Bezpečnostní management nebo management bezpečnosti?

Zbyněk Pitra – SVŠES, s. r. o. v Praze

Otázka představovaná názvem příspěvku není jen slovní hříčkou, i když tak na první pohled vypadá. Má hlubší smysl; vztahuje se ke správné volbě koncepce přístupu k zajištění vysoké efektivity podnikání dnešních organizací, působících v nejistém okolí, které je plné také bezpečnostních hrozeb. Po zániku bipolárního rozdělení světa v roce 1989 se situace na celém světě zásadně změnila. Uvolnil se prostor pro projevy rozporů, které předtím zůstávaly ve stínu rivality dvou ideologicky soupeřících supervelmocí nebo dokonce byly jejich soupeřením přímo či skrytě vyvolávány. Je smutné, že společnost bere tento výrazný kvalitativní zvrat, ke kterému ve stavu dnešního světa poměrně rapidně dochází od posledního desetiletí minulého století, na vědomí jen pomalu a proto také neochotně mění své dlouhodobé tradiční modely chování.

Zánik bipolárního světa otevřel dveře jevu, který se nazývá **globalizace**. Díky výsledkům vědeckotechnického rozvoje je dnešní svět stále těsněji komunikačně, dopravně, ekonomicky i kulturně propojen. Jakákoliv událost, ke které dojde v jedné části světa, už nezůstává geograficky izolovanou a projeví se určitými dopady i na všechny ostatní oblasti globálního světa. Výraz „*globální vesnice*“, kterým je stav dnešního světa s nadsázkou označován, zdaleka není jen sarkastickou licencí.

Globalizace je historicky *nevyhnutelný proces*, kterému je zbytečné se bránit, především v souvislosti s tím, že tento proces je v moha směrech žádoucí a má blahodárné účinky na většinu lidstva. Ale jako každý společenský jev má i globalizace své stinné stránky, svou odvrácenou tvář. Jednou z nich je to, že otevírá dveře do epochy, ve které zcela reálně může převládnout násilí a chaos. Tomuto nebezpečí však společnost zabránit může, dokonce musí. *Obrana proti globálním hrozbám musí být také globální* - musí se do ní zapojit celá společnost. Lidé nemohou ponechat - v souladu s tradičními modely chování - péči o svou bezpečnost pouze na bedrech státu, jehož jsou občany. Naopak, političtí představitelé jednotlivých států musí, i když se toho z různých důvodů obávají, přiznat realitu dnešního globálního světa. Sebesilnější a dobře organizovaný stát nemůže sám zajistit bezpečnost všech subjektů, působících na jeho území, jejich úplnou ochranu proti globálním hrozbám. Ochrana proti globálním hrozbám se dnes musí stát součástí **společenské zodpovědnosti** za vlastní činnost všech institucí (národních i nadnárodních), které působí v dnešním globálním světě. Výjimku z této zásady samozřejmě nemohou mít ani podnikatelské subjekty, organizace zabývající se prováděním různých podnikatelských činností.

Má-li jakýkoliv podnikatelský subjekt nebo instituce dostát svým závazkům, vyplývající z jeho společenské zodpovědnosti, musí mj. garantovat také to, že pořízení jím nabízených produktů nebo služeb nevystaví jejich zákazníky - potenciální uživatele těchto produktů anebo služeb - žádnému ohrožení Všechny podnikatelské subjekty proto dnes musí zajistit bezpečnost proti globálním hrozbám *především svými vlastními silami*. Pochopitelně musí se přitom spoléhat také na odbornou podporu vnějších specialistů. Musí přitom ve svém úsilí o zajištění bezpečnosti svých podnikatelských aktivit respektovat tři základní skutečnosti:

- mezi vlastní bezpečností a ohrožením zvenčí existuje přímá kauzální vazba;
- požadavky zajistit vlastní bezpečnost a dosáhnout vysoké efektivity podnikání jsou často v přímém rozporu;

- zdroje ohrožení - nebezpečné entity světového chaosu - jsou málo viditelné a jen obtížně se proti nim zasahuje.

V dnešním globálním světě má významnou úlohu zpracování informací na prostředcích informační a komunikační technologie. Právě tyto prostředky jsou často předmětem globálních bezpečnostních hrozeb. Přístupy, používané k zajištění bezpečnosti informačních systémů organizace, jsou proto vhodným ilustrativním příkladem úsilí, které musí organizace věnovat na splnění závazků své společenské zodpovědnosti.

Ilustrativní příklad:

Informační systémy organizace, provozované na počátku 21.století na prostředcích informační a komunikační technologie (ICT), mohou ohrozit její zákazníky chybným zpracováním informací a tím i nesprávným vyřízením objednávky anebo reklamace zboží či špatně provedeným inkasem platby za dodané produkty a služby. Mezi vlastní bezpečností informačních systémů organizace a jejich vnějším ohrožením existuje zřejmá kauzální vazba: příčiny nesprávného fungování informačních systémů a s tím spojeného ohrožení zákazníka je možné rozčlenit do tří hlavních kategorií:

- *fyzické* ohrožení - přírodní katastrofy, požáry, poruchy dodávek energie, technické závady;
- *programové* ohrožení - chybná funkčnost, viry, trojské koně či monitorovací programy;
- *lidské* ohrožení - zloději, průnikáři (hackeři), nepoučení uživatelé.

Zdroje těchto hrozeb jsou mimo dosah vlivu pracovníků organizace a většinou jsou jen obtížně identifikovatelné. Např. odhalit zkušeného hackera je za dnešních podmínek prakticky nemožné. Proto musí organizace při zajištění bezpečnosti svých informačních systémů uplatnit dva vzájemně se doplňující přístupy: *vnější* ochranu (metodami bezpečnostního managementu) z okolí informačního systému a *vnitřní* ochranu (metodami managementu bezpečnosti) prostřednictvím procesů, probíhajících uvnitř vlastního informačního systému.

Uplatnění metod *bezpečnostního managementu*, založené na ochraně technických prostředků ICT proti poškození a odcizení, komunikačních cest proti neoprávněným vstupům nebo monitorování, programových prostředků a datových základen proti neautorizovaným vstupům a cílenému poškození je realizováno z okolí informačního systému.

Využití metod *managementu bezpečnosti* spočívá v rozšíření funkcí systému, vyvolaného jeho doplněním o další prvky, změnou struktury vnitřní organizace systému a zejména jinými přístupy k managementu procesů zpracování informací. Metody managementu bezpečnosti provozu informačního systému organizace se uplatňují jako integrální součást jeho účelového fungování: zajištění jednotlivých podnikatelských procesů potřebným informačním servisem.

Příkladem takového rozšíření funkčnosti systému je:

- *Prvky*: zdvojení paměťových záznamů, stínění kabelů, záložní procesory, …
- Struktura: záložní zpracování výstupů, autentizace vstupů, programové kontroly transakcí, křížový audit, …
- Řízení: monitoring stavu transakcí, kontroly mezivýsledků, start záložních zdrojů, re-starty transakcí, ...

Uplatnění nástrojů bezpečnostního managementu, stejně jako rozšíření funkcí informačního systému o metody managementu bezpečnosti si vyžádá dodatečné náklady:

- zvýšené pořizovací náklady (kvalitní prostředky ICT, zdvojování prvků systému, ...);
- zvýšené provozní náklady (prodloužení doby zpracování, speciální služby, dodatečné kontrolní funkce, ...);

a také omezení pohodlí uživatelů informačního systému (složitější přihlašování se do systému, omezení svobody pohybu obsluhy, náročnější kontroly informačních transakcí, ...).

Za bezpečnost fungování svých informačních systémů musí organizace vždy zaplatit. To je v přímém rozporu s dnešním imperativem podnikání: trvale snižovat vlastní náklady. Úroveň zabezpečení provozu informačních systému organizace proti vnějším hrozbám je proto výsledkem kompromisu mezi náklady na bezpečnostní management i na procesy managementu bezpečnosti a akceptovatelnou mírou rizika ohrožení funkčnosti systému.

Při řešení rozporu mezi náklady na zajištění bezpečnosti informačních systémů a požadavky na jejich komplexní ochranu proti bezpečnostním hrozbám je nutno respektovat skutečnost,že **nikdy nelze zajistit 100% bezpečnost** funkcí informačního systému v organizaci.

V ilustračním příkladu se objevují dva pojmy, které se vyskytují také v názvu příspěvku. V zájmu přehlednosti dalších úvah v tomto příspěvku je účelné prezentovat na

tomto místě **koncepční sémantické východisko definic obou pojmů**, které je uvedeno dále v rámečku:

BEZPEČNOSTNÍ MANAGEMENT

- je souborem samostatných (nezávislých) činností, jejichž účelem je předejít bezpečnostní hrozbě nebo minimalizovat její následky, pokud se hrozba naplní,
- pracuje s vlastními nástroji a využívá speciální metodologii,
- zaměřuje se spíše na objekty a zdroje než na procesy,
- je zabezpečován autonomně - v nezávislých organizačních strukturách.

MANAGEMENT BEZPEČNOSTI

- je (či by měl být) integrální součástí managementu podnikání jakéhokoliv subjektu,
- je primárně orientován na procesy,
- je realizován ve stejných organizačních strukturách jako je zabezpečován management jednotlivých podnikatelských aktivit organizace.

Podnikatelský subjekt *nikdy nepůsobí izolovaně od vývoje společnosti*, probíhajícího v jeho okolí. Je proto při hledání výhodných podnikatelských příležitostí zcela zákonitě vystaven také vnějším rizikům či (mnohdy dokonce úmyslně nepřátelským) ohrožením.

Podnikatelský subjekt se v této situaci musí vyrovnat nejenom s *podnikatelskými* riziky a hrozbami (jako je nespolehlivost dodavatelů, výkyvy na finančních trzích, fluktuace zákaznických potřeb a přání apod.), ale také s dalšími kategoriemi politických, sociálních, přírodních a technologických rizik a hrozeb, vznikajícími v jeho okolí (jako je terorismus, pandemie chorob typu SARS, AIDS, ptačí chřipka, globální oteplování, ….). Jeho vedoucí představitelé jsou tudíž každodenně postaveni před hledání správných odpovědí na zásadní otázku:

Jak se vyrovnat s významnými hrozbami, jejichž vznik prakticky nelze ovlivnit a za které v podstatě nikdo nemá přímou zodpovědnost?

Při hledání odpovědí na tuto otázku si představitelé jednotlivých organizací musí být vždy vědomi toho, že *žádná hrozba není nezávislou entitou*! Vznik vnějších hrozeb je důsledkem změn, probíhajících v okolí organizace. Tyto změny jsou vyvolávány příčinami, souvislosti jejichž vzniku lze (s větší či menší přesností) identifikovat a tím také anticipovat možnost jejich vzniku. Přitom hrozby, způsobené nebo vyvolané člověkem, vždy vznikají v určitém společenském kontextu. Stejně jako reakce vedení podnikatelských subjektů na ně. Rozhodnutí o tom, jak hrozbu vnímat a jak na ni reagovat ovlivňuje sociální klima a interní kultura organizace; soubor jejími pracovníky uznávaných hodnot a většinový názor na jejich úspěšné prosazování.

Při volbě reakci na vnější hrozby organizace nevystačí s tradičními postupy managementu rizika Významné světové hrozby zatěžují podnikání každé organizace mnohem větší zodpovědností než si to její vedení mnohdy dokáže připustit. Pro ilustraci jsou uvedeny tyto dva příklady:

- Efekt „ mávnutí motýlího křídla“: Teroristický útok z 11. září 2001 vyvolal ekonomickou a finanční řetězovou reakci, která výrazně vystupňovala jeho primární ničivý účinek.
- V éře informační technologie využili dnešní teroristé moderní technologii k provedení svým pojetím archaických teroristických akcí.

Podcenění hrozby, které je mnohdy vyvoláno neochotou vedení organizace vynaložit na její odvrácení potřebné náklady, je častým projevem neochoty podnikatelských subjektů

přiznat si vlastní bezbrannost vůči hrozbám dnešního globálního světa. Je proto velmi aktuální otázka:

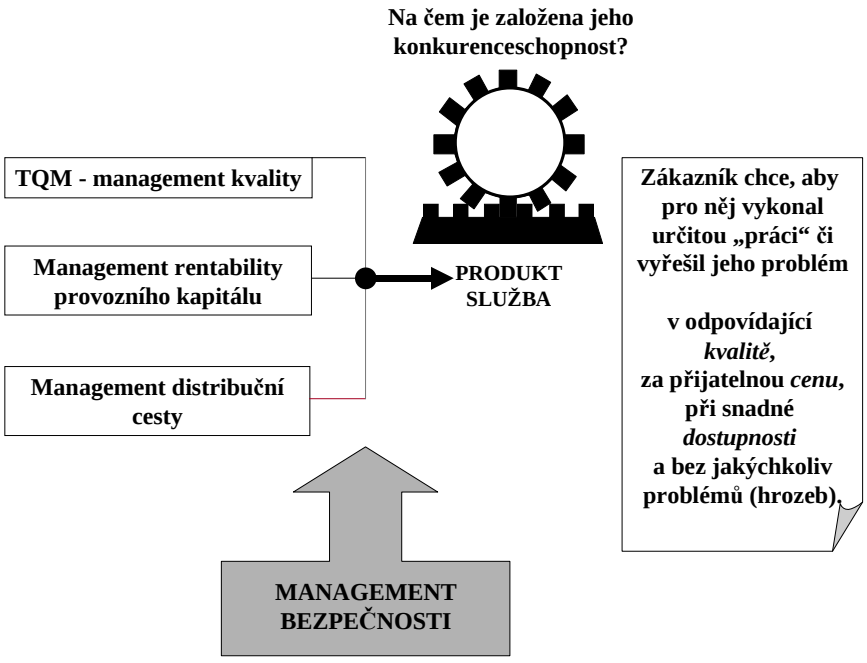
CO S TÍM AKTUÁLNĚ DĚLAT?

Ještě před tím, než se pokusím navrhnout možné odpovědi na tuto poměrně složitou a nepochybně zcela závažnou otázku, je nutné zodpovědět dvě koncepční otázky.

První z nich zní: *Může subjekt podnikat, aniž by uplatňoval bezpečnostní management?* Teoreticky může, ale pouze v ideálním světě. Avšak žádná organizace neprovádí své podnikatelské aktivity v ideálním světě. Proto společnost většinou trvá na dodržování bezpečnostních předpisů a norem, kterými je reflektováno to, že realita se od ideálu (často velmi zásadně) liší. A metodologie bezpečnostního managementu - ve své podstatě - vychází z respektování a prosazování těchto předpisů a norem při provádění podnikatelských aktivit.

Druhá otázka je podobná: *Může subjekt podnikat, aniž by uplatňoval management bezpečnosti?* Zde je odpověď zcela jednoznačná; nemůže, ani teoreticky. Je proto s podivem, kolik představitelů dnešních firem se domnívá, že se jimi vedené organizace bez uceleného konceptu komplexního managementu bezpečnosti obejdou. Role procesů managementu bezpečnosti přitom není - až na výjimky - legislativně vymezena. Jeho provádění a realizační potřeby jsou vymezeny požadavky plnění závazků společenské zodpovědnosti každé jednotlivé organizace individuálně.

Hrozba z okolí není pouhou sociální konstrukcí, vytvářenou představiteli managementu organizace pro účely jednodušší specifikace strategických scénářů postupu ke zvoleným podnikatelským příležitostem. Je (sociální) *realitou*, jejíž zvládnutí vyžaduje poměrně značné úsilí a náklady. Aby tyto náklady a úsilí byly pro vedení organizace akceptovatelné, musí představitelé organizace vnímat jak se náklady a úsilí věnované realizaci procesů managementu bezpečnosti zhodnotí ve zvyšování konkurenceschopnosti organizací nabízených produktů a služeb. Je proto nutné neustále zdůrazňovat skutečnost, že management bezpečnosti má v podnikání **strategickou roli** - zvyšuje konkurenceschopnost nabízených produktů a služeb, jak je zřejmé z následujícího schématu.



Ke třem klasickým faktorům, vymezujícím úroveň konkurenceschopnosti organizací nabízených produktů či služeb, představovaných kvalitou, dostupností a cenou, přistupuje čtvrtý rovnocenný faktor: *bezpečnost jeho každodenního užívání*. Proto je nutné procesy managementu podnikatelských operací doplnit - v zájmu zvýšení výdělečné síly organizace (tomu vedoucí představitelé firmy dobře rozumí!) - i o procesy managementu bezpečnosti.

To však stále není uspokojující odpovědí na principiální otázku: Co dělat s nevyhovujícím současným stavem managementu bezpečnosti ve všech moderních organizacích? Je nutné si uvědomit skutečnost, že odvracení bezpečnostní hrozby není jednorázovou akcí, ale musí být součástí trvalého, koncepčního a koordinovaného úsilí všech pracovníků organizace. Tato skutečnost musí být pravidelně komunikována do vnitřního prostředí organizace. Všem jejím pracovníkům se musí dostat příležitosti ke zvýšení svých odborných způsobilostí v aplikaci procesů managementu bezpečnosti při plnění každodenních podnikatelských úkolů.

Zní to možná překvapivě, ale budování těchto způsobilostí musí začít od maličkostí. Ukazují to přesvědčivě praktické výsledky těchto postupů. Bývalý starosta New Yorku R. Giuliani zahájil svou kampaň za zvýšení bezpečnosti a snižování zločinnosti ve městě zdánlivými maličkostmi: postihem sprayerů, vyhnáním bezdomovců z ulic a kontrolami dodržování zavírací doby v restauracích a barech. Byl mnohými označován jako fašista, který šikanuje obyvatele namísto toho, aby se věnoval boji se závažným zločinem. Po čase se ukázal jeho přístup jako velmi účinný; zločinnost v New Yorku poklesla o 50%. Právě kvůli této změně sociálního klimatu ve městě se jeho obyvatelé mohli relativně účinně a úspěšně vyrovnat s katastrofou, kterou vyvolaly útoky teroristů 11. září 2001.

Po zavedení pořádku v organizaci je nutné nad touto základnou rozvinout náročnější procesy managementu bezpečnosti. Mají-li být účinně zaváděny ve vnitřním prostředí jednotlivých podnikatelských subjektů, bude vhodné formálně upravit postupy managementu bezpečnosti příslušnou normou - analogicky tomu jak jsou postupy managementu kvality upraveny normou ISO 9000, v pojetí které ilustruje obsah následující tabulky.

ISO 9000		**ISO xxxx**
POLITIKA JAKOSTI Rozhodnutí vedení o cílech kvality a o postupech k jejich dosažení	1. úroveň: ***strategie***	POLITIKA BEZPEČNOSTI Rozhodnutí vedení o cílech bezpečnosti a o postupech k nim
PŘÍRUČKA KVALITY Popis vazeb a rozhraní mezi prvky systému	2. úroveň: ***systém***	„PŘÍRUČKA BEZPEČNOSTI“ Popis vazeb a rozhraní mezi prvky systému
SPECIFIKACE PROCESŮ Podrobný popis vlastností jednotlivých prvků systému	3. úroveň: ***prvky***	SPECIFIKACE OCHRAN Podrobný popis vlastností jednotlivých prvků systému
ZÁZNAMY O NESHODÁCH A JEJICH ODSTRANĚNÍ Výkazy o každodenním fungování systému a jeho výsledcích	4. úroveň: ***evidence***	ZÁZNAMY O PORUCHÁCH A JEJICH ODSTRANĚNÍ Výkazy o každodenním fungování systému a jeho výsledcích

Do sestavení této normy by se měly aktivně zapojit skupiny specialistů zaměřených na bezpečnostní ochranu, ale také specialisté z oblastí podnikání, financí, technického rozvoje a také specialisté z oblastí sociálních věd i zdravotnictví. Jen tak může nově zpracovaná norma získat charakter systémově vyváženého dokumentu a být účinně aplikována.

Literatura

[1] Bauer, A. - Raufer, X.: *Válka teprve začíná. Scénáře pro 21.století.* Praha : Themis, 2004
[2] Caruso, D.: *No Risk Is an Island.* Harvard Business Review 2005/2, str.40-41

Summary in English:
The paper deals with the interactions that must be developed between business activities management and management of these activities security assurance. The security risks that exist within the today global economy environment must be handled by specific and complex approach similarly to the way the total quality management is in the majority of modern companies performed. The security assurance processes that support company competitiveness must form an integral part of everyday management influence on regular business operations.

Klíčová slova:
Bezpečnostní management, konkurenceschopnost organizace, management bezpečnosti, podnikatelská procesy, řízení kvality, společenská odpovědnost firmy, systém řízení operací

prof. Ing. Zbyněk Pitra, DrSc., SVŠES, s. r. o., Lindnerova 575/1, Praha 8,
E-mail: zbynek.pitra@svses.cz