

Řízení rizik v bezpečnosti služeb IT

Petr Svojanovský, Jitka Kreslíková
Fakulta informačních technologií VUT, Božetěchova 2, 612 66 Brno
svojanov@fit.vutbr.cz, kreslika@fit.vutbr.cz

Abstrakt

Práce se zabývá zajištěním informační bezpečnosti IT služeb za použití nově vyvinutého systému řízení rizik. Vychází ze standardů ISO/IEC 20000 Informační technologie – Management služeb, ISO/IEC 27001:2005 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky a doporučení organizace Bank Information Technology Secretariat, která v souvislosti s řízením operačních rizik v bankovním prostředí v roce 2002 publikovala doporučení BITS Technology Risk Transfer Gap Analysis Tool. Nad těmito základy práce staví nový způsob zabezpečení poskytované služby tak, že hodnotí možnosti zvládnání rizik na obou stranách kontraktu a dle hodnocení opatření vybírá optimální varianty zvládnání rizik.

Klíčová slova

Řízení služeb IT, Informační bezpečnost, Řízení rizik, Poskytovatel služby IT, Konzument služby IT.

1. Úvod

V České republice rok od roku roste počet společností a firem orientovaných na IT, které se rozhodly certifikovat své vnitřní prostředí řízení dle některého z mezinárodních standardů. O tom je možné se snadno přesvědčit prohlídkou webových prezentací předních i méně známých dodavatelů IT služeb. Kromě certifikací systémů řízení kvality a environmentálního managementu jsou již dnes běžné certifikace pro řízení služeb IT (ISO/IEC 20000), informační bezpečnosti (ISO/IEC 27000), zatím bohužel zaostávají certifikace v oblasti řízení kontinuity činností organizace.

Pokud se blíže podíváme na standardy ISO/IEC 20000 a ISO/IEC 27000, zjistíme, že mají mnoho společného. I proto se organizace ISO/IEC chystají na vydání standardu zaměřeného právě na společnou implementaci těchto dvou oblastí, a to v plánované ISO/IEC 27013.

Tato práce vychází z myšlenky budoucí ISO/IEC 27013 a z potřeby zajistit informační bezpečnost v poskytovaných službách a byznys procesech. Z toho důvodu kvalitativně rozšiřuje Dohody o úrovni služeb (SLA) o Dohody o bezpečnosti (PLA). Dále si v práci autoři uvědomují, že již dávno se nelze soustředit pouze na ohraničené prostředí jedné organizace, ale řídit ho jako celek, a to včetně vstupů a výstupů v podobě například dodavatelů nebo konzumentů služby IT.

Toto se nemůže obejít bez propracovaného systému řízení rizik, který reflektuje novou situaci „vícedoménového“ prostředí. V předkládané práci je vyvinut unikátní systém řízení rizik (ne jejich identifikace a analýzy, pro kterou existuje nesčetně metod), který umožňuje optimalizovat výběr opatření na zvládnání rizik na jednotlivých stranách kontraktu poskytované služby IT. K tomu zavádí dva parametry hodnocení opatření, a to relevanci a jeho vyspělost. Z nich poté odvozuje schopnost daných opatření zvládat riziko s tím, že tato

schopnost může být rozdílná na rozdílných stranách kontraktu. Tento nově vyvinutý způsob představuje významný posun v oblasti řízení rizik, na kterém je možné stavět další postupy a modifikovat je dle konkrétních potřeb organizací. Je vhodné poznamenat, že tento nově vyvinutý systém řízení může být s úspěchem provozován i v „jednodimenzionálním“ prostředí, to znamená uvnitř jedné organizace.

Text je členěn následovně:

- Prvně jsou velmi stručně představena metodická východiska – oba standardy ISO/IEC 20000 a ISO/IEC 27000 a použitá metoda pro analýzu rizik;
- Následně jsou definovány Dohody o bezpečnosti poskytované služby IT;
- Druhou stěžejní část práce tvoří popis nového systému řízení rizik;
- Závěr práce je věnován případové studii, která prokazuje funkčnost metody a napomůže implementacím v praxi.

Záměrně není v práci podrobně diskutována metoda pro analýzu rizik. Důvodem je to, že práce ke svojí implementaci žádnou konkrétní nepotřebuje. Jediným požadavkem na analýzu rizik je, aby jako jednu z hodnocených služek rizika obsahovala zranitelnost, která je následně snižována, odděleně od ostatních parametrů.

2. Metodická východiska

Tato kapitola stručně představuje standardy a doporučení, na kterých práce stojí. Cílem samozřejmě není jejich detailní popis, ale poskytnutí základního rámce. Pro hlubší pochopení je nutné studium výše uvedených standardů.

2.1. ISO/IEC 20000

Standard ISO/IEC 20000 [1, 2] je určen pro implementaci procesů, které zajistí poskytování IT služeb dle tzv. best practices. Je to první mezinárodní standard zaměřený na management služeb v IT. Je založen na britském standardu BS 15000, který také nahrazuje. ISO/IEC 20000 Je procesně orientovaný standard. To znamená, že není určen pro hodnocení produktů nebo poskytovaných služeb.

ISO/IEC 20000 může být použit k implementaci procesů dle nejlepších praktik, vyslání pozitivního signálu zákazníkům – zákazník ví, že procesy podporující nakupovanou službu jsou na té nejvyšší úrovni, zabezpečení konzistentního přístupu všech dodavatelů v dodavatelském řetězci, měření současné úrovně procesní vyspělosti poskytovatele služeb IT, zlepšování efektivity a výkonu společnosti pomocí neustálého zlepšování.

ISO/IEC 20000 je tvořen dvěma částmi. Požadavky v [1] a doporučeními pro implementaci v [2]. Z jiného pohledu je standard tvořen popisem vzájemně provázaných procesů, jejichž stručný přehled následuje.

Požadavky na systém managementu: cílem je poskytnout efektivní systém managementu, kde vrcholoví představitelé společnosti poskytují doklady o své vlastní angažovanosti, stanovují politiku a komunikují ji dovnitř společnosti a v neposlední řadě poskytují svým zaměstnancům možnost vzdělávání tak, aby byli připraveni efektivně vykonávat své role.

Plánování a implementace managementu služeb: aplikuje dnes již, revoluční PDCA metodologii na všechny procesy. PDCA zastupuje slova Plan-Do-Check-Act neboli Plánuj-Dělej-Kontroluj-Jednej. Jedná o logický a intuitivní postup, kde je daná služba prvně naplánována (cíle a jak jich dosáhnout, politika organizace), poté jsou procesy naimplementovány do praxe a neustále monitorovány a zlepšovány. Revoluční proto, že PDCA cyklus byl navržen již po druhé světové válce, kdy byla do Japonska vyslána skupina statisticky orientovaných vědeckých pracovníků, aby pomohli přebudovat válkou zdevastovanou ekonomiku. Od té doby, tedy již více než padesát let, se PDCA stále používá jako základní princip veškerého řízení. Autorem PDCA je W. Edwards Deming.

Plánování a implementace nových nebo změněných služeb: tento proces zajišťuje proveditelnost nových a změněných služeb při daných nákladech a v dohodnuté kvalitě. Plány musí zahrnovat definici odpovědností za implementaci, komunikaci se všemi zainteresovanými stranami, smlouvy, požadavky na zdroje, metody a nástroje pro měření, rozpočty, atd.

Procesy dodávky služeb: tato kapitola normy mimo jiné popisuje požadavky na SLA (service level agreement, dohoda o úrovni služeb), které musí naprosto jasně specifikovat, jaká služba bude poskytována, jakou bude mít služba kvalitu, případné sankce za porušení dohody, metody monitoringu výkonnosti služby a jiné. Dále striktně nařizuje vést výkazy o službách, zajistit management kontinuity a dostupnosti dané služby. Dotýká se rozpočtování za IT služby, nařizuje provádět management kapacit a zajišťovat informační bezpečnost.

Procesy vztahů: jsou rozděleny na vztahy s byznysem a s dodavateli. Budování dobrých vztahů se zákazníky je založeno na chápání jejich požadavků, dobré komunikaci a proaktivitě. Dobré vztahy s dodavateli jsou nutné právě k uspokojení zákazníka a k udržení kontinuity dané služby.

Procesy řešení: jsou rozděleny na management problémů a incidentů. To jsou dva úzce spjaté pojmy, nicméně existuje mezi nimi rozdíl a je třeba je rozdílně i chápat. Incident je věc okamžité závady, která je v danou chvíli viditelná pro zákazníka. Jako příklad incidentu může být uveden výpadek internetového připojení. Problém je skutečná příčina incidentu. Pokud incidentem je výpadek připojení, potom problémem může být špatně nakonfigurovaný firewall.

Řídící procesy: management konfigurací – cílem je udržovat přesné konfigurační informace prvků služby v konfigurační databázi. Management změn – veškeré změny musejí být řízeny a zaznamenány.

Proces uvolnění: cílem je dodat, distribuovat a sledovat jednu nebo více změn obsažených v jednom uvolnění do produkčního prostředí. Také musejí být vypracovány plány pro případné stažení daného uvolnění v případě nekorektní funkčnosti v produkčním prostředí.

2.2. ISO/IEC 27000

Rodina mezinárodních standardů ISO/IEC 27000 se stala velmi uznávaným, hojně používaným a mnoha implementacemi odzkoušeným návodem pro zajištění informační bezpečnosti. Mezi nejvýznamnější části ISO/IEC 27000 patří:

- ISO/IEC 27001:2005 – specifikuje požadavky na systém řízení informační bezpečnosti (ISMS – Information Security Management System);
- ISO/IEC 27002:2005 (původně ISO/IEC 17799) – soubor postupů pro informační bezpečnost. Z praktického hlediska poskytuje návod, jak konkrétně zajistit vhodnou úroveň informační bezpečnosti a eliminovat tak bezpečnostní rizika;
- ISO/IEC 27005:2008 – řízení rizik v informační bezpečnosti.
- ISO/IEC 27004:2009 – měření v informační bezpečnosti.

Výše uvedený výčet není v žádném případě kompletní, kromě dalších, již platných členů rodiny 27000, ISO/IEC plánuje vydat například ISO/IEC 27013 – návod pro integrovanou implementaci ISO/IEC 20000 a ISO/IEC 27000, ISO/IEC 27036 – bezpečnostní doporučení pro outsourcing a další.

Pokud situaci kolem implementace informační bezpečnosti dle ISO/IEC 27001:2005 maximálně zjednodušíme, tak lze konstatovat, že ISO/IEC 27001:2005 stojí na třech absolutně zásadních nosných principech:

- Řízení informační bezpečnosti staví na PDCA cyklu, to jest na principu neustálého zlepšování. Tímto způsobem je také tento standard navázán například na ISO/IEC 27004:2009 v C fázi a podobně;

- Směry, kam je upřeno úsilí především, je dáno rizikovou analýzou;
- Na základě hodnocení rizik jsou implementována opatření z normy ISO/IEC 27002:2005 (seznam také obsahuje příloha A v ISO/IEC 27001:2005). Pro zajištění informační bezpečnosti organizace není nutno implementovat všechna opatření, například pokud organizace neprovozuje elektronických obchod, tato část samozřejmě nebude implementována. Je třeba však upozornit na to, že během auditu je nutné mít připravené dostatečně věrohodné vysvětlení, proč dané opatření není implementováno. Například nelze neimplementovat opatření týkající se lidských zdrojů prostě proto, že se organizaci nechce.

Tímto popis ISO/IEC 27000 končí, pro další výklad bude dostatečný. V dalších částech práce bude řeč zejména o „aplikaci opatření pro redukci rizika“ a tím je míněna právě implementace opatření ze standardu ISO/IEC 27002:2005.

2.3. Doporučení BITS

Tato část popisuje použitý algoritmus analýzy rizik, a jak je k nim přistoupeno v další práci. Bez dalších podrobností uveďme, že podle doporučení BITS [3] se výsledná hodnota počítá takto:

$$\text{riziko} = \text{dopad} * \text{hrozba} * \text{zranitelnost}$$

s tím, že dopad je potenciální škoda vzniklá při nastalé události, hrozba je pravděpodobnost dopadu a zranitelnost je vlastnost systému, kde hrozba působí. To znamená, že zranitelnost je ve výpočtu to jediné, co lze použít k numerické redukci rizika. Dvojice dopad a hrozba pak definují tzv. rizikový scénář. Veškeré informace o rizicích jsou pak shromažďovány v tzv. registru rizik. Na základě konkrétní metodiky jsou definovány numerické rozsahy pro dopad hrozbu a zranitelnost. Hrozba již byla definována jako pravděpodobnost, zranitelnost definujeme jako pravděpodobnost selhání již existujících opatření a dopad budeme hodnotit na relativní škále od nuly do hodnoty tisíc. Maximální hodnota rizika pak může být také nejvíce 1000. Více informací v [3] a v samotné ISO/IEC 27002:2008.

3. Informační bezpečnosti ve službách IT – dohody o úrovni bezpečnosti (PLA)

Ze stručného popisu ISO/IEC 20000 v předchozích částech práce je patrné, že poskytovatel služeb IT má dva základní úkoly. Řídit své vnitřní prostředí, kde výroba služby probíhá, a dále mít v dostatečné míře pod kontrolou své okolí. Jako příklad může posloužit řízení vztahů s dodavateli. Navíc, dodavatel musí mít absolutně jasnou představu o tom, jakou přesně formu poskytovaná služba má a jaké má parametry – toto je zakotveno v dohodě o úrovních služby (dále bude označováno pouze jako SLA). Pokud je cílem poskytovatele služby IT i adekvátně řídit bezpečnost služby, lze říci, že místo pro definici bezpečnostních parametrů služby je na téže místě, jako definice provozních parametrů – v SLA. Frankova a Yautsiukhin v [4] navrhuje zavedení řízení úrovně a bezpečnosti pro byznys procesy. Poskytovanou službu IT lze jistě považovat za byznys proces. Frankova a Yautsiukhin definují dohodu o úrovni bezpečnosti (dále jen PLA – Protection Level Agreement) jako smluvní verzi SLA se specifickými bezpečnostními kritérii, které poskytovatel služby musí splnit. Jako příklad uvádějí riziko porušení dat klienta při poskytování služby IT.

Tento přístup má však jeden nedostatek. Přijmeme myšlenku, že poskytovatel služby IT a její konzument nejsou nepřátelé, ale partneři, kde je společným cílem oboustranná spokojenost, do které jistě spadá i absence jakýchkoli bezpečnostních incidentů. Potom se lze domnívat, že PLA se skládá ze dvou částí:

- Požadavky na bezpečnost služby IT na straně poskytovatele;
- Podmínky, které musí splnit odběratel služby IT tak, aby byly platné závazky poskytovatele. Jinými slovy, sankce za porušení bezpečnostních parametrů nenese poskytovatel, pokud je závada na straně odběratele.

Kriticky důležitou částí PLA je registr rizik, který byl zmíněn v předchozí části. Musí být zajištěno, že je znám oběma stranám kontraktu a že jej obě strany stejně interpretují a akceptují.

4. Rizika v PLA

Řekli jsme si, že obě strany kontraktu mají zájem na informační bezpečnosti poskytované služby IT. Pokud existuje riziko, že požadovaná úroveň bezpečnosti nebude dodržena, potom obě strany jsou také zainteresovány v jeho zvládnání (snižování zranitelnosti na obou stranách, pokud existuje). Bylo již řečeno, že zranitelnost je snižována implementací opatření z katalogu ISO/IEC 27002:2005. Na každé straně kontraktu jsou samozřejmě vybírána ta opatření, která mají smysl pro dané konkrétní riziko. Aby bylo možno nějakým způsobem porovnávat opatření mezi sebou a mezi poskytovatelem a konzumentem služby, zavedeme následující dvě vlastnosti, které budeme hodnotit u opatření:

- **Relevance opatření** – neboli předpokládaná účinnost opatření je nově definovaný pojem. Vztahuje se k tomu, jak jedno dané konkrétní opatření z katalogu může různě redukovat zranitelnost. Uvedme si příklad: opatření 9.2.1 ISO/IEC 27002:2005 Umístění zařízení a jeho ochrana, bod d jistě může svým způsobem omezit škodu způsobenou požárem v serverovně vhodným umístěním serveru. Naproti tomu opatření 9.1.4 ISO/IEC 27002:2005 Ochrana před hrozbami vnějšku a prostředí (obsahuje také instalace hasících a zhášecích prostředků) má nepochybně vyšší účinnost v případě, že v serverovně požár skutečně vypukne. Proto definujeme množinu relevancí jako bezrozměrnou lineární diskrétní stupnici od 0 do 1, kde 1 značí maximální relevanci daného opatření k danému riziku. Poznamenejme ještě, že jako celé řízení rizik v mnoha ohledech spočívá v odhadech analytiků a manažerských rozhodnutích, tak i přiřazení relevance je úkolem pro zkušeného analytika. V budoucnu je možné rozšíření metodiky o měření na infrastrukturu tak, aby nebylo vždy nutné se spoléhat na odhady.
- **Vypělost opatření** – tento ukazatel je taktéž definován pro každé opatření z katalogu ISO/IEC 27002:2005 a značí, jak je dané opatření již funkční na určité straně kontraktu SLA/PLA. Pokud opatření neexistuje, je číselná hodnota ukazatele rovna nule, opačně jedničce. Tento ukazatel je v přímé souvislosti s tzv. GAP analýzou, která je prováděna v rámci rizikové analýzy dle metodiky BITS, částečně vychází z [5]. V doporučení BITS ale slouží pouze jako intuitivní ukazatel pro analytiku a manažery, zde se bude podílet na výpočtu zvladatelnosti rizika. Tento přístup opět významně rozšiřuje obzory v řízení rizik. Definujeme množinu vypělostí jako bezrozměrnou lineární diskrétní stupnici od 0 do 1, kde 1 značí maximální vypělost daného opatření.

Následující dvě tabulky přesně definují jednotlivé hodnoty relevance i vypělosti opatření:

<i>Stupeň:</i>	<i>Relevance opatření – popis:</i>
0	Opatření není relevantní k dané zranitelnosti, nebude aplikováno. V praxi je možné vypustit.
0,25	Opatření je slabě relevantní k dané zranitelnosti.
0,5	Opatření je relevantní k dané zranitelnosti.
0,75	Opatření je silně relevantní k dané zranitelnosti.
1	Opatření je absolutně relevantní k dané zranitelnosti.

<i>Stupeň:</i>	<i>Vypělost opatření – popis:</i>
0	Opatření není implementováno, jeho implementace se bude maximálně podílet na redukci zranitelnosti.
0,25	Provádění opatření je v praxi pouze intuitivní a opakovatelnost není zajištěna.
0,5	Opatření je definováno.
0,75	Opatření je implementováno a je měřitelné.
1	Opatření je v organizaci implementováno a optimalizováno. Na redukci zranitelnosti se tedy již nebude dalším způsobem podílet.

4.1. Zvladatelnost zranitelnosti

Nyní se podívejme, jak výše definovaná relevance a vypělost umožní hodnotit opatření podle toho, jakou mají schopnost zvládat riziko (jinými slovy zranitelnost). K tomu použijeme tyto dvě úvahy:

- Parametr relevance opatření popisuje, jakou měrou se opatření vztahuje k zvládnutí dané zranitelnosti. Slouží k porovnání jednotlivých opatření. Pokud je relevance jednoho opatření vyšší než jiného, potom více přispívá k redukci;
- Parametr vypělosti opatření definuje, jakým způsobem je již dané opatření v organizaci implementováno. Pokud je již na vysoké úrovni, potom oblasti opatření již není možné učinit významný krok kupředu a tudíž se na redukci nebude podílet takovou měrou, jako jiná opatření s vypělostí nižší.

Neformálně řečeno: každé opatření přispívá k redukci zranitelnosti dílem z relevance, který určuje vypělost. Matematicky:

$$Z_i = \text{relevance}_i * (1 - \text{vypelost}_i)$$

Kde $i \in \langle 1, n \rangle$ a n je počet vybraných opatření.

Pro praktickou použitelnost a odкрыtí určitých souvislostí, které mohou být zatím skryty, řekněme následující:

1. Pokud se na dva rizikové scénáře aplikují stejná opatření z katalogu ISO/IEC 27002:2005 (a žádná jiná), tak to znamená, že relevance opatření definovaná v předchozí části je totožná. Pokud ale má dojít k rozdílné redukci zranitelnosti, musí být v praxi také rozdílná vypělost daných opatření (v případě vyšší zranitelnosti je vypělost opatření nižší);
2. Pokud je relevance dvou opatření například 0,5 a 1, potom se na redukci zranitelnosti první podílí jednou třetinou a druhé dvěma třetinami;
3. Pokud je relevance daného opatření například 0,5 a v praxi je jeho vypělost již na hodnotě například také 0,5, potom se na redukci dané zranitelnosti bude toto opatření podílet pouze hodnotou 0,25 – v kontextu dalších opatření;
4. V katalogu ISO/IEC 27002:2005 vždy existuje minimálně jedno opatření, které má relevanci rovnou jedné. V teoretickém případě, že by takové opatření nebylo možné nalézt, se patrně nejedná o řízení informační bezpečnosti. V tomto případě je nutné zvážit použití jiného katalogu opatření nebo si vyvinout vlastní a s dalšími opatřeními nakládat tak, jako by byly součástí ISO/IEC 27002:2005. Toto není až tak hypotetická úvaha. Například sada kontrol 10.9 ISO/IEC 27002:2005 Služby elektronického obchodu – v případě, že je hlavní součástí byznysu organizace provozování elektronického obchodu, musí organizace zvážit (v souladu s požadavky ISO/IEC

27001:2005) použití i jiného katalogu vztahujícího se k dané oblasti, v tomto případě standardu PCI DSS;

5. Pokud analytik našel zranitelnost, ale identifikoval pouze opatření, která mají maximální vyspělost, udělal analytik chybu. Není totiž možné mít zranitelný systém, který není možné zlepšit. Pokud tomu tak je, je to z důvodu například příliš vysoké ceny opatření apod., ale možnost vždy musí existovat, tedy pokud riziko a s ním spojená zranitelnost systému existuje.

4.2. Agregovaná zvladatelnost zranitelnosti

V okamžiku, kdy jsou rizika zanalyzována (je vyčíslena jejich numerická hodnota), je dalším krokem výběr opatření pro jejich zvládnutí. O několik řádků výše bylo ukázáno, jak jedno dané konkrétní opatření zhodnotit ve smyslu zvladatelnosti rizika. Nyní si představme, že má před sebou analytik řadu opatření a má rozhodnout, které vybrat a které už ne, protože i když se může vázat k danému riziku, nemusí v konkurenci ostatních obstát.

Ještě než ale bude funkce agregované zvladatelnosti definována a ukázána její funkcionalita na příkladech, zopakujme krátce to, co již bylo řečeno. Pochopení tohoto faktu je klíčové: pokud uvažujeme identický rizikový scénář ve dvou rozdílných prostředích s diametrálně odlišnými zranitelnostmi, nutně musí v prostředí, kde je vyšší zranitelnost existovat větší prostor pro zlepšení a tudíž identifikovaná opatření musejí mít menší vyspělost, neboť relevance stejných opatření k stejným rizikovým scénářům je identická. Nebo může být vyšší hodnota zranitelnosti způsobena tím, že je menší počet kontrol implementován a potom je počet opatření vyšší.

Pro zvládnutí rizik vybere analytik sadu opatření, která se nějakým způsobem mohou podílet na zvládnutí zranitelnosti. Jsou dva extrémní případy – analytik vybere buď naprosto všechna vázající se opatření, nebo žádná. Lze očekávat, že rozumné řešení bude ležet někde mezi extrémny. V současných systémech řízení rizik se ono mezi jednoduše odhadne. My si nyní ukážeme, jak ono mezi vypočítat (kompletní výpočet bude dokončen v další podkapitole).

Definujme nejprve matici kombinací K typu (m, n) , kde $m=2^n$, n je počet vybraných opatření. Každá řádek matice je tvořen prvky binárního čísla získaného z převodu dekadického čísla $(m-1)$. Nyní formálně definujme funkci agregované zvladatelnosti zranitelnosti takto:

$$Z_{A_m} = \sum_{i=1}^n K(m, i) * Z_i$$

Kde suma je spočtena pro všechny možné kombinace ne/implementace opatření a Z_i jsou jednotlivé zvladatelnosti zranitelnosti opatření dané konkrétní kombinací.

Pro snadnější představu, jak výše definované formalismy fungují v praxi, uvažujme následující příklad definovaný následující tabulkou:

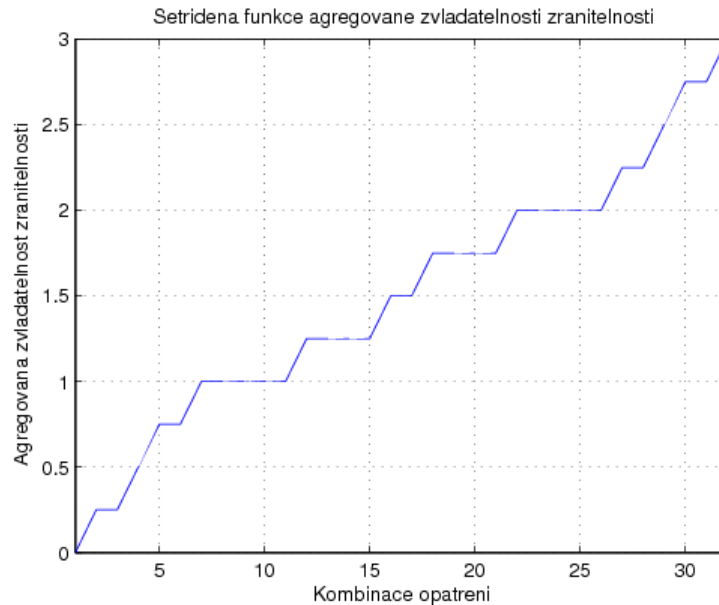
Opatření	1	2	3	4	5
Relevance opatření	0,75	1	0,25	0,5	1
Vyspělost opatření	0	0	0	0,5	0,25
Zvladatelnost zranitelnosti	0,75	1	0,25	0,25	0,75

Dále, kombinace ne/implementace opatření jsou dány následující „maticí“ (z implementačního hlediska nejde o nic jiného, než o převod dekadických čísel od 0 do $2^{\text{počet opatření}}$ do binární podoby):

0 0 0 0 0
0 0 0 0 1

0 0 0 1 0
 0 0 0 1 1
 ...až po
 1 1 1 1 1

Potom každý řádek matice je prvek po prvku vynásoben s vektorem Zvladatelnosti zranitelnosti a násobky jsou sečteny. Výsledek funkce agregované zvladatelnosti zranitelnosti má tedy tolik hodnot, kolik má matic kombinací řádků. Konkrétní hodnoty, pokud se setřídí od nejmenší po největší, jsou zobrazeny na tomto grafu:



Zajímavé je potom sledovat kombinace opatření, jak se změnilo po setřídění. Například v tomto případě vypadá posledních několik kombinací následovně:

0 1 1 1 1
 1 1 1 1 0
 1 1 0 0 1
 1 1 0 1 1
 1 1 1 0 1
 1 1 1 1 1

Už nyní předešleme, že pokud by tato opatření měla být implementována v SLA/PLA prostředí (například první tři opatření na straně poskytovatele a další dvě na straně konzumenta), bude tímto způsobem možné rozhodovat o tom, která opatření na které straně kontraktu budou implementována.

4.3. Funkce optimalizované redukce rizika

Posledním krokem je definice funkce Optimalizované redukce rizika. Nejprve definujme hodnotu „původního“ rizika, tedy v době, kdy je prováděna riziková analýza:

$$R_p = \text{dopad} * \text{hrozba} * \text{zranitelnost}_p$$

A ideální hodnotu rizika, které je dosaženo tehdy, pokud jsou implementována všechna vybraná opatření na 100% (tedy jejich vyspělost je 1).

$$R_I = \text{dopad} * \text{hrozba} * \text{zranitelnost}_I$$

Nyní definujme zranitelnost pro danou kombinaci opatření jako:

$$Zranitelnost_m = (Z_{Am} * (zranitelnost_P - zranitelnost_I)) + zranitelnost_I$$

Jde tedy o vyjádření následující myšlenky: hodnoty vektoru zranitelností nejsou od původní zranitelnosti k ideální zranitelnosti rozděleny rovnoměrně, ale podle hodnot agregované funkce zvladatelnosti zranitelnosti. Tedy podle toho, jak jsou dané kombinace implementovaných opatření přínosné uvnitř daného systému řízení rizik mezi sebou. Potom je hodnota rizika pro danou kombinaci opatření spočtena:

$$R_m = dopad * hrozba * zranitelnost_m$$

Pokračujme ve výše uvedeném příkladu s následující definicí rizikového scénáře (uvedme pouze numerické hodnoty bez příslušného kontextu, který by byl v praxi nutný): Dopad = 350, Hrozba = 50%, Zranitelnost = 50%. Tomu odpovídá hodnota rizika 87,5. Analytik na základě svých zkušeností vybral sadu opatření (viz příklad výše) a stanovil, že pokud budou všechna implementována na maximum, je možné dosáhnout snížení rizika až na hodnotu 2 (čemuž odpovídá hodnota ideální zranitelnosti 1,14%). Pro úplnost je ještě nutno definovat práh akceptovatelnosti rizika. To je v praxi dáno metodikou, my stanovíme hodnotu pro akceptaci 10 (zelená linka v grafu). V případě, že by byla implementace opatření příliš nákladná, je možné tolerovat až hodnotu 30 (s příslušným manažerským rozhodnutím). Potom hodnoty rizika na základě setříděné funkce agregované zvladatelnosti zranitelnosti vypadají následovně:



Příslušné kombinace opatření byly již ukázány výše.

5. Experimentální výsledky

Uvažujme organizaci poskytující služby v oblasti servisu hardware. Služba spočívá v tom, že poskytovatel svým zákazníkům dodává a následně servisuje hardware, kde kromě dohodnutých SLA (viz ISO/IEC 20000) požadavků jsou i požadavky na dodržení informační bezpečnosti. Bylo identifikováno následující riziko (pro demonstraci pouze jedno):

- Popis: riziko ohrožení citlivých informací – nosiče informací jdoucí na servis mohou obsahovat citlivé informace jako konfigurační soubory směrovačů a firewallů; pevné

disky ve stanicích a serverech obsahují další kritická data. Navíc mohou být nosiče dat ve stanicích a serverech posílány poskytovatelem služby IT třetí straně;

- Dopad: 450, pokud nejsou data bezpečně vymazána, může dojít k úniku citlivých informací;
- Hrozba: 0,3 (30%), výskyt hrozby může nastat – riziko se může projevit omylem správců. Úmyslná aktivita je málo pravděpodobná;
- Zranitelnost: 0,3 (30%), nižší úroveň informační bezpečnosti na straně konzumenta služby;
- Výsledná hodnota rizika = 40,5, což dle metodiky znamená požadavek na okamžité snížení.
- Jako ideálně dosažitelná hodnota při implementaci všech vybraných opatření (viz dále) byla stanovena hodnota rovna třem – nižší zřejmě nebude možné zvolit, neboť se jedná o vztah dvou rozdílných subjektů.

5.1. Výběr opatření z ISO/IEC 27002:2005

Pro zvládnutí rizika (zranitelnosti) byla na obou stranách kontraktu vybrána opatření z katalogu ISO/IEC 27002:2005. Následně byla ohodnocena z pohledu relevance k danému riziku a vyspělosti opatření v organizaci (dodavatele anebo konzumenta služby IT).

Na straně dodavatele služby IT byla vybrána a ohodnocena následující opatření:

- 6.1.3; Je nutné přesně určit odpovědnosti v oblasti bezpečnosti informací; relevance = 1; vyspělost = 0,75.
- 7.1.3; Mělo by být definováno a do praxe prosazeno přípustné použití aktiv; relevance = 1; vyspělost = 0,75.
- 7.2.1; Informace by měly být klasifikovány; relevance = 1; vyspělost = 0,75.
- 7.2.2; Na základě klasifikace by měla být aktiva označena; relevance = 1; vyspělost = 0,75.
- 8.2.2; Všichni zaměstnanci organizace (v případě nutnosti i třetí strany) by měli být pravidelně vzděláváni v oblasti bezpečnosti; relevance = 1; vyspělost = 0,75.
- 8.2.3; Musí existovat formální disciplinární řízení; relevance = 0,5; vyspělost = 0,5.

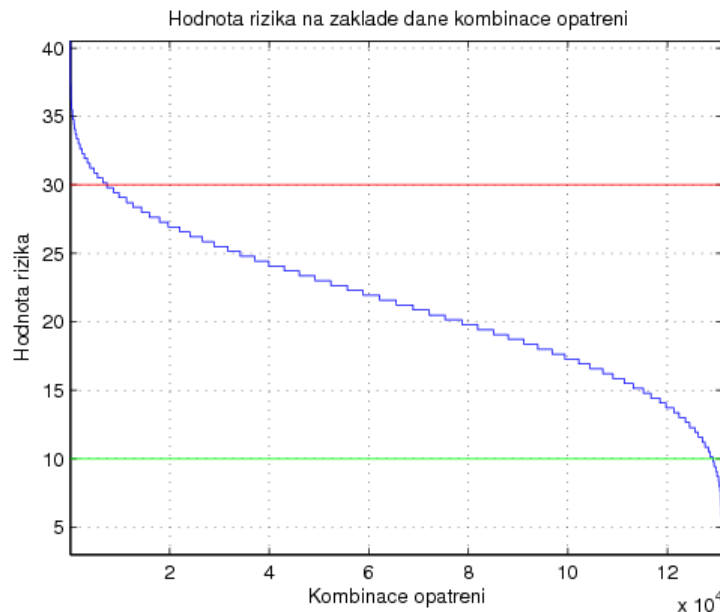
Na straně konzumenta služby IT byla vybrána a ohodnocena následující opatření:

- 6.1.3; Je nutné přesně určit odpovědnosti v oblasti bezpečnosti informací; relevance = 1; vyspělost = 0,75.
- 6.1.5; Měly by být dohodnuty a přezkoumávány požadavky na ochranu informací; relevance = 0,75; vyspělost = 0,75.
- 6.2.1; Měla by být identifikována rizika před tím, než je externímu subjektu povolen přístup k informacím; relevance = 0,25; vyspělost = 0,5.
- 7.1.1; Měla by být identifikována všechna aktiva a jejich seznam udržován aktuální; relevance = 1; vyspělost = 0.
- 7.1.2; Každé aktivum by mělo mít určeného vlastníka; relevance = 1; vyspělost = 0,25.
- 7.2.1; Informace by měly být klasifikovány; relevance = 1; vyspělost = 0,5.
- 7.2.2; Na základě klasifikace by měla být aktiva označena; relevance = 1; vyspělost = 0,5.
- 8.2.2; Všichni zaměstnanci organizace (v případě nutnosti i třetí strany) by měli být pravidelně vzděláváni v oblasti bezpečnosti informací; relevance = 1; vyspělost = 0,5.
- 8.2.3; Musí existovat formální disciplinární řízení; relevance = 0,5; vyspělost = 0,25.
- 9.2.6; Všechna paměťová média (i v zařízeních) by měla být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou data

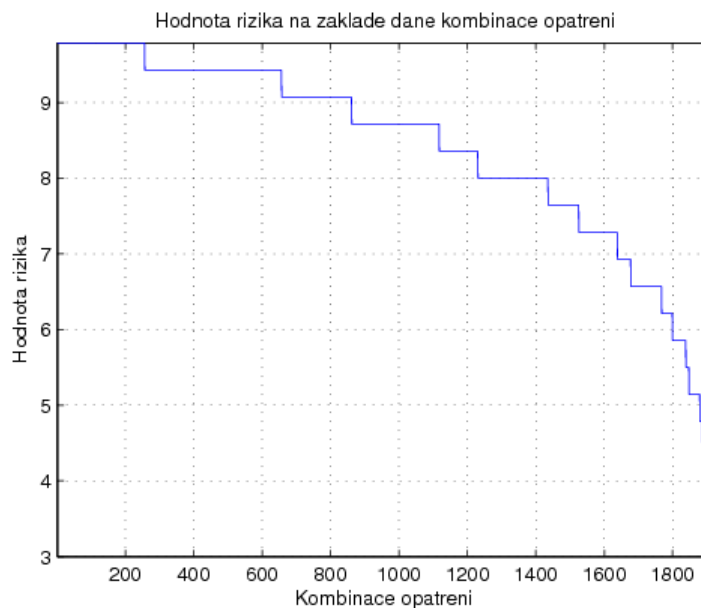
anebo programové vybavení odstraněna nebo bezpečně přepsána.; relevance = 1; vyspělost = 0,25.

- 10.1.2; Změny by měly být řízeny; relevance = 1; vyspělost = 0,75.

Vývoj hodnot rizika na základě setříděných kombinací opatření je zobrazen viz následující graf:



Hodnoty rizika v akceptovatelném pásmu jsou pak zobrazeny viz následující graf:



Pro optimalizaci ve výběru opatření je nutné sledovat jednotlivé kombinace opatření pro stanovené hodnoty reálného cílového rizika. Zde jsou pro určité hodnoty rizik jednotlivé kombinace pro dodavatele i konzumenta služby IT (jednotlivé jedničky a nuly ve stejném pořadí, jak byla definována jednotlivá opatření pro zvládnutí konkrétního rizika):

- Riziko = 4.7857; kombinace pro poskytovatele: 011111; konzumenta: 1011111111
- Riziko = 4.4286; kombinace pro poskytovatele: 011111; konzumenta: 1101111111
- Riziko = 4.7857; kombinace pro poskytovatele: 101111; konzumenta: 1011111111
- Riziko = 4.4286; kombinace pro poskytovatele: 101111; konzumenta: 1101111111
- Riziko = 4.7857; kombinace pro poskytovatele: 110111; konzumenta: 1011111111

- Riziko = 4.4286; kombinace pro poskytovatele: 110111; konzumenta: 11011111111
- Riziko = 4.7857; kombinace pro poskytovatele: 111011; konzumenta: 10111111111
- Riziko = 4.4286; kombinace pro poskytovatele: 111011; konzumenta: 11011111111
- Riziko = 4.7857; kombinace pro poskytovatele: 111101; konzumenta: 10111111111
- Riziko = 4.4286; kombinace pro poskytovatele: 111101; konzumenta: 11011111111
- Riziko = 4.7857; kombinace pro poskytovatele: 111110; konzumenta: 10111111111
- Riziko = 4.4286; kombinace pro poskytovatele: 111110; konzumenta: 11011111111
- Riziko = 4.7857; kombinace pro poskytovatele: 111111; konzumenta: 00111111111
- Riziko = 4.4286; kombinace pro poskytovatele: 111111; konzumenta: 01011111111
- Riziko = 4.0714; kombinace pro poskytovatele: 111111; konzumenta: 10011111111
- Riziko = 4.7857; kombinace pro poskytovatele: 111111; konzumenta: 10111111110
- Riziko = 4.4286; kombinace pro poskytovatele: 111111; konzumenta: 11011111110
- Riziko = 4.4286; kombinace pro poskytovatele: 111111; konzumenta: 11111111011

Výběr konkrétní kombinace záleží na hodnotě rizika, konkrétní situaci v organizaci a například nákladech na implementaci.

6. Závěr

V této práci byla představena nová dimenze zabezpečení poskytovaných služeb IT (dle ISO/IEC 20000) za použití ISO/IEC 27000. Za tímto účelem byl vyvinut nový systém řízení rizik. Toto bylo demonstrováno na případové studii. Tento systém řízení rizik může být použit i uvnitř jedné organizace (například řízení rizik v informační bezpečnosti) a dále použit k modelování aktuální hodnoty rizik v průběhu implementace ochranných opatření.

Samozřejmě je možné kontaktovat autory práce za účelem poskytnutí dalších informací anebo implementovaných algoritmů.

Poděkování

Tento výzkum byl podpořen Výzkumným záměrem č. MSM 0021630528, Výzkum informačních technologií z hlediska bezpečnosti.

Tento výzkum byl také podpořen projektem MASTER, což je vědecko-výzkumný projekt spolufinancovaný ze 7. rámcového programu pro vědu a výzkum EU. Projekt je realizován v rámci strategického cíle 1.4 Secure, Dependable and Trusted Infrastructures, který schválila Evropská komise v rámci pracovního programu na roky 2007 - 2008.

Autoři práce děkují Ludřku Novákovi ze společnosti ANECT, a.s. za konzultace.

Bibliografie

- [1] ISO/IEC 20000-1:2005, Informační technologie – Management služeb – Specifikace
- [2] ISO/IEC 20000-2:2005, Informační technologie – Management služeb – Soubor postupů
- [3] BITS Technology Risk Transfer Gap Analysis Tool:
<http://www.bits.org/downloads/Publications%20Page/GapAnalysis.pdf>
- [4] Frankova, G.; Yautsiukhin, A.: Service and Protection Level Agreements for Business Processes. In The 2nd European Young Researchers Workshop on Service Oriented Computing, University of Leicester, 2007, <http://www.cs.le.ac.uk/events/yrsoc2007/>
- [5] <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>
- [6] ISO/IEC 27000