Metody analýzy rizik podnikových informačních systémů – učební pomůcka pro předmět Bezpečnost informačních systémů

Methods of risk analysis for business information systems – a teaching aid for course information security systems

Bc. Jaroslav Krajča

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jaroslav KRAJČA**
Osobní číslo:	**A09377**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Metody analýzy rizik podnikových informačních systémů – učební pomůcka pro předmět Bezpečnost informačních systémů.**

Zásady pro vypracování:

1. **Proveďte literární rešerši k tématu práce.**
2. **Analyzujte možnosti analýzy rizik a proveďte srovnání dostupných metod.**
3. **Formou projektu připravte návrh obsahu a formy učební pomůcky včetně postupu realizace.**
4. **Realizujte zvolené řešení.**
5. **Proveďte diskusi nad řešením projektu.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno : Tribun, 2009. 134 s. ISBN 978-80-7399-731-1.**
2. **DOBDA , Luboš . Ochrana dat v informačních systémech . Praha : Grada, 2001. 288 s. ISBN 8071694797.**
3. **DOSEDĚL, Tomáš . Počítačová bezpečnost a ochrana dat . Praga : Computer Press, 2004. 200 s. ISBN 80-251-0106-1.**
4. **KOVACICH, Gerald L. Průvodce bezpečnostního pracovníka informačních systémů : zavádění a prosazování bezpečnostní politiky informačních systémů. Brno : UNIS, 2000. 200 s. ISBN 80-86097-42-0.**
5. **NORTHCUTT, Stephen ; ZELTSER, Lenny ; WINTERS, Scott . Bezpečnost počítačových sítí . Praha : Computer Press, 2005. 592 s. ISBN 80-251-0697-7.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je poskytnou čtenáři pohled na problematiku analýzy rizik informačních systémů. Práce uvádí základní metodologické postupy, které vedou ke tvorbě analýzy a jsou charakteristické především pro oblast IS. Prioritou bylo především vytvořit učební pomůcku, která by názorně a jednoduše ukazovala, jak postupovat při tvorbě analýzy rizik, která je zaměřená na informační systémy.

Klíčová slova:

Analýza rizik, informační rizika, informační bezpečnost.

ABSTRACT

The aim of this work is to give readers perspective on analysis of information systems risk. The work presents basic methodological procedures that lead to the formation analysis and are mainly characteristic for the IS. The priority was formation a teaching tool that would clearly and simply show how to proceed in developing a risk analysis that focuses on information systems.

Keywords:

Risk analysis, information risk, information security.

Chtěl bych poděkovat především vedoucímu mé bakalářské práce doc. Mgr. Romanu Jaškovi, Ph.D. za cenné připomínky a rady při řešení problémů související s diplomovou prací.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Dnešní doba je charakteristická tím, že téměř každý je závislý na informačních technologiích. Tento fakt se nedotýká pouze jednotlivců, ale také organizací a firem. Každý podnik se musí zabývat zpracováním informací, které jsou pro něj důležité a brát je při své činnosti v úvahu. V drtivé většině případů jsou tyto informace v elektronické podobě. Organizace na ně plně spoléhají při plánování, řízení a realizování svých aktivit a věnují mnoho prostředků a času na jejich zpracování a vyhodnocování.

Uvědomují si ale organizace skutečnou hodnotu těchto informací? Většinou podnik zjistí, jak hodnotná informace pro ně jsou až v okamžiku, kdy o ně přijdou. Může to být v důsledku výpadku proudu, poškození hardwaru nebo špatnou technologií zálohování. Je zde také možnost úmyslného pozměnění, ať už pachatel sleduje jakýkoliv záměr. Všechny tyto události mohou vést k poškození dobrého jména firmy, ztráty důvěry klientů nebo dokonce akcionářů. Organizace, která si uvědomuje hodnotu zpracovávaných informací, věnuje nemalé prostředky a čas k zachování jejich bezpečnosti.

Některé podniky přistupují k problému řešení bezpečnosti informací komplexně, jiné nahodile. Systematické řešení problému bezpečnosti v organizaci představuje dokumentovaný a propracovaný postup přechodu ze současného stavu ke stavu cílovému. Pro dosažení tohoto cíle je nezbytné vypracování celkové bezpečnostní politiky. Celková bezpečnostní politika je dokument, který má roli základního dokumentu pro budování bezpečnosti jak v oblasti informačních technologií podniku, tak v ostatních oblastech. Bezpečnostní politika nám tedy definuje, co chránit, proti čemu a jakým způsobem. Je to právě analýza rizik, která je základním stavebním kamenem, pro vypracování bezpečnostní politiky.

I. TEORETICKÁ ČÁST

1 CHARAKTERISTIKA ANALÝZY RIZIK A ZÁKLADNÍ POJMY

Analýza rizik se zabývá odhalováním a pochopením rizik. Poskytuje podklady pro rozhodnutí o nutnosti zabývat se určenými riziky a doporučuje nejvhodnější a nákladově efektivní strategii zvládání rizik. Analýza rizik obsahuje odhalení zdrojů rizik, jejich příznivých a nepříznivých následků a možností, že se tyto následky přihodí. Mohou být identifikovány faktory, které ovlivňují následky a jejich pravděpodobnosti. Rizika se analyzují spojením následků a jejich pravděpodobností. Ve většině případů se berou v úvahu už existující opatření.

Jedná se základní stavební pilíř pro výstavbu bezpečnostní politiky informačního systému, která má klíčovou roli pro zachování potřebné úrovně důvěrnosti, autenticity a integrity dat v informačním systému podniku.

Obrázek 1: Role analýzy rizik v informační bezpečnosti podniku

Představuje proces, který pomáhá odhalit bezpečnostní rizika působící na organizaci nebo informačním systému a přispívá ke zkvalitnění návrhu bezpečnostních opatření. V prvním kroku se provádí výběr bezpečnostních rizik, který představuje identifikaci aktiv a hrozeb. V dalším kroku se hodnotí zranitelnost aktiv vůči těmto hrozbám a pravděpodobnost jejich výskytu. V rámci hodnocení bezpečnostních rizik se také provádí odhad jejich potenciálního dopadu. Na základě výsledků hodnocení bezpečnostních rizik se navrhují bezpečnostní požadavky pro systém, které mají zajistit bezpečný provoz a využívání informačních systémů.

Analýza rizik zahrnuje:

- identifikaci aktiv
- identifikaci hrozeb
- ohodnocení aktiv
- určení pravděpodobnosti uplatnění hrozby
- určení zranitelnosti každého aktiva hrozbou
- výpočet hodnoty rizika pro každou dvojici aktiva a hrozby

1.1 Riziko

Riziko je historický výraz, pocházející údajně ze 17. století, kdy se objevil v souvislosti s lodní plavbou. Výraz „risico“ pochází z italštiny a označoval úskalí, kterému se museli plavci vyhnout. Následně se tím vyjadřovalo „vystavení nepříznivým okolnostem“. Ve starších encyklopediích najdeme pod tímto heslem vysvětlení, že se jedná o odvahu či nebezpečí, případně že „riskovat“ znamená odvážit se něčeho. Teprve později se objevuje i význam ve smyslu možné ztráty. Dnes již víme, že nebezpečí představuje něco poněkud jiného a v teorii rizika souvisí s hrozbou. Podle dnešních výkladů se rizikem obecně rozumí nebezpečí vzniku škody, poškození, ztráty či zničení, případně nezdaru při podnikání.

Neexistuje obecně uznávaná definice pojmu riziko a jejich výkladů můžeme naleznout nepřeberné množství:

- Pravděpodobnost či možnost vzniku ztráty, obecně nezdaru.
- Variabilita možných výsledků nebo nejistota jejich dosažení.
- Odchýlení skutečných a očekávaných výsledků.
- Pravděpodobnost jakéhokoliv výsledku, odlišného od výsledku očekávaného.
- Situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti.
- Nebezpečí negativní odchylky od cíle (tzv. čisté riziko).
- Nebezpečí chybného rozhodnutí.
- Možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko).
- Neurčitost spojená s vývojem hodnoty aktiva (tzv. investiční riziko).
- Střední hodnota ztrátové funkce.

Riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní. Riziko vzniká vzájemným působením hrozby a aktiva. Hrozba, která nepůsobí na žádné aktivum, nemusí být při analýze rizik brána v úvahu. Aktivum, na které nepůsobí žádná hrozba, není předmětem analýzy rizik.

Úroveň rizika je určena hodnotou aktiva, zranitelností aktiva a úrovní hrozby. Na růstu úrovně rizika se podílí úroveň hrozby, zranitelnost a hodnota aktiva. Jedině protiopatření úroveň rizika snižuje. Při návrhu protiopatření se používá pravidlo, které stanovuje, že náklady vynaložené na snížení rizika musí být přiměřené hodnotě chráněných aktiv (případně hodnotě škod, vzniklých dopadem hrozby). S tímto pravidlem souvisí stanovení referenční úrovně rizika, pod kterou se riziko prohlásí za zbytkové a nepodnikají se žádná protiopatření.

Zbytkové riziko je takové riziko, které je tak malé (nepřesáhne referenční úroveň), že je pro subjekt přijatelné a není nutné podnikat další protiopatření k jeho snížení. Referenční

úroveň je hranice míry rizika (stanovená hodnota velikosti rizika), která rozhoduje o tom, zda je riziko zbytkové (velikost rizika je menší než referenční úroveň), či není zbytkové (velikost rizika je větší než referenční úroveň). Tím se rozhodne, zda proti riziku je či není nutné podnikat další protiopatření pro jeho snížení. Referenční úroveň by měla být na takové úrovni, aby dopad hrozby byl tak malý, že jej lze zanedbat.

Z hlediska informačních systému je asi nejvýstižnější definice, která popisuje riziko jako pravděpodobnost, že určitá hrozba využije specifické zranitelnosti systému, překoná uplatněné opatření a způsobí narušení důvěrnosti, integrity nebo dostupnosti aktiva, a to povede ke vzniku škody.

1.2 Aktivum

Aktivum je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Aktiva se dělí na hmotná (například nemovitosti, cenné papíry, peníze apod.) a na nehmotná (například informace, předměty průmyslového a autorského práva, morálka pracovníků, kvalita personálu apod.). Aktivem ale může být sám subjekt, neboť hrozba může působit na celou jeho existenci.

Základní charakteristikou aktiva je hodnota aktiva, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti) aktiva pro daný subjekt, popřípadě kombinaci obou přístupů. Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení.

Při hodnocení aktiva se berou v úvahu především následující hlediska:

- pořizovací náklady či jiná hodnota aktiva
- důležitost aktiva pro existenci či chování subjektu
- náklady na překlenutí případné škody na aktivu
- rychlost odstranění případné škody na aktiv
- jiná hlediska (mohou být specifická případ od případu)

Příkladem aktiv typické pro informační systémy mohou být osobní počítače, notebooky, operační systémy, kancelářský software, účetní software a především uložená a zpracovávaná data.

Další charakteristikou aktiva, která vyjadřuje jeho citlivost na působení hrozby, je zranitelnost.

1.3 Hrozba

Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu. Hrozbou může být například požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy, ale i kontrola finančního úřadu nebo růst kursu české koruny vzhledem k evropské měně, apod.

Škoda, kterou způsobí hrozba při jednom působení na určité aktivum, se nazývá dopad hrozby. Dopad hrozby může být odvozen od absolutní hodnoty ztrát, do které jsou zahrnuty náklady na znovuobnovení činnosti aktiva nebo náklady na odstranění následků škod způsobených subjektu hrozbou.

Základní charakteristikou hrozby je její úroveň. Úroveň hrozby se hodnotí podle následujících faktorů:

- Nebezpečnost: schopnost hrozby způsobit škodu.
- Přístup: pravděpodobnost, že se hrozba svým působením dostane k aktivu (získá k němu přístup). Jednou z forem vyjádření může být i frekvence výskytu hrozby.
- Motivace: zájem iniciovat hrozbu vůči aktivu. Odhad motivace spočívá v pochopení skupinových a národních záměrů i záměrů jednotlivců, jejich cílů a politiky – to vše se analyzuje s ohledem na předchozí podmínky a činnost těchto ohrožovatelů (útočníků). Odhad motivace napomáhá při tvorbě expertních stanovisek a odhadů hrozeb.

Typickou informační hrozbou je malware, tedy škodlivý software jako počítačové viry, trojské koně, spyware a adware.

1.4 Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.

Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva se hodnotí podle následujících faktorů:

- Citlivost: náchylnost aktiva být poškozeno danou hrozbou.
- Kritičnost: důležitost aktiva pro analyzovaný subjekt.

Zranitelnost může přestavovat například neaktualizovaný operační systém bez záplat, antivirový program bez aktualizací nebo špatně nastavená pravidla firewallu.

1.5 Protiopatření

Protiopatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Protiopatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.

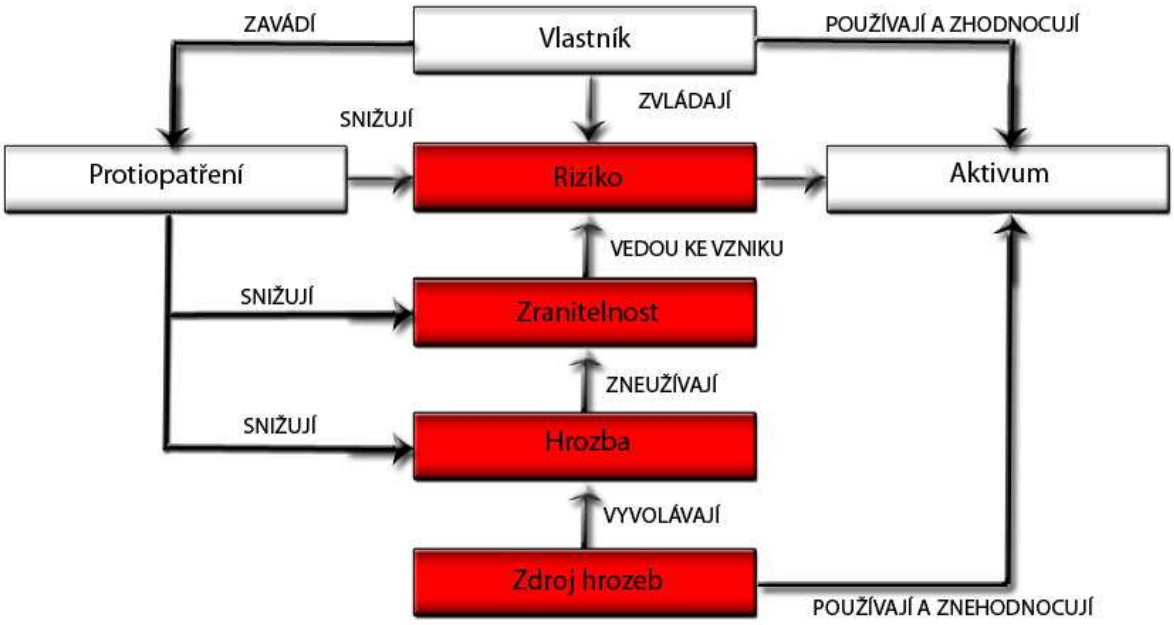
Z hlediska analýzy rizik je protiopatření charakterizováno efektivitou a náklady. Efektivita protiopatření vyjadřuje, nakolik protiopatření sníží účinek hrozby. Používá se ve fázi zvládání rizik jako jeden z hlavních parametrů při hodnocení vhodnosti použití daného protiopatření.

Protiopatření se zaměřují na oblasti snížení úrovně hrozby, snížení úrovně zranitelnosti, snížení následků působení hrozby, detekce nežádoucího vlivu s cílem včas indikovat

působení hrozby a předejít možnosti jejího plného uplatnění, dál se pak zaměřují na oblast obnovení činnosti po působení hrozby.

Do nákladů na protiopatření se započítávají náklady na pořízení, zavedení a provozování protiopatření. Společně s efektivitou protiopatření jsou tyto náklady důležitými parametry při výběru protiopatření. Výběr vhodného protiopatření spočívá v optimalizaci, kdy se hledají nejúčinnější protiopatření, jejichž realizace přinese co nejmenší náklady.

Protiopatření pro informační systémy jsou patche, záplaty, aktualizace, antivirové programy, firewall, antispywarové programy.



Obrázek 2: Riziko a jeho vazby

2 METODY ANALÝZY RIZIK

Způsob vyjádření veličin, s nimiž se v analýze rizik pracuje, lze použít jako základní hledisko pro rozdělení těchto metod. Existují přitom dva základní přístupy k jejímu řešení. Jsou to kvantitativní a kvalitativní metody vyjádření veličin analýzy rizik. V analýze rizik se používá buď jeden z těchto dvou přístupů, nebo jejich kombinace.

Kvalitativní metody

Kvalitativní metody se vyznačují tím, že rizika jsou vyjádřena v určitém rozsahu (například jsou obodována <1 až 10>, nebo určena pravděpodobností <0; 1> nebo slovně). Úroveň je určována obvykle kvalifikovaným odhadem. Kvalitativní metody jsou jednodušší a rychlejší, ale více subjektivní. Obvykle přináší problémy v oblasti zvládání rizik, při posuzování přijatelnosti finančních nákladů nutných k eliminaci hrozby, která může být kvalitativní metodou charakterizována třeba jako „velká až kritická“. Tím, že chybí jednoznačné finanční vyjádření, se kontrola efektivnosti nákladů znesnadňuje.

Kvantitativní metody

Kvantitativní metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Vyjadřují dopad obvykle ve finančních termínech jako například -tisíce Kč. Nejčastěji je vyjádřeno riziko ve formě roční předpokládané ztráty (anglicky AnnualizedLossExpectancy – ALE), která je vyjádřena finanční částkou. Kvantitativní metody jsou více exaktní než kvalitativní; jejich provedení sice vyžaduje více času a úsilí, poskytují však finanční vyjádření rizik, které je pro jejich zvládání výhodnější.

Nevýhodou kvantitativních metod je kromě jejich náročnosti na provedení a zpracování výsledků často vysoce formalizovaný postup, jenž může vést k tomu, že nebudou postihnuta specifika posuzovaného subjektu, která mohou vést k jeho vysoké zranitelnosti, a to z důvodů „zahlcení“ hodnotitele značným objemem formálně strukturovaných dat. (Dalo by se vyjádřit slovy „kvůli stromům není vidět les.“)

2.1 Kvalitativní metody

Kvalitativní analýza rizik používá slov k popisu rozsahu možných následků a pravděpodobností, že se tyto následky přihodí. Užité škály mohou být přizpůsobeny nebo upraveny tak, aby vyhovovaly okolnostem, a různá rizika mohou být popsána různým způsobem.

Kvalitativní analýza se používá:

- Jako úvodní přehled vedoucí k identifikaci rizik, která vyžadují podrobnější zkoumání.
- Tam, kde tento druh analýzy postačuje k rozhodování.
- Tam, kde číselné údaje nebo zdroje nejsou dostatečné k provedení kvantitativní analýzy.

Kvalitativní analýza by měla obsahovat skutečná fakta a dostupné údaje.

Kvalitativní přístupy a metody mohou být založeny na:

- Hodnocení využívající multioborové skupiny respondentů.
- Hodnocení specialistů a expertů.
- Strukturovaná interview a dotazníky.

Pozitiva tohoto přístupu jsou zejména ve schopnosti hodnotit dopady na organizaci nebo jedince, které nelze elementárně vyjádřit v peněžních jednotkách (jak je běžné u kvantitativních analýz). Hodnocení dopadů kvalitativním přístupem však v dnešních metodikách postrádá konzistentnost a schopnost pokrýt všechny aspekty, podle kterých je nutné dopady hodnotit. V praxi si každý rizikový analytik vytváří vlastní způsoby hodnocení dopadů a i dalších parametrů pro stanovení míry rizika.

Kvalitativní přístup pro hodnocení rizik je teoreticky definovaný, nicméně chybí jasná vazba na praktické využívání ve formě například vodítek hodnocení dopadů nebo detailních návodů na stanovení pravděpodobnosti.

Zejména univerzální vodítka pro hodnocení dopadů mohou dále nabídnout možnost porovnávat dopady a rizika mezi více projekty i organizacemi. V současnosti existuje vysoká poptávka po benchmarkingu, kdy jsou jednotlivá rizika srovnávána skrze více organizací. Například v oblasti bezpečnosti informací jsou na každoročním základě prováděny průzkumy, které odhalují dopady bezpečnostních incidentů nebo porovnávají úroveň a stav bezpečnosti v různých organizacích. Takové srovnání vyžaduje jednotnou metriku a sjednocený pohled na rizika, dopady nebo stanovování pravděpodobností.

2.2 Kvantitativní metody

Kvantitativní metody se ujaly především v oblasti bezpečnosti organizací a jejich informačních systémů – příkladem mohou být metodiky CRAMM, COBRA, MELISA.

Pravděpodobně nejznámější je Metodika CRAMM (CCTA Risk Analysis and Management Methodology) byla původně vyvinuta pro potřeby vlády Velké Britanie, ale v současné době je široce využívána jako uznávaný prostředek pro analýzu rizik v případech, kdy je vyžadován souhlas s normou ČSN ISO/IEC 13335 a mezinárodním standardem ISO/IEC 17799. Analýza v rámci CRAMM řeší ohodnocení systémových aktiv, seskupení aktiv do logických skupin a stanovení hrozeb, působících na tyto skupiny, prozkoumání zranitelnosti systému a stanovení požadavků na bezpečnost pro jednotlivé skupiny, na základě čehož jsou navržena bezpečnostní opatření, která jsou vymezena ve shodě s úrovní rizika při porovnání s již implementovanými systémovými opatřeními. Důležité je, že se vždy zkoumá model určitého systému – nikoliv systém samotný. CRAMM je silně závislý na výsledcích strukturovaných interview s odborníky uživatele. Cena systému je skutečně vysoká, jde o nástroj pro odborníky zabývající se bezpečností, nikoliv pro uživatele ze strany běžných subjektů.

Existují i obecné metodiky pro kvantitativní analýzu rizik, jako:

- @RISK
- RiskPAC

- RiskWatch

2.2.1 @RISK

Metodika využívá k analýze rizik simulačních metod Monte Carlo. Jedná se o zpracování celé problematiky ve formě tabulek. V této metodě se pak nejisté hodnoty zaměňují funkcemi, které reprezentují rozsah možných hodnot. Vybrané souhrnné hodnoty pak představují nástroj pro další rozhodování. Rozhodujícím faktorem této metody je návrh modelu, přičemž vytvořený model definuje danou situaci systému ve formě tabulek. Jedná se vlastně o kvantitativní metodu, která určuje pravděpodobnostní rozdělení hrozeb a rizik.

2.2.2 RiskPAC

Metodika RiskPAC slouží k automatizaci dotazníkových přístupů. RiskPAC umožňuje řešit zpracovanou metodu dotazníkových akcí formou automatizovaného hodnocení. Tento produkt zahrnuje techniky, které zpracovávají odpovědi na základě dotazníků a poskytují podklady pro vytvoření závěrů. V daném procesu se jedná o automatizaci stanovení jednotlivých rizik, nikoliv o expertní systém, pracující na bázi umělé inteligence.

2.2.3 RiskWatch

RiskWatch je programový produkt, který poskytuje metodický soubor pro zjištění, simulaci a následnou změnu parametrů jednotlivých rizik systému. Metoda je založena na vytvoření modelu, postaveném na získaných datech nebo simulační metodě Monte Carlo. Oba přístupy lze vhodně kombinovat a doplňovat. Jedná se tedy o automatizaci zpracování výsledků, získaných na základě souborů otázek, strukturovaných podle definovaných bezpečnostních oblastí.

2.3 Kvalitativní nebo kvantitativní analýza

Analytici upřednostňující kvantitativní přístup oproti kvalitativnímu často argumentují tím, že kvalitativní hodnocení dopadů je prováděno s vysokou mírou subjektivity, kdy výsledná hodnota závisí z velké části na osobním názoru hodnotitele.

Pro stanovení kvantitativní hodnot se využívají definované nástroje (simulace, analýza historických dat a statistik, marketingové průzkumy a analýzy trhu atd.), které však mohou v sobě zahrnovat také jistou míru subjektivity. Odborníci na finance mají k dispozici celou řadu nástrojů na výpočty odhadovaných hodnot, nicméně žádná předpověď rizik i matematicky podložená, nemůže být stoprocentní.

Kvantitativní přístupy využívající finanční škály jsou velmi vhodné, pokud je po provedené analýze nutné najít zdroje na pokrytí zjištěných rizik. Vedoucí projektu mnohem snáze obhájí požadavky na finanční prostředky, pokud je dokáže postavit proti rizikům vyjádřeným finanční ztrátou.

Kvalitativní	
+	-
• Snadná proveditelnost • Rychlost	• Značná subjektivita • Není k dispozici finanční hodnota aktiva • Kontrola efektivnosti nákladů

Tabulka 1: Klady a zápory kvalitativní analýzy

Kvantitativní	
+	-
• Podpora matematického aparátu • Snadná pochopitelnost • Srozumitelnost • Jednoznačnost • Riziko lze snadno vyjádřit v penězích	• Obtížnost • Časová náročnost • Velké ztráty s malou pravděpodobností mají stejný výsledek jako malé ztráty s velkou pravděpodobností

Tabulka 2: Klady a zápory kvantitativní analýzy

Jaký přístup tedy zvolit. Vzhledem k tomu, že tato práce má být především učební pomůckou, bude nejlepší zvolit kombinaci obou metod a přikloníme se k tzv. semikvantitativní analýze. V semikvantitativní analýze jsou výše uvedené kvalitativní

škály doplněny hodnotami. Cílem je vytvořit škály, které jsou podrobnější, než může obvykle poskytnout kvalitativní analýza.

3 JEDNOTLIVÉ FÁZE ANALÝZY

Analýzu můžeme rozdělit do několika základních kroků, které se budou postupem času provádět. Každá fáze se zaměřuje na cílenou skupinu problémů a postupně na sebe navazují. Je tedy potřeba provádět je v daném pořadí a dbát na to aby byly všechny fáze projektu byly pečlivě vypracované. Zdroje pojmenovávají tyto kroky různě, ale v zásadě se jedná o totožné činnosti. My je nazveme následovně:

- Identifikace aktiv
- Pravděpodobnost uplatnění hrozby
- Určení zranitelnosti aktiva
- Vyhodnocení rizik

3.1 Identifikace aktiva

Stanovení odpovědnosti za aktiva napomáhá udržení odpovídající bezpečnosti informací. Musí být identifikovaný vlastník každého identifikovaného aktiva nebo skupiny aktiv a vlastníkovi musí být přiřazena odpovědnost za udržování příslušných nástrojů řízení bezpečnosti. Odpovědnost za implementaci nástrojů řízení bezpečnosti může být delegována, ačkoliv zodpovědnost musí zůstat u určeného vlastníka aktiva.

Identifikace a ocenění aktiv, založené na podnikatelských potřebách organizace, jsou nezbytnými faktory pro posouzení rizik. Aby bylo možné identifikovat vhodnou ochranu aktiv, je nezbytné určit jejich hodnotu z hlediska jejich důležitosti pro podnikání nebo jejich potenciální hodnotu při různých podnikatelských příležitostech. Je také důležité brát v úvahu identifikované právní a firemní požadavky a výsledné dopady při ztrátě důvěrnosti, integrity a dostupnosti.

Jednou z možností, jak vyjádřit hodnotu aktiva, je ocenění dopadů na podnikání, které by mohly mít nežádoucí incidenty, jako prozrazení, pozměnění, nedostupnost a/nebo zničení, na aktivum a související podnikatelské zájmy, které by byly přímo nebo nepřímo poškozeny. Tyto incidenty by mohly následně vést ke ztrátě příjmů nebo zisku, tržního podílu, nebo image a reputace. Všechny tyto faktory se musí odrazit v hodnotě aktiva.

Tedy vše co má pro podnik nějakou hodnotu bude identifikováno. Je třeba brát především důraz na aktiva, u kterých je předpoklad, že bude snížena jejich hodnota v důsledku působení hrozby. Nabízí se otázka jak aktiva členit. Nejjednodušší dělení bude obligátně na hmotná a nehmotná.

Aktiva:

- Hmotná
  - Hardware
  - Software
  - Datové nosiče
- Nehmotná
  - Informace
  - Know-how

Samozřejmě se mohou aktiva informačního systému dělit různými způsoby.

Obrázek 3: Aktiva IS

Výsledkem tohoto snažení by tedy měl být seznam aktiv organizace nebo systému. Předpokládá se, že vzhledem obsáhlosti dokumentu bude více verzí seznamu. V seznamu by mělo být jasně znázorněno, která aktiva jsou pro systém nejhodnotnější.

Co by tedy měl seznam aktiv informačního systému obsahovat:

- určení všech aktiv a jejich vlastníků

- popis jednotlivých aktiv a vazeb mezi nimi
- seskupení aktiv
- ohodnocení aktiv

V této fázi projektu se předpokládá největší zapojení spolupracovníků zadavatele analýzy.

3.1.1 Určení a aktiv a přiřazení ke vlastníkům

Jedním z největších problémů tohoto kroku je určení vlastníka aktiva. Přitom se jedná o klíčový element analýzy a proto je mu potřeba věnovat patřičnou pozornost. Mnohým manažerům právě určení vlastníků dělá nemalé potíže a představuje pro ně jen velice těžko řešitelný problém. Kdo je tedy vlastníkem aktiva? Logicky by jím měl být ten kdo, kdo data vytváří a přebírá zodpovědnost za jejich správnost, věrnost, spolehlivost a provádí jejich klasifikaci. Zároveň by měl být vlastník ten, který přiřazuje a povoluje přístup k informacím a definuje rozsah přístupu.

Hlavní zásadou je fakt, že vlastník dat by měl být pouze jeden. Od vlastnictví se odvíjí celá řada činností analýzy, např. komu se mají prezentovat výsledky a podobně. Vlastník by tedy měla být určitá organizační jednotka nebo role v systému, nikoli osoba. K roli by mělo být samozřejmě přiřazeno konkrétní jméno, protože je zde jistá pravděpodobnost, že pracovník může opustit příslušnou pozici. Aktivum by po té zůstalo bez vlastníka.

Co tedy potřebujeme k naplnění tohoto cíle. Je nutný popis procesů a jednotlivých vazeb mezi nimi. Rozšiřují totiž pohled na rizika a mohou být používány i pro další identifikaci rizik a to nejen v oblasti informačních technologií. Potom by mělo následovat postupné seřazení procesů a k nim by měla bát přiřazena aktiva, která jsou při procesech používána.

Nejlepším zdrojem by mohly být dotazník, který by po schválení vedení společnosti byly vyplněny příslušnými manažery.

3.1.2 Popis a vazby mezi aktivy

Nyní můžeme přistoupit k popisu systému a definování jeho vazeb. Budeme systém rozebírat shora a pokusíme se ho rozčlenit na jednotlivé objekty, které můžeme později označovat jako aktiva. Tento přístup se nazývá objektová hierarchická dekompozice aktiv. Pro tento účel si procesy rozdělíme po třech vrstev:

- Organizační vrstva
- Logická vrstva
- Fyzická vrstva

3.1.2.1 Organizační vrstva

Nositel každého procesu, který byl identifikován manažerem, jsou lidé. Je tedy nutné určit jednotlivé uživatele systému a graficky znázornit vztahy mezi nimi. Předpokládá se aktivní zapojení respondentů z businessu.

3.1.2.2 Logická vrstva

V této vrstvě bychom již měli pojmenovat konkrétní operační systémy a pod nimi pracující aplikace a popsat informační toky mezi aplikacemi. Zde by již měli respondenty z businessu doplňovat kolegové z ICT.

3.1.2.3 Fyzická vrstva

Vychází z logické vrstvy, jsou do ní ale už začleněny konkrétní hardwarové komponenty. V této vrstvě se předpokládá aktivní zapojení ICT pracovníků. Nyní bychom měli mít dispozici aktiva a vztahy mezi nimi.

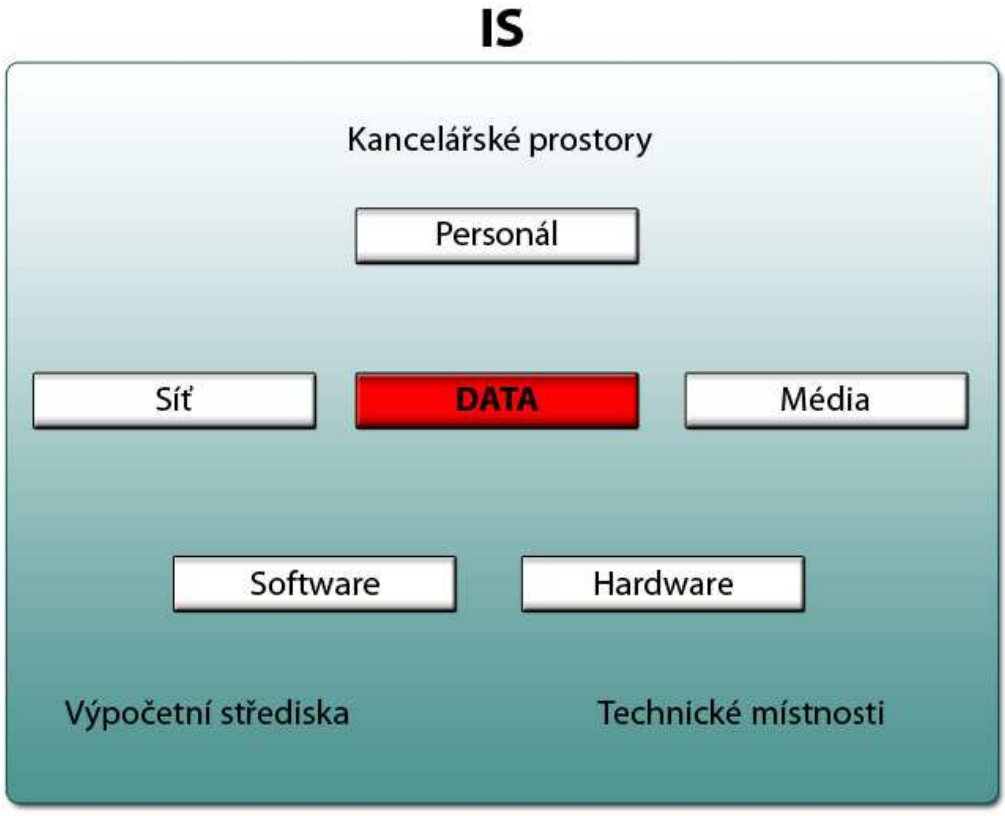
3.1.3 Seskupení

V tomto okamžiku, když jsme identifikovali všechna aktiva, která hrají roli v naší analýze rizik, je potřeba je začlenit do určitých bloků. Seskupuje je především pro potřeby jejich hodnocení vůči hrozbám a jejich zranitelnosti. Čím víc aktiv budeme mít, tím více času bude potřeba projektu věnovat. Aktiva tedy uspořádáme na základě jejich vlastností a účelu použití.

Po uspořádání do bloků budeme k těmto blokům přistupovat jako jednomu aktivu. Extrémem a zároveň pastí může být hodnocení celého informačního systému jako jednoho aktiva, což je velice nešťastné. Tato možnost na jednu stranu urychlí celou analýzu, ale zároveň přináší podstatné problémy při fázi zvládání rizik. Dále je nutné brát v potaz při stavení hodnoty aktiva, která jsou v příslušném bloku obsažena.

Po seskupení si tedy můžeme definovat na kterých aktivech je každý proces více či méně závislý:

- Hardware
- Software
- Síť
- Média
- Data
- Personál
- Prostory



Obrázek 4: Obecný model informačního systému

3.1.4 Ohodnocení aktiv

V okamžiku, kdy v rámci analýzy rizik provádíme hodnocení aktiv, klademe si obvykle otázku, jaký by byl finanční a nefinanční dopad v případě, že by došlo k narušení důvěrnosti, integrity a dostupnosti těchto aktiv. V případě dostupnosti datových aktiv bychom měli sledovat dvě hodnoty a to RPO (Recovery Point Objective) a RTO (Recovery Time Objective). Běžně se však hodnota dopadu stanovuje jen na základě RTO. Takovýto přístup však nemusí být zrovna ten nejvhodnější. Vždy bychom si měli položit tyto dvě otázky:

RTO

Jaké by byly finanční a nefinanční dopady, kdyby data, která jsou předmětem hodnocení, nebyla dostupná po dobu několika:

- sekund
- minut
- hodin
- dní

RPO

Jaké by byly finanční a nefinanční dopady, kdyby došlo ke ztrátě dat za posledních několik:

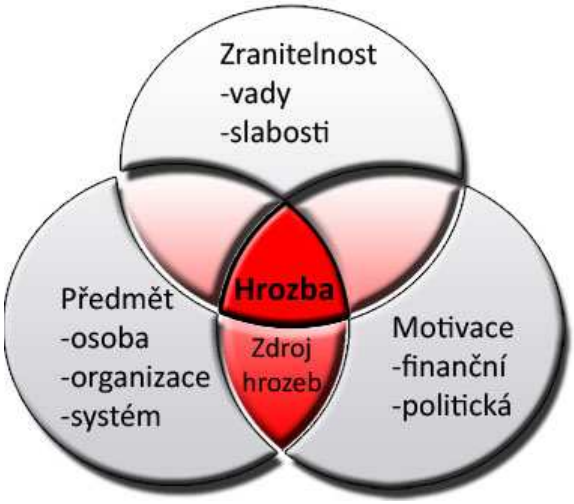
- sekund
- minut
- hodin
- dní

Všimněte si, že se jedná o dvě naprosto rozdílné otázky. Zatímco v prvním případě uvažujeme, že data nebudou dostupná jen po danou dobu, ve druhém případě o data za dané období přijdeme. Vidíme, že hodnota dopadu, co se týká dostupnosti datových aktiv, může teoreticky nabývat až 8 různých hodnot (4 x RPO + 4 x RTO).

Na základě znalosti vztahu mezi hodnotami RTO a RPO můžeme ve fázi zvládání rizik volit vhodná opatření pro zajištění požadované dostupnosti dat.

3.2 Pravděpodobnost uplatnění hrozby

Obecně hrozbu definujme jako potenciálně ničivou fyzikální událost, jev nebo lidskou aktivitu, která může zapříčinit ztrátu životů nebo zranění, škody na majetku, sociální a ekonomické poruchy nebo environmentální znehodnocení.



Obrázek 5: Definování hrozby

My budeme hrozbu definovat jako náhodnou nebo úmyslně vyvolanou událost, která má negativní dopad na důvěrnost, integritu a dostupnost aktiv, která jsou předmětem našeho zájmu.

Aktiva jsou předmětem mnoha druhů hrozeb. Hrozba může způsobit nežádoucí incident, který může mít za následek poškození organizace a jejích aktiv. K tomuto poškození může dojít v důsledku útoku na informace organizace a výsledkem může být např. nedovolené prozrazení, modifikace, zkomolení, zničení, nedostupnost nebo ztráta informací. Hrozby mohou vzniknout z náhodných nebo úmyslných příčin nebo událostí. Hrozba by vyžadovala využití jedné nebo více zranitelností systémů, aplikací nebo služeb využívaných organizací, aby úspěšně zapříčinila poškození aktiva. Hrozby mohou mít původ z prostředí uvnitř organizace, ale také z vnějšku.

Pro identifikaci hrozeb lze vycházet ze seznamu hrozeb, sestavených podle literatury, vlastních zkušeností, průzkumů dříve provedených analýz. Hrozby se mohou odvozovat také od subjektu, jeho statusu (podnikatelský subjekt, orgán státu, nezisková organizace, atd.), postavení na trhu, hospodářských výsledků, záměrů podnikatele. Pro získání

vlastního seznamu hrozeb subjektu je vhodné použít některou z metod jako brainstorming, metoda Delphi apod.

Je třeba poznamenat, že hrozby a zranitelnosti musí působit současně, aby způsobily incidenty, které by mohly poškodit aktiva. Je proto nezbytné pochopit vztah mezi hrozbami a zranitelnostmi, tj. jaká hrozba může těžit z určité zranitelnosti.

Po dokončení této fáze bychom měli mít k dispozici seznam všech hrozeb, které by mohly působit na sledovaná aktiva. Seznam by měl obsahovat:

- Hrozby a jejich původ
- Aktiva, na které hrozby působí
- Atributy jaké bezpečnostní hrozba působí
- Hodnocení hrozeb
- Nejvíce ohrožující hrozby pro systém.

Tuto část projektu rozdělíme do dvou kroků. Bude to identifikace a kvantifikace hrozeb.

3.2.1 Identifikace hrozeb

Jak už jsme si uvedli výše, hrozby mohou být z vnějšího prostředí organizace nebo z vnějšího prostředí. Zároveň působení hrozby na aktiva může být dočasné nebo trvalé a navíc se může v čase měnit. Důležité je také, na která aktiva hrozba působí, atribut bezpečnosti hrozby a co je zdrojem hrozby.

Dle původu může dělit hrozby:

- Hrozby prostředí
    - Požár
    - Blesk
    - Zemětřesení
    - Sopečná činnost

    - Svahové pohyby
    - Povodně
    - Tsunami
- Hrozby způsobené lidmi
    - Úmyslné
        - Zničení
        - Poškození
        - Krádež
    - Neúmyslné
        - Chyba uživatele
        - Chyba správce systému

Důležité je také uvědomit si, že jedna hrozba může působit na více aktiv, a zároveň také jedno aktivum může být vystaveno současnému působení více hrozeb. Hrozby působí na aktiva přímo nebo nepřímo.

Další možné dělení hrozeb je podle dopadu na systém. Toto dělení již není tak časté, ale umožňuje určit, na jaký atribut bezpečnosti (důvěrnost, integrita, dostupnost) hrozba působí:

- aktivní hrozby – dochází ke změně stavu systému v důsledku narušení integrity a dostupnosti
- pasivní hrozby – nedochází ke změně stavu systému, dochází k úniku informací

Pro vlastní provedení analýzy rizik nemá výše uvedené dělení hrozeb příliš velký smysl. Ovšem v okamžiku, kdy se definuje hloubka analýzy rizik, může být takovéto dělení přínosem, neboť je tímto způsobem možné přibližně vymezit typ hrozeb, které budou předmětem analýzy. Stejně tak nám ve fázi vyhodnocení rizik může zařazení hrozby do odpovídající kategorie poskytnout zajímavý obrázek o tom, který typ hrozeb představuje pro společnost největší riziko. Vzhledem k tomu, že ne všechna aktiva jsou vystavena působení všech hrozeb, je vhodné hrozby seskupit podle toho na jaké aktivum působí:

- operační systém
- aplikace

- databáze
- síť
- klient

V okamžiku, kdy budeme posuzovat míru zranitelnosti aktiva vůči působení hrozby, již nebudeme ztrácet čas vyhodnocováním, zda je daná hrozba relevantní či nikoliv.

Nejčastější hrozby, které nás z hlediska informačního systému zajímat jsou následující:

Selhání dodávky energie - selhání dodávky energie může způsobit problémy z hlediska integrity a následně může způsobit i další poruch (selhání HW apod.). Selhání dodávky se samozřejmě netýká jen vlastního HW, ale také klimatizace, celého síťového prostředí, zálohování podobně.

Škodlivý software - škodlivý software může být použit ke zmaření autentizace a všech souvisejících služeb a bezpečnostních funkcí. Ve svém důsledku může vést ke ztrátě dostupnosti, jestliže jsou např. data nebo soubory zničeny osobou, která získala neautorizovaný přístup pomocí škodlivého programového kódu, nebo vlastním škodlivým programovým kódem.

Selhání hardwaru - technické poruchy, např. v síti, mohou zničit dostupnost jakékoliv informace, která je uchovávána nebo zpracovávána v této síti. Mezi nejčastější příčiny selhání hardware patří například nedostatečná údržby, nejasné postupy při údržbě HW, nevhodné prostředí umístění HW (vlhkost, prach, výkyvy teploty apod.)

Selhání komunikačních služeb - chyby a poruchy komunikačních zařízení a služeb ohrožují dostupnost informací přenášených prostřednictvím těchto služeb. V závislosti na příčině chyby nebo poruchy.

3.2.2 Kvantifikace hrozeb

V tomto kroku se vyhodnotí hrozby, které byly identifikovány a ohodnotí se. Stanovíme si tedy úroveň hrozby pro každé aktivum, na které působí hrozba. Neexistuje přesný postup jak hodnotit hrozby. Výsledná úroveň je tedy ještě více závislá na hodnocení osoby, která ho provádí. Při stanovování úrovně rizik můžeme vycházet ze statistik nebo evidence dosavadních bezpečnostních incidentů. Pokud nemáme evidenci k dispozici, můžeme spolupracovat s organizacemi, které jsou nám podobné např. v lokalitě, velikosti, firemní kultuře, předmětu činnosti, zavedených procesech. Dalším zdrojem mohou být různé průzkumy, které můžeme provést např. dotazníkovým šetřením.

Pro účely stanovení úrovně hrozeb si hrozby rozdělíme do těchto skupin:

- přírodního původu
- technické selhání
- lidská chyba
- hacking
- sabotáž

Pokud máme stanovit míru hrozby, musíme zohlednit následující faktory:

- četnost výskytu
- příležitost
- motiv
- schopnosti
- peníze
- vybavení
- čas
- atraktivitu aktiva
- počet osob
- stáří aktiva

Četnost výskytu - U všech typů hrozeb můžeme pro stanovení míry hrozby vzít v úvahu četnost výskytu, ať už ze statistik, nejrůznějších průzkumů informační bezpečnosti nebo z ještě lépe z vlastní pečlivě vedené evidence bezpečnostních incidentů. Tímto způsobem můžeme poměrně spolehlivě určit pravděpodobnost výskytu dané hrozby.

Příležitost - Pravděpodobnost realizace hrozby je tím vyšší, čím vyšší je příležitost danou hrozbu realizovat. Pokud zaměstnanci denně přichází do styku s důvěrnými informace a ví, že jejich činnost v systému není monitorována, je větší pravděpodobnost, že některý z nich svého přístupu do systému zneužije a dojde tak např. k úniku informací.

Motiv - Motiv útočníka může být různý a někdy i těžko pochopitelný. Podstatné však je, že pravděpodobnost realizace hrozby je vyšší v době krize, fůzování, outsourcingu. To je dáno tím, že lidé v tomto období velice často přicházejí o místo a svůj příjem. Mohou se chtít pomstít nebo si „jen“ odnést něco, co se dá snadno zpeněžit nebo využít v novém zaměstnání.

Schopnosti - To, že jsou schopnosti uvedené jak u lidského selhání, tak i hackingu a sabotáže není náhoda. Vycházíme z toho, že méně chyb obvykle dělá člověk, který své práci rozumí. U hackingu a sabotáže zase předpokládáme, že pravděpodobnost dané hrozby bude vyšší v případě, kdy žádné speciální znalosti, schopnosti a dovednosti nejsou k realizaci hrozby potřeba.

Peníze - Pravděpodobnost hrozby je tím vyšší, čím nižší jsou náklady na její realizaci. Je to v celku logické, protože i útočník zvažuje, zdali se mu vyplatí do přípravy a realizace útoku investovat své prostředky.

Čas - Pravděpodobnost hrozby je tím vyšší, čím kratší je doba potřebná k přípravě a vlastní realizaci dané hrozby. To je dáno tím, že čím rychleji je možné daný útok provést, tím nižší je pravděpodobnost, že si někdo přípravy nebo vlastního provedení útoku všimne.

Vybavení - Pravděpodobnost hrozby je tím vyšší, čím jsou nižší nároky na HW a SW vybavení útočníka. Je rozdíl, zda nástroj k realizaci hrozby je možné stáhnout z internetu nebo je nutné ho vyvinout.

Atraktivita - Čím atraktivnější cíl, tím vyšší pravděpodobnost hrozby. Když chce hacker provést např. defacement vybere si spíš takový server, který je hodně navštěvován a znám, než web, na který nikdo nechodí. Je to podobné jako u zlodějů aut, jestliže se takový zloděj má rozhodnout, zda ukradne Jaguára nebo Trabanta, které auto to bude? Samozřejmě můžete namítnout, že Škodovka, protože těch je víc a nebude v ní budit takovou pozornost.

Počet osob - Čím větší počet osob přichází s hodnoceným aktivem do styku, tím větší je pravděpodobnost, že někdo z nich hrozbu realizuje. Podle jedné studie je v každé společnosti 10% lidí absolutně poctivých, 10% absolutně nepoctivých a ostatních 80% se nachází někde mezi nimi.

Stáří aktiva - To, že je stáří aktiva posuzováno i u lidí, není chyba. Možná to zní trochu cynicky, ale v obou případech je pro stanovení pravděpodobnosti selhání nebo chyby možno použít vanovou křivku, jen bude mít u různých aktiv trochu jiný průběh (např. nezkušený zaměstnanec – zkušený zaměstnanec – opotřebovaný zaměstnanec).

Vytvoříme si proto matici, která bude zachycovat, které faktory je třeba vzít při hodnocení jednotlivých hrozeb v úvahu.

Faktor/hrozba	Přírodní původ	Technické selhání	Lidská chyba	Hacking	Sabotáž
Četnost výskytu	x	x	x	x	x
Příležitost				x	x
Motiv			x	x	x
Schopnosti			x	x	x
Peníze				x	x
Čas				x	x
Vybavení				x	x
Atraktivita aktiva				x	x
Počet osob				x	x
Stáří aktiva		x	x	x	x

Tabulka 3: Faktory pro hodnocení hrozeb

Stanovení výsledné míry hrozby pro konkrétní dvojici hrozba – aktivum není triviální. V případě hrozby přírodního původu je určení míry hrozby poměrně snadné, neboť nám k jejímu stanovení stačí určit pravděpodobnost výskytu dané hrozby. V případě technického selhání můžeme kromě statistik vyjít i ze stáří aktiva a míru hrozby stanovit podle toho, v jakém bodě vanové křivky se právě nacházíme. V případě lidského selhání je možné též vyjít ze statistiky a vzít v úvahu aktuální náladu ve společnosti a kvalitu lidské obsluhy a určit trend.

V případě hodnocení úmyslných hrozeb však narazíme na problém. I kdybychom vzali v úvahu jen 3 nejčastěji uváděné faktory jako je schopnost, příležitost a motiv, znamená to zkoumat 7 různých kombinací a posoudit, která z nich je závažnější. V případě, že bychom chtěli vzít v úvahu všech 9 výše uvedených faktorů, které při hodnocení pravděpodobnosti realizace úmyslné hrozby připadají v úvahu, dostali bychom se na 511 různých kombinací. (Z čistě matematického pohledu se jedná o kombinace bez opakování, jejichž počet lze snadno spočítat.) Z tohoto pohledu se jeví vyhodnocení trendu a náročnosti provedení útoku jako zcela dostačující k určení pravděpodobnosti realizace dané hrozby.

Vycházíme z toho, že v době, kdy se členem organizované skupiny může stát v podstatě kdokoliv, vždy se najde někdo, kdo má motiv, příležitost, schopnosti a prostředky. Ostatní výše uvedené faktory je tedy třeba brát pouze jako doplňkové nebo se jimi vážně zabývat pouze v okamžiku, kdy statistické údaje nejsou k dispozici.

Co se týká kombinace jednotlivých faktorů, problém spočívá v tom, jak hodnotit např. takovou kombinaci, kdy bude pro jednu hrozbu splněna podmínka motivu a příležitosti, zatímco pro druhou naopak bude existovat příležitost a schopnost. Která hrozba bude v takovém případě závažnější? Jak spočítat míru hrozby? Je lepší vyhodnotit každý faktor a pak spočítat průměr? Nebo je vhodnější přidělit jednotlivým faktorům různé váhy?

Stanovení míry hrozby na základě četnosti výskytu dané hrozby je managementem obvykle akceptováno, neboť se tento způsob opírá o matematický aparát a míru hrozby je tak možné jednoduše vysvětlit a obhájit.

3.3 Zranitelnosti aktiva

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.

Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva se hodnotí podle následujících faktorů:

- Citlivost: náchylnost aktiva být poškozeno danou hrozbou.
- Kritičnost: důležitost aktiva pro analyzovaný subjekt.

Zranitelnost je tedy citlivost aktiva na působení hrozby. Je nutno počítat s tím, že pro každé aktivum existuje nějaké zranitelné místo, neboli existuje slabina aktiva, která může být využita ke způsobení škod nebo ztrát na tomto či jiném aktivu. Zranitelné místo je vlastně vždy jednou z vlastností informačního systému. Takové zranitelné místi může být:

- Fyzické, kdy je prvek informačního systému fyzicky umístěn v prostředí, ve kterém může snadno dojít k jeho poškození, zničení nebo ztrátě.
- Přírodní, kdy prvek informačního systému nemá schopnost vyrovnat se s některými objektivními faktory, jako je záplava, požár, blesk a podobně.
- Technologické, kdy prvek informačního systému svými konstrukčními charakteristikami neumožňuje zajistit například požadovaný trvalý plynulý provoz.
- Fyzikální, kdy prvek informačního systému pracuje na takových principech, které umožňují jejich zneužití. Příkladem může být elektromagnetické vyzařování některých zařízení, jako jsou monitory, kabeláž komunikační sítě a podobně.
- Lidské, kdy prvek informačního systému je ohrožen působením lidí, jejich omylů a neznalostí.

V této fázi se tedy zaměříme na vytvoření seznamu zranitelností, které jsou charakteristické pro sledovaná aktiva. Seznam by měl obsahovat:

- Seznam identifikovaných opatření

- Popis opatření a jaká aktiva před kterými hrozbami chrání
- Míru zranitelnosti pro každou dvojici hrozba – aktivum
- Znázornění největších zranitelností

3.3.1 Identifikace zranitelností

V tomto kroku projektu se pokusíme identifikovat všechna slabá místa na několika úrovních. Budeme se zabývat úrovní fyzické, logické, organizační, personální a technické bezpečnosti, která by mohla být zneužita hrozbou. Míra zranitelnosti je spojena především k úrovni stávajících bezpečnostních opatření, proto budeme míru zranitelnosti vztahovat přímo k nim.

Jednou z prvních činností, kterou bychom tedy měli provést, je prostudování příslušné dokumentace (politika, technická specifikace). Poté přistoupíme ke kontrole jednotlivých opatření.

3.3.2 Kvantifikace zranitelností

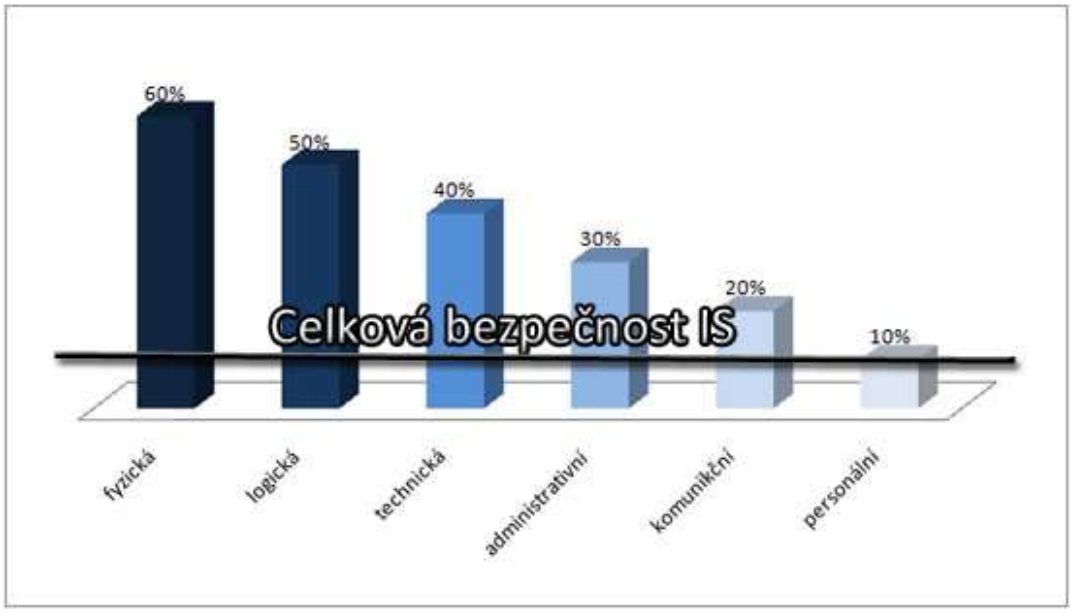
Jak už jsme si uvedli výše, při stanovování míry zranitelnosti ho budeme posuzovat vzhledem k prostředí a stávajícím protiopatřením, která mohou snižovat úroveň zranitelnosti. Postupujeme tedy tak, že se snažíme pro každou dvojici hrozba - aktivum respektive hrozba – skupina aktiv posoudit, nakolik je aktivum vůči působení dané hrozby odolné a to tak, že budeme posuzovat úroveň stávajících opatření. Měli bychom tedy zkontrolovat všechna implementovaná opatření a prověřit, zda pracují správně a efektivně.

Při určování hodnoty zranitelnosti je nutné brát v potaz prostředí, ve kterém se informační systém nachází. Prostředí se rychle mění a opatření jsou vystavena ve větší či menší míře působení hrozeb. Je tedy nutné posoudit proces zavádění těchto opatření. Pro tento účel využijeme pozměněnou stupnici vyzrálosti procesů:

0. Není zavedeno žádné opatření – pokud není opatření zavedeno, je téměř jisté, že hrozba se uplatní a můžeme proto hovořit o kritické zranitelnosti.

1. Opatření nejsou zdokumentována – opatření jsou zavedena, ale tím že nejsou zdokumentována, je pravděpodobné, že je ani nikdo nezkontroluje, dá se proto předpokládat, že dojde k uplatnění hrozby, zranitelnost je kritická.
2. Opatření jsou zdokumentována – vzhledem k tomu, že neprobíhá kontrola funkčnosti těchto opatření a už vůbec nedochází k jejich zlepšování, dá se předpokládat, že dojde k uplatnění hrozby, zranitelnost je vysoká.
3. Opatření jsou zdokumentována, kontrolována – lze předpokládat, že nefunkční opatření se povede v čas odhalit a hrozba tak nebude mít příležitost se uplatnit, ale vzhledem k tomu, že nedochází ke zlepšování opatření, nebude opatření dostatečně účinné proti novým zranitelnostem, zranitelnost je střední.
4. Opatření jsou zdokumentována, kontrolována a dochází k jejich průběžnému zlepšování – hrozba nebude mít s největší pravděpodobností příležitost se uplatnit, zranitelnost je nízká.

Je důležité si uvědomit, že některé hrozby a zranitelnosti je potřeba snižovat pomocí více opatření, a proto bychom měli vzít v úvahu fakt, že celý systém je tak bezpečný, jak je bezpečný jeho nejslabší článek. Výslednou hodnotu zranitelnosti bychom proto měli stanovit s ohledem na tuto skutečnost.

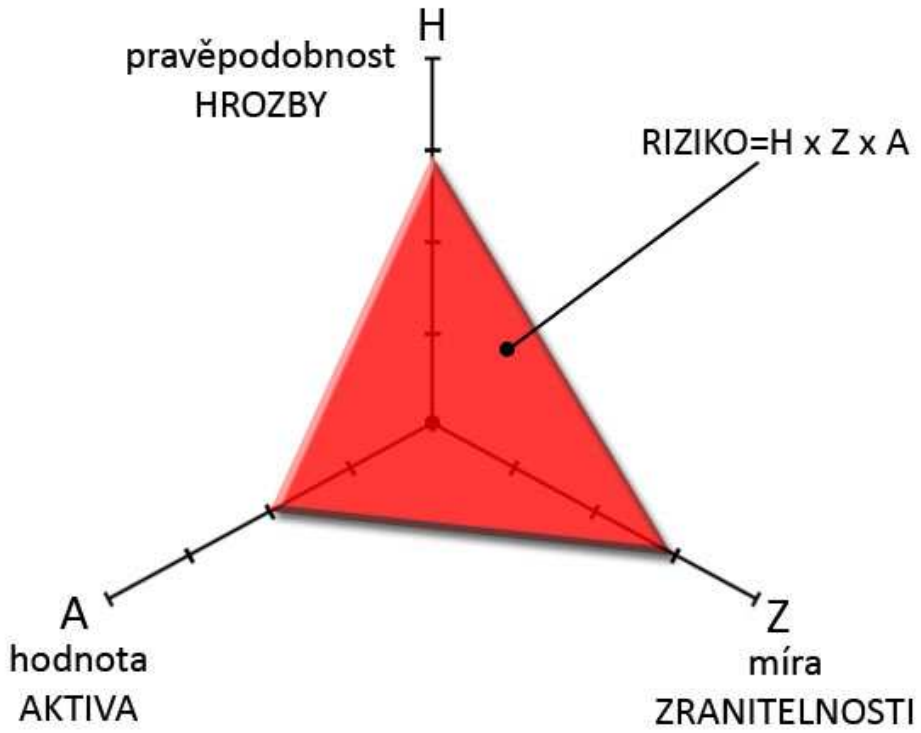


Obrázek 6: Úroveň bezpečnosti IS (maximální úroveň představuje 100%)

3.4 Vyhodnocení rizik

V této fázi analýzy se tedy budeme věnovat vyhodnocení všech rizik. Jedním z nejdůležitějších bodů této části projektu je uvědomit si, jaká je závislost mezi hodnotou aktiva, hrozbou a jeho zranitelností. Později zjistíme fakt, že čím vyšší je hodnota aktiva, hrozby a zranitelnosti, tím vyšší je i riziko.

Riziko vyjadřuje v číselné hodnotě míru zneužití určité zranitelnosti konkrétní hrozbou, jejímž důsledkem je dopad na uvažovaná aktiva. Matematicky je riziko dáno funkcí R (A, H, Z) tří proměnných (A, H, Z), které po řadě reprezentují jednotlivá aktiva, hrozby a zranitelnosti.



Obrázek 7: Matematické vyjádření rizika

Výpočet výše rizika R pro každou trojici aktiva, hrozby, zranitelnosti je dáno vztahem:

$$R = H \cdot Z \cdot A$$

A- Hodnota aktiva

H- Výše hrozby pro aktivum

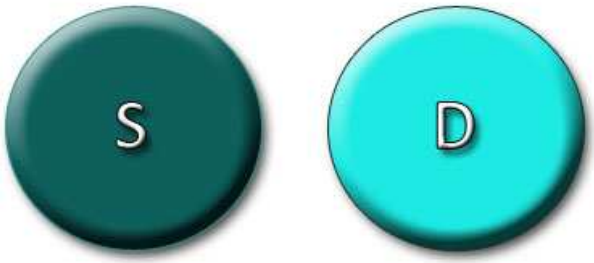
Z- Výše zranitelnosti vzhledem k hrozbě

Funkce R nabývá celočíselných hodnot z intervalu <0,100>. To je dáno rozsahem vstupních hodnot, kde hodnota aktiva je celé číslo z intervalu <0,100>, výše hrozby je číslo z intervalu <0,1> a výše zranitelnosti je též číslo z intervalu <0,1>. Z hlediska výše rizika lze riziko označit jako nízké, střední, vysoké a kritické. Zařazení rizika do jedné z těchto kategorií je dáno výsledkem výše uvedené funkce, která určuje, do jakého pásma riziko spadá. Rizika by měla být zvládána postupně od těch nejkritičtějších, kde je nutné okamžité rozhodnutí managementu, přes vysoká a střední, kde je možné jejich zvládání naplánovat, až po nízká, která je možno akceptovat a dále jen monitorovat.

3.4.1 Vyhodnocení opatření

V zásadě můžeme rozeznat několik možností, jak mohou být opatření účinná. Budeme k nim tedy přistupovat jako ke dvěma množinám. Jednu množinu budou tvořit stávající (S) opatření, a druhou ta doporučená (D).

Stávající opatření v žádném bodě neodpovídají doporučeným opatřením.

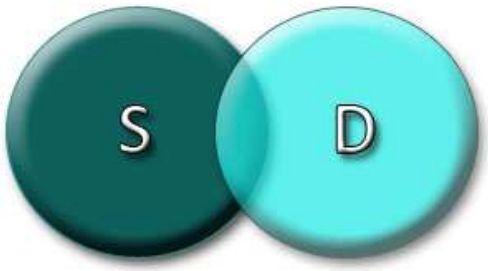


Obrázek 8: Vyhodnocení opaření případ 1

Na první pohled je zřejmé, že v minulosti byla implementována zcela jiná opatření než doporučená. K této situaci obvykle dochází, když nejsou v rámci analýzy rizik identifikovány hrozby nebo se analýza vůbec neprovádí. Stávající opatření nevedou ke

snížení zranitelnosti a tedy k ochraně aktiv před působící hrozbou. Je třeba si uvědomit, že tato nevhodná opaření zvyšují i náklady, neboť i jejich provoz něco stojí.

Stávající opatření v jen v některých bodech odpovídají doporučeným opatřením.



Obrázek 9: Vyhodnocení opaření případ 2

Jedná se o něco lepší případ než ten předchozí. Přesto se nabízí otázka, zda stávající opatření byla vybrána na základě analýzy nebo zcela náhodně. Může se jednat a často se jedná o základní sadu opatření.

Doporučená opatření jsou podmnožinou stávajících.

Obrázek 10: Vyhodnocení opaření případ 3

V tomto případě je nutné se ptát, proč rozsah stávajících opatření je větší než opatření doporučená. K této situaci často dochází v okamžiku, kdy se neprovádí identifikace

kvantifikace aktiv a přijímací se všechna opatření bez ohledu na to, zda jsou opravdu potřeba.

Stávající opatření jsou podmnožinou doporučených.

Obrázek 11: Vyhodnocení opaření případ 4

Ideální případ. Zbývá se jen zamyslet nad doplněním stávajících opatření o doporučovaná.

Doporučená opatření odpovídají stávajícím.

Obrázek 12: Vyhodnocení opaření případ 5

Všechna opatření jsou již nasazena. Ideální případ, který v reálné praxi obvykle nenastává, ale můžeme se alespoň snažit se mu přiblížit.

3.4.2 Výběr vhodných opatření

Ve skutečném systému je potřeba kombinovat více opatření, z nichž každé má jasně dané určitou úlohu. Nejčastěji se jedná o opatření, která vedou k:

- Odstrašení od útoku
- Zdržení útoku
- Detekci útoku
- Reakci na útok
- Obnově po útoku

Je zde ale fakt, že účinnost opatření nebude nikdy 100% a účinnost se postupně snižuje. Každé opaření má nějakou díru, kterou může hrozba zneužít.

Výběr vhodného opaření je velice komplikovaná činnost. Je nutné posoudit efektivitu opatření, náklady a jeho celkový přínos. Efektivita protiopatření určuje, nakolik protiopatření sníží účinek hrozby nebo zranitelnosti. Při určování nákladů je nutné přičíst k nákladům na pořízení a zavedení i náklady provozování daného opatření. Celkový přínos je tedy dán efektivitou protiopatření, náklady a vlastností snižovat současně více hrozeb nebo zranitelností. Máme tedy možnost vybrat takové protiopatření, které se sice při prvním pohledu jeví jako dražší, ale při hodnocení zjistíme, že je cenově výhodnější.

Je třeba brát také v potaz omezení, které může systém nebo podnik mít:

- Finanční – nemáme k dispozici do finančních prostředků
- Technická – opatření nelze nasadit
- Časová – opatření musí být realizováno do určitého termínu
- Právní – zákon nasazení opatření neumožňuje
- Prostředí – v daném prostředí nelze
- Kulturní
- Politická
- Sociální – mohlo by vyvolat nežádoucí reakce

Ve většině případů budeme tedy hledat opatření proti úmyslným a náhodným lidským a přírodním hrozbám a selhání technologie, které mohou v konečném důsledku vést k narušení integrity, důvěrnosti a dostupnosti aktiva.

Obrázek 13: Vztah mezi aktivem, zranitelností, opatřením a hrozbou

Stupnice pro hodnocení opatření je v podstatě analogická se stupnicí hrozeb a zranitelností. Účinnost opatření nabývá hodnot intervalu <0,100>. Opatření s největším přínosem je levné, lze ho snadno a rychle zavést a co nejvíce minimalizuje jedno nebo více rizik. Hodnota opatření se potom pohybuje v blízkosti horní hranice intervalu.

Jednou z nutností je vybírat taková opatření, která jsou vhodná pro konkrétní situaci a organizaci, a umět vysvětlit, proč zrovna toto opatření je nejvhodnější. Výběr by měl být tudíž proveden specialisty na danou oblast a je vhodné, když vychází z norem, standardů a zjištění již existujících opatření.

Po dokončení této fáze tedy máme seznam opatření, kde by měly být následující informace:

- Jednoznačná identifikace opatření.
- Název opatření.

- Stručný popis opatření.
- Jak lze opatření měřit.
- Jaké hrozby nebo zranitelnosti opatření snižuje.
- Osoba zodpovědná za zavedení opatření.
- Obtížnost zavedení opatření.
- Čas nutný k zavedení opatření.
- Účinnost opatření.
- Náklady na zavedení opatření.
- Priorita opatření.

II. PRAKTICKÁ ČÁST

4 KONKRÉTNÍ POSTUP ANALÝZY RIZIK IS

Tato práce má za cíl především poskytnout detailní pohled studentům na analýzu rizik a problematiku jejího vytvoření. Pro správné pochopení analýzy je tedy nutné si detailně vysvětlit fáze jejího vzniku a podrobně popsat, jak jsme získali příslušné dokumenty. Je třeba si uvědomit, že existuje mnoho metod a postupů pro vytvoření analýzy a každý podnik či firma bude upřednostňovat jinou metodiku. Uvedené postupy byly vybrány s ohledem na jejich srozumitelnost a názornost, které jsou u této práce prioritou.

Každá kapitola obsahuje tedy konkrétní postup příslušné fáze analýzy. Tyto fáze jsou již teoreticky popsány v teoretické části práce, budeme se na ně tedy často odkazovat. Proto jsou použité názvy kapitol totožné jako v teoretické části.

Činnosti, které tedy povedou k vytvoření analýzy rizik, budou:

- Aktiva
  - Identifikace
  - Rozdělení identifikovaných aktiv
  - Ohodnocení rozdělených aktiv
- Hrozby
  - Identifikace
  - Hodnocení hrozeb a jejich dopadů na aktiva
- Zranitelnosti
  - Identifikace
  - Hodnocení zranitelností
- Rizika
  - Vyhodnocení rizik
  - Vyhodnocení opatření
- Závěrečná zpráva

5 AKTIVA

5.1 Identifikace aktiv

Přistoupíme tedy k identifikaci aktiv a procesů. Následující kroky mají za cíl vytvořit seznam aktiv, která jsou předmětem analýzy. Pro provedení těchto činností je potřeba podpora vrcholového managementu podniku a účast manažerů zodpovědných za útvary, jejichž procesy a aktiva se budou zkoumat.

Tuto fázi si rozdělíme do několika kroků s ohledem na to, kdo ji bude provádět a jaký je její výsledek. Jsou to tyto činnosti:

- Vytvoření dotazníku pro identifikaci aktiv.
- Vysvětlení dotazníku uživatelům a jeho následné vyplnění.
- Vytvoření seznamu aktiv na základě vyplněných dotazníků

5.1.1 Dotazník pro identifikaci aktiv

Každý podnik a v něm IS mají alespoň trochu rozdílnou strukturu a procesy, které se zde uskutečňují. Podle toho jaké jsou možnosti, vytvoříme dotazník, který nám co nejlépe podá informace, které potřebujeme k identifikaci. Kromě přímého určení aktiva, je neméně důležité získat informace o procesech, manažerovi a části podniku, pod který aktivum spadá.

Přiložený návrh je pouze informativní. Dotazníky můžou být o poznání obsáhlejší a mohou se lišit. My se přikloníme k tomuto návrhu, protože se dotazuje přesně na ty informace, které považujeme za klíčové a zároveň je jednoduchý a přehledný. Posledně uvedený fakt, je výhodou hlavně z důvodu pozdějšího vyplnění uživateli.

Velkou výhodou a úsporou času můžou být připravené seznamy, ze kterých můžou respondenti následně vybírat hodnoty a údaje, které vyplňují. V případě webových formulářů, je použití seznamů a číselníků více než vhodné.

Název pole	Popis pole
Útvar	Číslo útvaru, měla by být možnost vybrat ho z číselníku.
Vedoucí pracovník	Jméno manažera útvaru, měla by být možnost vybrat ho ze seznamu.
Název procesu	Název útvaru by ho měl co nejvíce vystihovat.
Název aktiva	Aktivum, měla by být možnost vybrat ho ze seznamu.

Tabulka 4: Návrh formuláře pro identifikaci aktiv a procesů

5.1.2 Vysvětlení dotazníku uživatelům a jeho následné vyplnění

Nyní je načase, aby se zapojili také uživatelé. Po schválení vrcholového managementu podniku, rozešleme manažerům požadavek na vyplnění formulářů. Určíme datum, kdy uspořádáme nejlépe workshop, na kterém dojde k vysvětlení, a budou podány další relevantní informace. Je žádoucí, abychom se samotným formulářem zaslali i další informace, které se ho týkají.

Přistoupíme tedy k vyplnění navrhnutého formuláře. Před samotným vyplněním je nutné věnovat čas důkladnému vysvětlení všech potřebným informací, které uživatelé pro vyplnění potřebují.

Nabízí se také možnost realizovat formulář, jako webový. To by přineslo samozřejmě řadu výhod. Asi největší by bylo nepopiratelně menší množství času, které by respondenti potřebovali.

5.1.3 Vytvoření seznamu aktiv na základě vyplněných dotazníků

Nezbývá nám tedy nic jiného než zpracování vyplněných dotazníku. Vytvoříme tedy seznam, který bude obsahovat všechna sledovaná aktiva. Tento seznam bude dále brán jako zdroj pro další práci, je tedy na místě vysoká pečlivost a svědomitost. Uvědomme si, že to jak pracná a zdlouhavá bude tato práce, závisí především na kvalitě přípravy předešlých činností.

5.2 Rozdělení identifikovaných aktiv

Pro další zpracování a zkoumání je nutné již vytvořený seznam aktiv spořádat a rozdělit do vhodných kategorií. Kromě rozdělení do příslušné větve systému je nutné, aby bylo aktivum vhodně popsáno. Především je klíčový popis a role z hlediska procesu, ve kterém aktivum figuruje. Proto se provedou následující kroky:

- Rozčlení procesu na aktiva
- Seskupení

5.2.1 Rozčlenění procesu na aktiva

Nyní budeme tedy postupně rozdělovat každý proces. Teoreticky se mu věnuje kapitola Popis vazby mezi aktivy. Hierarchicky tedy dekomponujeme příslušný proces ze shora. Pro názornost si uvedeme příklad rozčlenění procesu.

Pro fungování procesu potřebujeme především vyškolené **zaměstnance.** Ti pro vykonávání své činnosti musí být umístěni v příslušném **prostoru.** Prostory musí být vybaveny **kancelářským vybavením** (stůl, židle) a musí ho doplňovat **výpočetní technika** (PC, notebook, tiskárna). Každý počítač musí být vybaven **síťovým zařízením** (Ethernet, Wi-fi, TCP/IP) aby mohl být připojen k **serveru,** na kterém funguje **aplikace.** Servery jsou ve **výpočetních střediscích** a jsou propojeny **optickým kabelem**.

5.2.2 Seskupení

Popsaná aktiva seskupení do logicky rozdělených bloků, které budou charakterizovat IS. Hlavním důvodem pro seskupení jsou další fáze analýzy, kdy budeme hodnotit, jaké hrozby na která aktiva působí. Když budeme mít aktiva uspořádána v blocích, radikálně nám to usnadní práci a tím pádem i čas.

Jaké máme možnosti seskupování a členění a podle čeho tak postupovat jsme si už uvedli výše v teoretické části. Je nutné dbát na logickou posloupnost a podobné vlastnosti aktiv, která rozdělujeme.

Seskupení aktiv informačního systému:

- Lidé
  - Uživatelé
  - Manažeři
  - Správci
    - Operační systémy
    - Aplikace
    - Databáze
    - Sítě
  - Dodavatelé
- Prostory
  - Budovy
  - Místnosti
    - Kanceláře
    - Společné
    - Zasedací
    - Technické
  - Chodby
  - Sklady
  - Garáže
  - Pozemky
- Hardware
  - Servery
    - Souborové
    - Webové
    - Aplikační
    - Databázové
    - Poštovní
    - Tiskové
    - Zálohovací
  - Klienti
    - Terminály
    - PC

        - Notebooky
        - Mobily
        - PDA
    - Tiskárny
        - Síťové
        - Lokální
- Software
    - Operační systémy
    - Aplikace
    - Databáze
- Síť
    - Pasivní prvky
        - Metalické kabely
        - Optické kabely
        - Racky
        - Zásuvky
        - Napájecí kabely
    - Aktivní prvky
        - Routery
        - Switche
        - Firewally
- Media
    - CD
    - DVD
    - Flash disky
    - Pásky
    - Papírová dokumentace
- Data
    - Veřejná
    - Interní
    - Důvěrná
    - Přísně důvěrná

5.3 Ohodnocení aktiv

Přistoupíme tedy k hodnocení aktiv. To se bude opět provádět v několika bodech. Nejdříve bychom měli, opět zapojit uživatele a získat potřebné informace. Až po té vyhodnotíme výši aktiva. Budeme tedy potupovat následovně:

- Připravíme formulář pro hodnocení aktiv
- Uživatelé vyplní formuláře
- Po diskuzi ohodnotíme aktiva

5.3.1 Formulář pro hodnocení

Nyní můžeme opět využít formulář, který byl použit při identifikace aktiv a procesů. Formulář je nutné doplnit o další datové položky. Budou to položky:

- Důvěrnost
- Integrita
- Dostupnost

Při zpřístupnění formuláře je nutné stanovit, jakým způsobem budeme aktiva hodnotit a zároveň způsob hodnocení detailně vysvětlit respondentům.

5.3.2 Hodnocení uživatelů

Pro hodnocení použijeme 4 riziková pásma, jak bývá zvykem. Každé pásmo si definujeme a výstižně pojmenujeme. Dále je důležité definovat, jaké jsou podle nás rozdíly mezi jednotlivými stupni. Respondent si tedy bude u každého aktiva pokládat otázku, co se stane, když dojde k narušení jeho důvěryhodnosti, integrity a dostupnosti a pokusíme se odhadnout výši finanční ztráty.

Stupeň	Zkratka	Dopad	Popis dopadu	od	do
1	N	nízký	Malé škody	0	0,3
2	S	střední	Vážné škody	0,3	3
3	V	vysoký	Velmi vážné škody	3	30
4	K	kritický	Přežití je ohroženo	30	100

Tabulka 5: Rizikové stupně

To je samo o sobě velice obtížné, a proto je vhodné dát respondentům podklady a návod jak výši dopadu odhadnout. K tomu nám poslouží následující tabulka:

Stupeň	1	2	3	4
Popis Dopadu	Malé škody	Vážné škody	Velmi vážné škody	Přežití je ohroženo
Finanční ztráta	0-5%	5-10%	10-30%	30% a více
Ztráta produktivity	Zpomalení nebo přerušení obchodní činnosti na několik minut.	Zpomalení nebo přerušení obchodní činnosti na několik hodin.	Zpomalení nebo přerušení obchodní činnosti na několik dnů.	Zpomalení nebo přerušení obchodní činnosti na několik týdnů.
Ztráta image	Jedna nepříznivá reportáž v médiích.	Několik nepříznivých reportáží v médiích.	Několik dnů trvající nepříznivé reportáže v médiích.	Několik týdnů trvající nepříznivé reportáže v médiích.
Porušení legislativy	Drobné porušení - napomenutí.	Porušení - vyšetřování a pokuta.	Závažné porušení - vyšetřování, soudní proces a pokuta.	Velmi závažné porušení - Soudní proces a společnosti hrozí zánik.
Důvěra klientů	Nemá zásadní dopad na důvěru klientů.	Část klientů odchází ke konkurenci.	Značná část klientů odchází ke konkurenci.	Naprostá většina klientů odchází ke konkurenci.
Důvěra akcionářů	Nemá zásadní dopad na důvěru akcionářů.	Ztráta důvěry akcionářů, dochází k změnám v managementu.	Značná ztráta důvěry akcionářů, dochází ke kompletní změně managementu.	Naprostá ztráta důvěry. Akcionáři posílají společnost do konkurzu.
Dopad na činnosti a zájmy státu	Má velmi malé dopady na činnosti a zájmy státu.	Ohrožuje stabilitu měny a výkon hospodářství. Hrozí stávky.	Ohrožuje stabilitu měny a výkon hospodářství. Hrozí občanské nepokoje.	Ohrožuje stabilitu měny a výkon hospodářství. Hrozí státní převrat.
Dopad na životní prostředí	Nepatrné následky na životní prostředí.	Krátkodobé poškození životního prostředí bez vlivu na ekosystém.	Závažné střednědobé poškození životního prostředí.	Velmi závažné dlouhodobé poškození životního prostředí.
Dopad na jednotlivce	Ohrožení bezpečnosti jedné osoby, poškození zdraví, zranění, žádné léčení.	Ohrožení bezpečnosti více osob, poškození zdraví, zranění, hospitalizace.	Ztráta života jedné osoby, nevratné poškození zdraví, zranění více osob.	Ztráta života více osob, významné nevratné poškození zdraví.

Tabulka 6: Hodnocení dopadu

5.3.3 Diskuze a samotné hodnocení

Po vyplnění formulářů je nutná diskuze, protože manažeři do problematiky vnáší svůj subjektivní názor a mají tendence hodnoty dopadů podhodnocovat nebo nadhodnocovat, podle toho jaké zájmy sledují. Teprve potom zahrneme hodnocení do seznamu. Máme tedy k dispozici kompletní seznam ohodnocených aktiv a můžeme se zabývat hrozbami.

6 HROZBY

6.1 Identifikace hrozeb

Při identifikaci hrozeb máme za úkol určit všechny hrozby, které působí na informační systém. Budeme tedy sledovat jevy, které by mohly ohrozit sledovaná aktiva. Připravíme si tedy seznam hrozeb, které splňují naše podmínky. Při tvoření seznamu bychom měli vycházet ze skutečností, jaké hrozby mohou působit nebo působily v naší lokalitě.

Hrozby budeme sledovat ze dvou pohledů:

- Z pohledu bezpečnostních atributů, na které hrozba působí, a původce jejich hrozby.
- Z pohledu jak působí na skupiny aktiv.

6.1.1 Bezpečnostní atributy hrozby a její původce

Informační systém, který je předmětem analýzy rizik, se po celou dobu analýzy snažíme hodnotit podle jeho důvěrnosti, integrity a dostupnosti. Je proto žádoucí, abychom tyto tři faktory měly spojeny s identifikovanými hrozbami.

Ve vytvořeném seznamu bychom neměli zapomenout na původce hrozby, tedy způsob jakým hrozba vzniká. Původce budeme rozdělovat na náhodou, úmyslnou a přírodní hrozbu.

Tyto atributy jsou tedy uvedeny v následujícím seznamu:

Hrozba	Bezpečnostní atribut			Původce vzniku		
	Důvěrnost	Integrita	Dostupnost	Náhodná	Úmyslná	Přírodní
Požár		x	x	x	x	x
Povodeň		x	x			x
Blesk		x	x			x
Zemětřesení		x	x			x
Výpadek el. proudu			x	x	x	x
Kolísání napětí		x	x	x	x	x
Chyba správce	x	x	x	x	x	
Chyba uživatele	x	x	x	x	x	
Průmyslová havárie			x	x		
Demonstrace			x	x		
Kyberterorismus	x	x	x		x	

Terorismus			x		x	
Odposlech	x				x	
Použití šk. SW	x	x	x		x	
Selhání hardwaru	x	x	x	x	x	
Selhání softwaru	x	x	x	x	x	
Selhání sítě		x	x	x	x	

Tabulka 7: Hrozby, jejich atributy a původce

6.1.2 Působení hrozeb na aktiva

Při identifikaci hrozeb musíme také brát v potaz na jaká aktiva nebo skupinu aktiv hrozba působí. Jeden z důvodů proč jsme aktiva logicky seskupily, byl právě tento krok. Nyní tedy do seznamu hrozeb také začleníme data o tom, na jakou skupinu aktiv působí.

Hrozba	Hardware	Software	Síť	Média	Data	Personál	Prostor
Požár	x		x	x			x
Povodeň	x		x	x			x
Blesk	x		x				x
Zemětřesení	x		x				x
Výpadek el. proudu	x		x		x		
Kolísání napětí	x		x				
Chyba správce	x	x	x	x	x		
Chyba uživatele	x	x	x	x	x		
Průmyslová havárie						x	
Demonstrace						x	
Kyberterorismus		x	x		x		
Terorismus	x		x	x		x	x
Odposlech			x				
Použití šk. SW		x	x		x		
Selhání hardwaru	x						
Selhání softwaru		x					
Selhání sítě			x				

Tabulka 8: Působení hrozeb na aktiva

Uvedené seznamy hrozeb jsou pouze ilustrativní a slouží ke znázornění a vysvětlení tvorby seznamu. Ve skutečnosti bude hrozeb působící na informační systém mnohem větší množství.

6.2 Hodnocení hrozeb

Pro stanovení úrovně hrozby opět využijeme formulář, který vyplní respondenti. Vyplnění formuláře a jeho vysvětlení může probíhat stejně jako u identifikace aktiv, tedy ve formě workshopu.

Název pole	Popis pole
Hrozba	Číslo hrozby
Zdůvodnění	Na základě čeho byla stanovena úroveň hrozby.
Hodnotitel	Kdo úroveň stanovil.
Stupeň síly	Vhodný stupeň.
Doba působení	V jednotkách času.
Úroveň hrozby	V %

Tabulka 9: Návrh formuláře pro identifikaci aktiv a procesů

Budeme používat 4 úrovně, jako jsme použili u hodnocení aktiv. Úroveň by měla být posouzena na základě všech relevantních faktorů. Hrozby budeme hodnotit v intervalu 0 – 100. 0 znamená, že hrozba neplatí, a 100 naopak, že uplatnění hrozby je jisté.

Stupeň	Zkratka	Úroveň hrozby	Popis hrozby	od	do
1	N	nízká	nepravděpodobná	0%	25%
2	S	střední	pravděpodobná	25%	50%
3	V	vysoká	vysoce pravděpodobná	50%	75%
4	K	kritická	jistá	75%	100%

Tabulka 10: Hodnocení úrovně hrozby

Je nutné hodnotit každou skupinu hrozeb zvlášť, podle toho jak jsme si je v identifikaci rozdělili. Budeme rozlišovat hrozby:

- Náhodné
- Úmyslné
- Přírodní

Po vyplnění formulářů je opět nutná diskuze z důvodu subjektivity, která má při hodnocení nezanedbatelný vliv.

7 ZRANITELNOSTI

7.1 Identifikace zranitelností

Jak už jsme si uváděli v teoretické části míra zranitelnosti je především závislá na úrovni stávajících bezpečnostních opatření. Vztáhneme tedy míru zranitelnosti k nim. Nezbývá nám tedy nic jiného, než prostudovat příslušnou dokumentaci (politika, technická specifikace a podobně) organizace nebo podniku, v němž, se sledovaný informační systém nachází. Musíme se taky zaměřit na důkladnou kontrolu stávajících opatření.

U studovaných dokumentů se zaměříme především na tyto vlastnosti:

- Způsob vydávání dokumentů
- Jejich aktualizace
- Váha dokumentu
- Závažný pokyn nebo jen doporučení
- Kdy byl dokument vydán
- Kým byl vydán
- Je-li aktuální a platný
- Dostupnost

Na základě zjištěných opatření vypracujeme seznam zranitelností, které jsou charakteristické pro naše aktiva.

7.2 Hodnocení zranitelností

Při hodnocení zranitelnosti budeme postupovat přesně tak, jak jsme si už uváděli v teoretické části. Pro každý pár hrozba - aktivum, lépe řečeno hrozba skupina – aktiv, budeme posuzovat, nakolik je aktivum imunní vůči působení dané hrozby. To se bude dít s ohledem na to jaká je úroveň stávajících opatření. Z identifikace opatření by už mělo být patrné, zda implementovaná opatření pracují správně a efektivně. Hodnocení zranitelnosti je posuzováno z více pohledů.

Pokud je analýza rizik a s ní spojené hodnocení zranitelností kombinováno s penetračními testy (v podstatě napodobení útoku hackera a podobně), je možné pro určení hodnoty zranitelnosti použít výsledky z penetračních testů daného informačního systému a hodnoty stanovit následovně.

Stupeň	Zkratka	Zranitelnosti	Popis zranitelnosti	od	do
1	N	nízká	Podařilo se získat informace o systému, které je možné použít k dalším útokům.	0%	25%
2	S	střední	Podařilo se přečíst některá data nebo některá data lze smazat, modifikovat nebo vložit.	25%	50%
3	V	vysoká	Podařilo se přečíst veškerá data a kamkoliv je možné data zapsat.	50%	75%
4	K	kritická	Podařilo se získat administrátorská práva a plnou kontrolu nad systémem.	75%	100%

Tabulka 11: Určení hodnoty zranitelnosti s použitím výsledků penetračních testů

Pokud je tedy proces vyzrálejší, je míra jeho zranitelnosti nižší. Tento fakt, je zachycen v následující tabulce.

Stupeň	Zkratka	Zranitelnosti	Opatření	od	do
1	N	nízká	Opatření jsou zavedena, dokumentována, kontrolována a zlepšována.	0%	25%
2	S	střední	Opatření jsou zavedena, dokumentována, kontrolována.	25%	50%
3	V	vysoká	Opatření jsou zavedena a dokumentována.	50%	75%
4	K	kritická	Žádná opatření nejsou zavedena, dokumentována, kontrolována a zlepšována.	75%	100%

Tabulka 12: Stupně míry zranitelnosti

Vyzrálost procesu však sama o sobě nestačí. Opaření může být dokumentováno, kontrolováno, optimalizováno a přesto dojde k uplatnění hrozby. Je tedy nasnadě

vyhodnotit taky tuto skutečnost. Jeden z možných návodů jak to udělat nám mohou dát tabulky, které jsou uvedeny níže.

Stupeň	Zkratka	Zranitelnosti	Bezpečnostní incidenty	od	do
1	N	nízká	Neexistují důkazy o žádných závadách či selhání bezpečnostních opatření.	0%	25%
2	S	střední	Existují důkazy o malém počtu závad či selhání bezpečnostních opatření.	25%	50%
3	V	vysoká	Existují důkazy o větším počtu závad či selhání bezpečnostních opatření.	50%	75%
4	K	kritická	Existují důkazy o rozsáhlých závadách či selhání bezpečnostních opatření.	75%	100%

Tabulka 13: Míra zranitelnosti a bezpečnostní incidenty

Stupeň	Zkratka	Zranitelnosti	Havarijní plány	od	do
1	N	nízká	Pro všechna potenciální narušení businessu jsou připraveny havarijní plány a jsou pravidelně testovány a optimalizovány	0%	25%
2	S	střední	Havarijní plány spíše neselžou	25%	50%
3	V	vysoká	Havarijní plány spíše selžou	50%	75%
4	K	kritická	Pro žádná potenciální narušení businessu nejsou připraveny žádné havarijní plány	75%	100%

Tabulka 14: Míra zranitelnosti a havarijní plány

Ještě před tím než provedeme hodnocení, je potřeba si uvědomit jaká opatření zabraňují sledovaným hrozbám. To si znázorníme níže na ilustračním seznamu opatření a seznamu hrozeb, kterým opatření snižují dopad na aktiva.

Seznam opatření je neúplný a jsou zde uvedena pouze opatření, které se týkají uvedených hrozeb.

1. Personální opatření
   - 1.1. Při přijímaní zaměstnanců
   - 1.2. Při trvání pracovního poměru
     - 1.2.5. Šetření - v případě porušení či podezření na porušení bezpečnostní politiky zahájit šetření.
     - 1.2.6. Vyvození důsledků – v případě porušení bezpečnostní politiky by měly být vyvozeny důsledky.
   - 1.3. Při ukončování pracovního poměru
2. Fyzická opatření
   - 2.1. Fyzický bezpečnostní perimetr
     - 2.1.1. Nenápadnost – vzhled a značení budovy by nemělo naznačovat její účel.
     - 2.1.4. Silné zdi – obvodové zdi by měly být pevné (např. železobeton)
     - 2.1.6. Okna – obzvlášť v přízemí by měla být vybavena bezpečnostní fólií.
   - 2.2. Kontrola pohybu osob
   - 2.3. Ochrana aktiv v objektu
     - 2.3.6. Nebezpečné a hořlavé materiály by měly být umístěny je na k tomu určených místech.
     - 2.3.8. Veškerý materiál a zboží by mělo být při převzetí prověřeno.
     - 2.3.9. Konzumace a kouření v blízkosti prostředků VT by mělo být zakázáno.
   - 2.4. Ochrana aktiv mimo objekt
   - 2.5. Ochrana aktiv před poškozením nebo zničením
     - 2.5.1. Blesk – hromosvod, ochranné filtry i na vnějších komunikačních linkách.
     - 2.5.3. Voda - aktiva by měla být mimo místa záplav a pravděpodobného výskytu úniku vody.
   - 2.6. Zabezpečení napájení
   - 2.7. Zajištění klimatizace
   - 2.8. Ochrana kabeláže
     - 2.8.1. Elektrické kabely a telekomunikační linky by měly být vedeny pod zemí.
     - 2.8.2. Datové kabely by měly být vedeny v kolektoru.
   - 2.9. Správa paměťových médií
   - 2.10. Zásada prázdného stolu
   - 2.11. Evakuační plány
3. Logická
   - 3.1. Správa přístupových oprávnění
   - 3.2. Správa privilegií
   - 3.3. Správa používání hesel
   - 3.4. Zásada prázdné obrazovky
   - 3.5. Řízení přístupu k síti a síťových prvků
   - 3.6. Řízení přístupu k operačnímu systému
   - 3.7. Řízení přístupu k aplikacím
   - 3.8. Řízení přístupu k výstupním zařízením
4. Technická
   - 4.1. Pro zajištění odpovídající dostupnosti by mělo být vybráno vhodné řešení.

4.2. Měla by být používána, tam kde je to potřeba, jen taková zařízení, která mají nízkou radiaci.
4.3. Měla by být používána taková zařízení, která jsou odolná vůči působení okolního prostředí.
4.4. Kryptografická opatření k zajištění důvěrnosti a integrity.

5. Administrativní
   5.1. Vlastní organizace
   5.2. Třetí strany
   5.3. Outsourcing
   5.4. Řízení přístupu
   5.5. Klasifikace informací
   5.6. Vývoj a údržba systému
   5.7. Auditing a monitoring IS
   5.8. Provozní deník
   5.9. Zálohování a archivace
   5.10. Ochrana před škodlivým kódem
   5.11. Zajištění kontinuity

č.	Hrozba	Opatření
1	Požár	2.3.6,2.3.8,2.3.9
2	Povodeň	2.5.3
3	Blesk	2.5.1
4	Zemětřesení	Žádné opatření
5	Výpadek el. proudu	2.6
6	Kolísání napětí	2.6
7	Chyba správce	1.2
8	Chyba uživatele	1.2
9	Průmyslová havárie	2.11, 5.11
10	Demonstrace	2.11, 5.11
11	Kyberterorismus	5.11
12	Terorismus	2.1.1, 2.11, 5.11
13	Odposlech	2.1.4, 2.1.6, 2.8.1, 2.8.2
14	Použití šk. SW	5.10, 1.2.5, 1.2.6
15	Selhání hardwaru	4.1, 4.3, 5.7, 5.8, 5.11
16	Selhání softwaru	5.7, 5.8, 5.11
17	Selhání sítě	5.7, 5.8, 5.11

Tabulka 15: Seznam hrozeb a opatření, které snižují jejich dopady

Po dokončení těchto činností, by neměl být problém vytvořit samotný seznam zranitelností a nic nám nebrání tomu, abychom se věnovali vyhodnocení rizik, které jsou charakteristické pro náš IS.

8 RIZIKA

8.1 Vyhodnocení rizik

Máme vše potřebné a můžeme přistoupit k samotnému vyhodnocení rizik. Pro každé aktivum vypočteme odpovídající riziko, podle hrozby, která na něj působí. Riziko je dáno součinem hodnoty aktiva, hrozby a jeho zranitelnosti. Jak by mohl výpočet vypadat, nám ukazuje následující tabulka:

Hrozba č.	Úroveň hrozby	Hodnota aktiva			Zranitelnost			Riziko			Max. Riziko
		Dův.	Int.	Dos.	Dův.	Int.	Dos.	Dův.	Int.	Dos.	
1	1%	5	25	50	20%	64%	95%	0	0	1	1
2	98%	5	25	50	54%	39%	58%	3	10	29	29
3	32%	5	25	50	94%	86%	88%	2	7	14	14
4	69%	5	25	50	65%	96%	41%	2	17	14	17
5	82%	5	25	50	19%	45%	52%	1	9	21	21
6	0%	5	25	50	70%	26%	4%	0	0	0	0
7	56%	5	25	50	3%	44%	27%	0	6	8	8
8	92%	5	25	50	77%	18%	29%	4	4	13	13
9	81%	5	25	50	73%	54%	97%	3	11	39	39
10	30%	5	25	50	60%	64%	24%	1	5	4	5
11	77%	5	25	50	11%	31%	33%	0	6	13	13
12	27%	5	25	50	17%	29%	71%	0	2	10	10
13	32%	5	25	50	57%	38%	10%	1	3	2	3
14	82%	5	25	50	39%	76%	95%	2	16	39	39
15	95%	5	25	50	87%	25%	54%	4	6	26	26
16	65%	5	25	50	19%	58%	12%	1	9	4	9
17	17%	5	25	50	50%	1%	85%	0	0	7	7
18	35%	5	25	50	79%	87%	83%	1	8	15	15
19	27%	5	25	50	82%	13%	48%	1	1	6	6
20	2%	5	25	50	43%	41%	55%	0	0	1	1

Tabulka 16:Výpočet rizika

Jak už bylo řečeno, celou dobu zkoumáme aktiva s ohledem na jejich důvěrnost, integritu a jejich dostupnost. Proto je pro každý tento atribut vypočtené riziko zvlášť. Uvedené hodnoty úrovně hrozby, hodnoty aktiva a zranitelnosti byly vybrány náhodně.

Stupeň	Zkratka	Výše rizika	Popis rizika	od	do
1	N	nízké	Riziko je možné akceptovat a dále jen monitorovat.	0	1
2	S	střední	Riziko musí být zvládáno podle plánu.	1	3
3	V	vysoké	Riziko musí být zvládáno podle plánu.	3	30
4	K	kritické	Riziko musí být ihned zvládáno.	30	100

Tabulka 17: Stupně rizika

Po výpočtu rizika a zařazení ho do příslušného stupně, bychom tedy měli mít k dispozici seznam rizik. Seznam by měl obsahovat tyto informace:

- aktiva, která jsou nejvíce ohrožena
- hrozby, které na ně působí
- na jaké atributy bezpečnosti hrozba působí
- zranitelnost aktiva vůči hrozbě
- finanční a jiné dopady v případě uplatnění hrozby

8.2 Vyhodnocení opatření

Součástí analýzy je samozřejmě také vyhodnocení stávajících opatření a doporučení nových opatření, které by ovlivňovaly určená rizika. Tato doporučení jsou jedním z nejdůležitějších výstupů, protože nám dávají návod, jak aktivně působit na dopady hrozeb. Měli bychom tedy věnovat velkou pozornost tomu, jaká opatření doporučíme a která budou posléze realizována.

Celkový přínos opatření je závislý na těchto pěti faktorech:

- Obtížnost zavedení opatření
- Doba potřebná k zavedení opatření
- Účinnost opatření
- Priorita opatření

- Celkové náklady

Stupeň	Zkratka	Obtížnost zavedení opatření	od	do
1	N	Zavedení opatření je téměř nemožné.	0%	25%
2	S	Zavedení opatření vyžaduje nadprůměrné znalosti.	25%	50%
3	V	Zavedení opatření vyžaduje průměrné znalosti.	50%	75%
4	K	Zavedení opatření je velice snadné.	75%	100%

Tabulka 18: Stupně obtížnosti zavedení opatření

Stupeň	Zkratka	Časová náročnost	od	do
1	N	Délka zavedení se pohybuje v řádově měsících.	0%	25%
2	S	Délka zavedení se pohybuje v řádově týdnech.	25%	50%
3	V	Délka zavedení se pohybuje v řádově dnech.	50%	75%
4	K	Délka zavedení se pohybuje v řádově hodinách.	75%	100%

Tabulka 19: Stupně časové náročnosti

Stupeň	Zkratka	Účinnost opatření	od	do
1	N	Nepatrně minimalizuje riziko.	0%	25%
2	S	Částečně minimalizuje riziko.	25%	50%
3	V	Významně minimalizuje riziko.	50%	75%
4	K	Zcela minimalizuje riziko.	75%	100%

Tabulka 20: Stupně účinnosti opatření.

Stupeň	Zkratka	Priorita opatření	od	do
1	N	Opatření musí být realizováno v dlouhodobém časovém horizontu.	0%	25%
2	S	Opatření musí být realizováno střednědobém časovém horizontu.	25%	50%
3	V	Opatření musí být realizováno v krátkodobém časovém horizontu.	50%	75%
4	K	Opatření musí být realizováno ihned.	75%	100%

Tabulka 21: Stupně priority opatření

Po zvážení všech těchto faktorů, bychom měli být schopni vytvořit seznam opatření, která jsou podle nás vhodná pro zavedení, a zároveň vhodná pro zkoumaný podnik nebo organizaci.

9 ZÁVĚREČNÁ ZPRÁVA

Dostáváme se k poslednímu kroku analýzy a tím je závěrečná zpráva. Její hlavním účelem je přesvědčit management společnosti, aby akceptoval výsledky analýzy rizik a zvolil vhodný způsob zvládání rizik a stanovil, jak se bude zacházet se zbytkovými riziky. Vedle samotné závěrečné zprávy je nanejvýš vhodné zpracovat prezentaci, která bude odrážet základní body zprávy.

Všechny závěry, ke kterým jsme při analýze dospěli, musí být formulovány jednoznačně a srozumitelně a nesmí připouštět jakékoliv pochybnosti.

Závěrečná zpráva by měla obsahovat:

- Předmět analýzy rizik – definování hranic analýzy
- Největší rizika
- Hodnocení dopadů
- Ohrožená aktiva
- Největší hrozby
- Doporučený způsob zvládání rizik
- Seznam aktiv
- Seznam hrozeb
- Seznam rizik
- Seznam opatření
- Kdo analýzu provedl – členové týmu podílejí se na vytvoření

ZÁVĚR

Hlavním úkolem této práce bylo, aby čtenáři nebo studenti více pronikli do problematiky bezpečnosti informačních systémů a uvědomili si, jaký význam má analýza rizik v bezpečnostní politice podniku. Práce se především zaměřuje na metodiku vytvoření analýzy. Jak už bylo řečeno, existuje mnoho postupů a metod. Použité postupy byly voleny s ohledem na jejich srozumitelnost a snadnou pochopitelnost.

Abychom pochopili, všechny aspekty a atributy informační bezpečnosti, je potřeba si nejprve definovat a vysvětlit jednotlivé pojmy. V teoretické části jsou proto nejprve uvedeny všechny důležité definice, které jsou klíčové pro bezpečnost informačních systémů. Dále jsou vysvětleny jejich vzájemné vztahy a to jak na sebe působí.

Na začátku analýzy rizik je klíčová otázka, jakým způsobem budeme analýzu rizik vytvářet. Od použité metodiky se odvíjí celý postup projektu, je proto důležité vybrat vhodný způsob, jakým budeme problém řešit. V práci jsou proto uvedeno základní dělení používaných metod a jejich klady a zápory. Mimo metodiky, je pro správné pochopení tvorby analýzy rizik, důležité si teoreticky popsat jednotlivé fáze analýzy. Každá část má svá specifika a je důležité si uvést, jaký má příslušná fáze význam z hlediska celého projektu a co je přesným cílem této činnosti.

Praktická část této práce se věnuje konkrétnímu postupu tvorby analýzy rizik, který je vhodný pro problematiku informačních systémů. Krok za krokem jsou popsány jednotlivé činnosti, které vedou k vytvoření analýzy. Aby čtenáři lépe pochopili princip zvolených postupů, jsou zde uvedeny příklady toho, jak řešit problémy při skutečném projektu.

Po dokončení analýzy musí probíhat další činnosti, které vedou k vytvoření kvalitní bezpečnostní politiky. Analýza je pouze základní stavební kámen, i když velice důležitý. Především zavedení doporučených opatření, které analýza uvádí, má zásadní vliv na bezpečnost informačního systému.

ZÁVĚR V ANGLIČTINĚ

The main goal of this study was to get readers and students delve into the issue of security of information systems and realizing the importance of risk analysis in the enterprise security policy. The work mainly focuses on a methodology of analysis. As already mentioned, there are many procedures and methods. The methods were chosen with regard to their clarity and ease of comprehension.

To understand all aspects and attributes of information security, we must first define and explain various concepts. In the theoretical part of the first set all the important definitions that are crucial for the security of information systems. Furthermore, explains their relationship and how to interact.

At the beginning of risk analysis is a key question of how we create a risk analysis. Since the methodology is based on the progress of the project, it is important to choose an appropriate way to solve the problem. The work is therefore referred to the basic division of the methods and their pros and cons. The methodology for creating a proper understanding of risk analysis is critical theory which describes the various stages of analysis. Each part has its own specifics, and it is important to note what is the appropriate stage of importance to the whole project and what is aim of this activity.

The practical part of this work is devoted to a specific procedure for developing risk analysis, which is suitable for the issues of information systems. Step by step description of the particular activities those lead to the creation of analysis. For readers better understand the principle of selected procedures, there are examples of how to solve problems in a real project.

After completion of the analysis must be other activities that lead to the creation of a good security policy. The analysis is a basic building block, albeit very important. In particular, the introduction of measures recommended by the analysis provides a vital safety information system.

SEZNAM POUŽITÉ LITERATURY

[1] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno : Tribun, 2009. 134 s. ISBN 978-80-7399-731-1.

[2] DOBDA , Luboš. *Ochrana dat v informačních systémech*. Praha : Grada, 2001. 288 s. ISBN 8071694797.

[3] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Praga : Computer Press, 2004. 200 s. ISBN 80-251-0106-1.

[4] KOVACICH, Gerald L. *Průvodce bezpečnostního pracovníka informačních systémů*: zavádění a prosazování bezpečnostní politiky informačních systémů. Brno : UNIS, 2000. 200 s. ISBN 80-86097-42-0.

[5] NORTHCUTT, Stephen ; ZELTSER, Lenny ; WINTERS, Scott . *Bezpečnost počítačových sítí.* Praha : Computer Press, 2005. 592 s. ISBN 80-251-0697-7.

[6] GÁLA, Libor ; POUR, Jan; TOMAN , Prokop. *Podniková informatika, Počítačové aplikace v podnikové a mezipodnikové praxi*. Praha : Grada Publishing , 2005. 484 s. ISBN 80-247-1278-4.

[7] STEINER, F.; TUPA, J. *Management rizik v systémech řízení bezpečnosti informací.* In MOPP 2007. V Plzni : Západočeská univerzita, 2007. s. 177-183. ISBN 978-80-7043-535-9.

[8] *Wiki - Wikipedie* [online]. 2011 [cit. 2011-05-23]. Dostupné z WWW: <http://cs.wikipedia.org >.

[9] *BusinessInfo.cz* [online]. 2006 [cit. 2011-05-23]. Dostupné z WWW: <http://www.businessinfo.cz>.

[10] *Security World.cz* [online]. 2011 [cit. 2011-05-23]. Dostupné z WWW: <http://securityworld.cz/>.

[11] *Digital Threat* [online]. 2009 [cit. 2011-05-23]. Dostupné z WWW: <http://www.digitalthreat.net>.

[12] *CleverAndSmart - ICT management* [online]. 2008 [cit. 2011-05-23]. Dostupné z WWW: <http:/www.cleverandsmart.cz>.

[13] *RISK ANALYSIS TECHNIQUES* [online]. 2007 [cit. 2011-05-23]. Dostupné z WWW: <http://www.drj.com>.

[14] *Managent rizik bezpečnosti informací* [online]. 2010 [cit. 2011-05-23]. Dostupné z WWW: <http://bpm-tema.blogspot.com>.

[15] *ISMS - Seriál o řízení bezpečnosti informací* [online]. 2010 [cit. 2011-05-23]. Dostupné z WWW: <http://www.chrantesidata.cz>.

[16] ŠEBESTOVÁ, Marie. Management bezpečnosti informací podle ISO/IEC 27001. In *SystemOnline* [online]. [s.l.] : [s.n.], 2010 [cit. 2011-05-23]. Dostupné z WWW: <http://www.systemonline.cz>.

[17] *Risk - Management* [online]. 2009 [cit. 2011-05-23]. Dostupné z WWW: <http://www.risk-management.cz>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AR	Analýza rizik
ALE	Annualized Loss Expectancy
CCTA	Central Computer and Telecommunications Agency
CRAMM	CCTA Risk Analysis and Management Methodology
HW	Hardware
ICT	Information and Communication Technologies
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol@

SEZNAM OBRÁZKŮ

SEZNAM TABULEK