UNIVERSITA KARLOVA V PRAZE

1. Lékařská fakulta

Systém řízení informačních rizik ve VFN

Vypracoval: Tomáš Jeníček

Obor studia: Specializace ve zdravotnictví – Zdravotnická technika

Vedoucí práce: Ing. Jiří Haase, MBA

Pracoviště: Úsek informatiky VFN

PRAHA 2008

Poděkování

Děkuji vedoucímu mé práce, Ing Jiřímu Haasemu, MBA za vedení mé práce.

Dále děkuji pracovníkům firmy MANA Consulting s.r.o. se kterými jsem během své práce spolupracoval, zejména panu Ing. Jaroslavu Škeříkovi a Jaromíru Novotnému, kteří mi poskytli odborné vedení, rady a podklady nezbytné pro mou práci.

Prohlášení:

Prohlašuji, že jsem závěrečnou práci zpracoval samostatně a uvedl jsem veškerou literaturu a prameny.

V Chrudimi dne 29. května 2008

Tomáš Jeníček

Obsah

Souhrn

V práci jsem se zabýval principem řízení informačních rizik v podmínkách Všeobecné fakultní nemocnice v Praze. V teoretické části jsem se věnoval nastínění problematiky řízení rizik (risk management), definici základních pojmů a pokusil se vysvětlit principy a postupy používané při řízení rizik.

V části praktické jsem se pak věnoval konkrétní implementaci řízení informačních rizik v podmínkách zdravotnictví, zejména ve Všeobecné fakultní nemocnici v Praze, dále jen VFN.

Summary

I was occupied oneself with principles of risk management in IT in General Faculty Hospital in Prague. In theoretical part I was trying to describe how the risk management work, describe main terms.

In practical part I wrote about IT risk management implementation in the hospital.

Úvod

Organizace mohou chtít řešit otázky stanovení rizika z různých důvodů. Ale co je to řízení rizik, a jak souvisí s informačními technologiemi?

Řízení rizik je postup, kterým zvládáme nejistotu vyvolanou hrozbou pomocí kroků vedoucích k rozpoznání hrozby a stanovením, zda hrozí možnost vzniku rizika. Pokud ano, je třeba riziko posoudit a případně navrhnout vhodná opatření.

Řízení informačních rizik je důležitou součástí řízení bezpečnosti informací v organizaci. Znalost konkrétních rizik přispívá k výběru vhodných bezpečnostních opatření, která pak mohou snížit pravděpodobnost uplatnění hrozby, případně snížit jejich negativní dopad. Pokud správně stanovíme rizika, úsilí, které vynaložíme při realizaci opatření, bude mít vyšší efektivitu. Systém řízení rizik by proto měl být nedílnou součástí systému řízení bezpečnosti informací a navíc velmi výrazně ovlivňuje celkovou efektivitu systému.

Teoretická část

1.0 Co je to riziko?

S pojmem riziko se setkáme každý den. Vždy, když se rozhodujeme k nějaké činnosti, tak intuitivně hodnotíme její riziko tzn. možnost jejího negativního dopadu na osobu, událost atd. Také povolání může být rizikové – pak dostáváme rizikový příplatek. Zde pak pojem riziko vyjadřuje zvýšenou míru nebezpečí. Jak je vidět z předcházejících příkladů, každý o riziku mluví, ale často v jiném kontextu. Takže jak by se dal pojem riziko definovat?

Podle Slovníku cizích slov[1] se jedná o: nebezpečí, možnost škody, ztráty, nezdaru.

Neexistuje jedna obecně uznávaná definice, např. podle knihy Řízení rizik ve firmách a jiných organizacích[2] je možné použít hned několik definic:

1. Pravděpodobnost či možnost vzniku ztráty, obecně nezdaru
2. Variabilita možných výsledků nebo nejistota jejich dosažení
3. Odchýlení skutečných a očekávaných výsledků
4. Nebezpečí negativní odchylky od cíle (tzv. čisté riziko)
5. Nebezpečí chybného rozhodnutí
6. Možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko)
7. Možnost, že specifická hrozba využije specifickou zranitelnost systému

Každopádně vždy se musí jednat o nejistý výsledek. Vždy musí být dvě možnosti, jak může situace dopadnout. Pokud víme jistě, že dojde ke ztrátě, nejedná se o riziko, ale o fakt, který nemá žádnou variabilitu. Dále pak musí být alespoň jedna z možností nežádoucí. A je jedno, zda se jedná přímo o ztrátu či nenaplnění předpokládaných zisků.

Podle různých definic rizika můžeme rizika řadit do různých skupin, např.: rizika podnikatelská (ztráta zakázek, zákazníků, ztráta dobrého jména organizace, krach firmy apod.), rizika ekonomická, resp finanční (finanční ztráta apod.), rizika marketingová (špatný odhad trhu, ztráta poptávky), apod.

Definic je možných opravdu mnoho, ale naší potřebě asi nejlépe vyhovuje definice: **„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, resp. hodnotou.“[3]

2.0 Pojmy

2.1 Aktivum

Aktivum je vše, co má pro danou organizaci hodnotu a je třeba pro vykonávání funkce organizace. Jeho hodnota může být snížena díky působení hrozby na aktivum, takže je třeba aktivum vhodnými prostředky chránit prostřednictvím tzv. bezpečnostních opatření. Aktiva dělíme na hmotná a nehmotná. Mezi hmotná patří např. prostory organizace, peníze, hardware, zaměstnanci. Nehmotná aktiva pak jsou v první řadě informace a software. Je jedno, zda se jedná o informace o samotné organizace (účetní) tak informace související se samotnou činností subjektu (data pacientů atd.)

Důležitým atributem aktiva je jeho hodnota. Ta může být objektivní (pořizovací náklady) nebo subjektivní, vyjadřující naše vnímání důležitosti aktiva pro fungování firmy.

Při hodnocení aktiva můžeme vycházet například z těchto hledisek:[4]

1. Pořizovací náklady či jiná hodnota aktiva
2. Důležitost aktiva pro existenci či chování subjektu
3. Náklady na překlenutí případné škody na aktivu
4. Rychlost odstranění případné škody na aktivu
5. Jiná hlediska (mohou být specifická případ od případu)

2.2 Zranitelnost

Zranitelnost je dalším důležitým atributem aktiva.

Jsou to nedostatky nebo slabiny v zabezpečení konkrétního aktiva, které můžou být využity jedním nebo více hrozbami a negativně aktivum ohrozit. Na konkrétní zranitelnost aktiva pak působí hrozba a tak vzniká riziko.

Úroveň zranitelnosti pak určíme podle citlivosti aktiva na hrozbu a významu aktiva pro organizaci. Čím lépe je aktivum chráněno (zabezpečeno) proti působení hrozby, tím menší je míra zranitelnosti, tedy citlivost aktiva vůči hrozbě.

2.3 Hrozba

Může jí být potenciální událost, konkrétní aktivita nebo činnost osoby, která má negativní vliv na bezpečnost aktiva a může na něm způsobit škodu.

Jako příklad hrozby může posloužit přírodní katastrofa, závada na elektroinstalaci, krádež, selhání lidského faktoru.

Dopad hrozby pak označuje škodu, kterou může hrozba na aktivu způsobit včetně všech následných škod, které mohou vzniknout poškozením, zničením aktiva nebo i jeho dočasnou nedostupností. Konkrétně pak můžeme dopad hrozby vyjádřit např. atributem aktiva nazývaného hodnota aktiva. viz vysvětlení pojmu Aktivum. Může se ale stát, že dopad hrozby hodnotu aktiva výrazně přesáhne.

Dopady hrozby mohou být přímé (finanční) a nepřímé (ztráta důvěry zákazníků, strádání lidí, poškození zdraví, zhoršení vztahů s dodavateli apod.)

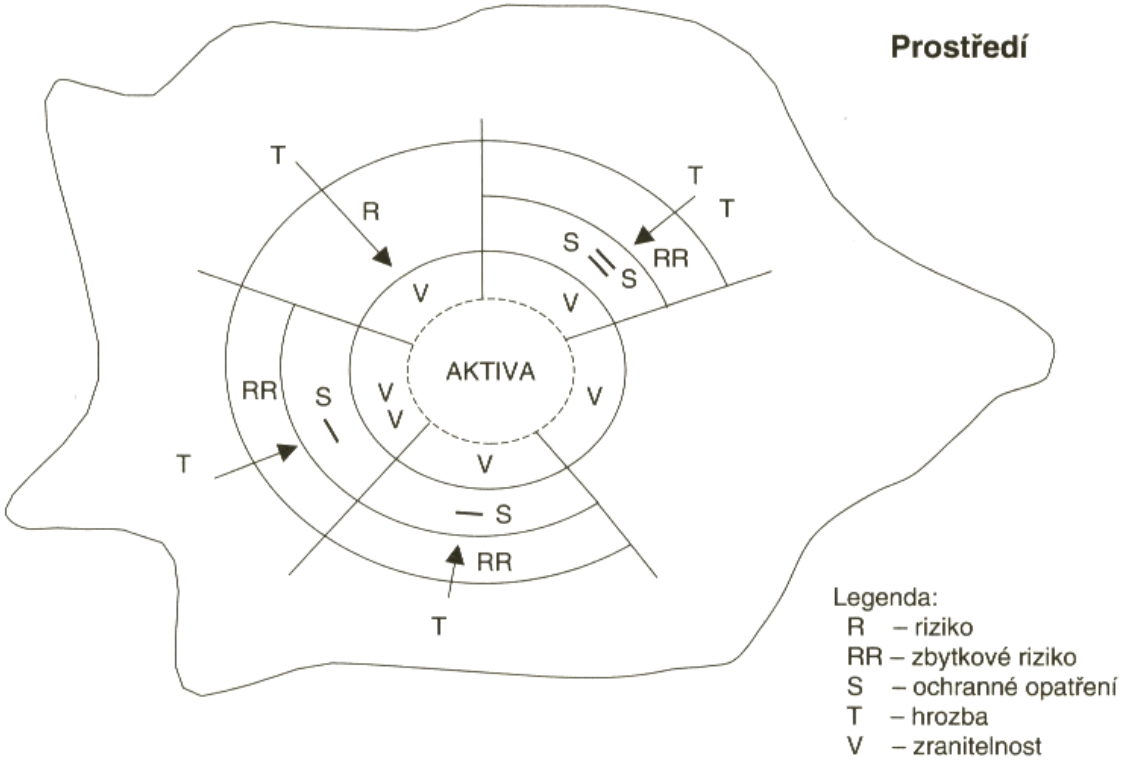
2.4 Protiopatření

„Je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminace), snížení zranitelnosti nebo dopadu hrozby.“[5]

Protiopatření navrhujeme ve snaze snížit možné škody vzniklé působením hrozby na zranitelnost aktiva nebo s úmyslem snížit dobu potřebnou pro překlenutí období, potřebného k uvedení aktiva do původního stavu a tím omezit následné škody způsobené nefunkčností nebo omezenou funkčností aktiva.

Při plánování protiopatření nás zajímá hlavně efektivnost, tj. poměr možných dopadů a nákladů vynaložených na snížení nebo eliminaci rizika. Efektivita popisuje, jak hodně klesne účinek hrozby, její nebezpečnost nebo jak dobře snížíme úroveň

zranitelnosti aktiva ve vztahu k nákladům potřebným k dosažení tohoto stavu. Důležitým prvkem je také snaha hrobu včas rozpoznat a zamezit jejímu plnému rozvinutí. U nákladů nás pak zajímá, kolik nás bude stát zavedení a provozování protiopatření.



Graf 1 Vztah aktiva, rizika, zranitelnosti a hrozby

3.0 Analýza rizika

Analýza rizik je chápána jako proces vedoucí ke stanovení hrozeb, pravděpodobnosti jejich naplnění a dopadu na aktiva. Po analýze rizik pokračujeme procesem řízení rizik viz dále.

Již při počáteční analýze je třeba stanovit úroveň, na kterou chceme rizika snížit.

3.1 Metody analýzy

Kvalitativní metody

Sem patří již výše zmíněné rozdělení rizik pomocí stupnice. Tato metoda je rychlejší, ale je zatížena chybou, která vzniká díky subjektivnímu hodnocení specialistou. Její nevýhodou je její využití při zvládání rizik. Zde narazíme na problém, že není jisté, kolik nás bude stát eliminace hrozby.

Kvantitativní metody

Oproti kvalitativním jsou založeny na matematickém modelu výpočtu rizika. Vychází se přitom z velikosti dopadu hrozby a z frekvence výskytu. Pak se provádí přepočet na dané období, buď čtvrtletí a nejčastěji na roční předpokládané ztráty. Jejich nevýhodou je časová náročnost a velké množství dat, které je třeba vyhodnotit.

3.2 Stanovení hranic analýzy rizika

Jedná se o vybrání aktiv, která zahrneme do analýzy rizik. Ne všechna aktiva chceme hodnotit. Jejich výběr závisí buď na vstupním auditu, na preferencích organizace, či na kombinaci obojího.

3.3 Soupis aktiv

Po vybrání aktiv, která chceme hodnotit, je sepíšeme. Soupis se může skládat jen ze seznamu aktiv, nebo můžeme připojit také jejich podrobnější popis, umístění a hodnotu aktiva viz další bod.

3.4 Stanovení hodnoty aktiv

Hodnotu aktiva stanovíme buď podle kupní ceny, vyjádříme ji subjektivní důležitostí pro organizaci, či pokud z aktiva plyne pravidelně zisk tak podle něj. Dále je třeba se zamyslet, jak dobře lze aktivum nahradit a co se bude dít, než se tak stane. Pokud se bude jednat o jedinečné aktivum, tak bude mít pro nás větší cenu, než aktivum ač finančně náročné na pořízení, ale snadno dostupné.

Zvláště obtížné je odhadnout, kolik nás bude stát ztráta důvěry zákazníků, pokuty, soudní náklady.

Pokud máme aktiv mnoho, můžeme je seskupit do bloků s podobnými vlastnostmi a na všechny pak jednoduše aplikovat stejné protiopatření.

3.5 Identifikace hrozeb

Když máme kompletní soupis aktiv i s jejich cenou, tak musíme určit hrozby, které připadají u konkrétného aktiva v úvahu. Pokud hrozba nemůže ovlivnit ani jedno aktivum, tak pro nás není relevantní a my se jí nezabýváme. Metody identifikace jsou různé. Je možné využít literatury a ze seznamu vybrat relevantní hrozby, brainstorming atd.

Každopádně je důležité, aby při identifikaci hrozeb byla vždy přítomna osoba, která má s daným aktivem zkušenosti a může tudíž nabídnout postřehy z praxe.

3.6 Analýza hrozeb a zranitelností

Vytvoříme dvojice hrozba – aktivum a stanovíme úroveň hrozby a úroveň zranitelnosti. Například pokud hrozbou bude útok hackerů a víme, že je hodně pravděpodobný, tak přiřadíme hrozbě velkou váhu. Na druhou stranu, ale pokud máme počítače dobře zabezpečené tzn. zranitelnost je nízká, tak výsledné riziko nebude velké.

3.7 Pravděpodobnost výskytu jevu

Je výhodné také stanovit, jak je pravděpodobný výskyt hrozby – každý den, jednou za rok, jednou za 10 let, téměř nikdy. Podle toho také stanovujeme úroveň hrozby.

3.8 Měření rizika

Při stanovování míry rizika pracujeme s veličinami, které většinou nelze přesně matematicky vyjádřit – změřit. Velikost rizika většinou určuje specialista a to kvalifikovaným odhadem založeným na jeho zkušenostech a citu. Proto se také pro označení míry rizika používají stupnice buď slovní (velké – malé) nebo bodová stupnice od 1 do 10, kdy 1 značí nejmenší riziko a 10 nejvyšší. Pokud bychom přesto chtěli zjistit, podle čeho se takový „odhad“ dělá, tak nejdůležitější faktorem je četnost výskytu respektive pravděpodobnost ztráty. Dalo by se říci, že riziko stoupá, čím je větší pravděpodobnost, že výsledek se odchýlí od příznivého výsledku.

Ještě je dobré připomenout, že je nutno hodnotit také podle možnosti výše ztráty. Jinak budeme hodnotit riziko, u kterého může dojít ke ztrátě 1000 Kč a jinak, když můžou jít ztráty do milionů.

4.0 Řízení rizika (Risk management)

Jedná se o proces, kdy se s pomocí získaných údajů snažíme zamezit vzniku rizika, navrhujeme opatření na snížení rizika, vyhodnocujeme efektivitu navržených opatření, přijímáme podněty na nová rizika. Pokud není možné riziko snížit

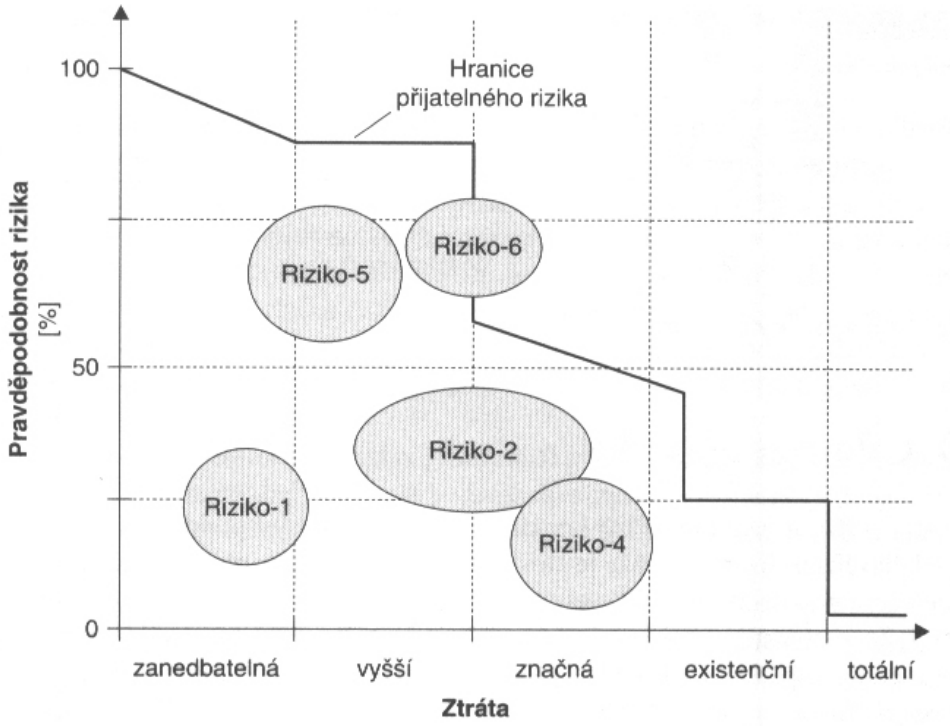
na akceptovatelnou úroveň, musíme mít připraven plán kontinuity, abychom mohli po výskytu hrozby provést co nejrychlejší nápravu a minimalizovat tak škody.

4.1 Cíle řízení rizika

Cíl, proč chceme řídit rizika, by se měl překrývat s podnikatelským záměrem. Tzn. rizika řídíme, aby firma mohla plnit své poslání. Pokud je naším cílem expandovat na trhu, pak se naše hlavní pozornost zaměří na analýzu možné velikosti ztrát, pokud nenaplníme náš záměr.

Po stanovení možného finančního dopadu na firmu u jednotlivých rizik je pak můžeme dělit do tří skupin[6]:

- kritické riziko – veškerá ohrožení, jejichž potenciální ztráty jsou takového řádu, že vyústí v bankrot firmy
- důležité riziko – ohrožení, jehož potenciální ztráty nevyústí v bankrot, avšak další provoz bude vyžadovat, aby si firma půjčila finanční prostředky
- běžné riziko – ohrožení, jehož potenciální ztráty mohou být pokryty stávajícími aktivy firmy nebo běžným příjmem, aniž by došlo k nepatřičnému finančnímu tlaku



Graf 2 Rizikové pozice

4.2 Přínosy řízení rizika

Z řízení rizika benefitují hlavně organizace a manažeři, kteří mohou lépe plánovat projekty a rozvoj firmy. Výhody přináší také pro klienty, protože mají záruku, že dodávané zboží nebo služby budou odpovídat zadaným kritériím.

Přínosy mohou být rozděleny do dvou skupin:

Tvrdé přínosy – statistika, rozhodování

Měkké přínosy – přínosy lidem

Tvrdé přínosy[7]

- Umožňují vypracování věrohodnějších plánů s lepšími informacemi, časovými plány a rozpočty.
- Zvyšují pravděpodobnost dodržování projektu podle tohoto plánu.
- Vedou k používání nejvhodnějšího typu smluv.
- Odrazují od přijetí finančně nezdravých projektů.
- Přispívají k vybudování statistických informací, které pomáhají lépe řídit budoucí projekty.
- Umožňují objektivnější porovnání alternativních návrhů.

Měkké přínosy[7]

- Zlepšují zkušenost korporace a celkovou komunikaci.
- Pomáhají rozvíjet schopnost zaměstnanců při hodnocení rizik.
- Soustřeďují pozornost managementu projektu na skutečné a nejdůležitější problémy.
- Usnadňují převzetí většího rizika a tak získání většího přínosu.

4.3 Klasifikace rizik

Základní dělení rizik je na neovlivnitelná a ovlivnitelná. Neovlivnitelné riziko je třeba politická situace nebo zvýšení úrokových sazeb ČNB. Na druhou stranu na ovlivnitelná rizika můžeme působit protiopatřeními a tím je snižovat či částečně odstranit. Jak již bylo zmíněno výše, je třeba si určit, zda a do jaké míry se nám snižovat riziko vyplatí. Pokud bychom chtěli riziko „snížit“ na nulu, pak se nutně musíme oblasti, kde se riziko vyskytuje, vyhnout, tzn. nevěnovat se jí.

Finanční a nefinanční

Pod pojmem finanční ztráta máme na mysli konkrétní objem peněz, o které jsme přišli. Např. ušlý zisk, poškození majetku. V konečném důsledku lze vyjádřit veškerý typ ztráty v penězích, ale nás zajímají hlavně ztráty s jasně definovanou cenou pro firmu.

A koho se finanční ztráta týká? Hlavním stranou finanční ztráty je samotná firma, konkrétně pak. aktivum, u kterého může dojít k poškození nebo ke ztrátě a dále pak hrozba, která ztrátu vyvolá.

Statické a dynamické

Ztráty díky statickým rizikům vznikají díky přírodním katastrofám či selhání jednotlivce. V jejich důsledku dochází k zničení či odcizení majetku a nemohou být nikdy pro společnost přínosem. Na druhou stranu jsou tato rizika celkem dobře předvídatelná a tak se na ně můžeme pojistit.

Oproti tomu dynamická rizika se špatně předvídají a nemůžeme je řídit. Pokud se ale vyskytnou, tak je můžeme využít i k růstu firmy. Jako příklad bych uvedl pokles kurzu koruny vůči dolaru. Míra této události se nedá předvídat v dostatečném časovém předstihu, neboť na ní má vliv mnoho faktorů, ale pokud jsme firma zabývající se dovozem, tak na ni vyděláme. Pokud bychom se ale zabývali vývozem, tak proděláme. My se dále budeme zabývat riziky dynamickými, u nichž existuje variabilita jejich zpracování.

Čistá a spekulativní

U čistého rizika buď ke ztrátě dojde a nebo nedojde. Není zde ale možnost něco získat. Pokud například vlastníme server, tak nám ho buď ukradnou a nebo ne. To se bavíme čistě o hardware jako o majetku.

Při spekulativním riziku může dojít ke ztrátě a nebo zisku. To záleží na okolnostech. Když se vrátím zpět k ilustraci za použití serveru. Pokud mám na něm uložena data pacientů, tak riziko představuje, že je mohu omylem smazat, což by se mi na papírové kartě pacienta tak snadno nestalo. Ale výhodou a možným ziskem vyvažujícím riziko je, že mám k datům rychlejší a snazší přístup. Takže pokud si uvědomím, jaké mně možnost uložit data na server přinese výhody a jaká přináší rizika, mohu pak přijmout opatření nasměrovaná proti hrozbě ztráty dat.

4.4 Metody snižování rizika

Obecně lze říci, že rizika patří neoddělitelně k běžnému provozu firmy a my máme hned několik možností, jak snížit jejich dopad na firmu. Pokud řešíme rizika ve firmě, tak je můžeme označit buď jako riziko s velkým dopadem (vysoká tvrdost) nebo riziko s nízkým dopadem (nízká tvrdost). Pak jej lze také zařadit podle pravděpodobnosti jeho výskytu – buď je pravděpodobnost vysoká, nebo nízká. A podle zařazení pak volíme metodu snížení rizika, podle následující tabulky.

	Vysoká pravděpodobnost	**Nízká pravděpodobnost**
Velký dopad (tvrdost)	Vyhnutí se riziku, redukce	Pojištění
Malý dopad (tvrdost)	Retence a redukce	Retence

Tab. 1 Metody pro řešení rizik ve firmě

Retence rizika

Zadržení (retence) rizika je velmi populárním řešením rizika. Jedná se o případ, kdy o riziku víme, ale přijmeme jeho možný dopad, pokud se projeví. To mluvíme o retenci vědomé. Ještě také existuje retence nevědomá, kdy o riziku nevíme – nerozpoznáme jej a to je velmi nebezpečný jev, kdy se nám může stát, že přehlédneme riziko s velkým dopadem, kdy měla být použita např. metoda redukce.

Stanovit hranici, kdy ještě není riziko tak velké, není snadné. Záleží hlavně na možnostech firmy, jak velký finanční objem si může dovolit ztratit. Něco lze pokrýt z rezerv firmy, z půjčky. Ale na některé ztráty nestačí ani tento postup.

Redukce rizika

Riziko můžeme snížit pomocí:

- eliminace nebo snížení pravděpodobnosti vzniku rizika
- zmenšením důsledků plynoucích z výskytu nepříznivé situace

Pojištění

Již jsme mluvili o možnosti riziko redukovat, dále můžeme riziko zadržet a dalším z důležitých mechanizmů je pojištění. Možná se to bude zdát na první pohled nerozumné, ale není dobré pojišťovat se na riziko, u kterého je vysoká pravděpodobnost výskytu. Proč? Protože pojištění bude v tomto případě velmi vysoké a pro nás bude výhodnější využít jiný způsob snížení rizika a to cestou vyhnutí se riziku nebo jeho

redukcí protiopatřeními. Je výhodné se pojišťovat na rizika, která můžou mít velký dopad, ale nejsou moc pravděpodobná. Pojišťovací suma nebude závratně vysoká, a pokud dojde k naplnění rizika, tak pojištění nám pomůže pokrýt jeho dopad.

Pojištění je vlastně přesun rizika a kapitálu z jednoho subjektu (naší firmy) na subjekt jiný (pojišťovna). Nevýhodou je sice nutnost pravidelně platit poplatky za pojištění, ale zase nemusíme mít vytvořeny rezervy a tím se nám zvýší objem kapitálu volného k investicím.

Důležité také je si podrobně prostudovat pojišťovací smlouvy, abychom věděli, na co se pojištění vztahuje a na co ne a v jaké výši nám uhradí pojišťovna případnou škodu.

Jako příklad, co lze pojistit bych uvedl: odpovědnosti za škodu, proti živelným katastrofám, úvěrová rizika atd. Ne všechno lze ale pojistit, např. ztrátu dobrého jména.

Vyhýbání se rizikům

Vyhýbání se rizikům je účinná metoda ve smyslu redukce rizika, ale na druhou stranu jde proti smyslu podnikání. Vyhnutí se rizikům může znamenat vyhnutí se příležitostem.

S každou aktivitou jde ruku v ruce určité riziko. Jak se říká: „Nevstoupíš dvakrát do téže řeky“ tak zrovna nemůžeme přesně vědět, co naše rozhodnutí přinese. Máme určitá očekávání a proti nim působí riziko, které nese. Pokud se budeme neustále vyhýbat ve firmě riziku, tak firma neporoste nebo zkrachuje, neboť konkurence, která bude zdravě riskovat, bude úspěšnější a přebere nám zákazníky.

Vytváření rezerv

Ke každému podnikání by mělo patřit vytváření rezerv. Většinou se jedná o materiálové nebo finanční rezervy. Zásoby materiálu jsou dobré pro pokrytí výroby v době váznutí dodávky. Finanční rezervy, a to ať už tvořené účetně z aktiv firmy a nebo lépe přímo finance uložení v samostatném fondu nám pomohou, stejně tak jako pojištění, když se firma dostane do potíží. Výhodné je kombinovat pojištění a vytváření rezerv, abychom měli dostatek zdrojů, ze kterých lze v případě krize čerpat.

5.0 Rizika v informačních technologiích

V dnešní době jsou informační systémy využívány k shromažďování a zpracování velkého množství informací organizace a z toho vyplývá možnost značného dopadu na fungování organizace při jejich ztrátě či kompromitaci. Musíme chránit informace nejen v psané formě, ale i digitální a mluvené, chránit informace při přenosu a zpracování. Potenciálním rizikem je používání telefonu, faxu, počítačových sítí ať již LAN, WAN, dálkového přístupu k datům nebo internetu.

Zde je pro příklad několik oblastí, o které bychom se měli zajímat:

5.1 Technologie jako taková

Zde se jedná o samotný hardware a software. Pokud třeba zavádíme další část sítě, další databázi a náš současný server či infrastruktura není dostatečně dimenzovaná zvládnout nový nápor. Nebo je naše vybavení zastaralé a nespolehlivé.

5.2 Zabezpečení prostředků

Zahrnuje jak fyzické zabezpečení vybavení, tak zabezpečení dat na počítačích. Příklady rizik jsou: ztráta nebo poškození konzistence dat např. při pádu sítě; povodeň či požár. Krádež dat nebo celého počítače. Neautorizovaný přístup k informacím např. přes internet nebo získání přímého fyzického přístupu k datům.

Zde je několik běžných příkladů, na co bychom neměli zapomínat:[8]

- Provádět pravidelné zálohy důležitých dat na počítačích a udržovat kopie na jiném místě
- Používat pravidelně aktualizovaný antivirový software
- Používat odpovídající firewall
- Používat hlavně u serverů zdroje nepřetržitého napájení (UPS)
- Na serverové straně využívat disková pole (RAID), abychom minimalizovali dopad poruchy pevného disku
- Při velkém množství dat je dobré mít záložní server, který bude možné použít, pokud dojde k poruše hlavního serveru
- Pravidelně záplatovat operační systém
- Pravidelně zálohovat a archivovat data, testovat integritu záloh
- Kvalitní servisní smlouvy

- Zabezpečení prostor
- Řízení přístupu do sítě a k aplikacím

5.3 Zdraví a bezpečnost

Zdánlivě toto téma nesouvisí s IT, ale opak je pravdou. S počítači pracují lidé a my musíme myslet na jejich bezpečnost. Jedním z rizik jsou rizika zdravotní: problémy s pohybovým aparátem, únava očí. Dalším z možných problému jsou volně položené kabely, špatně nainstalované zařízení, chyby v elektroinstalaci. To vše představuje potenciální riziko pro zaměstnance, potažmo pro firmu. Firma pak musí platit odškodné za úraz na pracovišti a v neposlední řadě jim zaměstnanec chybí, protože se léčí.

5.4 Právní postihy

V počítačích jsou uložena účetní data, informace o mzdách apod. Pokud dojde k jejich ztrátě, nebo jen nedostupnosti, tak se vystavujeme riziku finančního postihu např., ze strany finančního úřady, dále pak nemožnost vyplatit zaměstnancům mzdy atd.

Dále pak některé organizace musí podle zákona umožnit práci s informacemi a vybavením tělesně postiženým např. státní instituce musí mít přístupný web, aby s ním mohli pohodlně pracovat i zdravotně postižení lidé.

A v neposlední řadě je třeba dbát na nutnost mít licencovaný software, dodržovat ochranu osobních informací, autorský zákon, neumožnit zaměstnancům využívat výpočetní prostředky firmy k nelegální činnosti (např. stahování filmů z internetu).

Při porušování zákonných norem, vztahujících se k dané problematice, např. Zákona na ochranu osobních údajů 101/2000 Sb, hrozí pokuta až 10 mil. Kč.

5.5 Ztráta klíčové osoby

Tento problém je častý, pokud klíčové informace zná jen jedna osoba. Co se stane, pokud odejde nebo hůře – zemře? Je třeba informace rozložit na více osob, dokumentovat důležité informace a postupy (např. heslo administrátora).

Našim cílem tedy je dosažení dostatečné bezpečnosti. Její úroveň nejlépe zhodnotíme podle nějaké normy nebo standardu.

„Bezpečnost informací lze dosáhnout implementací soustavy opaření, která mohou existovat v podobě pravidel, natrénovaných postupů, procedur, organizační struktury a programových funkcí.“[9]

6.0 Normy a standardy

Problematika norem a ISO standardů je poměrně obsáhlá a složitá a přesahuje rámec této práce. Existuje několik norem, ze kterých lze vycházet, ať se již jedná o normy vydané v Británii - British Standards Institution nebo mezinárodní normy ISO či české ČSN. Aby to nebylo jednoduché, tak jedna z druhé vycházejí a jsou často aktualizovány. Vše ale směřuji k zpřehlednění a vytvoření nové série ISO 27000. V současnosti je k dispozici ISO 27001 s jehož výkladem nám může pomoci kniha Systém managementu bezpečnosti informací[10]. Jak tuto normu aplikovat nám pomůže ISO/EIC 17799. A konečně poslední důležitou normou je ISO/EIC TR 13335-1, která popisuje metodiku řízení. Pokud budete normy shánět, doporučuji se obrátit na Český normalizační úřad.

Více se dozvíte třeba na www.iso27001security.com.

Praktická část

Všeobecná fakultní nemocnice (dále VFN) se rozhodla, že vzhledem ke své velikosti, velké míře využívání výpočetní techniky a velkého množství citlivých dat podléhající legislativní ochraně (zdravotní dokumentace) implementuje vhodný systém řízení a zpracování rizik. Výsledkem by měl být transparentní a pružný systém, kde bude jasně dané, kdo za jakou činnost či aktivum odpovídá, jak je aktivum chráněno, jaká mu hrozí rizika a jak s nimi naložíme. V konečném důsledku budou data pacientů a nemocnice bezpečnější a bezpečnost půjde ověřit proti dané normě. V našem případě pak ISO 27001 potažmo norem, které s ní souvisí.

Ke spolupráci jsem se dostal ve fázi, kdy byl již proveden prvotní audit specializovanou firmou. Byly zjištěny nedostatky, kdy nejsou definovány některé z důležitých předpisů zabezpečení informací nebo jsou zastaralé, není přesně definováno proškolování zaměstnanců v oblasti výpočetní techniky. Je třeba také zlepšit zabezpečení prostor proti neoprávněnému vstupu a zlepšit pravidla pro používání

a likvidaci přenosných médií. Konkrétní nálezy pak jsou součástí podrobného auditu, který má k dispozici informační oddělení VFN.

Nyní probíhá intenzivní práce na nápravě nedostatků. Jednou z důležitých oblastí je také systém řízení informačních rizik tzn. konkrétní implementace výše zmíněné teorie řízení rizik pro potřeby VFN.

Při rozhodování jaký systém evidence a zpracování problematiky rizik nasadit, bylo nutné řídit se požadavky nemocnice. Jako nejvhodnější se vzhledem k velikosti organizace jevilo nasadit specializovaný software. Po poradě ale vzešel požadavek nepoužívat další software, a tak bylo rozhodnuto použít excelový soubor, který bylo potřeba upravit pro potřebu nemocnice, neboť dříve byl používán jen pro menší organizace.

Mým úkolem bylo právě přizpůsobit excelový soubor, pro potřeby VFN, potažmo větší organizace. Jelikož je pak know-how a postupy použité v souboru vlastnictvím firmy, která provádí jeho implementaci a pro kterou jsem úpravy dělal, tak není soubor součástí bakalářské práce. Upozorňuji, že některé dále uvedené postupy jsou duševním vlastnictvím firmy a vztahuje se na ně autorský zákon.

Moje práce se skládala ze dvou hlavních oblastí: přizpůsobit vzhled tabulek a vzorce potřebám větší organizaci a naprogramovat makra, která by ulehčila a zautomatizovala běžné činnosti při řízení rizik.

7.0 Využití excelu k řízení rizik

7.1 Karta Rizika

Rozhodl jsem se začít na listu Rizika, který je alfou a omegou celého řešení. Nejprve přišlo na řadu zjistit, která pole co dělají, neboli logiku fungování „aplikace“. Poté následovala diskuze nad zpracováním řešení určitých prvků. Například Aktuální stav rizika: pro vývěr sice existovala rozbalovací lišta, ale jelikož byla řešena přes funkci ověření dat, tak byl seznam vidět až po kliknutí na buňku. Provedl jsem tedy výměnu za formulářový prvek Pole se seznamem. Podobně jsem postupoval i u hodnocení kategorie hrozeb a hodnocení významu rizika, kde se původně prováděl výběr možností pomocí zapsání písmene „x“ do příslušné buňky. Já jsem je nahradil zaškrtávacími políčky potažmo přepínači.

U výsledků hodnocení jsem provedl ošetření, aby pokud není zadáno datum hodnocení se nezobrazoval koeficient i když omylem vyberu volbu v Hodnocení významu rizika, kterou jsme ještě nehodnotili.

Posledním krokem bylo vybrat pole, která budou použita při stanovení opatření a která budou posléze včleněna do Plánu zvládání rizik.

Jako zajímavost a vlastně nejjednodušší makro slouží tlačítko Nové hodnocení. Makro se nás zeptá na datum, ke kterému chceme provést nové hodnocení (přednastaveno je aktuální datum) a pak jej zapíše na příslušná místa na kartě Rizika.

Následovalo grafické sladění barev a formátů, aby byly jednotné napříč dokumentem.

7.2 Registr rizik

Jelikož je nemocnice velkou organizací, tak bude rizik poměrně hodně. Odhadem přibude každý rok 20–30 rizik. V jejich orientaci nám pomůže registr rizik. Makro má za úkol jednak zkopíruje list Šablona rizika, přejmenuje ji na číslo rizika, které ještě nemáme a zařadit za poslední vytvoření riziko. Dále pak vloží na volný řádek v listu Registr rizik odkazy na určená buňky z nové karty rizika. Odkazy proto, aby když provedeme změny na kartě rizika, tak se nám ihned promítnou do Registru rizik. Každý řádek tak odpovídá jedné kartě potažmo jednomu riziku.

7.3 Plán zvládání rizik (PZR)

Dalším důležitým prvkem řízení rizik je Plán zvládání rizik (PZR). Ten budeme generovat vždy ke konkrétnímu datumu, např. jednou za čtvrtletí. Makro provede vytvoření nového listu (kopie šablony) – podívá se jaké číslo plánu je poslední např. PZR1, PZR2. Dalším makrem pak automaticky projdeme všechny karty rizik, podíváme se, které Opatření ještě nemá přiřazeno číslo PZR a nebo má číslo shodné s aktuálním plánem a provedeme zkopírování údajů z Opatření do Plánu zvládání rizik. S tímto aktuálním plánem pak pracuje management při rozhodování, jak a s kterým rizikem v daném období naloží. Jakmile je plán schválen a má vyplněné datum, není možné jej znovu (omylem) generovat. Tentokrát se na data nevkládá odkaz, ale jsou přímo kopírována, aby bylo zamezeno nekonzistenci dat.

7.4 Registr Plánů zvládání rizik

Jedná se o obdobu Registru rizik. Na jednom listu vidíme přehled všech PZR s jejich základními údaji.

7.5 Šablony

Pro větší přehlednost jsem přesunul data, která se používala ve vyhodnocovacích vzorcích na samostatný list Parametry. Dále pak jsou listy Parametry, Šablona rizik a Šablona PZR skryté, a odhalí se jen po zadání hesla. Důvodem je snaha zabránit běžným uživatelům měnit výchozí parametry.

7.6 Celkový obsah souboru

Registr hrozeb – soubor nejčastějších hrozeb, které hrozí v oblasti výpočetní techniky

- Registr rizik – soupis všech rizik a jejich nejdůležitějších charakteristik
- Rating rizik – statistické vyjádření závažnosti rizika a jeho aktuálního stavu
- Registr plánů – soupis všech plánů zvládání rizik
- R1 – Rx – Konkrétní karty rizik
- PZR1 – PZRx – Plány pro určitá období
- SablonaR – šablona pro nové riziko
- SablonaPZR – šablona pro nový plán
- Parametry – zdroj proměnných

7.7 Problémy při tvorbě

Prvním z problémů, se kterým jsem se potýkal, byla nejednotná terminologie. Stejný údaj byl jinak označen na kartě rizika a jinak v registru rizik, některá pole pro datumy byla duplicitní apd.

Druhým problémem bylo samotné programování. Jelikož nejsem programátor a jazyk VBA téměř neznám, tak pro mne bylo náročné rychle proniknout do principu jeho fungování. Důsledkem toho jsou občas nehezké konstrukce v kódu makra, kdy by konkrétní postup šel řešit jistě elegantněji, ale zabral by mi mnohem více času při tvorbě. Samotný kód jsem opatřil množstvím komentářů, aby bylo snadnější v budoucnu něco dodělat či upravit.

8.0 Konkrétní kroky při řízení informačního rizika ve VFN

V následující části se pokusím přiblížit postup, jakým s riziky pracujeme. Jako zdroj používám pracovní postup Řízení informačních rizik vypracovaný pro VFN.

8.1 Identifikace rizika

Zdroje zjišťování slabých míst

- náměty zaměstnanců – jejich podněty pro zlepšení bezpečnosti a provozu
- havárie, výsledky řešení bezpečnostních incidentů
- interní a externí audity, revize
- nesoulad v průběhu plánování
- výstupy z monitoringu
- přezkoumání systému bezpečnosti informací

Tyto údaje shromažďujeme, a pokud najdeme relevantní hrozbu, která může působit na zranitelnost, vzniká riziko a my jej musíme zpracovat.

Číslo rizika

- jedná se o pořadové číslo rizika, shoduje se s číslem karty (karty pojmenované R1, R2, ... Rx) Toto pole nevyplňujeme, k jeho vyplnění dojde automaticky při vytvoření karty rizika makrem

Název rizika

- Jednoznačný název, který popíše riziko

Datum hodnocení

- Datum posledního hodnocení rizika

Aktuální stav rizika

- Pomocí roletkového menu nastavíme status, ve kterém se riziko nachází.
- Máme tyto možnosti: Identifikované riziko, Provedená analýza a hodnocení rizika, Plánované opatření, Schválené opatření, Realizované opatření, Opakované hodnocení, Akceptované riziko, Eliminované riziko, Vyhnutí se riziku

Zahrnuto do plánu kontinuity

- V roletkovém menu vyberu Ano/Ne
- Plán kontinuity popisuje, co dělat, pokud se hrozba projeví, respektive jakým způsobem uvést věci do stavu před působením hrozby

Číslo plánu kontinuity

- Uvedeme číslo plánu kontinuity

Zařazeno a vyřazeno dne

- Datum zařazení a vyřazení rizika tzn. od kdy jsme se o riziko začali zajímat a kdy jsme skončili

Popis zranitelnosti/rizika:

- Provedeme podrobný popis zranitelnosti a rizika a všech souvislostí, které jsou potřebné k hodnocení rizika

Kategorie hrozby

- Určuje kategorii možných dopadů, máme pět možností s tím, že mnohdy může mít hrozba více dopadů. Jsou to tyto:
- Ztráta důvěrnosti – Vyzrazení obsahu informací, zpřístupnění neoprávněným osobám
- Porušení integrity – zničení informací, poškození obsahu nebo struktury
- Ztráta dostupnosti – informace nejsou dostupné v potřebném čase
- Ztráta autentičnosti – nelze prokázat původ informace, nespolehlivá autentizace
- Ztráta spolehlivosti – nespolehlivý obsah informací např. chybné zadání informací nebo jejich nežádoucí modifikace

8.2 Hodnocení rizika

Odhad možné škody

Zhodnocení se provádí kvalifikovaným odhadem tzn. provede jej odborník zkušený v dané oblasti. Konkrétně v našem případě se rozhodujeme v kategoriích: do 10 tis., do 100 tis., nad 100 tis., nad 1 mil., nad 10 mil.

Zranitelnost

Správné určení úrovně zranitelnosti (slabého místa) má velký význam, pro zhodnocení, jak je riziko závažné a jak rychle se jím musíme zabývat. S určením zabezpečení nám může pomoci následující tabulka, ve které si najdeme sloupeček, který odpovídá současné úrovni bezpečnostních opatření, a pak v příslušném řádku odečteme úroveň zranitelnosti.

Slabé místo (zranitelnost)		**S aktivem související bezpečnostní opatření**				
		Absence/ nefunkčnost	Účinnost bezpečnostního opatření			Více účinných opatření
			Nízká	Střední	Vysoká	
Úroveň zranitelnosti	Zanedbatelná					X
	Nízká				X	
	Střední			X		
	Vysoká		X			
	Velmi vysoká	X				

Tab. 2 Určení úrovně zranitelnosti

Pravděpodobnost výskytu

Posledním důležitým parametrem je pravděpodobnost výskytu. Zde se rozhodujeme ve škále: Zanedbatelná, Nízká, Střední, Vysoká, Velmi vysoká, čemuž odpovídají hodnoty 1,2,3,4,5

Koeficient

Koeficient významu rizika získáme součinem koeficientu Zranitelnosti a Pravděpodobnosti výskytu.

Význam rizika

Výslednému koeficientu pak přiřadíme pro přehlednost slovní hodnocení podle tabulky:

Vyhodnocení významu (závažnosti) rizika	Koeficient	
	Od	Do
Zanedbatelný	1	5
Nízký	6	10
Střední	11	15
Vysoký	16	20
Velmi vysoký	21	25

Tab. 3 Vyhodnocení významu rizika podle koeficientu

8.3 Nakládání s rizikem

Riziko přijato

Zde máme volbu Ano/Ne. Určuje, zda jsme riziko přijali a nebudeme dělat žádná další opatření. Je důležité, pokud nějaké riziko přijmeme, abychom po nějakém čase zhodnotili, zda se nezměnily podmínky rizika, tzn. možná změna hrozeb a zranitelností. Pak se může stát, že budeme muset přijímat další opatření adekvátní nastalé situaci.

Organizace by se měla rozhodnout, že nelze akceptovat vysoká rizika. Ve VFN je prostřednictvím vnitřní směrnice určeno, že akceptovat riziko lze pouze, pokud není hodnoceno výše než „střední“.

Návrh opatření

Po každém zhodnocení rizika musí následovat (pokud riziko nepřijmeme) návrh opatření. Buď jednoho, nebo několika.

U opatření vyplňujeme jeho název, popis, číslo plánu zvládání rizik (viz dále), osobu, která za opatření zodpovídá, odhadované náklady na opatření a datum zápisu.

Důležité je datum zápisu, podle kterého poznáme, k jakému hodnocení se vztahuje.

Jako příklad opatření lze uvést: proškolení zaměstnanců, omezení související činnosti, zpracování havarijního plánu.

8.4 Konkrétní příklady rizik ve VFN

Riziko 1

Název: Škody způsobené zaměstnanci dodavatelů

Popis: Nedostatečná smluvní ujednání s dodavateli a servisními organizacemi mající přístup k informačním technologiím a informacím – nejsou prověřování zaměstnanci dodavatelů, chybí doložky mlčenlivosti, není sjednána povinnost pojistit se proti škodám způsobených zaměstnanci dodavatelů, atd.

Kategorie hrozby: Ztráta důvěrnosti, Porušení integrity, Ztráta dostupnosti, Ztráta spolehlivosti

Hodnocení: Při prvním hodnocení hodnoceno riziko jako vysoké.

Návrh opatření:

1. Úprava organizačně řídící dokumentace
   Vytvoření pravidel pro tvorbu smluv a stanovení odpovědnosti
2. Přenos rizika na jiný subjekt smlouvou
   Revize stávajících smluv a vytvoření dodatků
3. Nastavení stálého perimetru
   Prověřování znalostí zaměstnanců smluvních partnerů

Riziko 2

Název: Nepatřiční chování zaměstnanců, zpřístupnění citlivých informací

Popis: Chybí dokumentované postupy a pravidla pro žádoucí chování zaměstnanců, zaměstnanci nemají potřebné znalosti a zvyklosti

Kategorie hrozby: Ztráta důvěrnosti, Porušení integrity, Ztráta dostupnosti, Ztráta autentičnosti, Ztráta spolehlivosti.

Hodnocení: Při prvním hodnocení hodnoceno riziko jako velmi vysoké.

Návrh opatření:

1. Snížení nebo odstranění hrozby
   Implementovat normu ISO 27001:2006
2. Nastavení stálého perimetru
   Pravidelná školení, opakované prověřování zaměstnanců formou intranetových testů

Závěr

Řízení rizik se v dnešní době začíná věnovat velká pozornost a nejinak je tomu v oblasti výpočetní techniky. Ve své práci jsem se pokusil problematiku přiblížit co nejsrozumitelnějším jazykem, díky čemuž ale místy vznikly drobné nepřesnosti. Tato práce si neklade za cíl podat vyčerpávající informace o řízení informačních rizik, ale uvést do problematiky a na praktické ukázce z Všeobecné fakultní nemocnice demonstrovat jeden z přístupů, jak lze oblast informačních rizik řešit. (Pro získání podrobnějších informací doporučuji prostudovat uvedenou literaturu a normy.)

Pokud chceme v naší firmě zavést systém řízení rizik, máme dvě možnosti: buď se sami dáme do studování problematiky, projdeme všechny související směrnice, ISO normy a zákony, a nebo si najmeme firmu, které se touto problematikou zabývá a necháme na ní, aby zavedla systém řízení rizik v naší firmě. V prvním případě nás to bude stát mnoho času, než do problematiky pronikneme a je pravděpodobné, že nějakou důležitou věc přehlédneme. Druhá možnost od nás ale také bude vyžadovat účast. Vyžádá si několik porad s konzultanty firmy a neobejde se bez podpory managementu.

Každý, kdo se ve firmě bude podílet na implementaci systému řízení rizik, by se měl seznámit alespoň se základními pojmy jako jsou: aktivum, zranitelnost, hrozba či protiopatření. Dále je dobré, aby si firma a hlavně vedení byly vědomy, proč systém řízení rizik zavádějí – zda bude pro firmu přínosem a co pro jeho zavedení budou muset udělat.

Řízení informačních rizik je jen jednou z oblastí systému řízení rizik, ale lze na ni dobře demonstrovat obecně platné postupy a v případě úspěšného zavedení ve firmě může pak být řízení rizik využito i v jiných oblastech fungování firmy.

V případě VFN je výhodné zavést systém řízení informačních rizik proto, že každé oddělení využívá množství výpočetní techniky a bez ní by byl provoz v nemocnici velmi omezen.

Využití excelového souboru pro řízení rizik je vhodné spíše pro menší organizace než je VFN. Zde jsme přistoupili k jeho využití, protože nemocnice nechtěla instalaci dalšího softwaru. Pro organizaci o velikosti VFN bych doporučil využití specializovaného softwaru určeného pro řízení rizik.

Citace

1 KRAUSE, Jiří, PETRÁČKOVÁ. Věra. Akademický slovník cizích slov. Praha: Academia, 2001. 833 s. ISBN 80-200-0607-9. heslo: riziko.

2 SMEJKAL, Vladimír, RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. Praha: Grada Publishing a.s., 2006. 300 s. ISBN 90-247-1667-4. str. 78.

3 SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada Publishing a.s., 2006. 300 s. ISBN 90-247-1667-4. str. 83.

4 SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada Publishing a.s., 2006. 300 s. ISBN 90-247-1667-4. str. 82.

5 SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada Publishing a.s., 2006. 300 s. ISBN 90-247-1667-4. str. 83.

6 SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada Publishing a.s., 2006. 300 s. ISBN 90-247-1667-4. str. 104.

7 MERNA, Tony, AL-THANI, Faisal F. *Risk management – Řízení rizika ve firmě*. Brno: Computer Press a.s., 2007. 208 s. ISBN: 978-80-251-1547-3. str. 37.

8 LASA INFORMATION SYSTEMS TEAM. *ICT Risk Assessment* [online]. [cit. 30. 5. 2008] Dostupné z WWW: <http://www.icthubknowledgebase.org.uk/riskassessment>.

9 SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada Publishing a.s., 2006. 300 s. ISBN 90-247-1667-4. str. 198.

10 ŠEBESTA, V. Systém managementu bezpečnosti informací. Praha: ČNI. ISBN 978-80-7283-239-2.

Literatura

[1] SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada Publishing a.s., 2006. 300 s. ISBN 90-247-1667-4.

[2] MERNA, Tony, AL-THANI, Faisal F. *Risk management – Řízení rizika ve firmě*. Brno: Computer Press a.s., 2007. 208 s. ISBN: 978-80-251-1547-3.

[3] NOVÁK, Luděk. *Proč a jak řídit informační rizika ve veřejné správě* [online]. [cit. 30. 5. 2008] Dostupné z WWW: <http://www.anect.com/cs/info/tiskove-centrum/novinky/anect-na-konferenci-isss-2006/_files/rizika-lunovak.pdf>.

[4] LASA INFORMATION SYSTEMS TEAM. *ICT Risk Assessment* [online]. [cit. 30. 5. 2008] Dostupné z WWW: <http://www.icthubknowledgebase.org.uk/riskassessment>.

[5] WIKIPEDIA. *Risk management* [online]. [cit. 30. 5. 2008] Dostupné z WWW: <http://en.wikipedia.org/wiki/Risk_management>.

[6] ČSN ISO/IEC TR 13335-1:1999

[7] Pracovní postup VFN – Řízení informačních rizik

Seznam grafů a tabulek

Příloha č. 1

Ukázky z karty rizika:

Karta rizika **číslo: 1**

Název rizika: **Nepatřiční chování zaměstnanců, zpřístupnění citlivých informací**

Datum posl. hod: 30.6.2008 — Nové hodnocení

Aktuální stav rizika: Opakované hodnocení

Zahrnuto do plánu kontinuity: Ne — Číslo plánu:

Popis zranitelnosti/rizika: — Zařazeno dne: — Vyřazeno dne:

Chybí dokumentované postupy a pravidla pro žádoucí chování zaměstnanců, zaměstnanci namají potřebné znalosti a zvyklosti

Kategorie hrozby:	Ztráta důvěrnosti	Porušení integrity	Ztráta dostupnosti	Ztráta autentičnosti	Ztráta spolehlivosti
	☑	☑	☑	☑	☑

	Hodnocená kritéria	Datum	do 10 tis.	do 100 tis.	nad 100 tis.	nad 1 mil.	nad 10 mil.
	Odhad možné škody	05.01.08	○	○	○	○	◉
		05.03.08	◉	○	○	○	○
		30.6.2008	◉	○	○	○	○
			◉	○	○	○	○
			◉	○	○	○	○
			◉	○	○	○	○
			◉	○	○	○	○
			◉	○	○	○	○

Výsledky hodnocení

	Pořadí	Datum hodnocení	Koeficient	Význam rizika	Poznámka	Riziko přijato
	1	05.01.08	25	Velmi vysoký		Ne
	2	05.03.08	20	Vysoký	Byly vytvořeny některé postupy a pravidla	Ne
	3	30.6.2008	8	Nízký	Implementace normy ISO 2701, providelné školení a prověřová	Ano
	4					
	5					
	6					
	7					
	8					

	Název opaření	Číslo plánu	Zodpovídá	Náklady	Datum zápisu
1	Úprava OŘD (organizačně řídící dokumentace)	2			10.1.2008
Popis	Vytvořit providla pro zaměstnance - Řád používání informačních prostředků, směrnice pro ochranu osobních údajů apod.				
2	Snížení nebo odstranění hrozby	2			10.1.2008
Popis	Implementovat normu ISO 27001:2006				

Příloha č. 2

Ukázka makra včetně komentářů, které vytvoří katu nového rizika

```
Sub NoveRiziko()
'===Vytvořil: Tomáš Jeníček===
'===Revize: 4. 6. 2008===

'===Vytvoření nového listu rizika

Dim ws As Worksheet
Dim PocetRizik
Dim PosledniListRizik
PocetRizik = 0

   For Each ws In ActiveWorkbook.Worksheets 'pro všechny listy v sešitu
     If Left(ws.Name, 1) = "R" And IsNumeric(Mid(ws.Name, 2)) Then
'Pokud první znak je R a 2. je číslo
        PocetRizik = PocetRizik + 1 'Pak udělej toto
     End If
   Next

PosledniListRizik = "R" & PocetRizik

List12.Visible = xlSheetVisible 'Zobrazí dočasně list SablonaR

If PocetRizik = 0 Then 'Pokud není ani jedno riziko
  Worksheets("SablonaR").Copy After:=Worksheets("Rating rizik")
'Zkopíruje list SablonaR. Vznikne SablonaR (2)
  Worksheets("SablonaR (2)").Name = "R" & PocetRizik + 1
 'Přejmenuje list SablonaR (2) na R a číslo z proměné Pocet

'==Zapíše číslo listu
  Range("K1").Select 'Zapíše číslo rizika na nové kartě rizika
  ActiveCell.Formula = PocetRizik + 1

ElseIf PocetRizik > 0 Then 'Pokud již existuje nějaká karta rizika
  Worksheets("SablonaR").Copy After:=Worksheets(PosledniListRizik)
'Zkopíruje list SablonaR. Vznikne SablonaR (2)
  Worksheets("SablonaR (2)").Name = "R" & PocetRizik + 1
'Přejmenuje list SablonaR (2) na R a číslo z proměné Pocet

  Range("K1").Select 'Zapíše číslo rizika na nové kartě rizika
  ActiveCell.Formula = PocetRizik + 1
End If

List12.Visible = xlSheetVeryHidden 'Skryje list SablonaR

End Sub
```