RIADENIE INFORMAČNEJ BEZPEČNOSTI VO VEREJNEJ SPRÁVE

Katarína Kampová[*)]

ABSTRAKT

Príspevok sa zaoberá bezpečnosťou informačných systémov verejnej správy, ktorá je upravovaná výnosom ministerstva financií Slovenskej republiky z 9. júna 2010 č. 312/2010 o štandardoch pre informačné systémy verejnej správy. Tento článok poskytuje stručný návod ako splniť požiadavky tohto výnosu vzhľadom na manažment rizík.

Kľúčové slová:
Informačná bezpečnosť, zraniteľnosť, hrozba, aktívum, analýza rizík

ABSTRACT

The paper deals with the security of information systems in public administration, which is implemented under an act of Ministry of Finance of the Slovak Republic from 9. Jun 2010 number 312/2010 - Standards for information system of public administration. This article provides brief guidance on how to meet the requirements of mentioned act with regard to risk management

Key words:
Information security, vulnerability, threat, asset, risk analysis

1 ÚVOD

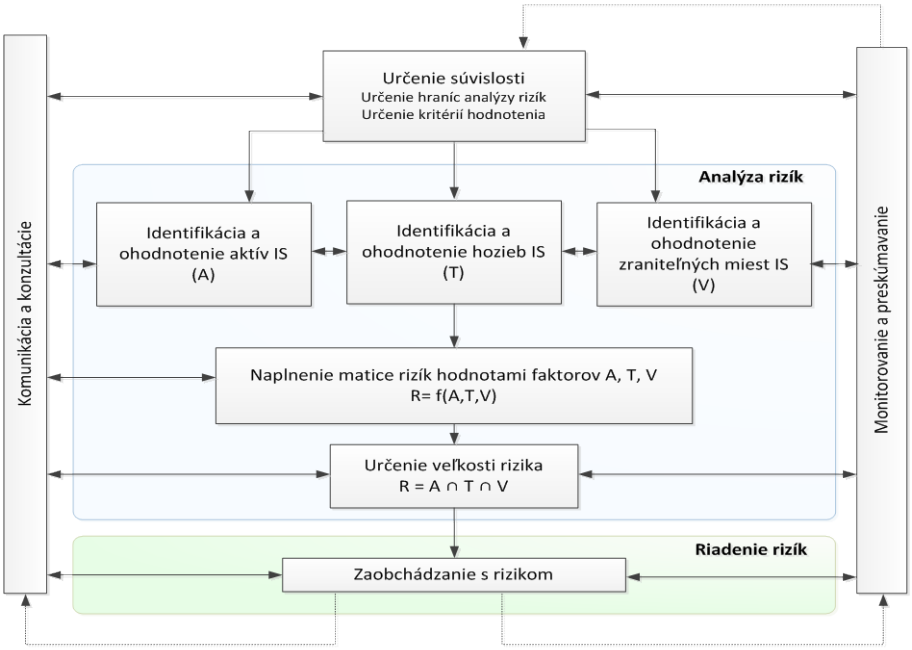
Ministerstvo financií Slovenskej republiky v súlade so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy, Výnosom z 9. júna 2010 č. 312/2010 o štandardoch pre informačné systémy verejnej správy a metodickým pokynom k tomuto výnosu vyžaduje zavádzanie a dodržiavanie štandardov týkajúcich sa bezpečnosti informačných systémov verejnej správy (§28 až §42 z Výnosu 312/2010). V rámci

*) Katarína Kampová, PhD., Katedra bezpečnostného manažmentu, FŠI ŽU, 1. Mája 32, 01026 Žilina, 041 5136661, Katarina.Kampova@fsi.uniza.sk

tohto článku bude popísaný systém manažmentu rizík založený na identifikácii, analýze a hodnotení rizík spojených s informačnou činnosťou.

2 MANAŽMENT RIZÍK

Manažment rizík je kľúčovým nástrojom pre systematické riadenie bezpečnosti informačných systémov. Dôkladná znalosť skutočných rizík v súvislosti s informačnými systémami rozhoduje o výbere a presadzovaní vhodných bezpečnostných opatrení, ktoré sú schopné znížiť možnosť výskytu, resp. rozsah negatívnych dopadov. Manažment rizík je preto základom pre každý systém riadenia informačnej bezpečnosti. Celý proces manažmentu rizík je znázornený na obrázok 1.



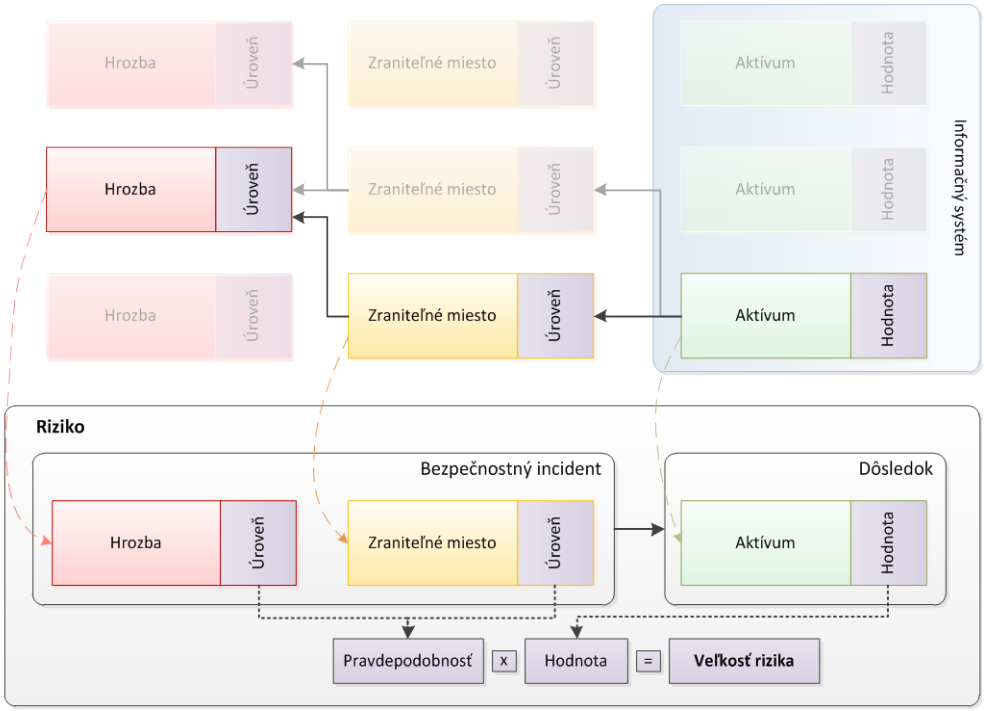
Obrázok 1 Proces manažmentu rizík

3 URČOVANIE SÚVISLOSTÍ MANAŽMENTU RIZÍK

Proces určenia súvislosti vytvára vstupný rámec analýzy rizík prostredníctvom dvoch podprocesov, a to určenie hraníc analýzy rizík a kritéria hodnotenie rizika informačných systémov.

Hranica analýzy rizík je pomyselná čiara oddeľujúca aktíva, ktoré budú zahrnuté do analýzy rizík, od tých ostatných. V rámci procesu riadenia rizík informačných systémov je nevyhnutné stanoviť všeobecne platné a jasné kritéria prijateľnosti a neprijateľností rizík, tak aby sa predchádzalo nedorozumeniam, z ktorých môžu vzniknúť rôzne krízové situácie. Tento prístup vychádza zo základnej definície rizika, ktorá vo všeobecnosti vníma riziko ako možnosť, že budúca udalosť bude mať nepriaznivé dopady. Možnosť vzniku udalosti je kvantifikovaná pravdepodobnosťou a nepriaznivé dopady hodnotou ohrozených záujmov. V prípade

rizík v súvislosti s informačnou bezpečnosťou daného subjektu sa riziko definuje unikátnou kombináciou aktíva a zraniteľného miesta (ktoré aktívum má) a hrozby (ktorá môže zraniteľné mesto využiť) viď. Obrázok 2.



Obrázok 2 Určenie veľkosti rizika pre oblasť informačnej bezpečnosti

Pri stanovení kritérií prijateľnosti či neprijateľnosti rizík pre oblasť informačnej bezpečnosti je možné vychádzať z kvalitatívnej metódy podľa STN ISO/IEC TR 13335, ktorá využíva na hodnotenie rizík informačných systémov, a ktorá umožňuje hodnotiť riziká na základe hodnoty aktíva, úrovne hrozby a úrovne zraniteľného miesta.

4 ANALÝZA RIZIKA

Analýza rizík informačných systémov predstavuje základný proces manažmentu rizík pre oblasť informačnej bezpečnosti. Tento proces je založený na identifikácii aktív podľa kritérií zvolených v rámci určenia hranice analýzy rizík, ohodnotení týchto aktív, a tiež identifikácii a ohodnotení hrozieb a zraniteľných miest, a určení pravdepodobnosti ich uskutočnenia a dopadov na analyzované aktíva.

Výsledkom analýzy rizík je kvantifikácia veľkosti rizika na základe kombinácií faktorov rizika (A, V, T). Tento proces stanovenia veľkosti rizika priamo súvisí so stanovenými kritériami hodnotenia rizík, a to tak, že získané miery rizík sa porovnávajú so stanovenými kritériami a klasifikujú sa do vytvorených troch úrovní (akceptovateľná miera rizika, akceptovateľná miera rizika za určitých podmienok a neakceptovateľná miera rizika).

Prístup k procesu analýzy rizík vychádza zo štandardov ako ISO/IEC 177799/2000 a STN ISO/IEC TR 13335, ktoré poskytujú odporúčania pre riadenie bezpečnosti informačných systémov. Na základe implementovania tohto prístupu je

daný subjekt verejnej správy schopný zaistiť ochranu informačných systémov a všetkých jeho prvkov a zároveň spĺňať predpoklady právnych predpisov platných na území SR v oblasti informačnej bezpečnosti. Proces analýzy rizík zahŕňa nasledovné oblasti:

- identifikácia a ohodnotenie aktív,
- identifikácia a ohodnotenie hrozieb,
- identifikácia a ohodnotenie zraniteľností,
- určenie veľkosti rizika a hodnotenie rizika.

3.1 IDENTIFIKÁCIA A OHODNOTENIE AKTÍV

Cieľom identifikácie aktív je vytvorenie zoznamov všetkých aktív, ktoré ležia vo vnútri stanovenej hranice analýzy rizík. Vo všeobecnosti sa pod termínom aktívum chápe všetko čo prináša ekonomický úžitok organizácií. V rámci analýzy rizík informačných systémov sa pod termínom aktívum budú chápať tieto kategórie:

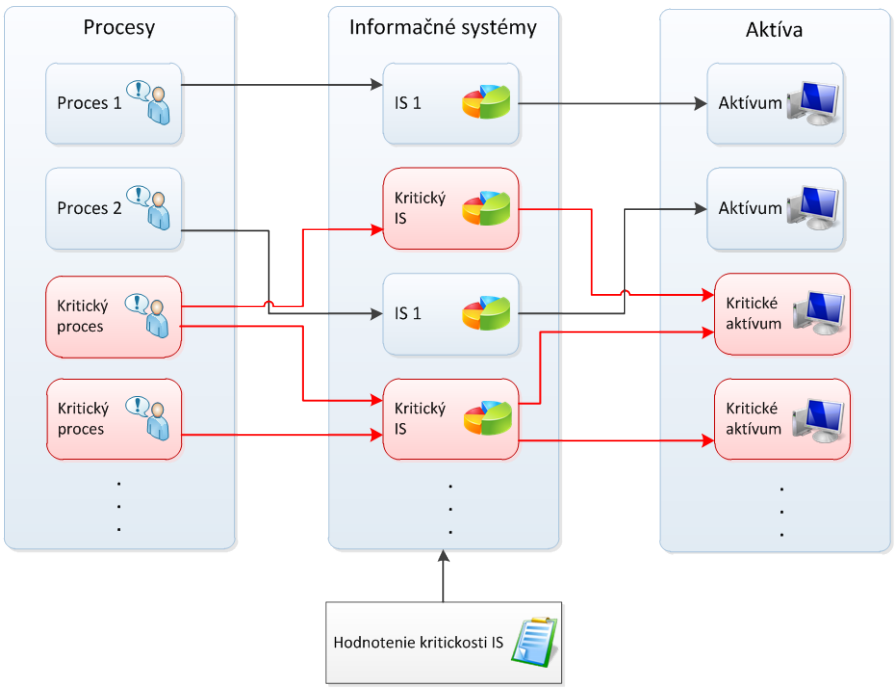
- informácie,
- programové vybavenie,
- technické zariadenia,
- ľudské zdroje.

Proces identifikácie aktív sa vykonáva formou štruktúrovaných rozhovorov, fyzickou obhliadkou miest, ako aj štúdiom relevantných dokumentov, smerníc, nariadení v rámci daného subjektu. Vytvorenie zoznamu všetkých aktív je predpokladom ďalšieho kroku procesu identifikácie aktív, ktorým je výber množiny aktív v rámci stanovenej hranice analýzy rizík. Implicitným kritériom pre tento výber je kritickosť aktíva. Preto je dôležité definovať štandardný postup pre určenie kritických aktív.

Kľúčovou vlastnosťou aktíva spadajúceho do manažmentu rizík pre oblasť informačnej bezpečnosti je, že je základnou súčasťou informačného systému. Teda informačný systém používa jednotlivé aktíva na realizáciu informačnej činnosti, ktorá je jeho primárnou úlohou. Samotná informačná činnosť je definovaná a organizovaná prostredníctvom procesov daného subjektu. Týmto sa vytvára vzťah medzi procesmi, informačným systémom a aktívami.

Centrálnym prvkom tohto vzťahu je informačný systém, ktorý predstavuje funkčný celok spájajúci procesy, ktoré zastrešujú informačnú činnosť a aktíva, prostredníctvom ktorých sa táto činnosť vykonáva. Pri identifikácii kritických aktív sa preto primárne vychádza z určenia kritickosti informačných systémov, pričom je možné vychádzať z predpokladu, že ak je informačný systém kritický tak aj jednotlivé jeho procesy sú kritické a analogicky aj všetky aktíva, ktoré sú nevyhnutné pre zabezpečenie informačnej činnosti prostredníctvom kritického informačného systému sú kritické.

Výsledkom celého procesu identifikácie kritických aktív je zoznam kritických aktív, ktoré sú predmetom ďalšej analýzy. Tento zoznam vytvára vstup pre následný proces ohodnotenia kritických aktív.



Obrázok 3 Proces identifikácie kritických aktív

Ohodnotenie kritických aktív je proces kvantifikácie ich významnosti vzhľadom na ich nevyhnutnosť v rámci informačnej činnosti prostredníctvom informačných systémov, resp. z pohľadu ich hodnoty a záujmu ochrany. Príklad možného ohodnotenia kritických aktív, ktorý vychádza zo zoznamu kritických aktív je v tabuľke Tabuľka 1.

Tabuľka 1 Ohodnotenie kritický aktív

Kritické aktíva	Hodnota	Popis
Server 1	Veľká (V)	Využívaný v rámci šiestich kritických procesov
Dátová knižnica	Veľká (V)	Neexistencia papierovej formy údajov
PC zostava	Malá (M)	Existencia externých záloh
Prístupové heslá	Stredná (S)	Iná osoba, ktorá pozná prístupové heslo
Router 2	Malá (M)	Alternatívne zariadenie pre zabezpečenie prístupu do internetu

3.2 IDENTIFIKÁCIA A OHODNOTENIE HROZIEB

V tejto etape analýzy rizík sa identifikujú a ohodnotia hrozby, ktoré predstavujú okolnosti, resp. udalosti, ktoré majú potenciál poškodiť aktíva informačných systémov, alebo v horšom prípade zničiť informačný systém ako taký. Hrozby tak predstavujú vecnú podstatu bezpečnostných incidentov, ktorá je nutnou, avšak nie

postačujúcou podmienkou, aby bezpečnostný incident nastal (na to, aby bezpečnostný incident nastal je potrebné využitie zraniteľného miesta).

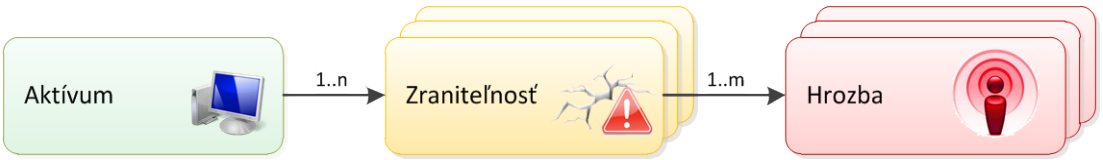
Pri identifikácií hrozieb je možné vychádzať zo zoznamov, ktoré sú súčasťou príloh technických noriem STN ISO/IEC TR 13335-3 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT.

Ohodnotenie úrovne hrozby je založené na zhodnotení možnosti, že nastane udalosť, ktorá hrozbu predstavuje. Pri hodnotení hrozby sa neprihliada na schopnosť hrozby poškodiť aktíva informačného systému, ale odhaduje sa striktne iba pravdepodobnosť, resp. možnosť výskytu udalosti, pričom sa abstrahuje od ďalších okolností, ktoré má tento výskyt potenciál spôsobiť.

V rámci hodnotenia hrozieb je možné použiť rôzne kvalitatívne kritéria na určenie hodnoty hrozby (napr. expertný odhad v závislosti od znalosti úrovne implementovaných ochranných opatrení apod.). Dôležité je, aby ohodnotenie hrozieb vyjadrovalo mieru presvedčenia hodnotiteľa o možnosti výskytu hrozby (udalosti) bez ohľadu na možné dopady hrozieb na aktíva.

3.3 IDENTIFIKÁCIA A OHODNOTENIE ZRANITEĽNÝCH MIEST

Zraniteľné miesta predstavujú vlastnosti prostredia (fyzického, personálneho a elektronického), v rámci ktorého sa realizuje informačná činnosť prostredníctvom informačných systémov a ktoré vytvárajú podmienky pre pôsobenie hrozieb na aktíva. Kvalitatívne sú tieto vlastnosti ovplyvňované najmä aplikovanými ochrannými opatreniami. Zraniteľné miesta tak vytvárajú logické prepojenie medzi hrozbami a aktívami (viď. Obrázok 4), ktorého dôsledkom je poškodenie, alebo zničenie informačného systému.



Obrázok 4 Vzťah medzi aktívami, zraniteľnými miestami a hrozbami

Cieľom procesu identifikácie a ohodnotenia zraniteľných miest je nájsť zraniteľné miesta, definovať prepojenia medzi hrozbami a aktívami a ohodnotiť významnosť identifikovaných zraniteľných miest.

Pri identifikácii zraniteľných miest sa postupuje formou štruktúrovaných rozhovorov, obhliadkou fyzického prostredia, ako aj štúdiom relevantných dokumentov, smerníc a nariadení. Jednotlivé zraniteľné miesta sa identifikujú vzhľadom na identifikované kritické aktíva a vzhľadom na identifikované hrozby, čím sa popisuje prepojenie hrozieb a aktív prostredníctvom zraniteľných miest. Výsledkom procesu hodnotenia zraniteľných miest je ich zoznam vzhľadom ku konkrétnemu aktívu. Samotné hodnotenie vo väčšine prípadov je vykonávane pomocou kvalitatívnych metód, ktorými sa ohodnotí veľkosť danej zraniteľnosti.

3.4 URČENIE VEĽKOSTI RIZIKA A HODNOTENIE RIZIKA

Veľkosť rizika je elementárna vlastnosť rizika, ktorá vyjadruje presvedčenie hodnotiteľa o možnosti výskytu rizikovej udalosti a závažnosti dôsledkov. Veľkosť rizika v rámci popísaného prístupu k analýze rizík informačných systémov sa stanovuje na základe kombinácie ohodnotených úrovní aktív, zraniteľných miest týchto aktív a hrozieb (viď. Tabuľka 2). Kombinácia ohodnotenej úrovne hrozby spolu s úrovňou zraniteľného miesta kvantifikujú možnosť vzniku bezpečnostného incidentu, ktorého negatívny dopad na aktívum je určený hodnotou aktíva. Veľkosť rizika je potom vyjadrená kombináciou pravdepodobnosti bezpečnostného incidentu a hodnoty aktíva

Tabuľka 2 Príklad ohodnotenia rizika

Faktor	Popis	Úroveň/Hodnota
Aktívum	Server 1	Veľká (V)
Zraniteľnosť	Nezabezpečený vchod do miestnosti v rámci pracoviska	Veľká (V)
Hrozba	Neodborná alebo neprimeraná manipulácia	Malá (M)

Cieľom určenia veľkosti rizika je definovať toleranciu rizika. Tolerancia rizika vyjadruje či je dané riziko akceptovateľné alebo neakceptovateľné z pohľadu požadovaného stavu informačnej bezpečnosti. Pri určení veľkosti rizika sa teda vychádza z ohodnotení jednotlivých faktorov rizika.

Hodnotenie rizika je proces, na základe ktorého sa porovnáva veľkosť rizika získaná v procese analýzy rizika s vopred určenými kritériami rizika. Výstupom z procesu hodnotenia rizika je prioritizovaný zoznam rizík, ktoré je nevyhnutné riadiť.

5 RIADENIE RIZÍK

Riadenie rizík je proces, v rámci ktorého sa identifikujú a navrhujú možnosti, ktorými je za aktuálnych podmienok možné reagovať na neakceptovateľné riziko za účelom zníženia jeho veľkosti.

Spôsob ako znížiť neakceptovateľnú mieru rizika, je implementovať adekvátne ochranné opatrenia, po prijatí ktorých sa riziko zníži na úroveň zostatkového rizika. Toto zostatkové riziko sa od pôvodného rizika líši práve o riziko redukované ochrannými opatreniami.

Návrh ochranných opatrení vychádza primárne z realizovanej analýzy rizík a identifikácie zraniteľných miest. Znalosť zraniteľných miest a ich kvalitatívnych vlastností umožňuje návrh preventívnych opatrení, ktoré zabraňujú tomu, aby bezpečnostný incident nastal. V prípade, že nie je technicky alebo ekonomicky možné zaviesť preventívne opatrenie, je možné navrhnúť ochranné opatrenia založené na transfere dopadov bezpečnostných incidentov na tretiu stranu (napr. poistenie, zmluvná pokuta, ..).

6 ZÁVER

Riadenie bezpečnosti informačných systémov je významnou časťou zachovania celkovej bezpečnosti jednotlivých organizácií verejnej správy. Predstavený prístup k implementácií požiadaviek bezpečnosti informačných systémov vyplývajúci z výnosu ministerstva financií č. 312/2010 o štandardoch pre informačné systémy verejnej správy môže pomôcť jednotlivým subjektom verejnej správy pri jeho zavádzaní. Tento prístup im poskytuje stručný návod na vykonanie procesu analýzy rizík, ktorý popisuje v kontexte celkového systému riadenia rizík informačných systémov.

LITERATÚRA

[1] ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky.

[2] STN ISO/IEC TR 13335 - Informačné technológie. Návod na manažérstvo bezpečnosti IT

[3] STN ISO/IEC 17799 Informačné technológie. Kódex praxe manažérstva informačnej bezpečnosti

[4] Zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy

[5] Výnosom Ministerstva financií č. 312/2010 o štandardoch pre informačné systémy verejnej správy

Tento článok bol spracovaný v rámci projektu APVV-0043-10

Článok recenzoval:
doc. Ing. Tomáš Loveček, PhD.