Bezpečnostné aspekty informatizácie na príklade Slovenska a Srbska

Zdeněk Dvořák a Zoran Čekerevac [1]

Anotácia
Článok opisuje niektoré princípy Stratégie informatizácie spoločnosti v Slovenskej republike a v Srbsku. Pozornosť je zameraná najmä na otázky bezpečnosti, definovanie rizík, hrozieb a pod.

Summary
The article describes some principles of Informatization Strategy of Slovak Republic and Serbia. The main attention is oriented on problems about security, define of risk, threat etc.

Úvod

Spolupráca medzi pracoviskami na Fakulte špeciálneho inžinierstva Žilinskej univerzity v Žiline a Viššou železničnou školu v Belehrade prešla z roviny úvodných stretnutí a návštev konferencií, do roviny odbornej spolupráce. Ako veľmi vhodná sa javí problematika informačnej bezpečnosti, informatizácie spoločnosti a súviace problémy.

Spoločné princípy stratégie informatizácie

Politika informatizácie spoločnosti vychádza zo schválenej Stratégie informatizácie v Slovenskej republike i v Srbsku. V obidvoch krajinách sa uplatňuje obdobný systém riadenia bezpečnosti - vývoj politiky bezpečnosti informačných technológií identifikáciu rolí a zodpovedností vo vnútri organizácie. Odporúčaná štruktúra je nasledovná:

- riadenie konfigurácie informačných systémov,
- riadenie zmien,
- povedomí všetkých zamestnancov o bezpečnosti informačných systémov,
- výber a implementácia vhodných ochranných opatrení,
- havarijn plány a plánovanie obnovy systémov a dát po havárii,
- manažment rizík, vrátane identifikácie a odhadov:
  - aktív, ktoré je potrebné chrániť,
  - hrozieb,
  - zraniteľností,
  - dopadov,
  - rizík,
  - ochranných opatrení,
  - ostatných rizík,
  - obmedzení.

1 Zdeněk Dvořák, doc. PhD., Fakulta špeciálneho inžinierstva, Žilinská univerzita v Žiline, 1.mája 32, Žilina, Slovenská republika, Tel: ++421 513 6854, Fax: ++421 513 6620.
Zoran Čekerevac, Prof. Dr., Viša železnička škola, Zdravka Čelara 14, Belgrade, Serbia, Tel: ++381 11 27 68 095, Fax: ++381 11 27 68 095

V rámci prípravy podkladov pre uvedenú problematiku je potrebné zamerať pozornosť aj na spracovanie cieľov, stratégie a bezpečnostnej politiky informačného systému. Veľmi dôležitým faktorom pri rozbore a riešení problematiky bezpečnosti je komplexný pohľad. Nie vždy sú použité riešenia vyvážené, celistvé a stáva sa, že neodpovedajú skutočným potrebám a požiadavkám. Nevyváženosť môže byť spôsobená zameraním sa na oblasť technického zabezpečenia, ktorá je v momentálnej situácií najviac v "kurze" a zabudnutím by sa dalo povedať "ľudského" zabezpečenia. Málokto si uvedomuje, že ide o najmenej dôležitú súčasť, ktorá spolu s technickými prostriedkami tvorí celé zabezpečenie informačného systému. Inak povedané, ak pri zabezpečovaní informačného systému volíme vyspelú techniku a premyslený systém opatrení proti útokom zvonka. Je nutné súbežne riešiť problematiku dotýkajúcu sa útokov zvnútra. To čo zaručí alebo nadobro zničí úspech ochrany nie je iba samotné technické riešenie, ale tiež uplatňovanie organizačných pravidiel. Tie je potrebné riešiť v rámci životného cyklu informačného systému. Celý systém riadenia bezpečnosti tak môžeme rozdeliť na dve časti:

1. **Výber a implementácia vhodných technických opatrení**

Tým môžeme rozumieť napr. zavedenie prístupových kariet, obmedzenie práv prístupu užívateľom k údajom podľa ich skutočných potrieb a stupňa dôležitosti údajov, nastavenia práv užívateľov komunikujúcich prostredníctvom internetu, antivírovou kontrolu komunikácie smerujúcej do i von z vnútornej siete. Zaistenie technickej časti bezpečnosti je možné dosiahnuť pomocou správneho nastavenia firewallov, voľbou vhodnej vnútornej architektúry siete.

2. **Povedomie všetkých zamestnancov o bezpečnosti informačných systémov**

Správna funkcia bezpečnostných opatrení vyžaduje - dodržovať základné pravidlá pri práci s počítačovými systémami. To znamená, že si užívatelia navzájom nehovoria prístupové mená, heslá a prístupové kódy. Tieto sú uložené v písomnej podobe v trezoru, ktoré sa otvárajú pri mimoriadnych a krízových situáciách. Okrem uvedeného je nutné dodržovať nariadenia o posielaní a príjme nepovolených typov príloh, sťahovaní neznámych aplikácií alebo samo spustiteľných súborov, navštevovaní nepovolených či rizikových www stránok. Správne nastavenie firewallu či pravidiel proxy serveru môže rizikové správanie užívateľov výrazne obmedziť.

Prínosy spracovania bezpečnostní politiky

- vypracovanie štúdie signalizuje vážny záujem organizácie zaoberať sa Informačnou bezpečnosťou,
- komplexný prístup ku všetkým aspektom bezpečnosti ukáže i na väzby vo vnútri spoločnosti,
- pohľad zvonka veľmi často odhalí a pomenuje chyby o ktorých všetci vedia, ale „nehovorí sa“ o nich.

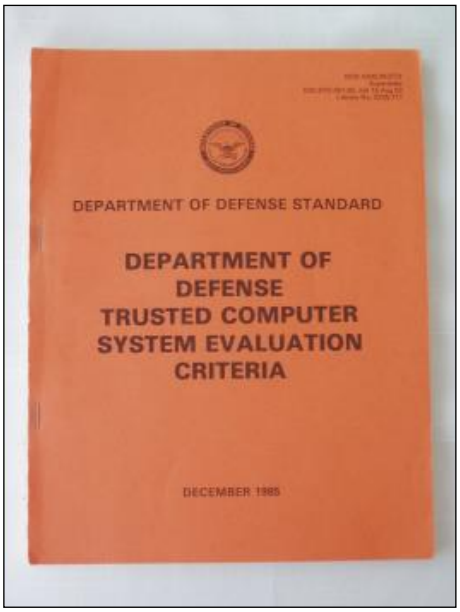
Spôsob vykonania a získanie podkladov k bezpečnostnej politike je vykonaný tak, že organizácia vytvorí neformálnu pracovnú skupinu zodpovedných pracovníkov jednotlivých oblastí, ktorých sa bezpečnosť dotýka a externého spracovateľa bezpečnostnej politiky. Informácie sa získavajú formou rozhovorov s jednotlivými pracovníkmi a tiež vhodne zostavenými dotazníkmi.

Bezpečnostná politika sa týka nasledujúcich oblastí

- bezpečnosť IT,
- fyzická bezpečnosť,
- legislatívne otázky,
- logická bezpečnosť,
- personálna bezpečnosť.

Ciele informačnej bezpečnosti

- minimalizovať škody spôsobené bezpečnostnými incidentmi a chybami, sledovať ich a učiť sa z nich,
- zaistiť, aby si užívatelia boli vedomí bezpečnostných hrozieb a boli pripravený sa podieľať na dodržiavaní bezpečnostnej politiky v priebehu svojej práce,
- znížiť riziko ľudskej chyby, krádeže, podvodu alebo zneužitie prostriedkov organizácie.



Obr. 1 Oranžová kniha

Definovanie aktív

Aktívom je to, čo má pre organizáciu hodnotu. Aktíva organizácie zahŕňajú:

- fyzické aktíva (napr. počítačový hardware, komunikačné prostriedky),
- informácie (dokumenty, databázy,...),
- nehmotné hodnoty (napr. abstraktná hodnota firmy, imidž, dobré vzťahy atď.),
- pracovná sila, školenie pracovníkov, znalosti zamestnancov, ich zapracovanie),
- schopnosť vytvárať určité produkty alebo poskytovať služby,
- software.

Všetky z uvedených aktív majú takú cenu, že si zaslúžia určitý stupeň ochrany.

Odhad hrozieb

Aktíva sú predmetom rôznych hrozieb. Hrozby majú prírodný alebo ľudský pôvod. Môžu byť náhodné alebo úmyselné. Škoda spôsobená incidentom môže byť dočasnej povahy alebo môže byť trvalá.

Analýza zraniteľností

Zraniteľnosti zahŕňajú slabé miesta v systéme, ktoré môžu byť hrozbou využité. Následne vedú k nežiaducim následkom. To sú príležitosti, ktoré vedú ku vzniku škôd. Napríklad absencia mechanizmu riadenia prístupov je zraniteľnosť. Analýza zraniteľností je preskúmanie slabých miest, ktoré môžu byť využité identifikovanými hrozbami.

Odhad dopadov

Dopad je dôsledok nežiaduceho incidentu, spôsobeného náhodne alebo úmyselne. Následky môžu mať podobu zničenia určitých aktív, poškodenia systému IT, a straty dôvernosti,

integrity, dostupnosti, autenticity, individuálnej zodpovednosti nebo spoľahlivosti. Meranie dopadov umožňuje vytvorenie rovnováhy medzi výsledkami nežiaducich incidentov a nákladmi na ochranné opatrenia a početnosti ich výskytov.

Kvantitatívne a kvalitatívne meranie dopadov sa vykonáva:

- použitím adjektív z vopred definovaného zoznamu, napr. nízky, stredný, vysoký, ...
- priradením empirickej stupnice sily, napr. 1 – 10,
- stanovením finančných nákladov,

Analýza rizík

Riziko je potenciálna možnosť, že daná hrozba využije zraniteľnosti, aby spôsobila stratu alebo poškodenie aktív alebo skupiny aktív. Riziko je charakterizované ako kombinácia dvoch faktorov, pravdepodobnosťou výskytu nežiaduceho incidentu a jeho dopadu.

Prijatie zvyškových rizík

Rizika sú obvykle použitím ochranných opatrení iba zmiernená. Zvyšné riziko sa nazýva zvyškové riziko. Súčasťou posúdení, či bezpečnosť odpovedá potrebám organizácie je akceptácia zvyškových rizík.

Stanovení obmedzení

Obmedzenia sú stanovené vedením organizácie, sú týchto typov:

- finančné,
- organizačné,
- personálne,
- právne,
- technické.

Monitorovanie a hodnotenie

Celý proces hodnotenia a monitorovania je dôležitou súčasťou udržateľného rozvoja IS systémov. Základný rozdiel medzi monitorovaním a hodnotením je v otázke, na ktorú odpovedajú. V srbskej Stratégii informatizácie je hodnotenie definované nasledovne:

- indikátory hodnotenia,
- metodológia pre hodnotenie,
- obdobie hodnotenia,
- autorizácia inštitúcií, ktoré môžu hodnotenie vykonávať.

Monitorovanie definujú:

- vopred určené indikátory,
- rozmer analýz,
- obnova a rozvoj politiky a stratégie.

Záver

Vzájomná spolupráca v odbornej oblasti môže priniesť celý rad prekvapivých zistení. Porovnávanie obsahu výučby je prvým krokom, nasleduje porovnanie lekčného fondu

a vyvrcholenie je vo výmene materiálov na prednášky a príkladov na cvičenia. Intenzívna spolupráca aj na vzdialenosť 800 km je dnes vďaka moderným IT technológiám doslova každodenná. Celý rad odborných problémov, zrod nových spoločných projektov je otázkou kvality vzájomnej komunikácie. Veríme, že v ďalšom kroku budú nasledovať vzájomné výmeny učiteľov a študentov v rámci rôznych programov a grantových schém.

♦♦♦

Literatúra

[1] ESEE. *Agenda for the Development of the Information Society.* Stability Pact. 4 June, 2002

[2] EU. *eEurope 2002: eEurope Benchmarking Report.* Brussels: Commission of the European Communities, 2002

[3] *eEurope e 2002: Impacts and Priorities*. Brussels: Commission of the European Communities, 2001

[4] *eEurope 2005: Benchmarking Indicators*. Brussels: Commission of the European Communities, 2002

[5] *eEurope: An Information Society for All.* Brussels: Commission of the European Communities, 2002