Bezpečnostní balance – hodnocení vyváženosti rizikových zábran

Tomáš Macák – SVŠES, s. r. o. v Praze

Kvalitativní bezpečnostní determinace

Bezpečnost je všeobecný pojem, který není vymezen v českém právním řádu a který se používá pro agregovaný popis determinantů, které je potřeba udržovat v přijatelných mezí klidového stavu. Z hlediska dopadu na újmu životní úrovně referenční skupiny subjektů při porušení tohoto ustálení klidového stavu, je nejvýstižnější následující definice bezpečnosti: „ Bezpečnost je stav, při kterém vznik újmy u životů a zdraví lidí, majetku, životního prostředí, lidské společnosti a v poslední době i u kritické infrastruktury má přijatelnou pravděpodobnost“.[1] Bezpečnost je ve své podstatě možno chápat jako žádoucí úroveň nastalé skutečnosti, která je ovlivňována především náhodnými negativními jevy, které mají fatální dopad na existenci sledovaného objektu. V současné době odborná veřejnost pracuje s pojmem „bezpečnost“ způsobem protikladného dualismu v ohledu na možnosti řízení bezpečnostních rizik.

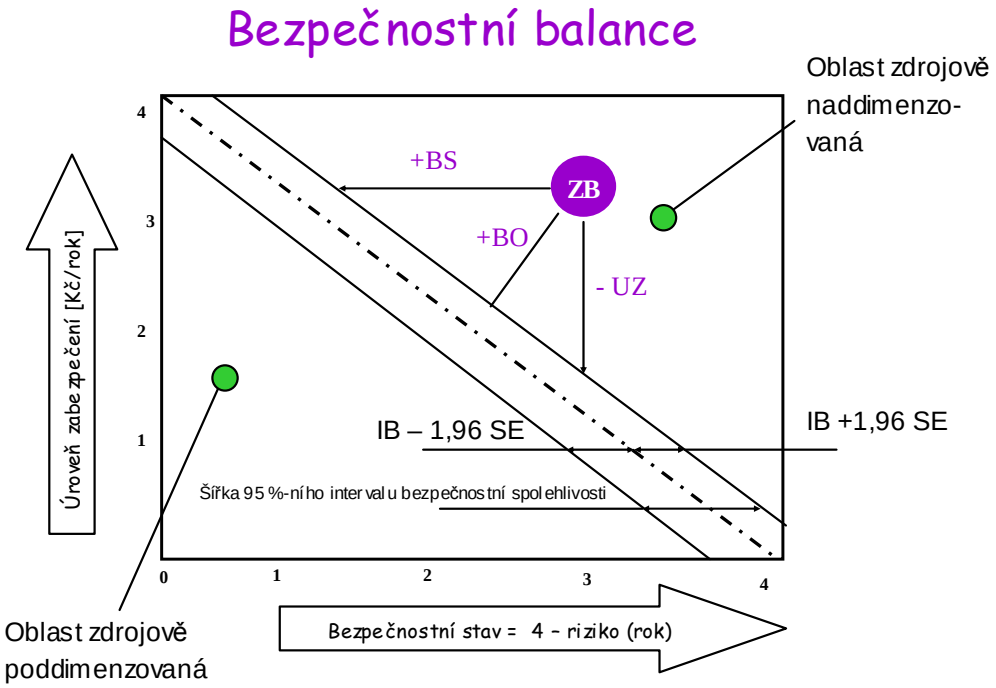
- ⇨ Technologický optimismus
  - představuje aplikaci konstruktivistického přístupu k řízení systému do oblasti bezpečnostního managementu. Tvrdí, že zárukou udržení žádoucího stavu bezpečnosti je technologicko-technický rozvoj společnosti založený na poznatcích základního výzkumu. Bezpečnost lze tímto způsobem regulovat v systému, jehož sledovaná veličina (agregovaná úroveň bezpečnosti) má lineární průběh v závislosti na čase.
- ⇨ Technologický skepticismus
  - - představuje aplikaci systémově - evolučního přístupu k řízení systému do oblasti bezpečnostního managementu. Tvrdí, že technologický pokrok má své produkční možnosti, která jsou časově determinované. Čím je systém objektu, u kterého se požaduje zajištění bezpečnosti sofistikovaněji zkonstruován, tím je u něj vyšší šance na vznik bezpečnostního rizika (vyšší zranitelnosti náhodným vlivem) a tím více se bezpečnostní veličina odklání od svého lineárního průběhu v čase.

Konkrétní regulace předmětu bezpečnosti je založena na nástrojích převzetích z oblasti řízení. V České republice existuje na úrovni státní odpovědnosti za bezpečnost společnosti procedura označovaná IDNDR (International Decade on Natural Disaster Reduction), mezinárodní desetiletá směrnice na eliminaci dopadů přírodních pohrom. Dále je předmětem státní odpovědnosti oblast jaderné technologie a stejné tendence se prosazují i u chemické technologie. Na úrovni podnikatelského subjektu jsou předmětem bezpečnostní odpovědnosti obecně jiné veličiny. Jedná se především o jevy, které je možné podnikatelským úsilím eliminovat a které je možné z pohledu statistické četnosti považovat za rizika s vysokou hustotou výskytů. Konkrétní příklady těchto hrozeb jsou obsaženy v následujícím modelu balance bezpečnosti.

Model bezpečnostního balance

Tento model vychází z předpokladu, že všechny vnější jevy, které mají dopad na výslednici subjektové (podnikové) bezpečnosti jsou v zásadě zjistitelné v potřebný čas. V případě, že v potřebném čase nejsou zjistitelné přímým změřením nebo hodnotovým přiřazením, pořád se ještě mohou vypočítat nebo předurčit – z minulé zkušenosti, resp. ze statistických údajů o výskytech jednotlivých bezpečnostních rizicí.

Obrázek 1 Modelové řešení bezpečnostní rovnováhy



Obrázek představuje situaci, ve které došlo k předimenzování bezpečnostního zabezpečení organizace (poloha zabezpečení v reakci na bezpečnostní stav je reprezentována bodem ZB). Úroveň zabezpečení je kvantifikována ve formě roční finanční investice do komplexního zabezpečovacího systému, dále investice do oblasti preventivní eliminace vzniku bezpečnostního rizika a nakonec investice do procedur minimalizace vzniklých škod při porušení bezpečnosti. Bezpečnostní stav je souhrnné ohodnocení jednotlivých oblastí, v kterých se bezpečnostní porucha může vyskytnout. Předmětem hodnocení bezpečnostního stavu jsou pouze existenčně relevantní oblasti podnikového chodu.

Ideální je situace, kdy se poloha podnikové situace nachází na hlavní diagonále grafu, tzn. kdy je úroveň zabezpečení organizace v souladu (balanci) s jejím bezpečnostním stavem. Určitá míra nesouladu mezi těmito dvěma veličinami je tolerována. Představa tolerance je na obrázku zachycena v podobě šířky bezpečnostního intervalu spolehlivosti. To znamená, že v případě polohy organizace reprezentované bodem ZB v pásmu 95% intervalu bezpečnostní spolehlivosti můžeme předpokládat, že ve dvaceti případech při výskytu bezpečnostního rizika bude pouze při jednom výskytu poruchy neadekvátní odezva ze strany bezpečnostního zabezpečení. Pro Studentovo $t_{0,025}$ rozdělení pravděpodobnosti výskytu bezpečnostních poruch platí pro směrodatnou odchylku hlavní diagonály grafu (bezpečnostní balance) SE vztah: Bezpečnostní stav

$$SE = t_{0,025} \frac{s}{\sqrt{n}} \tag{1}$$

Kde: s je výběrová směrodatná odchylka
n je rozsah zaznamenaných bezpečnostních poruch za minulé období

Podle stupňů volnosti – minimum nezbytných informací (tj. n-1) můžeme určit ze Studentova rozdělení pravděpodobnosti hodnotu kompenzačního koeficientu $t_{0,025}$ a ten dosadit do vztahu pro určení šířky pásma bezpečnostní spolehlivosti. V případě překročení pásma spolehlivosti, tj. bezpečnostní stav (BS) > BS + $t_{0,025}$ SE, potom se subjekt nachází v situaci naddimenzování bezpečnostního zabezpečení. Tato přehnaná opatrnost při extrémní averzi k riziku vede k plýtvání finančních a lidských zdrojů, bez možnosti ospravedlnění těchto marginálních výdajů potřebou větší jistoty. Bezpečnost se tak stává cílem organizace a ne její existenční potřebou. V případě nedosažení pásma spolehlivosti, tj. bezpečnostní stav (BS) < BS - $t_{0,025}$ SE, potom se subjekt nachází v situaci bezpečnostní poddimenzace. Toto podcenění hrozeb v dlouhodobém horizontu vede k bezpečnostní nefunkčnosti organizace a v nejhorším případě k její nedobrovolné likvidaci.

Aplikace bezpečnostního balance

Na ilustrativním příkladu je ukázána aplikace bezpečnostní rovnováhy. Úroveň zabezpečení i bezpečností stav jsou desagregovány na své složky. V případě úrovně zabezpečení se pro názornost hodnotí vliv roční komplexního zabezpečovacího systému, vliv preventivní eliminace vzniku bezpečnostního rizika a vliv minimalizace vzniklých škod při porušení bezpečnosti. Všechny vlivy je možné kardinálním způsobem ohodnotit pomocí spotřebovaných zdrojů, které svou úrovní vyvolávají. Bezpečnostní stav je charakterizován třemi zásadními vlivy, těmi jsou při ilustrativní situaci: bezpečnost v oblasti havárie technologického provozu, bezpečnost v oblasti utajení strategických informací organizace, bezpečnost v relaci živelné pohromy. Abychom mohli srovnávat jednotlivá kritéria hlavních veličin i samotné bezpečnostní veličiny, musíme jejich ať absolutně, tak nominálně změřené hodnoty převést na společnou bázi. Zde je tato báze tvořena intervalem hodnot od 0 do 4. Vyšší hodnoty ukazují na závažnější vliv bezpečnostního atributu, resp. na potřebu vyšší zdrojové (finanční) investice do dané kategorie zabezpečení. Po přiřazení hodnot jednotlivým kategoriím bezpečnosti a zabezpečení je potřeba ještě stanovit hodnoty relativních intenzit faktorů. Tyto intenzity představují jakési „váhy“ významnosti jednotlivých faktorů. Jejich hodnotové určení je u faktorů zabezpečení provedeno v poměrech relativních hodnot spotřebovaných zdrojů, resp. v poměrech nákladovosti jednotlivých druhů zabezpečení. Hodnotové určení intenzit faktorů charakterizující bezpečnost jsou získány v poměrech statisticky určených pravděpodobností vzniků jednotlivých druhů bezpečnostních poruch, viz. tabulka 1.

Tabulka 1 Hodnoty bezpečnostních veličin a jejich intenzity

	Úroveň zabezpečení (UZ)			Bezpečnostní stav (BS)		
oblast	zabezpečo-vací systém **(I)**	prevence náhodných poruch **(C)**	minimali-zace škod **(S)**	havárie technologie	utajení informací	bezpečnost živelné pohromy
hodnota	3	1	3	4	3	4
intenzita	0,3 = v_1	0,4= v_2	0,3= v_3	0,4= va	0,3= vb	0,3= vc

Bezpečnostní stav a úroveň zabezpečení se určí váženým součtem jejich dílčích hodnost s příslušnými intenzitami:

- ⇨ UZ = Σvi·hi = 0,4 · 4 + 0,3 · 3 + 0,3 ·4 = 3,7
- ⇨ BS = Σvj·hj = 0,3 ·3 + 0,4 · 1 + 0,3 ·3 = 2,0
- ⇨ Absolutní odchylka: AO = BS – UZ = 2 – 3,7 = -1,7

Bezpečnostní odchylka polohy BO:

$$BO: \quad BS - UZ = AO = \sqrt{2}BO \quad \Rightarrow o = \frac{BS - UZ}{\sqrt{2}} = \frac{AO}{\sqrt{2}} = 1{,}202 \tag{2}$$

Nyní je potřeba určit nové nastavení dílčích faktorů úrovně zabezpečení UZ. Existují dva možné způsoby postupu k nalezení řešení:

1. Vytvoření soustavy rovnic a při substitučním dosazení za dvě neznámé se převede soustava na rovnici o jedné neznámé.

2. Analytické vyjádření jednotlivých parametrů konkurenční síly v závislosti na atraktivitě trhu a vahách faktorů:

$$UZ = f(BS, v1, v2, v3,) \tag{3}$$

Při druhém způsobu napíšeme soustavu rovnic tří rovnic a z nich pak explicitně vyjádříme výrazy pro hodnoty jednotlivých faktorů UZ v souladu s bezpečnostní balance:

1) I : C : S = v1 : v2 : v3´

2) UZ = - BS + 4 = - 2 + 4 = 2

3) UZ = v1 I + v2 C + v3 S

Z prvé rovnice po úpravě dostaneme vyjádření C a S jako funkce I:

$$C = \frac{v_2}{v_1} I, \quad S = \frac{v_3}{v_1} I \tag{4}$$

Substitucí za C a S do rovnice (3) dostaneme explicitní vyjádření nové hodnoty zabezpečovacího systému I:

$$v_1 I + v_2 \frac{v_2}{v_1} I + v_3 \frac{v_3}{v_1} I = v_1 I + \frac{v_2^{\,2}}{v_1} I + \frac{v_3^{\,2}}{v_1} I = UZ \quad \Rightarrow I_2 \tag{5}$$

$$I = I_2 = \frac{UZ}{v_1 + \frac{v_2^{\,2}}{v_1} + \frac{v_3^{\,2}}{v_1}} = 2{,}35294 \tag{6}$$

Obdobným způsobem zjistíme nové hodnoty u prevence náhodných poruch **C** a u minimalizace škod **S:**

$$C = C_2 = \frac{UZ}{v_2 + \frac{v_1^{\,2}}{v_2} + \frac{v_3^{\,2}}{v_2}} = 1{,}765 \tag{7}$$

$$S = S_2 = \frac{UZ}{v_3 + \frac{v_1^{\,2}}{v_3} + \frac{v_2^{\,2}}{v_3}} = 1{,}765 \tag{8}$$

Zhodnocení možností bezpečnostního balance

Naléhavost změny organizační bezpečnosti reaguje nepřímo úměrně s pozitivním trendem úspěšnosti zvládání bezpečnostních hrozeb. Proto si je možné všimnout, že nejpříznivější okolnosti pro „odzkoušení“ nově vzniklého bezpečnostního opatření v podnikovém dění jsou v situaci, kdy má subjekt viditelné slabiny ve svých strategických oblastech bezpečnostní politiky. Paradoxně je procesu zavádění nebo nastavování nové úrovně zabezpečení nejvíce fanděno ve firmě, která zjistila svůj nepříznivý vývoj ve svém snažení eliminovat systémové poruchy bezpečnosti. Bohužel tento subjekt má mnohem menší potenciál pro tvorbu úspěšných zabezpečovacích inovací, díky existenci nevhodných předpokladů. Tato absence vhodných podmínek pro vytvoření konceptu pozitivní změny ale není daná neochotou odpovědných pracovníků. Na druhou stranu se nejlepší nápady neočekávaně často objevují v situaci zvýšených bezpečnostních hrozeb, které přerostly ve firemní krizi. Pracovníci zde pracují pod stresem a často ze sebe vydají to nejlepší. Z rozboru, co je překážkou vytvoření a implementace komplexního zabezpečení subjektu, vyplývá, že odpor proti přepokládané kladné změně v úrovni agregované bezpečnosti vzniká jak u úspěšných podniků, tak i u firem v situaci neúspěchu. U podniku, který má výhodný trend výsledků svého podnikatelského snažení, je brzdou bezpečnostní změny její implementace, kdežto ve firmě, která má výsledný podnikatelský trend složený z prohlubujících neúspěchů, je nevětší překážka ve vytvoření konceptu globální bezpečnosti..

Literatura

[1] Procházková, D.: *Krizové řízení*. Praha : MV ČR- GŘ HZS, 2004.
[2] Nečas, S., Seiler, M.,: *Loupežná přepadení pracovišť s peněžním provozem a jejich bezpečnost (policejní, kriminalistické a teoretické aspekty teorie a praxe ochrany osob a majetku)*. Praha : Policejní akademie ČR, 2004
[3] Pitra, Z.: *Příprava a provádění organizačních změn*. Praha : Grada, 1998.

Ing. Tomáš Macák, SVŠES, s. r. o., Lindnerova 575/1, Praha 8,
E-mail: tomas.macak@svses.cz