VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ŘÍZENÍ RIZIK V BEZPEČNOSTI IT SLUŽEB

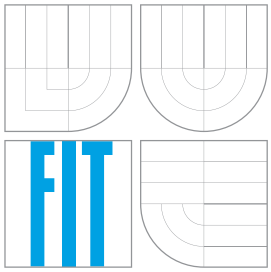
DISERTAČNÍ PRÁCE
PHD THESIS

AUTOR PRÁCE
AUTHOR

Ing. PETR SVOJANOVSKÝ

BRNO 2010

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ŘÍZENÍ RIZIK V BEZPEČNOSTI IT SLUŽEB

RISK MANAGEMENT IN IT SERVICE SECURITY

DISERTAČNÍ PRÁCE
PHD THESIS

AUTOR PRÁCE
AUTHOR

Ing. PETR SVOJANOVSKÝ

VEDOUCÍ PRÁCE
SUPERVISOR

doc. RNDr. JITKA KRESLÍKOVÁ, CSc.

BRNO 2010

Abstrakt

Disertační práce se zabývá efektivním řízením rizik informační bezpečnosti v poskytování služeb IT. Práce vychází z rozšířených praktik managementu služeb IT a informační bezpečnosti, tzv. *best practices*, zakotvených v mezinárodních standardech ISO/IEC 20000 a ISO/IEC 27000. Řešení vychází z řízení úrovně služeb, nad kterým staví řízení bezpečnosti tak, aby byly efektivně eliminovány bezpečnostní incidenty poskytované IT služby. Toho je dosaženo řízením rizik informační bezpečnosti, kde se obě strany kontraktu (případně více stran) podílejí na eliminaci zranitelností, a to na základě svých preferencí, potřeb byznysu a smluvně uzavřených dohod o bezpečnosti. Práce propojuje obě výše zmíněné oblasti řízení IT s cílem uspokojení všech stran kontaktu. Praktické výsledky a přínosy práce jsou ukázány na případových studiích, které simulují praktické prostředí a umožňují čtenáři, nejčastěji byznys vlastníkům IT služby, procesním inženýrům a rizikovým analytikům, přenést poznatky do praxe.

Abstract

In the thesis, we develop a novel approach for optimized risk management in IT service information security. A new method is based on widely used internation standards, best practices, for IT service management (in ISO/IEC 20000) and Information security management system (in ISO/IEC 27000). Firstly, IT service information serurity approach is developed based on Service level management extension. Secondly, a new risk management approach, where multidomain environment between parties is considered, is developed with a goal of all parties satisfaction. Optimalization in risk management is achieved by evaluation of risk treatment controls from relevancy and maturity aspects on both sides of contract. Finally, results are presented on real case studies to enable risk analysts, IT service business owners and process engineers to transfer new methods into real business.

Klíčová slova

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

Keywords

IT service management, Information security, Risk management, Optimized risk management, IT service provider, IT service consumer.

Citace

Petr Svojanovský: ŘÍZENÍ RIZIK V BEZPEČNOSTI IT SLUŽEB, disertační práce, Brno, FIT VUT v Brně, 2010

ŘÍZENÍ RIZIK V BEZPEČNOSTI IT SLUŽEB

Prohlášení

Prohlašuji, že jsem tuto disertační práci vypracoval samostatně pod vedením paní doc. RNDr. Jitky Kreslíkové, CSc., a uvedl všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Petr Svojanovský
8. srpna 2010

Poděkování

Především děkuji vedoucí práce práce doc. RNDr. Jitce Kreslíkové, CSc. za to, že byla vždy připravena trpělivě vyslechnout mé nápady a poskytla mi neocenitelné rady, motivaci v náročných a vypjatých okamžicích a osobní přístup.
Také velmi děkuji Ing. Luďku Novákovi, Ph.D. za mimořádně podnětné diskuze, rady a konzultace.

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

Tento výzkum byl také podpořen projektem MASTER, což je vědeckovýzkumný 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.
Metody vyvinuté v rámci této disertační práce jsou do projektu MASTER implementovány v rámci svěřené kompetence za oblast řízení rizik.

Obsah

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Nejen 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. Důvodem je to, že mezinárodní standardy vycházejí z takzvaných nejlepších praktik (anglicky best practices), což jsou postupy v řízení dané oblasti, na kterých se shodli přední světoví hráči spolu se standardizačními ústavy.

V České republice jsou kromě certifikací systémů řízení kvality a environmentálního managementu 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 standardizační 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 autor uvědomuje, 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 disertační práci je vyvinut unikátní systém řízení rizik (ne jejich identifikace a analýzy, pro kterou existuje nesčetně metod), který umožňuje optimalizovat výběr opatření na zvládání rizik na jednotlivých stranách kontraktu poskytované služby IT. K tomu zavádí dva parametry hodnocení opatření, a to relevanci opatření a existující vyspělost opatření. 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 jej 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, například v rámci řízení rizik v informační bezpečnosti.

Výzkum provedený v rámci této disertační práce je inovativní v následujících směrech:

1. Zavádí nový systém Dohod o úrovni bezpečnosti služeb, kdy oproti jednoduchým jed-

nostranným požadavkům na službu nebo byznys proces klade požadavky na všechny strany kontraktu (na všech stranách totiž může dojit k bezpečnostnímu incidentu).

2. Zavádí hodnocení opatření, kterými jsou redukována rizika. Z těchto hodnocení je následně odvozena schopnost opatření redukovat rizika.

3. Na základě ohodnocených opatření, které může být pro jedno opatření rozdílné na různých stranách kontraktu, potom stanovuje optimální varianty ve zvládání rizik (reálné implementace opatření) na základě potřeb a bezpečnostních požadavků na jednotlivých stranách kontraktu.

4. Vyvinuté metody nejsou závislé na metodách analýzy rizik, které jsou obvykle v různých organizacích odlišné. Jediným požadavkem je, aby byla hodnocena zranitelnost organizací (viz dále).

5. Poslední výhodou je možnost modelování snižování rizik. V současné době se totiž reziduální riziko pouze odhaduje.

Vyvinuté metody nejsou nijak omezené pro další rozvoj. Z pohledu hodnocení opatření jsou zavedena hlediska jejich relevance a vyspělosti, mohou být ale libovolně rozšířena o další aspekty, například náklady na implementaci opatření. Tyto další parametry pak mohou být zahrnuty do výpočtu "atraktivity" opatření. Je možné tedy poznatky z této práce rozšířit i další jiné potřeby konkrétního byznysu.

Na první pohled by se mohlo zdát, že se disertační práce zabývá dvěma neslučitelnými, nebo minimálně poněkud vzdálenými, oblastmi, a to je řízení rizik a informační bezpečnost. Opak je však pravdou – informační bezpečnost nikdy nelze úspěšně řídit bez kvalitního řízení rizik, jak je ostatně naprosto striktně požadováno v ISO/IEC 27001:2005.

Dále, v řízení rizik existují dva extrémní přístupy – první je založen pouze na matematice a numerických hodnoceních, ten druhý bez kvalitního matematického modelování rozhoduje o chodu organizací. Autor disertační práce ve své praxi poznal, že vhodný přístup leží někde mezi. Systém, kde jsou rizika řízena, je třeba matematicky zkoumat a modelovat, avšak vždy hraje tu nejdůležitější úlohu lidský mozek, který dělá manažerská rozhodnutí. Tomu odpovídají i metody vyvinuté v této práci – na jednu stranu zavádějí jednoduché a pragmatické matematické modelování, na stranu druhou se stále spoléhají na vstupy od analytika. Výsledky, které jsou potom analytikovi předloženy mu pouze umožňují, aby se mohl lépe rozhodovat nejen na základě pocitů a zkušeností, ale i na základě matematického modelu.

I když přístupy vyvinuté v této disertační práci mohou být samozřejmě použity kdekoli na světě, práce reflektuje okolní prostředí, to jest prostředí České republiky potažmo Evropy. Odráží se to v použití mezinárodních standardů typických právě pro toto prostředí, to jest standardů ISO/IEC.

Hlavním cílem práce je tedy vyvinout takovou metodiku řízení rizik a informační bezpečnosti služeb IT, která umožní definovat požadavky na bezpečnost služby IT a s tím související rizika, které bude následně možno zvládat na obou stranách uzavřeného kontraktu podle typu rizik a vnitřního prostřední partnerů kontraktu.

Pro splnění tohoto cíle je disertační práce rozdělena do těchto úkolů a etap:

- Vymezit metodická východiska pro řízení služeb IT, bezpečnosti a rizik, ze kterých bude vycházeno ve vývoji.

- Tato metodická východiska zanalyzovat tak, aby s nimi byly nově vyvinuté metody v plném souladu a respektovaly tak současný průmyslový standard využití best practices.
- Navrhnout nový způsob zabezpečení služby IT za účasti inovovaného systému řízení rizik.
- Tyto nové metody implementovat a použít na reálných příkladech z praxe.
- Zhodnotit dosažené výsledky.

Z etapizace práce pak vyplývá následující struktura textu disertační práce:

- Kapitola číslo 2 se krátce věnuje popisu vědeckovýzkumného projektu MASTER a tomu, jak souvisí s touto disertační prací. Důvodem je to, že poznatky z této disertační práce jsou do něj implementovány.
- Kapitoly 3, 4 a 5 představují oblasti standardizace, ze kterých vyvinuté metody vycházejí. Jedná se o mezinárodní standard ISO/IEC 20000 pro řízení služeb IT, rodinu standardů ISO/IEC 27000 pro řízení informační bezpečnosti, ty v sobě zahrnují i řízení rizik. Pro řízení rizik je použit i standard IEC/ISO 31010:2009 a další publikace a díla.
- Kapitola 6 tvoří první stěžejní část disertační práce, a to je zavedení bezpečnosti IT služeb.
- Logicky navazuje kapitola 7 řízením rizik.
- Kapitola 8 se krátce věnuje možnostem modelování. To ale jen okrajově, jedná se o intuitivní záležitost, je ale samozřejmě zmíněna, jelikož v praxi může být velmi užitečná.
- Kapitola 9 předkládá plnou verzi metodiky pro řízení rizik v bezpečnosti služeb IT.
- A konečně kapitola 10 je věnována případovým studiím.
- Poslední kapitola je samozřejmě věnována závěru a možnostem dalšího rozvoje.

1.1 Současný stav

Současný stav problematiky je dán především mezinárodními standardy pro dané oblasti, které představují best practices pro danou oblast. Z nich se také v této disertační práci vychází a jsou popsány v kapitolách 3, 4 a 5.

Kapitola 2

Mezinárodní vědeckovýzkumný projekt MASTER

Autor disertační práce se v rámci plnění svých profesních povinností podílí na výzkumu v rámci mezinárodního vědeckovýzkumného projektu MASTER [1]. Autor práce považuje za velký úspěch, že se mu daří inovativní metody prezentované v této disertační práci prosazovat i do tak náročného prostředí, jako je v projektu MASTER. V současné době autor práce spolupracuje s kolegy z British Telecom (oddělení Information Security Research BT Innovate and Design) na vývoji softwarového nástroje, který v sobě bude mít implementované inovativní metody prezentované v této disertační práci.

Projekt MASTER (dále jen projekt) je jako vědeckovýzkumný projekt součástí Sedmého rámcového plánu Evropské komise, navazuje na podobné projekty Šestého rámcového plánu. Cílem projektu je poskytnout organizacím metodiky a infrastrukturu umožňující monitorovat, vynucovat a auditovat kvantifikované indikátory bezpečnostních parametrů byznys procesů. Tím je docíleno poskytnutí řiditelných úrovní bezpečnosti a důvěry a soulady s regulatorními požadavky a mezinárodními standardy (jako například HIPAA [2], SOX [3], CobiT [39, 4, 20] a další standardy ISO/IEC [5, 6, 7]) v servisně orientované architektuře. To vše v kontextu jedné organizace (single-trust domain), komunikace mezi více organizacemi či partnery (multi-trust domain) anebo v případě outsourcingu. K dosažení výše uvedených cílů projekt definuje následující inovativní komponenty: key assurance indikátory, key security indikátory, ochranné a regulatorní modely – podpořené metodickými a kontrolními nástroji pro analýzu a ohodnocení business procesů. Základem je MASTER infrastruktura pro monitoring, vynucení, reakci a diagnostiku právě indikátorů uvnitř i mezi více organizacemi. Výstupy projektu jsou pilotně nasazovány v prostředí komunikace mezi nemocnicí a pojišťovnou, kde jsou kladeny vysoké požadavky na spolehlivost a bezpečnost komunikace, stejně tak na dodržování legislativních a normativních požadavků. Konkrétně se jedná o dvě organizace z finanční a zdravotnické oblasti, CESCE – pojišťovací instituce a HSR – zdravotnické zařízení.

2.1 Partneři projektu

Na celém projektu se podílejí organizace z průmyslového odvětví i z oblasti výzkumu. Do oblasti průmyslu patří: SAP Německo, Atos Origin Španělsko, Engineering Itálie, British Telecom Velká Británie, IBM Švýcarsko, ANECT Česká Republika. Za oblast výzkumu do projektu přispívají univerzity z Trenta, Stuttgartu, Dublinu, Osla a ETH Švýcarsko,

Fraunhofer Gesellschaft Německo. Už jen z výčtu partnerů je patrné, jak je projekt rozsáhlý a jak ambiciózní cíle si klade ve svém tříletém trvání.

Celý projekt je rozdělen do několika vědeckovýzkumných aktivit, jak je popsáno v následující kapitole.

2.2 Aktivity projektu a jejich cíle

Značný rozsah projektu vedl jeho tvůrce k jeho rozdělení na sedm jednotlivých aktivit, které jsou ještě dále členěny na tzv. pracovní balíčky (work packages). Všechny aktivity i jejich pracovní balíčky mají svého lídra z organizací specifikovaných výše, který koordinuje vývoj ve své oblasti a spolupracuje s dalšími lídry tak, aby na sebe aktivity vzájemně navazovaly. Stručný popis jednotlivých aktivit pro ilustraci následuje:

Aktivita 1 (scenario analysis and validation) – aktivita je zaměřena na komunikaci s koncovými uživateli (CESCE a HSR) pilotního nasazení projektu MASTER s cílem upřesnění cílového prostředí (komunikace mezi finanční institucí a zdravotním zařízením), zdůrazněme však, že cílem projektu je vybudování bezpečnostní infrastruktury implementovatelné v jakémkoli reálném prostředí. Pro integraci pilotního nasazení MASTERu je zvolen obvyklý iterativní přístup – definice požadavků, opakované testování, kontroly a zlepšení, následuje finální prototyp.

Aktivita 2 (conceptual model) – cílem aktivity A2 je vývoj architektury, modelů a formálního jazyka pro kvantifikaci a kvalifikaci celkového konceptu projektu, indikátorů a politik v rámci bezpečnostního managementu. Takové modely budou sloužit pro kontrolu úrovně souladu s regulatorními požadavky, standardy, bezpečnostními požadavky a politikami v servisně orientované architektuře. Formální jazyk umožní vyjádřit metriky a bezpečnostní indikátory v heterogenním prostředí při komunikaci mezi organizacemi a pro ověření, vzájemné porovnání a monitoring úrovně shody s požadavky na bezpečnost.

Aktivita 3 (design time support) – výstupem této aktivity budou softwarové nástroje a metodiky umožňující v cílové organizaci modelovat, analyzovat a verifikovat míry pro monitoring a vynucení daných dohod o úrovni bezpečnosti (protection level agreements - PLAs) v servisně orientované architektuře. Během návrhového procesu (implementace MASTERu v organizaci) budou pomocí těchto nástrojů zachyceny PLAs, KPIs (key performance indicators) a KSIs (key security indicators) a z nich vyplívající hrozby a rizika, které musí daná služba podporující business proces zohlednit v kontextu s cíli organizace. Na základě této analýzy jsou navrženy kontrolní procesy, běžící paralelně s business procesem zajišťující požadavky na jeho bezpečnost, chování a výkon.

Aktivita 4 (monitoring and signalling infrastructure) – aktivita A4 definuje infrastrukturu poskytující ustanovení indikátorů KAIs a KSIs za účasti online monitoringu událostí vztahujících se k úrovni shody a bezpečnosti aplikace, respektive služby. Cílem je zachytit veškeré akce a události ve vztahu právě ke shodě a aplikaci bezpečnostních politik. Zachycené události jsou předzpracovány a předány dále do vynucovací vrstvy (aktivita 5) a do úrovně ukládání dat (aktivita 6). Monitorovací komponenta využívá jako vstupů obecnou definici politik a požadavků (aktivity 1 a 2). Poněkud detailněji, aktivita 4 zkoumá a specifikuje monitorovací politiky stejně tak jako monitorovací komponenty, které jsou nezbytné k vynucení požadavků politik.

Aktivita 5 (enforcement infrastructure) – zde je cílem vybudovat mechanizmy které vynutí dodržení bezpečnostních politik (zahrnují i regulatorní požadavky apod.) přes všechny subjekty propojené infrastrukturou MASTERu. Prakticky je vynucení rozlišeno na vynucení kontrolou a vynucení reakcí. Základní rozdíl mezi vynucením kontrolou a reakcí je,

že v prvním případě je daným systémem poskytnuta prevence před porušením bezpečnostních politik, zatímco v druhém případě jsou akce soustředěny do kompenzací následků škod, pokud vynucení kontrolou nemůže být použito.

Aktivita 6 (assessment infrastructure) – aktivita 6 vyvíjí techniky a nástroje pro governance, respektive podporuje lidské zdroje v: (1) hodnocení bezpečnostního stavu procesů a služeb chráněných produkty MASTER a identifikaci potenciálních bezpečnostních problémů jako například procesy/procedury v neshodě s požadavky na bezpečnost nebo s požadavky zakotvenými v PLAs; (2) intervenci bezpečnostního governance procesu; (3) koordinaci intervencí zajišťujících bezpečnost a důvěru mezi organizacemi, kde cílem je garantovat jejich vhodnou úroveň.

Aktivita 7 (dissemination and exploitation) – aktivita probíhající intenzivně po celou dobu trvání projektu. Cílem je zajistit, že vývoj a výzkum probíhající v projektu je v každý okamžik orientován na současné i budoucí příležitosti na trhu a připravit efektivní začlenění výstupů projektu MASTER do cílových prostředí.

2.3 Inovativní komponenty podrobněji

Závěrem si ještě v bodech shrňme klíčové oblasti, ve kterých je projekt MASTER jedinečný a kde přináší skutečnou inovaci. Jde zejména o oblast definice jednotlivých typů indikátorů a o jejich implementaci softwarovými nástroji do funkční MASTER infrastruktury, jenž zajistí vzájemnou důvěru napříč organizacemi, které se rozhodly implementovat MASTER:

- Key assurance indicator (KAI) – měřitelný indikátor dohodnutý mezi klientem a poskytovatelem služby, jehož cílem je ukázat, že business cíle klienta jsou vhodně adresovány, tj. nedojde k nerušením, které by poškodily aktiva či oprávněné zájmy klienta.
- Key security indicator (KSI) – měřitelný technický bezpečnostní indikátor použitý poskytovatelem k zajištění vysoké úrovně bezpečnosti, tzn. zajištění přítomnosti a kvality bezpečnostních a regulatorních modelů.
- Protection and regulatory model (PRM) – stavební blok bezpečnostních politik, jehož vynucení, monitoring a auditování garantuje požadovanou úroveň KSI na vhodné úrovni abstrakce.
- Security model transformations (SMT) – je PRM transformace mezi rozdílnými úrovněmi byznysu poskytující mapování mezi rozdílnými úrovněmi bezpečnosti.

Volněji řečeno, KSI je interní metrika použitá poskytovatelem k ohodnocení vnitřních systémů, zatímco KAI je externí metrika mezi klientem a poskytovatelem služby. Při uzavření standardní SLA dohody o poskytování služeb by měla být uzavřena i dohoda o úrovní bezpečnosti, která se odkazuje právě na KAI anebo KSI. Poznamenejme, KAI a KSI jsou vzájemně provázány.

PRM je stavební blok na úrovní businessu, který je podřízený KSI a umožňuje verifikovat KSI celého business procesu kombinací jeho stavebních komponent. Příkladem PRM jsou dobře známé "best practices", které nařizují, jak vyhovět KSI. SMP pomáhá mapovat různé bezpečnostní modely, tj. transformovat KSI z jedné úrovně abstrakce na druhou a zpět.

MASTER inovativní koncepty výrazně rozšiřují možnosti CobiT [4, 20] a ITIL [8, 19] tím, že jsou "machine available" a tím jsou i okamžitě měřitelné a vykonavatelné v případě, že je očekáváno porušení KSI.

2.4 Shrnutí

Úkolem projektu je vytvoření metodiky a infrastruktury, které budou schopné monitorovat, vynucovat a auditovat kvantifikovatelné metriky bezpečnosti souběžně s business procesem. Tím zajistit na manažerské úrovni danou o úroveň bezpečnosti, důvěry a soulad s vnějšími (mandatorními) požadavky legislativy, standardů a regulátorů. To vše v dynamické servisně orientované architektuře v centralizovaném i distribuovaném multidoménovém prostředí a při využití poskytovatelů dalších služeb (outsourcingu).

2.5 Návaznost projektu na disertační práci

V rámci aktivity 3 (design time support) je vyvíjen softwarový produkt, jehož součástí je i implementovaný registr rizik a s ním spojená inovativní metodika pro řízení rizik. Vývoj metody a algoritmů pro řízení rizik je plně v kompetenci autora této disertační práce. Na vývoji softwarového nástroje se potom autor disertační práce podílí spolu s kolegy z British Telecomu.

Další návazností potom je souvislost mezi výše popsanými bezpečnostními indikátory a hodnocením opatření, zejména jeho vyspělosti (viz další části disertační práce). V budoucnu bude možné alespoň u částí opatření jejich reálnou vyspělost měřit a ne jen odhadovat. Toto ale není zatím implementováno, je to ale velmi zajímavé možné rozšíření du budoucna.

V rámci projektu MASTER jsou také vytvářeny odborné texty, které slouží k dokumentaci vývoje a k vytváření dokumentace pro budoucí uživatele. Přehled dokumentů, na kterých se autor disertační práce podílel je uveden v příloze D.2.

Kapitola 3

Řízení služeb IT

Tato kapitola se věnuje řízení služeb v IT [11, 12, 8, 18, 19]. ISO/IEC 20000 je první mezinárodní standard zaměřený na řízení služeb v IT. Je založen na britském standardu BS 15000, který také nahrazuje. ISO/IEC 20000 je procesně založený standard. To znamená, že není určen pro hodnocení produktů nebo poskytovaných služeb. Standard ISO/IEC 20000 může být použit k:

1. Implementaci procesů dle nejlepších praktik, tzv. *best practices*.
2. Vyslání pozitivního signálu zákazníkům – zákazník ví, že procesy podporující nakupovanou službu jsou na té nejvyšší úrovni.
3. Zabezpečení konzistentního přístupu všech dodavatelů v dodavatelském řetězci.
4. Měření současné úrovně procesní vyspělosti poskytovatele služeb IT.
5. Zlepšování efektivity a výkonu společnosti pomocí neustálého zlepšování.

Standard specifikuje úzce svázané procesy managementu služeb IT. Pro certifikaci dané služby dle ISO/IEC 20000-1:2005[1], a také plnou funkcionalitu implementovaného systému řízení, je nezbytně nutné implementovat do praxe všechny procesy, nestačí pouze některé. Funkcionalitu jednotlivých procesů lze shrnout následovně:

1. 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.
2. Plánování a implementace managementu služeb – aplikuje dnes již, dalo by se říci, revoluční PDCA princip 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 implementovány do praxe a neustále monitorovány a zlepšovány. Revoluční proto, že PDCA cyklus byl navržen již po druhé světové válce, kdy byla do Japonska

[1] Velmi často se nesprávně označují jednotlivé standardy nebo rodiny standardů. Dobrým zvykem je u označení rodiny standardů nepoužívat letopočet vydání (což je logické, neboť jednotlivé standardy mohou mít rok vydání odlišný) a teprve u konkrétních standardů za jeho číslo a dvojtečku(:) umístit letopočet.

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 řízení, jehož nedílnou součástí je kontinuální zlepšování. Autorem PDCA je W. Edwards Deming.

3. 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.

4. 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 zajistit informační bezpečnost.

5. Procesy vztahů – zde se vztahy rozdělují na ty 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.

6. Procesy řešení – dělí se 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 nevhodně nakonfigurovaný firewall.

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

8. 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.

Je vhodné znovu upozornit na nutnost provázanosti procesů a na to, že není možné určitý proces jednoduše vypustit. Například, dobrých vztahů se zákazníkem nikdy nebude dosaženo bez perfektního zvládnutí incident managementu, z procesů uvolnění se bez dokonalého managementu změn stane naprostý chaos.

ISO/IEC 20000 se skládá ze dvou částí:

1. ISO/IEC 20000-1:2005 Informační technologie – Management služeb – Specifikace.

2. ISO/IEC 20000-2:2005 Informační technologie – Management služeb – Soubor postupů.

Z výše uvedeného je jasně vidět, že pokud se poskytovatel jakékoli služby rozhodne pro certifikaci dle ISO/IEC 20000, zákazník bude uspokojen na maximální možné úrovni a poskytovatel tak získává významnou konkurenční výhodu na trhu.

Kapitola 4

Informační bezpečnost

V úvodu práce bylo zmíněno, že je brána v potaz regionální působnost autora. Tedy to, že v Evropě převládá využívání standardů ISO/IEC, zatímco například v USA jsou hojně používány standardy NIST. Pak existují další regionální specifika, jako například standardy AS/NZS pro Austrálii a Nový Zéland.

Tato kapitola představuje rodinu standardů ISO/IEC 27000 (někdy značené ISO/IEC 2700x), jejíž použití je typické pro region Evropy. 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 27004:2009 – měření v informační bezpečnosti.
- ISO/IEC 27005:2008 – řízení rizik 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 řada dalších, více informací např. [5, 6, 7]

Nyní se stručně podívejme na první tři jmenované standardy, protože právě ty budou hrát důležitou roli v další práci.

4.1 ISO/IEC 27001:2005

Prvním standardem rodiny ISO/IEC 27000 je ISO/IEC 27001:2005 převzatý i Českým normalizačním institutem jako ČSN ISO/IEC 27001:2006. Podle ISO/IEC 27001:2005 respektive ČSN ISO/IEC 27001:2006 se prování certifikace.

Pokud situaci kolem implementace informační bezpečnosti dle ISO/IEC 27001:2005 pro začátek maximálně zjednodušíme, tak lze konstatovat, že ISO/IEC 27001:2005 stojí na třech absolutně zásadních nosných principech [22, 21, 30]:

1. 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.

2. Směry, kam je upřeno úsilí především je dáno rizikovou analýzou.

3. 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.

ISO/IEC 27001:2005 také nevylučuje použití jiného katalogu opatření než je ISO/IEC 27002:2005, například pro elektronický obchod existuje standard PCI DSS [9].

Poznámka: jazyk ISO/IEC 27001:2005 je postaven na příkazové slovní formě, je tedy použito slovíčko "musí" – tím je reflektována definice požadavků, ze kterých není možné slevit při certifikace nebo pokud je cílem organizace skutečně dosáhnout vyspělého systému řízení informační bezpečnosti. Oproti tomu je v ISO/IEC 27001:2005 používáno výhradně obratu "měl by", čímž je řečeno, že není vždy nutné naplnit tyto požadavky – ovšem pouze pokud to situace a výsledky rizikové analýzy dovolují.

Nyní podrobněji k ISO/IEC 27001:2005. Nejprve začněme pojmy, které standard zavádí, je třeba je zde zmínit, jelikož jsou v této disertační práci hojně užívány a je potřeba, aby jejich interpretace byla jednotná. Pojmy, jenž ISO/IEC 27001:2005 zavádí, jsou následující[1], pokud jsou uvedeny poznámky autora práce, jsou v poznámce pod čarou:

- Aktivum[2] – cokoliv, co má pro organizaci nějakou hodnotu (ISO/IEC 13335-1:2004).

- Dostupnost – zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby (ISO/IEC 13335-1:2004).

- Důvěrnost – zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni (ISO/IEC 13335-1:2004).

- Bezpečnost informací – zachování důvěrnosti, integrity a dostupnosti informací a a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost (ISO/IEC 17799:2005).

- Bezpečnostní událost – identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací (ISO/IEC TR 18044:2004).

[1] Pojmy i jejich vysvětlení je převzato z ČSN ISO/IEC 27001:2006

[2] Z pohledu informační bezpečnosti je jako aktivum chápána především informace a její hodnota. Někteří autoři mylně stanovují hodnotu jako například pořizovací cenu serveru a neberou v úvahu hodnotu informací na serveru uložených, která může mnohonásobně převyšovat cenu hardware.

- Bezpečnostní incident – jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací (ISO/IEC TR 18044:2004).
- Systém managementu bezpečnosti informací ISMS (information security management system) – část celkového systému managementu organizace založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.
- Integrita – zajištění správnosti a úplnosti informací (ISO/IEC 13335-1:2004).
- Zbytkové riziko – riziko zbývající po uplatnění zvládání rizik (ISO/IEC Guide 73:2002).
- Akceptace rizik – rozhodnutí přijmout riziko (ISO/IEC Guide 73:2002).
- Analýza rizik – systematické používání informací k odhadu rizika a k identifikaci jeho zdrojů (ISO/IEC Guide 73:2002).
- Hodnocení rizik – celkový proces analýzy a vyhodnocení rizik (ISO/IEC Guide 73:2002).
- Vyhodnocení rizik – proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu (ISO/IEC Guide 73:2002).
- Management rizik – koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika (ISO/IEC Guide 73:2002).
- Zvládání rizik – proces výběru a přijímání opatření ke změně rizika (ISO/IEC Guide 73:2002).

V jednotlivých fázích PDCA cyklu standard ISO/IEC 27001:2005 nařizuje provádět tyto činnosti:

- P fáze – ustanovit ISMS (Information Security Management System).
- D fáze – zavést a provozovat ISMS.
- C fáze – monitorovat a přezkoumávat ISMS.
- A fáze – udržovat a zlepšovat ISMS.

4.1.1 P fáze – ustanovení ISMS

V úvodní části zavádění ISMS (ať už je cílem certifikace či nikoli, a to platí i pro ostatní fáze) je organizace povinna:

1. Definovat, zdokumentovat a vedením organizace schválit rozsah ISMS. To znamená určit, které části organizace podléhají řízení ISMS. Stejně jako s výběrem opatření z katalogu pro eliminaci rizik, není možné bezdůvodně z rozsahu vyloučit například informační systém, kde by mohla implementace ISMS činit potíže.
2. Definovat politiku ISMS – definovat základní přístup organizace k informační bezpečnosti.

3. Definovat metodiku pro řízení rizik, což je kompletní proces od identifikace aktiv a rizik až po jejich zvládání. Taková metodika řízení rizik je definována i touto disertační prací a je specifická o nově vyvinutý systém řízení rizik v bezpečnosti služeb IT.

4. Identifikovat rizika – a to včetně jejich složek, tedy dopadů (dle hodnot aktiv v rozsahu ISMS), hrozeb a zranitelností.

5. Analyzovat rizika – kvalitativní anebo kvantitativní ohodnocení identifikovaných rizik (všech složek) pro konečné ohodnocení rizik.

6. Rozhodnout o variantách zvládání rizik, což zahrnuje aplikaci opatření, akceptování rizik (pokud to dovoluje vedením přijatá metodika řízení rizik), vyhnutí se rizikům (je třeba dát pozor na to, že vyhnutí se riziku může samo o sobě generovat další rizika, která před vyhnutí se nebyla platná) a konečně přenesení rizik na třetí stranu (často pojišťovna, dodavatel a podobně).

7. Pro rizika, která byla vybrána pro implementaci opatření (v praxi to je většina rizik) identifikovat opatření z ISO/IEC 27002:2005 případně dalších standardů.

8. Vedení organizace musí odsouhlasit navrhovaná zbytková rizika a následné zavedení ISMS.

9. Připravit prohlášení o aplikovatelnosti – technický detail nepodstatný pro tuto disertační práci, pro ISMS však jeden z nejdůležitějších dokumentů.

4.1.2 D fáze – zavádění a provozování ISMS

Za částí implementace ISMS v P fázi následuje vlastní implementace ISMS. Po prostudování ISO/IEC 27002:2005 může čtenáře či potenciálního implementátora ISMS odradit značný rozsah ISO/IEC 27002:2005, který představuje 133 jak technických, tak i netechnických opatření. Pro praxi je však dobré řídit se výsledky rizikové analýzy a dbát jednoznačně určených priorit v implementaci opatření.

Během této fáze je nutné provést následující činnosti:

1. Definovat plán zvládání rizik a ten následně zavést.

2. Zavést bezpečnostní opatření (včetně měřících metod pro vyhodnocení účinnosti opatření), která byla vybrána na základě rizikové analýzy.

3. Definovat a zavést program pro budování bezpečnostního povědomí zaměstnanců včetně třetích stran, které přicházejí do styku s informacemi v rozsahu ISMS.

4. Řídit provoz a zdroje ISMS.

4.1.3 C fáze – monitorování a přezkoumání ISMS

Monitoringu ISMS se věnuje samostatný standard ISO/IEC 27004:2009 (Information technology – Security techniques – Information security management – Measurement). Jeho náplní je návod, jak zabudovat kontrolní mechanizmy do jednotlivých fází PDCA cyklu. Velmi přehledně popisuje proces získávání informací a derivaci bezpečnostních indikátorů v jednotlivých místech PDCA. Zároveň doporučuje zavést program měření výkonu informační bezpečnosti, což je významný posun oproti situaci před jeho vydáním. Před vydáním

tohoto standardu samozřejmě také existoval požadavek na měření, ale vzdáním standardu se situace významně zjednodušila a zpřehlednila.

Kromě vysvětlení toku informace při měření úrovně informační bezpečnosti také v informativní příloze A poskytuje šablony a příklady jednotlivých měření, na kterých lze dále stavět při budování vlastních měřících mechanizmů. Mezi uvedené příklady metrik (indikátorů) patří měření vzdělávání v ISMS, kontroly fyzického vstupu, bezpečnost v dohodách se třetí stranou a mnoho dalších.

4.1.4 A fáze – udržování a zlepšování ISMS

V závěrečné části PDCA cyklu musí organizace:

1. Zlepšení z předchozí fáze zavádět do praxe.
2. Provádět nápravné a preventivní činnosti – jinými slovy, provádět management incidentů a rizik a tyto dva procesy spolu provázat.
3. Veškeré zlepšující návrhy projednávat se všemi relevantními stranami (např. i třetí strany a podobně).
4. Napnout všechno úsilí k tomu, aby cíle definované ve zlepšeních byly skutečně dosaženy.

Kromě striktních požadavků na obsah jednotlivých fází PDCA cyklu standard ISO/IEC 27001:2005 klade požadavky na dokumentaci, odpovědnost a angažovanost vedení, provádění interních auditů ISMS, přezkoumávání a zlepšování ISMS vedením organizace.

4.2 ISO/IEC 27002:2005

Tato kapitola poskytuje stručný přehled o standardu ISO/IEC 27002:2005. Opravdu stručný, protože vzhledem k celkovému počtu 102 stránek standardu a rozsahu této disertační práce není ani jiná možnost. I tak by ale text měl poskytnout dostatečný přehled o tom, co je obsahem standardu. Úvodem předešleme, že informační bezpečnost se netýká pouze počítačů, jak by se mohlo zdát. Komplexní zajištění informační bezpečnosti spočívá i v kontrolách fyzického přístupu pracovníků, jejich prověřování a vzdělávání a v dalších oblastech. Klíčovou otázkou je, jak konkrétně má být jedno dané opatření implementováno v organizaci. Například, mají být dveře do počítačového sálu pancéřované nebo stačí běžné dveře pouze s kontrolou přístupu? Odpovědi na tyto otázky dává právě riziková analýza, která umožňuje poměrně obecná doporučení standardu ISO/IEC 27002:2005 promítnou do života organizace.

Struktura standardu ISO/IEC 27002:2005 má tři úrovně. První tvoří v podstatě nadpis dané oblasti, například Bezpečnost z hlediska lidských zdrojů. Druhou úroveň definují jednotlivé podoblasti, jako například Bezpečnost z hlediska lidských zdrojů – Před vznikem pracovního vztahu. Třetí úroveň je již tvořena jednotlivými kontrolami. Kontrola znamená způsob, jak může být sníženo konkrétní riziko, samozřejmě pouze pokud s daným rizikem souvisí. Na tomto místě budou představeny pouze první a druhá úroveň, kompletní seznam kontrol včetně třetí úrovně je v příloze B.

5 Bezpečnostní politika, 5.1 Politika bezpečnosti informací: Cílem je určit základní směr v bezpečnosti informací, toto by mělo být v souladu s požadavky organizace, samozřejmě existujícími zákony a již existujícími směrnicemi. Politika by měla být platná v

celé organizaci a stanovovat jasný směr postupu. Například získání certifikace, nebo zlepšení existujícího ISMS v určitých oblastech a podobně.

6 Organizace bezpečnosti informací, 6.1 Interní organizace: Měl by být definován rámec pro řízení implementace a následné zlepšování informační bezpečnosti v organizaci, jehož součástí je schválení bezpečnostní politiky a koordinace implementace. K tomu může napomoci i povolání odborníka do organizace, který zajistí implementaci podle nejnovějších trendů zejména ve styčných bodech informační bezpečnosti.

6.2 Externí subjekty: Cílem je pomocí jednotlivých kontrol zajistit bezpečnost informací (tj. zajištění důvěrnosti, integrity i dostupnosti) i pokud je nutný přístup externích subjektů k informačním aktivům organizace. Toto zahrnuje provedení rizikové analýzy zaměřené na přístup externích stran a jejich následné zvládání.

7 Řízení aktiv, 7.1 Odpovědnost za aktiva: U všech důležitých informačních aktiv by měl být stanoven jejich vlastník. Tím je propojena zodpovědnost za aktiva s individuální zodpovědností. Odpovědnost za aktiva může být delegována a také se to často děje, například ředitel oddělení lidských zdrojů může jen těžko zajistit jejich ochranu na technologické úrovni. Vlastník aktiv potom vystupuje jako osoba, která rozumí hodnotě aktiva a definuje ve spolupráci s odborníkem na informační bezpečnost požadavky na bezpečnost a potenciální dopady při porušení bezpečnosti.

7.2 Klasifikace informací: Aktiva by měla být klasifikována podle klasifikačního schématu přijatého organizací a korektně označena. Jen tak je možné vymáhat požadavky na dodržení požadavků informační bezpečnosti.

8 Bezpečnost z hlediska lidských zdrojů, 8.1 Před vznikem pracovního vztahu: Obsahuje veškeré požadavky na bezpečnost lidských zdrojů před vznikem pracovního poměru, to zahrnuje: zahrnutí třetích stran, prověření na dostatečné úrovní odpovídající klasifikaci informací, se kterými daný subjekt přijde do styku, a samozřejmě uzavření smluvních podmínek, kde nedílnou součást tvoří požadavky na informační bezpečnost.

8.2 Během pracovního vztahu: Obsahuje veškeré požadavky na bezpečnost lidských zdrojů při trvání pracovního poměru, to zahrnuje: odpovědnosti vedoucích zaměstnanců, zajištění programu pro budování bezpečnostního povědomí (klíčové ve vymahatelnosti) a zajištění existence formálního disciplinárního řízení[3].

8.3 Ukončení nebo změna pracovního vztahu: Obsahuje veškeré požadavky na bezpečnost lidských zdrojů při a po zániku pracovního poměru, to zahrnuje: definici činností při ukončení poměru, navrácení prostředků a přístupových práv.

9 Fyzická bezpečnost a bezpečnost prostředí, 9.1 Zabezpečené oblasti: Fyzická bezpečnost je v ISO/IEC 27002:2005 dělena jednoduše: na bezpečnost prostředí a bezpečnosti IT. Cílem zajištění fyzické bezpečnosti prostředí (zde v oblasti 9.1) je zajištění bezpečnostního perimetru (recepce, odpovídající zábrany (okna, dveře, mříže, elektronický zabezpečovací systém apod.)) a s tím souvisejících kontrol osob a nakonec ochrana před hrozbami z vnějšího prostředí (voda, vítr apod.). Speciální číst tvoří práce v zabezpečených oblastech.

9.2 Bezpečnost zařízení: Cílem je chránit IT zařízení a tak i informační aktiva organizace. Toho je docíleno vhodným umístěním zařízení, zajištěním podpůrných služeb jako klimatizace a podobně, údržbou pro zajištění požadované funkcionality, ale i bezpečnou likvidací a ochrany zařízení, pokud je mimo organizaci.

[3] Zde by se jeden mohl domnívat, že čím vyšší sankce pracovníkovi hrozí, tím vyšší zajištění bezpečnosti je zaručeno. Opak ale může být pravdou – pokud přijmeme skutečnost, že cílem není vymáhat sankce ale zajistit informační bezpečnost, potom může být vysoká sankce kontraproduktivní tím, že v případě provinění je toto úzkostlivě tajeno a nemusí takto být bezpečnost na prvním místě.

10 Řízení komunikací a řízení provozu, 10.1 Provozní postupy a odpovědnosti: Zde jde o stanovení postupů a procedur pro řízení a správu prostředků pro zpracování informací. Velmi důležitou částí je požadavek na oddělení odpovědností, čímž je sníženo riziko sabotáže. Příkladem může být oddělená databáze, kde pouze obě části dohromady tvoří funkční celek s tím, že k jednotlivým částem jaou přidělena oddělená oprávnění jak na úrovní technologií, tak i na úrovní lidských zdrojů.

10.2 Řízení dodávek služeb třetích stran: Cíl je jasný – udržet požadovanou bezpečnost i v případě přístupu třetí strany k aktivům organizace.

10.3 Plánování a přejímání informačních systémů: Zajistit současné a budoucí požadavky na kapacitu IT prostředků pomocí vhodného plánování, měření pro odhady budoucích požadavků a korektní dokumentace.

10.4 Ochrana proti škodlivým programům a mobilním kódům: Ochránit aktiva organizace před škodlivými kódy, ale i nepovoleným programovým vybavení.

10.5 Zálohování: Plánování a provádění záloh, které musejí být s ohledem na kritičnost a použité médium i pravidelně testovány.

10.6 Správa bezpečnosti sítě: Zajistit ochrany všech zařízeních připojených do počítačové sítě. Toto musí být zajištěno i v případě, že síť přesahuje hranice organizace – ochrany zde je zajištěno jak technologicky, tak i pomocí uzavření smluvních a sankčních požadavků.

10.7 Bezpečnost při zacházení s médii: Obsahuje doporučení na správu a manipulaci počítačových médií (toto opatření má silnou vazbu na klasifikaci a označování aktiv v kapitole 7 normy), bezpečná likvidace médií a definování postupů pro manipulaci s informacemi.

10.8 Výměna informací: Cílem je definice a dodržení dohod při výměně informací, a to jak elektronickou cestou, tak pomocí přepravovaných médií anebo informací v papírové formě. Tyto postupy by měly být formulovány ve formální politice.

10.9 Služby elektronického obchodu: Zajistit bezpečné služby elektronického obchodu, včetně transakcí a ochrany uložených informací. K tomuto tématu je doporučeno využít i jiné standardy, například PCI DSS.

10.10 Monitorování: Zajištění monitoring IT zařízení i obslužného personálu včetně uživatelů. Monitoring by měl být v souladu s politikami organizace a jejím přístupem k zajištění informační bezpečnosti.

11 Řízení přístupu, 11.1 Požadavky na řízení přístupu: Měla by být stanovena formální politika, na jejímž základě bude řízen přístup k veškerým informacím, což zahrnuje prostředky, pomocí nichž je přistupováno.

11.2 Řízení přístupu uživatelů: Cílem je zajistit přístup oprávněným uživatelům a zabránit přístupu neoprávněným uživatelům (ochrana důvěrnosti a dostupnosti informačních aktiv). Měl by existovat a být schválen formální postup pro přidělování i odebírání práv (vazba na kapitolu 8 standardu). Speciální pozornost by měla být věnována přidělování privilegovaného přístupu k informacím.

11.3 Odpovědnosti uživatelů: Cílem je předcházet neoprávněnému uživatelskému přístupu a porušení požadavků na důvěrnost informačních aktiv. Opět zde existuje vazba na kapitolu 8 ISO/IEC 27002:2005.

11.4 Řízení přístupu k síti: Mělo by být předcházeno neautorizovanému přístupu k síťovým službám za použití vhodného řízení, definice a implementace rozhraní sítí a odpovídajících autentizačních mechanizmů. Další kroky, ke kterým může být přistoupeno je identifikace zařízení v sítích a použití principů oddělení sítí a řízení síťových spojení.

11.5 Řízení přístupu k operačnímu systému: Prostředky omezující přístup k operačnímu systému by měly být schopné autentizace, záznamu událostí, spouštění varování

při porušení definovaných a implementovaných politik a v případě nutnosti omezení doby připojení uživatele.

11.6 Řízení přístupu k aplikacím a informacím: Mělo by být předcházeno neoprávněnému přístupu k informačním aktivům, které jsou uloženy v počítačových systémech.

11.7 Mobilní výpočetní zařízení a práce na dálku: Pro práci na dálku by měla být přijata adekvátní opatření na ochranu informací – mělo by být zváženo riziko práce v nechráněném prostředí a komunikace skrz nechráněné prostředí.

12 Akvizice, vývoj a údržba informačních systémů, 12.1 Bezpečnostní požadavky informačních systémů: Cílem je zajistit, aby se bezpečnost stala i součástí informačních systémů, což zahrnuje infrastrukturu, interní i externí produkty.

12.2 Správné zpracování v aplikacích: Obsahuje validaci vstupních dat a kontrolu vnitřního zpracování v aplikacích, to se týká i vyměňování dat mezi aplikacemi a počítačovým vybavením. Takto je dosaženo ochrany integrity informačních aktiv.

12.3 Kryptografická opatření: Kryptografické prostředky by měly být používány v souladu s politikou organizace a klíče patřičně chráněny.

12.4 Bezpečnost systémových souborů: Přístup k systémovým souborům a zdrojovým kódům by měl být řízen odpovídajícím způsobem reflektující konkrétní situaci v organizaci. Mělo by být přihlédnuto k rizikům plynoucím z použití testovacího prostředí.

12.5 Bezpečnost procesů vývoje a podpory: Za tímto, možná poněkud zavádějícím, termínem se skrývá doporučení na řízení změn, přezkoumání aplikací a operačních systémů po změnách (to znamená i po pravidelných aktualizacích) a doporučení na dohlížení nad vývojem programového vybavení externí stranou, pokud je to možné.

12.6 Řízení technických zranitelností: Měla by být zajištěna včasná detekce technických zranitelností a vyhodnocena kritičnost pro organizaci. Poté by v souladu s řízením změn měla být sjednána náprava.

13 Zvládání bezpečnostních incidentů, 13.1 Hlášení bezpečnostních událostí a slabin, 13.2 Zvládání bezpečnostních incidentů a kroky k nápravě: Cílem je včas (to znamená i preventivně) detekovat bezpečnostní události a incidenty a integrovat do podniku schopnost ponaučit se z nich. Jinými slovy, integrovat procesy řízení incidentů a problémů (v jazyce ISO/IEC 20000) a tyto provázat s procesem řízení rizik. Součástí je také implementace plánu pro obnovu po incidentu, což má návaznost na řízení kontinuity činností v následující části standardu.

14 Řízení kontinuity činností organizace, 14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací: Na základě rizikové analýzy by měly být definovány, implementovány a v pravidelných intervalech přezkušovány plány kontinuity činností organizace. Obecně lze říci, že předmětem plánování kontinuity se stávají oblasti definované riziky s potenciálním velmi vysokým dopadem a nízkou pravděpodobností výskytu.

15 Soulad s požadavky, 15.1 Soulad s právními normami: Samozřejmou součástí standardu je požadavek na dodržení zákonných norem včetně jejich povinné identifikace, ochrana duševního vlastnictví (převážně nelegální činnosti běžných uživatelů) a ochrana osobních údajů.

15.2 Soulad s bezpečnostními politikami, normami a technická shoda: Zde je cílem zajistit shodu používaných systémů s politikami organizace a požadovanými normami. Toto by mělo být pravidelně přezkoumáváno a v případě detekce kolize by měla být náprava sjednána okamžitě, ale řízeným způsobem.

15.3 Hlediska auditu informačních systémů: Cíl je maximálně zefektivnit činnosti auditů a minimalizovat zásahy do chodu organizace. Auditorské nástroje technologického

rázu by měly být chráněny.

4.3 ISO/IEC 27005:2008

Ačkoli se řízení rizik věnuje samostatná kapitola této disertační práce, řízení rizik v rámci rodiny standardů ISO/IEC 27000 je diskutováno zde pro zajištění konzistence výkladu. Pro praxi je důležité následující vysvětlení k požadavku ISO/IEC 27001:2005 na řízení rizik: standard neříká, jak přesně musejí být rizika řízena, například jaké stupnice musejí mít škály pro hodnocení. Standard ISO/IEC 27001:2005 striktně nařizuje, že rizika musejí být řízena a standard ISO/IEC 27005:2008 pak dává návod na to, jak je možné rizika řídit.

ISO/IEC 27005:2008 poskytuje základní rámec pro řízení rizik organizace a je nutné ho zasadit do konkrétního kontextu organizace. V úvodu definuje termíny pro oblast řízení rizik, z nichž některé si zde uvedeme s cílem zavedení jednotného názvosloví po zbytek práce. Na poli rizik totiž panuje obrovská nejednotnost v tom, jak jsou pojmy definovány a následně interpretovány.

ISO/IEC 27005:2008 definuje, mimo jiné, následující pojmy:

- Dopad – nepříznivá změna do dosahování byznys cílů.
- Riziko informační bezpečnosti – potenciální možnost, že hrozba využije zranitelnost a tímto způsobem poškodí organizaci změnou aktiv nebo skupin aktiv.
- Vyhnutí se riziku – vyhnutí se rizikové situaci (ISO/IEC Guide 73:2002).
- Komunikace rizik – výměna informací, které se týkají rizik mezi zainteresovanými stranami (ISO/IEC Guide 73:2002).
- Odhad rizika – proces přiřazení hodnot k pravděpodobnostem a následkům rizik (ISO/IEC Guide 73:2002).
- Identifikace rizik – proces nalezení rizik a jejich částí (ISO/IEC Guide 73:2002).
- Redukce rizika – aktivity vedoucí ke snížení pravděpodobnosti anebo dopadu rizika (ISO/IEC Guide 73:2002).
- Zadržení rizik – akceptace (ISO/IEC Guide 73:2002).
- Přenesení rizika – přenesení rizika na třetí stranu (ISO/IEC Guide 73:2002).

Patrně nejdůležitější informace, kterou ISO/IEC 27005:2008 přináší, je ta, že celý proces řízení rizik staví opět na PDCA principu. Podle zkušeností autora disertační práce je právě toto v praxi zcela neopodstatněně opomíjeno – analytici se domnívají (nebo je to možná z pohodlnosti), že stačí rizika nalézt, poté je ohodnotit čísly a tím práce končí. Opak je pravdou – tím práce v řízení rizik teprve začíná, respektive začíná první PDCA cyklus. Potřeba PDCA je umocněna zejména tím, že v rizicích se pracuje vždy s, do jisté míry, nepřesnými informacemi a právě neustálý monitoring a zlepšování odhadů vede v praxi k úspěchům.

Ve stručnosti, ISO/IEC 27005:2008 obsahuje následující:

- Kapitola věnující se hodnocení rizik začíná popisem procesu identifikace rizik, to znamená identifikace aktiv, hrozeb, identifikace existujících bezpečnostních opatření a s tím souvisejících zranitelností. Následně stručně popisuje metody pro hodnocení rizik (tzv. kvalitativní a kvantitativní) a výsledné ohodnocení rizika. Zajímavostí je, a bylo to zde již předestřeno, že neobsahuje žádné škály pro hodnocení ani vzorce. Z tohoto pohledu je poměrně velmi obecná a organizace si sama musí vyvinout vlastní nebo převzít metodiku pro řízení rizik.

- Další kapitola se samostatně a poněkud podrobněji v kontextu s předchozí kapitolou věnuje zvládání rizik (anglický termín treatment). Přehledně rozebírá všechny možnosti, které je možné zvolit mezi nalezením a akceptací rizika. Jedná se o redukci rizika (implementace opatření z katalogu ISO/IEC 27002:2005), zadržení rizika, vyhnutí se a přenesení rizika. Výsledkem každého řešení je reziduální riziko, což může na první pohled působit nelogicky. Má to ale svoji logiku – například i přenesení rizika na třetí stranu samo o sobě riziko neruší naprosto ani pro organizaci, která ho přenáší, jen je v tomto stavu akceptovatelné.

- Samostatná kapitole je věnována akceptaci rizika.

- Další kapitoly se věnují komunikaci rizik, jejich monitoringu a zlepšování celého procesu. Je to dáno kontextem s dalšími standardy (převážně ISO/IEC 27001:2005 a ISO/IEC 27002:2005) a samozřejmě PDCA.

Kapitola 5

Řízení rizik

Tato kapitola se věnuje řízení rizik [16, 10, 38, 23, 25, 24, 32, 52], to znamená přehledu jednotlivých postupů a metod. Na první pohled by se mohlo zdát, že se jedná o jednoduchý úkol, ale není tomu tak. Důvodem je to, že na poli rizik existuje naprostá nejednotnost například už jen v termínech. Dalším zdrojem nejednotnosti je samozřejmě také to, že rizika jsou řízena ve velmi odlišných činnostech a to si samozřejmě žádá rozdílné přístupy k řízení rizik. Budou zde tedy popsány pouze některé přístupy a pohledy s tím, že cíl v řízení rizik je vždy stejný – předem se připravit na potenciální problémy a těm se vyhnout. Pokud již nastanou, tak minimalizovat jejich následky. Nelze také zapomenout na fakt, že cílem řízení rizik bývá i snaha vytěžit maximum například z rizik v prostředí konkurence.

Kapitola tedy popisuje pohled autora disertační práce a v žádném případě si neklade být arbitrem a říkat, co je v rizicích správně a co ne – co je v kontextu jedné organizace nepřijatelné, to může být v jiném prostředí akceptovatelné nebo dokonce žádoucí.

Z pohledu autora práce (a je to v souladu s ISO/IEC 27005:2008) se celý proces řízení rizik skládá z těchto částí:

1. Identifikace rizik – v této oblasti existuje mnoho metod s jediným cílem: nalézt rizika a jejich složky. Metody jsou převážně typu různých pohovorů, sběru historických dat a zkoumání auditních nálezů a podobně.

2. Analýza rizik – jejich numerické vyjádření a z toho plynoucí plánování, co s výslednými riziky učinit. I na tomto poli existuje nesčetné množství metod a algoritmů. To je důvodem, proč tato disertační práce nepřispívá do oblasti analýzy. Autor práce je toho názoru, že je plně postačující vybrat a použít takovou existující metodu pro analýzu, která již prostě uspokojuje požadavky konkrétní oblasti – tedy analýzy rizik v informační bezpečnosti.

3. Zvládání rizik – toto je pole působnosti autora disertační práce. V praxi je totiž zatím postupováno tak, že jsou jednoduše vybrána opatření a k nim je odhadnuta hodnota zbytkového rizika (samozřejmě v případě, že se organizace rozhodne pro tento způsob zvládání rizika). Tato práce tento trend mění a umožňuje tento proces analyzovat, modelovat a přijímat manažerská rozhodnutí.

Tyto tři body jsou striktně zasazeny do PDCA cyklu. Je až neuvěřitelné, jak je tento fakt v praxi opomíjen a tak vetšinou celé řízení rizik končí například tabulkou s čísly, které nakonec skončí tak, jak jsou vypracovány a nejsou dále použity. Přitom tato data musí

být základním pracovním nástrojem rizikového analytika a musí být udržovány ve stálé platnosti.

Poznámka, ona zmíněná nejednotnost na poli řízení rizik je eliminována tak, že všude, kde to je možné, se vychází z mezinárodních standardů. V tomto případě se jedná o standard IEC/ISO 31010:2009 [10], který poskytuje přehled jednotlivých metod pro identifikaci, analýzu i evaluaci. Modelování zvládání rizik samozřejmě chybí a to mění tato disertační práce.

5.1 Identifikace rizik

Ve většině případů je alespoň z části v identifikaci rizik postupováno tak, že se analytik účastní a pořádá pohovory s byznys vlastníky aktiv, pracovníky IT oddělení a zástupci vedení společnosti. Je velmi důležité, pokud má být výsledek přínosem, tuto část dobře zvládnout psychologicky a navázat s klientem důvěrný vztah. Je důležité vždy zdůrazňovat, že cílem není odhalit to, kde například uživatel porušuje daná pravidla a sankcionovat jej, ale pochopit jeho potřeby. A pokud se porušování pravidel dopouští s nějakým cílem, je dobré jeho cíl zachovat, ale navrhnout jiné řešení, které není rizikem. Toto se během praxe autora práce mnohokrát potvrdilo, výsledky pohovorů byly velmi přínosné z pohledu řízení rizik, ale také zejména z pohledu klienta!

V identifikaci rizik nelze začít jinak než Brainstormingem: s trochou nadsázky se dá říci, že jej používá každý, kdo má v organizaci řešit nějaký problém. Jde o skupinovou poradu přibližně dvanácti lidí, optimální trvání 15 až 45 minut. Další pravidla jsou: jasně formulovat problém, určit jasnou metodu pro zachycení myšlenek, přijmout prvotní stanovisko "každý nápad je dobrý", posudek odložit a nápady nechat "dozrát" a opět se k nim vrátit. Ze zkušeností autora této disertační práce má, i přes svoje téměř masové použití, brainstorming své nevýhody [50, 38]:

1. Ne každý je z řízení rizik nadšený a i takový člověk se může dostat na brainstorming. V tomto případě je schován v davu a nepřináší své znalosti.

2. Ve skupinách existuje tzv. tlak konformity – přizpůsobení se dominantnímu názoru.

3. Skupina má tendenci činit riskantnější rozhodnutí (sdílená odpovědnost za špatné nebo žádné rozhodnutí).

Tyto nedostatky jsou eliminovány tak, že jsou účastníci od sebe odděleni, a je pak úkolem pro analytika, aby jednotlivcům zprostředkoval názory skupiny. Jedná se o metodu Delfi a pohovory.

Delfi metoda byla vyvinuta společností RAND Corporation pro technické předpovědi. Respondenti jsou zde od sebe odděleni a jsou vyzváni k tomu, aby sdělili své názory na rizika. Analytik poté z odpovědí vytvoří skupinový názor a pokud se jednotlivé odpovědi liší od názoru skupiny, jsou požádání o revizi. Tento postup je opakován tak dlouho, dokud není dosaženo skupinového konsensu. Tato metoda se od pohovorů liší pouze tím, že probíhá například pomocí elektronické komunikace a je tak velmi dobře použitá například v nadnárodních korporacích.

Z dalších metod bude ještě zmíněna například HAZOP [10] a FMECA [10].

HAZOP (Studie ohrožení a provozuschopnosti): jedná se o induktivní postup původně vyvinutý pro identifikaci rizik v chemických závodech společností Imperial Chemicals Ltd. Jde o strukturalizovaný brainstorming, kde skupina systematicky zkoumá prvky procesu

a definuje záměr procesu. Slova “ne”, “více” a “méně” se pak používají pro identifikaci možných odchylek od záměru.

FMECA (Kritická analýza možných vad a jejich příčin): induktivní postup, za jehož výsledek ručí a také jej tvoří jeden analytik velmi dobře rozumějící danému problému. Zvažuje se každá komponenta systému a je identifikován každý způsob potenciálního selhání. Postup se často používá pro audit hardware a zařízení společnosti.

Výstupy z identifikace rizik jsou zároveň vstupem do jejich analýzy.

5.2 Analýza rizik

Cílem analýzy rizik je jednotlivým složkám rizika (nejčastěji dopadu a pravděpodobnosti) přiřadit určité hodnoty (numerické nebo nenumerické) a na jejich základě potom stanovit, zdali je výsledné riziko akceptovatelné, či se musí redukovat (případně jiná forma zvládání).

Velmi často se rozdělují na kvalitativní a kvantitativní a činí tak i standard ISO/IEC 27005:2008.

Kvalitativní analýza používá škálu kvalitativních atributů pro popis velikosti potenciálního dopadu a pravděpodobností. Výhodou je jednoduché porozumění a komunikace rizik, zatímco nevýhoda spočívá ve značné subjektivitě. Tento druh analýzy je většinou použit jako základní analytická metoda a tam, kde postačuje k učinění příslušných manažerských rozhodnutí.

Kvantitativní analýza používá numerické hodnoty pro dopady i pravděpodobnosti. Pomocí tohoto způsobu lze velmi podrobně vyjádřit situaci s rizicích, což je zároveň i její slabina a to vzhledem k tomu, že se jedná vždy jen o odhady.

Poměrně zajímavou otázkou je, kde je hranice mezi kvalitativní a kvantitativní analýzou. I kvalitativní atributy mohou být vyjádřeny numericky, například hodnotami 1 až 5 nebo 1 až 10, jakkoli. Když si potom uvědomíme, že v případě kvantitativní stejně nemá smysl použít absolutně celý rozsah numerické škály (například při vyjádření pravděpodobnosti v procentech absolutně nemá smysl rozlišovat například mezi pravděpodobností 30% a 32%, jelikož se jedná o odhad). Potom si lze představit, že rozdíl mezi kvalitativní analýzou a kvantitativní analýzou nemusí být až tak podstatný. Rozumným kompromisem by mohl být ten přístup, kdy v začátcích řízení rizik v dané oblasti je použit spíše kvalitativní přístup, neboť dostatečné množství informací nebývá k dispozici. Postupem času jsou tyto kvalitativní údaje zpřesňovány tak, že nabývají kvantitativního charakteru.

Způsobů, jak se z ohodnocených dopadů a pravděpodobnosti stanovuje výsledná hodnota rizika, existuje obrovské množství. Zkušenost autora disertační práce je taková, že ještě ve své praxi nepotkal dvě organizace, které by přistupovaly k rizikům identicky. Uveďme se pro představu alespoň některé metody s tím, že se mohou celé nebo jejich části překrývat s identifikací rizik.

SWIFT (Strukturovaná “What-if” technika) [10]: původně vyvinutá jako jednodušší varianta HAZOPu. Předmětem strukturovaných pohovorů jsou známá rizika, předchozí zkušenosti z incidentů, identifikace existujících kontrol a regulatorních požadavků a omezení. Diskuze je vedená právě otázkami typu “co když”. Výsledkem je registr rizik [49] s uspořádanými úkoly vzhledem k rizikům. Tento registr je pak základem pro plán zvládání rizik.

RCA (Root Cause Analysis) [10]: hlavním přínosem této metody je pokus odhalit tu nejzákladnější část příčiny poškození aktiva respektive organizace. Vstupem RCA jsou veškeré záznamy z předchozích selhání anebo ztrát. Tyto vstupy zpracovávají experti na danou

oblast. Výstupem jsou předpokládané hypotézy, závěry nad nimi a z nich plynoucí základní příčiny, doporučení pro zvládání rizik.

Matice následků a pravděpodobností (anglicky consequence/probability matrix): je způsob, jak kombinovat kvalitativní nebo polo-kvalitativní hodnocení dopadů a pravděpodobností do výsledné hodnoty rizika. Konkrétní algoritmus a formát matice je vždy závislý na daném kontextu organizace. V principu jde ale o matici, kde například sloupce tvoří hodnocení dopadu a řádky představují stupnici pravděpodobností. Jednotlivé prvky matice pak určují závažnost rizika a z toho plynoucí požadavky na jeho zvládání.

ETA (Event tree analysis) [10]: grafická technika pro reprezentaci vzájemně exkluzivních sekvencí událostí, které následují pro úvodní iniciační události. Jednotlivé na sebe navazující události jsou ohodnoceny pravděpodobnostmi, z nichž nakonec plyne pravděpodobnost daného řetězce událostí s odpovídajícím dopadem. Variantou ETA je analýza příčin a následků, kde jsou pravděpodobnosti degradovány na hodnoty 0 a 1. Vstupy pro tyto dvě analýzy může tvořit například výstup HAZOPu.

RIPRAN (RIsk PRoject ANalysis) [36, 35]: je metoda navržená pro analýzu projektových rizik, v určitých případech ji lze velmi úspěšně použít i pro analýzy jiných, než projektových rizik. Metoda RIPRAN se sestává z těchto fází: příprava analýzy rizika, identifikace rizika, kvantifikace rizika, odezva na riziko a celkové hodnocení rizika.

Další z možných přístupů je dívat se na informace o rizicích jako na tzv. fuzzy informace a tak k nim také přistupovat při zpracování a analýze. Více o této problematice ve spojení s řízením rizik lze nalézt například v [46].

Jako další lze zmínit Markovovu analýzu [10], simulaci Monte Carlo [10] pro velmi složité systémy a mnoho dalších, které jsou bohatě popsány v dostupné literatuře a na internetu.

5.3 Zvládání rizik

Z předchozích dvou sekcí je zřejmé, že ať je použita jakákoli metoda, vždy jde o identifikaci toho, co se může stát a o definici nápravných kroků, které mají organizaci ochránit před dopadem. Tohoto je dosaženo pomocí nejrůznějších kvalitativních anebo kvantitativních metod. Tímto však veškeré analýzy končí a již nelze modelovat to, jak jsou rizika skutečně snižována. Také nelze na základě výpočtů vybírat nápravná opatření.

Tato disertační práce tento trend mění v následujících částech s tím, že v následující kapitole je definován přístup k řízení rizik tak, aby byl celý proces co nejvíce efektivní.

5.4 Lze rizika řídit efektivně?

Tato sekce práce se zabývá úvahami nad tím, jak přistoupit k řízení rizik efektivně a pragmaticky. **Je důležité si uvědomit, že řízení rizik pracuje s odhady možných dopadů, které mohou být více či méně přesné. A právě vyšší míra nepřesnosti informací o rizicích a vyšší úroveň dynamiky zvyšuje význam řízení rizik na úkor tzv. analýzy rizik, jejichž statická povaha je v rozporu s dynamikou dnešního světa využívání IT.** Poznámka: text této kapitoly vychází zejména z [40].

V praxi jsou dnes aplikovány převážně klasické metody řízení rizik (z velké části diskutované v předchozí části), které zdůrazňují analytický charakter řízení. To vede ke stavu, kdy jsou prováděny relativně složité analytické operace, jejichž výsledkem je více či méně přesné vyjádření existujících bezpečnostních rizik. Následně dochází k návrhu vhodných bezpečnostních opatření, která mají existující rizika snížit či úplně eliminovat. Společným

znakem těchto řešení je časté využití komplexních analytických nástrojů a poměrně dlouhý časový odstup mezi prováděním jednotlivých analýz (většinou v řádu několika roků). Při použití klasických metod řízení rizik se setkáme s několika podstatnými nedostatky. V první řadě je to relativně dlouhá doba mezi jednotlivými analýzami, která je v přímém rozporu s potřebami zajistit flexibilní fungování informačních a komunikačních technologií, to v sobě samozřejmě zahrnuje i zajištění bezpečnosti poskytování služeb IT. Běžně se tak stává, že při dokončení cyklu analýzy jsou data z počátku cyklu již neplatná. Vedle toho začínají být pro klasické metody problémem složité vnitřní vazby, které se promítají do výpočtu rizik a do výběru bezpečnostních opatření. Jinými slovy, není vůbec snadné v analýze cokoli jednoduše upravit či doplnit. To podstatným způsobem omezuje schopnosti těchto metod při řízení rizik, která jsou zjištěna během provozování systému. Oba hlavní nedostatky jsou dány především tím, že klasické metody nejsou navrženy s cílem každodenního řízení bezpečnostních rizik. Pozornost metod se primárně věnuje detailní analýze rizik. Zvládání rizik je pojímáno jako jednorázový akt, kterým jsou upřesňovány cíle a obsah nový bezpečnostní projektů. Zároveň existují pouze omezené možnosti integrovat do klasických metod řízení rizik externí zdroje informací (např. zprávy z auditu, interní podněty, výsledky monitorování bezpečnosti, výsledky bezpečnostních testů apod.).

5.4.1 Moderní přístupy k řízení rizik

Se stále vyššími potřebami uplatňování systematických a efektivních přístupů k managementu bezpečnosti informací jsou rozvíjeny i metody pro analýzu a zvládání rizik. Na rozdíl od dříve užívaných jednorázových analýz s dlouhodobě platnými výsledky je důležitou snahou soudobých metod aplikovat analýzy při každodenním managementu bezpečnosti informací. **Pozornost se tudíž přesouvá více ve prospěch řízení a zvládání rizik.**

Základní prvkem moderních metod je vybudování tzv. registru rizik, do kterého jsou ukládány informace o všech bezpečnostních rizicích. Hlavním záměrem je vybudování a udržování aktuálního přehledu o známých bezpečnostních rizicích. Cílem je všechna zjištěná rizika evidovat, ohodnotit jejich významnost, určit osobu, která je odpovědná za zvládání rizika a sledovat postup zvládání rizika v čase. Tyto moderní metody řízení rizik především dovolují neustále kontrolovat aktuální situaci okolo bezpečnostních rizik a rychle zapracovávat nově zjištěná rizika. Při zvládání rizik má bezpečnostní manažer aktuální přehled o odpovědných osobách, o stavu řešení a v případě potřeby je schopen zpracovávaná rizika náležitým správným způsobem interně komunikovat. Všechny tyto informace mohou být využity pro správné rozhodování v rámci managementu bezpečnosti, což vede ke snadnějšímu prosazování a vyšší efektivitě managementu bezpečnosti informací.

Aplikace moderních metod řízení rizik IT, klade důraz na následující aspekty:

1. Jednoduché hodnocení rizik – jednou z možností, o které se mohou efektivní metody pro řízení rizik opírat, je 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 [17]. Riziko se zde jednoduše počítá jako prostý součin možných dopadů, pravděpodobnosti výskytu dopadu a pravděpodobného selhání provedených opatření, což je jednoduché a všem srozumitelné vyjádření rizika a zároveň dostatečné pro vyhodnocení působnosti daného rizika.

2. Definice struktury pro řízení rizik s cílem provázat metodu řízení rizik s konkrétním prostředím informačních a komunikačních systémů. Snahou je především jednoznačně

určit odpovědnosti související s řízením rizik, definovat pravidla pro rozhodování, způsoby komunikace či vykazování apod.

3. Posílení schopnosti zvládání rizik – použité metody a nástroje dovolují sledovat tzv. životní cyklus rizika (od odhalení a ohodnocení rizika, přes návrh způsobu zvládání včetně určení odpovědných osob, až po kontrolu skutečného prosazení vhodných opatření).

4. Využití a analýza různých zdrojů vstupních informací s cílem umožnit využití širokého spektra a složitých vazeb vstupních informačních zdrojů. Proto je žádoucí definovat registr rizik IT, jako automatizovaný nástroj pro systematické shromažďování a vyhodnocování informací o rizicích IT. Registr je základem pro evidenci rizik IT a pro shromažďování a vyhodnocování informací, které jsou pro efektivní řízení rizik IT potřebné.

Z výše uvedeného vyplývá, že základem systému řízení rizik IT, je jednoznačné stanovení používaných metod pro analýzy a zvládání rizik spojené s použitím registru rizik IT. Důležitým cílem je také upřesnění jednotlivých stupnic, podle kterých budou posuzována aktiva, hrozby, zranitelnosti a rizika. Dalším úkolem je upřesnění terminologie související s rozdělením a strukturováním prostředí IT včetně určení příslušných odpovědných pracovníků a garantů.

Registr rizik by měl podporovat minimálně následující funkce:

1. Identifikaci aktiv – vymezení hranic pro řízení rizik IT a popis aktiv či služeb, které jsou do rozsahu řízení rizik IT zahrnuty.

2. Stanovení hodnoty aktiv – určení hodnoty aktiv či služeb a jejich význam pro organizaci, ohodnocení možného dopadu jejich ztráty, změny či poškození.

3. Identifikaci hrozeb a zranitelností – určení scénářů, které mohou ovlivnit negativně hodnotu aktiv či služeb, a určení zranitelností, které mohou umožnit negativní působení těchto hrozeb.

4. Stanovení závažnosti hrozeb a míry zranitelnosti – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti prostředí vůči dané hrozbě.

5. Definici ochranných opatření – pro eliminaci identifikovaných a ohodnocených rizik je třeba navrhnout účinné nápravné opatření a to provázat s daným rizikem, respektive aktivem, na které riziko potenciálně působí.

Zopakujme, hlavní výhodou uvedeného moderního pojetí je výrazné posílení schopností zvládání rizik. Metoda na jedné straně dovoluje sledovat tzv. životní cyklus rizika (od odhalení a ohodnocení rizika, přes návrh způsobu zvládání včetně určení odpovědné osoby, až po kontrolu skutečného prosazení bezpečnostních opatření).

Pro vlastní analýzu rizik je vhodné v případě moderního pojetí využívat metody, které dovolí identifikovat a popsat bezpečnostní rizika, která jsou specifická pro dané prostředí. Vhodná je například metoda FRAP [41], která se opírá o řízené workshopy mezi odbornými garanty, uživateli informačního systému či aplikace a pracovníky informatiky odpovědnými za vývoj a provoz systému. Hlavní výhodou metody FRAP je snaha o otevřenou komunikaci mezi oběma stranami, která přispívá ke sdílení představ a zlepšení vzájemné výměny informací a často vede k odhalení doposud skrytých bezpečnostních rizik [47].

5.5 Doporučení BITS

Jako východisko pro řízení rizik v této práci byla vybrána metodika BITS [17]. Riziko se zde jednoduše počítá jako prostý součin možných dopadů, pravděpodobnosti výskytu dopadu a pravděpodobného selhání provedených opatření, což je jednoduché a všem srozumitelné vyjádření rizika a zároveň dostatečné pro vyhodnocení působnosti daného rizika. Metodika je obohacena o definici škál pro hodnocení dopadu, hrozby a zranitelnosti. Škály pro hodnocení jsou numerické. Významným přínosem této metody je však to, že i ve výpočtu od sebe odděluje hrozbu a zranitelnost, což je v souladu s ISO/IEC 27005:2008. Lze tak pohodlně modelovat vlastnost systému, kde se uplatňují hrozby.

Kapitola 6

Bezpečnost IT služeb

Tato kapitola se věnuje možnosti propojení managementu služeb IT a informační bezpečnosti [48]. Ukazuje příbuzná témata obou oblastí ve dvou rovinách:

1. Prvně se zaměřuje na zlepšení systémů řízení informační bezpečnosti za přispění procesního řízení oblasti ISO/IEC 20000.

2. Následně je pohled zaměřen na řízení služeb IT s cílem zajistit bezpečnost služby.

I když v dalších částech práce je rozvíjen pohled druhý, první část je zde rozebírána proto, aby byl jasný následující fakt: adopce procesů ISO/IEC 20000 významně zlepšuje systémy řízení informační bezpečnosti a opačně – poskytování služeb IT bez zajištění informační bezpečnosti není možné (viz kapitola 6.6 standardu ISO/IEC 20000-1:2005).

6.1 Role ISO/IEC 20000 v informační bezpečnosti

V této sekci budou uvedeny možnosti vylepšení ISMS na základě standardů ISO/IEC 20000. Konkrétněji, bude uveden seznam procesů vhodných k tomuto účelu a budou poskytnuty příklady praktického nasazení pro zlepšení ISMS. Nicméně, důrazně doporučujeme studium ISO/IEC 20000 pro identifikaci specifických potřeb byznysu a informační bezpečnosti. Poznamenejme ještě, že oblasti již pokryté standardy řady ISO/IEC 27000 nejsou brány v úvahu (například odborná způsobilost, povědomí a výcvik, bezpečnost informací samotná atd.). Text v této sekci částečně vychází z [48].

Řízení úrovně služeb: veškeré poskytované služby včetně jejich měřitelných charakteristik musím být odsouhlaseny všemi zainteresovanými stranami; každá dohoda musí být zdokumentována; změny v dohodách a poskytovaných službách podléhají procesu řízení změn; dohody musejí být přezkoumávány a jim podléhající služby pravidelně měřeny a z měření plynoucí nedostatky řešeny.

Využití v informační bezpečnosti: každá dohoda o úrovni služeb by měla zohledňovat i dohodnuté požadavky na informační bezpečnost za využití měřitelných veličin, tzv. ISMS metrik. Dohodnuté bezpečností parametry musejí taktéž podléhat přezkoumání a zlepšování. Důležitým aspektem jsou i dohodnuté podmínky, za kterých je bezpečnost ze strany dodavatele garantována.

Kontinuita služeb a řízení dostupnosti: cílem je zajistit za všech okolností splnění závazků vyplývajících z dohod o úrovních služeb; plány pro zajištění kontinuity a dostupnosti musejí být nejméně jednou ročně přezkoumány a testovány (toto je prováděno i po

každé významné změně služby); dostupnost musí být měřena, zaznamenávána a zjištěné nesrovnalosti napraveny. Poznámka: řízení kontinuity je samostatně ošetřeno standardem BS 25999.

Využití v informační bezpečnosti: jádrem ISMS je systém pro řízení rizik v informační bezpečnosti. Předmětem řízení kontinuity by mela být rizika, která mají kritický potenciální dopad, ale jejich pravděpodobnost výskytu je malá.

Řízení kapacit: zajišťuje, že ve všech okamžicích poskytování služby bude mít poskytovatel dostatečné kapacity pro uspokojení zákazníků a naplnění dohod o úrovních služeb; kapacity musejí být plánovány, monitorovány a predikovány.

Využití v informační bezpečnosti: například v případě technologických systémů pro zajištění IT bezpečnosti (IPS, IDS), zajištění dostatečných výpočetních kapacit je nutným požadavkem pro zajištění technické funkcionality.

Vztahy se zákazníky a dodavateli: je zřejmé, že cílem je vybudovat dobré vztahy s dodavateli poskytovatele služeb i jeho zákazníky; základ dobrých vztahů je v proaktivitě a sledování potřeb zákazníka i dodavatele.

Využití v informační bezpečnosti: v případě dodávky služby, kde nedílnou část tvoří informační bezpečnost a zároveň je část dodávané služby outsourcována dodavateli, hrají dobré vztahy s dodavatelem kritickou roli.

Management incidentů a problémů: jsou dva velmi úzce provázané procesy; cílem řízení incidentů je co nejrychlejší obnovení služby po jejím výpadku; veškeré incidenty by měly být zaznamenány, prioritizována a řešeny v soulady s potřebami byznysu; cílem managementu problémů je předcházet incidentům a to i proaktivně.

Využití v informační bezpečnosti: management incidentů je již pokryt ISO/IEC 27000, význam ISO/IEC 20000 je zejména v rozšířeném pohledu na řízení problémů.

Řízení konfigurací: jádrem procesu je konfigurační databáze (CMDB), která obsahuje veškeré informace o aktivech důležitých pro byznys; CMDB zahrnuje kromě položek i vztahy mezi nimi, jejich verze a změny; cílem procesu je udržování CMDB, její pravidelné přezkoumání a řešení případných nedostatků.

Využití v informační bezpečnosti: zřejmé využití může být například v detekci neaktuální verze firmwaru bezpečnostního prvku na IT infrastruktuře. Velmi zajímavou oblastí je ale podpora hodnocení informačních aktiv z hlediska důvěrnosti, integrity a dostupnosti a fakt, že registr rizik informační bezpečnosti není z pohledu ISO/IEC 20000 nic jiného, než část CMDB.

Řízení změn: veškeré změny musejí být ohodnoceny, odsouhlaseny, implementovány a kontrolovány řízeným způsobem; veškeré změny musejí být dokumentovány pro detekci trendů a potenciálních problémů v budoucnu; hodnocení musí být provedeno z pohledu potenciálního rizika a dopadu na byznys.

Využití v informační bezpečnosti: je zřejmé, že neautorizované anebo neohodnocené změny mohou mít významný dopad na informační bezpečnost v mnoha oblastech.

Proces uvolnění: je úzce spjat s managementem změn a konfigurací; cílem je dodávka a řízení změny do produkčního prostředí; každé uvolnění musí být plánováno se zákazníkem a patřičně testováno; každá dodávka musí obsahovat i procedury pro návrat v případě selhání dodávky.

Využití v informační bezpečnosti: jeden z přínosů lze vidět právě v existenci procedur pro návrat do původního stavu, když nové uvolnění ohrozí bezpečnost cílového prostředí.

6.2 Informační bezpečnost v službách IT – dohody o úrovni bezpečnosti

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 témže místě, jako definice provozních parametrů – v SLA. Frankova a Yautsiukhin v [27] navrhují 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. Přijměme 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[1]:

1. Požadavky na bezpečnost služby IT na straně poskytovatele.
2. 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.

Situace je znázorněna na obrázku 6.1, zdůrazněny jsou dvě části PLA. Důležité je poznamenat, že jak prostředí dodavatele tak i konzumenta služby IT ohrožují rizika, která je nutno eliminovat na akceptovatelnou úroveň.

Příklad: Společnost má dle ISO/IEC 20000-1:2005 certifikovanou službu Servis. Ta spočívá v poskytování servisních zásahů na software i hardware dle dohodnutých SLA. V konkrétním PLA se poskytovatel služby zavázal, že ručí za zajištění požadované důvěrnosti informačních aktiv, které jsou uloženy na servisovaných nosičích. Na druhou stranu, konzument služby se zavázal k tomu, že informační nosiče (pevné disky, flash moduly síťových zařízení apod.) budou obsahovat jen taková informační aktiva, která jsou v souladu s přijatým klasifikačním schématem konzumenta služby[2]. Jednoduše řečeno, vysoce důvěrná data budou uložena jen na nosičích k tomu určených a označených, ne jinde.

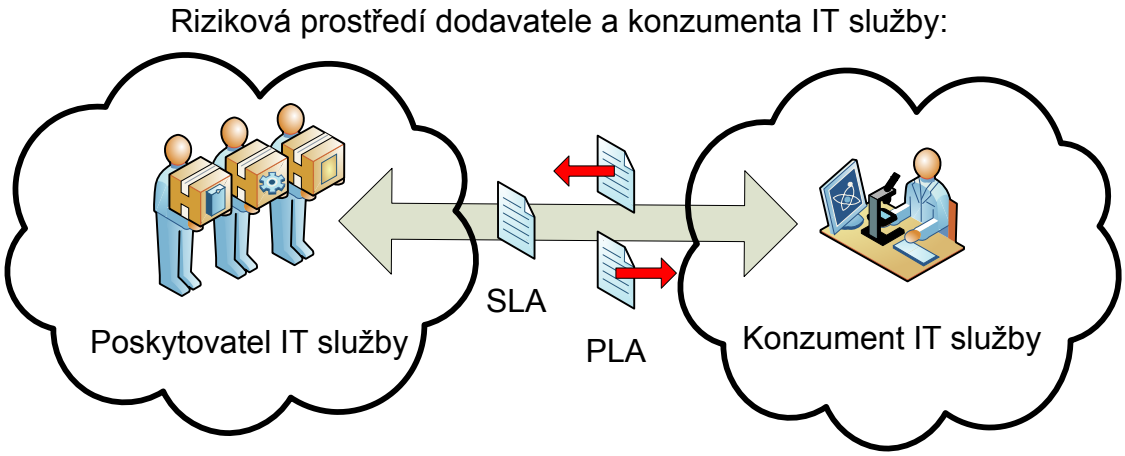
[Konec příkladu.]

6.2.1 Navrhovaná struktura PLA

Tato podkapitola obsahuje navrhovanou strukturu PLA, jedná se o návrh, vychází z [11, 12, 13, 14, 15, 16]. V praxi musí samozřejmě reflektovat potřeby konkrétního byznysu a

[1] Tento přístup byl také implementován do mezinárodního vědeckovýzkumného projektu MASTER (http://www.master-fp7.eu/) v rámci Sedmého rámcového programu Evropské unie (http://cordis.europa.eu/fp7/home_en.html). Na výzkumu se také podíleli Jan Fanta a Luděk Novák ze společnosti ANECT, a.s.

[2] V informační bezpečnosti se k eliminaci rizik používá katalogu ISO/IEC 27002:2005, kde jsou na základě rizikové analýzy aplikovány kontroly z katalogu a tím je v praxi dosaženo snížení rizika na akceptovatelnou úroveň. Zde se jedná o kontroly kapitoly 7 ISO/IEC 27002:2005.



Obrázek 6.1: Umístění PLA mezi dodavatelem a konzumentem služby IT.

požadavků na bezpečnost poskytované služby IT.

- Stručný popis bezpečnostních parametrů služby.
- Platnost PLA, mechanizmus řízení změn PLA.
- Způsoby autorizace.
- Dohodnuté způsoby komunikace zahrnující incident a problém reporting apod.
- Popis dohodnutých bezpečnostních kontrol zajišťujících eliminaci bezpečnostních rizik na obou stranách kontraktu SLA/PLA:

  Bezpečnostní politika.

  Bezpečnostní kontroly zajišťující ochranu aktiv (tedy v rámci služby IT) jako personál, informace, software a hardware.

  Prvky fyzické ochrany.

  Principy ochrany před škodlivým software.

  Mechanizmy zajišťující detekci potenciální ztráty nebo ohrožení důvěrnosti, integrity anebo dostupnosti chráněných aktiv.

  Procedury zajišťující, že dohodnutá aktiva budou bezpečně zničena nebo navrácena po ukončení platnosti kontraktu anebo v dohodnutou dobu.

  Požadovanou úroveň důvěrnosti, integrity a dostupnosti chráněných aktiv v rámci poskytování/konzumování služby IT.

  Restrikce zohledňující přípustné sdílení informací.

  Mechanizmy zajišťující zvyšování odborného povědomí vzhledem k individuálním zodpovědnostem.

  Jasné procedury pro reporting.

- Odpovědnosti konzumenta souvisejících s ochranou dat.
- Dohodnuté reakce v případě výpadku poskytované služby IT nebo bezpečnostního incidentu.

- Registr rizik.

Kriticky důležitou částí PLA je registr rizik, který byl diskutován v předchozích částech práce. Musí být zajištěno, že je znám oběma stranám kontraktu a že jej obě strany stejně interpretují.

6.3 Shrnutí

V této kapitole byly definovány PLA – dohody o úrovni bezpečnosti služeb IT. PLA obsahuje společné ujednání pro poskytovatele i konzumenta a dále obsahuje požadavky, které musejí oba partneři splnit, aby bylo dosaženo společného cíle, dohodnuté úrovně bezpečnosti. Dále bylo konstatováno, že oba partneři se pohybují v určitém rizikovém prostředí, tudíž mohou oba zapříčinit selhání bezpečnosti. Byla uvedena možná struktura PLA, ze které se bude vycházet při konkrétní implementaci.

Kapitola 7

Řízení rizik v PLA

V úvodu práce byly stručně představeny metody pro analýzu rizik. Tato kapitola se blíže věnuje rizikovému prostředí mezi dodavatelem a konzumentem služby IT, protože má svoje specifika, jak bude ukázáno dále. Poznámka: v následujících částech práce je používán termín "řízení rizik v PLA", tím je myšleno řízení rizik informační bezpečnosti poskytované služby IT. Tento termín je zvolen jako krátké a výstižné vyjádření.

7.1 Přístup k analýze rizik

Jak již bylo zmíněno v úvodu práce, metoda analýzy rizik vychází z doporučení BITS [17]; to znamená, že pro každý rizikový scénář hodnotí dopad, hrozbu a zranitelnost. Ze zkušeností autora práce však vyplývá, že interpretace těchto pojmů může být značně odlišná. Lépe řečeno, autor práce se ještě nesetkal s tím, že by tyto pojmy byly interpretovány naprosto identicky např. v různých organizacích. Proto je nutné přesně definovat jejich význam tak, jak bude použit v dalších částech práce – jasně definovat vlastní interpretaci a použití těchto pojmů.

7.1.1 Dopad

Pojem DOPAD bude chápán jako záporná hodnota užitku [45, 29, 31, 42][1]. To znamená, že dopad nebude chápán pouze jako finanční ztráta, plynoucí například z poškození serveru požárem, ale jako celková škoda plynoucí z realizace rizikového scénáře. Tedy, i kdyby byla peněžní hodnota ztráty rovna "pouhým" 100 000 Kč, může být následkem i poškození důvěryhodnosti společnosti apod., které finanční částku značně převyšuje. Definujme proto následující relativní stupnici pro vyjádření dopadu (negativního užitku), viz Tabulka 7.1.

Jak již bylo řečeno, i interpretace tak základních pojmů jako dopad, hrozba a zranitelnost se liší společnost od společnosti[2], kde je systém řízení rizik implementován, tudíž definice škál taktéž. Důležité je však zdůraznit, že závěry a postupy plynoucí z této práce nejsou závislé na konkrétní definici, lze je snadno převést na libovolný systém řízení rizik.

7.1.2 Hrozba

Pojem HROZBA bude chápán jako pravděpodobnost dopadu, pokud nejsou implementována žádná ochranná opatření. Bylo by možné vést diskuzi o tom, zdali je tento termín

[1] Pojem pocházející z ekonomiky, viz například http://en.wikipedia.org/wiki/Utility

[2] Tato vychází z doporučení BITS, to platí i pro škály hrozby, zranitelnosti a výsledného rizika.

Stupeň	**Dopad – popis**	Min. [-]	Max. [-]
Nízký	Dopad působí v malém rozsahu, má omezený časové trvání a není katastrofický.	0	3
Střední	Dopad působí v omezeném rozsahu a má omezené časové trvání.	4	30
Vysoký	Dopad působí v omezeném rozsahu, ale jeho následky jsou trvalé anebo katastrofické.	31	300
Kritický	Dopad působí plošně, trvale a katastroficky.	301	1000

Tabulka 7.1: Definice stupňů dopadu.

korektní, ale to není cílem této práce. Definujeme následující stupnici pro hrozbu, viz Tabulka 7.2.

Stupeň	**Hrozba – popis**	Min. [%]	Max. [%]
Nízký	Výskyt hrozby není očekávaný.	0	25
Střední	Výskyt hrozby může nastat.	26	50
Vysoký	Výskyt hrozby zřejmě nastane.	51	75
Kritický	Výskyt hrozby je velmi pravděpodobný nebo jistý.	76	100

Tabulka 7.2: Definice stupňů hrozby.

7.1.3 Zranitelnost

Pojem ZRANITELNOST je chápán jako pravděpodobnost, že selže ochranné opatření. Některé přístupy stanovují zranitelnost jako zranitelnost aktiva, některé oddělují aktivum od ochrany. Nehledě na přístup, zranitelnost je to, co lze ovlivnit. Zranitelnost popisuje vlastnost systému, vlastnost (slabiny) řízení, technologií, organizace jako celku apod. Celé řízení rizik se tak vlastně zabývá efektivním snižováním zranitelnosti tak, aby nedošlo k realizaci rizikového scénáře. Definujeme následující stupnici pro zranitelnost, viz Tabulka 7.3.

Stupeň	**Zranitelnost – popis**	Min. [%]	Max. [%]
Nízký	Bezpečnostní opatření jsou aplikována a jejich zranitelnost či selhání je možné vyloučit.	0	25
Střední	Bezpečnostní opatření jsou aplikována a jejich zranitelnost či selhání není možné vyloučit, nicméně selhání bude neprodleně odhaleno.	26	50
Vysoký	Bezpečnostní opatření jsou aplikována a jejich zranitelnost či selhání není možné vyloučit.	51	75
Kritický	Bezpečnostní opatření nejsou aplikována anebo jsou vysoce zranitelná/neúčinná.	76	100

Tabulka 7.3: Definice stupňů zranitelnosti.

Ještě než přejdeme k vyčíslení celkového rizika, je třeba zdůraznit jeden fakt, který je klíčový pro celou analýzu rizik pomocí rizikových scénářů. A to i vzhledem k tomu, že v praxi, podle zkušeností autora práce, tento fakt není velmi často pochopen. Proměnné dopad, hrozba a zranitelnost definují riziko. To jest pravděpodobnost, že nastane hrozba využije zranitelnost a způsobí dopad. Ale definice konkrétního scénáře je dána pouze na úrovni dopadu a hrozby. Uveďme si příklad: pravděpodobnost toho, že dojde ke ztrátě dat (například ztráta notebooku v tramvaji) a ta budou následně zneužita je jistě menší, než pravděpodobnost pouhé ztráty dat. V prvním případě je vyšší dopad (negativní hodnota užitku) a nižší pravděpodobnost, v druhém opačně. Ale vzhledem k faktu, že vyčíslení výsledného rizika je dáno násobkem jeho složek, celková hodnota rizika se nemění. A právě absence pochopení tohoto faktu bývá v praxi často důvodem, proč jsou analýzy rizik zbytečné "rozvláčné" a obsahují mnoho nepodstatných informací, které jsou redundantní a řízení rizik podstatně znepřehledňují. Jsou totiž zahrnovány scénáře typu server vyhoří částečně a server vyhoří úplně, apod.

Nyní se vraťme zpět k dokončení přístupu k analýze rizik. Ještě je totiž nutné přesně definovat, jak naložit s výsledným rizikem. K tomu definujme následující škálu, viz Tabulka 7.4.

Stupeň	**Riziko – popis**	Min. [-]	Max. [-]
Nízký	Riziko je tolerováno a považováno za zbytkové.	0	10
Střední	Riziko je monitorováno a, s ohledem na účelnost, eliminováno méně náročnými bezpečnostními opatřeními. V případě vyšší náročnosti řešení je přípustné riziko akceptovat.	11	30
Vysoký	Riziko by mělo být systematicky odstraňováno a jeho dlouhodobá existence není přípustná.	31	300
Kritický	Výskyt rizika není přípustný a vždy musí být neprodleně zahájeny kroky k jeho odstranění.	301	1000

Tabulka 7.4: Definice stupňů rizika.

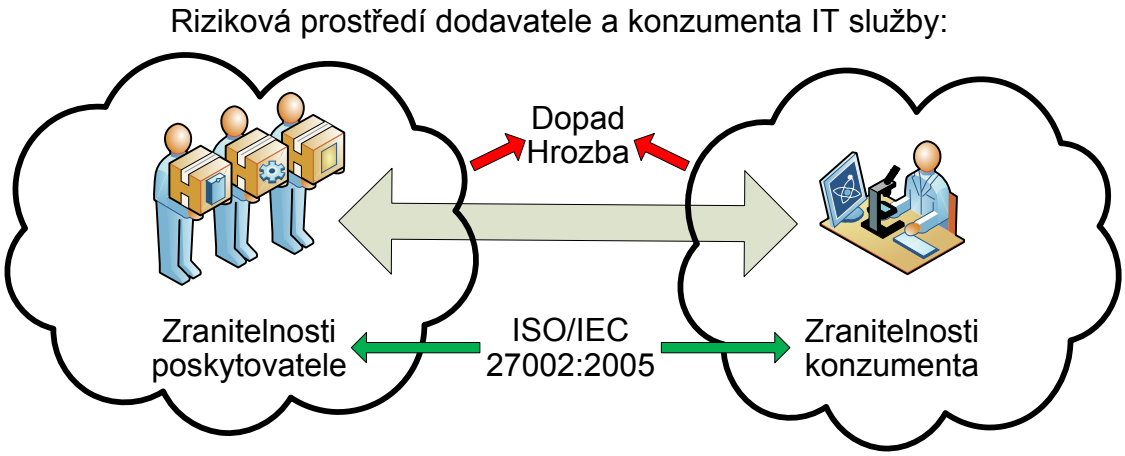
Z tabulky 7.4 je patrné, že pokud výsledná hodnota rizika nepřekročí 10, riziko lze tolerovat. Co ale s rizikem hodnoty 15? Dle definice je zvládáno s ohledem na efektivitu, účinnost daných opatření a náročnost. Ale jak změřit onu náročnost a jak změřit efektivitu opatření? A co když je prostředí poskytovatele a konzumenta služby IT rozdílně vyspělé, co se týká bezpečnosti? Odpovědi na tyto otázky dává text v následujících částech práce.

7.2 Zvládání rizika v PLA

Po tom, co jsme obecně definovali přístup k analýze rizik, je čas definovat rizikový scénář s ohledem na zkoumané prostředí – prostředí mezi dodavatelem a konzumentem služby IT[3].

Obrázek 7.1 zobrazuje jednotlivé složky rizika a způsoby zvládání rizika pomocí snižování zranitelností. Obrázek 7.1 je v souladu s definicí PLA, konkrétně s částí vztahující odpovědnost za bezpečnost služby IT na poskytovatele i konzumenta služby IT. Pokud se na

[3]Celá metodika je ale vyvíjena tak, aby bylo možné přístup použít i na komplexnější struktury, jenž se v praxi mohou vyskytnout. Poskytovatel IT služby může mít také své dodavatele, kteří mohou ovlivnit celý systém řízení bezpečnosti služeb IT.



Obrázek 7.1: Rizikový scénář v PLA a jeho zvládání.

zvládání rizik podílí více subjektů dohromady, je otázka efektivního zvládání rizika mnohem komplikovanější, než v případě jednoho subjektu. V potaz je třeba vzít všechna relevantní hlediska jako třeba i finanční zdroje potřebné k implementaci konkrétního opatření.

Každý manažer rizik se ve své práci setká s otázkou, jaká opatření na zvládnutí daného rizika aplikovat a která ne. Opatření mohou být rozdílně účinná na daný typ zranitelnosti, náklady na implementaci opatření jsou také různá a v praxi se nemusejí vždy vyplatit. Pro to, abychom byli schopni hodnotit, jak je dané opatření přínosné, zavedeme následující ukazatele:

1. Relevance opatření.
2. Vyspělost opatření.

7.2.1 Relevance 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. Uveďme si příklad: opatření 9.2.1 ISO/IEC 27002:2005 Umístění zařízení a jeho ochrana, toto opatření 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 definujme množinu relevancí jako lineární diskrétní stupnici od 0 do 1, kde 1 značí maximální relevanci daného opatření k danému riziku:

$$R = \{0; 0,25; 0,5; 0,75; 1\} \tag{7.1}$$

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 infrastruktuře tak, aby nebylo vždy nutné se spoléhat na odhady. Následující tabulka z významového hlediska radikálně rozšiřuje použitou metodiku BITS i jiné systémy řízení rizik, se kterými se autor ve své praxi a v

dostupné literatuře setkal – definice stupňů relevance, viz Tabulka 7.5[4].

Stupeň	Relevance opatření – popis
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.

Tabulka 7.5: Definice relevancí opatření katalogu opatření.

Poznámka, definice stupně nula relevance je zde pouze pro úplnost. V praxi toto opatření jistě nebude zavedeno, neboť neredukuje příslušnou zranitelnost.

7.2.2 Vyspělost opatření

Vyspělost 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. V doporučení BITS ale slouží pouze jako intuitivní ukazatel pro analytiky a manažery, zde se bude podílet na výpočtu zvladatelnosti rizika. Tento přístup opět významně rozšiřuje obzory v řízení rizik. Definujme množinu vyspělostí jako lineární diskrétní stupnici od 0 do 1, kde 1 značí maximální vyspělost daného opatření:

$$V = \{0; 0,25; 0,5; 0,75; 1\} \tag{7.2}$$

Definice vyspělosti daného opatření, viz Tabulka 7.6. Definice škály částečně vychází z velmi uznávané metodiky CobiT [4, 39], kde je také možné nalézt další informace.

Na ukazatel vyspělosti však existuje ještě druhý pohled. Čím je opatření méně vyspělé, tím dražší pro organizaci bude jeho implementace. Náklady budou různé pro různá opatření ISO/IEC 27002:2005 a v různých prostředích (například nákup technologie versus implementace procesu, implementace procesu v již procesně vyspělém prostředí versus "na zelené louce"). Tato práce se však nezabývá odhady nákladů v projektech a náklady budou sloužit pouze jako pomocný ukazatel. V budoucnu je ale cílem tuto metodiku rozšířit i o analýzu nákladů [44] na bezpečnost a zakomponování těchto dat do výpočtu efektivity zvládání rizik.

Z tabulek 7.5 a 7.6 plyne, že pokud je ukazatel relevance na maximu a naopak ukazatel vyspělosti na minimu, dané opatření se bude maximálně podílet na redukci zranitelnosti konkrétního rizika.

Výše uvedené ukazatele lze libovolně rozšířit o další podle potřeb konkrétního byznysu, taktéž jednotlivé definice mohou být nastaveny podle konkrétních potřeb.

[4]Toto nemusí být žádné dogma, organizace si samozřejmě může zvolit svoje vlastní škály, to platí i pro definici vyspělosti.

Stupeň	Vyspělost opatření – popis
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.

Tabulka 7.6: Definice stupnice pro vyspělosti opatření.

7.3 Redukce zranitelnosti

Tento oddíl práce se věnuje způsobu redukce rizika snižováním zranitelnosti, vzhledem k:

1. Relevanci opatření.
2. Vyspělosti daného opatření.
3. Výsledné hodnotě rizika.

Ještě ale před tím, než bude přístup formalizován, je zapotřebí na příkladu uvést celou filozofii, jak se k redukci bude přistupovat. Jde o vysvětlení jedné z klíčových části práce. Tento způsob prezentace je zvolen z důvodu, který byl již zmíněn – na poli řízení rizik existuje velké množství různých interpretací daného problému a pro přínos této práce je důležité, aby byl celý koncept interpretovatelný pouze jedním způsobem.

Pro tuto chvíli pracujme s dvěma rizikovými scénáři tak, jak je uvedeno v následující tabulce, viz Tabulka 7.7. Poznámka: D značí dopad, H značí hrozbu, Z označuje zranitelnost.

D	H	Z počáteční	Z požadovaná	Z rozdíl
350	15	30	19	11
350	15	20	19	1

Tabulka 7.7: Příklady hodnot rizikových scénářů.

Každý řádek v tabulce obsahuje identicky ohodnocený rizikový scénář (hodnoty 350 a 15 % pro dopad resp. hrozbu), předpokládejme, že fakticky popisuje scénář totožnou situaci. Z numerických hodnot je dále vidět, že vlastnosti prostředí, kde je rizikový scénář popisován, jsou poněkud odlišné – viz zranitelnost 30 % respektive 20 %. Vzhledem ale k výpočtu rizika ($Riziko = Dopad * Hrozba * Zranitelnost$) a hranici pro akceptaci rizika rovnu hodnotě přibližně 10 (viz Tabulka 7.4) je jasné, že v praxi musí být učiněn mnohem větší krok k nápravě tam, kde je zranitelnost vyšší. Bylo totiž řečeno, že zranitelnost popisuje vlastnost systému a jen tu lze v rizikovém scénáři měnit – popsáno posledním sloupečkem v tabulce.

Redukce zranitelností má s ohledem na definované relevance a vyspělosti opatření několik specifik, které je nutno zdůraznit:

1. Pokud se na oba 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 vyspělost daných opatření (v případě vyšší zranitelnosti je vyspělost 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 vyspělost 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 případu, 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[5].

5. Pokud analytik nalezl 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.

Body popsané výše jsou velmi důležité pro vykreslení kontextu navrhované metodiky s realitou řízení rizik. Každý systém řízení rizik se nutně musí opírat o odhady, pozorování, zkušenosti a rozhodnutí. Matematické nástroje a metodiky poskytují systémům řízení rizik určitá vodítka a mantinely a proto je třeba posuzovat celek komplexně a ne odděleně.

Nyní formálně definujme následující funkce, které budou klíčové pro řízení rizik v PLA. Jedná se o:

1. Funkci “zvladatelnosti zranitelnosti”.

2. Funkci “agregované zvladatelnosti zranitelnosti”.

3. Funkci “optimalizované redukce rizika”.

7.3.1 Funkce zvladatelnosti zranitelnosti

Zavedení hodnocení zvladatelnosti zranitelnosti pro každé opatření, jenž analytik vybral pro redukci rizika, je jedním ze základních inovativních přínosů předkládané práce. Tato myšlenka již byla nastíněna v předešlé části, nyní bude detailně definována a formalizována.

Pro každé opatření byl definován parametr relevance a vyspělosti. Právě tyto nové parametry slouží pro výpočet zvladatelnosti zranitelnosti a to následovně:

[5]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.

1. Parametr relevance opatření popisuje, jakou měrou se opatření vztahuje k zvládání dané zranitelnosti. Slouží k porovnání jednotlivých opatření. Pokud je relevance jednoho opatření vyšší než jiného, potom více přispívá k redukci.

2. Parametr vyspělosti 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 vyspělostí nižší.

Definujme funkci zvladatelnosti zranitelnosti pro každé opatření (vybrané pro zvládání rizika) z katalogu ISO/IEC 27002:2005 (případně dalších) jako funkci relevance a vyspělosti opatření následovně:

$$Z_i = r_i * (1 - v_i) \tag{7.3}$$

kde:

- Z_i je hodnota zvladatelnosti zranitelnosti pro uvažované opatření.
- r_i je hodnota relevance pro uvažované opatření.
- v_i je hodnota vyspělosti pro uvažované opatření.
- index i značí jedno konkrétní opatření, $i \in \langle 1, n \rangle$ a n je počet vybraných opatření.

Hodnota v_i vstupuje do výpočtu po převodu na "nižší hodnota je žádoucí", respektive nižší hodnota vyspělosti se více podílí na zvladatelnosti zranitelnosti.

Důležitá poznámka: do výpočtu jsou zahrnuta opatření všech zúčastněných stran SLA/PLA kontraktu.

Příklad: mějme variantu, kde jsou účastníky kontraktu pouze poskytovatel služby IT a její konzument. Tabulka 7.8 pro vybraná opatření (zatím označena pouze pořadovým číslem) zobrazuje rizikovým analytikem definované relevance a vyspělosti opatření.

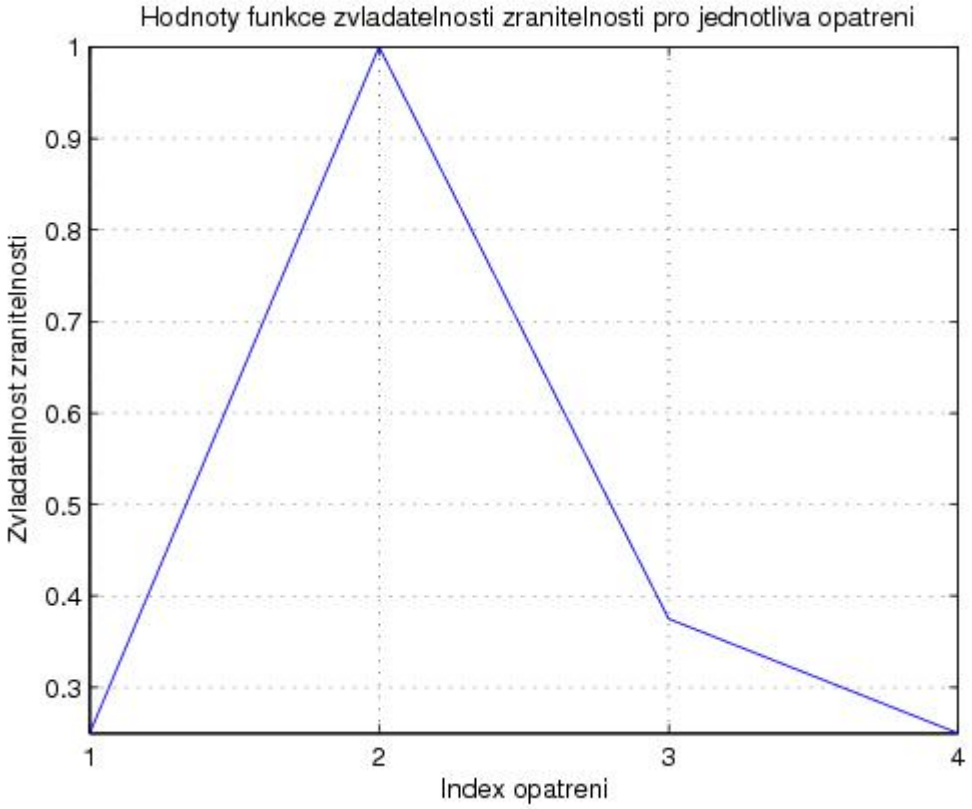
	1	2	3	4
Relevance opatření	1	1	0,75	0,25
Vyspělost opatření	0,75	0	0,5	0

Tabulka 7.8: Hodnocení opatření poskytovatele služby IT.

Graf na obrázku 7.2 zobrazuje hodnoty funkce zvladatelnosti zranitelnosti pro jednotlivá opatření definovaná v tabulce 7.8. Lze poukázat na fakt, že poslední opatření s indexem 4 má pouze o něco málo nižší schopnost zvládat riziko než opatření s indexem 3, ačkoli je u něho mnohem nižší hodnota relevance. Je to dáno tím, že vyspělost je na mnohem nižší úrovni.

Současně konzument poskytované služby IT může disponovat (má je implementovány na určité úrovni nebo je bude teprve implementovat v rámci zabezpečení služby IT) škálou opatření viz Tabulka 7.9. Poznámka, index opatření se stejným číslem značí to samé opatření z katalogu.

V tabulce 7.9 je vidět, že opatření s indexem 1 již evidentně existuje v obou prostředích a je rozdílně vyspělé. Zatímco v případě poskytovatele služby IT je již implementováno, na



Obrázek 7.2: Hodnoty zvladatelnosti zranitelnosti opatření pro poskytovatele služby IT.

	1	9	10	11
Relevance opatření	1	0,5	0,5	0,5
Vyspělost opatření	0	0	0	0

Tabulka 7.9: Hodnocení opatření konzumenta služby IT.

straně konzumenta nikoli a tudíž se bude podílet vyšší měrou na zvládání rizika. Relevance stejných opatření musejí být samozřejmě totožná.

Graf na obrázku 7.3 zobrazuje celou situaci graficky.

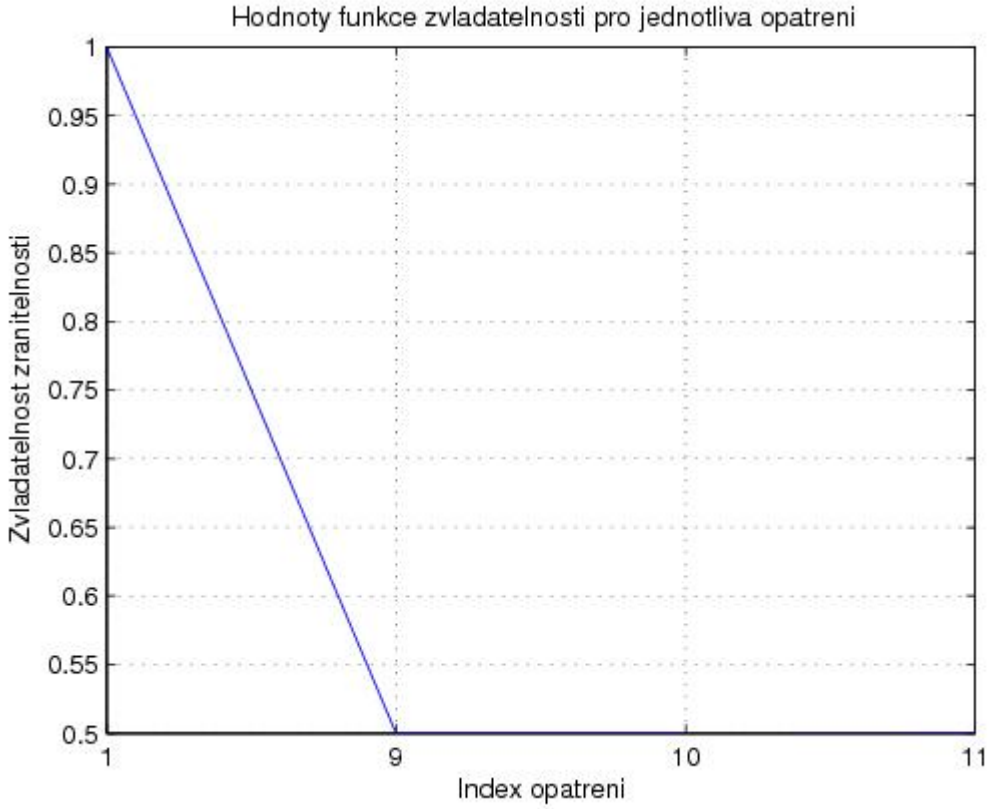
[Konec příkladu.]

Samozřejmě se může v praxi stát, a v případě řízení více rizik se to děje naprosto typicky, že jedno opatření se váže na zvládání více rizik. Jedná se jak o technologická, tak i o organizační opatření, příkladem může být bezpečnostní politika, rozdělení pravomocí apod.

V tomto případě se zachází s relevancí a vyspělostí opatření následovně:

- Relevance opatření se pro jednotlivá rizika sčítají. Cílem je ohodnotit opatření přes celý systém řízení rizik a potom, i když může opatření nabývat malých relevancí u mnoha rizik, se z opatření jako celku stane důležitý bezpečnostní projekt, který se podílí na zvládání mnoha rizik.

- Vyspělost opatření zůstává na své původní hodnotě, jako v případě řízení jednoho



Obrázek 7.3: Hodnoty zvladatelnosti zranitelnosti opatření pro konzumenta služby IT.

rizika. Je to očekávané, neboť vyspělost opatření jednoduše hodnotí, jak je daná bezpečnostní kontrola funkční v okamžiku analýzy a nemění na tom nic ani fakt, že se opatření již podílí, nebo teprve bude podílet, na zvládání více rizik.

7.3.2 Funkce agregované zvladatelnosti zranitelnosti

V okamžiku, kdy jsou rizika zanalyzována (je vyčíslena jejich numerická hodnota), je dalším krokem výběr opatření pro jejich zvládání. 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 zvládání rizik vybere analytik sadu opatření, která se nějakým způsobem mohou podílet na zvládání zranitelnosti. Jsou dva extrémní případy – analytik vybere buď naprosto všechna vázající se opatření nebo žádné. Lze očekávat, že rozumné řešení bude ležet někde

mezi. V současných systémech řízení rizik se ono "mezi" jednoduše odhadne. My si nyní ukážeme, jak ono "mezi" vypočíst (kompletní výpočet bude dokončen v další podkapitole). Definujme nejprve matici kombinací K typu (m, n), kde $m = 2^n$ a n značí počet vybraných opatření. Každý řádek matice je tvořen prvky binárního čísla získaného z převodu dekadického čísla $(m - 1)$. Nyní definujme:

$$Z_{A_m} = \sum_{i=1}^{n} K(m, i) * Z_i \tag{7.4}$$

kde:

- Z_{A_m} je hodnota funkce agregované zvladatelnosti zranitelnosti pro danou kombinaci opatření.
- K je matice kombinací typu (m, n).
- Z_i je hodnota zvladatelnosti zranitelnosti pro konkrétní opatření.
- i je index jednotlivých vybraných opatření, $i \in \langle 1, n \rangle$.
- n označuje počet jednotlivých vybraných opatření.

Příklad: mějme společné prostředí dodavatele služby IT a jejího konzumenta v SLA/PLA prostředí. Výběr opatření a jejich evaluace je popsána následovně (Tabulka 7.10 a 7.11):

	1	2
Relevance opatření	1	1
Vyspělost opatření	0,75	0

Tabulka 7.10: Hodnocení opatření poskytovatele služby IT.

	1	5
Relevance opatření	1	0,5
Vyspělost opatření	0	0,5

Tabulka 7.11: Hodnocení opatření konzumenta služby IT.

Jelikož se obě strany SLA/PLA kontraktu podílejí na zvládání rizik, lze veškerá opatření shrnout, jakoby situace odpovídala řízení rizik v jednodimenzinálním systému, viz Tabulka 7.12:

	1	2	1	5
Relevance opatření	1	1	1	0,5
Vyspělost opatření	0,75	0	0	0,5

Tabulka 7.12: Hodnocení opatření poskytovatele služby IT.

Matice kombinací je dána maticí A (první sloupec řídí zapojení prvního opatření, druhý druhého, atd.; počet řádků matice udává počet hodnot funkce agregované zvladatelnosti zranitelnosti):

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

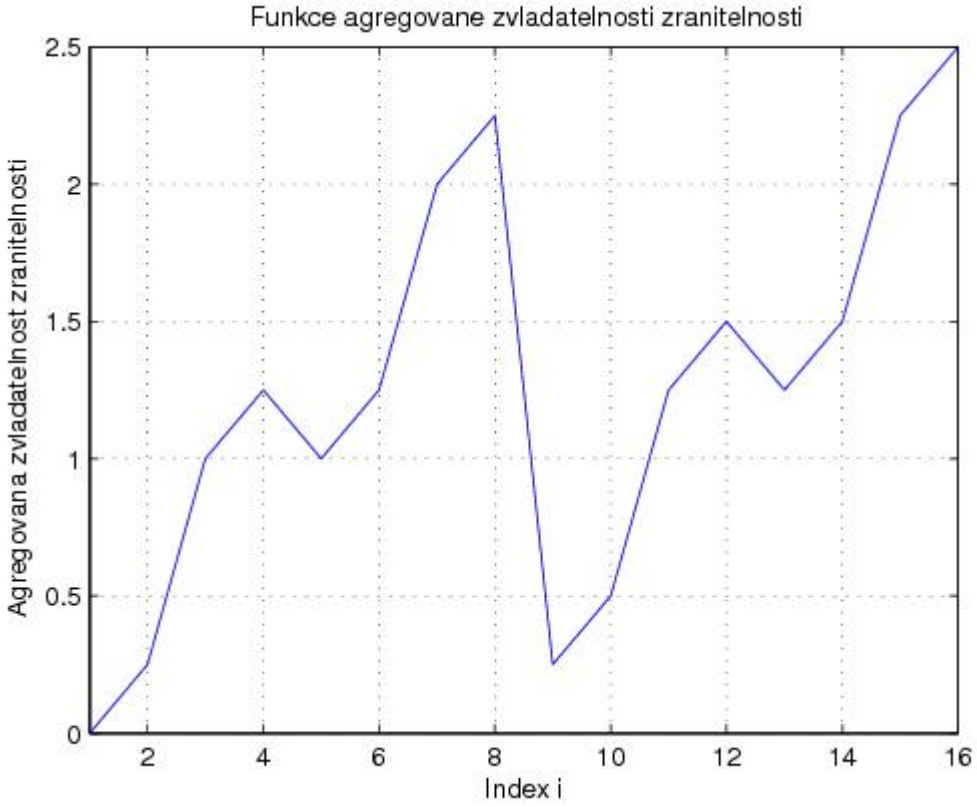
Potom lze hodnoty funkce agregované zvladatelnosti zranitelnosti zobrazit na následujícím grafu (Obrázek 7.4):

Nás však budou zajímat hodnoty funkce agregované zvladatelnosti zranitelnosti setříděné od nejmenší hodnoty po nejvyšší – to přesně odpovídá žádnému zvládání rizika a maximálnímu. Připomeňme, že hledáme určitou "zlatou střední cestu", neboť řízení rizik v jakémkoli oboru je, mimo jiné, o přiměřeném chování v dané situaci. Obrázek 7.5 ukazuje setříděné hodnoty funkce agregované zvladatelnosti zranitelnosti.

Velmi zajímavý je pak výstup v matici B ukazující, jak se na základě setřídění hodnot funkce agregované zvladatelnosti změnili řádky matice A:

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Výsledek je do jisté míry očekávaný – první řádek matice obsahuje samé nuly, poslední jedničky. Důležité jsou však hodnoty ve spodní části matice, které právě ukazují, která



Obrázek 7.4: Hodnoty funkce agregované zvladatelnosti zranitelnosti.

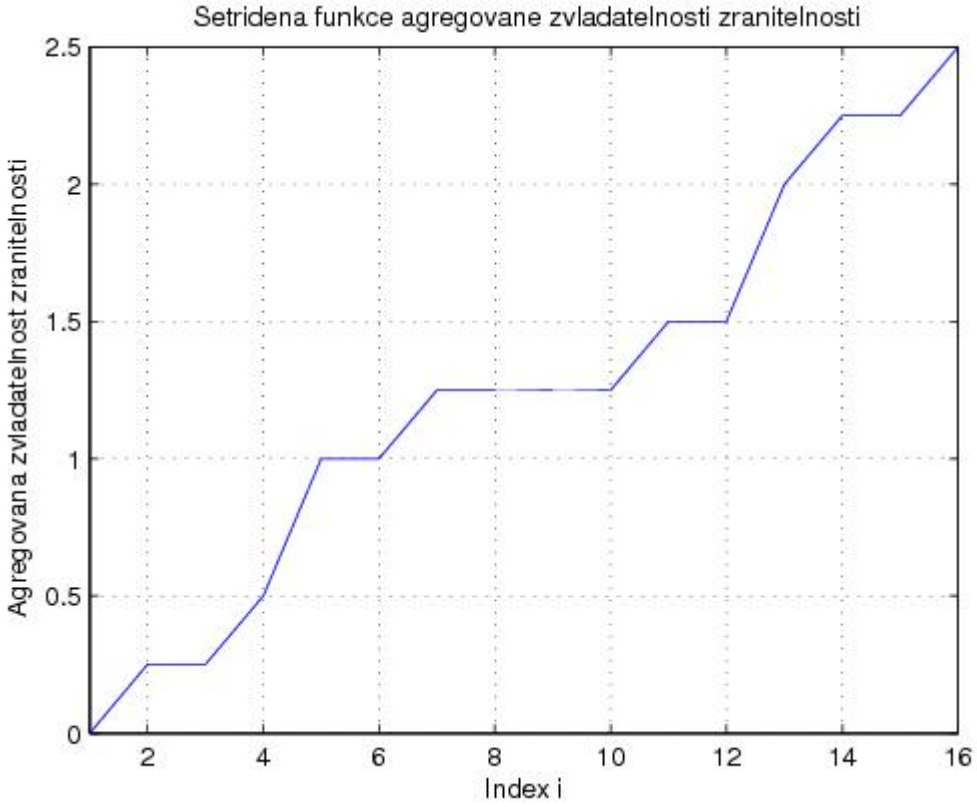
opatření (ať na straně dodavatele služby IT nebo konzumenta) již není nutné implementovat, viz následující sekce.

Pokud budeme ale hodnoty na Obrázku 7.5 zkoumat blíže, zejména ty s vyššími hodnotami, vidíme, že se například v grafu vyskytují dvě hodnoty $0,25$. To odpovídá indexům v předposledním a předpředposledním řádku matice. Vyplývá z toho zajímavý závěr, aniž bychom ještě hodnotili hodnotu rizika – z pohledu zvládání rizik je jedno, jestli bude implementováno první opatření u poskytovatele služby IT nebo poslední u konzumenta (viz Tabulka 7.12). Rozhodnutí pak závisí na dalších hlediscích, například na nákladech na zavedení opatření [44] nebo vůbec na ochotě daného subjektu věnovat se bezpečnosti.

[Konec příkladu.]

7.3.3 Funkce optimalizované redukce rizika

Ještě než bude poslední část systému pro optimalizované řízení rizik formalizována a uvedeny příklady, zopakujme, proč je důležité ke zvládání rizik přistupovat onou rozumnou zlatou střední cestou. Příklad: i když si to mnoho lidí nemusí uvědomit, rizika řídí na každém kroku svého života a zvažuje, co ještě podniknout, aby se vyhnuli nežádoucím incidentům. Například při přecházení vozovky je určitě rozumné se dobře rozhlédnout a až pokud člověk nazná, že mu nehrozí vážné nebezpečí, přejde. Pokud by se člověk vůbec nerozhlédl (neimplementoval ochranná opatření), je mnohem větší pravděpodobnost, že utrpí újmu nebo dokonce zemře. Na druhou stranu, jistě je zbytečné si například obstarávat detailní statistiky o tom, v jakou denní dobu daným místem projíždí největší množství



Obrázek 7.5: Hodnoty setříděné funkce agregované zvladatelnosti zranitelnosti.

osobních vozidel, nákladních vozidel a jak často zrovna daným místem projíždí nelegální závod luxusních automobilů. Každý člověk má samozřejmě svou vlastní interpretaci toho, co rozumné je a co už není. Proto v nikde v této práci není řečeno "právě toto" je správně, ale jsou dány alternativy na zvážení – tedy přesně tak, jak každý člověk řídí rizika ve svém vlastním životě i v organizaci při řízení bezpečnosti služeb IT.

Pro vyjádření různých přístupů k redukci rizik (odborně nazýváno risk apetit) se definujme následující:

$$R_P = dopad * hrozba * zranitelnost_P \tag{7.5}$$

kde:

- R_P je původní hodnota rizika, před zvládáním.
- *dopad* a *hrozba* definují rizikový scénář standardním způsobem.
- $zranitelnost_P$ je původní hodnota zranitelnosti.

a

$$R_I = dopad * hrozba * zranitelnost_I \tag{7.6}$$

kde:

- R_I je ideálně dosažitelná hodnota rizika, pokud budou všechna vybraná opatření implementována naprosto dokonale.

- $zranitelnost_I$ je ideální hodnota zranitelnosti, pokud budou všechna vybraná opatření implementována naprosto dokonale.

a

$$zranitelnost_m = (Z_{A_m} * (zranitelnost_P - zranitelnost_I)) + zranitelnost_I \tag{7.7}$$

kde:

- $zranitelnost_m$ je hodnota zranitelnosti při dané hodnotě funkce agregované zvladatelnosti zranitelnosti.

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

$$R_m = dopad * hrozba * zranitelnost_m \tag{7.8}$$

kde:

- R_m je aktuální hodnota rizika při dané kombinaci opatření.

Nyní budou uvedeny dva příklady, jak výše uvedené formalizmy použít pro optimalizaci jednoho a více rizik.

Funkce optimalizované redukce rizika – jedno riziko

Definujme riziko následujícím rizikovým scénářem: $Dopad = 350$, $Hrozba = 0,5$ (což odpovídá 50%). Zranitelnost systému byla analýzou stanovena taktéž na 50%. Tomu odpovídá hodnota rizika $87,5$. Analytik na základě svých zkušeností vybral sadu opatření (viz níže) a stanovil, že pokud budou všechna implementována na maximum, je možné dosáhnout snížení rizika až na hodnotu 2 (čemuž odpovídá hodnota ideální zranitelnosti $1,14$%). V předchozích částech práce bylo však definováni, že hodnota pro akceptaci rizika je rovna deseti a rizika hodnoty až třicet jsou akceptovatelná, pokud by jejich redukce znamenala příliš velké náklady nebo bylo rozhodnuto z jiných důvodů, že daná opatření nebudou implementována.

Nyní uvažujme následující sadu opatření (Tabulka 7.13):

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

Tabulka 7.13: Hodnocení opatření daného systému řízení.

Potom funkce agregované zvladatelnosti vypadá následovně (Obrázek 7.6):

Potom hodnoty setříděné funkce agregované zvladatelnosti vypadají takto (Obrázek 7.7):

Z hodnot setříděné funkce agregované zvladatelnosti zranitelnosti plynou následující kombinace opatření (matice C):

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Na základě ale toho, jak se vyvíjí hodnota rizika při daných opatřeních (viz Obrázek 7.8), lze stanovit, že zajímavá oblast, kde je prostor pro manažerská rozhodnutí, je u posledních cca šesti kombinací zavedení opatření, tedy následujících, daných maticí D:

$$D = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Pokud by se navíc jednalo o SLA/PLA prostředí jako v předchozích podsekcích, bylo by možné optimalizovat, na jaké straně kontraktu bude opatření implementováno.

Poznámka, na grafu vývoje hodnot rizika (viz Obrázek 7.8), zelená a červená linka naznačuje hranice pro nutnou a možnou akceptaci rizika.

Funkce optimalizované redukce rizika – více rizik

V případě optimalizace více rizik je nutné vyhnout se následujícímu potenciálnímu problému. Pokud by byla opatření pro jednotlivá rizika hodnocena odděleně, mohlo by se stát, že po optimalizaci redukce rizika budou vypadávat opatření, která nejsou z pohledu řízení jednoho rizika tak atraktivní. Vezměme například bezpečnostní politiku organizace. Lze předpokládat, že její relevance bude k mnoha rizikům spíše na nižší úrovni a pokud by navíc měla již poměrně vysokou vyspělost, bude v porovnání s jinými opatřeními zřejmě málo atraktivní.

Tento problém je eliminován tak, že jsou všechna opatření analyzována z pohledu řízení jednoho rizika. To znamená, že veškeré relevance jsou pro dané opatření sečteny, vyspělosti opatření pochopitelně zůstávají, a na základě nich je vypočtena jejich optimální kombinace. Poté jsou již v rámci jednotlivých rizik posuzovány pouze odpovídající opatření, ale v původní kombinaci, kde byly relevance sečteny. Je tak dosaženo jak pohledu z celé organizace, tak pohledu řízení a optimalizace jednotlivých rizik.

Uvažujme následující seznam ohodnocených opatření (viz Tabulka 7.14):

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

Tabulka 7.14: Hodnocení opatření daného systému řízení.

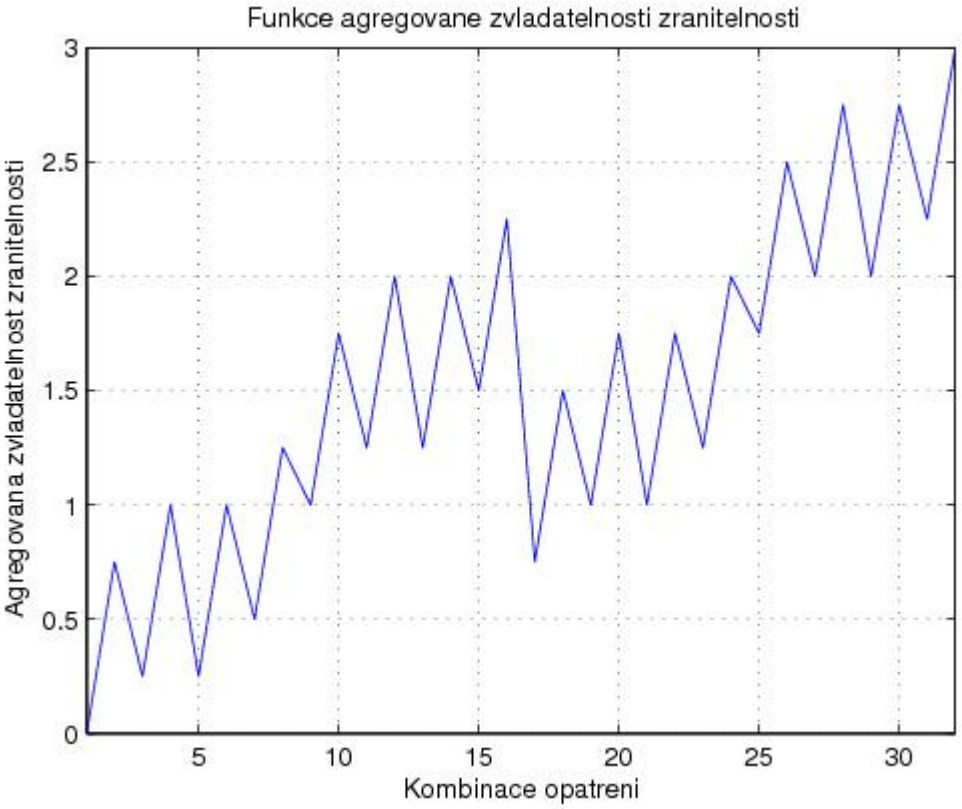
Ale s tím podstatným rozdílem, že opatření s indexem 2 se podílí na zvládání více rizik. Dále předpokládejme, že tabulka opatření pro jedno konkrétní riziko vypadá takto (viz Tabulka 7.15):

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

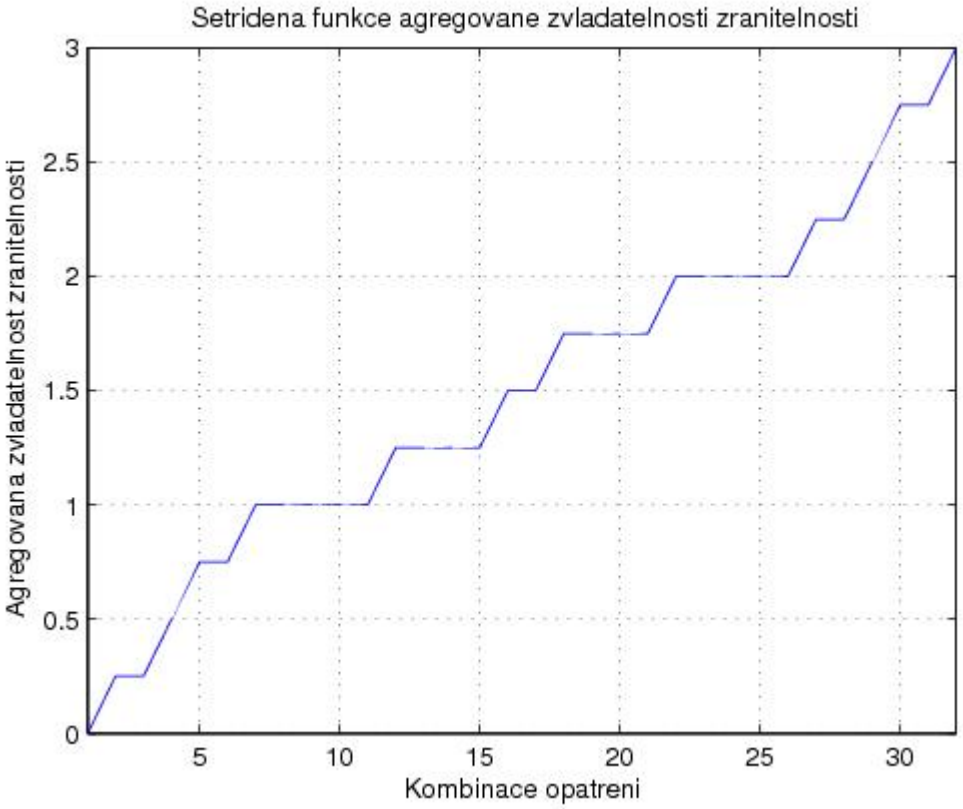
Tabulka 7.15: Hodnocení opatření daného systému řízení.

Na základě algoritmů výše uvedených byly propočítány jednotlivé kombinace implementace opatření (na základě dat v tabulce 7.14, odpovídají pohledu na bezpečnost organizace), ale do optimalizace rizika byla vzata data z tabulky 7.15) (odpovídající pohledu optimalizace rizika). Výsledek lze vidět na obrázku 7.9.

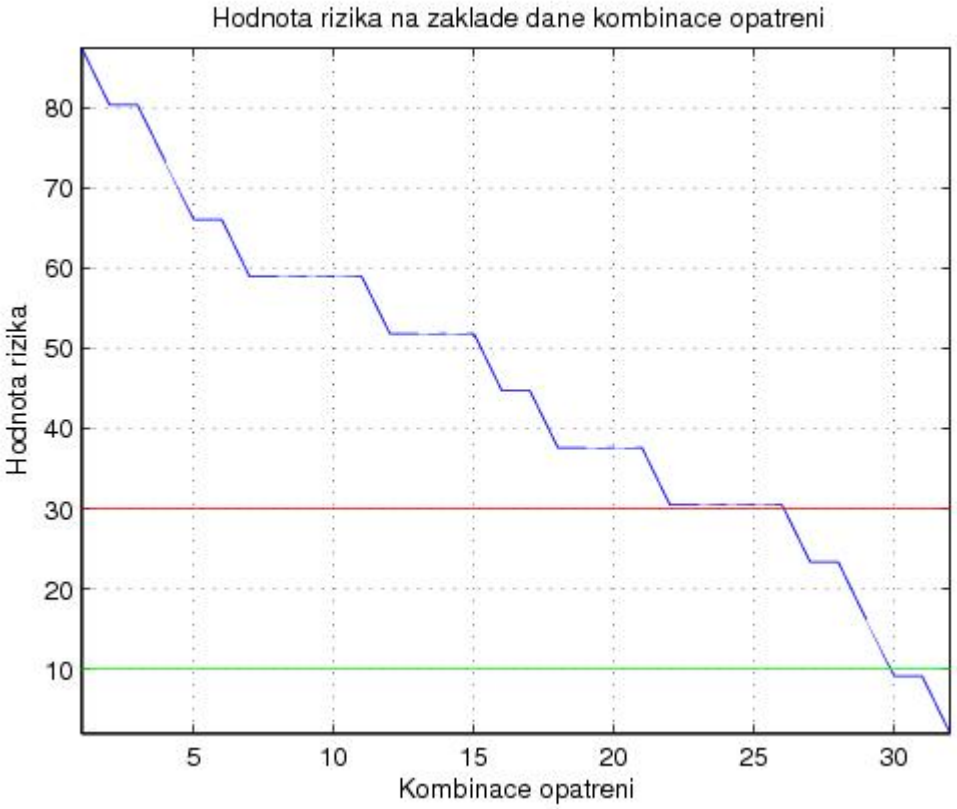
Oproti předchozímu grafu (Obrázek 7.8) je zobrazena křivka v černé barvě, která odpovídá optimalizaci jediného rizika. Je vidět, že průběh již není tak “hladký”, jako v případě optimalizace jediného rizika a takto čeká analytika o něco obtížnější úkol v rozhodování, což ale plně odpovídá typům rozhodnutí v řízení rizik obecně.



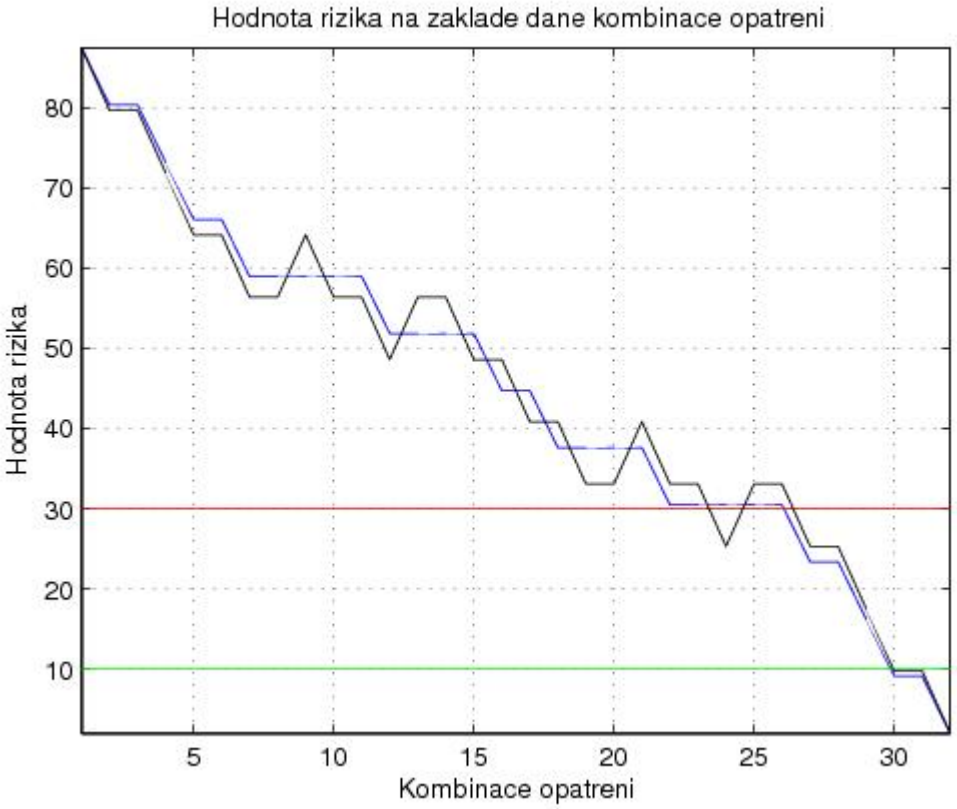
Obrázek 7.6: Hodnoty funkce agregované zvladatelnosti zranitelnosti.



Obrázek 7.7: Hodnoty setříděné funkce agregované zvladatelnosti zranitelnosti.



Obrázek 7.8: Hodnoty vývoje rizika na základě implementovaných kombinací opatření.



Obrázek 7.9: Hodnoty vývoje rizika na základě implementovaných kombinací opatření.

Kapitola 8

Modelování

Až do této chvíle byla řeč o optimálním výběru opatření ke zvládání rizik na základě jejich relevance a vyspělosti. To je skutečně jeden ze základních přínosů této práce. Navíc lze ale najít i další, a to je možnost modelování a výpočtu současného zbytkového rizika.

Představme si situaci, kdy ke zvládání rizika analytik vybere, na základě algoritmů výše definovaných, optimální strategii. V tu chvíli ale je stále hodnota rizika stejná jako v době analýzy a je užitečné, aby bylo při postupné implementaci opatření možno sledovat, jak se hodnota rizika snižuje. Navíc, nikde není řečeno, a v praxi to tak může být, že vyspělost opatření pouze roste. Například, pokud bude jako jedno z opatření vybrána bezpečnostní politika, tak ta musí být také dobře komunikována uvnitř společnosti, jinak je, volněji řečeno, k ničemu. Pokud ale dojde z různých důvodů k výrazné obměně zaměstnanců v organizaci, což může být v současné době ekonomické krize a rozbouřených finančních trhů aktuální téma, jistě nějakou dobu potrvá, než bude opět bezpečnostní politika komunikována dovnitř společnosti na uspokojivé úrovni. Pokud se k tomu navíc přidají ještě další opatření, jejichž vyspělost díky aktuálním okolnostem poklesne, může dojít ke zpětnému zvýšení rizika až na takovou úroveň, že se stane prioritou v organizaci a bude řešeno přednostně.

Do současné doby, kdy je zbytkové riziko pouze odhadováno, toto umožněno není. Pokud ano, tak pouze na základě hlubokých zkušeností analytika. Ty jsou samozřejmě užitečné vždy, ale nástroj, který mu umožní modelovat a zobrazovat situaci v reálném čase, jistě přispěje k efektivnějšímu řízení rizik.

8.1 Výpočet aktuálního zbytkového rizika

Pro ilustraci, jak je možné v průběhu zvládání rizik, což je de-facto nikdy nekončící proces, monitorovat jejich aktuální hodnotu, bude použit následující příklad:

Příklad: Mějme tato opatření – Tabulka 8.1:

	1	2	3
Relevance opatření	1	1	1
Vyspělost opatření	0	0	0

Tabulka 8.1: Opatření v modelování výpočtu zbytkového rizika – původní stav.

Opatření jsou již vybrána na základě předchozích algoritmů. Opatření se nepodílejí

na zvládání jiných rizik. Rizikový scénář je numericky ohodnocen takto: $Dopad = 400$, $Hrozba = 0,3$, $Zranitelnost = 0,25$, tudíž hodnota rizika je $Riziko = 30$. Na základě výpočtu kombinací vhodných opatření směřující k ideální hodnotě rizika bylo analytikem stanoveno, že jako cílová hodnota rizika bude postačující dosáhnout hodnoty 15. Z toho plyne hodnota cílové zranitelnosti $0,125$.

Je zřejmé, že cílové hodnotě rizika odpovídá tento stav opatření – Tabulka 8.2:

	1	2	3
Relevance opatření	1	1	1
Vyspělost opatření	1	1	1

Tabulka 8.2: Opatření v modelování výpočtu zbytkového rizika – cílový stav.

Plná implementace jednoho opatření tedy odpovídá snížení rizika o hodnotu $\frac{30-15}{3} = 5$, to samé platí například i pro poloviční implementaci dvou opatření anebo třetinovou implementaci všech tří opatření. Plná implementace dvou opatření odpovídá hodnotě $\frac{30-15}{3} * 2 = 10$ a tak dále. Na druhou stranu, pokud dojde ke snížení vyspělosti některého z opatření, analogickým postupem se hodnota rizika zvyšuje. Pochopitelně, pokud by byla relevance opatření nižší anebo již opatření mělo určitou vyspělost, díl ke snížení zranitelnosti by byl poměrně nižší, než v případě opatření v tabulce 8.2.

Korektní způsob je samozřejmě výpočet konečné hodnoty rizika přes snižování hodnoty zranitelnosti.

Tímto způsobem je možné sledovat časový vývoj všech rizik v organizace skrze aktualizaci vyspělostí jednotlivých opatření. Tato funkcionalita by měla být implementována registrem rizika tak, aby bylo umožněno analytikovi pohodlné sledování vývoje rizik.

[Konec příkladu.]

Kapitola 9

Plná verze metodiky řízení rizik v bezpečnosti služeb IT

Ještě před tím, než budou závěry z předchozích kapitol demonstrovány na případových studiích, bude uvedena plná verze navrhované metodiky řízení rizik služeb IT. Tato metodika částečně vychází z doporučení BITS, dále z metodiky používané autorem disertační práce ve své praxi a je doplněna o aspekty řízení bezpečnosti služeb IT a to zejména o nově vyvinutý způsob řízení rizik. Nikde v textu však nebude zmíněno, zdali se jedná o multidimenzionální prostředí (v našem případě SLA/PLA prostředí) nebo pouze jednodimenzionální. Je to z toho důvodu, aby text metodiky nebyl zavádějící a mohl být použit libovolně, je však zaměřen na informační bezpečnost. Je vhodné poznamenat, že uvedená metodika není žádné dogma. Může být libovolně modifikována pro uspokojení potřeb konkrétního byznysu anebo zvyklostí organizace či analytika, klíčová část se týká pouze navrhovaného způsobu řízení rizik.

Je důležité poznamenat, že uvedená metodika je mezi těmi, které měl autor práce možnost studovat naprosto ojedinělá. Všechny se totiž týkaly pouze identifikace a analýzy rizik. Nikoli však analýzy jejich zvládání. V tomto směru tato metodika vyplňuje významnou mezeru na trhu.

Účelem metodiky je provádět analytika procesem analýzy a řízení rizik. Algoritmy jsou implementovány v registru rizik, který analytik používá.

9.1 Všeobecná ustanovení

Řízení rizik je klíčovým prvkem pro vybudování informační bezpečnosti. Jeho maximální účinnost je podmíněna dodržením následujících principů:

- Multidisciplinární přístup – ohodnocení a zvládání rizik vyžaduje zapojení širokého spektra uživatelů s hlubokými znalostmi fungování organizace. Ne všichni uživatelé mají stejný pohled na hodnocení vážnosti jednotlivých aspektů bezpečnostních opatření.
- Systematické a centralizované řízení – definované procesy a centrální řízení a koordinace zajišťují standardizovaný, jednotný a úplný pohled na řízení rizik.
- Integrovaný proces – řízení rizik je východiskem pro budování uceleného systému řízení informační bezpečnosti a na základě analýzy rizik mají být vybírána a implementována vhodná bezpečnostní opatření.

- Odpovědnost za činnosti – hlavní odpovědnost za řízení rizik nese nejvyšší vedení, které musí upřesnit rozsah a pověřit střední management spoluprací s bezpečnostním manažerem.
- Dokumentace – zdokumentování procesu řízení rizik pomáhá zajistit celistvost a úplnost celého procesu. Zároveň je důležitá pro prosazení pravidelného opakování procesu.
- Zlepšení znalostí – řízení rizik zvyšuje znalosti managementu o způsobu a formě zpracování informací a význam IT (informačních a komunikačních technologií) pro činnost organizace.
- Pravidelná aktualizace – postup řízení rizik by měl být pravidelně aktualizován v souladu s vývojem a implementací nových technologií a to nejméně jednou ročně.

Pro potřeby řízení rizik v informační bezpečnosti používá organizace registr rizik. Základem metody řízení rizik je doporučení BITS Technology Risk Transfer Gap Analysis Tool od sdružení Bank Information Technology Secretariat (BITS) z dubna 2002. Za správnost informací uvedených v registru rizik odpovídá bezpečnostní manažer. Bezpečnostní manažer provádí průběžně aktualizaci informací a jejich vyhodnocení, 1x za rok předkládá výstupy řízení rizik vedení organizace.

9.2 Identifikace a ohodnocení aktiv

9.2.1 Identifikace aktiv a jejich garantů

Aktivum je komponenta nebo část celkového systému, které má pro organizaci určitou hodnotu, a proto je nutné tuto hodnotu chránit. Při identifikaci aktiv je nutné vzít v úvahu, že systémy IT netvoří jen technické a programové vybavení a že cena vlastních informací ve většině případů převyšuje hodnoty vlastních technologií.

Identifikace aktiv se opírá o následující obecné typy aktiv:

- Informační aktiva (primární aktivum) – datové a databázové soubory, dokumentace systému, uživatelské příručky a jiné školicí materiály, popisy procesů a postupů, smlouvy a jiné papírové dokumenty apod.
- Služby IT (primární aktivum) – informační a komunikační služby, definovaná rozhraní informačních systémů podle katalogu služeb.
- Softwarová aktiva (sekundární aktivum) – aplikační software, systémový software, vývojové nástroje a utility.
- Fyzická aktiva (sekundární aktivum) – počítačové a komunikační zařízení, magnetická a optická média, další technické vybavení (např. UPS, tiskárny, klimatizace, . . .) apod.
- Personál (sekundární aktivum) – lidské zdroje, tzn. management IS, vývojoví a provozní pracovníci, uživatelé a odběratelé apod.
- Podpůrné služby (sekundární aktivum) – technické a další služby nutní pro zajištění běžného chodu IT jako např. dodávka tepla či chladu, elektrické energie, apod.
- Ostatní aktiva (sekundární aktivum) – nábytek, trezory, zabezpečené prostory apod.

Nezbytnou součástí identifikace aktiv je určení vlastníka (garanta) aktiva. Jedná se o osobu, které za aktivum věcně odpovídá.

Evidenci všech aktiv provádí bezpečnostní manažer v registru rizik.

9.2.2 Ohodnocení aktiv

Klíčovým prvkem je určení hodnoty identifikovaných aktiv. Při ocenění aktiv jsou především následující oblasti:

1. Osobní údaje a obchodní tajemství.
2. Právní povinnosti a jiné závazky.
3. Narušení vnitřních řídících a kontrolních činností.
4. Finanční ztráty.
5. Ztráta dobrého jména.

Pro hodnocení aktiv a skupin aktiv jsou definovány následující tři stupnice, ve kterých jsou měřítka pro vyjádření míry důvěrnosti, integrity, dostupnosti (tabulky 9.1, 9.2 a 9.3):

Stupeň	Důvěrnost
Nízký	Informace jsou veřejně dostupné anebo jsou určené ke zveřejnění. Informace určené pro zveřejnění jsou do doby zveřejnění značeny slovy “Veřejné” nebo zkratkou “VEŘ”.
Střední	Informace nejsou veřejně dostupné např. informace potřebné pro připravení rozhodnutí organizace či informace, kde zákon neumožňuje zveřejnění či umožňuje odepřít zveřejnění. Aktiva jsou označována jako informace pro vnitřní potřebu. Informace pro vnitřní potřebu nejsou označeny vůbec nebo jsou značeny slovy “Pro vnitřní potřebu” nebo zkratkou “VP”.
Vysoký	Informace nejsou veřejně dostupné a jejich neoprávněné prozrazení může závažně ohrozit či ztížit činnost organizace, mít závažné negativní právní důsledky, například způsobit újmu fyzické nebo právnické osobě nebo osobě které se informace týká, přičemž se tato osoba může domoci náhrady za tuto. Chráněné informace jsou značeny slovy “Chráněné informace” nebo zkratkou “CH”.
Kritický	Informace jsou vysoce citlivé a jejich ochrana vyžaduje zvláštní bezpečnostní režim. Jedná se především o osobní údaje či citlivé osobní údaje podle zákona č. 101/2000 Sb. případně o utajované informace podle zákona č. 412/2005 Sb. Osobní údaje jsou značeny slovy “Osobní údaje” nebo zkratkou “OSÚ”.

Tabulka 9.1: Metodika – definice stupňů důvěrnosti.

Za ohodnocení aktiv odpovídají vlastníci (garanti) aktiv. Přehled o ohodnocení všech aktiv vede bezpečnostní manažer v registru rizik.

Stupeň	Integrita
Nízký	Narušení integrity dat neohrožuje oprávněné zájmy organizace. Ochrana integrity dat není vyžadována.
Střední	Narušení integrity dat může zapříčinit poškození oprávněných zájmů organizace, ale nemá zásadní vliv na plnění podstatných činností organizace. Pro ochranu integrity jsou využity standardní prostředky.
Vysoký	Narušení integrity vede k poškození oprávněných zájmů organizace a projevuje se přímými dopady. Pro ochranu integrity dat by měly být využity speciální prostředky, které provedené změny propojí s individuální odpovědností osoby.
Kritický	Narušení integrity vede k velmi vážnému poškození oprávněných zájmů organizace a projevuje se neschopností naplnit stanovený byznys organizace. Pro ochranu integrity dat musí být využity speciální prostředky, které provedené změny propojí s individuální odpovědností osoby.

Tabulka 9.2: Metodika – definice stupňů integrity.

9.3 Hodnocení vyspělosti bezpečnostních opatření

Bezpečnostní manažer pravidelně hodnotí vyspělost jednotlivých bezpečnostních opatření, a to jednou ročně nebo po každé významné změně. Bezpečnostní manažer uvede zdůvodnění pro aktuální stav, kdy není opatření zavedeno nebo je zavedeno jen částečně, například:

- Finanční omezení (závisí na existujícím rozpočtu na bezpečnost).
- Vliv prostředí (výběr opatření ovlivňuje prostor, klimatické podmínky, přírodní a městské okolní prostředí apod.).
- Technologické důvody (opatření nelze realizovat v případě neslučitelnosti hardware a software).
- Časové omezení (všechna opatření nemohou být implementována okamžitě).
- Situace, kdy nejsou požadavky opatření v organizaci aplikovatelné.

Bezpečnostní manažer hodnotí vyspělost opatření numericky a to na základě následující stupnice (Tabulka 9.4):

9.4 Identifikace bezpečnostních rizik

Při identifikaci bezpečnostních rizik a potřeb je nezbytné zvážit následující oblasti:

- Právní, regulatorní a smluvní požadavky (ochrana duševního vlastnictví, ochrana dokladů organizace, ochrana osobních údajů a soukromí, prevence zneužití prostředků pro zpracování informací, regulace kryptografických prostředků, shromažďování důkazů).

Stupeň	Dostupnost
Nízký	Narušení dostupnosti není důležité a jsou tolerovány delší výpadky (cca do 1 týdne).
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne.
Vysoký	Narušení dostupnosti aktiva by nemělo překročit dobu hodin. Výpadek je nutné řešit neprodleně. Organizace u aktiva toleruje výpadky v rozsahu několika málo hodin.
Kritický	Narušení dostupnosti aktiva není přípustné a vede k přímému ohrožení oprávněných zájmů organizace. Organizace u aktiva toleruje výpadky v rozsahu několika minut.

Tabulka 9.3: Metodika –definice stupňů dostupnosti.

Stupeň	Vyspělost opatření – popis
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.

Tabulka 9.4: Metodika –stupnice vyspělosti opatření.

- Funkční požadavky informační bezpečnosti (outsourcing, shoda se standardy, shoda s bezpečnostní politikou, koordinace informační bezpečnosti, bezchybné zpracování informací, dostupnost informací a prostředků pro jejich zpracování).
- Požadavky dané ohodnocením hrozeb a zranitelností (nedodržování informační bezpečnosti, právní, regulativní a smluvní požadavky, incidenty a selhání, zneužití, neautorizované změny, neautorizovaný přístup, škodlivé programy, nepřesné informace, bezpečná výměna informací a softwaru, použití kryptografických opatření, mobilní výpočetní prostředky a práce na dálku, chyba uživatele, fyzická bezpečnost, kontinuita činnosti organizace).

Při řešení musí být identifikovány relevantní rizikové scénáře a bezpečnostní potřeby, u kterých musí být vyhodnocena míra uplatnění hrozby a míra zranitelnosti systému. Součástí bezpečnostních rizik a potřeb jsou též výsledky šetření bezpečnostních incidentů a doporučení z provedených auditů.

Přehled o bezpečnostních rizicích a potřebách informační bezpečnosti vede bezpečnostní manažer v registru rizik.

9.4.1 Identifikace dopadů

Pro hodnocení dopadu je definována logaritmická stupnice, která hodnotí míru poškození společnosti v případě uplatnění výskytu nepředvídatelné události (tj. při plné účinnosti dané hrozby) – Tabulka 9.5.

Stupeň	**Dopad – popis**	Min. [-]	Max. [-]
Nízký	Dopad působí v malém rozsahu, má omezený časové trvání a není katastrofický.	0	3
Střední	Dopad působí v omezeném rozsahu a má omezené časové trvání.	4	30
Vysoký	Dopad působí v omezeném rozsahu, ale jeho následky jsou trvalé anebo katastrofické.	31	300
Kritický	Dopad působí plošně, trvale a katastroficky.	301	1000

Tabulka 9.5: Metodika – stupně dopadu.

Informace o dopadu bezpečnostních rizika a potřeb informační bezpečnosti a jejich zdůvodnění vede bezpečnostní manažer v registru rizik.

9.4.2 Identifikace hrozeb

Pro hodnocení hrozby je definována lineární procentuální stupnice, která vyjadřuje pravděpodobnost uplatnění hrozby tj. míru očekávání incidentu – Tabulka 9.6.

Stupeň	**Hrozba – popis**	Min. [%]	Max. [%]
Nízký	Výskyt hrozby není očekávaný.	0	25
Střední	Výskyt hrozby může nastat.	26	50
Vysoký	Výskyt hrozby zřejmě nastane.	51	75
Kritický	Výskyt hrozby je velmi pravděpodobný nebo jistý.	76	100

Tabulka 9.6: Metodika – stupně hrozby.

Informace o stupni hrozeb jednotlivých bezpečnostních rizik a potřeb informační bezpečnosti a jejich zdůvodnění vede bezpečnostní manažer v registru rizik.

9.4.3 Identifikace zranitelností

Pro hodnocení zranitelnosti je definována lineární procentuální stupnice, která vyjadřuje pravděpodobnost úspěšnosti uplatnění hrozby, tj. míru selhání bezpečnostních opatření – Tabulka 9.7.

Informace o stupni zranitelnosti jednotlivých bezpečnostních rizik a potřeb informační bezpečnosti a jejich zdůvodnění vede bezpečnostní manažer v registru rizik.

Stupeň	**Zranitelnost – popis**	Min. [%]	Max. [%]
Nízký	Bezpečnostní opatření jsou aplikována a jejich zranitelnost či selhání je možné vyloučit.	0	25
Střední	Bezpečnostní opatření jsou aplikována a jejich zranitelnost či selhání není možné vyloučit, nicméně selhání bude neprodleně odhaleno.	26	50
Vysoký	Bezpečnostní opatření jsou aplikována a jejich zranitelnost či selhání není možné vyloučit.	51	75
Kritický	Bezpečnostní opatření nejsou aplikována anebo jsou vysoce zranitelná/neúčinná.	76	100

Tabulka 9.7: Metodika – stupně zranitelnosti.

9.5 Ohodnocení rizik

Pro hodnocení rizik je definována logaritmická stupnice, která hodnotí míru rizika a je určena vztahem $riziko = dopad * hrozba * zranitelnost$. Součástí stupnice jsou podmínky pro zacházení s riziky a přípustné úrovně akceptovatelných a zbytkových rizik – Tabulka 9.8.

Stupeň	**Riziko – popis**	Min. [-]	Max. [-]
Nízký	Riziko je tolerováno a považováno za zbytkové.	0	10
Střední	Riziko je monitorováno a, s ohledem na účelnost, eliminováno méně náročnými bezpečnostními opatřeními. V případě vyšší náročnosti řešení je přípustné riziko akceptovat.	11	30
Vysoký	Riziko by mělo být systematicky odstraňováno a jeho dlouhodobá existence není přípustná.	31	300
Kritický	Výskyt rizika není přípustný a vždy musí být neprodleně zahájeny kroky k jeho odstranění.	301	1000

Tabulka 9.8: Metodika – stupně rizika.

Výpočet stupně rizika je proveden v registru rizik. Bezpečnostní manažer doplní komentář o způsobu zvládání rizika.

Bezpečnostní manažer u každého rizika stanoví ideálně dosažitelnou hodnotu, které je možné dosáhnout při ideální implementaci všech relevantních opatření definovaných níže. Při odhadu dosažitelné hodnoty bezpečnostní manažer přihlíží k typu rizika a k reálným možnostem jeho eliminace. K odhadnuté hodnotě připojuje bezpečnostní manažer podrobný komentář s odůvodněním výběru.

9.6 Identifikace a hodnocení variant pro zvládání rizik

Aby byla snížena odhadnutá rizika na přijatelnou úroveň, musí být identifikována a vybrána vhodná a oprávněná bezpečnostní opatření. Aby bylo možné provést správný výběr, je nutné přihlédnout k existujícím a plánovaným bezpečnostním opatřením, k bezpečnostní

architektuře IT a k omezením různého druhu. Existují čtyři základní možnosti zvládání rizika:

1. Aplikování vhodných kontrol (z katalogu opatření ISO/IEC 27002:2005, ISO/IEC 20000-1:2005 apod.).
2. Vědomé a objektivní akceptování rizik za předpokladu, že naplňují kritéria pro akceptaci rizik.
3. Vyhnutí se rizikům.
4. Přenesení rizik spojených s činností organizace na třetí strany, např. na pojišťovny, dodavatele.

V případě rozhodnutí o implementaci ochranných opatření bezpečností manažer stanovuje relevance mezi opatřeními a riziky – Tabulka 9.9:

Stupeň	Relevance opatření – popis
0	Opatření není relevantní k dané zranitelnosti, nebude aplikováno.
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.

Tabulka 9.9: Metodika – relevance opatření katalogu opatření.

9.7 Výběr optimální kombinace opatření

Bezpečnostní manažer pro každé riziko stanovuje z grafu optimální kombinaci opatření, která budou použita pro zvládání rizika. Přihlíží k dalším aspektům, jako jsou náklady a celkový přístup organizace k bezpečnosti. Závěry bezpečnostní manažer prezentuje vedení společnosti při jednáních bezpečnostního výboru. Závěry musí odsouhlasit bezpečnostní výbor organizace.

Zároveň bezpečnostní manažer jedenkrát měsíčně přehodnocuje vyspělosti jednotlivých opatření, sleduje aktuální hodnoty rizik a v případě nutné reakce reflektuje svá pozorování v registru rizik a informuje bezpečnostní výbor.

9.8 Prohlášení o aplikovatelnosti

Cíle opatření a jednotlivé opatření definovaná v katalogu normy ISO/IEC 27002:2005, které jsou vybrané pro nasazení v rámci řízení informační bezpečnosti se automaticky promítnou do prohlášení o aplikovatelnosti. V případě, že v katalogu uvedené bezpečnostní opatření není pro daný systém řízení informační bezpečnosti vybráno, musí být uvedeny důvody tohoto rozhodnutí. Stav opatření označuje, jaký je stav aplikace vybrané kontroly do praxe.

V rámci tvorby prohlášení o aplikovatelnosti je potřeba upřesnit, v kterém dokumentu řízení organizace a ve které jeho části je daná bezpečnostní kontrola zdokumentována.

Kapitola 10

Případové studie

Tato kapitola demonstruje přínosy vyvinuté metodiky na některých reálných případech z praxe, se kterými se autor setkal. Vzhledem ale k tomu, že se jedná o vysoce citlivá data zákazníků, nikdy nebude konkrétní zákazník přímo pojmenován a uvedená data budou mírně modifikována s cílem univerzálnosti pro většinu organizací (jedná se tedy o rizika, se kterými se pravděpodobně setká každá organizace). Přehled případových studií začíná od nejzákladnější varianty a to je řízení rizik uvnitř jednoho subjektu, příklad bude uveden na řízení rizik v informační bezpečnosti. Je to z toho důvodu, že i přes ambice prosadit tuto metodiku do multidoménového prostředí (prostředí mezi více subjekty než jedním), mohou být výhody prezentovaného návrhu úspěšně použity i v rámci jedné organizace. Závěrem úvodu ještě poznamenejme, že i na vnitřní prostředí jedné organizace lze pohlížet jako na multidoménové prostředí – spolupráce více organizačních celků uvnitř organizace.

Oblastí případových studií jsou následující:

- Řízení rizik uvnitř jednoho subjektu, informační bezpečnost.
- Řízení rizik bezpečnosti služby IT.

10.1 Řízení rizik uvnitř jednoho subjektu, informační bezpečnost

Tato sekce obsahuje případovou studii z řízení rizik v informační bezpečnosti, kde jsou aplikovány algoritmy uvedené v této disertační práci. Je nutné zavést určitá zjednodušení, aby studie svým rozsahem vhodně odpovídala. Tato zjednodušení se týkají těchto oblastí:

1. Není uvedena analýza aktiv a jejich ohodnocení, tyto informace vstupují do odhadu dopadu rizika, pro zjednodušení bude dopad jednoduše uveden bez náležitostí, které by v praxi byly nutné; pro účely demonstrace algoritmů však toto zjednodušení není nijak omezující.
2. Algoritmy budou demonstrovány na třech rizicích, i když je zřejmé, že v praxi by se jistě jednalo o více rizik. Ani toto omezení není zásadní, naopak je vhodné zmínit, že systémy řízení rizik by měly obsahovat určitý "rozumný" počet rizik, která jsou řízena. Důvodem je reálná nemožnost řídit obrovský objem změn – v úvodu práce bylo uvedeno, že jedním z přínosů rizikové analýzy je jednoduše stanovení priorit v řízení, podle zkušeností autora práce je rozumný počet cca 30 řízených rizik. V tomto

počtu se ještě neztrácí priority a úsilí je směřováno do míst, která musejí být aktuálně řešena.

Je třeba také zdůraznit následující: pokud je cílem certifikovat výsledný ISMS (Information Security Management System) dle ISO/IEC 27001:2005, nelze se v žádném případě libovolně vyhýbat implementaci vhodných kontrol po eliminaci rizik. Neaplikování kontroly musí být dobře zváženo a odůvodněno. A to jak pro účely auditu, tak i z praktického pohledu. I tak jsou ale algoritmy publikované v této disertační práci dobře použitelné, neboť pokud na základě výpočtu není určité opatření vybráno pro zvládání daného rizika (případně dané sady rizik), může tak být proto, že má již dostatečnou vyspělost a jeho malé zlepšení by již nepředstavovalo významný posun organizace v informační bezpečnosti. Jinými slovy, priority leží jinde. Samozřejmě je velmi užitečné zde prezentované algoritmy použit pro monitoring a modelování snižování (zvyšování, pokud se díky změnám v organizaci snižuje vyspělost daných opatření) hodnoty rizik.

10.1.1 Rizikové scénáře

Uvažujme rizikové scénáře uvedené v tabulkách 10.1, 10.2 a 10.3:

Popis rizika:	Riziko ohrožení citlivých informací – nejsou stanovena pravidla a opatření pro správu a používání služeb sítě. Správa sítě je plně závislá na jednotlivých garantech (správcích), včetně možných zásahů do konfigurace (používání šifrování, nastavení LAN). Důsledkem může být například obcházení firewallu při přístupu na Internet, odchytávání nešifrovaných informací v síti (hesla ke směrovačům).
Stupeň dopadu:	350
Popis dopadu:	Nesprávná činnost správců může vést k nekontrolovanému ohrožení informačních aktiv.
Stupeň hrozby:	30%
Popis hrozby:	Výskyt hrozby může nastat – riziko se může projevit omylem správců. Úmyslná aktivita je málo pravděpodobná.
Stupeň zranitelnosti:	35%
Popis zranitelnosti:	Jsou stanovena pravidla, nicméně není možné prosadit vyšší stupeň kontroly správců.
Výsledná hodnota rizika:	36,75

Tabulka 10.1: Studie – informační bezpečnost, popis prvního rizika.

10.1.2 Výběr opatření

Pro zvládání prvního rizika (Riziko ohrožení citlivých informací – nejsou stanovena pravidla a opatření pro správu a používání služeb sítě. Správa sítě je plně závislá na jednotlivých garantech (správcích), včetně možných zásahů do konfigurace (používání šifrování, nastavení LAN). Důsledkem může být například obcházení firewallu při přístupu na Internet,

Popis rizika:	Riziko neoprávněného přístupu k informacím – není zaveden proces pro přidělování přístupových práv. Není zaveden proces pro přidělování přístupových práv, který by definoval veškeré činnosti od požadavku, schválení, zavedení uživatele, nastavení práv, změn, odebrání práv, rušení uživatele a zejména dokumentaci činností, revize práv a nezávislé kontroly. V důsledku absence tohoto procesu může dojít k nežádoucí kumulaci práv nebo jejich chybnému či neoprávněnému nastavení.
Stupeň dopadu:	400
Popis dopadu:	Vyzrazení dat důvěrného charakteru.
Stupeň hrozby:	30%
Popis hrozby:	Výskyt hrozby může nastat – nedefinování pravidel znamená chybné nastavení přístupových práv, resp. neodebrání práv včas osobám, které nejsou nadále oprávněné.
Stupeň zranitelnosti:	20%
Popis zranitelnosti:	Pravidla jsou stanovena přístupovou politikou.
Výsledná hodnota rizika:	24

Tabulka 10.2: Studie – informační bezpečnost, popis druhého rizika.

odchytávání nešifrovaných informací v síti (hesla ke směrovačům).) byla vybrána následující opatření z katalogu ISO/IEC 27002:2005 s uvedeným popisem[1] a relevancemi:

1. 9.2.2 – IT zařízení by mělo být ochráněno před selháním napájení i před dalšími výpadky způsobenými selháním podpůrných služeb a zařízení. RELEVANCE = 0,25.
2. 10.1.1 – Provozní postupy a procedury by měly být zdokumentovány a udržovány platné a měly by být dostupné všem uživatelům podle potřeby. RELEVANCE = 0,5.
3. 10.1.2 – Jakékoli změny IT systémů a prostředků pro zpracování informací by měly být řízeny. RELEVANCE = 0,75.
4. 10.1.3 – Snížení příležitostí k neoprávněné modifikaci nebo zneužití aktiv by mělo být zajištěno oddělením jednotlivých povinností a odpovědností. RELEVANCE = 1.
5. 10.5.1 – Záložní kopie informačních aktiv a programových aktiv organizace by měly být pravidelně pořizovány a pravidelně testovány. RELEVANCE = 0,25.
6. 10.6.1 – Pro ochranu před hrozbami a pro zaručení bezpečnosti systémů, aplikací využívajících sítí a informací při přenosu, by počítačové sítě měly být vhodně spravovány a kontrolovány. RELEVANCE = 1.
7. 10.6.2 – Měly by být nalezeny a do dohod o poskytování síťových služeb zahrnuty požadavky na bezpečnost, úroveň poskytovaných služeb a požadavky na správu síťových služeb, a to v případech interního i externího zajištění (outsourcingu). RELEVANCE = 1.

[1] Popis zde i u dalších rizik přesně vychází z ISO/IEC 27002:2005, je však upraven, aby nedošlo k porušení autorských práv Mezinárodní organizace pro normalizaci ISO. Větná forma typická pro popis doporučení je zachována.

Popis rizika:	Riziko nedostatečné ochrany informací – nejsou definována bezpečnostní pravidla pro manipulaci s dokumenty (elektronickými i listinnými) a médii. Nejsou definována opatření k bezpečné manipulaci a ochraně elektronických médií. Nejsou definována systematická opatření na ochranu informací při výměně se zákazníky a dodavateli (např. požadavek zahrnout konkrétní opatření do smluv). Důsledkem může být narušení důvěrnosti nebo integrity informací (ztráta médií, popření původu zprávy, apod.).
Stupeň dopadu:	350
Popis dopadu:	Narušení důvěrnosti nebo integrity informací.
Stupeň hrozby:	35%
Popis hrozby:	Výskyt hrozby může nastat – nedefinování pravidel může znamenat mylné použití nedostatečně označených aktiv.
Stupeň zranitelnosti:	20%
Popis zranitelnosti:	Pravidla jsou stanovena směrnicí pro řízení informačních aktiv.
Výsledná hodnota rizika:	24,5

Tabulka 10.3: Studie – informační bezpečnost, popis třetího rizika.

8. 10.8.5 – Na ochranu informací v podnikových informačních systémech by měla být vytvořena a zavedena politika a odpovídající směrnice. RELEVANCE = 0,5.

9. 10.10.1 – Záznamy obsahující chybová hlášení a další významné bezpečnostně události by měly být pořizovány a uchovávány po předem definované období tak, aby se daly použít pro budoucí vyšetřování a pro účely řízení přístupu. RELEVANCE = 1.

10. 10.10.2 – Měla by být definována pravidla pro monitoring prostředků pro zpracovávání informací, výsledky těchto monitorování by měly být pravidelně přezkoumávány. RELEVANCE = 1.

11. 10.10.3 – Prostředky pro zaznamenávání informací včetně vytvořených záznamů by měly být vhodným způsobem chráněny proti neoprávněné modifikaci a přístupu. RELEVANCE = 1.

12. 10.10.4 – Aktivity administrátora a systémového operátora by měly být zaznamenávány. RELEVANCE = 1.

13. 10.10.5 – Chyby by měly být zaznamenány a analyzovány a přijata příslušná opatření. RELEVANCE = 0,75.

14. 10.10.6 – Systémový čas všech důležitých systémů pro zpracování informací by měl být v rámci organizace nebo bezpečnostní domény synchronizován s předem definovaným zdrojem přesného času. RELEVANCE = 0,75.

15. 11.4.4 – Přístup k diagnostickým a konfiguračním portům by měl být řízen. RELEVANCE = 0,75.

16. 11.4.6 – U sítí, včetně těch, které přesahují hranice organizace, by měly být omezeny možnosti pro přístup uživatelů. Omezení by měla být v souladu s politikou a příslušnými požadavky. RELEVANCE = 0,75

17. 11.4.7 – Řízení směrování sítě by mělo být zavedeno pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace. RELEVANCE = 0,5.

18. 12.4.1 – Instalace programového vybavení na provozních systémech by měly být kontrolovány podle zavedených postupů. RELEVANCE = 0,5.

19. 12.4.2 – Testovací data by měla být pečlivě vybrána, chráněna a kontrolována. RELEVANCE = 0,5.

20. 12.6.1 – Přístup ke zdrojovým kódům by měl být omezen. RELEVANCE = 0,5.

Pro zvládání druhého rizika (Riziko neoprávněného přístupu k informacím – není zaveden proces pro přidělování přístupových práv. Není zaveden proces pro přidělování přístupových práv, který by definoval veškeré činnosti od požadavku, schválení, zavedení uživatele, nastavení práv, změn, odebrání práv, rušení uživatele a zejména dokumentaci činností, revize práv a nezávislé kontroly. V důsledku absence tohoto procesu může dojít k nežádoucí kumulaci práv nebo jejich chybnému či neoprávněnému nastavení.) byla vybrána následující opatření z katalogu ISO/IEC 27002:2005 s uvedenými relevancemi:

1. 8.1.1 – Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti informací by měly být přesně definovány a dokumentovány v souladu s bezpečnostní politikou. RELEVANCE = 1.

2. 8.1.2 – Všichni uchazeči o zaměstnání, smluvní a třetí strany by měly být prověřeni podle daných zákonů, předpisů a v souladu s etikou. Prověření by měla být provedena na základě požadavků stanovených organizací, dále s ohledem na klasifikaci informačních aktiv, ke kterým by měli získat přístup, ale také z hlediska jejich spolehlivosti a možných rizik. RELEVANCE = 1.

3. 8.1.3 – Smlouvy uzavřené se zaměstnanci, smluvními a třetími stranami by měly obsahovat ustanovení o jejich odpovědnostech za informační bezpečnost. RELEVANCE = 1.

4. 8.2.1 – Vedoucí zaměstnanci by měli po uživatelích, smluvních a třetích stranách požadovat dodržování bezpečnosti v souladu se zavedenými politikami a postupy. RELEVANCE = 1.

5. 8.2.2 – Všichni zaměstnanci organizace i pracovníci smluvních a třetích stran, by měli s ohledem na svoje zařazení absolvovat odpovídající a pravidelně se opakující školení v oblasti bezpečnosti informací, bezpečnostní politiky a směrnic organizace. RELEVANCE = 1.

6. 8.2.3 – Mělo by existovat formalizované disciplinární řízení vůči zaměstnancům, v případě narušení bezpečnosti. RELEVANCE = 1.

7. 8.3.1 – Měly by být definovány a přiděleny odpovědnosti pro případ ukončení nebo změny pracovního vztahu. RELEVANCE = 1.

8. 8.3.2 – Při ukončení pracovního vztahu, smluvního vztahu nebo dohody by měli zaměstnanci, pracovníci smluvních a třetích stran, kterých se to týká, odevzdat veškeré jim zapůjčené prostředky, které jsou majetkem organizace. RELEVANCE = 1.

9. 8.3.3 – Při ukončení pracovního vztahu, smluvního vztahu nebo dohody by měla být uživatelům, smluvním a třetím stranám odejmuta přístupová práva k informacím a prostředkům pro zpracování informací. RELEVANCE = 1.

10. 11.2.1 – Měl by být definován postup pro formální registraci uživatele včetně zrušení, který zajistí autorizovaný přístup ke všem informačním systémům, službám a prostředkům pro zpracování informací. RELEVANCE = 1.

11. 11.2.2 – Přidělování a používání privilegií by mělo být přesně definováno, omezeno a řízeno. RELEVANCE = 1.

12. 11.2.3 – Používání (přidělování, odebírání) hesel by mělo být řízeno formálním procesem. RELEVANCE = 1.

13. 11.2.4 – Vedení organizace by mělo v pravidelných intervalech formálně přezkoumávat přístupová práva uživatelů. RELEVANCE = 1.

14. 11.3.1 – Při používání hesel by mělo být po pracovnících požadováno, aby dodržovali definované bezpečnostní postupy. RELEVANCE = 0,5.

15. 11.4.1 – Uživatelé by měli mít přístup pouze a jenom k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni a jejich přístup byl formálně schválen. RELEVANCE = 0,75.

16. 11.5.1 – Přístupy k operačním systémům by měl být řízen postupy bezpečného přihlášení. RELEVANCE = 0,5.

17. 11.5.2 – Všichni uživatelé by měli mít přiřazen výhradní osobní jedinečný identifikátor (uživatelské ID), měl by být také zvolen vhodný způsob autentizace pro ověření jejich identity. RELEVANCE = 0,75.

18. 11.6.1 – Uživatelé systémů, včetně pracovníků podpory, by měli mít přístup k informacím a funkcím aplikačních systémů omezen v souladu s definovanou politikou řízení přístupu. RELEVANCE = 0,75.

19. 11.7.1 – Měla by být ustanovena formální pravidla a přijata opatření na ochranu proti rizikům používání mobilních výpočetních a komunikačních zařízení. RELEVANCE = 0,5.

20. 11.7.2 – Organizace by měla definovat a do praxe zavést zásady, plány a postupy pro práci na dálku. RELEVANCE = 0,75.

21. 15.1.5 – Mělo by být zakázáno používat prostředky pro zpracování informací jinak než autorizovaným způsobem. RELEVANCE = 0,25.

Pro zvládání třetího rizika (Riziko nedostatečné ochrany informací – nejsou definována bezpečnostní pravidla pro manipulaci s dokumenty (elektronickými i listinnými) a médii. Nejsou definována opatření k bezpečné manipulaci a ochraně elektronických médií. Nejsou definována systematická opatření na ochranu informací při výměně se zákazníky a

dodavateli (např. požadavek zahrnout konkrétní opatření do smluv). Důsledkem může být narušení důvěrnosti nebo integrity informací (ztráta médií, popření původu zprávy, apod.).) byla vybrána následující opatření z katalogu ISO/IEC 27002:2005 s uvedenými relevancemi:

1. 6.1.5 – Měly by být definovány a pravidelně přezkoumávány dohody obsahující požadavky na ochranu důvěrnosti anebo dostupnosti informačních aktiv, reflektující potřeby organizace na ochranu informací. RELEVANCE = 0,5.
2. 6.2.1 – Před povolením přístupu externím subjektům k informacím organizace a prostředkům pro zpracování informací, by měla být identifikována rizika a implementována vhodná opatření na jejich redukci na akceptovatelnou úroveň. RELEVANCE = 1.
3. 6.2.2 – Před umožněním přístupu klientům k informacím nebo aktivům organizace, by měly být identifikovány všechny požadavky na informační bezpečnost bezpečnost. RELEVANCE = 0,75.
4. 6.2.3 – Dohody s třetími stranami, zahrnující přístup, zpracování, šíření anebo správu informací organizace anebo správu prostředků pro zpracování informací (případně dodávku produktů nebo služeb k zařízení pro zpracování informačních aktiv) by měly pokrývat veškeré relevantní bezpečnostní požadavky organizace. RELEVANCE = 0,75.
5. 7.1.3 – Měla by být definována, dokumentována a do praxe zavedena pravidla pro přípustné použití informačních aktiv souvisejících s prostředky pro zpracování informací. RELEVANCE = 1.
6. 7.2.1 – Informační aktiva by měla být korektně klasifikována a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost. RELEVANCE = 1.
7. 7.2.2 – Pro označování informací a zacházení s nimi by měly být definovány a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací. RELEVANCE = 1.
8. 10.9.3 – Informace uložené na veřejně přístupných systémech by měly být chráněny proti neautorizované změně. RELEVANCE = 0,5.

10.1.3 Bezpečnostní projekty, analýza vyspělosti opatření

Tato podsekce popisuje v souhrnu veškerá vybraná opatření, pokud se opatření podílí na zvládání více rizik, potom se relevance sčítají – odtud název bezpečnostní projekty. Tento seznam, pro jednotlivá rizika, vstupuje do výpočtu a seřazení kombinací funkce agregované zvladatelnosti zranitelnosti. Odhady vyspělostí opatření v moment analýzy jsou v této práci samozřejmě fikce, v praxi musejí odrážet reálný stav organizace. Následující výčet obsahuje v pořadí tyto informace:

1. Číslo opatření z katalogu ISO/IEC 27002:2005.
2. Příslušnost k riziku (značeno R1, R2, R3).
3. Relevanci (nedosahuje hodnoty nula, jinak by nebylo vybráno).
4. Vyspělost (nedosahuje hodnoty 1, jinak by nebylo vybráno).

Výčet:

1. 6.1.5; R3; relevance = 0,5; vyspělost = 0,5.
2. 6.2.1; R3; relevance = 1; vyspělost = 0,5.
3. 6.2.2; R3; relevance = 0,75; vyspělost = 0,25.
4. 6.2.3; R3; relevance = 0,75; vyspělost = 0,5.
5. 7.1.3; R3; relevance = 1; vyspělost = 0,25.
6. 7.2.1; R3; relevance = 1; vyspělost = 0,75.
7. 7.2.2; R3; relevance = 1; vyspělost = 0,5.
8. 8.1.1; R2; relevance = 1; vyspělost = 0,75.
9. 8.1.2; R2; relevance = 1; vyspělost = 0,75.
10. 8.1.3; R2; relevance = 1; vyspělost = 0,75.
11. 8.2.1; R2; relevance = 1; vyspělost = 0,5.
12. 8.2.2; R2; relevance = 1; vyspělost = 0,75.
13. 8.2.3; R2; relevance = 1; vyspělost = 0,75.
14. 8.3.1; R2; relevance = 1; vyspělost = 0,75.
15. 8.3.2; R2; relevance = 1; vyspělost = 0,75.
16. 8.3.3; R2; relevance = 1; vyspělost = 0,5.
17. 9.2.2; R1; relevance = 0,25; vyspělost = 0,5.
18. 10.1.1; R1; relevance = 0,5; vyspělost = 0,25.
19. 10.1.2; R1; relevance = 0,75; vyspělost = 0,5.
20. 10.1.3; R1; relevance = 1; vyspělost = 0,5.
21. 10.5.1; R1; relevance = 0,25; vyspělost = 0,75.
22. 10.6.1; R1; relevance = 1; vyspělost = 0,5.
23. 10.6.2; R1; relevance = 1; vyspělost = 0,25.
24. 10.8.5; R1; relevance = 0,5; vyspělost = 0,5.
25. 10.10.1; R1; relevance = 1; vyspělost = 0,5.
26. 10.10.2; R1; relevance = 1; vyspělost = 0,25.
27. 10.10.3; R1; relevance = 1; vyspělost = 0,25.
28. 10.10.4; R1; relevance = 1; vyspělost = 0,75.

29. 10.10.5; R1; relevance = 0,75; vyspělost = 0,5.
30. 10.10.6; R1; relevance = 0,75; vyspělost = 0,5.
31. 11.2.1; R2; relevance = 1; vyspělost = 0,75.
32. 11.2.2; R2; relevance = 1; vyspělost = 0,75.
33. 11.2.3; R2; relevance = 1; vyspělost = 0,75.
34. 11.2.4; R2; relevance = 1; vyspělost = 0,75.
35. 11.3.1; R2; relevance = 0,5; vyspělost = 0,75.
36. 11.4.1; R2; relevance = 0,75; vyspělost = 0,75.
37. 11.4.4; R1; relevance = 0,75; vyspělost = 0,5.
38. 11.4.6; R1; relevance = 0,75; vyspělost = 0,5.
39. 11.4.7; R1; relevance = 0,5; vyspělost = 0,25.
40. 11.5.1; R2; relevance = 0,5; vyspělost = 0,75.
41. 11.5.2; R2; relevance = 0,75; vyspělost = 0,75.
42. 11.6.1; R2; relevance = 0,75; vyspělost = 0,5.
43. 11.7.1; R2; relevance = 0,5; vyspělost = 0,75.
44. 11.7.2; R2; relevance = 0,75; vyspělost = 0,75.
45. 12.4.1; R1; relevance = 0,5; vyspělost = 0,5.
46. 12.4.2; R1; relevance = 0,5; vyspělost = 0,75.
47. 12.6.1; R1; relevance = 0,5; vyspělost = 0,75.
48. 15.1.5; R2; relevance = 0,25; vyspělost = 0,5.

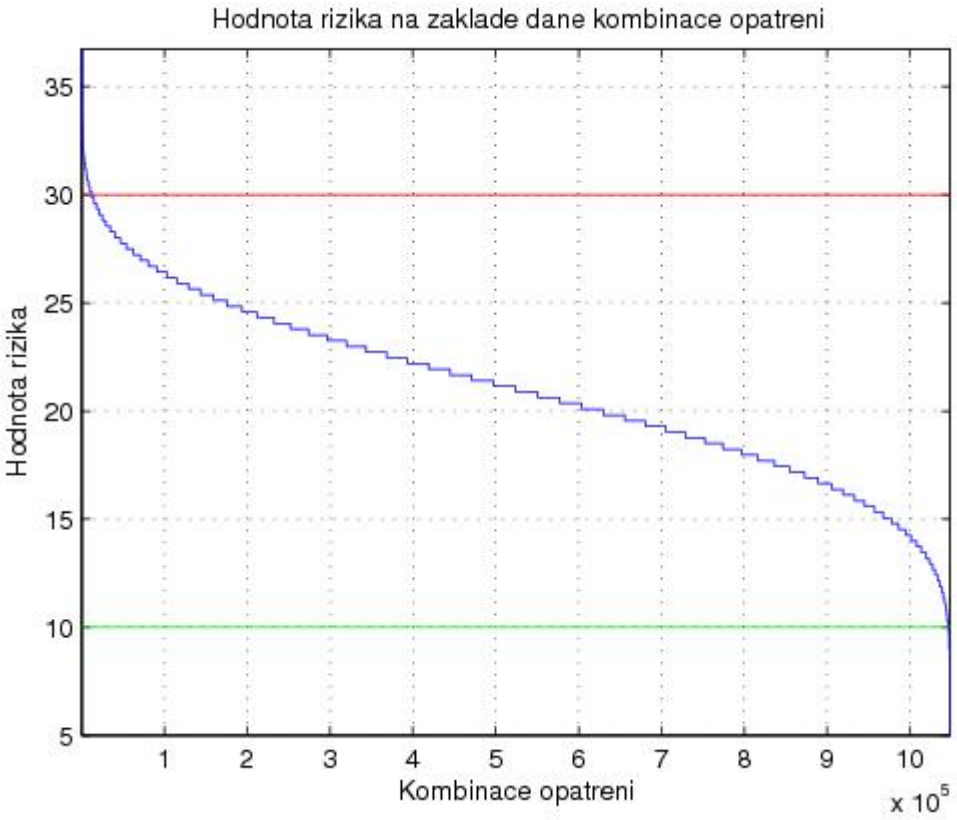
Poznámka: ohodnocení vyspělostí je platné v dobu provedení rizikové analýzy. Jelikož řízení rizik není projekt, ale nikdy nekončící proces, vyspělost je s postupem implementace opatření měněna tak, aby odrážela reálný stav organizace. Pokud se, a je to obvyklé, v průběhu procesu řízení rizik objeví nové riziko, které není doposud řízeno, vyspělosti relevantních opatření opět odpovídají danému stavu – je tedy logické, že pokud by určité riziko existovalo už v tuto chvíli, ale bylo odhaleno později s tím, že již nějaká opatření byla implementována, jeho ohodnocení bude nižší (skrze nižší hodnocení zranitelnosti).

Optimalizované zvládání prvního rizika

Prvním krokem v samotné optimalizaci je odhad ideálně dosažitelné hodnoty, které riziko nabude, pokud budou implementována všechna vybraná opatření na 100%. Zopakujme, že se jedná o toto riziko: riziko ohrožení citlivých informací – nejsou stanovena pravidla a opatření pro správu a používání služeb sítě. Správa sítě je plně závislá na jednotlivých garantech (správcích), včetně možných zásahů do konfigurace (používání šifrování, nastavení LAN). Důsledkem může být například obcházení firewallu při přístupu na Internet, odchytávání nešifrovaných informací v síti (hesla ke směrovačům).

Je zřejmé, že se jedná o netechnologické riziko, jehož naplnění značně záleží ne lidském faktoru, na loajalitě pracovníků, dále na jejich osobní motivaci k provedení útoku apod. Z toho plyne, že v praxi není možné dosáhnout velmi nízké hodnoty rizika (hodnoty rizika 0 až 10 jsou akceptovatelné, hodnoty 11 až 30 akceptovatelné, pokud by eliminace rizika znamenala přílišné náklady apod. – viz vzorová metodika). Stanovme, že vzhledem k charakteru rizika bude ideálně dosažitelná hodnota rovna pěti.

Nyní se podívejme na výsledný vývoj hodnoty rizika (jeho numerické vyjádření na základě dopadu, hrozby a zranitelnosti ukazuje Tabulka 10.1) na základě setříděných hodnot funkce agregované zvladatelnosti zranitelnosti vybraných opatření – viz Obrázek 10.1.

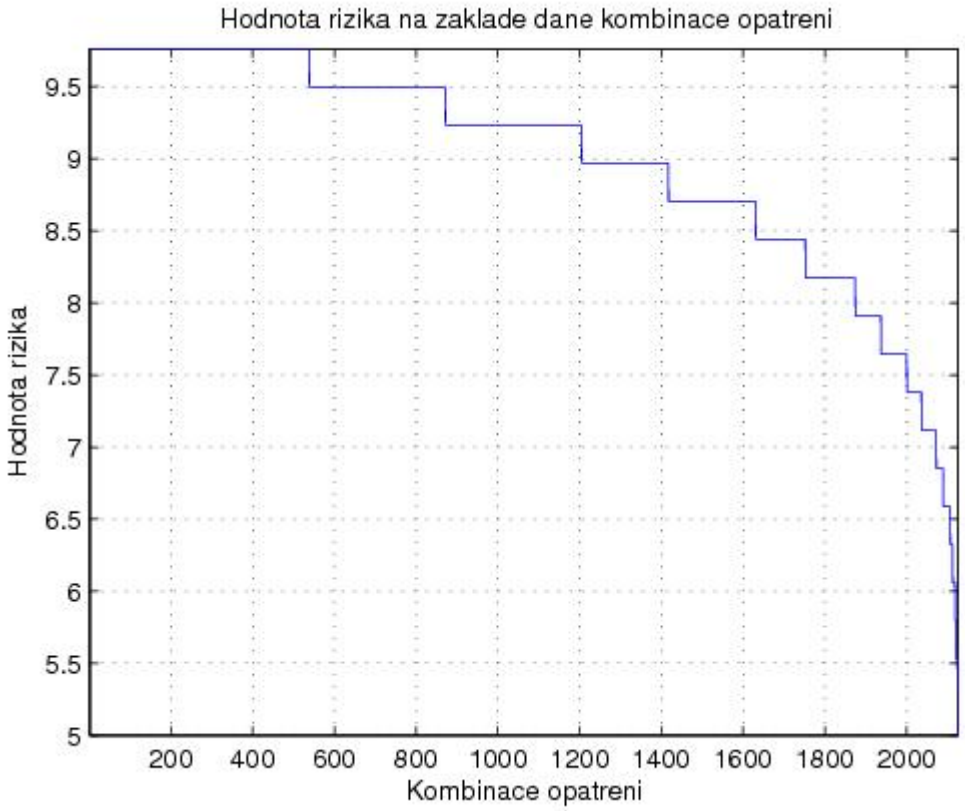


Obrázek 10.1: Studie informační bezpečnosti – vývoj hodnoty prvního rizika.

Diskuze k vývoji hodnot rizika pro jednotlivé kombinace opatření je následující: výsledná hodnota rizika na obou koncích osy X se významně mění z toho důvodu, že se radikálněji liší počet "zapnutých" respektive "vypnutých" opatření v algoritmu (opatření, která jsou implementována či nikoli); vývoj hodnot rizika uprostřed osy X není tak odlišný, jelikož

počet implementovaných opatření je obdobný.

Nás samozřejmě zajímají nižší hodnoty výsledného rizika, dle metodiky, pokud možno, hodnoty nižší než 10, které zobrazuje Obrázek 10.2.



Obrázek 10.2: Studie informační bezpečnosti – vývoj hodnoty prvního rizika, akceptovatelné riziko.

Nyní je na rozhodnutí a úvaze analytika, jakou přesně cílovou hodnotu rizika zvolí, respektive jak přesně bude vypadat kombinace implementovaných opatření. Vzhledem k tomu, že se do značné míry jedná o netechnologické riziko, jeví se jako rozumné cílit na implementaci všech opatření. Realita je totiž taková, že opatření týkající se lidských zdrojů nebude nikdy funkční naprosto dokonale. Doporučení je tedy implementovat všechna opatření s cílovou hodnotou rizika 5 a na základě zde uvedených algoritmů monitorovat aktuální hodnotu rizika, která v praxi rovna pěti nikdy nebude.

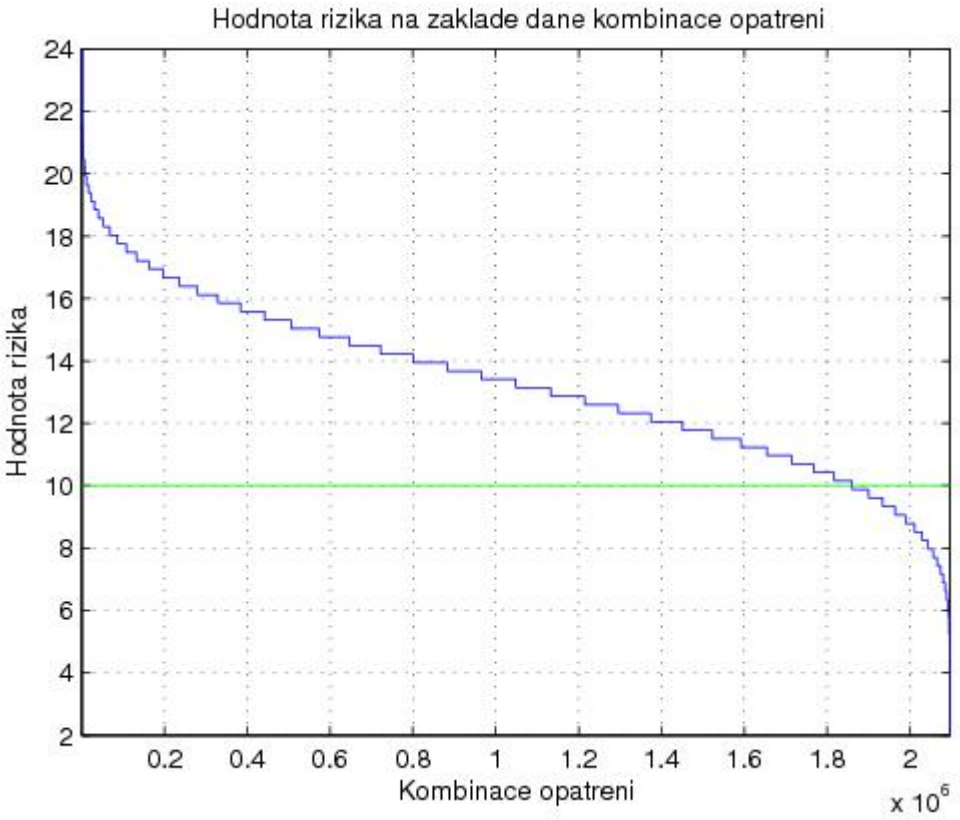
Optimalizované zvládání druhého rizika

Jedná se o riziko: riziko neoprávněného přístupu k informacím – není zaveden proces pro přidělování přístupových práv. Není zaveden proces pro přidělování přístupových práv, který by definoval veškeré činnosti od požadavku, schválení, zavedení uživatele, nastavení práv, změn, odebrání práv, rušení uživatele a zejména dokumentaci činností, revize práv a nezávislé kontroly. V důsledku absence tohoto procesu může dojít k nežádoucí kumulaci práv nebo jejich chybnému či neoprávněnému nastavení.

Detailní popis včetně ohodnocení viz Tabulka 10.2.

Cílová ideální hodnota rizika: vzhledem k tomu, že pro eliminaci rizika je nutné "pouze" zavést příslušné procesy a poté vyžadovat a kontrolovat jejich důsledné plnění, lze dosáhnout relativně velmi nízké hodnoty. Samozřejmě ne rovné nule, to by odpovídalo vyhnutí se riziku. Stanovme cílovou ideální hodnotu rizika rovnu dvěma. Blíže nule nepůjdeme, neboť i kontrola dodržování procesů může mít své nedostatky a v praxi nebude mít valného smyslu zavadění kontroly kontroly, případně dalších kontrol.

Vývoj hodnot rizika na základě setříděných kombinací opatření je zobrazen viz Obrázek 10.3.

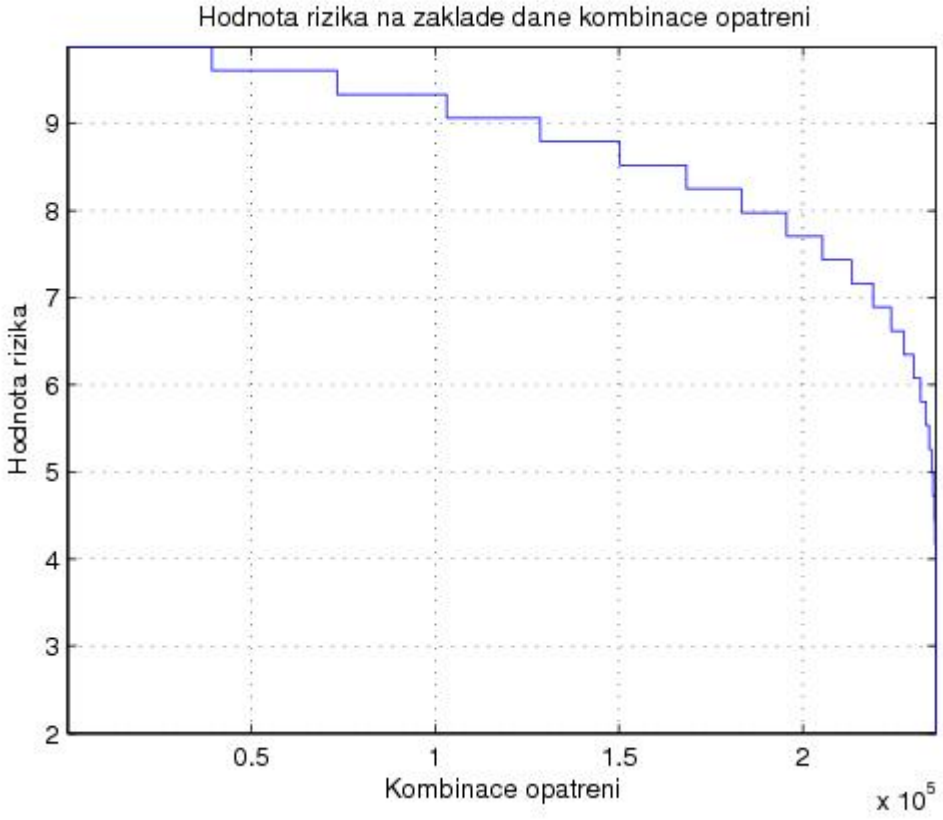


Obrázek 10.3: Studie informační bezpečnosti – vývoj hodnoty druhého rizika.

Hodnoty rizika v akceptovatelném pásmu jsou pak zobrazeny viz Obrázek 10.4.

Pro optimalizaci ve výběru opatření je nutné sledovat jednotlivé kombinace opatření pro stanovené hodnoty reálného cílového rizika. Vzhledem k charakteru rizika, kdy při jeho naplnění může například i propuštěný zaměstnanec mít stále VPN přístup do společnosti, budeme sledovat kombinace opatření kolem cílové reálné hodnoty rizika rovné třem.

Pro hodnotu rizika rovnu 3,0864 jsou možné kombinace opatření následující:
01111111111101111111
01111111111111011111
01111111111111111011
01111111111111111110
10111111111101111111
10111111111111011111
10111111111111111011



Obrázek 10.4: Studie informační bezpečnosti – vývoj hodnoty druhého rizika, akceptovatelné riziko.

10111111111111111110
11011111111101111111
11011111111111011111
11011111111111111011
11011111111111111110
11110111111101111111
11110111111111011111
11110111111111111011
11110111111111111110
11111011111101111111
11111011111111011111
11111011111111111011
11111011111111111110
11111101111101111111
11111101111111011111
11111101111111111011
11111101111111111110
11111110111101111111
11111110111111011111
11111110111111111011

11111110111111111110
11111111011101111111
11111111011111011111
11111111011111111011
11111111011111111110
11111111101101111111
11111111101111011111
11111111101111111011
11111111101111111110
11111111110101111111
11111111110111011111
11111111110111111011
11111111110111111110
11111111111001111111
11111111111011011111
11111111111011111011
11111111111011111110
11111111111101011011
11111111111101011110
11111111111101111010
11111111111110101111
11111111111110111101
11111111111111011010
11111111111111101101
11111111111111110111

Je zřejmé, že v každém řádku výše jednotlivé nuly/jedničky značí ne/implementaci daného opatření ve stejném pořadí, jak byly vybrány pro zvládání tohoto rizika, tedy 8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2, 8.2.3, 8.3.1, 8.3.2, 8.3.3, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.3.1, 11.4.1, 11.5.1, 11.5.2, 11.6.1, 11.7.1, 11.7.2 a 15.1.5 z ISO/IEC 27002:2005.

Pro zvolení daného řádku je třeba sledovat kontext organizace, tedy to, co bude v dané organizaci činit nejmenší potíže při implementaci. Důležitým ukazatelem mohou být také celkové náklady [44] na implementaci dané kombinace opatření. Pokud bude analytik v konkrétní organizaci sledovat tento ukazatel, tedy ukazatel nákladů, může ze všech možných kombinací opatření, jejichž implementace generuje danou hodnotu rizika, vybrat tu, která je pro organizaci nejlevnější.

Optimalizované zvládání třetího rizika

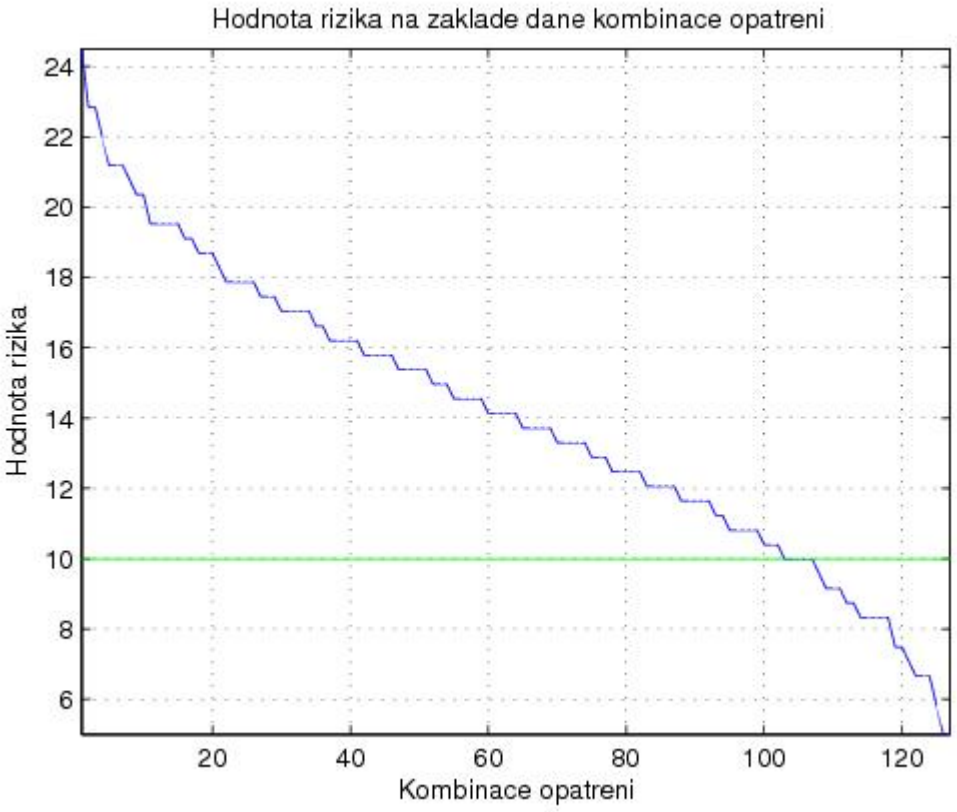
Riziko: riziko nedostatečné ochrany informací – nejsou definována bezpečnostní pravidla pro manipulaci s dokumenty (elektronickými i listinnými) a médii. Nejsou definována opatření k bezpečné manipulaci a ochraně elektronických médií. Nejsou definována systematická opatření na ochranu informací při výměně se zákazníky a dodavateli (např. požadavek zahrnout konkrétní opatření do smluv). Důsledkem může být narušení důvěrnosti nebo integrity informací (ztráta médií, popření původu zprávy, apod.).

Detailní popis včetně ohodnocení viz Tabulka 10.3.

Cílová ideální hodnota rizika stanovena na hodnotu pět, neboť se jedná i o komunikaci mezi organizací a třetí stranou (zákazníky a dodavateli) a tudíž nebude nikdy možné mít

zcela pod kontrolou technologie a procesy mimo organizaci.

Vývoj hodnot rizika na základě setříděných kombinací opatření je zobrazen viz Obrázek 10.5.

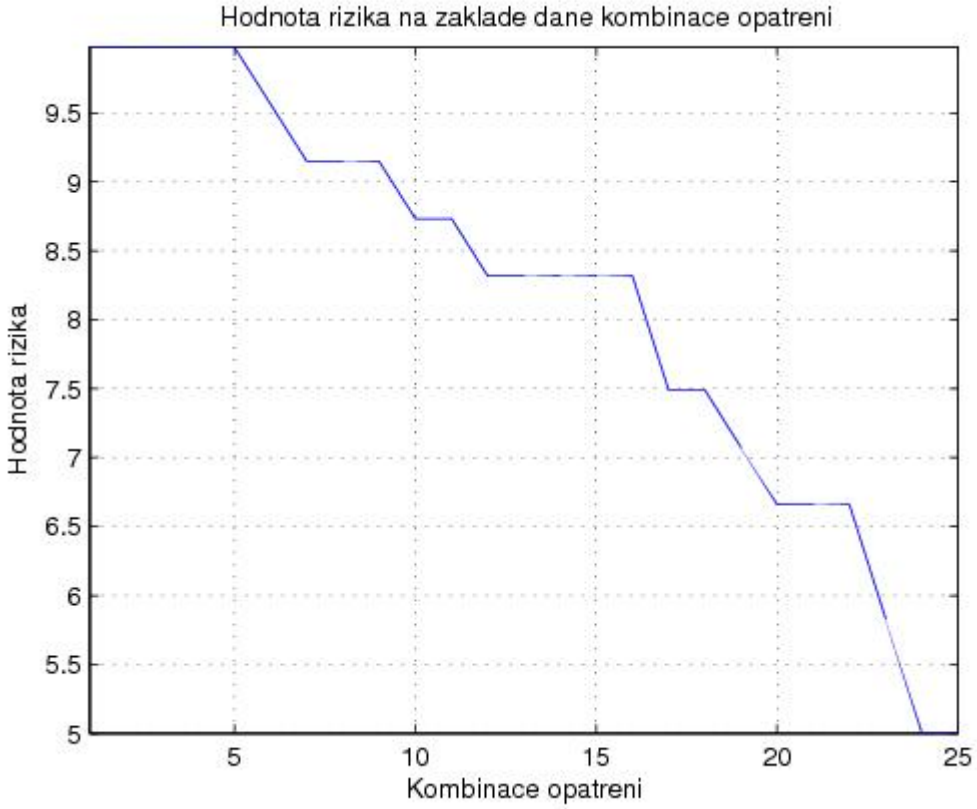


Obrázek 10.5: Studie informační bezpečnosti – vývoj hodnoty třetího rizika.

Hodnoty rizika v akceptovatelném pásmu jsou pak zobrazeny viz Obrázek 10.6.

Vzhledem k charakteru rizika je vhodné implementovat všechna vybraná opatření, pokud by se organizace rozhodla pro akceptaci vyšší úrovně rizika, zde jsou jednotlivé kombinace opatření pro dané hodnoty rizik:

Riziko = 5.8298; kombinace = 1110111
Riziko = 6.6596; kombinace = 0111101
Riziko = 6.6596; kombinace = 1011111
Riziko = 6.6596; kombinace = 1111110
Riziko = 7.0745; kombinace = 1101111
Riziko = 7.4894; kombinace = 0110111
Riziko = 7.4894; kombinace = 1110101
Riziko = 8.3191; kombinace = 0011111
Riziko = 8.3191; kombinace = 0111110
Riziko = 8.3191; kombinace = 1011101
Riziko = 8.3191; kombinace = 1111011
Riziko = 8.3191; kombinace = 1111100
Riziko = 8.7340; kombinace = 0101111
Riziko = 8.7340; kombinace = 1101101



Obrázek 10.6: Studie informační bezpečnosti – vývoj hodnoty třetího rizika, akceptovatelné riziko.

Riziko = 9.1489; kombinace = 0110101
Riziko = 9.1489; kombinace = 1010111
Riziko = 9.1489; kombinace = 1110110
Riziko = 9.5638; kombinace = 1100111
Riziko = 9.9787; kombinace = 0011101
Riziko = 9.9787; kombinace = 0111011
Riziko = 9.9787; kombinace = 0111100
Riziko = 9.9787; kombinace = 1011110
Riziko = 9.9787; kombinace = 1111001

Komentáře k tomuto riziku jsou obdobné jako v předchozím případě.

10.2 Řízení rizik bezpečnosti služby IT

Druhá případová studie je již z řízení informační bezpečnosti služeb IT. Cílem je především demonstrovat, jak je možné při dané hodnotě rizika, při aplikaci zde uvedených algoritmů, optimalizovat implementaci opatření redukujících riziko na obou stranách kontraktu.

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. Byla identifikována následující dvě rizika (Tabulka 10.4 a 10.5), kterým musí poskytovatel i konzument společně čelit.

Popis rizika:	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.
Stupeň dopadu:	450
Popis dopadu:	Pokud nejsou data bezpečně vymazána, může dojít k úniku citlivých informací.
Stupeň hrozby:	30%
Popis hrozby:	Výskyt hrozby může nastat – riziko se může projevit omylem správců. Úmyslná aktivita je málo pravděpodobná.
Stupeň zranitelnosti:	30%
Popis zranitelnosti:	Nižší úroveň informační bezpečnosti na straně konzumenta služby.
Výsledná hodnota rizika:	40,5

Tabulka 10.4: Studie – informační bezpečnost služby IT, popis prvního rizika.

Popis rizika:	Riziko neplnění SLA požadavků – při selhání zařízení hrozí prodlevy v hlášení incidentu a tím ke nedodržení SLA na straně poskytovatele služby, zároveň hrozí zbytečně dlouhý výpadek hardware na straně konzumenta služby.
Stupeň dopadu:	350
Popis dopadu:	Ohrožení plynulého byznysu na straně konzumenta služby.
Stupeň hrozby:	30%
Popis hrozby:	Výskyt hrozby může nastat .
Stupeň zranitelnosti:	35%
Popis zranitelnosti:	Jsou stanovena pravidla, nicméně není možné prosadit vyšší stupeň kontroly.
Výsledná hodnota rizika:	36,75

Tabulka 10.5: Studie – informační bezpečnost služby IT, popis druhého rizika.

10.2.1 Výběr opatření

Pro zvládání prvního rizika (Tabulka 10.4) byla na straně **dodavatele služby IT** vybrána následující opatření ISO/IEC 27002:2005 (včetně relevancí a vyspělostí na straně dodavatele):

1. 6.1.3; Je nutné přesně určit odpovědnosti v oblasti bezpečnosti informací; relevance = 1; vyspělost = 0,75.

2. 7.1.3; Mělo by být definováno a do praxe prosazeno přípustné použití aktiv; relevance = 1; vyspělost = 0,75.
3. 7.2.1; Informace by měly být klasifikovány; relevance = 1; vyspělost = 0,75.
4. 7.2.2; Na základě klasifikace by měla být aktiva označena; relevance = 1; vyspělost = 0,75.
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 = 0,75.
6. 8.2.3; Musí existovat formální disciplinární řízení; relevance = 0,5; vyspělost = 0,5.

Pro zvládání prvního rizika (Tabulka 10.4) byla na straně **konzumenta služby IT** vybrána následující opatření ISO/IEC 27002:2005 (včetně relevancí a vyspělostí na straně konzumenta):

1. 6.1.3; Je nutné přesně určit odpovědnosti v oblasti bezpečnosti informací; relevance = 1; vyspělost = 0,75.
2. 6.1.5; Měly by být dohodnuty a přezkoumávány požadavky na ochranu informací; relevance = 0,75; vyspělost = 0,75.
3. 6.2.1; Měla by být identifikována rizika před tím, než je externímu subjektu povolen přístup k informacím; relevance = 0.25; vyspělost = 0,5.
4. 7.1.1; Měla by být identifikována všechna aktiva a jejich seznam udržován aktuální; relevance = 1; vyspělost = 0.
5. 7.1.2; Každé aktivum by mělo mít určeného vlastníka; relevance = 1; vyspělost = 0,25.
6. 7.2.1; Informace by měly být klasifikovány; relevance = 1; vyspělost = 0,5.
7. 7.2.2; Na základě klasifikace by měla být aktiva označena; relevance = 1; vyspělost = 0,5.
8. 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.
9. 8.2.3; Musí existovat formální disciplinární řízení; relevance = 0,5; vyspělost = 0,25.
10. 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.
11. 10.1.2; Změny by měly být řízeny; relevance = 1; vyspělost = 0,75.

Pro zvládání druhého rizika (Tabulka 10.5) byla na straně **dodavatele služby IT** vybrána následující opatření ISO/IEC 27002:2005 (včetně relevancí a vyspělostí na straně dodavatele):

1. 10.2.2; Třetí strana by měla být pravidelně monitorována a přezkoumávána; relevance = 0,5; vyspělost = 0,75.

2. 10.2.3; Změny služeb poskytovaných třetí stranou by měly být řízeny; relevance = 0,5; vyspělost = 0,75.

3. 13.2.1; Pro zajištění odpovídající systematické reakce by měly být zavedeny příslušné odpovědnosti a postupy; relevance = 1; vyspělost = 0,75.

4. 13.2.2; Z proběhnutých incidentů by měla být přijata příslušná opatření; relevance = 1; vyspělost = 0,75.

Pro zvládání druhého rizika (Tabulka 10.5) byla na straně **konzumenta služby IT** vybrána následující opatření ISO/IEC 27002:2005 (včetně relevancí a vyspělostí na straně konzumenta):

1. 10.2.3; Změny služeb poskytovaných třetí stranou by měly být řízeny; relevance = 0,5; vyspělost = 0,25.

2. 13.1.1; Bezpečnostní události by měly být co nejdříve hlášeny dohodnutými komunikačními kanály; relevance = 1; vyspělost = 0.

3. 13.1.2; Jakékoli bezpečnostní slabiny nebo podezřelé události by měly být hlášeny; relevance = 1; vyspělost = 0.

4. 13.2.1; Pro zajištění odpovídající systematické reakce by měly být zavedeny příslušné odpovědnosti a postupy; relevance = 1; vyspělost = 0.

5. 13.2.2; Z proběhnutých incidentů by měla být přijata příslušná opatření; relevance = 1; vyspělost = 0.

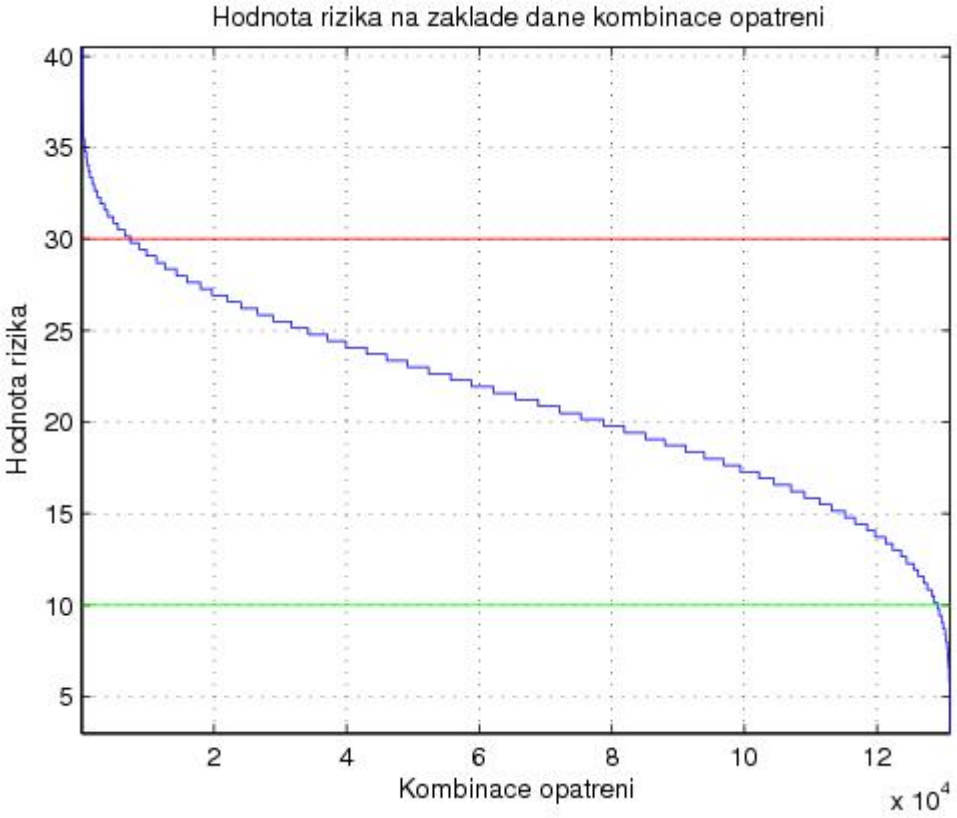
10.2.2 Možnosti zvládání prvního rizika

Jako ideálně dosažitelná hodnota prvního rizika (Tabulka 10.4) při implementaci všech vybraných opatření byla stanovena hodnota rovna třem – nižší zřejmě nebude možné zvolit, neboť se jedná o vztah dvou rozdílných subjektů.

Vývoj hodnot rizika na základě setříděných kombinací opatření je zobrazen viz Obrázek 10.7.

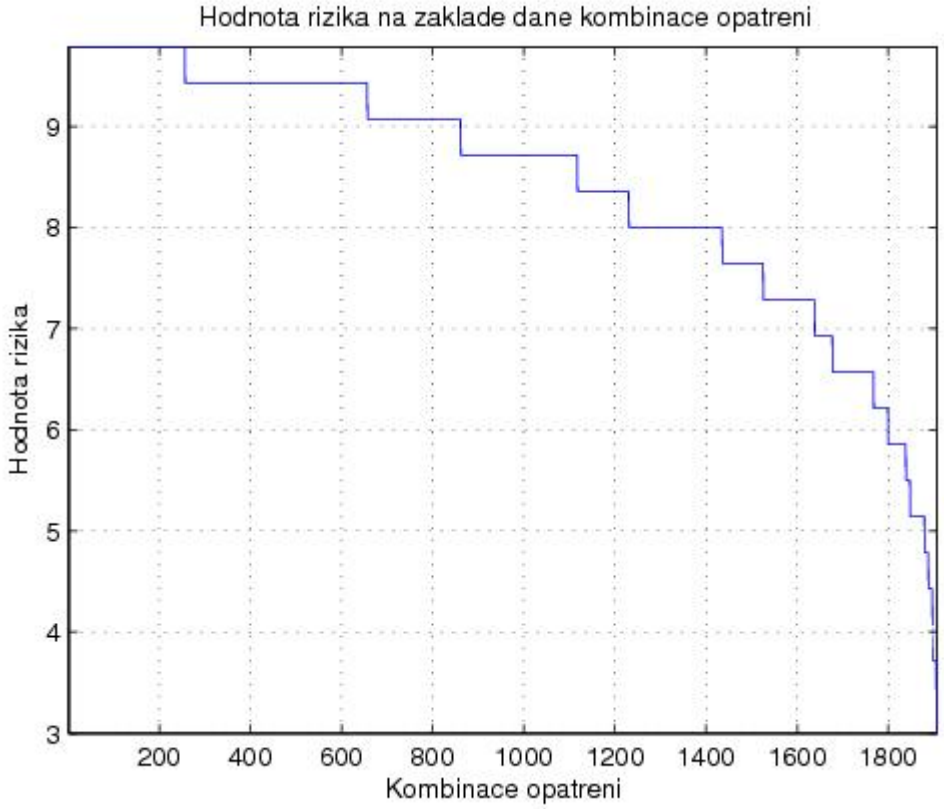
Hodnoty rizika v akceptovatelném pásmu jsou pak zobrazeny viz Obrázek 10.8.

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 (opět jsou jednotlivé jedničky a nuly ve stejném pořadí, jak byla definována jednotlivá opatření pro zvládání konkrétního rizika):
Hodnota rizika = 4.7857; kombinace pro poskytovatele = 011111; kombinace pro konzumenta = 10111111111
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 011111; kombinace pro konzumenta = 11011111111
Hodnota rizika = 4.7857; kombinace pro poskytovatele = 101111; kombinace pro konzumenta = 10111111111
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 101111; kombinace pro konzumenta = 11011111111
Hodnota rizika = 4.7857; kombinace pro poskytovatele = 110111; kombinace pro konzumenta = 10111111111
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 110111; kombinace pro konzumenta = 11011111111



Obrázek 10.7: Studie informační bezpečnosti služby IT – vývoj hodnoty prvního rizika.

Hodnota rizika = 4.7857; kombinace pro poskytovatele = 111011; kombinace pro konzumenta = 10111111111
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 111011; kombinace pro konzumenta = 11011111111
Hodnota rizika = 4.7857; kombinace pro poskytovatele = 111101; kombinace pro konzumenta = 10111111111
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 111101; kombinace pro konzumenta = 11011111111
Hodnota rizika = 4.7857; kombinace pro poskytovatele = 111110; kombinace pro konzumenta = 10111111111
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 111110; kombinace pro konzumenta = 11011111111
Hodnota rizika = 4.7857; kombinace pro poskytovatele = 111111; kombinace pro konzumenta = 00111111111
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 111111; kombinace pro konzumenta = 01011111111
Hodnota rizika = 4.0714; kombinace pro poskytovatele = 111111; kombinace pro konzumenta = 10011111111
Hodnota rizika = 4.7857; kombinace pro poskytovatele = 111111; kombinace pro konzumenta = 10111111110
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 111111; kombinace pro konzu-



Obrázek 10.8: Studie informační bezpečnosti služby IT – vývoj hodnoty prvního rizika, akceptovatelné riziko.

menta = 11011111110
Hodnota rizika = 4.4286; kombinace pro poskytovatele = 111111; kombinace pro konzumenta = 11111111011

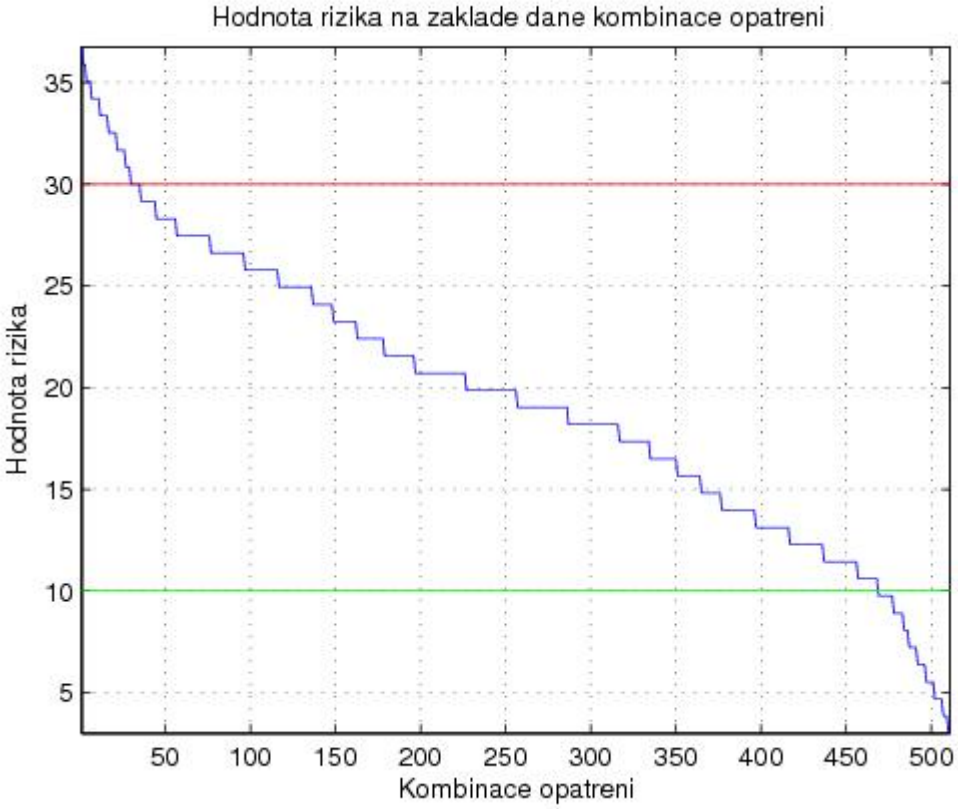
10.2.3 Možnosti zvládání druhého rizika

Jako ideálně dosažitelná hodnota prvního rizika (Tabulka 10.5) při implementaci všech vybraných opatření byla stanovena hodnota rovna třem – nižší zřejmě nebude možné zvolit, neboť se jedná o vztah dvou rozdílných subjektů.

Vývoj hodnot rizika na základě setříděných kombinací opatření je zobrazen viz Obrázek 10.9.

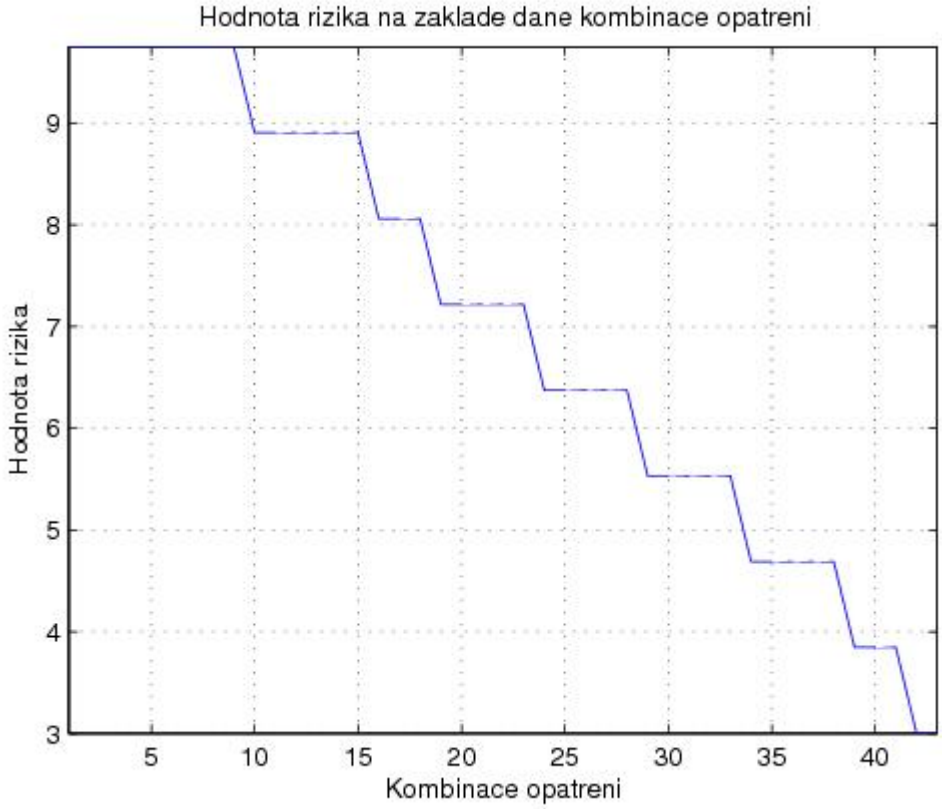
Hodnoty rizika v akceptovatelném pásmu jsou pak zobrazeny viz Obrázek 10.10.

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 (opět jsou jednotlivé jedničky a nuly ve stejném pořadí, jak byla definována jednotlivá opatření pro zvládání konkrétního rizika):
Hodnota rizika = 7.2187; kombinace pro poskytovatele = 0000; kombinace pro konzumenta = 11111
Hodnota rizika = 5.5312; kombinace pro poskytovatele = 0001; kombinace pro konzumenta = 11111



Obrázek 10.9: Studie informační bezpečnosti služby IT – vývoj hodnoty druhého rizika.

Hodnota rizika = 5.5312; kombinace pro poskytovatele = 0010; kombinace pro konzumenta = 11111
Hodnota rizika = 6.3750; kombinace pro poskytovatele = 0011; kombinace pro konzumenta = 01111
Hodnota rizika = 6.3750; kombinace pro poskytovatele = 0100; kombinace pro konzumenta = 11111
Hodnota rizika = 7.2187; kombinace pro poskytovatele = 0101; kombinace pro konzumenta = 01111
Hodnota rizika = 4.6875; kombinace pro poskytovatele = 0101; kombinace pro konzumenta = 11111
Hodnota rizika = 7.2187; kombinace pro poskytovatele = 0110; kombinace pro konzumenta = 01111
Hodnota rizika = 4.6875; kombinace pro poskytovatele = 0110; kombinace pro konzumenta = 11111
Hodnota rizika = 5.5312; kombinace pro poskytovatele = 0111; kombinace pro konzumenta = 01111
Hodnota rizika = 6.3750; kombinace pro poskytovatele = 1000; kombinace pro konzumenta = 11111
Hodnota rizika = 7.2187; kombinace pro poskytovatele = 1001; kombinace pro konzumenta = 01111
Hodnota rizika = 4.6875; kombinace pro poskytovatele = 1001; kombinace pro konzumenta



Obrázek 10.10: Studie informační bezpečnosti služby IT – vývoj hodnoty druhého rizika, akceptovatelné riziko.

= 11111
Hodnota rizika = 7.2187; kombinace pro poskytovatele = 1010; kombinace pro konzumenta = 01111
Hodnota rizika = 4.6875; kombinace pro poskytovatele = 1010; kombinace pro konzumenta = 11111
Hodnota rizika = 5.5312; kombinace pro poskytovatele = 1011; kombinace pro konzumenta = 01111
Hodnota rizika = 5.5312; kombinace pro poskytovatele = 1100; kombinace pro konzumenta = 11111
Hodnota rizika = 6.3750; kombinace pro poskytovatele = 1101; kombinace pro konzumenta = 01111
Hodnota rizika = 6.3750; kombinace pro poskytovatele = 1110; kombinace pro konzumenta = 01111
Hodnota rizika = 4.6875; kombinace pro poskytovatele = 1111; kombinace pro konzumenta = 01111

Kapitola 11

Závěr a další možnosti rozvoje

V rámci této disertační práce byl vyvinut unikátní přístup k řízení informační bezpečnosti služeb IT. Toho je dosaženo, mimo jiné novým, značně rozšířeným systémem pro řízení rizik ve vícedoménovém prostředí. Práce staví na mezinárodních standardech a je tak zaručeno, že vychází z nejlepších praktik, které jsou dostupné na trhu.

Možnosti dalšího rozvoje lze spatřovat v:

- V tuto chvíli jsou hodnoty vyspělostí definovány analytikem. V budoucnu by mělo být možné použít namísto odhadů, alespoň v některých případech, přímé měření [34] na IT infrastruktuře nebo metody pro měření výkonnosti procesů.
- Algoritmy v současné době v sobě nezahrnují odhad nákladů [44] na implementaci opatření. Při nákupu nových technologií je stanovení ceny jednoduchá záležitost, ale při implementaci procesů a obecně bezpečnostních projektů již toto tak snadné není. Mohlo by být jednoduše použito nákladů na hodinovou sazbu pracovníků, kteří by se na implementaci netechnologických opatření podíleli. Zapojení tohoto indikátoru by mohlo dále usnadnit výběr kombinace opatření při požadované hodnotě rizika.
- Tyto algoritmy by měly být implementovány do registru rizik, což se v současnosti děje v rámci projektu MASTER. Nicméně, ambice autora je toto provést v registru, který denně používá ve své praxi a u svých klientů. Toto bude tvořit významnou odlišnost v řízení rizik oproti konkurenci.

Úplným závěrem shrňme, v čem je tato práce konkrétně inovativní:

1. Zavádí nový systém Dohod o úrovni bezpečnosti služeb, kdy oproti jednoduchým jednostranným požadavkům na službu nebo byznys proces klade požadavky na všechny strany kontraktu (na všech stranách totiž může dojit k bezpečnostnímu incidentu).
2. Zavádí hodnocení opatření, kterými jsou redukována rizika. Z těchto hodnocení je následně odvozena schopnost opatření redukovat rizika.
3. Na základě ohodnocených opatření, které může být pro jedno opatření rozdílné na různých stranách kontraktu, potom stanovuje optimální varianty ve zvládání rizik (reálné implementace opatření) na základě potřeb a bezpečnostních požadavků na jednotlivých stranách kontraktu.

4. Vyvinuté metody nejsou závislé na metodách analýzy rizik, které jsou obvykle v různých organizacích odlišné. Jediným požadavkem je, aby byla hodnocena zranitelnost organizací (viz dále).

5. Poslední výhodou je možnost modelování snižování rizik. V současné době se totiž reziduální riziko pouze odhaduje.

Literatura

[1] Domovská stránka projektu MASTER (online červenec 2010), dostupné na: http://www.master-fp7.eu/.

[2] Zdroj informací k regulaci HIPAA (online červenec 2010), dostupné na: http://www.hipaa.org/.

[3] Zdroj informací k regulaci SOX (online červenec 2010), dostupné na: http://www.sarbanes-oxley.com/.

[4] Oficiální stránky organizace ISACA (online červenec 2010), dostupné na: http://www.isaca.org/.

[5] Web společnosti ISO (online červenec 2010), dostupné na: http://www.iso.org/.

[6] Web společnosti IEC (online červenec 2010), dostupné na: http://www.iec.ch/.

[7] Web týkající se informační bezpečnosti za použití standardů ISO/IEC 27000 (online červenec 2010), dostupné na: http://www.iso27001security.com/.

[8] Zdroj informací k ITILu (online červenec 2010), dostupné na: http://www.itil-officialsite.com/home/home.asp/.

[9] Standardy PCI (online červenec 2010), dostupné na: http://www.pcisecuritystandards.org/.

[10] IEC/ISO 31010:2009 Risk management – Risk assessment techniques.

[11] ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification.

[12] ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of practice.

[13] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.

[14] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management.

[15] ISO/IEC 27004:2009 Information technology – Security techniques – Information security management – Measurement.

[16] ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management.

[17] BITS: BITS Technology Risk Transfer Gap Analysis Tool. 2002, http://www.bits.org/.

[18] Boer, S.: *Six Sigma for IT Management.* Van Haren Publishing, 2006, iSBN-10 90-77212-30-2.

[19] van Bon, J.: *Foundations of IT Service Management Based on ITIL V3.* Van Haren Publishing, 2008, iSBN 978-90-8753-057-0.

[20] Brand, B.-H., K.: *IT Governance based on CobiT.* Van Haren Publishing, 2007, iSBN 978-90-8753-116-4.

[21] Calder, A.: *Implementing Information Security based on ISO 27001 and ISO 17799.* Van Haren Publishing, 2007, iSBN 978-90-77212-78-3.

[22] Calder, A.: *Information Security based on ISO 27001 and ISO 17799.* Van Haren Publishing, 2008, iSBN 978-90-77212-70-7.

[23] Chittenden, J.: *Risk management based on MoR.* Van Haren Publishing, 2006, iSBN 90-77212-68-X.

[24] Clemen, R.: *Making Hard Decisions.* Brooks Cole Publishing Company, 1996, iSBN 0-534-26034-9.

[25] Edwards, M.-R. W. D., W.: *Advances in Decision Analysis.* Cambridge University Press, 2007, iSBN 978-0-521-86368-1.

[26] Řepa, V.: *Podnikové procesy Procesní řízení a modelování.* GRADA Publishing, 2007, iSBN 978-80-247-2252-8.

[27] 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/.

[28] Garlick, A.: *Estimating Risk A Management Approach.* Gover Publishing Company, 2007, iSBN 987-0-566 08776-9.

[29] Gibbons, R.: *Game theory for applied economists.* Princeton University Press, 1958, iSBN 0-691-04308-6.

[30] Halouzka, J.: *Informační bezpečnost Self Assessment.* TATE International, 2003, iSBN 80-902858-9-9.

[31] Hendricks, H.-P., V.: *Game theory 5 questions.* Automatic Press, 2007, iSBN-10 87-991013-4-3.

[32] Koller, G.: *Risk Assessment and Decision Making.* Chapman and Hall CRC, 2005, iSBN 1-58488-477-0.

[33] Koller, G.: *Risk Assessment and Decision Making in Business and Industry.* Chapman and Hall, 2005, iSBN 1-58488-477-0.

[34] Kovacich, H.-E., G.: *Security Metrics Management.* Elsevier Inc, 2006, iSBN-13 978-0-7506-7899-5.

[35] Lacko, B.: The Risk Analysis of Soft Computing Projects. In *Proceedings International Conference on Soft Computing, 2004, European Polytechnical Institute Kunovice, Czech Republic*, 2004.

[36] Lacko, B.: Inovace metody RIPRAN a řízení rizik softwarových projektů. In *Sborník celostátní konference Tvorba softwaru 2007, VŠB-TU Ostrava*, 2007.

[37] Šmída, F.: *Zavádění a rozvoj procesního řízení ve firmě*. GRADA Publishing, 2007, iSBN 978-80-247-1679-4.

[38] Merna, A.-t. F., T.: *Risk management*. Computer press, 2007, iSBN 978-80-251-1547-3.

[39] Novák, L.; Svojanovský, P.: Přehled metodik pro strategické řízení IT. In *Professional Computing*, 2009, iSSN 1214-5335.

[40] Novák, L.; Svojanovský, P.: Řízení rizik ICT účelně a prakticky? In *Konference Internet ve státní správě a samosprávě*, 2010, http://www.isss.cz/.

[41] Peltier, T.: *Information security risk analysis*. CRC Press Taylor and Francis Group, 2005.

[42] Schelling, T. C.: *The strategy of conflict*. Harvard University Press, 1980, iSBN 0-674-84031-3.

[43] Schuyler, J.: *Risk and Decision Analysis in Projects*. Project Management Institute, 2001, iSBN 1-880410-28-1.

[44] Schwalbe, K.: *Řízení projektů v IT*. Computer Press, 2007, iSBN 978-80-251-1526-8.

[45] Sedláček, T.: *Ekonomie dobra a zla*. 65.pole, 2009, iSBN 978-80-903944-3-8.

[46] Smejkal, R.-K., V.: *Řízení rizik ve firmách a jiných organizacích*. Grada Publishing, 2006, iSBN 80-247-1667-4.

[47] Svojanovský, P.: Řízení rizik ICT v praxi. In *ICT and Security, Sborník přednášek*, 2009.

[48] Svojanovský, P.; Hradecká, L.: Process improvement towards information security. In *Současnost a budoucnost krizového řízení*, 2009, iSBN 978-80-254-5912-6.

[49] Svojanovský, P.; Kreslíková, J.: Rizika v implementaci procesů managementu služeb IT. In *Projektový management – jistota x riziko*, 2009, iSBN 978-80-7318-807-8.

[50] Thagard, P.: *Úvod do kognitivní vědy*. Portál, 2001, iSBN 80-7178-445-1.

[51] Tvrdíková, M.: *Aplikace moderních informačních technologií v řízení firmy*. GRADA Publishing, 2008, iSBN 978-80-247-1679-4.

[52] Vose, D.: *Risk Analysis*. John Wiley and Sons, 2008, iSBN 978-0-470-51284-5.

[53] Vose, D.: *Risk Analysis A quantitative guide*. John Wiley and Sons, 2008, iSBN 978-0-470-51284-5.

Příloha A

Seznam zkratek

Seznam zkratek, které jsou použity v této disertační práci je uveden viz Tabulka A.1.

Zkratka:	Význam:
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ČSN	Československá státní norma, Československá norma, Česká soustava norem, Česká technická norma
NIST	National Institute of Standards and Technology
HIPAA	Health Insurance Portability and Accountability Act
SOX	Sarbanes–Oxley Act
COBIT	Control Objectives for Information and related Technology
MASTER	Managing Assurance, Security and Trust for sERvices
BITS	Bank Information Technology Secretariat
PCI DSS	Payment Card Industry Data Security Standard
ISMS	Information Security Management System
SLA	Service Level Agreement
PLA	Protection Level Agreement
IT	Information Technology
PDCA	Plan Do Check Act
HAZOP	HAZard and OPerability studies
FMECA	Failure Modes and Effects and Criticality Analysis
SWIFT	Structure WhaT IF
RCA	Root cause analysis
ETA	Event Tree Analysis
FRAP	Facilitated Risk Analysis Process
CMDB	Configuration Management Database
IPS	Intrusion Prevention System
IDS	Intrusion Detection System

Tabulka A.1: Seznam zkratek.

Příloha B

Kompletní přehled opatření ISO/IEC 27002:2005

Tato příloha obsahuje převzatou strukturu standardu ISO/IEC 27002:2005; jinými slovy, obsahuje opatření, jejichž prosazením v praxi lze dosáhnout snížení rizika informační bezpečnosti. Pro detailní informace je nutné studium celého standardu ISO/IEC 27002:2005. Poznámka: čísla u jednotlivých opatření odpovídají přesně kapitolám v normě tak, aby byla zajištěna konzistence.

5 Bezpečnostní politika; 5.1 Politika bezpečnosti informací; 5.1.1 Dokument bezpečnostní politiky informací; 5.1.2 Přezkoumání bezpečnostní politiky informací.

6 Organizace bezpečnosti informací; 6.1 Interní organizace; 6.1.1 Závazek vedení směrem k bezpečnosti informací; 6.1.2 Koordinace bezpečnosti informací; 6.1.3 Přidělení odpovědností v oblasti bezpečnosti informací; 6.1.4 Schvalovací proces prostředků pro zpracování informací; 6.1.5 Dohody o ochraně důvěrných informací; 6.1.6 Kontakt s orgány veřejné správy; 6.1.7 Kontakt se zájmovými skupinami; 6.1.8 Nezávislá přezkoumání bezpečnosti informací; 6.2 Externí subjekty; 6.2.1 Identifikace rizik vyplývajících z přístupu externích subjektů; 6.2.2 Bezpečnostní požadavky pro přístup klientů; 6.2.3 Bezpečnostní požadavky v dohodách se třetí stranou.

7 Řízení aktiv; 7.1 Odpovědnost za aktiva; 7.1.1 Evidence aktiv; 7.1.2 Vlastnictví aktiv; 7.1.3 Přípustné použití aktiv; 7.2 Klasifikace informací; 7.2.1 Doporučení pro klasifikaci; 7.2.2 Označování a zacházení s informacemi.

8 Bezpečnost z hlediska lidských zdrojů; 8.1 Před vznikem pracovního vztahu; 8.1.1 Role a odpovědnosti; 8.1.2 Prověřování; 8.1.3 Podmínky výkonu pracovní činnosti; 8.2 Během pracovního vztahu; 8.2.1 Odpovědnosti vedoucích zaměstnanců; 8.2.2 Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací; 8.2.3 Disciplinární řízení; 8.3 Ukončení nebo změna pracovního vztahu; 8.3.1 Odpovědnosti při ukončení pracovního vztahu; 8.3.2 Navrácení zapůjčených prostředků; 8.3.3 Odebrání přístupových práv.

9 Fyzická bezpečnost a bezpečnost prostředí; 9.1 Zabezpečené oblasti; 9.1.1 Fyzický bezpečnostní perimetr; 9.1.2 Fyzické kontroly vstupu osob; 9.1.3 Zabezpečení kanceláří, místností a prostředků; 9.1.4 Ochrana před hrozbami vnějšku a prostředí; 9.1.5 Práce v zabezpečených oblastech; 9.1.6 Veřejný přístup, prostory pro nakládku a vykládku; 9.2 Bezpečnost zařízení; 9.2.1 Umístění zařízení a jeho ochrana; 9.2.2 Podpůrná zařízení; 9.2.3 Bezpečnost kabelových rozvodů; 9.2.4 Údržba zařízení; 9.2.5 Bezpečnost zařízení mimo prostory organizace; 9.2.6 Bezpečná likvidace nebo opakované použití zařízení; 9.2.7 Přemístění majetku.

10 Řízení komunikací a řízení provozu; 10.1 Provozní postupy a odpovědnosti; 10.1.1 Dokumentace provozních postupů; 10.1.2 Řízení změn; 10.1.3 Oddělení povinností; 10.1.4 Oddělení vývoje, testování a provozu; 10.2 Řízení dodávek služeb třetích stran; 10.2.1 Dodávky služeb; 10.2.2 Monitorování a přezkoumávání služeb třetích stran; 10.2.3 Řízení změn služeb poskytovaných třetími stranami; 10.3 Plánování a přejímání informačních systémů; 10.3.1 Řízení kapacit; 10.3.2 Přejímání systémů; 10.4 Ochrana proti škodlivým programům a mobilním kódům; 10.4.1 Opatření na ochranu proti škodlivým programům; 10.4.2 Opatření na ochranu proti mobilním kódům; 10.5 Zálohování; 10.5.1 Zálohování informací; 10.6 Správa bezpečnosti sítě; 10.6.1 Síťová opatření; 10.6.2 Bezpečnost síťových služeb; 10.7 Bezpečnost při zacházení s médii; 10.7.1 Správa výměnných počítačových médií; 10.7.2 Likvidace médií; 10.7.3 Postupy pro manipulaci s informacemi; 10.7.4 Bezpečnost systémové dokumentace; 10.8 Výměna informací; 10.8.1 Postupy a politiky při výměně informací a programů; 10.8.2 Dohody o výměně informací a programů; 10.8.3 Bezpečnost médií při přepravě; 10.8.4 Elektronické zasílání zpráv; 10.8.5 Informační systémy organizace; 10.9 Služby elektronického obchodu; 10.9.1 Elektronický obchod; 10.9.2 On-line transakce; 10.9.3 Veřejně přístupné informace; 10.10 Monitorování; 10.10.1 Pořizování auditních záznamů; 10.10.2 Monitorování používání systému; 10.10.3 Ochrana vytvořených záznamů; 10.10.4 Administrátorský a operátorský deník; 10.10.5 Záznam selhání; 10.10.6 Synchronizace hodin.

11 Řízení přístupu; 11.1 Požadavky na řízení přístupu; 11.1.1 Politika řízení přístupu; 11.2 Řízení přístupu uživatelů; 11.2.1 Registrace uživatele; 11.2.2 Řízení privilegovaného přístupu; 11.2.3 Správa uživatelských hesel; 11.2.4 Přezkoumání přístupových práv uživatelů; 11.3 Odpovědnosti uživatelů; 11.3.1 Používání hesel; 11.3.2 Neobsluhovaná uživatelská zařízení; 11.3.3 Zásada prázdného stolu a prázdné obrazovky monitoru; 11.4 Řízení přístupu k síti; 11.4.1 Politika užívání síťových služeb; 11.4.2 Autentizace uživatele pro externího připojení; 11.4.3 Identifikace zařízení v sítích; 11.4.4 Ochrana portů pro vzdálenou diagnostiku a konfiguraci; 11.4.5 Princip oddělení v sítích; 11.4.6 Řízení síťových spojení; 11.4.7 Řízení směrování sítě; 11.5 Řízení přístupu k operačnímu systému; 11.5.1 Bezpečné postupy přihlášení; 11.5.2 Identifikace a autentizace uživatelů; 11.5.3 Systém správy hesel; 11.5.4 Použití systémových nástrojů; 11.5.5 Časové omezení relace; 11.5.6 Časové omezení spojení; 11.6 Řízení přístupu k aplikacím a informacím; 11.6.1 Omezení přístupu k informacím; 11.6.2 Oddělení citlivých systémů; 11.7 Mobilní výpočetní zařízení a práce na dálku; 11.7.1 Mobilní výpočetní zařízení a sdělovací technika; 11.7.2 Práce na dálku.

12 Akvizice, vývoj a údržba informačních systémů; 12.1 Bezpečnostní požadavky informačních systémů; 12.1.1 Analýza a specifikace bezpečnostních požadavků; 12.2 Správné zpracování v aplikacích; 12.2.1 Validace vstupních dat; 12.2.2 Kontrola vnitřního zpracování; 12.2.3 Integrita zpráv; 12.2.4 Validace výstupních dat; 12.3 Kryptografická opatření; 12.3.1 Politika pro použití kryptografických opatření; 12.3.2 Správa klíčů; 12.4 Bezpečnost systémových souborů; 12.4.1 Správa provozního programového vybavení; 12.4.2 Ochrana dat pro testování systému; 12.4.3 Řízení přístupu ke knihovně zdrojových kódů; 12.5 Bezpečnost procesů vývoje a podpory; 12.5.1 Postupy řízení změn; 12.5.2 Technické přezkoumání aplikací po změnách operačního systému; 12.5.3 Omezení změn programových balíků; 12.5.4 Únik informací; 12.5.5 Programové vybavení vyvíjené externím dodavatelem; 12.6 Řízení technických zranitelností; 12.6.1 Řízení, správa a kontrola technických zranitelností.

13 Zvládání bezpečnostních incidentů; 13.1 Hlášení bezpečnostních událostí a slabin; 13.1.1 Hlášení bezpečnostních událostí; 13.1.2 Hlášení bezpečnostních slabin; 13.2 Zvládání bezpečnostních incidentů a kroky k nápravě; 13.2.1 Odpovědnosti a postupy; 13.2.2

Ponaučení z bezpečnostních incidentů; 13.2.3 Shromažďování důkazů.

14 Řízení kontinuity činností organizace; 14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací; 14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace; 14.1.2 Kontinuita činností organizace a hodnocení rizik; 14.1.3 Vytváření a implementace plánů kontinuity; 14.1.4 Systém plánování kontinuity činností organizace; 14.1.5 Testování, udržování a přezkoumávání plánů kontinuity.

15 Soulad s požadavky; 15.1 Soulad s právními normami; 15.1.1 Identifikace odpovídajících předpisů; 15.1.2 Ochrana duševního vlastnictví; 15.1.3 Ochrana záznamů organizace; 15.1.4 Ochrana dat a soukromí osobních údajů; 15.1.5 Prevence zneužití prostředků pro zpracování informací; 15.1.6 Regulace kryptografických opatření; 15.2 Soulad s bezpečnostními politikami, normami a technická shoda; 15.2.1 Shoda s bezpečnostními politikami a normami; 15.2.2 Kontrola technické shody; 15.3 Hlediska auditu informačních systémů; 15.3.1 Opatření k auditu informačních systémů; 15.3.2 Ochrana nástrojů pro audit informačních systémů.

Příloha C

Příklad zdrojového kódu

V této příloze je uveden příklad zdrojového kódu pro výpočet optimálních kombinací vybraných opatření pro eliminaci rizika. Je použito prostředí Matlab (http://www.mathworks.com) pro jeho univerzálnost a snadnost použití. Lze ale předpokládat, že implementovaný kód v průmyslovém registru rizik bude například makro v Excelu, kód Java (tento přístup byl zvolen v projektu MASTER) a podobně. Řádky začínající znakem procent (%) jsou komentář zdrojového kódu – dle syntaxe Matlabu. Zdrojový kód je uveden z případové studie řízení informační bezpečnosti služeb IT, optimalizace prvního rizika. Pro prvotní testy případných experimentátorů je možné pouze zkopírovat kód do Matlabu (případně převést do jiného prostředí) a začít na něm stavět případně svoje vlastní modifikace. Názvy proměnných jsou voleny tak, aby celý kód byl maximálně návodný.

```
clear all;
close all;

%definice relevanci a vyspelosti opatreni
%v pripade rizeni rizik nekolika stran kontraktu jsou hodnoty spojeny
%na konci kodu je treba dat pozor na oddeleni jednotlivych kombinaci
%nula u vyspelosti znamena neni implementovano
rel = [1 1 1 1 1 0.5 1 0.75 0.25 1 1 1 1 1 0.5 1 1];
vys = [0.75 0.75 0.75 0.75 0.75 0.5 0.75 0.75 0.5 0 ...
    0.25 0.5 0.5 0.5 0.25 0.25 0.75];

%definice rizikoveho scenare
dopad = 450;
hrozba = 0.3;
zranitelnost = 0.3;
idealne_dosazitelne_riziko = 3;

%test stejne delky vektoru rel a vys
if length(rel) ~= length(vys),
    disp('Chyba - rozdilna delka vektoru relevanci a vyspelosti');
    break;
end

%ohodnoceni opatreni
```

```
ohodnocena_opatreni = rel .* (1 - vys);

%alokace pameti
ohodnocena_opatreni_kombinace = zeros (1,((2^length(rel))-1));

%vypocet kombinaci ne/implementace ohodnocenych opatreni
for ii = 1:length (ohodnocena_opatreni_kombinace),
    %nula znamena zadne opatreni neni implementovano
    kombinace_dekadicky = ii - 1;
    kombinace_binarne = dec2bin (kombinace_dekadicky);
    %funkce dec2bin vraci string, prevod na integer
    kombinace_binarne = strrep (kombinace_binarne, '0', '0 ');
    kombinace_binarne = strrep (kombinace_binarne, '1', '1 ');
    kombinace_binarne = str2num (kombinace_binarne);
    %zajisteni stejne delky jako u relevanci a vyspelosti
    nuly_plus = zeros (1,(length (rel) - length (kombinace_binarne)));
    kombinace_binarne = [nuly_plus kombinace_binarne];
    %finalni ohodnoceni dane kombinace opatreni
    ohodnocena_opatreni_kombinace (ii) = ...
        sum(kombinace_binarne .* ohodnocena_opatreni);
end

%uchovani nesetridenych kombinaci pro rekonstrukci kombinace opatreni
nesetridene_kombinace = ohodnocena_opatreni_kombinace;

%setrideni jednotlivych kombinaci
[ohodnocena_opatreni_kombinace, ind] = ...
    sort (ohodnocena_opatreni_kombinace,2,'ascend');

%vypocet idealni zranitelnosti
zranitelnost_idealni = idealne_dosazitelne_riziko / (dopad * hrozba);

%prevod setridene agregovane zvladatelnosti zranitelnosti na hodnotu rizika
ohodnocena_opatreni_kombinace = max(ohodnocena_opatreni_kombinace) - ...
    ohodnocena_opatreni_kombinace;
vektor_zranitelnosti = ohodnocena_opatreni_kombinace / ...
    max(ohodnocena_opatreni_kombinace);
vektor_zranitelnosti = vektor_zranitelnosti * ...
    (zranitelnost - zranitelnost_idealni);
vektor_zranitelnosti = vektor_zranitelnosti + zranitelnost_idealni;

%uchovani nesetridenych kombinaci pro rekonstrukci kombinace opatreni
nesetridene_kombinace = max(nesetridene_kombinace) - nesetridene_kombinace;
nesetridene_kombinace_zranitelnosti = ...
    nesetridene_kombinace / max(nesetridene_kombinace);
nesetridene_kombinace_zranitelnosti = ...
    nesetridene_kombinace_zranitelnosti *...
    (zranitelnost - zranitelnost_idealni);
```

```
nesetridene_kombinace_zranitelnosti = ...
    nesetridene_kombinace_zranitelnosti + zranitelnost_idealni;

%vypocet hodnot rizika pro jednotlive kombinace
vektor_rizik = vektor_zranitelnosti * dopad * hrozba;

%uchovani nesetridenych kombinaci pro rekonstrukci kombinaci opatreni
nesetrideny_vektor_rizik = ...
    nesetridene_kombinace_zranitelnosti * dopad * hrozba;

%tisk grafu
figure;
plot(vektor_rizik); axis tight; grid on;
title ('Hodnota rizika na zaklade dane kombinace opatreni');
xlabel ('Kombinace opatreni');
ylabel ('Hodnota rizika');

%akceptovatelne riziko, viz metodika
rozsahy_os = axis;
hold on;
plot([rozsahy_os(1) rozsahy_os(2)],[10 10],'g');
plot([rozsahy_os(1) rozsahy_os(2)],[30 30],'r');
hold off;

%akceptovatelne riziko graf
figure;
plot(vektor_rizik(find(vektor_rizik < 10))); axis tight; grid on;
title ('Hodnota rizika na zaklade dane kombinace opatreni');
xlabel ('Kombinace opatreni');
ylabel ('Hodnota rizika');

%definice pasma, kde jsou zkoumany kombinace analytikem
pasmo = find (and((nesetrideny_vektor_rizik>4),...
    (nesetrideny_vektor_rizik<5.1)));

%tisk kombinaci opatreni pro dane hodnoty rizik v danem pasmu
for ii=1:length(pasmo),
    disp([num2str(nesetrideny_vektor_rizik(pasmo(ii))) ' ' ...
        num2str(dec2bin(pasmo(ii)-1))]);
end
```

Příloha D

Publikace autora disertační práce

Tato příloha obsahuje vybrané publikace autora disertační práce, které se pojí se zde prezentovaným tématem. Jejich popis je rozdělen do dvou částí:

1. Publikace zveřejněné v rámci odborných článků a přednášek.
2. "Dodávky" do vědecko-výzkumného projektu MASTER s krátkým popisem; tam, kde se jedná o veřejně přístupné dodávky je uveden i odkaz, kde je možné publikace stáhnout. Je třeba zdůraznit, že v těchto dodávkách působí autor disertační práce jako člen širšího konsorcia a je tedy vždy spoluautorem, ne samostatným autorem dodávky. Je také uveden datum, kdy byla dodávka zaslána Evropské komisi, aby byl usnadněn přehled, kdy byla dodávka v rámci projektu dodána.

Publikace jdou dostupné na fakultní webové stránce autora disertační práce.

D.1 Standardní vybrané publikace

D.1.1 Process Improvement Towards Information Security

Svojanovský Petr, Novák Luděk, Kreslíková Jitka: Process Improvement Towards Information Security, In: Security and Protection of Information 2009, Brno, CZ, UNOB, 2009, s. 15-22, ISBN 978-80-7231-641-0

Přednáška s názvem Process Improvement Towards Information Security se týkala možnosti využití implementace standardu ISO/IEC 20000 pro zlepšení informační bezpečnosti. Konala se během konference Security and Protection of Information v rámci mezinárodního veletrhu IDET.

Další informace: http://www.vabo.cz/spi/program.asp

D.1.2 Role Řízení IT služeb v Informační Bezpečnosti

Svojanovský Petr, Novák Luděk, Kreslíková Jitka: Role řízení IT služeb v informační bezpečnosti, In: Současnost a budoucnost krizového řízení 2009, Praha, CZ, T-SOFT, 2009, s. 5, ISBN 978-80-254-5912-6

Příspěvek ve sborníku a konferenci s názvem Současnost a budoucnost krizového řízení. Článek se opět věnoval možnosti propojení řízení informační bezpečnosti a řízení IT služeb. Pozornost byla věnována praktickým příkladům využití.

Další informace: http://www.tsoft.cz/konference/2009/

D.1.3 Přehled metodik pro strategické řízení IT

Svojanovský Petr, Novák Luděk: Přehled metodik pro strategické řízení IT, In: Professional Computing , roč. 10, č. 12, 2009, Brno, CZ, s. 27-29, ISSN 1214-5335

Příspěvek v časopise Professional Computing se týkal přehledu a možnostem využití metodik CobiT, Val IT a Risk IT. Zaměření příspěvku je spíše na strategické řízení IT, než každodenní provoz. Je tedy upřednostněn IT Governance před IT Management.

Další informace: http://www.anect.com/cs/novinky/prehled-metodik-pro-strategicke-rizeni-it.html

D.1.4 Rizika v implementaci procesů managementu služeb IT

Svojanovský Petr, Kreslíková Jitka, Novák Luděk: Rizika v implementaci procesů managementu služeb IT, In: Projektový management jistota x riziko, Zlín, CZ, UTB ve Zlíně, 2009, s. 13, ISBN 978-80-7318-808-5

Příspěvek v rámci konference Jistota X Riziko se zabýval implementací řízení služeb IT dle ISO/IEC 20000 a rizikovostí tohoto procesu. Kromě ISO/IEC 20000 bylo vysvětleno řízení rizik ve spojení se zaváděním řízení služeb. Následovala také ukázka a vysvětlení funkce registru rizik.

Další informace: http://agentura.utb.cz/projekt//s/86/p

D.1.5 Řízení rizik ICT účelně a prakticky?

Svojanovský Petr, Novák Luděk: Řízení rizik účelně a prakticky?, In: Konference Internet ve státní správě a samosprávě, Hradec Králové, CZ, Triada, 2010, s. 170-174, ISBN 978-80-904566-0-0

V rámci konference iSSS pod záštitou bývalého premiéra ČR Jana Fischera, ministra vnitra ČR Martina Peciny a Asociace krajů ČR byly představeny metody pro efektivní řízení rizik se zaměřením na státní správu. Diskutovány byly prvně klasické metody analytického typu a vysvětleny jejich nevýhody, na což bylo navázáno vysvětlením efektivních principů v řízení rizik.

Další informace: http://www.isss.cz/

D.1.6 Řízení rizik v bezpečnosti služeb IT

Svojanovský Petr, Kreslíková Jitka: Řízení rizik v bezpečnosti služeb IT, dostupné online na http://www.risk-management.cz/, ISSN 1802-0496

Jádro disertační práce je publikováno na odborném webu, který se věnuje výhradně problematice řízení rizik. V článku jsou představeny zejména optimalizace v řízení rizik vyvinuté v rámci této disertační práce. Tato forma prezentace je zvolena z důvodu snadného přístupu masové veřejnosti i profesionálů k novým myšlenkám v řízení rizik.

Další informace: http://www.risk-management.cz/

D.1.7 Risk Identification in ISO/IEC 20000:2005 Implementation

Svojanovský Petr, Kreslíková Jitka, Novák Luděk: Risk Identification in ISO/IEC 20000:2005 Implementation, In: Proceedings of 43rd Spring International Conference MOSIS'09 Modelling and Simulation of Systems, Ostrava, CZ, MARQ, 2009, s. 7, ISBN 978-80-86840-45-1

Příspěvek se zabývá řízením rizik v tak specifické oblasti, jako je implementace procesů ISO/IEC 20000 ve středně velké společnosti. Je rozebrán celý proces řízení se svými specifiky pro tuto oblast.

D.1.8 Specific Attitude to Risk Management on the Background of Global Software Development

Svojanovský Petr, Kreslíková Jitka: Specific Attitude to Risk Management on the Background of Global Software Development, In: 3rd IFIP Central and Eastern European Conference on Software Engineering Techniques CEE-SET 2008, Wroclaw, PL, PWR WROC, 2008, s. 271-282, ISBN 978-83-7493-421-3

Text se věnuje řízení rizik v nadnárodní korporaci s celosvětovým rozsahem. Přínosem článku je ukázka řízení ve virtuálních týmech, kde je obtížná komunikace díky tomu, že jednotliví členové týmů jsou rozprostřeni po celém světě a mnohdy se osobně ani neznají.

D.2 Dodávky do vědecko-výzkumného projektu MASTER

D.2.1 D1.1.2: Regulatory Compliance Analysis

Dodávka popisuje metody identifikace regulatorních a standardizačních požadavků pro aplikaci bezpečnostních kontrolních aktivit, dále popisuje, jak dosáhnout souladu systému organizace s těmito požadavky.

Dodávka se skládá z následujících částí:

1. Popis metody, jak získat důležité informace ze standardů a regulatorních požadavků. Tyto informace jsou pak mapovány z pohledu potřeb informační bezpečnosti.

2. Analýza regulatorních požadavků s ohledem na zaměření projektu MASTER a harmonizace právního prostředí EU: Italian Legislative Decree no. 196, File F Regulatory Framework, Joint Commission Accreditation, ISO/IEC 20000-1:2005, Royal Decree 239/2007, Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA) 1996.

3. Další část popisuje mapování mezi výše definovanými regulatorními požadavky a ISO/IEC 27002:2005.

4. Výsledkem pak je vývoj 51 bezpečnostních kontrol, jejichž implementace zajišťuje soulad s výše definovanými regulatorními požadavky.

Vlastní přínos autora disertační práce: mapování mezi vyvinutými bezpečnostními kontrolami a regulatorními požadavky.

Datum dodání Evropské komisi: 24. 6. 2009

Dokument dostupný online: http://www.master-fp7.eu/index.php?option=com_docman&task=doc_download&gid=51&Itemid=60

D.2.2 D1.1.3: Risk Analysis Modelling

Dokument popisuje obecný přístup k řízení rizik a jeho různé varianty a metody. Hlavní část dokumentu popisuje přístup k řízení rizik z pohledu projektu MASTER a zdůvodňuje důvody pro výběr konkrétního přístupu k řízení rizik v projektu. Dokument má návaznost na další dodávku – viz dále.

Vlastní přínos autora disertační práce: popis analýzy rizik metodou rizikových scénářů s využitím registrů rizik a odůvodnění výběru teto metody.

Datum dodání Evropské komisi: 10. 7. 2009

Dokument dostupný online: http://www.master-fp7.eu/index.php?option=com_docman&task=doc_download&gid=52&Itemid=60

D.2.3 D3.2.2: The Protection & Assessment Workbench: First Integrated Prototype

Dokument popisuje softwarový nástroj vyvíjený v rámci projektu MASTER, který bude sloužit pro monitorování IT infrastruktury ve smyslu měřit, hodnotit a vynucovat bezpečnostní kontroly s cílem dosažení souladu s regulatorními požadavky. Součástí tohoto nástroje (tzv. Workbench) je i registr rizik s implementovanou metodikou analýzy a řízení rizik.

Vlastní přínos autora disertační práce: vlastní vývoj SW části Workbench pro analýzu a řízení rizik a příslušný popis v rámci tohoto dokumentu. Další verze dokumentu bude obsahovat popis metod uvedených v této disertační práci. Samozřejmě bude dodávka obsahovat i příslušnou SW část Workbench (tohoto bude dosaženo na konci roku 2010, použité vývojové prostředí je Eclipse Ganymede – http://www.eclipse.org/ganymede/, konkrétně Eclipse Modelling Framework a Eclipse Graphical Modelling Framework).

Datum dodání Evropské komisi: 12. 2. 2010

Tato verze dokumentu není dostupná online.

Příloha E

Obsah CD

Přiložený kompaktní disk obsahuje:

1. Zdrojový kód textu disertační práce v prostředí LaTeX.
2. Zdrojový kód implementovaných algoritmů v prostředí Matlab.