

MANAŽÉRSTVO RIZIKA LOGISTICKÝCH SYSTÉMOV

Jozef Gnap¹ – Drahomír Géc²

Význam bezpečnostných systémov v rámci celého výrobného distribučného reťazca vzrástol po 11. septembri 2001 aj v dôsledku ďalších udalostí. Globálne „zosieťovanie“ a z neho vyplývajúce tovarové toky poskytujú priestor pre teroristické útoky, ktoré si okrem zámerného zabíjania ľudí kladú za cieľ aj oslabenie svetovej ekonomiky. Zničenie plne naloženej kontajnerovej lode by mohlo spôsobiť obrovské hospodárske škody. Z toho vyplývajúce zastavenie kontajnerovej dopravy ako reakcia na útoky alebo jej vážne ohrozenie by mohlo dokonca spôsobiť ťažko odhadnuteľné straty. Kontajnery vo veľkých prístavoch sa čoraz viac kontrolujú na prítomnosť výbušnín. Kontajnery smerujúce do USA sa „scanujú“ už skoro na 100 %. Väčšina nákladov, ktoré smerujú do iných kútov sveta sa však nakladá a prekladá bez kontroly. Dokonca aj v oblasti leteckej dopravy sa stále vyskytujú bezpečnostné medzery pri kontrole osôb a príručnej batožiny. Príbúdajúce bezpečnostné opatrenia, zároveň sa zvyšujú náklady na dopravu.

Okrem terorizmu ohrozujú bezpečnosť logistického reťazca aj krádeže. Ročne podľa odhadov je rozsah priamych škôd spôsobených krádežami v hodnote 50 až 60 miliárd dolárov. Okrem materiálnych škôd ovplyvňujú krádeže aj stabilitu dodávateľského reťazca a spôsobujú zvýšenie poisťného. K tomu treba pripočítať i mieru pašovania, ktorá predstavuje ročne jedno až tri percentá celosvetového obchodu. Tieto čísla by sa dali znížiť účinnými kontrolami. Aby sa predišlo výslednému konfliktu medzi zvýšenou bezpečnosťou dosahovanou zavedením rozsiahlych kontrol nákladu a rýchlosťou v dodávateľskom reťazci, je úlohou logistiky integrovať do reťazca procesov efektívne bezpečnostné systémy tak, aby im neprekážali a nespomaľovali ich [1].

Na zníženie týchto rizík môžu prispieť aj procesy aplikované do procesov logistických a zasielateľských firiem. Tu môže byť veľmi dobrou pomôckou STN 01 0380 Manažérstvo rizika [3].

Manažérstvo rizika je interaktívny proces skladajúci sa z dobre definovaných krokov, ktoré svojou postupnosťou podporujú lepšie rozhodovanie tým, že prispievajú k lepšiemu pochopeniu rizík a ich následkov.

Proces manažerstva rizika možno použiť na akúkoľvek situáciu, v ktorej by mohol zavážiť neželateľný výstup alebo kde sa zistia takéto možnosti. Tí, čo prijímajú rozhodnutia, musia poznať možné výstupy a urobiť opatrenia na kontrolu ich následku.

Certifikácia je postup, ktorým tretia strana (certifikačný orgán) poskytuje písomné ubezpečenie (certifikát), že výrobok, postup alebo služba sú v zhode so špecifickými požiadavkami. Ide o nezávislé, nestranné a odborné *posúdenie* (vykonané podľa medzinárodne prijatých pravidiel vzťahujúcich sa na činnosť certifikačných orgánov) *zhody* (určených znakov a vlastností jednoznačne definovaného výrobku, systému, služby alebo osoby) s požiadavkami deklarovанныmi v príslušných predpisoch a *oficiálne uznanie* a potvrdenie tejto zhody.

Certifikácia systému manažerstva tvorí jeden z prostriedkov, ktorým organizácia poskytuje zákazníkom, dodávateľom a ostatným zainteresovaným stranám záruku, že systém

¹ Prof. Ing. Jozef Gnap, PhD., vedúci katedry cestnej a mestskej dopravy, Fakulta PEDAS, Žilinská univerzita v Žiline, e-mail:jozef.gnap@fpedas.uniza.sk

² Ing. Drahomír Géc, DHL Slovakia, externý doktorand Fakulta PEDAS, Žilinská univerzita v Žiline

manažerstva vyhovuje špecifickým požiadavkám, je schopný dosahovať stanovené ciele a je efektívne implementovaný.

ISO 28000:2007 (E) Špecifikácia systému riadenia bezpečnosti v dodávateľskom reťazci

ISO 28000 séria noriem týkajúca sa bezpečnosti dodávateľského reťazca a riadenia systémov, ktoré boli práve aktualizované na verejne dostupné špecifikácie, ako plnohodnotné medzinárodné štandardy, pomôžu znížiť riziko pre ľudí a tovar v rámci dodávateľského reťazca. Normy riešia potenciálne bezpečnostné problémy na všetkých stupňoch dodávateľského procesu, teda zameriavajú sa na hrozby ako je terorizmus, krádeže, podvody a pirátstvo.

Séria noriem ISO 28000:

- ISO 28000:2007 - Špecifikácia systému riadenia bezpečnosti v dodávateľskom reťazci;
- ISO 28001:2007 - Bezpečnostné systémy pre riadenie dodávateľského reťazca,
 - najlepšie postupy pre vykonávanie bezpečnosti dodávateľského reťazca - posúdenia a plány,
 - požiadavky a pokyny;
- ISO 28003:2007 - Bezpečnostné systémy pre riadenie dodávateľského reťazca
 - požiadavky na inštitúcie poskytujúce audit a certifikáciu bezpečnosti dodávateľského reťazca a riadenie systémov;
- ISO 28004:2007 - Bezpečnostné systémy pre riadenie dodávateľského reťazca,
 - usmernenia pre uplatňovanie ISO 28000.

Táto medzinárodná norma špecifikuje požiadavky na systém riadenia bezpečnosti, vrátane tých aspektov, ktoré riadia bezpečnosť v rámci dodávateľského reťazca. Riadenie bezpečnosti je spojené s mnohými inými aspektmi obchodného manažmentu. Aspekty zahŕňujú všetky činnosti riadené alebo ovplyvňované organizáciami, ktoré majú vplyv na riadenie bezpečnosti dodávateľského reťazca.

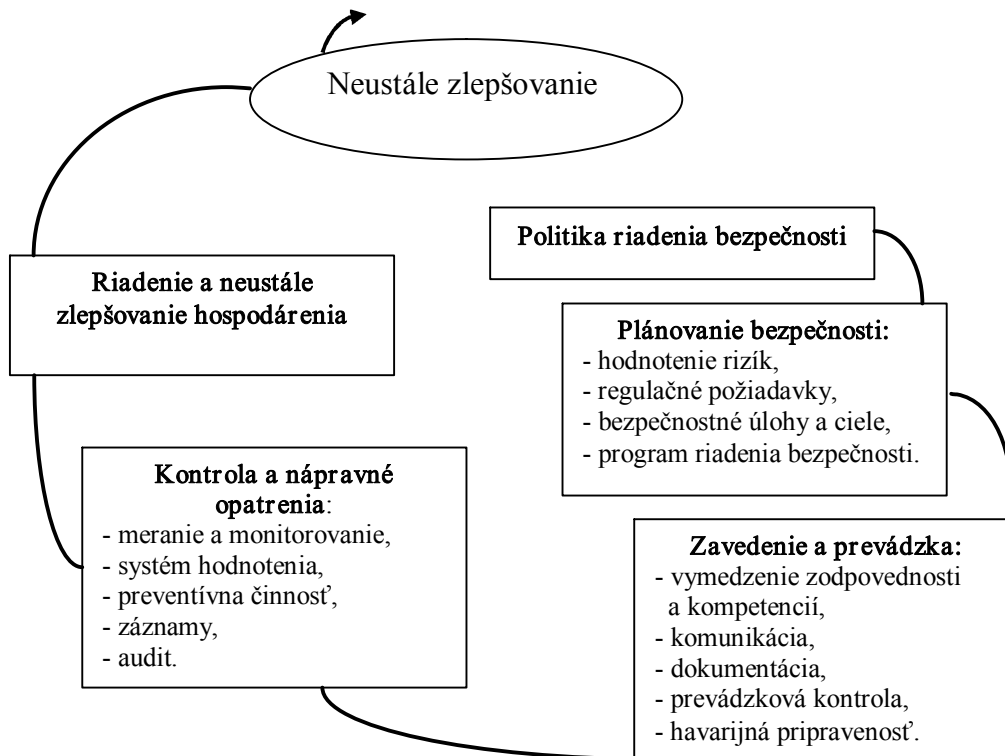
Táto norma je určená pre všetky typy spoločností, od malých po viacnárrodné, vo výrobe, službách, skladovaní alebo preprave, v akejkoľvek časti dodávateľského reťazca, ktoré chcú:

- vytvoriť, zaviesť, udržiavať a zlepšovať systém riadenia bezpečnosti,
- zabezpečiť zhody s uvedenou politikou riadenia bezpečnosti,
- sa usilovať o certifikáciu svojho systému riadenia bezpečnosti akreditovanou certifikačnou organizáciou, atď.

Podľa normy ISO 28000:2007(E) sa pod pojmom bezpečnosť rozumie: *odolnosť voči úmyselnej alebo neoprávnenej činnosti, predurčenej na spôsobenie škody v dodávateľskom reťazci alebo jeho zničenie* [2].

Prvky systému riadenia bezpečnosti sú na obr. 1. Táto medzinárodná norma je založená na formáte ISO 14001:2004 (pozri aj obr. 1) avšak organizácie, ktoré si osvojili procesný prístup

k riadeniu manažérstva kvality podľa ISO 9001:2001 resp. ISO 9001:2008 môžu byť schopné využiť existujúci systém riadenia ako základ pre systém riadenia bezpečnosti.



Obr. 1 Prvky systému riadenia bezpečnosti
Zdroj: ISO 28000:2007 (E)

Základnou požiadavkou tejto normy je, že organizácia musí v súlade s ňou vytvoriť, zdokumentovať, zaviesť, udržiavať a neustále zlepšovať efektívny systém riadenia bezpečnosti pre identifikovanie hrozieb, hodnotenie rizík, ich kontrolu a zmiernenie ich následkov.

Organizácie, ktoré si vyberú certifikáciu treťou stranou môžu preukázať, že významne prispievajú k bezpečnosti dodávateľského reťazca.

TAPA certifikácia

Predísť poškodeniu alebo zničeniu zásielky je možné najmä pomocou vhodne zvolených technologických postupov (napr. správna voľba dopravného prostriedku resp. druhu dopravy, vhodným prepravným obalom, správnym spôsobom jazdy a pod.)

V prípade krádeží a strát tovaru je možné takýmto rizikám predchádzať technickým zabezpečením, organizáciou práce a veľmi dôležitú úlohu pri tomto bezpečnostnom riziku zohráva ľudský faktor. Preto je potrebné venovať pozornosť výberu pracovníkov a práci s ľuďmi.

Práve na elimináciu bezpečnostných rizík spojených s kriminálnou činnosťou (krádeže, straty) počas logistických a prepravných operácií sa zameriava organizácia TAPA.

Organizácia TAPA bola založená v roku 1997 v severnej Amerike. Vznik tejto organizácie iniciovali výrobcovia tovarov s vysokou hodnotou a výrobcovia tzv. high-tech výrobkov (najmä z oblasti výpočtovej techniky, elektroniky, mobilných telefónov atď.).

Pôvodná skratka TAPA znamenala: The technology asset protection association (Organizácia na ochranu technológií), čo vyplývalo s charakteru zakladajúcich členov. Dôvodom na vznik organizácie bol rýchly technologický rozvoj high-tech tovarov počas deväťdesiatych rokov a zvyšujúci sa medzinárodný obchod s týmito tovarmi. S týmto rozvojom ale súčasne začala narastať kriminalita v tejto oblasti, čo bolo spôsobené najmä vysokou hodnotou týchto výrobkov, ktoré sa tak stali lukratívnou záležitosťou pre organizovanú kriminalitu. Dôsledkom bol narastajúci počet krádeží a „strát“, čo samozrejme spôsobovalo značné finančné straty.

TAPA odhaduje, že náklady súvisiace s kriminalitou sa pohybujú medzi 30 – 60 mld. dolárov ročne. Aktivity organizácie získavali veľmi rýchlo popularitu aj na ostatných kontinentoch, dôsledkom čoho bol vznik „dcérskych“ organizácií. V súčasnosti sú iniciatívy a aktivity organizácie TAPA vykonávané prostredníctvom štyroch organizácií, rozdelených podľa ich geografickej pôsobnosti.

- 1) TAPA EMEA (2000, Európa, Middle East, Africa) pôsobí v Európe, na Strednom východe a v Afrike,
- 2) TAPA Asia (2000),
- 3) TAPA Brazil (2003) pre južnú Ameriku a samozrejme
- 4) TAPA Americas pôsobiaca v severnej Amerike.

Vzhľadom na postupné rozširovanie aktivít na celú oblasť distribučnej logistiky (preprava, skladovanie, manipulácia, triedenie, atď.) sa zmenil v roku 2006 aj pôvodný názov na Transported asset protection association (Organizácia pre ochranu majetku pri preprave).

Základnou myšlienkou organizácie je ochrana výrobkov v rámci logistického reťazca. Za týmto účelom boli vypracované bezpečnostné štandardy FSR – freight security requirements (požiadavky na ochranu tovaru). Tieto štandardy stanovujú minimálne požiadavky pre získanie certifikátu TAPA, ktoré musia spĺňať subjekty, ktoré chcú tento certifikát získať (dopravcovia, logistickí operátori, zasielateľia).

Tieto štandardy obsahujú napr. požiadavky na skladovacie priestory, min. bezpečnostné vybavenie, termíny a postup pri bezpečnostných auditoch, postup pri prípadných stratách výrobkov, požiadavky na dopravné prostriedky, atď. Štandardy FSR sa týkajú najmä oblasti skladovania a manipulačných operácií v rámci skladovania.

TAPA sa však nezameriava iba na oblasť skladovania, ale na celý proces distribúcie, distribučnej logistiky a supply chain. Preto boli vypracované doplnkové bezpečnostné štandardy TSR – truck security requirements (požiadavky na ochranu pri cestnej doprave). Požiadavky sa týkajú najmä cestných dopravcov, nákladných vozidiel a operácií pri preprave (nakládka, vykládka, manipulačné zariadenia atď.).

Ďalšou aktivitou organizácie (okrem bezpečnostných štandardov) je vytvorenie, prevádzkovanie a aktualizácia centrálnej informačnej databanky IIS (Incident Information Service). V tejto databanke sa zaznamenávajú kriminálne prípady (krádeže, vlámnia, prepady, atď.), ktoré sa stali členom organizácie. Údaje z databanky sú k dispozícii členom organizácie a tiež orgánom činným v trestnom konaní.

Certifikácia TAPA

Spoločnosť, ktorá úspešne implementuje požiadavky bezpečnostných štandardov (FSR resp. TSR) do svojich logistických činností a procesov, preukazuje zavedenie a dodržiavanie týchto štandardov certifikátom organizácie TAPA. Tento certifikát je preukazom toho, že spoločnosť

sa podieľa na prevencii a boji proti kriminalite a úspešne sa snaží minimalizovať riziko hospodárskych strát súvisiacich s kriminalitou (krádeže, vlámania, straty, atď.).

Certifikácia sa vzťahuje na prevádzky, v ktorých sú vykonávané logistické činnosti (distribučné a logistické centrá, terminály, prekladiská) a tiež na samotné prepravné činnosti.

Teda samotný proces certifikácie nevykonáva organizácia TAPA, ale ňou poverená auditorská spoločnosť. V rámci Európy momentálne pôsobia štyri subjekty, ktoré majú od organizácie TAPA poverenie vykonávať audity pre získanie certifikátu a môžu udeľovať tieto certifikáty:

- 1) *Bureau Veritas Certification for EMEA Londýn,*
- 2) *Germanischer Lloyd Certification GmbH Hamburg,*
- 3) *Lloyd's Register Quality Assurance Rotterdam,*
- 4) *SGS TAPA EMEA Centre Birmingham* [4].

Súčasťou certifikácie je tiež bezpečnostný audit, ktorého úlohou je overiť implementáciu štandardov do praxe a ich úspešnú realizáciu. V súčasnosti je vo svete certifikovaných viac ako 1000 prevádzok, ktoré spĺňajú štandardy FSR resp. TSR. V Európe je certifikovaných 213 zariadení úrovňou A (najvyššia úroveň) a 50 zariadení úrovňou B [4]. Celkovo je možné získať certifikát v troch úrovniach A,B,C, ktoré sa odlišujú nárokmi na plnenie jednotlivých požiadaviek. Na Slovensku sú momentálne certifikované podľa najvyššieho stupňa bezpečnosti (level A):

- *terminál spoločnosti Schenker v Bratislave (24. júla 2007)*
- *slovenská pobočka TNT Express (24. marec 2009).*

Treba upozorniť, že na rozdiel od certifikácie systému manažérstva kvality podľa ISO 9001:2008 je platnosť certifikátu len dva roky.

Na záver

Je potrebné aj v logistických a zasielateľských organizáciách manažérstvo rizika chápať ako integrálnu súčasť dobrej manažérskej praxe. Aby bolo čo najefektívnejšie, manažérstvo rizika by sa malo stať súčasťou podnikateľských plánov. Je potrebné identifikovať a riadiť procesy manažérstva rizika systematickou aplikáciou politiky, postupov a praktík manažérstva na úlohy, ktoré určujú súvislosti, ktoré určujú súvislosti, identifikujú, analyzujú, hodnotia riziko, zaoberajú sa rizikom, monitorujú ho a prijímajú nápravné a preventívne opatrenia.

LITERATÚRA

- [1] BAUMGARTNER, H.: *Entwicklungstrends der Logistik und strategische Ableitungen*, Mníchov 2006
- [2] ISO 28000:2007 (E): *Specification for security management systems for the supply chain*
- [3] STN 010380:2003 Manažérstvo rizika (AS/NZS 4360:1999), SUTN, *Bratislava, 2003*
- [4] MORAVČÍK, T.: Certifikácia TAPA a zvyšovanie bezpečnosti, *Logistický monitor*, Žilina, apríl 2008, ISSN 1336-5851