Měření Operačních Rizik

Jan Mikulecký, Ph.D., CISM

Článek byl publikován v roce 2008 v říjnovém vydání IS Control Journal – Journal Online

Před několika lety byla mezi operační rizika zahrnuta všechna ostatní rizika, která nejsou tržní nebo kreditní. Tato vágní negativní definice však byla zcela nedostatečná, aby mohla být operační rizika správně a efektivně řízena. Základem pro měření rizik je pochopit jejich podstatu, zdroje rizik, konsekvence, což bez jasné definice nelze zajistit.

BASEL II (International Convergence of Capital Measurement and Capital Standards) definuje operační riziko jako riziko ztráty vyplývající z nedostatečně či chybně nastavených interních procesů, z chyb způsobených lidmi, systémy nebo externími vlivy. Tento standard pro řízení rizik je určený pro banky a jiné finanční instituce, kde je termín *operační riziko* poměrně zažitý a ustálený.

Operační riziko je i v ostatních (nebankovních) organizacích často spojováno zejména s informačními systémy a proto je operačním rizikem často míněno *riziko provozní*. Jeho měření tak více souvisí s hodnocením rizik informačních systémů a s úrovní a kvalitou jejich bezpečnosti.

Výše uvedené definice a termíny určitě pomáhají pochopit problematiku měření operačních rizik, avšak, podobně jako jiné definice, dávají poměrně velký prostor pro diskusi, co vlastně znamená „měření rizik“. Každá taková diskuse by měla být zaměřena spíše na účel měření než na jeho přesnou definici. Otázky, co by mělo měření rizik přinést organizaci nebo jak by takové měření mělo prospět ke zvýšení bezpečnosti, jsou zásadní a odpovědi na ně směřují k přesné definici pojmu „měření rizik“, která bude relevantní pro konkrétní firmu a organizaci. Bez ohledu na definici „měření rizik“ a nebo pojmenování rizik operačními nebo provozními musí měření kvantifikovat data pro pochopení podstaty rizik. Měření operačních rizik lze tedy rozdělit na dva fundamentální procesy:

- Měření velikosti operačních rizik;
- Měření úrovně zvládání operačních rizik.

Cílem obou měření je kvantifikace předem stanovené veličiny, která vyjadřuje velikost rizika, míru jeho pokrytí (zvládnutí) nebo například počet či poměr akceptovaných rizik. V ideálním prostředí pro řízení rizik by do procesu měření operačních rizik mělo patřit také měření přínosů. Možnost kvantifikace efektivnosti bezpečnostních opatření a nebo zvýšení úrovně bezpečnosti by měla být v portfoliu každého risk manažera. Nicméně měření přínosů zvládání operačních rizik není jednoduché a využívané nástroje a metody se v dnešní době omezují na velmi jednoduché tabulky v excelu.

Případová studie banky

Každá slovenská banka musí na základě Opatrenia Národnej banky Slovenska č. 12/2004 o rizikách a systéme riadenia rizik provádět mimo jiné i pravidelné analýzy operačních rizik v souvislosti s informačními technologiemi. Jedná se o obdobu Opatření České národní banky č. 2 ze dne 3. února 2004 k vnitřnímu řídicímu a kontrolnímu systému banky a částečně také nové vyhlášky 123/2007, která je prováděcí k zákonu 256/2004 a prakticky se jedná o implementaci BASEL II.

Provedení analýzy rizik bylo jen jednou částí celého projektu, jehož hlavním cílem bylo zavedení procesu měření operačních rizik. Analýza byla prvotním krokem k poznání aktuální velikosti měřených rizik, ale celý proces musel zahrnovat adaptaci osvědčené metodiky pro analýzu rizik a vytvoření opakovatelných postupů pro celkové řízení operačních rizik. Součástí tak bylo i sestavení jednoduše pochopitelných a transparentních metrik pro měření zaprvé velikosti, zadruhé úrovně zvládání operačních rizik.

Metriky musely splňovat několik základních parametrů, které byly definovány zejména na základě zkušeností amerických odborníků. Každá metrika musela být[1]:

- Konzistentně měřitelná, bez subjektivních kritérií – pokud jednu metriku použije více osob, musí dojít ke shodným výsledkům;
- Jednoduše naplnitelná, ideálně automatickou cestou;
- Vyjádřitelná v kardinálních číslech nebo procentech, nikoli v kvalitativních škálách „nízká, střední, vysoká“;
- Vyjadřující vše v jedné jednotce, například hodiny, incidenty, finanční ztráty

V první fázi vznikly globální metriky pro měření velikosti rizik a úrovně zvládání rizik. Následně byly zaváděny další, více detailní metriky zaměřené na konkrétní operační rizika a zranitelnosti (např. síla hesla v jednotlivých systémech, bezpečnostní incidenty) a také například metrika souladu s bezpečnostní normou ISO/IEC 27001. Všechny metriky byly sestaveny tak, aby sběr dat byl snadný a rychlý, pokud možno co nejvíce automatizovaný.

Sekundárním cílem stanoveným pro rok 2008 je vytvoření rozhraní metrik pro metodiku RMA and RiskBusiness KRI Framework Study, která v bance slouží jako hlavní přístup pro řízení rizik v souladu s BASEL II.

Měření velikosti operačních rizik

Velikost, nazývaná také míra rizika, byla výstupem z analýzy rizik, která byla provedena kvalitativní metodikou. První část analýzy zkoumala velikost dopadů narušení bezpečnosti na činnosti banky a dosahování jejích obchodních cílů. Ve druhé části byla analyzována pravděpodobnost, která byla stanovena na základě hodnocení hrozeb a zranitelností ICT.

Metrika pro stanovení velikosti rizika obsahovala škálu 1-7, v rámci které bylo vypočteno 27.893 hodnot jednotlivých rizik. Toto extrémní číslo zahrnuje různé kombinace identifikovaných následků, pravděpodobností a aktiv informačního systému banky. Z pohledu operačních rizik jich bylo hodnoceno 21 a tento počet hodnot byl také součástí finálního souhrnu, který byl prezentován na konci projektu. Manažerské shrnutí, které bylo kromě jiného součástí každé zprávy o hodnocení rizik, vypadalo následovně.

Graf ukazuje velikost rizika ve škále 1-7 a jeho charakteristiku, tedy poměr jednotlivých složek rizika (dopad a 2 složky pravděpodobnosti – úrovně hrozeb a zranitelností), jak se podílejí na výsledné míře.

Měření úrovně zvládání operačních rizik – základní metriky

Všechna analyzovaná rizika byla po provedené analýze vyhodnocena a bylo rozhodnuto, která budou akceptována, a která zvládnuta, a nebo zda budou zvolena taková opatření, aby se riziko eliminovalo zcela (vyhnout se riziku).

Pro všechna rizika, která nebylo možné akceptovat ani se jim vyhnout, byla navržena opatření, která měla pokrýt konkrétní operační riziko a tím zajistit jeho zvládnutí. Při návrhu detailních opatření bylo nutné brát v úvahu také ta stávající. Zhodnocení stávajícího stavu bylo jedním z parametrů, na základě kterého je později určena mj. i priorita pokrývání daného rizika. Využívaná metodika pro hodnocení rizik obsahovala rozsáhlý seznam protiopatření. Byla tak k dispozici celá řada doporučení jak určitá rizika zvládnout.

Doporučená bezpečnostní byla po vyhodnocení rozdělena na dvě množiny, které se staly základem pro další metriku. Protiopatření, která byla doporučena pro pokrytí daného rizika a již byla implementována, spadala do první zelené skupiny. Opatření, která nebyla zatím zavedena, tvořila druhou červenou skupinu. Porovnáním seznamu opatření se skutečností bylo tedy možné určit míru pokrytí rizika, která byla stanovena na základě počtu existujících - zelených a doporučených – červených opatření.

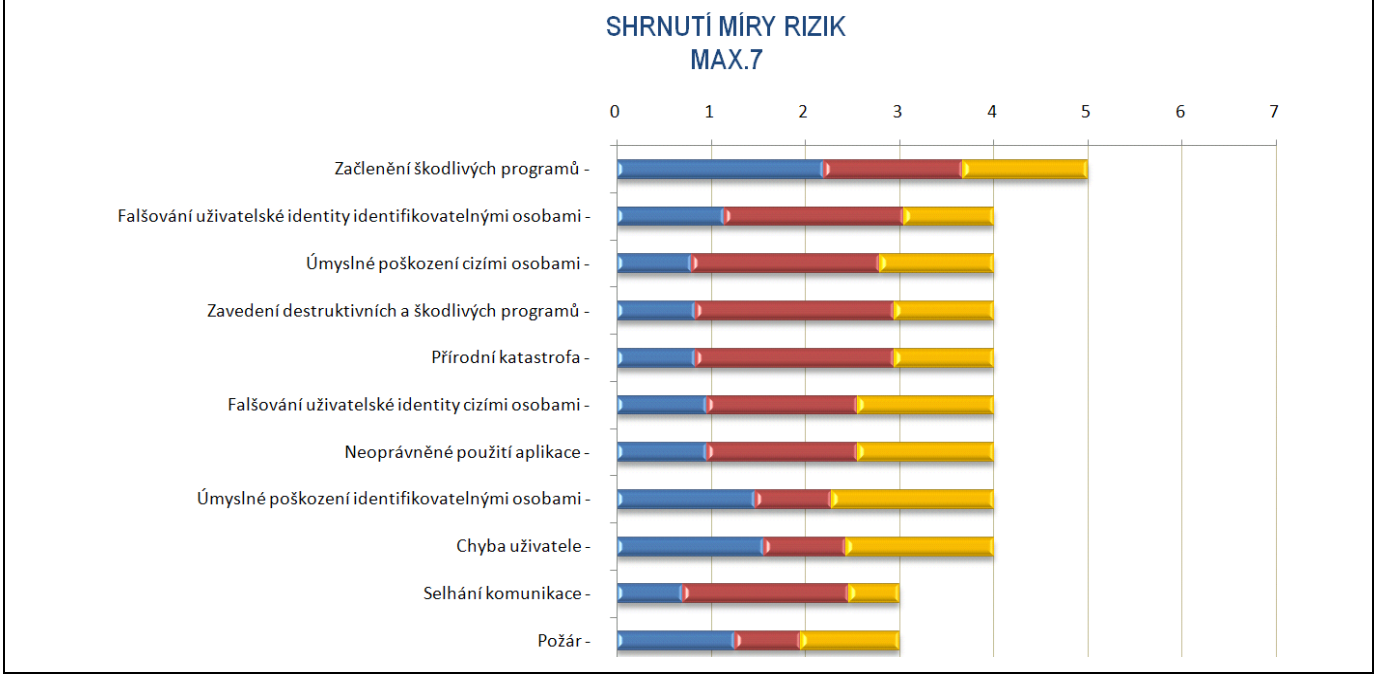
Mezi riziky a protiopatřeními byla vazba n:n, tzn. že pro jedno riziko bylo doporučeno opatření, které zároveň pokrývalo riziko jiné. Podstatou metriky však bylo procento pokrytí jednotlivých rizik a z tohoto pohledu bylo každé opatření unikátní. Proto i v případě, že protiopatření bylo do metriky započítané několikrát, nijak metriku nenarušovalo.

Výsledkem vyhodnocení doporučených bezpečnostních opatření byl následující graf (opět uveden v manažerském souhrnu).

Celkový obrázek stavu bezpečnosti v bance dokreslují oba grafy posazené proti sobě. Při ukázce výsledků analýzy byly obě metriky prezentovány současně, aby vznikl jednotný a sumární pohled na velikost operačního rizika a zároveň na úroveň jeho pokrytí.

První riziko v grafech dosahuje úrovně 5 (ve škále 1-7) a je pokryto z přibližně 93%. Tento přístup tedy transparentně naplňoval dva základní procesy měření – velikost operačního rizika a úroveň jeho pokrytí. Díky své jednoduchosti byly prezentované výsledky pro manažery banky velmi rychle srozumitelné a nenastala situace, kdy krčili své nosy a pokládali útočné otázky, jako například „…a tohle mi je k čemu?“.

Figure 1: Graf shrnutí míry rizik



Měření úrovně zvládání operačních rizik – detailní metriky

Bezpečnostní opatření však nebyla posuzována pouze výše uvedeným binárním zeleno-červeným způsobem. Metodika pro analýzu rizik dovolovala popsat více situací, v jakých se nachází určité aktuální bezpečnostní opatření.

Některá prvotně doporučená opatření byla při dalším vyhodnocování operačních rizik označena jako *Akceptovatelná*. Bylo rozhodnuto, že takové protiopatření nebude i přes jeho jasné přínosy implementováno. V tomto případě zůstalo riziko částečně nepokryté a bylo nutné určit, zda úroveň nepokrytí rizika nepřesahuje předem stanovenou akceptovatelnou míru 8% (reálně byla akceptovaná úroveň rizika 4,11%).

Vybraná opatření byla také označena jako *Neaplikovatelná*, protože navržený způsob zvyšování bezpečnosti nebyl technologicky proveditelný nebo šel zcela proti hlavnímu businessu banky. Opatření, která nebyla zatím zavedena, ale ustavičně se pracovalo na jich implementaci (projekty byly v běhu), byla označena stavem *Návrh se realizuje*.

Použitím dalších stavů bezpečnostních opatření vznikly více detailní metriky, které znázorňovaly celkový pohled na informační bezpečnost banky. Je jasně vidět, že proces zvládání operačních rizik byl správně nastaven, nicméně stále existují rizika, která nejsou pokryta (červený sloupec). Graf také ukazuje očekávaný progres v implementaci nových protiopatření, která byla realizována v průběhu analýzy (celkem analýza trvala 5 měsíců).

Následující graf znázorňuje jednotlivé oblasti bezpečnosti a poměr zavedených, neaplikovatelných, doporučeních a dalších bezpečnostních opatření.

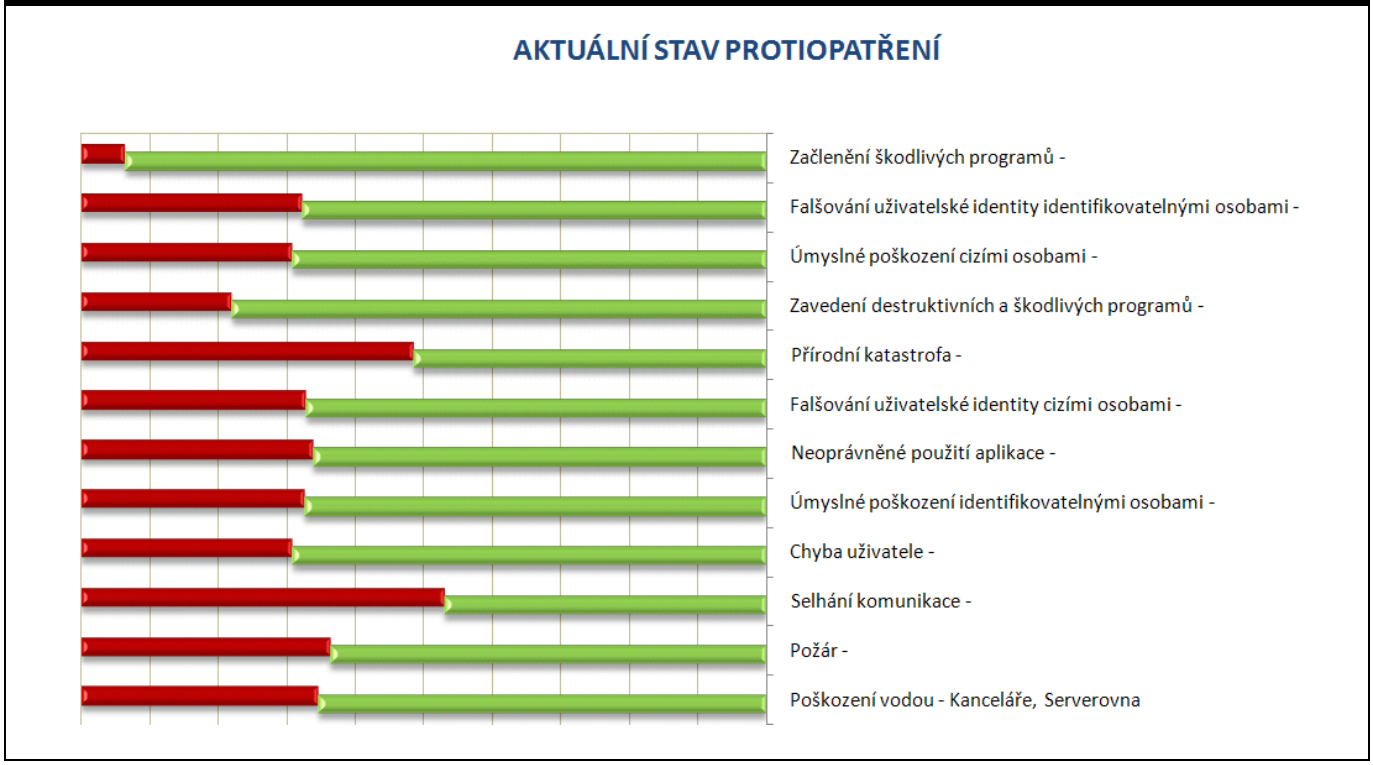
Každá výše popsaná metrika za sebou skrývala tisíce detailních hodnot, které však ve svém analytickém detailu nebyly prezentovatelné. Cílem zjednodušených grafů bylo ukázat v rychle pochopitelné formě pohled na výsledky analýzy a na úroveň zvládání operačních rizik v bance. Na základě čtyřech parametrů metrik, které byly stanoveny na začátku projektu, byl každý graf sestavován tak, aby mohl být aktualizován v okamžiku a s nejmenším úsilím. Zároveň byly vytvořeny postupy pro sběr hodnot v čase, aby mohl být stav zvládání rizik posuzován v čase.

Graf ukazuje, jak narostl počet zavedených opatření, tzn. že proces zvládání rizik byl vylepšen. Ostatní stavy klesly a změnil se i celkový počet protiopatření. Proces identifikoval nová rizika a zároveň došlo ke změnám v informačním systému. V rámci procesu řízení změn byly posouzeny bezpečnostní dopady a navržena ideální opatření na pokrytí aktuálních operačních rizik.

Měření přínosů zvládání operačních rizik

Implementace protiopatření pro zvládání rizik není jednoduché a jako optimální způsob se ukázalo vytvoření implementačních projektů, které měl realizovat personál banky. Zvýšit bezpečnost autentizace do systému SAS je většinou mnohem složitější než provést projekt Implementace Smart-Cards v systému SAS (i když ve skutečnosti se jedná o stejnou věc). Složitější zejména ve smyslu přidělení a schválení zdrojů na projekt. Sehnat sponzora pro implementaci skupiny bezpečnostních opatření je v bankách, na peníze orientovaných institucích, záležitost téměř nemožná. Oproti tomu sehnat sponzora pro *projekt* je, ne přímo jednoduché, nicméně méně složité.

Figure 2: Graf aktuálního stavu bezpečnostních opatření



Jednotlivá opatření doporučená k realizaci a nebo jejich skupiny tvořily obsah projektů zaměřených vždy na určitou problematiku. Pro banku bylo tedy vytvořeno 13 implementačních projektů; níže jsou uvedeny příklady pěti z nich:

- Log Management – nákup a implementace řešení pro kontinuální vyhodnocování aplikačních i systémových logů;
- Dvoufaktorová autentizace pro VPN – nákup a implementace prostředků dvoufaktorové autentizace pro připojení prostřednictvím VPN;
- Poplachy IPS a IDS – zvýšení efektivity využívání IPS (Intrusion Prevention System) a IDS (Intrusion Detection System) pro automatické poplachy při narušení bezpečnosti;
- Havarijní plány – vytvoření havarijních plánů a plánů kontinuity pro všechny systémy SZRB jednotlivě s řízeným přístupem k daným dokumentům;
- Práce s médii – vytvoření a prosazení řídícího dokumentu pro práci s médii (pásky, CD, DVD, paměti flash apod.).

Figure 3: Graf stavů protiopatření

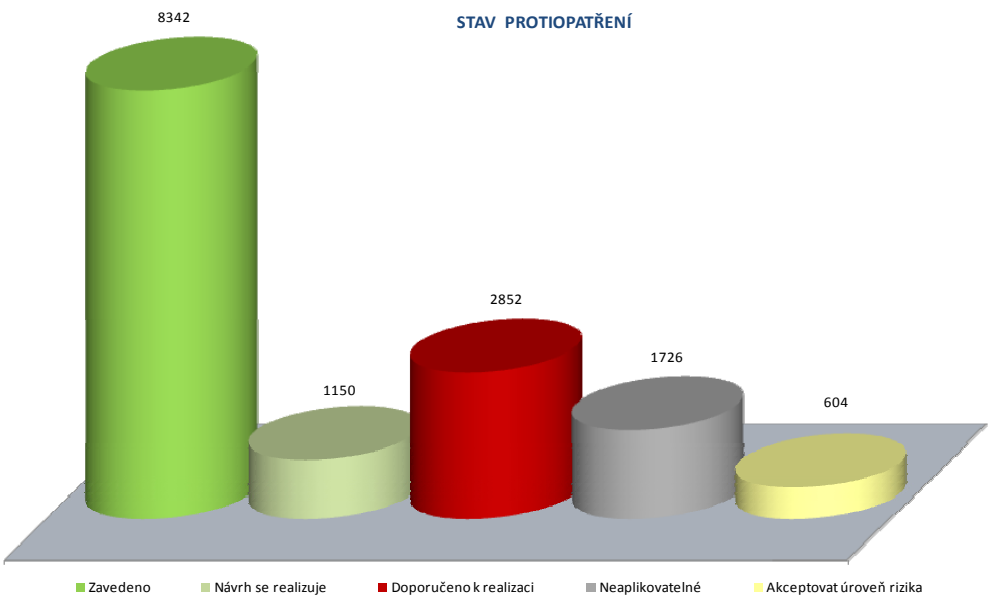


Figure 4: Graf stavů protiopatření podle oblasti bezpečnosti

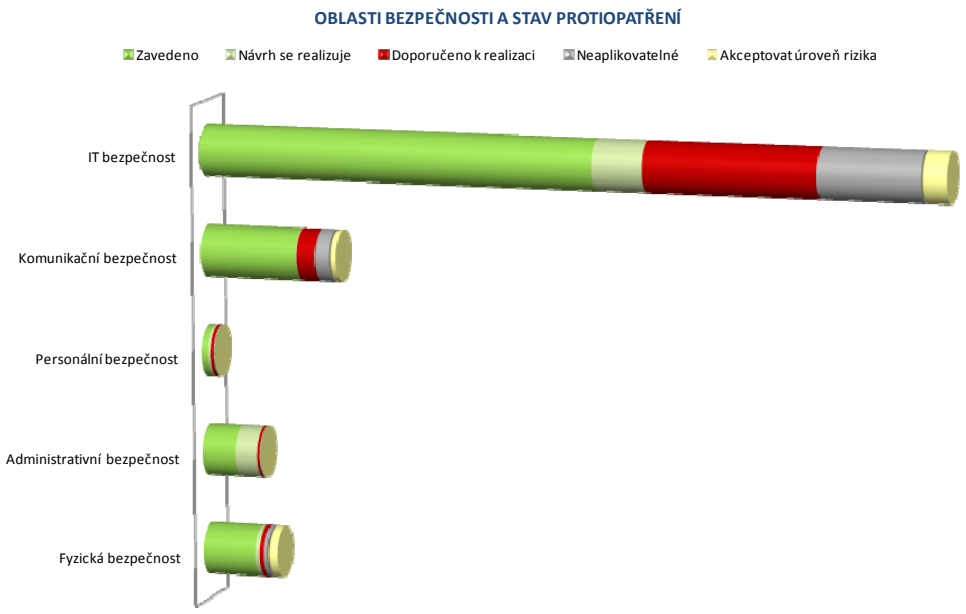
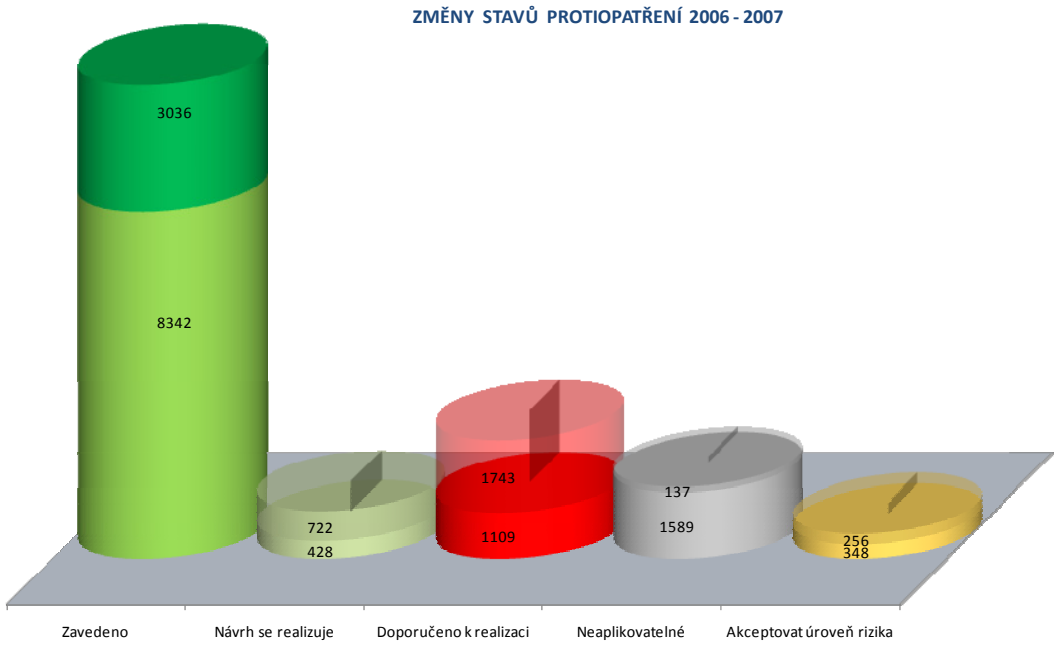


Figure 5: Graf změn stavů protiopatření v čase



Cílem projektu bylo implementovat určitou sadu protiopatření, což v praxi znamenalo změnit jejich stav „z *červeného* na *zelený*“. Výše uvedené metriky pracovaly právě se s stavy protiopatření, proto nebylo složité měřit přínos implementace. Pro manažerskou prezentaci přínosů implementačních projektů byla zvolena metrika, kde základem byla oblast bezpečnosti (IT, komunikační, personální, fyzická, administrativní). Provedený projekt tedy změnil stavy protiopatření v dané oblasti bezpečnosti a byl tak určitým přínosem pro danou oblast. Pokud byl projekt proveden, byla zvýšena bezpečnost v dané oblasti a relevantní rizika byla lépe zvládána. Měřítkem, o kolik se pokrytí rizik zvýšilo, byly počty stavu protiopatření.

Následující horní graf ukazuje aktuální stav v oblasti bezpečnosti PŘED implementací skupiny opatření realizované v rámci jednoho projektu. Spodní graf ukazuje stav PO dokončení projektu. Opatření, která byla doporučena k implementaci (červená barva), změnila po dokončení projektu svůj stav a stala se opatřeními existujícími (zelená barva).

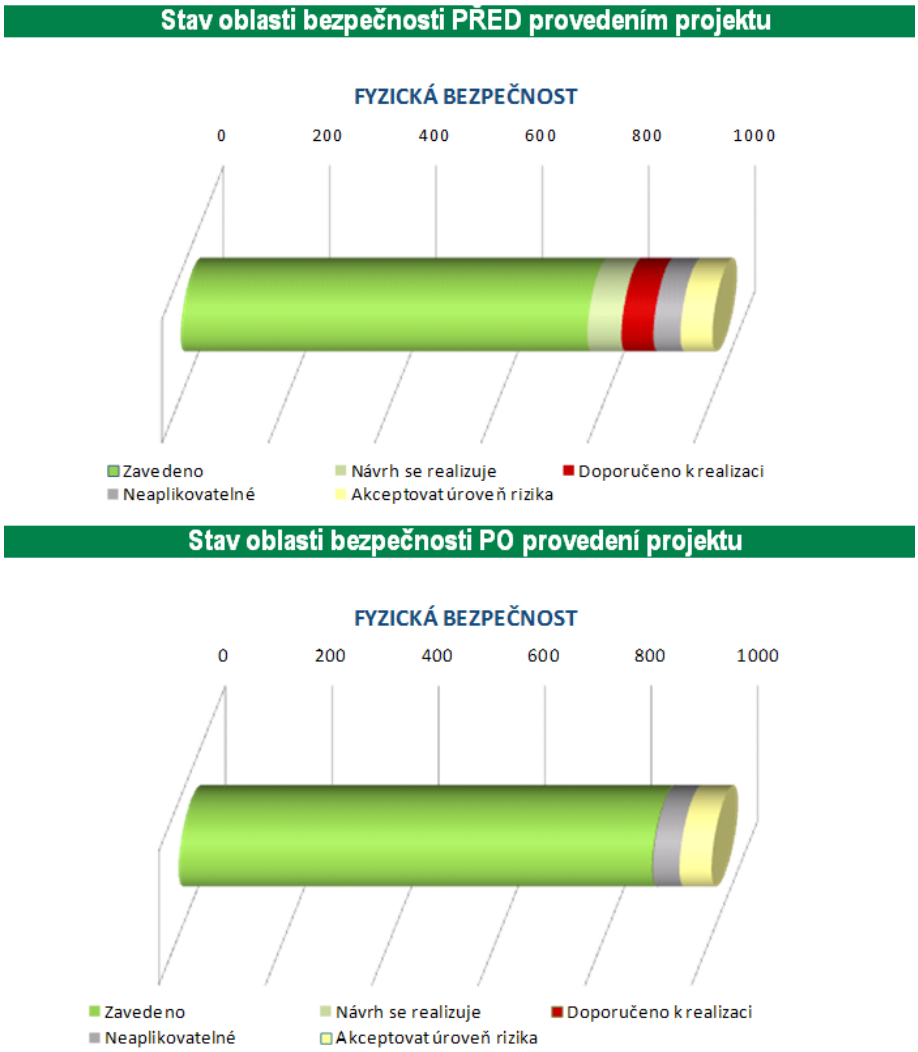
Podle počtu opatření a jejich aktuálních stavů bylo možné prokazatelně predikovat úroveň pokrytí jednotlivých rizik s ohledem na navržené projekty. Každé opatření, které pokrývalo určité riziko nebo rizika, bylo začleněno do daného projektu. Pokud byl určen aktuální a budoucí stav opatření, bylo možné transparentně stanovit aktuální i budoucí úroveň pokrytí jednotlivých operačních rizik nebo souhrnně stanovit budoucí úroveň bezpečnosti v bance, v její části nebo v určité oblasti.

Závěr

Základním kamenem pro správně měření operačních rizik je, aby bylo prováděno stále stejnou metodikou, nebo aby byla využita dostatečně kvalitní rozhraní mezi různými metodikami a nástroji. Je velmi důležité sestavit takové metriky, aby bylo jednoduché a rychle pochopitelné stanovovat úroveň rizik a jejich zvládání v čase a sledovat tak trendy nebo provádět pravidelně benchmarking.

Měření nejen operačních rizik, ale celé bezpečnosti, je stále nová oblast, která bude v příští letech mnohem více skloňovaná. Doba pokročila do stádia, kdy řada „IT-driven“ organizací má zavedené systémy řízení bezpečnosti a umí měřit rizika. Přínosy bezpečnosti, změny v úrovních zvládání rizik nebo vývoj bezpečnosti v čase jsou však veličiny, které zatím umí vyhodnotit málokterý bezpečnostní manažer. Hlavním důvodem je právě neznalost procesů měření a malé povědomí o metrikách, jejich sestavování, využívání a prezentaci. V očekávání je nový standard ISO/IEC 27004 Information security management measurements, který by měl vnést světlo do bezpečnostních metrik a celkového procesu měření. Zatím je k dispozici několik jiných standardů a zahraničních publikací, viz zdroje.

Figure 6: Grafy stavů bezpečnosti před po provedení implementačního projektu



Zdroje a reference

[1] AZ/NZS 4360:2004 Risk Management

[2] ISO/IEC 27001 & 27002 Implementation Guidance and Metrics

[3] BIP 0074 Measuring of effectiveness of ISMS implementation

[4] NIST SP 800-55 Security Metrics Guide for Information Technology Systems

[5] NIST SP 800-80 Guide for Developing Performance Metrics for Information Security

[6] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley, 2007

Poznámky

[1] Andrew Jaquith, Security Metrics, Addison-Wesley, 2007, str. 22

Jan Mikulecký, Ph.D., CISM

Pracuje jako senior konzultant ve společnosti Risk Analysis Consultants od roku 1999. Hlavní specializací je provádění analýzy rizik informačních systémů a zavádění ISMS a BCM ve velkých organizacích. Dále školí metodiky a standardy v oblasti bezpečnosti informací v Česku i dalších zemích Evropy. Absolvoval ČVUT v Praze, kde získal titul doktor.

Kontakt: jan.mikulecky@rac.cz.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.