Manažérstvo životného prostredia 2012 ▲ Management of Environment ´2012
Zborník z XII. konferencie so zahraničnou účasťou, 19. - 20. 11. 2012, Bratislava
Proceedings of the 12rd International Conference, Bratislava, November 19-20, 2012
■ Žilina: Strix. Edícia ESE-12, Prvé vydanie. ISBN 978-80-89281-85-5 ■ Rusko, M. [Ed.] ■

BEZPEČNOSTNÉ MANAŽÉRSTVO A SYSTÉM INFORMAČNEJ BEZPEČNOSTI

SAFETY MANAGEMENT AND SYSTEM OF INFORMATION SAFETY

Miroslav RUSKO - Vojtech KOLLÁR

Abstrakt
Systematický prístup v rámci systému manažérstva informačnej bezpečnosti je potrebný nielen z procesného pohľadu, ale aj so zameraním na vývoj, obstarávanie a implementáciu samotných informačných systémov. Dôležitý je komplexný prístup k informačnej bezpečnosti. Významnú úlohu zohrávajú kritéria hodnotenia systémovej informačnej bezpečnosti, metriky a normy informačnej bezpečnosti.

***Kľúčové slová**: bezpečnosť, informácia, systém, manažérstvo*

Abstract
Systematic approach in the ranks of the information management security system is needed not only from the process point of view but also with focusing on development, gaining and implementation of the information systems alone. Copmlex approach to the information security is important. Criterions of assessment of the information security systems are playing an important role.

***Key words:** safety, security, information, system, management*

Úvod

Bezpečnosť informácií je možné dosiahnuť implementáciou sústavy opatrení, ktoré môžu existovať vo forme pravidiel, natrénovaných postupov, procedúr, organizačnej štruktúry a programových funkcií. Tieto opatrenia musia byť zavedené preto, aby sa dosiahli špecifické bezpečnostné ciele organizácie.
Bezpečnostné manažérstvo nedokáže zabezpečiť absolútne vylúčenie akéhokoľvek rizika, nehôd a krízových situácií. Ponúka možnosti, spôsoby a metódy preventívneho zaobchádzania s potenciálnymi rizikami, pričom otvára možnosti odhaľovania a vyšetrovania bezpečnostných incidentov a krízových situácií. Zároveň definuje opatrenia ako im v budúcnosti predchádzať a eliminovať ich. Bezpečnostné manažérstvo patrí medzi významné manažérske aktivity. V plejáde manažérskych nástrojov a metód sa často kombinuje najmä s nástrojmi manažérstva kvality a environmentu. Z hľadiska uplatňovania jednotlivých prístupov k zabezpečeniu bezpečnosti sa pozornosť sústreďuje na ekonomickú bezpečnosť, environmentálnu bezpečnosť, energetickú bezpečnosť, informačnú bezpečnosť, fyzickú bezpečnosť osôb a majetku, bezpečnosť a ochranu zdravia pri práci, bezpečnosť infraštruktúry a logistiky, teritoriálnu bezpečnosť, technická a technologická bezpečnosť, bezpečnosť produkcie, občiansku bezpečnosť, právnych aspektov bezpečnosti a prevencie kriminality.

Pojem bezpečnosť býva doplňovaný aj rôznymi adjektívami, ktoré sa vzťahujú predovšetkým k charakteru :

- hrozieb, ktoré bezpečnosť ohrozujú,
- opatrení, nástrojov alebo inštitúcií, ktoré majú bezpečnosť zabezpečovať a chrániť,
- objektov, ktorých bezpečnosť má byť chránená. [5]

Bezpečnosť je zložitý atribút, ktorého obsah, štruktúra a funkcie presahujú hranice nielen jedného vedného odboru, ale dokonca i celých vedných oblastí. [1]

Bezpečnostné manažérstvo sa zameriava primárne na

- manažérstvo rizík (analýza bezpečnostného prostredia, analýza rizík, preventívne prístupy a technické, organizačné a administratívne opatrenia na elimináciu neželaných negatívnych udalostí),
- manažérstvo bezpečnostných incidentov (prístupy a technické, organizačné a administratívne opatrenia v prípade negatívnej udalosti).

Bezpečnostná politika je základným dokumentom pre riešenie bezpečnosti v celom komplexe. Definuje východiská pre všetky ďalšie aktivity prevádzkujúceho subjektu v oblasti bezpečnosti. Bezpečnostná analýza je dôležitým východiskom pre proces syntézy získaných poznatkov a vypracovaní bezpečnostných opatrení s cieľom dosiahnuť ciele sformulované v bezpečnostnej politike.
Bezpečnostná situácia je vymedzená podmienkami, okolnosťami, stavmi, v ktorých je realizovaná bezpečnostná činnosť. Pojem incident má rôzny význam v socio-ekonomických, technických, resp. prírodovedných oblastiach. Pod incidentom sa chápe jav, proces, úkaz, skutočnosť. Bezpečnostný incident je proces, ktorý sa pripravuje, vzniká, má svoj priebeh a zaniká a ktorý má za následok vznik bezpečnostnej situácie. V informatike sa chápe ako incident udalosť v informačnej bezpečnosti, ktorá nastane a spôsobí poruchu alebo výpadok počítačového informačného systému. Bezpečnostná identifikácia sa uplatňuje pri zisťovaní totožnosti - personálnej, technickej, technologickej. V posledných rokoch dochádza k významnému a efektívnemu uplatňovaniu informačných a komunikačných technológií v praxi.

Právne predpisy súvisiace s bezpečnosťou informácií

Medzi významné právne predpisy patria najmä:

- Zákon č. 211/2000 Z.z. o slobodnom prístupe,
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností,
- Zákon č. 428/2002 Z.z. o ochrane osobných údajov,
- Zákon č. 215/2002 Z. z. o elektronickom podpise,
- Obchodný zákonník č. 513/1991 Zb.

Systém manažérstva informačnej bezpečnosti

Informácie sú aktíva, ktoré majú pre spoločnosť veľkú hodnotu a teda potrebujú byť vhodným spôsobom chránené. Bezpečnosť informácií je zameraná na širokú škálu hrozieb a zabezpečuje tak kontinuitu činností organizácie, minimalizuje obchodné straty a maximalizuje návratnosť investícii a podnikateľských príležitostí. Informácie môžu existovať v rôznych podobách. Môžu byť tlačené, písané, zachytené na filme alebo posielané elektronickou poštou. Nech už majú akúkoľvek formu alebo sú zdieľané akýmikoľvek prostriedkami, vždy by mali byť vhodne chránené.
Pri úspešnom riadení informačnej bezpečnosti spoločnosti je nevyhnutné vychádzať z rôznych podmienok a vplyvov na spoločnosť, ktoré sú východiskom pre určenie spôsobu riadenia. [4]
Systém manažérstva informačnej bezpečnosti (Information Security Management System - SMIB) pomôže organizácii identifikovať a znížiť kritické bezpečnostné riziká, pretože umožní správne zacielenie úsilia organizácie a ochranu informácií. [6]
Systematický prístup v rámci SMIB je potrebný nielen z procesného pohľadu, ale aj so zameraním na vývoj, obstarávanie a implementáciu samotných informačných systémov. Systematický prístup je možné riešiť prostredníctvom kritérií hodnotenia bezpečnosti samotných IS.

Bezpečný informačný systém by mal obsahovať:

- POLITIC - Musí byť explicitne a presne definované za akých okolností môže nejaký subjekt pristupovať k nejakému objektu v systéme.
- STAMPING - Každý objekt v systéme sa musí dať označiť bezpečnostnou značkou, ktorá určuje úroveň dôvernosti tohto objektu.
- IDENTIFICATION - Každý subjekt musí byť jednoznačne identifikovateľný, tak aby mohol byť každý prístup k informáciám autorizovaný na základe toho kto chce k informáciám pristupovať.
- MONITORING - Bezpečný systém musí byť schopný zaznamenávať výskyt každej z bezpečnostného hľadiska relevantnej udalosti. Tento záznam musí byť chránený pred modifikáciou a neautorizovaným vymazaním.
- ASSURANCE - IS musí obsahovať mechanizmy pomocou ktorých je možné dostatočne sa uistiť že systém zabezpečuje prvé štyri požiadavky.
- SECURITY CONTINUITY: Bezpečný systém musí byť kontinuálne chránený. [2]

Kritéria hodnotenia systémovej informačnej bezpečnosti

Kritéria hodnotenia systémovej informačnej bezpečnosti vychádzajú z

- TCSEC *(Trusted Computer Systems Evaluation Criteria) orange book* **-** kritériá špecifikujú bezpečnosť počítačového systému ako jeho schopnosť zachovania dôvernosti údajov. [7], [9]
- ITSEC *(Information Technology Security Evaluation Criteria)* chápe bezpečnosť systému ako zachovanie atribútov dôvernosti, integrity a dosiahnuteľnosti údajov. Bezpečnosť objektu (môže ním byť ucelený systém, ako aj jeho jednotlivé komponenty – produkty) sa hodnotí podľa bezpečnostných funkcií, ktoré poskytuje, a podľa stupňa istoty v účinnosť týchto mechanizmov. V druhom prípade sa ešte rozlišuje medzi istotou v účinnosť bezpečnostných mechanizmov („sú postačujúce pre daný bezpečnostný cieľ?“) a istotou v správnosť ich návrhu a implementácie. ITSEC nemá hierarchiu tried, ako je to v prípade TCSEC. Hierarchicky sú usporiadané len požiadavky na kvalitu návrhu a implementácie.
- CTCPEC *(Canadian Trusted Computer Product Evaluation Criteria)* sú kombináciou ITSEC a TCSEC. Vývojom týchto kritérií začali vznikať Common Criteria. Kritériá zobrazujú 2 typy požiadaviek: a/ požiadavky na funkcionalitu, t.j. kritériá orientované na 4 politiky: dôvernosť, integrita, dostupnosť, sledovateľnosť; b/požiadavky na zaistenie.
- CC *(Common Criteria)* - v CC sa pojem bezpečnosť chápe nielen ako dôvernosť + integrita + dosiahnuteľnosť, ale zohľadňujú sa aj iné aspekty, ktoré sa nedajú jednoznačne zaradiť do jednej z týchto kategórií (napríklsad ochrana súkromia používateľov hodnoteného produktu). V Common Criteria sa používa nové štruktúrovanie kritérií – zoskupovanie bezpečnostných požiadaviek na triedy, ktoré sa delia na rodiny, ktoré sa skladajú z komponentov: a/trieda (class) – spoločný bezpečnostný zámer, ale rozdielne pokrytie bezpečnostných cieľov; b/ rodina (family) – spoločné ciele, rozdielny dôraz resp. rigoróznosť; c/ komponenty (components) – v CC najmenšie zoskupenie bezpečnostných požiadaviek.[8]

Metriky informačnej bezpečnosti

Skutočná hodnota informácií a informačných aktív spoločnosti je odhalená až pri ich strate dostupnosti, dôvernosti, integrity, príp. autenticity. Vo všeobecnosti nie je dôležité, ktorý atribút je samostatne dôležitejší, ale to, že má určitú hodnotu v konkrétnom systéme spracovania informácií. Pokiaľ chceme objektívne zmerať hodnotu informácií v informačných systémoch, ich kritickosť pre obchodné procesy a pre udržanie konkurencieschopnosti, môžeme použiť rôzne metriky. Metriky slúžia často ako podporný nástroj pre audit informačnej bezpečnosti spoločnosti. Či už sa jedná o interný, či certifikačný audit dané normy slúžia veľmi dobre ako nástroje merania informačnej bezpečnosti, pričom sú plne v súlade s normou ISO 9001.[3]

Medzi významné nástroje patrí

- ISO/IEC 15504 *Informačné technológie - hodnotenie procesov,*
- ISO/IEC 21827 SSE-CMM *Systems security engineering capability maturity model,*
- COBIT *(Control objectives for information and related technology - Ciele riadenia v oblasti informačných a súvisiacich technológií)*
- INTOSAI – smernice pre štandardy vnútornej kontroly pre verejný sektor
- TICKIT SCHEME - metrika uznávaná len zo strany certifikačných spoločností akreditovaných akreditačnými spoločnosťami UKAS a SWEDAC.
- NIST Special Publication 800-80 - návod pre vytváranie metrík na meranie výkonnosti informačnej bezpečnosti.

Normy informačnej bezpečnosti

V rámci SMIB sa uplatňujú viaceré štandardy, najmä normy ISO:

- Norma ISO 17799: 2005 - je jednou z kľúčových noriem pre zavádzanie a certifikáciu systémov riadenia organizácie. Norma uplatňuje komplexný prístup k informačnej bezpečnosti. Aktíva, ktoré si vyžadujú ochranu, zahŕňajú digitálne informácie, dokumenty v papierovej forme a fyzické aktíva (počítače a siete), vedomosti a znalosti jednotlivých zamestnancov. Systém danej organizácie sa musí adresne zaoberať celým radom otázok počnúc rozvojom spôsobilosti zamestnancov až po technickú ochranu proti krádeži priamo z počítača. Norma pre systém manažérstva informačnej bezpečnosti je výsledkom požiadaviek jednotlivých hospodárskych odvetvi, štátnej správy a tiež samotného trhu. Vytvára spoločný rámec, ktorý umožňuje rozvoj, zavedenie a efektívne meranie praxe v oblasti riadenia informačnej bezpečnosti. Norma pozostáva z dvoch časti

- ISO/IEC 20000 *IT service management* - ITSM predstavuje definovanie procesov, ktoré by mali byť v podniku implementované za účelom zaistenia trvale kvalitnej dodávky IT služieb pri vynaložení optimálnych nákladov.
- ISO 15489 *Riadenie záznamov* - norma zameraná na riadenie v oblasti spracovania záznamov spoločnosti.
- PAS 56 (Publicly Accessible Specification 56) - bola vytvorená ako Sprievodca manažmentu BCM (Business Continuity Management) obchodnej kontinuity činnosti Britským štandardizačným inštitútom a Britským inštitútom kontinuity. Bola nahradená Britským štandardom BS 25999, časť 1.
- ISO/IEC 13335 *Informačné technológie - Smernice pre riadenie bezpečnosti IT* ● Štandardy aplikované pri riešení informačnej bezpečnosti, najmä jej projektovej oblasti. Norma je preto odporúčaná v projektoch na ochranu osobných údajov, projektoch jednotlivých oblastí ochrany utajovaných skutočností, ale aj v iných zákonmi nešpecifikovaných oblastiach. Nevýhodou normy je najmä to, že sa ako technická špecifikácia zameriava len na riešenie IT bezpečnosti. V súčasnosti je preto norma používaná ako doplnok k iným normám.
- ISO/IEC 18028 IT *Sieťová bezpečnosť* - štandard zložený z 5 častí, ktorý vyplýva zo štandardu ISO/IEC 27002 a bližšie špecifikuje jeho časti 10.6 a 11.4 a rozširuje ustanovenia riadenia IT bezpečnosti ustanovené v štandarde ISO/IEC 13335. Norma podrobne špecifikuje operácie a mechanizmy potrebné k implementácii sieťovej bezpečnosti kontrolou a bezpečnosťou v širšom meradle sieťového prostredia, v prípade spojenia medzi celkovým riadením IT sieťovej bezpečnosti a technickou implementáciou IT sieťovej bezpečnosti. S normou priamo súvisí norma ISO/IEC 27033, ktorá vo svojich súčasných 7 častiach pojednáva bližšie o jednotlivých častiach normy ISO/IEC 18028.
- Normy radu ISO 27000 *Informačné technológie, Zabezpečovacie techniky* - predstavujú medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti. Sú v súlade s normou ISO/IEC 20000, pričom konkretizujú činnosti ICT v oblasti informačnej bezpečnosti a jej riadenia. Základom normy sú štandardy vyvíjané britským štandardizačným inštitútom (odvodené od britských štandardov rady BS 7799), ktoré sa v súčasnosti postupne zapracovávajú do sústavy ISO/IEC. V štandardizačnom systéme sa tejto norme venuje spoločná komisia ISO a IEC s názvom JTC1, pod ktorou pôsobí podvýbor SC27. Norma ISO/IEC 27000: 2009 *Information security management systems - Fundamentals and vocabulary* predstavuje základný prehľad a úvod do štandardov ISO/IEC 27000 ako aj prehľad základnej terminológie používanej v jednotlivých štandardoch tejto rady.

Systém riadenia informačnej bezpečnosti podľa ISO 27001: 2005

Norma vychádza zo štandardu BS 7799 Part 2:2002 a špecifikuje požiadavky na vytvorenie, budovanie, prevádzkovanie, monitorovanie, kontrolovanie, udržiavanie a zlepšovanie dokumentovaného systému riadenia informačnej bezpečnosti v rámci organizácie. Štandard je zostavený tak, že dokáže pokryť potreby ľubovoľného typu organizácie, od súkromných spoločností až po štátne inštitúcie. Podstatou štandardu je cyklický model PDCA (Plan-Do-Check-Act) – Plánuj-Vykonaj-Kontroluj-Prevádzkuj, ktorého cieľom je vytváranie, budovanie, monitorovanie a neustále zlepšovanie SRIB v rámci organizácie.

Optimálna kombinácia implementácie štandardu ISO/IEC 27001: 2005 je spolu so štandardom ISO/IEC 27002: 2005 *Code of Practice for Information Security Management* (Praktická príručka pre riadenie informačnej bezpečnosti). [11]

Systém riadenia informačnej bezpečnosti podľa ISO 27001: 2005 *Information Security Management System – Requirements* (Systém riadenia informačnej bezpečnosti - požiadavky)

- je základ pre posudzovanie systémov riadenia bezpečnosti informácií pre organizáciu ako celok alebo len pre jej časť,
- je možné použiť ako základ pre formalizovaný postup k certifikácii,
- je určený k ochrane informácií a teda k zvládaniu rizík, ktoré tieto informácie môžu potenciálne ohrozovať,
- je dokumentovaný systém dokazujúci, že identifikované informačné aktíva sú chránené, riziká bezpečnosti informácií sú riadené, sú zavedené opatrenia s požadovanou úrovňou záruky a tie sú kontrolované. ISMS môže byť zavedený pre špecifický IS, jednotlivé časti IS alebo môže zahŕňať celú organizáciu,
- obsahuje špecifikáciu pre systémy riadenia bezpečnosti informácií.

Pre účely tejto normy je bezpečnosť informácií charakterizovaná ako zachovanie dôvernosti, integrity a dostupnosti. Dôležitou súčasťou normy ISO 27001: 2005 je popis k vybudovaniu a prevádzke systému riadenia bezpečnosti informácií.
Organizácie musia realizovať analýzu rizík, aby bolo možné určiť špecificky optimálne bezpečnostné ciele a opatrenia, implementovať ich a aplikovať podľa vlastných požiadaviek. [10] Po ich identifikácii je ich potrebné zrozumiteľne zdokumentovať pre všetky osoby v organizácii, pre ktoré budú aplikované. Tieto podklady musia byť k dispozícii pre manažérov, zamestnancov a vybrané nezávislé strany (napr. interných audítorov, certifikačných audítorov atď.). Zdokumentované bezpečnostné ciele a opatrenia, dokumentácia bezpečnostnej politiky a postupy, ako aj všetky ostatné záznamy, dôležité z hľadiska IS, sa označujú ako systém riadenia bezpečnosti informácií organizácie.

Závery

Systém manažérstva informačnej bezpečnosti sa uplatňuje v jednotlivých hospodárskych odvetviach, štátnej správe a samospráve. Postupne sú zavádzané štandardizované rámce umožňujúce rozvoj, zavedenie a efektívne uplatnenie systematického prístupu v oblasti riadenia informačnej bezpečnosti.
So zvyšujúcim sa objemom a zložitosťou strojového spracovania informácií sa zvyšujú nároky na úspešné riadenie a bezpečnostný prehľad. Platí zásada, že informačná bezpečnosť nie je úlohou pre jedného zamestnanca, prípadne jedného procesu, ale je to komplexná činnosť spoločnosti ako celku, do ktorej sa zapájajú a sú ovplyvnené všetky dotknuté zložky. So zvyšovaním objemu a náročnosti informačnej bezpečnosti rastú nároky na jej efektivitu a riadenie.
ISO/IEC normy rady 27000 predstavujú medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti odvodené od britských štandardov rady BS 7799. Systém manažérstva informačnej bezpečnosti danej organizácie sa musí adresne zaoberať celým radom otázok počnúc rozvojom spôsobilosti zamestnancov až po technickú ochranu proti krádeži priamo z počítača. Systém si môžu zaviesť a nechať certifikovať výrobné, obchodné, servisné, montážne, či poradenské a vzdelávacie organizácie zo všetkých oblastí priemyslu a služieb.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] HOLCR, K. - VICENÍK, J., 1998: K niektorým vybraným filozofickým a metodologickým otázkám konštituovania policajnej vedy. Policajná teória a prax, č. 1/1998, s. 19-20.

[2] KALUŽA Štefan, 2008: Prehľad metodík, metrík a kritérií hodnotenia efektívneho ISMS. Časť I.- Security Revue - ISSN 1336-9717 [on-line] Available on - URL: >http://www.securityrevue.com/<, >http://www.securityrevue.com/article/2008/07/prehlad-metodik-metrik-a-kriterii- hodnotenia-efektivneho-isms-cast-i/<

[3] KALUŽA Štefan, 2008: Prehľad metodík, metrík a kritérií hodnotenia efektívneho ISMS. Časť II.- Security Revue - ISSN 1336-9717 [on-line] Available on - URL: >http://www.securityrevue.com/article/2008/09/prehlad-metodik-metrik-a-kriterii-hodnotenia-efektivneho-isms-cast-ii/<

[4] LOVEČEK, T., 2007: Bezpečnostné systémy – Bezpečnosť informačných systémov. -Žilina: EDIS vydavateľstvo ŽU v Žiline, 2007. ISBN 978-80-8070-767-5

[5] MAREŠ, M., 2002: Bezpečnost. - In : Česká bezpečnostní terminologie. Výklad základních pojmů, Brno: ÚSS VA v Brně, 113 s. (výstup z řešení výzkumného úkolu S-1-031: Perspektivy vývoje bezpečnostní situace, vojenství a obranných systémů do roku 2015 s výhledem do roku 2025).

[6] RUSKO, M., 2010: Bezpečnostné a environmentálne manažérstvo. - Žilina: Strix, Edícia EV-7, 4. revidované vydanie. ISBN 978-80-89281-58-9. 335 s.

[7] VYSKOČ, J: Kritéria hodnotenia bezpečnosti I. - [on-line] Available on - URL: >http://pc.server.sk/—bezpecnost-vseobecne-kriteria-hodnotenia-bezpecnosti–category-je-2-x-id-je-1619<

[8] VYSKOČ, J: Kritéria hodnotenia bezpečnosti II. - [on-line] Available on - URL: >http://pc.server.sk/—bezpecnost-vseobecne-information-technology-security-evaluation-criteria-itsec–category-je-2-x-id-je-1635<

[9] Trusted Computer Systems Evaluation Criteria (Oorange book). - [on-line] Available on - URL: >http://www.boran.com/security/tcsec.html<

[10] Systém manažérstva informačnej bezpečnosti. - [on-line] Available on - URL: >http://www.kiwiki.info/mediawiki/index.php/Syst%C3%A9m_mana%C5%BE%C3%A9rstva_informa%C4%8Dnej_bezpe%C4%8Dnosti< [cit.: 2012-10-09]
[11] Prehľad štandardov ISO/IEC 27000. - [on-line] Available on - URL: >http://www.csirt.gov.sk/informacna-bezpecnost/standardy-a-legislativa/isoiec-27000-814.html< [cit.: 2012-11-01]

ADRESY AUTOROV

Miroslav RUSKO, RNDr., PhD., Slovenská technická univerzita v Bratislave, Materiálovotechnologická fakulta STU v Trnave, Ústav bezpečnostného a environmentálneho inžinierstva, Botanická 49, 817 254 Trnava, e-mail: >mirorusko@centrum.sk<

Vojtech KOLLÁR, prof. Ing., PhD. Katedra bezpečnostného manažmentu, Vysoká škola ekonómie a manažmentu verejnej správy v Bratislave, Furdekova 16, 851 04 Bratislava, Slovenská republika

RECENZENT

Jozef ŠTEFFEK, prof. RNDr., PhD., Technická univerzita vo Zvolene, Fakulta ekológie a environmentalistiky, T. G. Masaryka 24, 960 53 Zvolen, Slovenská republika