnosti je specifikována jedenácti **funkčními třídami** (třídou je v tomto pojetí je myšlena určitá tématicky a obsahově příbuzná množina parametrů) bezpečnosti, které se dále dělí na rodiny a ty se pak skládají z jednotlivých parametrů. Pro každý parametr si může uživatel zvolit tři úrovně intenzity sledování – základní rozšířený a detailní. Schéma systému Common Criteria včetně názvu funkčních tříd je uvedeno na obr. 2.

Výhody takto postaveného systému hodnocení bezpečnosti IS/ICT pro uživatele spočívá v možnosti uživatele přesně specifikovat, která aktiva chce chránit a také s jakou silou ochrany. Proto je tento systém velmi vhodný pro komerční organizace, které si tak mohou přesně určit, co chtějí chránit a naopak, která aktiva budou ohrožena vyššími riziky. Vztahy mezi výše uvedenými standardy jsou podrobněji rozvedeny např. v [5].

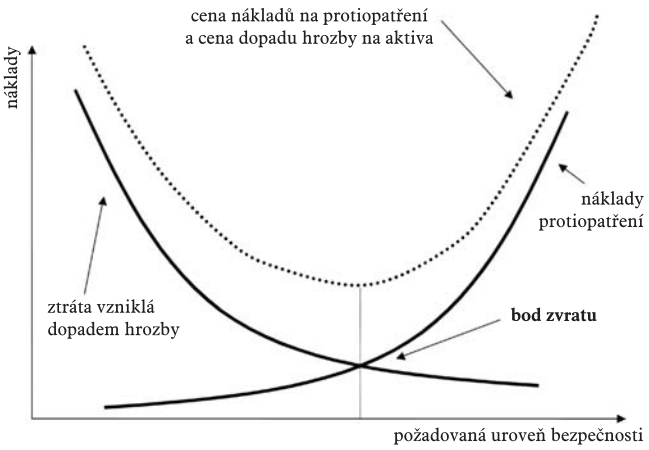
Vytvoření bezpečnostní politiky organizace. Po ujasnění si, jaká aktiva chce organizace chránit a s jakou intenzitou, je nutné, aby vedení organizace oficiálně deklarovalo svůj zájem na ochraně aktiv IS/ICT – **Jaké jsou cíle organizace v oblasti bezpečnosti a jak jich bude dosaženo.** K tomuto slouží sestavení a zejména vyhlášení bezpečnostní politiky organizace. Bezpečnostní politika je strategický deklaratorní dokument, který vyhlašuje vrcholové vedení organizace a v němž jsou stanoveny strategické cíle, způsob jejich dosažení a nástroje bezpečnosti IS/ICT. Samotná definice cílů bezpečnosti, stejně jako další návazné kroky – tvorba strategie a politiky bezpečnosti IS/ICT, však nestojí samy o sobě ve vzduchoprázdnu. Mají vazby na obecnější roviny, takže v ideálním případě bezpečnost IS/ICT v záměru i ve skutečnosti podporuje celkovou bezpečnost organizace, která dále přispívá k naplnění hlavních cílů organizace stanovených podnikatelskou strategií. Vzhledem k tomu, že budování bezpečnosti IS/ICT je permanentní proces, je nutné bezpečnostní politiku v pravidelných časových intervalech přehodnocovat a aktualizovat. Za východiska pro změny v bezpečnostní politice organizace jsou obvykle považovány závěry analýzy rizik, výsledky monitorování, vyhodnocování bezpečnostních incidentů a závěry kontrolních a auditorských zpráv.

Provedení analýzy rizik. Je prvním výkonným krokem při budování systému řízení bezpečnosti IS/ICT. Předmětem analýzy jsou identifikované hrozby, které aktuálně hrozí aktivům IS/ICT. Účinnost výchozí analýzy rizik velmi závisí a zkušenostech pracovního týmu, který takovou analýzu provádí, a také na komplexnosti podkladů, které jsou týmu poskytnuty jako vstupy od vedení organizace. Analýza bezpečnostních rizik a její řízení představuje základní nástroj v rukou vrcholového vedení organizace k ochraně investic vynaložených do informačních systémů a tím i do podpory hlavních procesů organizace. Vlastní provedení analýzy rizik je možné rozlišit podle podrobnosti a hloubky přístupů k řešení:

- nedělat nic,
- neformální přístup – analýza rizik se provádí živelně bez dokumentace přesných postupů,
- základní přístup – postupy jsou rámcově zdokumentovány organizace má celkovou koncepci a vizi řešení bezpečnosti IS/ICT,
- detailní přístup – všechna rizika jsou analyzována podrobně podle předem definované a dodržované metodiky,
- přístup kombinovaný – některá rizika jsou analyzována podrobně, některá jsou případně při analýze i opominuta.

Varianta „nedělat nic“, a tedy akceptovat rizika neznámého rozsahu a síly, je sice také možná, s moderním přístupem k řízení organizace má však málo společného, leč … přežití není povinné. To však neznamená, že nemůže být v určitém časovém úseku nejefektivnější neimplementovat žádná ochranná protiopatření. V takovém případě by si mělo být vedení organizace vědomé, že se tím automaticky rozhodlo příslušná rizika plně akceptovat. Základní východiska, doporučení a postupy pro provedení analýzy rizik jsou uvedeny v ČSN ISO/IEC 13335 1-5. Na základě analýzy rizik je pak možné specifikovat příslušná protiopatření vzhledem k identifikovaným hrozbám. Protiopatření na ochranu aktiv a jejich výběr je součástí realizace bezpečnostní politiky organizace. Při jejich výběru hraje obvykle také roli ekonomická stránka věci. Tou je většinou úvaha spojená se zjištěnou hodnotou aktiva a výší nákladů, které musí být na jeho ochranu vynaloženy, při dodržení určité požadované úrovně bezpečnosti. Ekonomický aspekt je v praxi realizován oceněním jednotlivých aktiv – jejich hodnotou, pro vrcholové vedení organizace. Oceňování aktiv není záležitostí nijak jednoduchou, neboť informační systém organizace může ovlivňovat i její nehmotná aktiva typu know-how organizace, její konkurenční výhodu na trhu, good-will – její dobrou pověst apod. Radu, jak taková nehmotná aktiva oceňovat, je velmi obtížné dávat, ale většinou jejich ocenění závisí na dohodě odpovědných pracovníků a managerů organizace. Ovšem ani oceňování hmotných aktiv není jednoduché a je vhodné a by se na této práci podílelo více odpovědných managerů organizace, nejlépe z rozdílných organizačních jednotek, neboť často se stává, že některé aktivum má jinou hodnotu pro vrcholové vedení organizace a jinou pro vedení některé organizační jednotky nebo výkonné pracovníky. Ocenění aktiv bývá v praxi východiskem pro stanovení maximálních nákladů na realizaci protiopatření na jejich ochranu. Vztahy mezi hodnotou aktiva, resp. mezi ztrátou vzniklou pro případ jeho zničení nebo poškození a náklady na realizaci ochrany aktiva formou protiopatření jsou uvedeny na obr. 3.

Přestože jsou pro vztahy pro ocenění dopadu hrozby a ocenění nákladů na protiopatření dány různými, praxí prověřenými meto-



Obr.3 Ekonomické hranice realizace protiopatření

dami, finální rozhodnutí o volbě protiopatření a tím i o jeho finanční náročnosti zůstane vždy na odpovědných managerech.

Po ukončení iniciačních kroků v budování bezpečnosti IS/ICT jsou v organizaci dány předpoklady pro efektivní vybudování jejího celého systému.

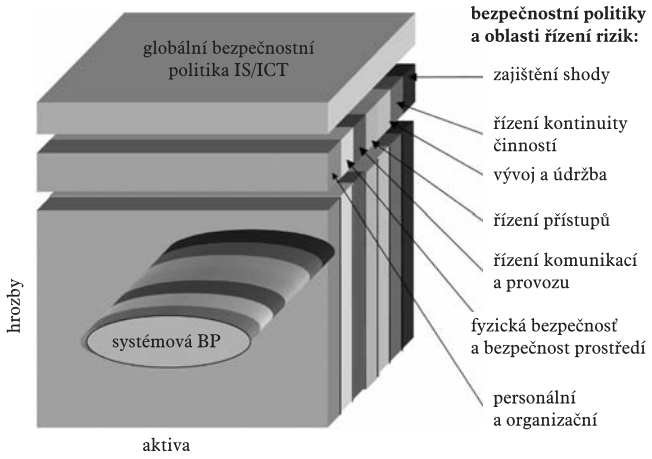
Jak vybudovat?

Úvodní kroky daly organizaci bezpečnostní politiku IS/ICT, kterou vyhlásilo vrcholové vedení firmy, a přehled potenciálních rizik. Na dosažené výsledky je nutné navázat dalším snažením spojeným již s vybudováním systému řízení bezpečnosti. Systémem řízení bezpečnosti myslíme zejména vytvoření a zavedení:

- organizačních struktur zabývajících se a prosazující bezpečnost IS/ICT,
- dokumentace bezpečnosti včetně interního legislativního rámce (směrnice a interní příkazy),
- systému kontroly a auditu bezpečnosti.

Za základ pro vybudování systému řízení bezpečnosti byl přijat původní národní standard Velké Británie – British Standard 7799. Přesněji řečeno, byla převzata jeho první část, jako norma ISO/IEC 17799. V ní jsou také uvedeny všechny základní zásady a doporučení pro budování systému řízení bezpečnosti informačního systému z manažerského pohledu. Struktura standardu je uvedena na obr. 4.

V ČSN ISO/IEC 17799 jsou uvedeny problémové oblasti, které musí řešitel systému řízení bezpečnosti zvládnout a vyřešit (např. zajištění organizační a personální bezpečnosti, zajištění fyzické bezpečnosti, řízení vztahů se třetími stranami, apod.). Kromě toho norma strukturuje i způsob vedení dokumentace bezpečnosti v organizaci – doporučuje totiž vedení speciálních, v závislosti na řešené oblasti, specifických dílčích bezpečnostních politik, které vycházejí z celkové bezpečnostní politiky organizace. Problémem výše citovaného aktuálního znění ISO/IEC 17799:2000 je ten, že jeho obsahem je znění standardu právě z roku 2000. Tehdy se původně akceptovaný BS 7799:1999 ještě neřídil konceptem PDCA. V současné době probíhá v organizaci ISO připomínkové řízení k nové verzi ISO/IEC 17799:2005, která bude již plně respektovat PDCA koncept. Je již hotový finální text této normy a předpokládá se, že bude vydána v květnu roku 2005. Velmi významnou pomůckou pro implementaci systému řízení bezpečnosti je druhý díl původního britského standardu – BS 7799-2. Tento díl britské normy není sice vymezující, ale je to příručka založená na nejlepších zkušenostech z praxe. Můžete v ní nalézt doporučené postupy k zavádění a zavedení systémů řízení bezpečnosti IS/ICT do organizací. BS 7799-2 byl listopadu roku 2004 převzat do normativního rámce České republiky technickou normou ČSN BS 7799 (Informační technologie – Soubor postupů pro řízení informační bezpečnosti).

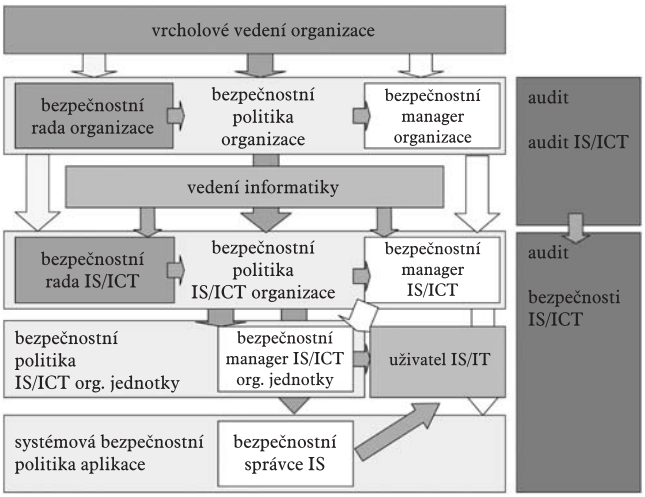


Obr.4 Struktura ČSN ISO/IEC 17799

A co dál?

Jednou ze součástí vybudování systému řízení bezpečnosti je i vybudování odpovídajících organizačních struktur zabývajících se zavedením bezpečnosti a její následnou kontrolou a auditem. Pro organizační aspekty bezpečnosti platí důsledně dodržovat zásady oddělení výkonné a kontrolní pravomoci. To má pro menší organizace a firmy závažné důsledky. Velké organizace nemají problémy s velkým počtem pracovníků případně s větším množstvím rolím přidělených jednomu pracovníkovi. V malých organizacích je takové sdílení rolí velmi problematické, neboť v nich není ani tolik pracovníků, kterých by podle uznávaných metodik bylo pro vybudování a realizaci systému řízení bezpečnosti potřebné. Pro budování systému řízení bezpečnosti IS/ICT v malých firmách je nutné kreativně vyjít z platných standardů, ale musí se přistoupit k výrazné redukci rolí v strategických, výkonných i kontrolních a auditorských orgánech.

Organizační struktury zejména pro velké firmy jsou uvedeny na obr. 5.



Obr.5 Odpovědnosti a pravomoci v systému řízení bezpečnosti IS/ICT

Strategické a koncepční role jsou zejména:

- vrcholové vedení organizace – jeho nejdůležitější úlohou je na strategické úrovni deklarovat zájmy a cíle v oblasti bezpečnosti, formulovat bezpečnostní politiku organizace, řešit dopady nejzávažnějších bezpečnostních incidentů a pravidelně vyhodnocovat stav bezpečnosti v organizaci,
- bezpečnostní rada organizace – je poradním orgánem vrcholového vedení organizace pro otázky bezpečnosti, je spoluautorem bezpečnostní politiky organizace,
- bezpečnostní rada IS/ICT – je poradním orgánem vrcholového vedení organizace pro otázky bezpečnosti IS/ICT, je spoluautorem bezpečnostní politiky IS/ICT organizace; definuje plán realizace bezpečnosti a kontroluje jeho provádění, schvaluje administrativní opatření a přijaté vnitroorganizační standardy, hodnotí účinnost bezpečnostních politik, prosazuje zvyšování bezpečnostního vědomí pracovníků organizace; jejími členy jsou obvykle zástupce vrcholového vedení organizace odpovědný za bezpečnost IS/ICT, bezpečnostní manager IS/ICT, odborní pracovníci z oblasti informačních technologií a případně přizvaní externí odborníci.

Výkonné role:

- bezpečnostní manager organizace – zodpovídá za realizaci bezpečnosti v organizaci, vede bezpečnostní radu organizace, odpovídá za bezpečnost v organizaci, metodicky vede bezpečnostního managera IS/ICT,
- bezpečnostní manager IS/ICT – zodpovídá za zavedení a realizaci bezpečnosti IS/ICT v organizaci, vede bezpečnostní radu

IS/ICT organizace, řeší závažné bezpečnostní incidenty spojené s informačním systémem firmy, zodpovídá za dokumentaci bezpečnosti IS/ICT, spolupracuje s bezpečnostním managerem organizace, zodpovídá za vedení a aktuálnost dokumentace bezpečnosti IS/ICT v organizaci, má reportovací povinnost o stavu bezpečnosti a řešení bezpečnostních incidentů směrem k vedení organizace a její bezpečnostní radě, metodicky je řízen bezpečnostním managerem organizace,

- bezpečnostní manager IS/ICT organizační jednotky – zodpovídá za prosazování bezpečnosti IS/ICT v organizační jednotce, řeší bezpečnostní incidenty na pracovištích a podává zprávy o stavu bezpečnosti a bezpečnostních incidentech managerovi bezpečnosti IS/ICT organizace, metodicky je řízen bezpečnostním manažerem IS/ICT organizace, metodicky řídí bezpečnostní správce informačního systému na své organizační jednotce, formuluje a rozpracovává specifika organizační jednotky v oblasti bezpečnosti IS/ICT (např. organizační jednotka používá jiný síťový protokol pro komunikaci na interních počítačových sítích – orientuje rozpracování bezpečnostní politiky v oblasti komunikací tímto směrem na specifika příslušného protokolu),
- bezpečnostní správce aplikace – výkonný bezpečnostní orgán, spolupracuje s bezpečnostním managerem IS/ICT organizace i organizační jednotky a je jimi metodicky řízen, je odpovědný za provozování bezpečnostních funkcí tak, jak jsou popsány v bezpečnostní politice, vyšetřuje a oznamuje bezpečnostní incidenty spojené s určitou aplikací a reaguje na ně, zodpovídá za korektní nastavení parametrů zajišťujících bezpečnost v určité aplikaci, spolupracuje s bezpečnostním managerem IS/ICT organizační jednotky a bezpečnostním managerem IS/ICT organizace.

Kontrolní role (interní):

- auditor – úloha auditora v organizaci je standardní – provádí audit celé firmy,
- auditor bezpečnosti IS/ICT – provádí v rámci pravidel interního auditu firmy audit oblasti IS/ICT včetně auditu bezpečnosti. Pravidla a postupy auditu jsou stanoveny interní firemní metodikou.

Pro malé firmy je účelné výkon většiny strategických a koncepčních rolí řešit formou outsourcingu, výkonné role potom účelně spojovat např. do jedné role spojit bezpečnostního managera organizace, bezpečnostního managera IS/ICT a případně managera organizační jednotky. Potom je vhodné oddělit roli bezpečnostního správce aplikace (případně ji i řešit formou outsourcingu). Vždy je ovšem nezbytné oddělit roli auditora bezpečnosti od všech předchozích rolí. Pokud je to v malých firmách potřebné, je možné roli auditora řešit formou externí dodávky specializovanou konzultační firmou.

Závěr

Vybudování a následný provoz funkčního systému řízení bezpečnosti IS/ICT je výzvou a úkolem, do jehož řešení musí být nezbytně zapojeni všichni zaměstnanci organizace – nejen vyvolení pracovníci oddělení nebo úseku informačních systémů. S jejím zavedením má každý zaměstnanec svoje nová práva, ale zejména povinnosti. Dalším rysem bezpečnosti informačního systému je, že pro ni platí tzv. řetězový efekt – tj. že organizace musí klást důraz v této oblasti na svůj nejslabší článek (obvykle pracovník nebo zaměstnanec), který určuje sílu systému bezpečnosti IS/ICT jako celku a tím určuje míru ochrany aktiv organizace. Kromě toho musím zdůraznit, že sama bezpečnost IS/ICT a její realizace je běh na dlouhou trať. Jedná se totiž o dlouhodobý, finančně i personálně náročný proces. Měly by jej ale podstoupit všechny organizace, které se chtějí zapojit do evropského integračního procesu. Zároveň bezpečnost informačního systému a její vybudování představuje jakousi formu pojištění proti ztrátám v oblasti informačních technologií. Když se nic nestane – žádný bezpečnostní incident, byla to investice zdánlivě zbytečná, ale pokud k incidentu dojde, tak je již pozdě o čemkoli bádat. Charakter informačních technologií a jejich nasazení v současných organizacích a firmách varuje před podceněním rizik spojených s IS/ICT. V případě jejich výpadku nebo zabránění jejich podpory hlavním procesům, může vést ve velmi krátké době ke ztrátě pozice na trhu a ve finále až k definitivní likvidaci firmy.

K úplnému dobudování systému řízení bezpečnosti je ještě nutné vytvořit funkční dokumentaci celého systému řízní bezpečnosti a navrhnout systém kontroly a auditu. Těmto činnostem je věnováno další pokračování cyklu.

Literatura

[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] ISO/IEC 17799:2005 – Information technology – Security techniques – Code of practice for information security management

[5] TEPELOVSKÁ, H.: Štandardy ochrany a bezpečnosť informácií, In: AT&P journal 12/2004, ISSN 1335-2237

Petr Doucek

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