INTEGROVANÁ BEZPEČNOSŤ PROSTREDIA • 2019 • INTEGRATED SAFETY OF ENVIRONS
Recenzovaný zborník z medzinárodnej vedeckej konferencie konanej 27. septembra 2019 v Bratislave
Proceedings of the International Scientific Conference, Bratislava, September 27, 2019, Slovak Republic
Žilina: Strix et SSŽP, Edition ESE-49, First Edition, ISBN 978-80-89753-34-5
Slovak Society for Environment • Bratislava • Slovak Republic

POSUDZOVANIE RIZÍK

Alojz BARTEK

RISK ASSESSMENT

INTEGRATED SAFETY OF THE ENVIRONS

INTEGRATED SAFETY OF ENVIRONS ´2019

ABSTRAKT
Analýza rizík v kontexte bezpečnosti zahŕňa analýzu hodnôt aktív, hrozieb a zraniteľnosti a určenie potenciálnych rizík. Riziká sú určené z hľadiska možného dopadu spôsobeného narušením dôvernosti, integrity, dostupnosti, individuálnej zodpovednosti, autenticity alebo spoľahlivosti. Analýza rizík je proces, prostredníctvom ktorého sa identifikujú bezpečnostné riziká, ktoré je potrebné kontrolovať alebo akceptovať.

KĽÚČOVÉ SLOVÁ: *bezpečnosť, podnik, riziko*

ABSTRACT
Risk analysis in the context of security involves analyzing asset values, threats and vulnerabilities and identifying potential risks. Risks are identified in terms of the potential impact caused by violations of confidentiality, integrity, availability, individual responsibility, authenticity or reliability. Risk analysis is the process by which security risks are identified that need to be controlled or accepted.
KEY WORDS: *safety, enterprise,risks*

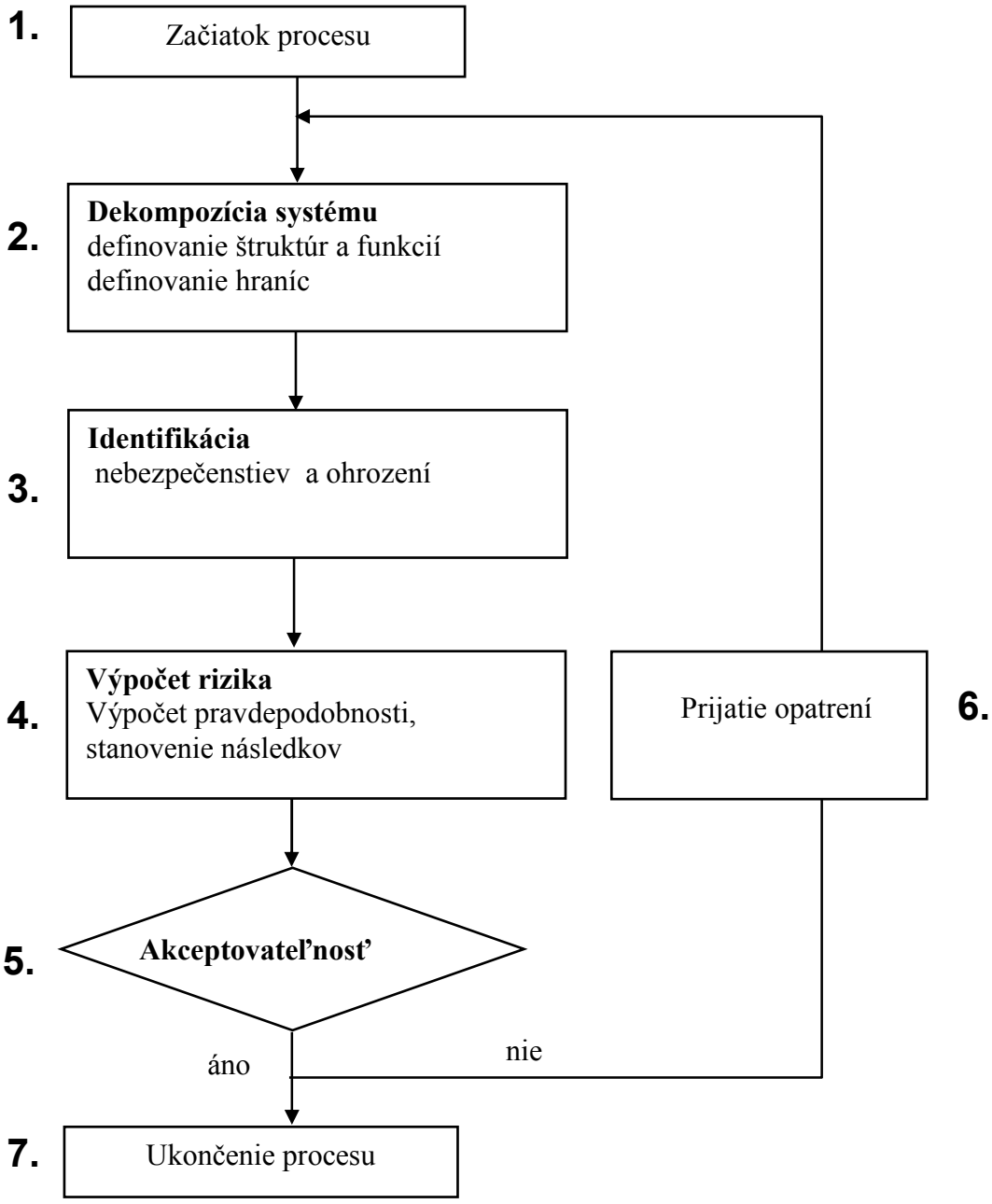
Úvod
Analýza rizík je proces, prostredníctvom ktorého sa identifikujú bezpečnostné riziká, ktoré je potrebné kontrolovať alebo akceptovať.

Analýza rizík v kontexte bezpečnosti zahŕňa analýzu hodnôt aktív, hrozieb a zraniteľnosti a určenie potenciálnych rizík. Riziká sú určené z hľadiska možného dopadu spôsobeného narušením dôvernosti, integrity, dostupnosti, individuálnej zodpovednosti, autenticity alebo spoľahlivosti. Výsledkom analýzy rizík je poznatok o pravdepodobných rizikách týkajúcich sa aktív poisťovne. Analýza rizík je východiskom pre manažment rizík a môže byť vykonaná bez zbytočných časových investícií a investícií do zdrojov, uskutočnením počiatočnej krátkej analýzy všetkých systémov. Analýza určí, ktoré systémy môžu byť adekvátne chránené pomocou vzorovej sústavy prijatých praktických postupov a základných kontrol a pre ktoré systémy bude potrebné vykonať podrobnú analýzu rizík.

Posudzovanie rizík – všeobecne

Metódy posudzovania rizík prešli prudkým vývojom. Dnes sú štandardizované vo výpočtových programoch s možnosťou rýchlej aplikácie. S ohľadom na rozsiahlosť riešenia týchto problémov (rozličné systémy, rôzna fyzikálna, chemická, biologická podstata) nebola vytvorená univerzálna metóda pre posudzovanie rizík. Existujú však princípy, ktorých aplikovaním pre akýkoľvek systém je možné vytvoriť postup, ktorým je možné posúdiť riziko v novo skonštruovanom produkte. Proces riadenia rizika sa realizuje podľa všeobecnej schémy (obr. 1).

Všeobecná schéma postupu riadenia rizík



Obr. 1Všeobecná schéma riadenia rizika (Tkáč et al., 2002)

1. krok - začiatok procesu

- Stanovenie cieľa posudzovania rizika.
- Zadefinovanie požiadaviek na proces posudzovania rizika.
- Stanovenie pracovného tímu, ktorý vykoná posúdenie rizík.
- Zabezpečenie potrebných podkladov a informácií pre posúdenie rizík.

2. krok - dekompozícia systému, definovanie charakteristických štruktúr a funkcií

- Stanovenie hraníc (časové a priestorové)posudzovaného systému.
- Dekompozícia systému na podsystémy.
- Charakteristické väzby medzi podsystémami.
- Určenie vstupov, výstupov a medziproduktov systému.

3. krok - identifikácia nebezpečenstiev a ohrození

- Identifikácia nebezpečenstiev zvoleným postupom.
- Identifikácia ohrození v čase a priestore príslušnými metódami.
- Aplikovanie princípu verifikácie v rámci primárnej selekcie.
- Primárna selekcia.
- Vytvorenie charakteristických scenárov.

4. krok - výpočet rizika

- Výpočet dôsledku pre príslušný scenár - nežiaduca udalosť.
- Výpočet pravdepodobnosti výskytu udalosti.
- Výpočet rizika.

5. krok - posúdenie akceptovateľnosti rizika

- Matica rizík s hranicami akceptovateľnosti.
- Porovnanie výsledného rizika príslušného scenára s akceptovateľnými hranicami.

6. krok - prijatie opatrení na zníženie rizika

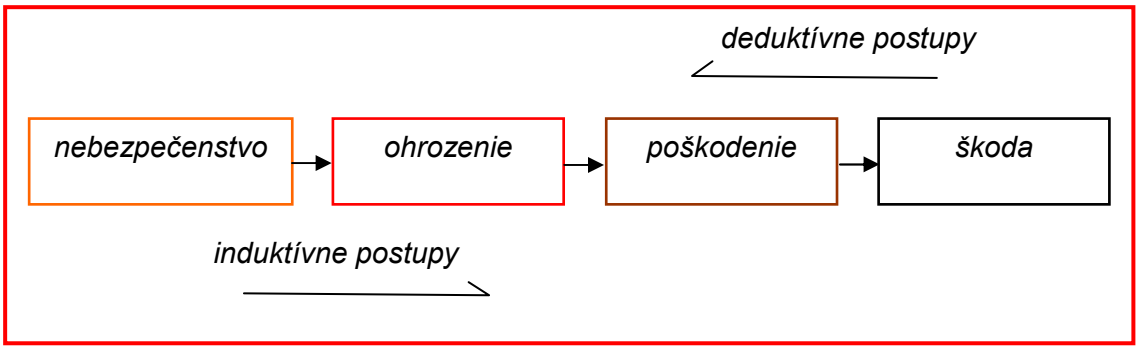
- Návrh a realizovanie opatrení na minimalizovanie rizika.
- Presunutie rizika do finančnej roviny - poistenie.

7. krok - ukončenie procesu

- Vyhodnotenie procesu posudzovania rizika.

Pojmy kauzálnej závislosti

Medzi hlavné pojmy, s ktorými pracuje teória rizík patria pojmy nebezpečenstvo, ohrozenie, poškodenie, škoda, riziko. Procesné pojmy akými sú identifikácia, hodnotenie, posúdenie slúžia na popis postupov v rámci posudzovania rizík. Existujú pridružené pojmy akými sú akceptovateľné resp. zostatkové riziko. Všetky tieto pojmy sú definované nižšie v kontexte vývoja a prístupov v oblasti teórie rizík. Pre posúdenie rizík je pojem nebezpečenstvo nenahraditeľný. V nemecky hovoriacich krajinách je jasný rozdiel medzi pojmami Gefahr, Gefährdung a Risiko (Nebezpečenstvo, Ohrozenie a Riziko). Obdobou sú pojmy Danger, Hazardous situation, Hazard a Risk (Pozor, Nebezpečný stav, Riskovať a Risk).Všetky postupy posudzovania rizík, či už deduktívne alebo induktívne, pracujú s príčinnou závislosťou. Na obr. 2 je zobrazená táto závislosť.



Obr. 2 Príčinná závislosť

Posudzovanie rizík – špecifické

Analýza rizík je komplex opatrení zahŕňajúci nasledujúce činnosti:

- stanovenie hraníc systému – treba zvážiť, čo všetko sa bude analyzovať a v akom rozsahu. Môže sa napr. rozhodnúť, že sa nebude riešiť WAN komunikácie a táto oblasť bude prenechaná špecializovanej firme,
- identifikácia a ocenenie aktív – treba vytvoriť zoznam všetkých dôležitých častí systému a vykonať ich ohodnotenie na základe napr. ceny alebo časovej dostupnosti apod. Toto ocenenie musí zohľadniť účel a priority celého informačného systému,
- identifikácia a ocenenie hrozieb – treba zistiť aké hrozby pôsobia na systém a aká je pravdepodobnosť ich výskytu,
- identifikácia a ocenenie slabín (zraniteľnosť) – treba identifikovať slabé miesta systému, oceniť ich a rozhodnúť o ich eliminácii,
- profil a miera rizika – zahŕňa ocenenie dopadu jednotlivých hrozieb na konkrétne aktíva systému. Vo všeobecnosti možno tento proces nazvať stanovením miery ohrozenia systému,
- návrh protiopatrení – hlavným cieľom týchto opatrení je eliminovať dopad hrozieb na konkrétne časti systému.

Prístupy k analýze rizík

Podľa ISO/IEC TR 13335, pred začatím akýchkoľvek aktivít súvisiacich s analýzou rizík, by spoločnosť mala mať k dispozícii stratégiu pre túto analýzu. Jej podstatné zložky (metódy, techniky, atď.) by mali byť dokumentované v politike bezpečnosti spoločnosti. Prostriedky a kritériá pre výber metódy analýzy rizík by mali byť odsúhlasené. Stratégia analýzy rizík by mala zaistiť, že vybraný prístup k analýze rizík je vhodný pre dané prostredie, a že zameriava bezpečnostné úsilie tam, kde je to skutočne potrebné. Ďalej opísané alternatívy charakterizujú štyri rôzne prístupy k analýze rizík. Základným rozdielom medzi nimi je uplatňovaná hĺbka analýzy rizík. Keďže je zväčša príliš nákladné vykonávať detailnú analýzu rizík pre všetky systémy prevádzkované spoločnosťou a súčasne nie je vhodné venovať len malú pozornosť vážnym rizikám, je potrebné dosiahnuť rovnováhu medzi týmito alternatívami.

Okrem možnosti nerobiť nič, t. j. prijať fakt, že aktíva sú vystavené neurčitému množstvu rizík neznámej veľkosti a závažnosti, existujú základné možnosti pre analýzu rizík spoločnosti:

- použiť rovnaký základný prístup pre riešenie bezpečnosti všetkých systémov, bez ohľadu na riziká hroziace systémom a akceptovať, že zaisťovaná úroveň bezpečnosti nemusí byť vždy primeraná;
- použiť pre vykonanie analýzy rizík neformálny prístup a sústrediť sa na tie systémy, ktoré sú vnímané ako systémy vystavené vysokým rizikám;
- vykonať detailnú analýzu rizík s využitím formálneho prístupu pre všetky systémy;
- vykonať počiatočnú analýzu rizík „na vysokej úrovni“ s cieľom identifikovať systémy vystavené vysokým rizikám. Tam kde sú pre podnikateľské aktivity riziká kritické následne realizovať detailnú analýzu rizík týchto systémov a súčasne aplikovať základnú bezpečnosť pre všetky ostatné systémy.

Ak sa spoločnosť rozhodne nerobiť s bezpečnosťou nič alebo odloží implementáciu bezpečnostných opatrení, manažment by si mal byť vedomý možných následkov tohto rozhodnutia. Hoci takéto riešenie problému riadenia bezpečnosti nevyžaduje žiaden čas, peniaze, personál ani iné zdroje, má množstvo nevýhod. Ak si spoločnosť je istá nekritickou povahou svojich systémov, môže zotrvávať na pozícii nesystémovo nechránenej spoločnosti voči vážnym následkom.

Súčasne však platí, že spoločnosť nekoná v súlade s legislatívou, jej reputácia môže utrpieť

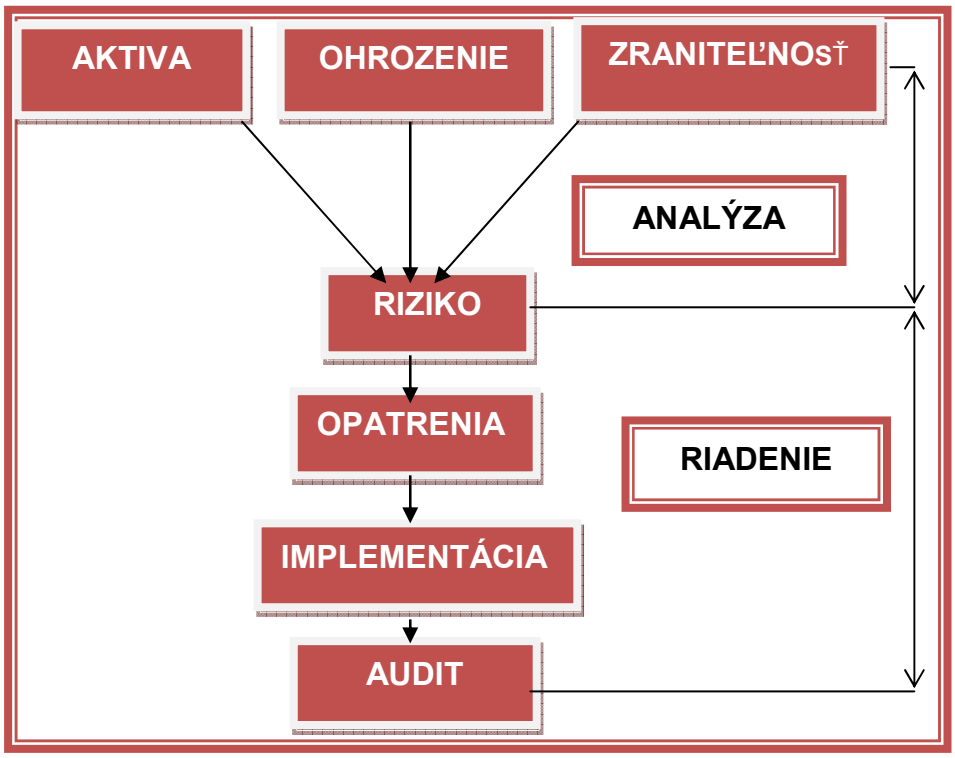
následkom narušenia bezpečnosti a môže sa ukázať, že zo strany spoločnosti neboli vykonané potrebné preventívne kroky.

Ak sa bezpečnosť týka spoločnosti len veľmi málo alebo ak spoločnosť nemá žiadne podnikateľsky kritické systémy, potom môže byť táto stratégia vhodná (dočasne akceptovateľná).

Procesy analýzy a riadenia sú znázornené na obr. 3.

Takáto spoločnosť je však v pozícii, že nepozná, aká dobrá alebo zlá je jej bezpečnostná situácia v skutočnosti, čo pravdepodobne nie je dobré riešenie pre väčšinu spoločností. Rozdelenie prístupov k analýze rizík je popísané v tab. 1.

Obr. 3 Procesy analýzy a riadenia



Tab. 1Rozdelenie prístupov k analýze rizík

	Základný prístup	Neformálny prístup	Detailná analýza	Kombinovaný prístup
Základný popis	Pri tejto alternatíve by spoločnosť mala aplikovať základnú bezpečnosť pre všetky systémy, výberom štandardných bezpečnostných opatrení. Škála štandardných bezpečnostných opatrení je navrhnutá v základných dokumentoch a praktických kódexoch vydaných jednotlivými štátmi.	Táto možnosť znamená vykonať neformálne pragmatické analýzy rizík. Neformálny prístup nie je založený na štruktúrovaných metódach, ale využíva vedomosti a skúsenosti jednotlivcov.	Detailná analýza rizík zahŕňa hĺbkovú identifikáciu a ohodnotenie aktív, ohodnotenie hrozieb pre tieto aktíva a ohodnotenie zraniteľností. Výsledky týchto aktivít sa potom použijú na ohodnotenie rizík a následne na identifikovanie opodstatnených bezpečnostných opatrení, implementovaním ktorých sa dosiahne požadovaná úroveň bezpečnosti systémov.	Analýza rizík na vysokej úrovni pre všetky systémy, koncentrujúc sa na hodnotu daných systémov z hľadiska spoločnosti a na vážne riziká, ktorým sú vystavené.
Výhoda	Na analýzu rizík a manažment rizík je potrebné len minimálne množstvo zdrojov, preto sa na výber, ak veľké množstvo systémov používaných v spoločnosti funguje v podobnom prostredí a ak ich bezpečnostné potreby sú porovnateľné, základné opatrenia môžu ponúknuť nákladovo-efektívne riešenie, pretože tie isté alebo podobné opatrenia môžu byť bez veľkého úsilia zavedené v mnohých systémoch, bezpečnostných opatrení vynaloží menej času a úsilia.	Zvyčajne nevyžaduje mnoho zdrojov ani času. Na vykonanie takejto neformálnej analýzy nie sú potrebné žiadne dodatočné odbornosti a je vykonávaná rýchlejšie než detailná analýza rizík.	Je pravdepodobné, že budú pre všetky systémy identifikované vhodné opatrenia; výsledky detailných analýz môžu byť použité pri riadení zmien v spôsobe zaisťovania bezpečnosti.	Použitie počiatočného rýchleho a jednoduchého prístupu. Pravdepodobne pomôže získať podporu vedenia, malo by byť možné rýchlo si vytvoriť strategickú predstavu o bezpečnostnom programe spoločnosti. Tento prístup je dobrou pomôckou pri plánovaní spoločnosti pre schválenie programu realizácie komplexu analýz rizík.
Nevýhoda	Ak je základná úroveň stanovená privysoko, v niektorých systémoch môže byť úroveň bezpečnosti nadmerná; ak je úroveň stanovená prinízko, v niektorých systémoch môže byť nedostatočná úroveň bezpečnosti, čo má za následok vyšší stupeň vystavenia rizikám; môžu byť ťažkosti s riadením bezpečnostne - relevantných zmien.	Bez určitého druhu formálneho prístupu alebo kompletného kontrolného zoznamu narastá pravdepodobnosť vynechania niektorých dôležitých detailov; do procesu analýzy môže byť zavedený určitý stupeň subjektivity; osobné predsudky posudzovateľa môžu ovplyvniť výsledky.	Získanie výsledkov vyžaduje značné množstvo času, úsilia a odborných znalostí. Je možné, že bezpečnostné potreby niektorého kritického systému budú ošetrené príliš neskoro, lebo všetky systémy IT sa posudzujú rovnako podrobne a na ukončenie analýz je potrebné značné množstvo času.	Počiatočné analýzy rizík vykonané na vysokej úrovni sú potenciálne menej presné, a preto niektoré systémy nemusia byť správne identifikované ako systémy, vyžadujúce detailnú analýzu rizík.

Hodnotenie požiadaviek a hrozieb

Pre efektívny výber vhodných opatrení je potrebné pochopiť bezpečnostné záujmy podnikových operácií podporovaných posudzovaným systémom. S pomocou identifikácie bezpečnostných záujmov, berúc do úvahy relevantné hrozby, ktoré by mohli ohroziť tieto záujmy, môžu byť vybrané vhodné bezpečnostné opatrenia (tab. 2.)

Tab. 2Bezpečnostné záujmy/hrozby

Strata	Dôvernosti	Integrity	Dostupnosti	Zodpovednosti	Autenticity	Spoľahlivosti
Môže viesť ku	strate dôvery verejnosti alebo pokazeniu verejného imidžu spoločnosti;	prijímaniu nesprávnych rozhodnutí,	prijímaniu nesprávnych rozhodnutí,	manipulácii systémov používateľmi,	podvodu,	podvodu,
	právnym záväzkom, vrátane tých, ktoré môžu vzniknúť z porušenia legislatívy na ochranu dát;	podvodu,	neschopnosti vykonávať kritické úlohy,	podvodu,	použitiu neplatných dát v platnom procese, čo by viedlo k zavádzajúcemu výsledku,	strate podielu na trhu,
	negatívnym účinkom na politiku organizácie;	narušeniu podnikateľského procesu,	strate dôvery verejnosti alebo zničeniu verejného imidžu,	priemyselnej špionáži,	manipulácii organizácie zvonka,	demotivácii pracovníkov,
	ohrozeniu osobnej bezpečnosti;	strate dôvery verejnosti alebo pokazeniu verejného imidžu,	finančným stratám,	nesledovateľným činnostiam,	priemyselnej špionáži,	nespoľahlivým dodávateľom,
	k finančným stratám	finančnej strate	právnym záväzkom, vrátane tých, ktoré môžu vzniknúť z porušenia legislatívy na ochranu dát a z nedodržania zmluvných termínov,	falošným obvineniam	falošným obvineniam,	strate dôvery zákazníkov,
		právnym záväzkom, vrátane tých, ktoré môžu vzniknúť z porušenia legislatívy na ochranu napr. osobných dát.	značným nákladom na obnovu	právnym záväzkom, vrátane tých, ktoré by mohli vzniknúť z porušenia legislatívy na ochranu dát.	právnym záväzkom, vrátane tých, ktoré by mohli vzniknúť z porušenia legislatívy na ochranu dát.	právnym záväzkom, vrátane tých, ktoré by mohli vzniknúť z porušenia legislatívy na ochranu dát.

Bezpečnostné záujmy/hrozby môžu zahŕňať:

- stratu dôvernosti,
- stratu integrity,
- stratu dostupnosti,
- stratu zodpovednosti,
- stratu autenticity a
- stratu spoľahlivosti.

Cieľom zabezpečenia a základnými bezpečnostnými komponentmi je zabezpečenie proti útoku na tieto bezpečnostné rysy systému:

- dostupnosť (aktíva sú dostupné iba autorizovaným subjektom),
- dôvernosť (udržanie aktív v tajnosti, zabránenie odhaleniu dôverných aktív a zamedzenie prístupu neautorizovaným subjektom, dôvernosť procesov komunikácie),
- integrita (dôveryhodná informácia, jej prenos a ochrana),
- autenticita (aktíva nesmú byť modifikované a/alebo rušené neautorizovaným spôsobom, je overiteľný deklarovaný pôvod),
- spoľahlivosť (všetko funguje tak ako má fungovať),
- zodpovednosť (odoslanie správy, prijatie správy, autorstvo dokumentu).

Záver

Opísaný výber opatrení podľa bezpečnostných záujmov a hrozieb možno použiť nasledovne:

- prvým krokom je identifikovať a ohodnotiť bezpečnostné záujmy organizácie/ spoločnosti/podniku. Mali by sa posúdiť požiadavky na dôvernosť, integritu, dostupnosť, zodpovednosť, autenticita a spoľahlivosť. Sila a počet vybraných opatrení by mali byť primerané ohodnoteným bezpečnostným záujmom,
- pre každú z bezpečnostných požiadaviek sa uvedú typické hrozby a pre každú hrozbu sa navrhnú bezpečnostné opatrenia v závislosti na posudzovanom systéme .

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ISO/IEC 73:2002 – Risk Management. Vocabulary. Guidelines for use in standards.
ISO/IEC TR 27000:2009 – Information technology. Security techniques. Code of practice for information security management
PROCHÁZKOVÁ,D., ŘÍHA, J. Krizové řízení. MV- generální ředitelství Hasičského záchranného sboru České republiky. ISBN: 80-86640-30-2
Kolektív autorov - Zranitelnost kritickej infrastruktúry. VŠB-TU Ostrava, 2008
SGS Interný audit podľa normy ISO/IEC 27001:2005, Príručka účastníka, 2006
ISO/IEC TR 18044:2004 – Information technology. Security techniques. Information security incident management.
JONES, J. A. CISSP, CISM, CISA, An Introdukction to Factor Ananlysis of Information Risk (FAIR) [cit. 15.5. 2009].Dostupné na internete <http://riskmanagementinsight.com/media/docs/Fair_introduction.pdf.>.
Zákon Národnej rady Slovenskej republiky č. 42/1994 Z. z. o civilnej ochrane obyvateľstva.
Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti.
ORAVEC, M. Posudzovanie rizík: Bezpečnosť strojných systémov, bezpečnosť chemických prevádzok, bezpečnosť líniových stavieb. Ostrava: SPBI, 2008. ISBN 978-80-7385-043-2.
Legislatíva Európskej únie [online]. [cit. 15.5. 2009]. Dostupné na internete <http://www.euroinfo.gov.sk/index/go.php?id=272.>
Výber Smerníc Európskej únie [online]. [cit. 1.5. 2009]. Dostupné na internete <http://www.telecom.gov.sk/externe/legeu/zoznam.htm.>
Medzinárodné bezpečnostné normy [online]. [cit. 2.5. 2009]. Dostupné na internete <http://www.euroiso.sk/.>
ISO/IEC TR 13335-1:2004 – Information technology - Guidelinesfor the management of IT Security Part 1: Concepts and models for IT Security
Zbierka zákonov Slovenskej republiky [online]. [cit. 26.5. 2009]. Dostupné na internete <http://www.zbierka.sk/.>
Zákon Národnej rady Slovenskej republiky č. 461/2003 Z. z. o sociálnom poistení.

Zákon č. 513/2006 Z. z. o sociálnom poistení. Úplné znenie zákona č. 461/2003 Z. z. o sociálnom poistení, ako vyplýva zo zmien a doplnení vykonaných zákonom.
Ústavný zákon č.227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.
Vyhláška Ministerstva obrany Slovenskej republiky č. 353/2004 Z. z., ktorou sa ustanovujú kritériá na zaradenie objektov obrannej infraštruktúry do kategórie objektov osobitnej dôležitosti a do kategórie ďalších dôležitých objektov.
Sektory kritickej infraštruktúry [online]. [cit. 26.5. 2009]. Dostupné na internete < http://www.minv.sk/?ochrana-kritickej-infrastruktury.>
Uznesenie vlády SR č. 120 zo 14. februára 2007 k návrhu Koncepcie kritickej infraštruktúry v Slovenskej republike a spôsobu jej ochrany a obrany.
PROCHÁZKOVÁ,D. Bezpečnost lidského systému. Edice SPBI Ostrava 2007. ISBN: 978-80-86634-97-5.
ORAVEC, M. Posudzovanie rizík: Bezpečnosť strojných systémov, bezpečnosť chemických prevádzok, bezpečnosť líniových stavieb. Ostrava: SPBI, 2008. ISBN 978-80-7385-043-2.
TKÁČ, V., MARCHEVKA, P., CHÚPEK,A. Terminologická príručka krízového manažmentu v rezorte ministerstva obrany. Bratislava, 2002, s. 15
STN IEC 1025 Analýza stromu poruchových stavov.
HANÁČEK, P., STAUDEK, J. 2000. Bezpečnost informačních systémů, Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologi., Úřad pro státní informační systém 2000.
LÁTAL,I.a kol. Ochrana informací, dát a počitačových systému. EUROUNION, Praha, 1999.
STRAUS,J. Bezpečnostní teorie a praxe. Policejní akademie ČRv Praze 2007. ISSN 1801-8211.
BUZALKA,J. Vybrané otázky teórie krízového manažmentu a civilná ochrana. Akadémia Policajného zboru v Bratislave 2001. ISBN: 80-8054-165-5.
LÁTAL, I., ŠTANTEJSKÝ, M. Bezpečnostní zásady ochrany podniku. Praha 2004.
Zákon č. 290/2005Z. z., ktorým sa dopĺňa zákon č. 50/1976 Zb. o územnom plánovaní a stavebnom poriadku (stavebný zákon) v znení neskorších predpisov a o doplnení niektorých zákonov.
Ochrana objektov spoločenského významu [on line]. [cit. 2.5. 2009]. Dostupné na internete<http://www.minv.sk/?ministerstvo-vnutra&subor=1142.>
Návrh smernice rady ES o identifikácii a označovaní európskej kritickej infraštruktúry a zhodnotení potreby zlepšovať jej ochranu. [on line]. [cit. 10.3. 2009]. Dostupné na internete<www.ecb.eu/ecb/legal/pdf/com2006_0787cs01.pdf,.>
Zákon Národnej rady Slovenskej republiky č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.
KRATOCHVÍLOVÁ, D. Typy mimoriadnych alebo krízových situácií. Zborník mezinárodní konference Ochrana obyvatel 2001. Ostrava, VŠB. ISBN 80-86634-86-8
SINAY,J. Riziká technických zariadení – manažérstvo rizika. TU Košice, VSŽ Košice, 1997. ISBN 80-967783-07.
Vyhláška Ministerstva obrany Slovenskej republiky č.353/2004 Z. z., ktorou sa ustanovujú kritériá na zaradenie objektov obrannej infraštruktúry do kategórie objektov osobitnej dôležitosti a do kategórie ďalších dôležitých objektov.
BARTLOVÁ, I., BALOG, K. Analýza nebezpečí a prevence prúmyslových havárií. Edice SPBI Ostrava 2007. ISBN: 978-807385-005-0.
REKTORÍK, J. a kol.. Krizový managment ve verjnej správě, teoriea praxe. Ekopress, s.r.o., Praha 2004. ISBN:80-86119-83-1.
Zákon č. 659/2005 Z. z., ktorým sa mení a dopĺňa zákon č. 291/2002 Z. z. o štátnej pokladnici a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa mení a dopĺňa zákon č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
Zákon Národnej rady Slovenskej republiky č. 461/2003 Z. z. o sociálnom poistení.
Zákon č. 677/2006 Z. z., ktorým sa mení a dopĺňa zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a o zmene a

doplnení zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov.
Zákon č. 513/2006 Z. z. o sociálnom poistení. Úplné znenie zákona č. 461/2003 Z. z. o sociálnom poistení, ako vyplýva zo zmien a doplnení vykonaných zákonom.
ZÁKON č. 555/2007 Z. z., ktorým sa mení a dopĺňa zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.
Analýza územia okresu Bratislava I.
Strategické zámery [online]. [cit. 26.5. 2009]. Dostupné na internete <http://www.socpoist.sk/strategicke-zamery-cinnosti-socialnej-poistovne/17139s.>
Analýza súčasného stavu strategických zámerov [online]. [cit. 29.5. 2009]. Dostupné na internete <http://www.socpoist.sk/spravy-o-plneni-strategickych-zamerov-cinnosti-socialnej-poistovne/17143s.>
PORADA,V., STACHO, P. a kol. Úvod do teórie činnosti policajno-bezpečnostných orgánov. Bratislava APZ 2000.
TKÁČ,V., MARCHEVKA, P., CHÚPEK,A. Terminologická príručka krízového manažmentu v rezorte ministerstva obrany. Bratislava, 2002.
OHSAS 18002:2000: Occupational health and safety management system –Guidelines for the implementation of OHSAS 18001, British Standards institution, London, 2000.
PROCHÁZKOVÁ,D. Strategie řízení bezpečnosti a udržiteného rozvoje území. Policejní akadémie České republiky v Praze 2007. ISBN 978-807251-243-0.
Bezpečnostný projekt [online]. [cit. 8. 4. 2009] Dostupné na internete <:http://www.proenergy.sk/bezpecnostny-manazment/komplexna-bezpecnost-podnikov.>
BUZALKA, J. Vybrané otázky teórie krízového manažmentu a civilná ochrana. Akadémia Policajného zboru v Bratislave 2001. ISBN: 80-8054-165-5.
STN EN ISO Bezpečnosť strojov , princípy posudzovania rizika 8/1998.
STN EN ISO 12100-1 Bezpečnosť strojov – Základné termíny, všeobecné zásady konštruovania strojov. SÚTN 2003.
Perimetrická ochrana [online]. [cit. 2.3. 2009]. Dostupné na internete <: http://www.fittich.sk/download/web%20site/EZS/Detektory/Defensor.pdf.>
Systém organizačných opatrení fyzickej bezpečnosti [online].[cit.10. 4. 2009] Dostupné na internete <:http://www.securityrevue.com/tbm/part1_o.html#ochrana-objektu.>
STN EN 50131-1 Poplachové systémy, Elektrické zabezpečovacie systémy, Časť 1: Všeobecné požiadavky.
Bloková schéma Elektrickej zabezpečovacej signalizácie [online]. [cit. 2009-05-12]. Dostupné na internete <:http://www.alarm.szm.sk/images/alarm-schema.jpg.>
STN IEC 60300-3-9, Manažérstvo spoľahlivosť, časť 3, oddiel 9, Analýza rizika technických systémov. SÚTN. 12/2000.
STN EN 50131-1 Poplachové systémy. Elektrické zabezpečovacie systémy.
Optimálna bezpečnosť [online]. [cit. 7. 2. 2009] Dostupné na internete <:http://www.securityrevue.com/tbm/images/optimalna_bezpecnost.gif.>
Schéma diaľkového ovládania a monitorovania RIZ [online]. [cit. 4. 3. 2009] Dostupné na internete<:http://www.nextriraone.sk/.>
STN 33 1500: 2002, Vykonávanie revízií elektrických zariadení.
Vyhláška MPSVR č. 718/2002 Z. z. na zaistenie bezpečnosti a ochrany zdravia pri práci a bezpečnosti technických zariadení.
Monitorovanie riadiaceho a identifikačného zariadenia [online]. [cit. 15. 5. 2009]. Dostupné na internete <:http://www.tsoft.cz.>
KELLER, J. Sociológie a ekológie. Sociologické nakladatelství, Praha 1997.
Zariadenia Uzavretého televízneho okruhu [online]. [cit. 6. 6. 2009]. Dostupné na internete <:http://www.hwgroup.cz/dowland/PortBox_IO_Controler_cz.>
Kamery a príslušenstvo [online]. [cit. 9. 5. 2009]. Dostupné na internete <:http://www.opalmultimedia.sk.>

Zariadenia Uzavretého televízneho okruhu [online]. [cit. 8.4. 2009]. Dostupné na internete <:http://www.hwgroup.cz/dowland/PortBox_IO_Controler_cz.>
Videoserver[online]. [cit. 10. 2. 2009]. Dostupné na internete <:http:// www.emergency.cz.>
STN EN 50132-7: 2003, Poplachové systémy, Sledovacie systémy CCTV na používanie v bezpečnostných aplikáciách, Časť 7: Pokyny na používanie
STRNÁD,O.,OLELJNÍK,A.,STRNÁD,A.ml.: Životný cyklus IS, Testovanie, metodika pre testovanie. Bratislava, 2002.
Systém kontroly vstupov [online]. [cit. 13. 4. 2009]. Dostupné na internete <:http:// www.expan.cz.>
Schéma architektúry systému kontroly vstupov [online]. [cit. 14. 3. 2009]. Dostupné na internete <:http:// www.olympo.cz.>
STN EN 1143-1 Bezpečnostné úschovne objekty Požiadavky, klasifikácia a metódy skúšania odolnosti proti vlámaniu.
ADAMEC, V. Bezpečnostní managementí. Časopis 112, 2003, č.1, str. 10-11, ISSN 1213-7057.
Vyhláška MV SR č.726/2002 Z. z., ktorou sa ustanovujú vlastnosti EPS, podmienky jej prevádzkovania a zabezpečenia jej pravidelnej kontroly.
Vyhodnotenie signálu narušenia [online]. [cit. 2009-06-16]. Dostupné na internete <:http:// www.emergency.cz.>
BALOG,K. Hasiace látky a jejich technológie. Edice SPBI Ostrava, 2004. ISBN 80-86634-49-3.
STRNÁD,O. Budovanie Komplexného systému riadenia bezpečnosti IS, metodický materiál. Bratislava, 2000.
Schéma zapojenia systému security monitoring [online].[cit. 17. 6.2009]. Dostupné na internete <:http://www.ebr.org.>
Pulty centrálnej ochrany (PCO) [online]. [cit. 17. 5.2009]. Dostupné na internete <:http:// www.rts.sk.>
ROSENAU,M. D.Řízení projektů, řízení aplánovaní. Computer Press, a.s. 2007 ISBN: 978-80-251-1506-0.
SMEJKA,L.V.,RAIS,K. Řízení rizik. Grada Publishing a.s., Praha 2003. ISBN: 80-247-0198-7.
NEMEC, V. Projektový management. GRADA Publishing, Praha 2000.
GELENEKY,M. Metodika činnosti pracoviska analýzy a manažmentu rizík. Bratislava 2008.

ADRESA AUTORA

Ing. Alojz BARTEK, PhD.
Wüstenrot stavebná sporiteľňa, a. s., Grösslingova 77, 824 68 Bratislava, Slovenská republika
e-mail: alojz.bartek@gmail.com

RECENZIA TEXTOV V ZBORNÍKU
Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS
Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.