O bezpečnosti podniku

Imrich Dufinec[1]

On Enterprice Security

ABSTRAKT

Pre riadenie bezpečnosti podniku treba implementovať do praxe niekoľko kľúčových štandardizovaných postupov. Výber postupov závisí od prijatej bezpečnostnej politiky, cieľov a stratégie dosahovania bezpečnostných cieľov. Kľúčom úspešného riadenia bezpečnosti podniku je bezpečnostný systém, ktorého hlavným záujmom je minimalizácia rizík podniku vo všetkých aspektoch jeho ohrozenia. Bezpečnostný systém môže byť s manažérstvom podniku spojený ako integrovaný manažérsky systém alebo môže fungovať od manažérstva podniku oddelene ako externá činnosť. Nástrojom oboch foriem fungovania bezpečnostného systému je manažérstvo rizík. Riadenie bezpečnosti podniku je certifikovateľné v rozsahu relevantného integrovaného manažérskeho systému.

ABSTRACT

For enterprise security management practices shell to be implemented in a number of key standardized procedures. The procedures selected depend on the adoption of a security policy, objectives and strategies for achieving safety objectives. The key success of enterprise security management is a security system whose main concern is to minimize the risks of concern in all aspects of his threat. The security system can be connected to the management of the company as an integrated management system or can operate from management business separately as an external activity. Tool for both forms of the functioning of the security system is Risk management. Enterprise security management is certifiable to the extent relevant integrated management system.

Kľúčové slová: Bezpečnosť podniku, bezpečnostný manažér, ochrana aktív, integrovaný manažérsky systém, ohrozenie a riziká podniku.

Key words: *Business security, security manager, protection of assets, integrated management system, threats and risks facing a business or company.*

1. ÚVOD

Podnik realizuje svoje podnikateľské zámery a uskutočňuje procesy tvorby a predaja svojej produkcie. Na uskutočnenie svojich zámerov uplatňuje **manažérsky systém** prostredníctvom svojho manažmentu. Sprievodným znakom činnosti podniku je všade prítomné podnikateľské **riziko**, či ohrozenie jeho bezpečnosti, vo všetkých jej relevantných prejavoch. Môžu to byť napr. environmentálne aspekty, odpady, znečisťovanie vody a kontaminácia pôdy, krádeže hmotného i nehmotného majetku , sabotáž, únik osobných a inak citlivých údajov, útoky hackerov, daňové podvody, hluk, strata trhov, konkurencia, riziká pracovného prostredia a pod. Toto všetko tvorí **bezpečnostné prostredie podniku**.

Manažérsky systém prostredníctvom bezpečnostnej politiky, cieľov a stratégie odpovedá na bezpečnostné prostredie podniku ako ucelený **bezpečnostný systém**. Podnik spolu s jeho bezpečnostným prostredím sa tak stáva stredobodom záujmu bezpečnostného systému. Bezpečnostný systém má za úlohu zabezpečiť minimalizáciu rizík a ohrození podniku a zabezpečiť tak bezpečnosť podniku vo všetkých jej relevantných prejavoch.

Bezpečnosť podniku, ako objektu v ktorom prebiehajú procesy realizácie jeho produktu, vnímame v zásade ako dostatočnosť bezpečnostného systému čeliť hrozbám znižovania alebo dokonca straty hodnôt aktív podniku a bezpečnosti osôb v ňom pôsobiacich.

[1] Dr.h.c. doc. Ing. Imrich Dufinec, CSc., MBA, IDEEX PLUS, s.r.o., Mlynárska 15, 040 01 Košice: www.ideex.sk, dufinec@ideex.sk Mimoriadny profesor Dr.habil. WSH Kielce, Poľsko,

Aktíva podniku predstavujú majetok podniku, hmotného i nehmotného charakteru[2], ktorý je v majetkovej súvahe aktív a pasív krytý kapitálom ako jeho pasíva[3].

Majetok podniku je teda všetko to, čím podnik podniká, uskutočňuje svoje zámery. Pretváranie majetkovej podstaty procesmi, ktoré sú nositeľmi niektorých z inherentných rizík, stotožňuje toto podnikové manažérstvo s bezpečnostným manažérstvom relevantných rizík, pretože relevantné riziká sú prevažne spojené s realizačnými procesmi produktov podniku.
Aj keď niektoré riziká nie sú bezprostredne spojené s realizačnými procesmi pretvárania majetkovej podstaty podniku a sú riadené externými bezpečnostnými systémami, sú súčasťou tej istej majetkovej podstaty, ktorú podnik chráni. Prepojenie vnútorných bezpečnostných systémov, alebo integrovaného systému s vonkajším bezpečnostným systémom, podnik vytvára komplexné riadenie bezpečnosti podniku, čím komplexne chráni osoby a majetok nachádzajúce sa v podniku. Komplexná bezpečnosť podniku nie je stavová ale toková veličina, meniaca sa so zmenou majetkovej podstaty podniku[4].

2. BEZPEČNOSTNÝ SYSTÉM

Bezpečnostný systém predstavuje nástroj tvorby a realizácie bezpečnostnej politiky v danom bezpečnostnom prostredí podniku v reálnom čase.

Pokiaľ je bezpečnostný systém riadený vlastným manažmentom, je manažérsky od podniku odtrhnutý a pre podnik vykonáva, ako predmet svojho záujmu, **platenú externú službu**. Najznámejším príkladom sú súkromné bezpečnostné služby ako outsorcovaná činnosť. Môže sa týkať tak fyzickej ochrany ako aj ochrany duševného vlastníctva, environmentálneho manažérstva, či BOZP a pod., ako chránené záujmy. Ide o **model outsorcovanej bezpečnosti podniku.**

Pokiaľ je bezpečnostný systém riadený podnikovým manažmentom, potom je bezpečnostné manažérstvo totožné s podnikovým manažérskym systémom, pričom podnik sám sebe, prostredníctvom vlastného podnikového manažmentu poskytuje bezpečnostnú službu, ako **vlastnú, internú službu I**ntegrovaným **M**anažérskym **S**ystémom (IMS), nazývaným tiež aj **G**enerickým **M**anažérskym **S**ystémom (GMS). Je charakteristický aplikovanou normou manažérstva kvality podľa ISO 9001, pričom ďalšie štandardy ISO 14001, ISO 27001, resp. OHSAS 18001 a ďalšie, sú generickými normami k norme ISO 9001. Chránené záujmy sú pri tom podobne ako u predchádzajúceho modelu viazané, napr. kvalita a bezpečnosť produkcie požiadavkami odberateľov a možnosťami dodávateľov, environmentálne manažérstvo požiadavkami spoločnosti a verejnosti, bezpečnosť pri práci pracovníkmi a legislatívou, a napokon majetok a kapitál, resp. aktíva a pasíva požiadavkami akcionárov a majiteľov podniku. Ide o **model integrovanej bezpečnosti podniku**.

Modely outsorcovanej a integrovanej bezpečnosti sú dva základné modely, pričom v bežnej praxi podnikania sa medzi uvedenými modelmi riadenia bezpečnosti môžu nachádzať rôzne, viacmenej kombinované modely uvedených dvoch.

3. MANAŽÉRSTVO RIZÍK

Podnikateľské prostredie podniku, v ktorom sa osoby a majetok nachádzajú, je nositeľom rôznych rizík a ohrození týchto osôb a majetku. To mu dáva **charakter bezpečnostného prostredia**. Ako už bolo povedané, podnik toto bezpečnostné prostredie zvláda riadením, t.j. primeraným bezpečnostným systémom, aplikovaným bezpečnostným

[2] Aktíva podniku, napr. peniaze, zásoby, stroje, informácie, know-how,...
[3] Pasíva podniku, napr. základné imanie, príjmy, úvery, záväzky, fondy,...
[4] Na rozdiel od pojmu „bezpečný podnik“, ako stavová veličina, ktorý vyjadruje stav a má skôr certifikačný a komerčný význam.

manažérstvom. Nutné bezpečnostné opatrenia vykonáva v súlade s prijatou bezpečnostnou politikou a celkovou stratégiou podnikania, prostredníctvom realizovaných procesov bezpečnostného systému.

Riziko vyjadruje pravdepodobnosť vzniku neistého javu s neistými dôsledkami, založenú na posúdení a hodnotení faktov, ktoré vyžadujú primerané riadenie[5].

V prípade orientácie na negatívne javy a negatívne dôsledky hovoríme o čistom riziku **ohrozenia**, čo vyžaduje náležitý manažment a manažérstvo[6].

S cieľom byť na trhu úspešným[7], je potrebné rizikám predchádzať, riziká zmenšovať alebo riziká prenášať na tretiu osobu. Manažérstvo rizík tak predstavuje čistú formu prevencie, profylaktiky, ktorú podnik vytvára aby predchádzal negatívnym javom a negatívnym dôsledkom, v ktoromkoľvek aspekte ľubovoľnej zložky komplexnej bezpečnosti podniku. V manažérstve rizík sa uplatňujú štandardizované postupy, predovšetkým norma manažérstva rizík ISO 31000 a norma techník manažérstva rizík ISO 31010.

V prípade, že sa naplní pravdepodobnosť negatívneho javu s negatívnymi dôsledkami, vtedy hovoríme o **incidente**. Riešenie incidentov je jedným zo základných činností bezpečnostného manažérstva, opäť v ktoromkoľvek bezpečnostnom aspekte ľubovoľnej parciálnej zložky komplexnej bezpečnosti podniku[8]. Typickými príkladmi incidentov sú incidenty informačnej bezpečnosti, napr. napadnutie informačného systému vírusmi, a pod.

4. AUDIT BEZPEČNOSTNÉHO SYSTÉMU

Audit bezpečnostného systému je auditom manažérskeho systému a prebieha podľa príslušnej manažérskej normy, pričom predmetom auditu sú aj riziká ohrozujúce relevantnú zložku bezpečnosti[9] .

Audit predstavuje systematický, nezávislý, zdokumentovaný proces získavania dôkazov preverovania a ich objektívneho vyhodnocovania za účelom posúdenia spravného fungovania predmetu preverovania. Je to predovšetkým manažérsky nástroj spätnej väzby na monitorovanie a overovanie efektívneho zavedenia politiky podniku, s jej príslušnými aspektmi, napr. aspektom bezpečnosti.

V prípade, že bezpečnostný systém je stotožnený s manažérskym systémom podniku[10], to znamená, že manažment podniku reaguje na účinky príslušného bezpečnostného prostredia sám, potom audit bezpečnostného systému je totožný s auditom manažérskeho systému tak, ako bolo uvedené. Pokiaľ sa audit týka integrovaného manažérskeho systému, audit sa vykoná ako kombinovaný audit IMS pomocou kombinovaných checklistov, zahŕňajúcich príslušné normy manažérskeho systému, ako aj relevantné riziká a ohrozenia[11].

V prípade, že bezpečnostný systém nie je stotožnený s manažérskym systémom podniku, to znamená, že tento je od manažérskeho systému podniku odtrhnutý, potom audit bezpečnostného systému má svoje vlastné zásady a princípy, ktoré môžu byť od auditu manažérskeho systému podniku odlišné. Môže sa to týkať, napr. bezpečnostného systému ochrany osôb a majetku, ako nakupovanej služby SBS[12]. Audit bezpečnostného systému bude závisieť predovšetkým od zadefinovaného bezpečnostného systému a jeho manažérstva, vrátane všetkých nástrojov, prostriedkov a foriem. Príznačné pre takýto audit je okrem

[5] ISO 31000 – Manažérstvo rizík
[6] Pozri ISO 31000 – Manažérstvo rizík, ISO 31010 – Techniky manažérstva rizík, atď.
[7] Z pohľadu komplexnej bezpečnosti
[8] Napr. krádež hmotného majetku, útok hackera na počítačovú sieť, a pod.
[9] ISO 9001/ISO 31000, ISO 14001/ISO 31000, ISO 9001/ISO 27001,... atď
[10] Monotematickým alebo integrovaným
[11] ISO 9001/IS0 14001/ISO 31000, ISO 9001/OHSAS 18001, ISO 9001/ISO 14001/OHSAS 18001,...atď.
[12] **S**úkromná **B**ezpečnostná **S**lužba

manažérskej častí[13] preverovanie funkcií mechanických a technických zabezpečovacích prostriedkov, ktoré podľa ich zložitosti môžu byť jednoduché ale i integrované. Každý z nich vyžaduje samostatný audit jeho spôsobilosti, funkčnosti v systéme a spoľahlivosti.

Audit ma svoju logickú štruktúru preverovania a vždy končí písomnou správou o výsledku. Ako proces je v manažérskom systéme lokalizovaný do časti merania, analýzy a zlepšovania a je vstupom do procesov trvalého zlepšovania nápravnými a preventýnymi opatreniami.

Výstupy z auditu a nasledné opatrenia sú predmetom preskúmania manažmentom, ktoré je rovnako ako interný audit obligatórnou povinnosťou manažmentu, vedúcej k trvalému zlepšovaniu.

5. ZÁVER

Na základe reálneho pohľadu z početných auditov, osobných skúsenosti a štúdia súčasných podmienok riadenia podnikov možno povedať, že integrácia parciálnych zložiek bezpečnosti podniku siaha od najslabšej integrácie, t.j. integrácie dvoch manažérskych, resp. bezpečnostných systémov, po integráciu maximálne štyroch až šiestich manažérskych, resp. bezpečnostných systémov. Integrácia sa týka najmä systémov podľa noriem ISO 9001, ISO 14001, ISO/TS 16949, ISO/IEC 17025, ISO 31000, STN OHSAS 18001, ISO 50000, ISO 27001, ISO 21500 a ďalších generických noriem podľa špecializácie a to vždy v rôznej kombinácií, pričom počet noriem neprekračuje číslo šesť.

Bezpečnostný systém ochrany osôb a majetku podniku, ako taký, je zatiaľ ťažko integrovateľný, bez ohľadu na prijatý model riadenia. Jeden dôvod je odtrhnutie od manažérskeho systému podniku, druhý dôvod je, že SBS nie sú riadené štandardne a nie sú ani certifikované. Pre integráciu musia byť splnené obe podmienky, t.j. certifikácia a stotožnenie bezpečnostného systému s manažérskym systémom podniku. Toto by bolo možné spĺňať pri ochrane osôb a majetku vlastnou bezpečnostnou zložkou, zahrnutou do certifikovaného manažérskeho systému. Podniky väčšinou túto službu nakupujú. Kritériom pre takúto voľbu sú totiž ekonomické výhody outsorcingu[14]. Na druhej strane, podniky, ktoré majú vlastnú bezpečnostnú zložku a sú certifikované, napr. podľa ISO 9001, majú manažérsky systém zadefinovaný s výlukou bezpečnostnej služby pre jej špecifičnosť. Vzniká začarovaný kruh, ktorý manažment nerieši predovšetkým z dôvodov vysokej zaangažovanosti predovšetkým na výrobe a predaji a nízkeho bezpečnostného povedomia komplexne chápanej bezpečnosti podniku.

LITERATÚRA

[1] DUFINEC, Imrich. *Bezpečnosť podniku. Vysokoškolská učebnica,* VŠBM Košice 2014, v tlači, počet strán 102.

[2] HRUBEC, J – VIRČÍKOVÁ, E. – DUFINEC, I. a kol: *Integrovaný manažérska systém*, SPU Nitra, 2009, ISBN: 798-80-552-0231-0

[3] JURAN, J. M.: *Quality Control Handbook*, 4. vydanie, 1808 str. McGraw-Hill Book Company, New York, 1988. ISBN 0-07-033176-6

[4] MASING, Walter: *Handbuch Qualitätsmanagement.* Carl Hanser Verlag München, 5. prepracované vydanie, 2007. 1063 s. ISBN 978-3-446-40752 7

[5] MESÁROŠ, Marián: *Ochrana osôb a majetku v kontexte ochrany ľudských práv a chránených záujmov*, VŠBM Košice, 2012, ISBN: 978-80-224-1240-7

[13] Napr. podľa ISO 9001

[14] Podniky zväčša volia cestu outsorcingu, ako cestu budovania bezpečnostného útvaru