UNIVERZITA PALACKÉHO V OLOMOUCI

FILOZOFICKÁ FAKULTA

Analýza rizik bezpečnosti informací ve vybrané společnosti

Bakalářská práce

Autor: Jan Vajda

Vedoucí práce: Ing. Martin Drastich, Ph.D., MBA

Olomouc 2023

Prohlášení

Místopřísežně prohlašuji, že jsem bakalářskou práci na téma: „Analýza rizik bezpečnosti informací ve vybrané společnosti“ vypracoval samostatně pod odborným dohledem vedoucího práce a uvedl jsem v ní všechny použité podklady a literaturu.

V Olomouci dne 13. 11. 2023 Podpis: Vajda Jan

Poděkování

Rád bych poděkoval vedoucímu mé diplomové práce panu Ing. Martinu Drastichovi, Ph.D., MBA za cenné rady, připomínky a odborné vedení. Mé poděkování patří zároveň firmě B4B INKASSO s.r.o. za ochotu a poskytování informací potřebných pro vypracování mé bakalářské práce. Především bych chtěl poděkovat panu Petru Skulinovi, provoznímu řediteli firmy B4B INKASSO s.r.o. Děkuji také své rodině a přátelům za podporu při zpracovávání bakalářské práce.

Obsah

Úvod

V dnešní době mají informace vysokou hodnotu pro společnosti. Z tohoto důvodu se bezpečnost informací stává jedním z klíčových faktorů úspěšného fungování každé firmy. Vždy hrozí rizika, jako jsou úniky dat, hackerské útoky nebo interní zneužívání informací. Proto je analýza rizik nezbytnou součástí řízení informační bezpečnosti v každém podniku. Analýza rizik nám pomůže identifikovat potencionální hrozby a zranitelnosti, a vypracovat strategii, jak s nimi bojovat.

Cílem bakalářské práce je analýza rizik bezpečnosti informací ve vybraném podniku. V průběhu analýzy budou identifikovány možné hrozby a zranitelnosti informací. Tyto rizika budou následně posouzená z hlediska jejich pravděpodobnosti výskytu a dopadu na společnost.

Teoretická část bakalářské práce je rozdělena na několik částí. První část práce je zaměřena na popis rizika – jeho definice, klasifikace, identifikace, zdroje a řízení rizik.

Další část práce se zaměřuje na analýzu rizik. V této části jsou zejména vysvětleny pojmy analýzy rizik a metody, které lze pro analýzu použít.

Po teoretické části následuje část praktická. V této části je představen analyzovaný podnik a metoda, který byla vybrána pro následnou analýzu. Následně je analýza popsána a je představen seznam identifikovaných rizik. Pro rizika, které překročí stanovenou hodnotu jsou navržena opatření, jak daným rizikům předcházet.

Teoretická část

1. Riziko

„Neexistuje jedna obecně uznávaná definice rizika. Rizikem se obecně rozumí nebezpečí vzniku určité škody, poškození, ztráty či zničení. Pojem riziko se poprvé objevil někdy v 17. a 18. století v matematice při popisu pravděpodobnosti výhry v hazardních hrách a v pojištění lodí. V prvním případě bylo cílem odhadnout pravděpodobnost výhry a v druhém jakou má loď šanci, že se vrátí s nákladem zpět do přístavu a neskončí někde na dně oceánu nebo roztříštěná o skaliska.“[1]

Nedílnou součástí každého podnikatele je podstupování tzv. podnikatelského rizika, které na jedné straně může být spojeno s nadějí na dosažení vynikajících hospodářských výsledků, avšak na straně druhé, to také přináší nebezpečí podnikatelského neúspěchu, který může vést ke ztrátám. Tyto ztráty mohou být někdy tak závažné, že značně naruší finanční stabilitu společnosti a mohou vést až k jejímu zániku. [2]

Pro tuto bakalářskou práci je velmi důležitá bezpečnost informací. Pro toto riziko se nejčastěji uvádí definice, která riziko popisuje jako možnost, že specifická hrozba využije specifickou zranitelnost systému, překoná stávající opatření a způsobí narušení důvěrnosti, integrity nebo dostupnosti aktiva, a to povede ke vzniku škody.[3]

[1] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. Knihovnicka.cz. s. 12-13. ISBN 978-80-7399-731-1.
[2] FOTR, Jiří. Jak hodnotit a snižovat podnikatelské riziko. Praha: Management Press, 1992, s. 9. ISBN 80-85603-06-3.
[3] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. Knihovnicka.cz. s. 12-13. ISBN 978-80-7399-731-1

Jak už bylo řečeno, pro riziko neexistuje jedna obecně uznávaná definice. Avšak podle knihy „Řízení rizik ve firmách a jiných organizacích“ můžeme riziko definovat následovně:

„1. Pravděpodobnost či možnost vzniku ztráty, obecně nezdaru.

2. *Variabilita možných výsledků nebo nejistota jejich dosažení.*
3. *Odchýlení skutečných a očekávaných výsledků.*
4. *Pravděpodobnost jakéhokoliv výsledku, odlišeného od výsledku očekávaného.*
5. *Situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti.*
6. *Nebezpečí negativní odchylky od cíle (tzv. čisté riziko)*
7. *Nebezpečí chybného rozhodnutí.*
8. *Možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko).*
9. *Neurčitost spojená s vývojem hodnoty aktiva (tzv. investiční riziko).*
10. *Střední hodnota ztrátové funkce.*
11. *Možnost, že specifická hrozba využije specifickou zranitelnost systému.“* [4]

[4] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90. ISBN 978-80-247-3051-6.

Model na následujícím obrázku předpokládá, že riziko je složeno ze čtyř základních parametrů: pravděpodobnost výskytu, závažnost dopadu, citlivost na změnu, stupně vzájemné závislosti a z ostatních faktorů rizika. Pokud nejsou přítomny veškeré faktory zmíněné výše, tak potom se situace nebo událost nemůže označovat jako riziko.[5]

Obrázek 1 - Typické parametry rizika

Zdroj: MERNA, Tony a Faisal F AL-THANI. *Risk management: řízení rizika ve firmě*. Vyd. 1. Brno: Computer Press, 2007, xii, s. 8. ISBN 978-80-251-1547-3.

[5] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 8. ISBN 978-80-251-1547-3.

1.1. Klasifikace rizika

Všeobecně platí, že podnikání zahrnuje určitou investici kapitálu, a to s nadějí na dosažení zisku. Pokud se však věci nevyvíjejí podle plánu, může investice skončit ztrátou. Tato rizika jsou neodmyslitelnou součástí podnikání a mohou být způsobena různými faktory, které mohou vést k úpadku podnikání nebo ztrátě. Variace v těchto faktorech a jejich důsledky slouží jako poklad pro různou kategorizaci rizik.[6]

1.1.1. Finanční a nefinanční riziko:

V nejširším kontextu slova se riziko týká scénářů zahrnujících nepříznivé okolnosti, které mohou, ale nemusí vést k nepříznivým podmínkám. Tyto podmínky mohou někdy vést ke finanční ztrátě a někdy ne. Tato část se zaměřuje na rizika, která jsou spojena s finančními ztrátami. Finanční riziko se dá definovat jako vztah mezi subjektem a jeho majetkem nebo příjmy, které mohou být ohroženy nebo sníženy.[7]

*„**Finanční** riziko je obvykle ovlivněno třemi faktory, a to:*

1. *Subjektem, který je vystaven možnosti ztráty,*
2. *Aktivy či příjmem, jejichž snížení hodnoty, zničení nebo změna vlastnictví jsou příčinou finanční ztráty,*
3. *Hrozbou (nebezpečím), které může zavinit ztrátu“* [8]

[6] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 123-125. ISBN 978-80-247-3051-6.
[7] Tamtéž
[8] Tamtéž

První složka finančního rizika se vztahuje k situacím, ve kterých je jedinec ovlivněný výskytem jiné události. Druhý a třetí aspekt finančního rizika se týká hodnotných předmětů a hrozeb, které mohou způsobit jejich ztrátu.[9]

1.1.2. Statické a dynamické riziko

Další významné rozlišení provádíme mezi statickým a dynamickým rizikem.

Dynamická rizika:

Dynamická rizika vycházejí z dvou souborů faktorů a jsou způsobena změnami v okolí firmy a samotné firmě. První soubor faktorů představují faktory vnějšího prostředí, jako je politika, ekonomika, průmysl, konkurence a spotřebitelé. Tyto faktory obvykle nelze ovlivnit na úrovni firmy, ale mohou být příčinou finančních nebo jiných ztrát. Dynamická rizika mají tendenci postihnout velké množství jednotlivců a vyskytují se nepravidelně, což je činí obecně obtížně předvídatelnými ve srovnání se statickými riziky.[10]

Statická rizika:

Statická rizika se týkají ztrát, které nejsou způsobeny ekonomickými změnami, ale spíše vnějšími faktory, mezi které se řadí přírodní katastrofy nebo lidská nepoctivost. Mezi potenciální ztráty patří například materiální poškození a převzetí vlastnictví kvůli neetickému jednání nebo lidskému selhání. V kontrastu k dynamickým rizikům, statická rizika nepřinášejí žádné přímé prospěchy společnosti.[11]

---

[9] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 123-125. ISBN 978-80-247-3051-6.
[10] Tamtéž
[11] Tamtéž

1.1.3. Čisté a spekulativní riziko

Jedno z nejužitečnějších rozlišení rizik je dělení na rizika čistá a spekulativní.

Spekulativní riziko:

Spekulativní riziko je spojeno se situací, kdy je možné, jak realizovat ztrátu, tak zisk. Podnikání často představuje příklad spekulativního rizika, kde se naděje na úspěch prolíná s možností neúspěchu. Dalším ilustrativním příkladem spekulativního rizika je jakákoli hazardní hra, kde je podstoupeno riziko s nadějí na zisk. Mezi dalšími faktory, jež předurčují vznik ztrát a tvoří základ spekulativního rizika, se řadí manažerská rozhodnutí v rámci společnosti. Vedení každé organizace přijímá rozhodnutí ohledně výrobních postupů, financování výroby a obchodní strategie firmy. V případě úspěchu firmy na trhu a přijetí cen výrobků či služeb ze strany zákazníků, může firma zaznamenat zisk. V opačném případě, pokud se firmě nedaří, může utrpět ztrátu.[12]

Čisté riziko:

Čisté riziko se týká situací, kde existuje pouze možnost ztráty nebo absence ztráty. Skvělým příkladem čistého rizika je možnost ztráty majetku. Například, při nákupu osobního automobilu se jedinec potýká s možností jeho poškození nebo dokonce zničení v případě havárie. V tomto případě jsou výsledky buď ztráta nebo žádná ztráta.[13]

[12] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 123-125. ISBN 978-80-247-3051-6.
[13] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 123-125. ISBN 978-80-247-3051-6.

1.1.4. Další členění rizik

Rizika můžeme členit také podle jejich věcné náplně. Například:

Technicko-technologická: Vztahují se k neúspěšné aplikaci výsledků vědeckého a technologického vývoje, což může vést k selhání při vývoji nových výrobků a technologií. Také se vztahují k neschopnosti správně řídit technologický proces, což může vést k poklesu výrobní kapacity.

Výrobní: Tyto rizika se často projevují nedostatkem různých druhů zdrojů, jako jsou suroviny, materiály, energie nebo kvalifikovaná pracovní síla, což může zpochybnit průběh výrobního procesu a jeho výsledky.

Ekonomická: Jedná se zejména o širokou paletu nákladových rizik, které jsou vyvolána růstem cen surovin, materiálu, energií, služeb a dalších nákladových položek.

Legislativní: Toto riziko obvykle vzniká jako důsledek hospodářské nebo legislativní politiky vlády (např. změna zákonů). Mezi velmi důležitou složku tohoto rizika můžeme uvést nedostatečnou ochranu duševního vlastnictví (patenty, obchodní známky, autorská práva)

Spojená s lidským činitelem: Jedná se o rizika managamentu, ztrátu klíčových pracovníků (především manažerů nebo specialistů), podvodné či nezákonné jednání zaměstnanců, stávky a sabotáže.

Informační: Informační rizika se týkají veškerých firemních informačních systémů a dat, u kterých může nedostatečná ochrana býti zneužita interními nebo externími subjekty.[14]

[14] FOTR, Jiří a Jiří HNILICA. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada), s. 21-23. ISBN 978-80-247-5104-7.

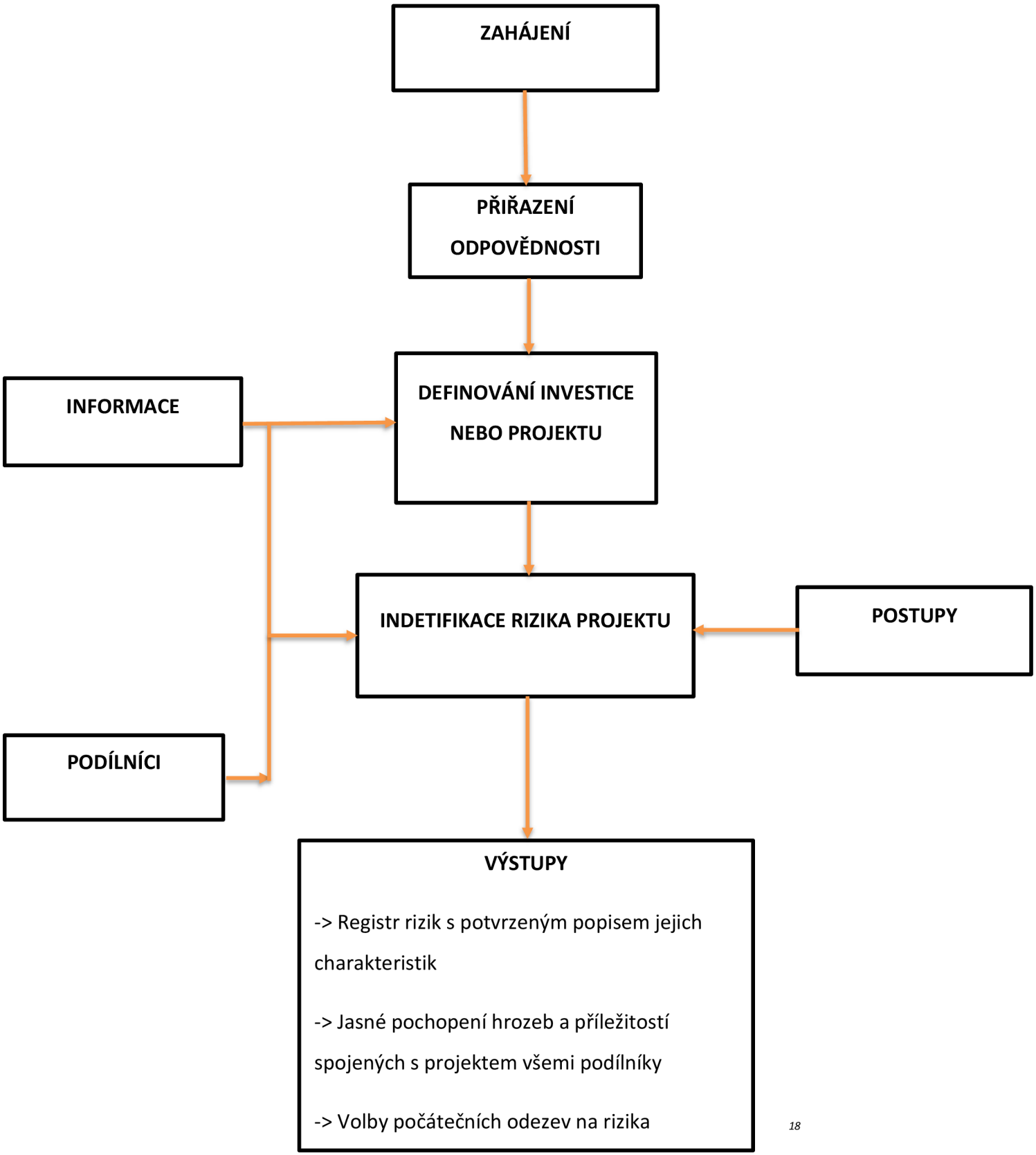
1.2. Identifikace rizika

„Identifikace rizik a stanovení jejich významnosti patří mezi nejdůležitější fáze analýzy rizika, neboť navazující kroky této analýzy i managamentu rizika pracují pouze s těmi faktory, které byli včas rozpoznány.“[15]

Proces identifikace rizika zahrnuje rozpoznání potenciálních rizik, která mohou ovlivnit průběh projektu, a zdokumentování charakteristik každého z nich. Při identifikaci rizika by měla být zohledněna jak interní, tak externí rizika. Klíčové zdroje rizika, které mohou výrazně ovlivnit projekt, by měly být identifikovány a klasifikovány podle toho, jak mohou ovlivnit náklady, časové plány a cíle projektu.[16]

Cílem identifikace rizik je získat úplný seznam faktorů rizik, které mohou mít dopad na ekonomické nebo jiné výsledky společnosti, hodnotu určitých aktiv nebo úspěšnost připravovaných nebo realizovaných projektů.[17]

[15] FOTR, Jiří a Jiří HNILICA. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada), s. 25. ISBN 978-80-247-5104-7.
[16] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 28. ISBN 978-80-251-1547-3.
[17] FOTR, Jiří a Jiří HNILICA. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada), s. 25. ISBN 978-80-247-5104-7.



18

[18] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 30. ISBN 978-80-251-1547-3.

1.2.1. Nástroje identifikace rizik

Nejvýznamnějšími nástroji používaných k identifikaci rizik nebo rizikových faktorů jsou:

Kontrolní seznamy (check listy) – poskytují vyčerpávající přehled potencionálních rizikových faktorů firmy či jejích aktivit. Uplatnění seznamu snižuje nebezpečí opomenutí některých rizik.

Pohovory s experty a skupinová diskuze – tyto diskuze mohou mít formu brainstormingových schůzek, kdy skupinu tvoří pracovníci firmy, externí experti atd.

Nástroje strategické analýzy – jedná se především o analýzy podnikatelského prostředí (SWOT analýza, PEST analýza, Porterův model pěti sil atd.), které podporují především identifikaci externích rizik.

Kognitivní (myšlenkové) mapy – *„představují grafický nástroj zobrazení jednotlivých faktorů rizika a jejich vzájemných vazeb. Rizikové faktory se zapisují na list papíru a orientovanými spojnicemi se zobrazují jejich vzájemné vazby. Spojnice vychází z faktorů rizika na straně příčiny a šipka směřuje k faktoru na straně dopadu rizika.“*

[19]

[19] FOTR, Jiří a Jiří HNILICA. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada), s. 26. ISBN 978-80-247-5104-7

1.3. Zdroje rizika

„Existuje mnoho zdrojů rizik, která musí organizace vzít do úvahy před tím, než učiní rozhodnutí. Je proto důležité, že tyto zdroje rizika jsou k dispozici, a tak je možné provést nezbytnou identifikaci, analýzu a odezvu.“[20]

Za zdroj rizika lze považovat jakýkoliv faktor, který může ovlivnit průběh projektu nebo výkonnost firmy. Riziko se objevuje v situacích, kdy je tento vliv současně nejistý a má výrazný dopad na projekt či výkonnost podniku. Jinými slovy, definice cílů projektu a kritéria pro hodnocení výkonu hrají klíčovou roli při stanovení úrovně rizika projektu.[21]

[20] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 11-12. ISBN 978-80-251-1547-3.
[21] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 11-12. ISBN 978-80-251-1547-3.

Název:	Změna a nejistota z důvodu:
Politika	Vládní politika, veřejné mínění, změna ideologie, dogma, legislativa, nepokoje (válka, terorismus, pouliční bouře)
Životní prostředí	Kontaminovaná půda nebo odpovědnost za její znečištění, nepříjemnosti (např. hluk), povolení, veřejné mínění, vnitřní/korporativní politika, zákon o ochraně životního prostředí nebo enviromentální předpisy, praxe nebo požadavky týkající se „dopadu“ na prostředí
Plánování	Požadavky na povolení, politika a praxe, užití půdy, socioekonomické dopady, veřejné mínění
Trh	Poptávka (výhled), konkurence, zastarávání, uspokojení zákazníka, móda
Ekonomika	Politika finanční správy, daně, nákladová inflace, úrokové míry, kurzy měn
Finance	Bankrot, marže, pojištění, podíl na zisku
Příroda	Nepředvídatelné půdní podmínky, počasí, zemětřesení, požár nebo exploze, archeologický výzkum
Projekt	Definice, strategie nákupu zásob, požadavky na výkon, normy, schopnost vést, organizace (zralost, závazek, pravomoc a zkušenost),

	plánování a řízení kvality, program, pracovní zdroje, komunikace a kultura
Technika	Přijatelnost návrhu, provozní účinnost, odpovědnost
Kompetentní orgány	Změny kompetentních orgánů
Lidský faktor	Omyl, nekompetence, ignorace, únava a vyčerpání, komunikační schopnost, kultura, práce ve tmě nebo v noci
Zločinnost	Nedostatek bezpečnosti, vandalismus, krádeže, podvody, korupce
Bezpečnost	Předpisy (např. bezpečnost a zdraví při práci), nebezpečné látky, kolize, kolaps, záplavy, požár a exploze
Právní zásady	Ty, které jsou spojeny se změnami v legislativě jak na státní úrovni, tak ve směrnicích EU

Tabulka 1 - Typické zdroje rizik

Zdroj: MERNA, Tony a Faisal F AL-THANI. *Risk management: řízení rizika ve firmě*. Vyd. 1. Brno: Computer Press, 2007, xii, s. 11-12. ISBN 978-80-251-1547-3.

1.4. Řízení rizik

Řízení rizik zahrnuje systematický přístup, kdy se organizace snaží zmírnit dopad současných i budoucích faktorů. Jeho cílem je předložit řešení, která mohou neutralizovat důsledky nepříznivých vlivů a zároveň využít příležitosti plynoucí z pozitivních vlivů. Tento proces řízení rizik zahrnuje rozhodovací rámec založený na důkladné analýze rizik. S přihlédnutím k různým faktorům, jako jsou ekonomické, technické, sociální a politické aspekty, řízení rizik identifikuje, hodnotí a porovnává potenciální preventivní a regulační opatření. Nakonec vybírá opatření, která účinně minimalizují aktuální rizika. [22]

Abychom úspěšně zavedli proces řízení rizik, je nezbytné se nejdříve seznámit se samotnou organizací a prostředí, ve kterém působí. Poté je nutné získat podporu managamentu a vytvořit politiku pro řízení rizik.

Vzhledem k tomu, že se informační systémy neustále vyvíjí a probíhají změny ve vnitřním a vnějším prostředí, je nutné proces řízení rizik pravidelně vyhodnocovat a následně provádět podle potřeby jeho optimalizaci.[23]

Výběr nejefektivnějšího řešení je klíčovým krokem v procesu řízení rizik. Tento krok začíná posouzením úrovně rizika, pokračuje hodnocením ekonomických nákladů a přínosů různých řešení zaměřených na snížení rizika a končí analýzou možných důsledků rozhodnutí pro subjekt i jeho okolí. Následně se rozhoduje o realizaci opatření ke snížení identifikovaných rizik.[24]

[22] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 112. ISBN 978-80-247-3051-6.
[23] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. Knihovnicka.cz. s. 17. ISBN 978-80-7399-731-1.
[24] Tamtéž

Na závěr každé fáze procesu řízení rizik je přijato rozhodnutí. Výsledkem tohoto rozhodnutí je obvykle několik možných řešení. Pokud je úroveň rizika považována za nepřijatelnou, probíhající proces se zastaví a přijmou se kroky ke zmírnění rizika. Pokud je riziko přijatelné, ale není zanedbatelné, a existuje významný potenciál zisku, často následuje formulace souboru preventivních opatření určených k minimalizaci rizika. Pro zbytková rizika, která nelze účinně zmírnit prostřednictvím protiopatření, se vypracovávají pohotovostní plány. Zásadní je stanovit priority optimalizace fáze snižování a eliminace rizik tak, aby se pohotovostní plány a scénáře vytvářely pouze pro ta zbývající rizika. [25]

[25] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 112. ISBN 978-80-247-3051-6.

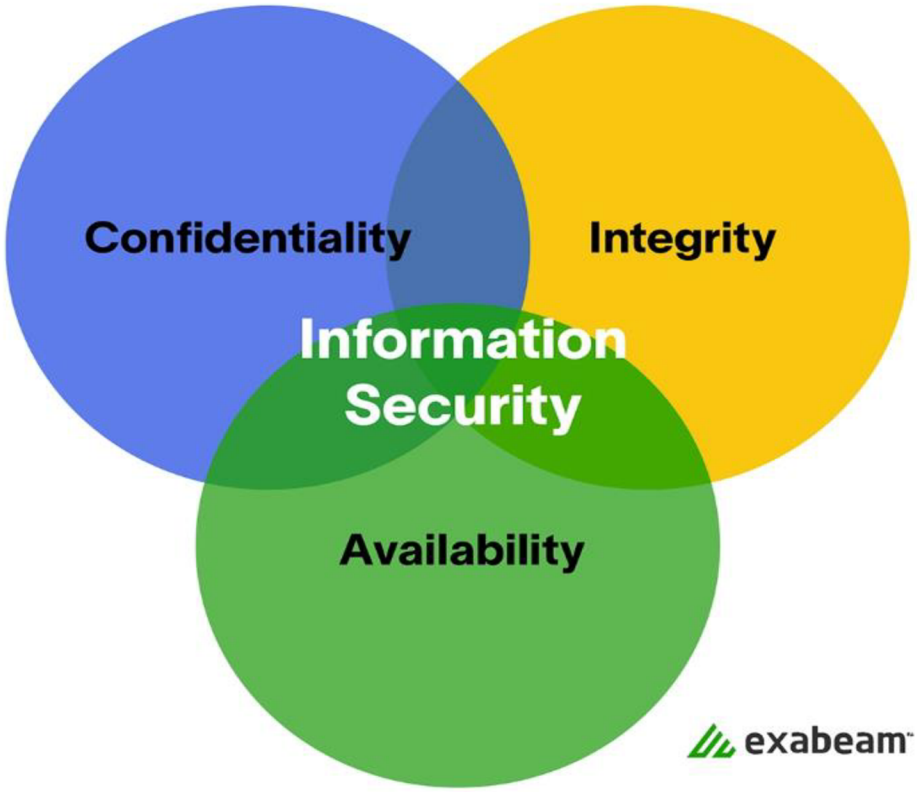
2. Bezpečnost informací

V dnešní době můžeme pozorovat rostoucí závislost organizací na informacích, které jsou stále častěji uloženy pouze v elektronické podobě. Tyto informace hrají klíčovou roli v plánování, řízení a realizaci aktivit organizace, což vede k vynakládání značných finančních prostředků na jejich získávání, zpracování a vyhodnocování. Mnohé organizace si však často neuvědomují skutečnou hodnotu svých informací a až v případě jejich ztráty či poškození si uvědomují, jak důležité jsou pro zachování dobrého jména firmy a důvěry klientů. Například únik strategických informací nebo ztráta dat mohou mít fatální následky a vést ke ztrátě pozice na trhu či dokonce k zániku společnosti. Z tohoto důvodu organizace, které si uvědomují hodnotu svých informací a mají zájem na jejich ochraně a zachování kontinuity podnikání, investují nemalé finanční prostředky do zajištění bezpečnosti svých informačních systémů.[26]

„Co je to ale bezpečnost? Bezpečnost je obecně chápána jako ochrana něčeho před zničením, poškozením nebo ztrátou. V případě bezpečnosti informací hovoříme o zachování jejich důvěrnosti, integrity a dostupnosti.“ [27]

Na obrázku na další stránce s názvem „*Obrázek 1 – Vztah atributů*“ je znázorněn vztah mezi atributy důvěrnosti, integrity a dostupnosti. *„Dostupnost si můžeme definovat jako vlastnost, že informace je pro osobu, která je oprávněna se s ní seznamovat, k dispozici v okamžiku, kdy s ní potřebujeme pracovat. Důvěrnost znamená, že s informacemi se mohou seznamovat pouze oprávněné osoby. Zachování integrity spočívá v tom, že informaci můžeme důvěřovat a spolehnout se na to, že nebyla pozměněna.“* [28]

[26] [26] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. Knihovnicka.cz. s. 11. ISBN 978-80-7399-731-1.
[27] Tamtéž
[28] Tamtéž



Obrázek 2 - Vztah atributů

Zdroj: The 12 Elements of an Information Security Policy. Exabeam - Cybersecurity & Compliance with Security Log Management and SIEM [online]. Copyright © 2023 Exabeam [cit. 15.04.2023]. Dostupné z: https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/

Další definice říká, že informační bezpečnost je soubor zásad, postupů a principů pro ochranu digitálních dat, informací, procesů a systémů proti různým hrozbám, které mohou ohrozit jejich důvěrnost, integritu a dostupnost. Bezpečnost informací zahrnuje mnoho oblastí, jako je ochrana počítačových sítí a systémů, fyzická ochrana přístupu k informacím, zálohování a obnova dat, řízení rizik, školení zaměstnanců atd. Cílem informační bezpečnosti je minimalizovat rizika spojená s útoky na informace, krádeží dat, ztrátou dat a dalšími hrozbami. K povinnostem v oblasti informační bezpečnosti

patří vytvoření souboru procesů, které chrání informační aktiva bez ohledu na to, jak jsou tyto informace formátovány, přenášeny nebo zpracovávány. [29]

Rozdílné definice bezpečnosti informací můžeme pozorovat i v závislosti na konkrétní normě. V této souvislosti lze uvést příklad dvou norem - ISO 27001 a ISO 27005, které byly použity při tvorbě této bakalářské práce.

Podle normy ISO/IEC 27001, bezpečnost informací je definována jako zachování důvěrnosti, integritu a dostupnosti informací tím, že se minimalizuje riziko úmyslného či náhodného narušení informací a minimalizuje se riziko nedostupnosti informací kvůli případným incidentům.[30]

Norma ISO/IEC 27005 dále definuje bezpečnost informací jako proces identifikace, analýzy a hodnocení rizik, které mohou ohrozit důvěrnost, integritu a dostupnost informací. Tyto rizika mohou být například spojena s neoprávněným přístupem k informacím, ztrátou dat nebo neoprávněnou změnou dat. Cílem je minimalizovat tyto rizika a zajistit, aby byly informace chráněny v souladu s potřebami organizace a relevantními zákonnými předpisy.[31]

[29] What is Information Security (Infosec)? – TechTarget Definition. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/information-security-infosec

[30] ČSN EN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. Praha: Český normalizační institut, 2014.

[31] ČSN EN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

Bezpečnost informací může mít mnoho různých prvků, nejčastěji se ale setkáme s následujícími typy:

- **Fyzická bezpečnost:** ochrana budovy nebo prostoru, kde jsou uloženy informace před neoprávněným přístupem, kradením nebo poškozením.

- **Bezpečnost aplikací a sítě:** ochrana aplikací, softwarových systémů, počítačových sítí před neoprávněným přístupem, zneužitím nebo napadením.

- **Bezpečnost dat:** ochrana dat před neoprávněným přístupem, krádeží, poškozením nebo ztrátou.

- **Identifikace a ověření:** ochrana informací před neoprávněným přístupem pomocí hesel, šifrování a dalších metod

- **Zálohování a obnova dat:** záloha a obnovení dat po nečekané události, které způsobila jejich ztrátu

- **Školení zaměstnanců:** školení zaměstnanců v oblasti bezpečnosti informací

- **Plánování a řízení bezpečnosti:** strategické plánování a řízení bezpečnosti informací, včetně identifikace rizik, stanovení procesů a postupů v rámci zlepšování informační bezpečnosti.

[32]

[32] What is Information Security (Infosec)? – TechTarget Definition. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/information-security-infosec

3. Analýza rizik

„Prvním krokem procesu snižování rizik je přirozeně jejich analýza. Analýza rizik je obvykle chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti.“ [33]

Podle normy ČSN ISO 27001:2019 je analýza rizik definována jako proces systematického hodnocení informačních bezpečnostních rizik spojených s aktivy organizace, ohroženími a zranitelnostmi, aby se určila pravděpodobnost výskytu rizika a možné důsledky.[34]

Cílem analýzy rizik je tedy rozpoznání negativních nebo nepříznivých účinků, které by se mohli v organizaci vyskytnout během jejího fungování, při změně jakéhokoli zásadního cíle organizace nebo před zahájením jakéhokoli nového důležitého projektu. Hlavním cílem je odhadnout rozsah rizika, které se může v organizaci vyskytnout a následně určit metody a přístupy, které pomohou dané riziko řídit a snížit jeho dopad.[35]

---

[33] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 93. ISBN 978-80-247-3051-6

[34] ČSN ISO/IEC 27001:2014 informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – požadavky. Praha: Český normalizační institut, 2014.

[35] Risk Analysis (Definition, Methods) | Qualitative & Quantitative. Investment Banking, Financial Modeling & Excel Blog [online]. Copyright © 2023 . CFA Institute Does Not Endorse, Promote, Or Warrant The Accuracy Or Quality Of WallStreetMojo. CFA [cit. 04.03.2023]. Dostupné z: https://www.wallstreetmojo.com/risk-analysis/

„Analýza rizik zpravidla zahrnuje:

1) ***Identifikaci aktiv*** *– vymezení posuzovaného subjektu a popis aktiv, které vlastní,*

2) ***Stanovení hodnoty aktiv –*** *určení hodnoty aktiv a jejich význam pro subjekt, ohodnocení možného dopadu jejich ztráty, změny či poškození na existenci či chování subjektu*

3) ***Identifikaci hrozeb a slabin –*** *určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv, určení slabých míst subjektu, která mohou umožnit působení hrozeb,*

4) ***Stanovení závažnosti hrozeb a míry zranitelnosti –*** *určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě*,“ [36]

[36] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 93. ISBN 978-80-247-3051-6.

3.1. Základní pojmy analýzy rizik

V této kapitole si vysvětlíme a charakterizujeme základní pojmy analýzy rizik.

3.1.1. Aktivum

Aktiva představují všechny prvky, které mají pro daný subjekt určitou hodnotu, jež může být ovlivněna nějakou hrozbou. Tyto prvky se rozdělují na hmotná, například nemovitosti a stroje, a nehmotná, jako jsou informace a software. Navíc může být aktivem i samotný subjekt, protože hrozba může ohrozit jeho celkovou existenci.[37]

Základní charakteristikou aktiva je jeho hodnota, která může být určena objektivním vyjádřením obecně uznávané ceny nebo subjektivním posouzením důležitosti daného aktiva pro konkrétní podnik. V některých případech může dojít i ke kombinaci těchto dvou přístupů. Je však důležité zdůraznit, že hodnota aktiva je relativní a závisí na perspektivě, z níž je provedeno hodnocení.[38]

„Při hodnocení aktiva se nejvíce berou v úvahu následující hlediska:

1. *Pořizovací náklady nebo 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).“* [39]

[37] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[38] Tamtéž
[39] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.

3.1.2. 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 kurzu české koruny vzhledem k evropské měně apod.“ [40]

Dopad hrozby je označení pro škodu, která vzniká v důsledku působení hrozby na konkrétní aktivum. Dopad hrozby je možné vyčíslit na základě absolutní hodnoty ztrát, která zahrnuje náklady na obnovení činnosti aktiva a také náklady spojené s odstraněním následků škod způsobených touto hrozbou pro příslušný subjekt.[41]

Při hodnocení hrozby musíme nejdřív posoudit její úroveň, která se zakládá na následujících faktorech:

- **Nebezpečnost:** míra s jakou může hrozba způsobit škodu
- **Přístup:** míra pravděpodobnosti, že se hrozba dostane ke svému cílovému aktivu a bude na něj působit. Tento faktor lze vyjádřit například frekvencí výskytu hrozby.
- **Motivace:** zájem iniciovat hrozbu vůči aktivu. K odhadu motivace je nutné porozumět skupinovým a národním záměrům, ale i individuálním cílům a politice, a to v kontextu předchozích podmínek a činnosti těchto ohrožovatelů (útočníků). Odhad motivace přispívá k tvorbě expertních posudků a odhadů hrozeb.[42]

[40] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[41] Tamtéž
[42] Tamtéž

3.1.3. Zranitelnost:

Jedná se o jev, kdy hrozba může využít zranitelnosti, chyby nebo jiného aspektu zkoumaného aktiva (nebo případně subjektu) s cílem negativně ovlivnit systém. Zranitelnost, jako jedná z hlavních vlastností aktiva, popisuje, jak náchylné je toto aktivum na účinky konkrétní hrozby.[43]

„Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti se hodnotí podle následujících faktorů: ***Citlivost:*** *náchylnost aktiva být poškozeno danou hrozbou.*
Kritičnost: *důležitost aktiva pro analyzovaný subjekt.“* [44]

3.1.4. Protiopatření

Protiopatření je opatření přijaté k omezení účinků hrozby (či její odstranění), snížení zranitelnosti nebo zmírnění důsledků hrozby. Může se jednat o opatření, proces, proceduru, technickou metodu nebo cokoli jiného. Protiopatření si klade za cíl zabránit negativním důsledkům nebo snížit dopad již vzniklé škody.[45]

Mezi dvě základní vlastnosti protiopatření při analýze rizik se řadí efektivita a náklady. Efektivitu protiopatření změříme tím způsobem, že zhodnotíme, jak dobře dokáže snížit účinky nebezpečí. Efektivita slouží jako jedno z klíčových kritérií pro rozhodnutí, zda dané protiopatření má být implementováno během fáze řízení rizika.[46]

---

[43] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[44] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[45] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[46] Tamtéž

Protiopatření mají za cíl snížit úroveň hrozby, zranitelnosti a následků působení hrozby. Dále se soustředí na detekci nežádoucích vlivů, aby bylo možné včas indikovat působení hrozby a předejít plnému uplatnění. V neposlední řadě protiopatření také plní funkci obnovení činnosti po působení hrozby.[47]

Náklady na protiopatření zahrnují také náklady na nákup, nasazení a údržbu. Při výběru vhodného protiopatření jsou tyto náklady společně s efektivitou důležitými faktory protiopatření. V rámci procesu optimalizace, který zahrnuje výběr protiopatření, se hledají nejlepší protiopatření s důrazem na co nejnižší náklady.[48]

[47] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[48] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.

3.2. Obecný postup při analýze rizik

Rizika zpravidla neexistují izolovaně, nýbrž často představují kombinaci různých rizik, která mohou pro daný subjekt představovat nebezpečí. Při zohlednění rozmanitosti rizik je důležité stanovit priority z hlediska jejich dopadu a pravděpodobnosti výskytu a soustředit se na klíčové oblasti rizika.[49]

3.2.1. Identifikace aktiv a následné stanovení jejich hodnoty

Významným aspektem tohoto kroku je vytvoření dokumentu, který bude obsahovat seznam všech aktiv obsažených v rámci rozsahu analýzy rizik. Během procesu rozhodování, zda zařadit dané aktivum na seznam, vždy uvádíme jeho název a umístění.[50]

Další krok spočívá v posouzení hodnoty vybraného aktiva. Tato hodnota vychází ve většině případů z pořizovací ceny aktiva a je založena na základě velikosti škody, která by vznikla při ztrátě či zničení daného aktiva. Tato hodnota může ovšem také vycházet z výnosových charakteristik, mezi které můžeme zařadit nepřímé vlastnosti aktiva, které přispívají k dosahování zisků společnosti (například know-how či postavení na trhu). [51]

*„Velmi podstatné je rozlišit, zda se jedná o **jedinečné aktivum,** nebo o aktivum jednoduše nahraditelné. Do hodnoty se promítá závislost subjektu na existenci, ale i na správném fungování hodnoceného aktiva, tedy k jakým škodám dojde omezením*

[49] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[50] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 99. ISBN 978-80-247-3051-6.
[51] Tamtéž

funkčnosti nebo ztrátou aktiva, než dojde k jeho obnově. Hodnota aktiva pro analýzu rizik se může stanovit také jako vážený průměr hodnot podle všech použitých hledisek.“ [52]

Podniky ve většině případů disponují velkým množstvím aktiv. Proto je důležité počet těchto aktiv snížit, a to nejlépe za pomocí seskupení aktiv s podobnými vlastnostmi (na základě podobného účelu, ceny nebo jiných kritérií) do jedné skupiny. Výsledná skupina se následně chová jako jednotlivé aktivum. Je nezbytné klást značný důraz na zajištění, že navržená protiopatření budou aplikovatelná na všechna aktiva ve vybrané skupině. [53]

Jak už bylo zmíněno, aktivum je prvek nebo určitá část systému, kterému firma přiřazuje určitou hodnotu a které je třeba býti chráněno. Důležitost aktiv se liší podle činnosti podniku. Zpravidla lze ale konstatovat, že mezi nejdůležitější aktiva řadíme data, informace, duševní vlastnictví, technické a programové prostředky, komunikační zařízení, listiny a personál firmy.[54]

[52] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 99. ISBN 978-80-247-3051-6.
[53] Tamtéž
[54] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.

3.2.2. Identifikace hrozeb

V této fázi analýzy rizik jsou identifikovány hrozby, které jsou relevantní pro danou analýzu rizik. Proces identifikace hrozeb je založen na výběru hrozeb, které mají potenciál ohrozit alespoň jedno z aktiv podniku.[55]

„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 získávání vlastního seznamu hrozeb subjektů je vhodné použít některou z metod jako brainstorming, metoda Delphi apod.“ [56]

3.2.3. Analýza hrozeb a zranitelností

„Každá hrozba se hodnotí vůči každému aktivu (skupině aktiv). U těch aktiv, na něž se hrozba může uplatnit, se určí úroveň hrozby vůči tomuto aktivu a úroveň zranitelnosti aktiva vůči této hrozbě.“ [57]

Před analýzou hrozeb je důležité určit míru hrozby a zranitelnosti. Míra hrozby je stanovována na základě faktorů jako nebezpečnost, motivace a přístup. Míra zranitelnosti je stanovována na základě faktorů jako citlivost a kritičnost. V rámci analýzy hrozeb a zranitelností se přihlíží k možným protiopatřením, která budou disponovat potenciálem na snížení úrovní hrozeb nebo zranitelnosti. V rámci této analýzy vzniká

[55] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[56] Tamtéž
[57] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.
[57] Tamtéž

seznam dvojic "hrozba <-> aktivum", který obsahuje informace o úrovních hrozby a zranitelnosti. Tento seznam zahrnuje pouze ty dvojice, u kterých je možné aplikovat hrozbu na vybrané aktivum.[58]

3.2.4. Pravděpodobnost jevu

Existují situace, ve kterých nemáme jistotu, jestli konkrétní jev, který zkoumáme se stane či nikoli. Výsledky tohoto jevu mohou být ovlivněny různými počátečními podmínkami a mohou vykazovat různé výsledky. V těchto situacích je velmi důležité uvést pravděpodobnost, s níž se daný jev může vyskytnout, aby bylo možné s touto pravděpodobností počítat. Pro výpočet pravděpodobnosti musíme nejprve určit, zda je daný jev náhodný či nikoliv, zda spadá do určitého intervalu pravděpodobnosti, zda jej lze vyloučit, a jaké jsou jeho pravděpodobnostní charakteristiky.[59]

3.2.5. Měření rizika

Klíčovou fází analýzy rizika pro podnik, jeho aktiv, investičních a výzkumných projektů je stanovení velikosti rizika. Tato velikost závisí na hodnotě aktiva, jeho zranitelnosti a úrovni hrozby. Následná velikost rizika pak představuje významnou informaci pro hodnocení tohoto rizika z hlediska jeho přijatelnosti, či nepřijatelnosti. Tyto údaje také pomáhají vybrat nejvhodnější možnost pro danou rizikovou aktivitu nebo projekt. [60]

---

[58] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.

[59] Tamtéž

[60] FOTR, Jiří a Jiří HNILICA. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada), s. 56. ISBN 978-80-247-5104-7.

Při provádění analýzy rizik je často potřeba pracovat s proměnnými, které nelze přesně kvantifikovat. Proto je určení jejich rozsahu závislé na kvalifikovaném odhadu odborníka, který se spoléhá na své zkušenosti. Tento odhad bývá často vyjádřen pomocí kvalifikátorů jako „malý“, „střední“ nebo „velký“ a stupnicí s hodnotami od 1 do 10. [61]

[61] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 90-105. ISBN 978-80-247-3051-6.

3.3. Metody analýzy rizik

Rozdělení metod používaných v analýze rizik může být založeno na způsobu, jakým jsou vyjádřeny veličiny, s nimiž se pracuje. Existují dvě základní metody pro vyjádření těchto veličin: kvantitativní a kvalitativní. V analýze rizik se může buď použít jedna z těchto metod, nebo jejich kombinace.[62]

3.3.1. Kvalitativní metody

„Kvalitativní metody jsou postaveny na popisu závažnosti potencionálního dopadu a na pravděpodobnosti, že daná událost nastane.“[63]

Tyto metody pro popis výše dopadu, hrozeb, zranitelností a výsledného rizika používají diskrétní škály (např. 1 až 10) nebo slovní popis (velmi nízká až velmi vysoká).

Výhodou kvalitativní metody je její snadná proveditelnost a rychlost, jelikož není nutné vyčíslovat finanční ztrátu a zkoumat statistiku výskytu hrozeb. Tato metoda je převážně založena na subjektivním odhadu hodnotitele. [64]

Nevýhodou kvalitativních metod je, že občas přinášejí problémy v oblasti zvládání rizik, při posuzování přijatelnosti finančních nákladů nutných k eliminaci hrozby, která může být kvalitativní metodou charakterizována jako „velká až kritická“. Díky tomu, že neexistuje jednoznačné finanční vyjádření, se kontrola efektivnosti nákladů znesnadňuje.

---

[62] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 108-109. ISBN 978-80-247-3051-6

[63] Tamtéž

[64] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. Knihovnicka.cz. s. 27-29. ISBN 978-80-7399-731-1.

Tento typ analýzy se většinou využívá při nedostatku kvality a kvantity získaných číselných dat pro jejich využití v kvantitativních metodách.[65]

3.3.2. Kvantitativní metody

„Kvantitativní metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Používají číselné ocenění jak v případě pravděpodobnosti vzniku události (či lépe řečeno incidentu), tak i při ocenění dopadu dané události. Vyjadřují dopad obvykle ve finančních termínech, například „tisíce kč". Nejčastěji je riziko vyjádřeno ve formě roční předpokládané ztráty (annualised loss expectancy – ALE), která je vyjádřená finanční částkou."[66]

Metoda ALE (metoda očekávaných ročních ztrát) je vůbec prvním představitelem kvantitativních metod analýzy rizik. ALE vypočteme tak, že SLE (ztráta při jednom výskytu hrozby) vynásobíme ARO (pravděpodobnost výskytu hrozby za rok).

Kvantitativní metody mají výhodu silné podpory matematického aparátu, což vede k jednoduššímu pochopení a srozumitelnosti výsledků. Výsledná rizika jsou vyjádřena v kontinuálních číselných škálách a lze je snadno vyjádřit také v penězích, což je klíčové pro zájmy managamentu a umožňuje jim s výsledky pracovat. [67]

Nevýhodou kvantitativních metod je jejich vysoká náročnost na provedení, čas a prostředky. Další nevýhodou kvantitativních metod je jejich častý velice vysoce formalizovaný postup, který může vést k tomu, že nebudou postihnuta specifika posuzovaného subjektu, což může vést k jeho vysoké zranitelnosti, a to z důvodu

[65] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 108-109. ISBN 978-80-247-3051-6
[66] Tamtéž
[67] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. Knihovnicka.cz. s. 27-29. ISBN 978-80-7399-731-1.

„zahlcení“ hodnotitele velkým množstvím formálně strukturovaných dat. Kvalita této metody tudíž velice souvisí s relevantností získaných dat. [68]

3.3.3. Kombinované metody

Kombinované metody využívají numerických dat, které kombinují s kvalitativním hodnocením, aby se co nejblíže přiblížily realitě a minimalizovali rozdíly mezi předpoklady a skutečností, které se často vyskytují zejména v kvantitativních metodách. Je důležité mít ale na paměti, že údaje použité v kvalitativních metodách nemusí vždy přesně odrážet pravděpodobnost nebo výši dopadu událostí, ale mohou být ovlivněny měřítkem stupnice, která je v konkrétní metodě použita. [69]

[68] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 108-109. ISBN 978-80-247-3051-6.
[69] Tamtéž

3.4. Metody analýzy a stanovení rizik

Pro analýzu rizik existují stovky analytických metod. Z tohoto důvodu si pro účel bakalářské práce zmíníme pouze několik z nich, jelikož není možné popsat všechny.

3.4.1. Brainstorming

Brainstorming se zrodil na Madison Avenue v 50. letech 20. století. V nedávné době se dostal na přední místo a používá se ve všech možných firmách, ve státní správě, manažerských a vědeckých projektech.[70]

„Optimální velikost pro brainstormingovou poradu je 12 lidí a ideální délka času je mezi 15 a 45 minutami.

Základní pravidla lze shrnout takto:

- *Stanovit časový limit*
- *Jasná formulace problému*
- *Určit metodu zachycení myšlenek, například na flip-chart*
- *Zanechat nápady na nějakém viditelném místě a nechat je dozrát*
- *Přijmout princip, že žádná myšlenka je špatná myšlenka*
- *Odložit posudek*
- *Povzbudit účastníky, uvolnit jejich zábrany a ponechat je snít a pohybovat se kolem problému*
- *Povzbuzovat spíše k množství než ke kvalitě (vyhodnocení může přijít později)*
- *Vzájemně zúrodňovat myšlenky sběrem skupinových nápadů a jejich rozvojem.“* [71]

[70] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.
[71] Tamtéž

Proces brainstormingu zahrnuje opětovné definování problému, generování myšlenek, hledání možných řešení, vyvíjení vybraných proveditelných řešení a řízení vyhodnocování.[72]

3.4.2. Metoda „What If“

„Při metodě "What if" jde o to vyhledávat dopady předem vybraných nebezpečných situací v provozu. Tuto analýzu provádí kvalifikovaní pracovníci, kteří mají zkušenosti s daným provozem či konkrétním pracovním procesem. Tato metoda hodnocení rizik se používá nejčastěji při prověřování pracovních a technologických postupů, provozní bezpečnosti, zkoumání budov, skladů, ale také produktů. Často dochází také k identifikaci a posuzování zdrojů rizik a již existujících ochranných a bezpečnostní opatření. Základním kamenem této analýzy je brainstorming (bouře mozků) a diskuze. Provádí se tak, že se formou dotazů a odpovědí prověřují neočekávané situace, které při práci mohou nastat. Všechny dotazy by se měly formulovat pomocí věty "Co se stane, když…?". Na základě toho se pak vyhledávají scénáře průběhu potenciální havárie.“ [73]

[72] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.

[73] Metody a způsoby hodnocení rizik na pracovišti | BOZP.cz. Dokumentace BOZP a PO | BOZP.cz [online]. Copyright © 2023 CRDR spol. s r.o. [cit. 06.03.2023]. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/

3.4.3. Metoda Delphi

Tento postup se používá k předpovídání budoucích událostí nebo výstupů a zahrnuje skupinu odborníků, kteří jsou požádáni, aby dali své předpovědi. Nejprve každý odborník dá nezávisle svou předpověď a poté se skupina musí shodnout na výsledku, aby se vyhnula extrémním názorům. V některých situacích se mohou použít subjektivní pravděpodobnosti pro možné budoucí výstupy, aby se dospělo k závěru.[74]

Definice:

Metoda účelových rozhovorů, známá také jako metoda Delphi, zahrnuje strukturovanou komunikaci mezi skupinou expertů a zástupci hodnoceného subjektu.[75]

„Oproti jiným metodám, založených na strojovém zpracování velkého počtu dotazníků, používá metoda Delphi pro rizikovou analýzu soubor otázek, prodiskutovaných na účelových pohovorech, přičemž obvykle jsou tyto otázky tvořeny dvěma částmi – pevnou, předem danou, a variabilní, podle průběhu pohovoru a postavení respondenta. Respondenti nepřicházejí při zpracování odpovědí (provádění pohovorů) do styku, čímž je zaručeno vzájemné neovlivňování. Výhodou této metody je menší náročnost na spotřebu zdrojů a/nebo času, zohlednění specifik posuzovaného systému, jeho správce, okolí, uživatelů apod. Metoda Delphi je vhodná pro analýzu rizik především proto, že určuje, co se může stát a za jakých podmínek.“ [76]

[74] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.
[75] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 110. ISBN 978-80-247-3051-6.
[76] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada), s. 110. ISBN 978-80-247-3051-6.

Shrnutí procesu:

- *„Respondenti jsou dotazováni tak, aby řekli své názory na rizika, která se týkají daného projektu nebo investice.*
- *Předsedající osobo potom sbírá informace a vydává shrnutí závěrů zpět respondentům a požaduje, aby zrevidovali své názory v souladu se společným názorem skupiny.*
- *Tyto kroky se opakují, dokud není dosaženo konsensu nebo až předsedající osoba cítí, že další opakování už nebude mít žádný přínos.“* [77]

3.4.4. Kontrolní seznamy

Kontrolní seznamy jsou deduktivní postupy založeny na zkušenostech s minulými riziky a nabízejí efektivní způsob, jak rychle identifikovat možná rizika. Tyto seznamy mohou mít formu sady otázek nebo seznamu témat, která je nutno zvážit. Organizace mohou vytvářet své vlastní kontrolní seznamy nebo používat standardní seznamy, které jsou k dispozici pro daný sektor nebo odvětví.[78]

[77] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.
[78] Tamtéž

3.4.5. Metoda HAZOP

HAZOP (Hazard Operation Process) je induktivní postup, který byl vyvinut společností Imperial Chemicals Ltd. za účelem identifikace rizik v chemických závodech. Jedná se o typ strukturalizovaného brainstormingu, kdy skupina systematicky zkoumá prvky procesu a definuje záměr každé skupiny.[79]

Tato metoda je založená na pravděpodobnosti ohrožení a vyplývajících rizik. Jedná se o jednu z nejrozšířenějších analýz k identifikaci rizik, hlavně zejména v chemickém průmyslu. Metoda HAZOP zkoumá hlavně ohrožení a provozuschopnost. Hlavním cílem této metody je identifikace scénářů potencionálního rizika. Díky této metodě je možné najít kritická místa systému a vyhodnotit potencionální rizika a nebezpečné stavy.[80]

[79] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.

[80] Metody a způsoby hodnocení rizik na pracovišti | BOZP.cz. Dokumentace BOZP a PO | BOZP.cz [online]. Copyright © 2023 CRDR spol. s r.o. [cit. 06.03.2023]. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/

3.4.6. Metoda FMEA a FMECA

„Metoda FMEA (Failure Mode and Effect Analysis) je analýza selhání a jejich dopadů. Jedná se o metodiku, která je založená na průzkumu možností selhání a jejich dopadů. Tento postup umožňuje hledání dopadů a příčin prostřednictvím systematických a strukturovaně vymezených selhání zařízení. Je to metoda vyvinutá pro potřeby studia poruch systémů. FMEA stanovuje postup od vzniku přes průběh až po důsledky poruchy. Často se používá ve výrobě a dokáže odhalit rizika už v rané fázi plánování, což umožňuje úsporu času, ale i investice do vývoje produktu a procesu. Metoda FMEA zároveň detailně dokumentuje výrobní postup daného produktu.“[81]

Pro maximální efektivnost je nutné realizovat tuto metodu v týmové spolupráci s lidmi, kteří mají různé postavení ve firmě a ideálně i napříč obory. Tato metoda není nijak složitá, avšak vyžaduje velké zkušenosti a perfektní znalost zkoumaného produktu.[82]

Podobnou metodou je metoda FMECA (Failure Modes and Effects Criticality Analysis). Tato metoda je založené na induktivní postupu, za něhož se zaručuje a zkoumá ho jediný analytik s důkladnými znalostmi systému. *„Tento postup se může zaměřit na hardware zapojený do procesu a koncentrovat se na potencionální chyby zařízení nebo na události s důrazem na jejich výstupy a na dopad jejich selhání v systému. Zvažuje se každá komponenta systému a je identifikován každý způsob selhání.“* [83]

[81] Metody a způsoby hodnocení rizik na pracovišti | BOZP.cz. Dokumentace BOZP a PO | BOZP.cz [online]. Copyright © 2023 CRDR spol. s r.o. [cit. 06.03.2023]. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/

[82] Tamtéž

[83] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.

„Cílem obou metod je:

- *Vyhodnocení důsledků a posloupnost úkonů či jevů, které vedou k poruše*
- *Vyhodnocení závažnosti důsledků poruchy s přihlédnutím na správný výkon funkce*
- *Zařazení do klasifikace poruch dle podmínek diagnostiky*
- *Identifikace ukazatelů závažnosti a pravděpodobnosti vzniku poruchy“* [84]

„Metodu FMEA je vhodné použít tam, kde je nutné vyhodnotit jednotlivé prvky systému, které by mohly ohrozit selhání celého systému. Nedoporučujeme tuto metodu používat u složitých systémů, které mají mnoho prvků. Navíc tato analýza vyžaduje použití počítače, specializovaného softwaru a konkrétně cílené databáze.“[85]

[84] [84] Metody a způsoby hodnocení rizik na pracovišti | BOZP.cz. Dokumentace BOZP a PO | BOZP.cz [online]. Copyright © 2023 CRDR spol. s r.o. [cit. 06.03.2023]. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/

[85] Tamtéž

3.4.7. Registry rizik

Registr rizik je dokument nebo databáze, která zaznamenává každé riziko příslušející k projektu nebo konkrétní investici, nebo k základními majetku. Tyto registry rizik mohou sloužit jako nástroj pro identifikaci rizik a mohou být použity obdobně jako kontrolní seznamy pro předchozí projekty.[86]

Registr rizik umožňuje, aby data shromážděná během procesu řízení identifikace rizik byla zachycena a uložena jako přehled a zásobník informací podle zvoleného softwaru na řízení rizik.[87]

V registru rizika musí být následující nezbytné údaje:

- Název projektu
- Identifikace projektu
- Identifikace aktivity
- Akronym aktivity
- Jméno vedoucího týmu a jednotlivých členů
- Seznam popisů aktivity
- Postup
- Největší pravděpodobnost. Odhaduje jí odborník pro aktivity. Je to hodnota používaná v balíku softwaru na řízení rizika, kolem kterého působí optimistické a pesimistické hodnoty. Společně se to nazývá tříbodový odhad.[88]

[86] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.
[87] Tamtéž
[88] Tamtéž

Z registru rizika mohou být vypracovány diagramy míry rizika. Cílem těchto diagramů není řešit riziko, ale přiřadit úkoly odpovědné straně.[89]

„Například:

- *Scénář – změna vlády*
- *Činnost – pečovat o politickou neutralitu; předpovědět rozsah nebo změny kontraktů ze strany nových funkcionářů.*

Z těchto úkolů může odpovědná strana ihned provádět analýzy rizika v dalších detailech.“[90]

Priorita	Popis	Pravděpodobnost	Dopad	Vlastník	Klíčové údaje	Současné činnosti	Datum Kontroly
1							
2							
3							
x^n							

Tabulka 2 - Typické shrnutí výstupu registru rizika

Zdroj: MERNA, Tony a Faisal F AL-THANI. *Risk management: řízení rizika ve firmě.* Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.

[89] MERNA, Tony a Faisal F AL-THANI. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007, xii, s. 42-45. ISBN 978-80-251-1547-3.
[90] Tamtéž

Praktická část

4. Analýza rizik bezpečnosti informací ve vybrané společnosti

V této části bakalářské práce bude představen podnik, ve kterém bude provedena analýza rizik bezpečnosti informací, identifikace rizik dle hrozby a pravděpodobnosti výskytu, a následně bude vyhotoven návrh opatření, jak daným rizikům předcházet.

4.1. Charakteristika vybrané společnosti

Pro účely bakalářské práce byla vybrána společnost B4B INKASSO s. r. o.

B4B INKASSO je česká rodinná firma, která se nachází v moravskoslezském kraji se sídlem v Havířově. Společnost byla založena 22. ledna 2003 a z právní formy se jedná o společnost s ručeným omezeným. V současnosti je společnost vlastněna třemi společníky a to Ing. Miroslavem Rozbrojem, Ing. Vladislavem Bubíkem a rakouskou společností B4B Forderungsmanagament und Inkassogesellschaft GmbH.

Společnost zaměstnává 53 zaměstnanců a zvláštní zřetel klade B4B na celosvětovou, obor přesahující kompetenci. Prostřednictvím poboček v Rakousku, Polsku a na Slovensku, jakož i propojenými partnerskými podniky po celém světě, může konferovat ve všech jazycích, vyhotovit upomínky nebo zpracovat rešerše.[91]

Hlavní podnikatelskou činností firmy je mimosoudní vymáhání pohledávek, které je v nezbytných případech doplněno také o vymáhání soudní a exekuční. B4B INKASSO vymáhá pohledávky jak pro velké nadnárodní společnosti, tak také pro malé a střední podniky a živnostníky.

[91] VAJDOVÁ, Eva. *Analýza týmové práce v inkasní firmě.* Ostrava, 2008, 49 s. Diplomová práce. Vysoká škola Báňská, Fakulta metalurgie a materiálového inženýrství, Katedra ekonomiky a managementu v metalurgii. Vedoucí práce Ing. Andrea Samolejová, Ph.D.

Inkaso je u B4B zasazeno do profesionálního managementu pohledávek, vyškolení spolupracovníci zpracovávají pohledávky individuálně, upomínají nebo rozpracovávají platební alternativy, vše dle přání klienta. Vedle mnoha automatických postupů je u B4B základním principem individuální péče. Speciálně vyvinutý internetový portál zaručuje klientovi v každém okamžiku nahlédnutí do aktuálního stavu věci.[92]

[92] VAJDOVÁ, Eva. *Analýza týmové práce v inkasní firmě.* Ostrava, 2008, 49 s. Diplomová práce. Vysoká škola Báňská, Fakulta metalurgie a materiálového inženýrství, Katedra ekonomiky a managementu v metalurgii. Vedoucí práce Ing. Andrea Samolejová, Ph.D.

4.2. Metodika výzkumu

Pro určení rizik bezpečnosti informací (ISO 27005 a 31000) ve firmě B4B INKASSO s. r. o. byla použita metoda „WHAT – IF“, tzn. „Co by se stalo kdyby…“ a jaké následky by splnění rizika mělo na činnost organizace. Tato metoda byla použitá z důvodu její vhodnosti pro vybraný podnik. Hodnocení podléhají všechna aktiva ve společnosti, která spadají pod „informační bezpečnost“, tj. data, software, technické prostředky, hardware, lidé a fyzická místa.

Rizika jsou hodnocena za pomocí vzorce:

IR = PV x N

- IR = index rizika
- PV = pravděpodobnost výskytu rizika
- N = následek rizika

4.2.1. Pravděpodobnost výskytu rizika

Pravděpodobnost rizika byla stanovena po konzultaci s vybranou společností na základě zkušeností z praxe. Podle pravděpodobnosti výskytu daného rizika je k danému stupni pravděpodobnosti přiřazena váha, která se následně zaznamenává do tabulky analýzy rizik.

Pravděpodobnost výskytu rizika se klasifikuje do pěti kategorií, které jsou prezentovány písmeny VN, N, S, V, VV. Každá kategorie představuje jinou úroveň rizika.

Dále jsou klasifikovány váhy rizika, ty jsou klasifikovány do pěti kategorií a jsou reprezentovány čísly 1, 2, 4, 8, 16. Váhy rizika představují, jak vážné je dané riziko vzhledem k jeho pravděpodobnosti výskytu. Například riziko s pravděpodobností výskytu VN (více než 10 let) s váhou 1 znamená, že je to prakticky nemožné riziko, které

by mohlo nastat jen velmi zřídka, a pokud ano, mělo by jen minimální dopad. Na druhou stranu riziko s pravděpodobností výskytu VV (průměrně 1x měsíčně) s váhou 16 znamená, že se toto riziko pravidelně opakuje a má významný dopad na organizaci, což vyžaduje okamžitou pozornost a návrh řešení.

Tabulka 3 - Pravděpodobnost výskytu rizika

Pravděpodobnost výskytu rizika	**Váha**
Prakticky nemožný výskyt – VN (> 10 let)	1
Nedošlo ještě k výskytu, ale za určitých okolností může nastat – N (1x za 3 roky)	2
Možný výskyt, už tato situace nastala – S (1x ročně)	4
Častý výskyt – V (výskyt 1x za 4 měsíce)	8
Pravidelný, stále se opakující výskyt – VV (průměrně 1x měsíčně)	16

Zdroj: Vlastní zpracování dle doporučení vedoucího práce

4.2.2. Následek rizika

Pro následek rizika byla vytvořena tabulka, ve které je každému riziku přirazené číslo, které vyjadřuje „úroveň“ rizika podle její hodnoty. Následná závažnost rizika je vypočtena podle vzorce: 2^n, přičemž n = 1, 3, 5.

Kritéria pro ohodnocení rizika:

- Charakteristika – je to číselné ohodnocení rizika, které vychází z kombinace dvou čísel. První číslo určuje úroveň důležitosti procesu, kde se riziko vyskytuje, a druhé číslo určuje míru závažnosti rizika.
- Popis závažnosti rizika – popisuje, jaké jsou důsledky pro organizaci, pokud se dané riziko vyskytne, a jaké jsou ztráty

Tabulka 4 - Následek rizika

Úroveň	Kritérium závažnosti K=	Charakteristika	Popis závažnosti rizika
1	2^1=2	Nevýznamný	Nevýznamné porušení procesů a postupů v části organizace. Existuje možnost okamžité nápravy, bez vlivu na chod organizace a bez finančních ztrát.
2	2^3 = 8	Střední	Neoprávněné nakládání s aktivy uvnitř organizace, porušení pravidel ISMS, větší finanční ztráty (nad 100 tis. CZK), závažná překážka efektivního chodu organizace, nevědomé porušení legislativních předpisů a norem.
3	2^5 = 32	Katastrofální	Kritické problémy při plnění hlavních úkolů organizace, příp. zastavení klíčových procesů společnosti projevující se vlivem na komunikaci a plnění úkolů vzhledem k externím stranám (zákazníkům, dodavatelům atd.) Velmi vysoké finanční ztráty (nad 500 tis. CZK), okamžitý úbytek zákazníků (o 50 % za sledované období), únik citlivých a osobních údajů, trvalé poškození dobrého jména. Vědomé porušení legislativních předpisů a norem vedoucí k významným ztrátám v organizaci.

Zdroj: Vlastní zpracování dle doporučení vedoucího práce

4.2.3. Index rizika (výsledné riziko)

Index rizika vyjadřuje reálné výsledné riziko, které firmě hrozí. Index rizika je určen výpočtem, při kterém provádíme součin pravděpodobnosti a závažnosti rizika. Na základě ohodnocení rizika je možné určit rizikovou skupinu jako výsledek celé analýzy:

IR = PV x N

IR = index rizika

PV = pravděpodobnost výskytu rizika

N = následek rizika

Riziková skupina je stanovena podle výše uvedeného indexu rizika.

Tabulka 5 - Riziková skupina

Riziková skupina	Popis
1 (IR max. 8)	Běžné riziko, doporučuje se dodržování běžných postupů a procedur stanovených v bezpečnostní politice.
2 (IR 16 – 32)	Zvýšená úroveň rizika, doporučuje se zvýšit úroveň bezpečnostních opatření v bezpečnostní politice a jejich pravidelnou kontrolu.
3 (IR nad 32)	Velmi vysoká úroveň rizika, doporučuje se přijmout a implementovat takové technické a organizační opatření, které povedou ke zvýšení bezpečnostních procesů a procedur a jejich systematické monitorování a analýzu.

Zdroj: Vlastní zpracování dle doporučení vedoucího práce

4.3. Průběh analýzy

Aby bylo možné provést analýzu rizik bezpečnosti informací, musela být nejdříve vytvořena tabulka aktiv v programu Microsoft Excel. Aktiva byla zvolena podle dodané mapy procesů a po konzultaci s firmou.

č.	Název aktiva	Typ aktiva	Kód aktiva	Vlastník aktiva	Popis aktiva	Rizika
1	Strategie a plánování, Interní audit, managament zdrojů	Proces	1	Manažer kvality, Provozní ředitel	Procesy strategie a plánování, Interní audit. Management zdrojů	Rizika nesplnění procesu
2	Klasické, bankovní, tele, soudní a externí inkaso	Proces	1	Vedoucí pracovníci na každém oddělení	Procesy vymáhání pohledávek	Rizika nesplnění procesu
3	Vnitřní komunikace	Proces	1	Provozní ředitel	Proces vnitřní komunikace	Rizika nesplnění procesu
4	Nakupování materiálů a služeb	Proces	1	Ožanová	Proces Nakupování	Rizika nesplnění procesu
5	Údržba výpočetní techniky	Proces	1	ICT technik	Proces údržby informačních systémů	Rizika nesplnění procesu
6	Řízení dokumentace QMS, Řízení externí dokumentace, Řízení záznamů, Interní audit, Nápravná opatření	Proces	1	Provozní ředitel, Ožanová	Procesy Přezkoumání požadavků, Řízení dokumentace IMS, Řízení externí dokumentace, Řízení záznamů, Opatření k nápravě Preventivní opatření	Rizika nesplnění procesu
7	OÚ zaměstnanců	Informace	2	Vedoucí oddělení administrativy	Dokumenty obsahující osobní údaje zaměstnanců	Nedodržení zákona o ochraně osobních údajů, úniky údajů o zaměstnancích, penále
8	Interní informace klientů	Informace	2	Vedoucí týmu, ICT	Dokumenty obsahující informace poskytované klientem a informace o klientovi	Penále za nedodržení GDPR, zhoršení pověsti firmy, ztráta klienta, dlouhodobé finanční následky
9	Kamerové záznamy	Informace	2	Provozní ředitel	Záznamy z kamer	Penále za nedodržení GDPR, zákon na OOÚ.
10	Obchodní a marketingový plán	Informace	2	Obchodní manažer	Obchodní a marketingový plán	Špionáž, předání informací konkurenci.
11	Docházkový systém (OrpheusX)	SW	3	ICT, Provozní ředitel	Docházkový systém	Ztráta dat, ztráta spojení, zpoždění, neúplnost, chyba nastavení, napadení, kopírování
12	Mzdový systém (Pamica)	SW	3	Účetní, Provozní ředitel	Mzdy	Ztráta dat, ztráta spojení, zpoždění, neúplnost, chyba nastavení, napadení, kopírování
13	Účetní program (Pohoda)	SW	3	Účetní, Provozní ředitel	Účetní program	Ztráta dat, ztráta spojení, zpoždění, neúplnost, chyba nastavení, napadení, kopírování
14	Informační systém (Inkas)	SW	3	ICT	Informační systém	Ztráta dat, ztráta spojení, zpoždění, neúplnost, chyba nastavení, napadení, kopírování
15	Kancelářský software (Open office, Libre office, Microsoft 365)	SW	3	ICT	Kancelářský software/balík	Ztráta dat, ztráta spojení, zpoždění, neúplnost, chyba nastavení, napadení, kopírování
16	Kamerový systém	HW	4	Provozní ředitel	Kamerový systém	Poškození, nefunkčnost, krádež, zneužití
17	Mobilní telefony	HW	4	Provozní ředitel, ICT	Mobilní telefon	Poškození, nefunkčnost, krádež, zneužití
18	Pc, notebook, USB, CD, DVD	HW	4	ICT	Mobilní zařízení	Poškození, nefunkčnost, krádež, zneužití
19	Severy	HW	4	ICT	Servery, zálohovací zařízení	Nedostupnost, havárie, krádež
20	Síť	HW	4	ICT	Intranet, wifi, dokumentace	Nedostupnost, nefukčnost, havárie
21	Tiskárny, skenery, kopírky	HW	4	ICT	Zařízení sloužící k tisku a skenování	Poškození, nefunkčnost, krádež, zneužití
22	Jednatelé	Lidé	5	Jednatelé	Vedení firmy, zastupování firmy na venek	Úmrtí, dlouhodobá nepřítomnost, selhání, zneužití informací nebo firemních prostředků, sabotace
23	Zaměstnanci	Lidé	5	Jednotlivý zaměstnanci firmy	Všichni zaměstnanci firmy - interní a externí	Úmrtí, dlouhodobá nepřítomnost, selhání, zneužití informací nebo firemních prostředků, sabotace
24	Pracovníci personalistiky a mezd	Lidé	5	Pracovníci personalistiky a mezd	Práce s osobními údaji zaměstnanců	Úmrtí, dlouhodobá nepřítomnost, selhání, zneužití informací nebo firemních prostředků, sabotace
25	Managament firmy	Lidé	5	Managament firmy	Pracovníci managamentu/cotrollingu	Úmrtí, dlouhodobá nepřítomnost, selhání, zneužití informací nebo firemních prostředků, sabotace
26	Správa sítě společnosti	Lidé	5	ICT	Informační a kumunikační technologie	Úmyslné / neumyslné zpřístupnění dat neoprávněným osobám (zanedbání povinnosti při správě cizí věci), zneužití informací
27	Budova	Fyzická místa	6	Provozní ředitel	Budova společnosti	Živelná pohroma, požár, pád letadla, náraz auta, úmyslná poškození, napadení 3. osobou

Obrázek 3 - Seznam aktiv

Zdroj: Vlastní zpracování

Tato tabulka na obrázku „Obrázek 2 - Seznam aktiv“ obsahuje informace o aktivách společnosti a souvisejících rizicích. V tabulce jsou uvedena aktiva, která spadají do 6. skupin – procesy, informace, software, hardware, lidé a fyzická místa. Každému aktivu je taky přidělen tzv. vlastník aktiva neboli osoba odpovědná za dané aktivum. Popis aktiva uvádí informace o procesu a funkci aktiva, a rizika se zaměřují na možné problémy, které mohou nastat, pokud proces nebude řádně splněn nebo se naskytnou komplikace. Tyto rizika se mohou týkat například nedodržení zákonů o ochraně osobních

údajů (GDPR), ztráty dat, zpoždění, neúplnost, chybné nastavení, napadení, nebo kopírování citlivých dat.

Pro analýzu byl následně vytvořen hlavní excelový soubor. Tento soubor se skládá z celkového počtu 29 listů. První list s názvem „Souhrn“ slouží pro shrnutí a výsledky analýzy rizik, zatímco listy 2-28 jsou označeny čísly odpovídajícími hodnoceným aktivům. Poslední 29. list s názvem „data“ obsahuje tabulku s aktivy firmy, která je zobrazena v „Obrázek 3 – seznam aktiv“.

Následně byl vytvořen samostatný list pro jednotlivá aktiva a jejich následné hodnocení, viz. „Obrázek 4 – Hodnocené aktivum“. Pro tento účel byl vytvořen seznam rizik a zranitelností, které mohou aktiva firmy ohrozit. Seznam rizik a zranitelností obsahuje: uživatel se vydává ze někoho jiného, pracovník smluvní organizace se vydává za někoho jiného, cizí osoba se vydává ze někoho jiného / nepovolený vstup, nedovolené použití aplikace, zavedení poškozujícího nebo poškozeného softwaru, zneužití systémových zdrojů, infiltrace komunikací, odposlech komunikace v síti, manipulace s komunikací v síti, popření odpovědnosti, poruchy komunikací, vložení zlomyslného kódu, chybné směřování, technická závada počítače, technická závada paměťového zařízení, technická závada tiskového zařízení, technická závada síťové distribuční komponenty, technická závada serveru, technická závada síťového rozhraní, technická závada síťové služby, přerušení dodávky elektrické energie, porucha klimatizace, chyba systémového nebo síťového softwaru, chyba aplikačního softwaru / dlouhá odezva, chyba operátora / administrátora, chyba pracovníka údržby HW / SW, ztráta dat a dokumentace, chyba uživatele, požár, poškození vodou, přírodní pohroma, náhle snížení počtu zaměstnanců/zastupitelnost, krádež/kopírování ze strany vlastních zaměstnanců, krádež / kopírování ze strany cizích osob, úmyslné poškození vlastními zaměstnanci, úmyslné poškození cizími osobami, terorismus.

	A	B C	D	E	F	G	H
1	č	**Hodnocené aktivum**	**strategie a plánování, interní audit,**				
2	1	Typ procesu	**Proces**				
3		Popis aktiva	Procesy strategie a plánování, interní audit. Managemer				
4		Vlastník aktiva	**Manažer kvality, Provozní ředitel**				
5	**Pravděpodobnost výskytu** (jak často lze průměrně		**VN=1**	**N=2**	**S=4**	**V=8**	**VV=16**
6	očekávat incident, Pravděpodobnost vzniku - PV)		<10 let	3 roky	1 rok	3 měs.	1 měs.
7	**Následek - Úroveň zranitelnosti**		**N=2**		**S=8**	**V=32**	
8	(dojde-li k incidentu,jaký bude dopad - následek - N)		malý		střední	velký	
9			**PV**	**N**	**Index Rizika IR=PV*N**		
10	1	Uživatel se vydává za někoho jiného	1	2	2		
11	2	Pracovník smluvní organizace se vydává za někoho jiného	1	2	2		
12	3	Cizí osoba se vydává za někoho jiného, nepovolený vstup	1	2	2		
13	4	Nedovolené použití aplikace	1	2	2		
14	5	Zavedení poškozujícího nebo poškozeného softwaru	1	2	2		
15	6	Zneužití systémových zdrojů	1	2	2		
16	7	Infiltrace komunikací	1	2	2		
17	8	Odposlech komunikace v síti	1	2	2		
18	9	Manipulace s komunikací v síti	1	2	2		
19	10	Popření odpovědnosti	1	2	2		
20	11	Poruchy komunikací	1	2	2		
21	12	Vložení zlomyslného kódu	1	2	2		
22	13	Chybné směrování	1	2	2		
23	14	Technická závada hostitelského počítače	1	2	2		
24	15	Technická závada paměťového zařízení	1	2	2		
25	16	Technická závada tiskového zařízení/Plotru	1	2	2		
26	17	Technická závada síťové distribuční komponenty	1	2	2		
27	18	Technická závada serveru	1	2	2		
28	19	Technická závada síťového rozhraní	1	2	2		
29	20	Technická závada síťové služby	1	2	2		
30	21	Přerušení dodávky elektrické energie	1	2	2		
31	22	Porucha klimatizace	1	2	2		
32	23	Chyba systémového nebo síťového softwaru	1	2	2		
33	24	Chyba aplikačního softwaru, padání, dlouhá odezva	1	2	2		
34	25	Chyba operátora / administrátora	1	2	2		
35	26	Chyba pracovníka údržby HW, SW - automat.odhlášení	1	2	2		
36	27	Ztráta dat, dokumentace	1	2	2		
37	28	Chyba uživatele	1	2	2		
38	29	Požár	1	2	2		
39	30	Poškození vodou	1	2	2		
40	31	Přírodní pohroma	1	2	2		
41	32	Náhlé snížení počtu pracovníků, zastupitelnost	1	2	2		
42	33	Krádež, kopírování ze strany vlastních zaměstnanců	1	2	2		
43	34	Krádež, kopírování ze strany cizích osob	1	2	2		
44	35	Úmyslné poškození vlastními zaměstnanci	1	2	2		
45	36	Úmyslné poškození cizími osobami	1	2	2		
46	37	Terorismus	1	2	2		

Obrázek 4 - Hodnocené aktivum

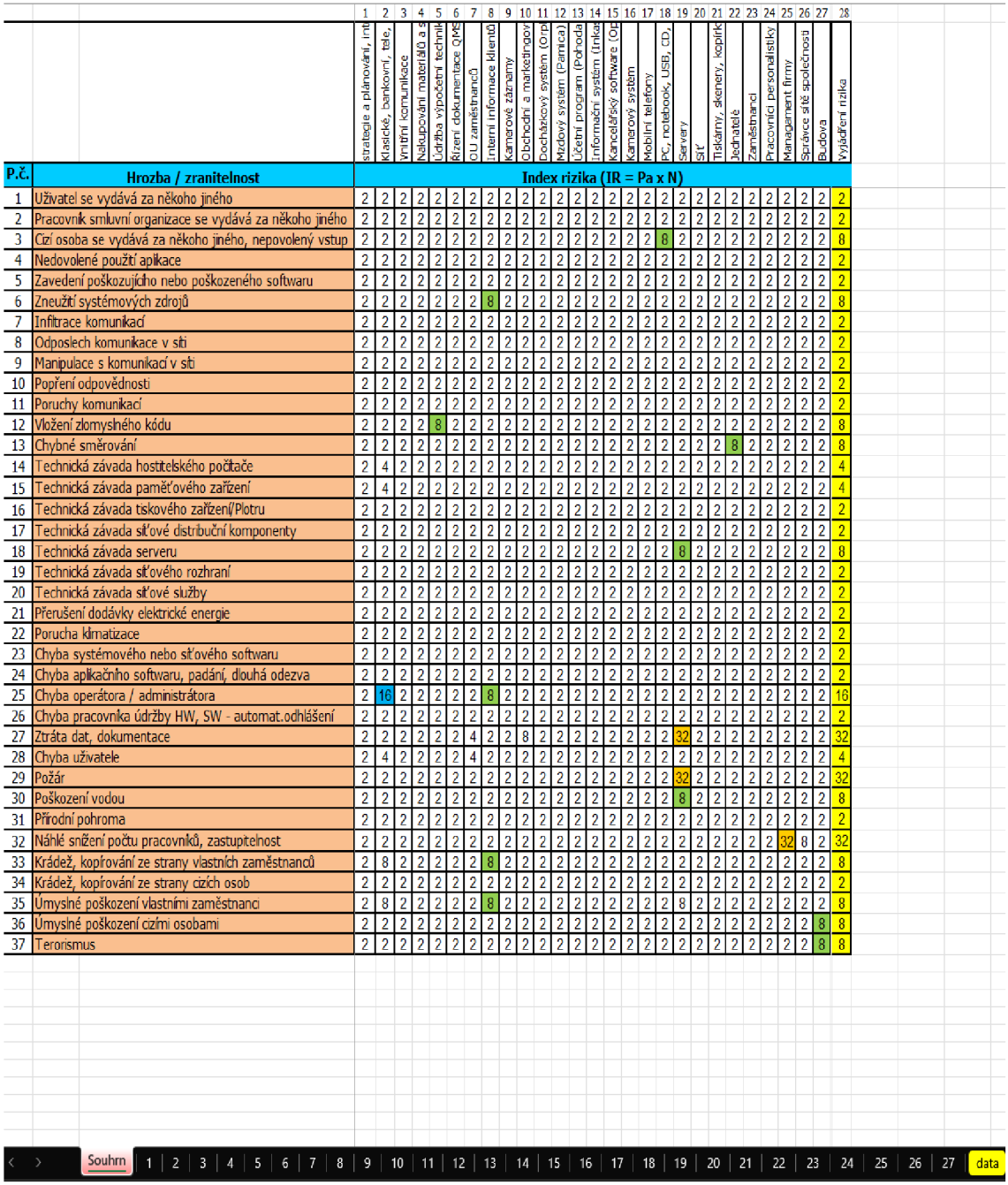
Zdroj: Vlastní zpracování

Dne 15. 11. 2022 proběhla ve společnosti B4B INKASSO s.r.o. schůzka s provozním ředitelem a zaměstnancem ICT. Hlavním cílem této schůzky bylo zhodnocení rizika a hrozeb, kterým firma čelí. Schůzka byla strukturována jako rozhovor a brainstorming, během kterého byly kladeny otázky na fungování firmy, jejich procesy, aktiva, rizika a hrozby. Cílem bylo identifikovat a posoudit rizika jednotlivých aktiv a hledat způsoby, jak je minimalizovat.

Brainstorming probíhal přibližně 2 hodiny a byl zaměřen na otázky a posuzování hrozeb jednotlivých aktiv. Každé aktivum bylo diskutované do hloubky se zaměřením na rizika, která aktivu mohou hrozit, a na pravděpodobnost, s jakou se dané riziko může vyskytovat.

Následně byly podle odpovědí provozního ředitele a zaměstnance ICT vyplněny tabulky hodnocených aktiv. Ke každému riziku byla přiřazena jeho pravděpodobnost výskytu a následek, což za použití vzorce „IR = PV x N“ nám dalo výsledný index rizika., viz. „Obrázek 4 – Hodnocené aktivum“.

Tyto tabulky pak sloužily jako podklad pro vytvoření nového listu s názvem „Souhrn“. Souhrn tabulky ukazuje výsledek analýzy rizik. Tabulka bere data ze všech hodnocených aktiv a ukazuje nám, u které hrozby máme nejvyšší riziko, které firmě hrozí. Můžeme si to představit jako bodový graf, při kterém osa X vyjadřuje hodnocená aktiva a osa Y vyjadřuje hrozby / zranitelnosti. Z této tabulky lze následně vyčíst, u kterých aktiv a u které hrozby nám hrozí nejvyšší riziko, viz. „Obrázek 5 – Souhrn a vyjádření rizika“



P.Č.	Hrozba / zranitelnost	Index rizika (IR = Pa x N)																										
		1 strategie a plánování, int	2 Klasické, bankovní, tele.	3 Vnitřní komunikace	4 Nakupování materiálů a s	5 Údržba výpočetní techni	6 Řízení dokumentace QMS	7 OU zaměstnanců	8 Interní informace klientů	9 Kamerové záznamy	10 Obchodní a marketingov	11 Docházkový systém (Orp	12 Mzdový systém (Pamica)	13 Účetní program (Pohoda	14 Informační systém (Inka	15 Kancelářský software (OF	16 Kamerový systém	17 Mobilní telefony	18 PC, notebook, USB, CD,	19 Servery	20 Síť	21 Tiskárny, skenery, kopírk	22 Jednatelé	23 Zaměstnanci	24 Pracovníci personalistiky	25 Management firmy	26 Správce sítě společnosti	27 Budova	28 Vyjádření rizika
1	Uživatel se vydává za někoho jiného	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	Pracovník smluvní organizace se vydává za někoho jiného	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	Cizí osoba se vydává za někoho jiného, nepovolený vstup	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8	2	2	2	2	2	2	2	2	8
4	Nedovolené použití aplikace	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5	Zavedení poškozujícího nebo poškozeného softwaru	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
6	Zneužití systémových zdrojů	2	2	2	2	2	2	2	8	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8
7	Infiltrace komunikací	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
8	Odposlech komunikace v síti	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
9	Manipulace s komunikací v síti	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
10	Popření odpovědnosti	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
11	Poruchy komunikací	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
12	Vložení zlomyslného kódu	2	2	2	2	8	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8
13	Chybné směrování	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8	2	2	2	2	8
14	Technická závada hostitelského počítače	2	4	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	4
15	Technická závada paměťového zařízení	2	4	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	4
16	Technická závada tiskového zařízení/Plotru	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
17	Technická závada síťové distribuční komponenty	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
18	Technická závada serveru	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8	2	2	2	2	2	2	2	8
19	Technická závada síťového rozhraní	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
20	Technická závada síťové služby	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
21	Přerušení dodávky elektrické energie	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
22	Porucha klimatizace	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
23	Chyba systémového nebo síťového softwaru	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
24	Chyba aplikačního softwaru, padání, dlouhá odezva	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
25	Chyba operátora / administrátora	2	16	2	2	2	2	2	8	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	16
26	Chyba pracovníka údržby HW, SW - automat.odhlášení	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
27	Ztráta dat, dokumentace	2	2	2	2	2	4	2	2	8	2	2	2	2	2	2	2	2	2	32	2	2	2	2	2	2	2	32
28	Chyba uživatele	2	4	2	2	2	4	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	4
29	Požár	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	32	2	2	2	2	2	2	2	32
30	Poškození vodou	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8	2	2	2	2	2	2	2	8
31	Přírodní pohroma	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
32	Náhlé snížení počtu pracovníků, zastupitelnost	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	32	8	2	32
33	Krádež, kopírování ze strany vlastních zaměstnanců	2	8	2	2	2	2	8	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8
34	Krádež, kopírování ze strany cizích osob	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
35	Úmyslné poškození vlastními zaměstnanci	2	8	2	2	2	2	8	2	2	2	2	2	2	2	2	2	2	2	8	2	2	2	2	2	2	2	8
36	Úmyslné poškození cizími osobami	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8	8
37	Terorismus	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	8	8

Obrázek 5 - Souhrn a vyjádření rizika

Zdroj: Vlastní zpracování

4.4. Identifikována rizika

V této kapitole budou představeny identifikovaná rizika na základě analýzy rizik bezpečnosti informací v předchozí kapitole. Rizik existuje veliké množství, a proto budou představena jen ta, u kterých vyšel vyšší index rizika.

Ztráta dat a dokumentace

Jedno z významných rizik podniku B4B INKASSO s. r. o. je ztráta dat a dokumentace. Toto riziko zahrnuje ztrátu všech důležitých dat, jako jsou například soubory, software, databáze, e-maily a další informace, které jsou uloženy na serveru. Firma B4B INKASSO s. r. o. je z důvodu své podnikatelské činnosti na těchto datech závislá a případná ztráta dat by měla pro podnik velké dopady. Případné dopady závisí na množství ztracených, či nepřístupných dat. Mezi tyto dopady můžeme zařadit narušení firemních procesů a fungování firmy, ztrátu produktivity, finanční ztrátu, snížení důvěryhodnosti u zákazníků a klientů.

Firma B4B INKASSO s.r.o. má uložena všechna svá data na serverovně v budově. Firma nedisponuje externí serverovnou nebo cloudovými úložišti. V případě jakékoli nechtěné akce může firma o data ze serveru přijít bez možnosti návratu, což by pro firmu mělo velký negativní dopad.

Existuje velké množství faktorů, které mohou vést ke ztrátě dat na serveru včetně technických problémů, jako jsou selhání hardwaru, chybné aktualizace, škodlivého softwaru a nechtěných akcí, jako například náhodné smazání souboru, požár nebo úmyslný útok hackerské skupiny.

Aby se minimalizovala pravděpodobnost ztráty dat a dokumentace, je důležité provádět pravidelné zálohy dat a mít plán obnovy dat v případě havárie. Také by měly být zavedeny bezpečnostní opatření, jako jsou firewally, antivirové programy a systémy pro detekci hackerských útoků, aby se minimalizovala pravděpodobnost útoků na

server. Další velmi důležitou prevencí je zajištění pravidelných aktualizace softwaru a hardwaru, aby se snížila pravděpodobnost technických problémů, které by mohly vést ke ztrátě dat.

Náhle snížení počtu pracovníků, zastupitelnost

Společně se ztrátou dat a dokumentací tvoří tohle riziko největší hrozbu pro podnik. Firma B4B INKASSO s. r. o. a její chod je ze značné části závislá na provozním řediteli z důvodu jeho rozsahu práce a nezastupitelnosti. Pokud by v důsledku neočekávaných situacích, jako jsou například nemoci, úrazy nebo nepředvídatelné události provozní ředitel vypadl, byl by ohrožen celkový chod firmy.

Ve firmě B4B INKASSO s.r.o. zastává provozní ředitel vícero funkcí, jako například bezpečnostního manažera a vedoucího ICT. Z tohoto důvodu je provozní ředitel ve firmě B4B INKASSO s.r.o. nenahraditelným článkem firmy. Aby se minimalizovalo riziko složité zastupitelnosti provozního ředitele, má firma vypracovaný krizový plán a příručku, ve které jsou popsány všechny úkony provozního ředitele v případě jeho výpadku. Avšak je potřeba brát v úvahu, že provozní ředitel zastává velmi široké spektrum funkcí a zodpovědností v rámci společnosti. Z tohoto důvodu vyplývá, že toto opatření není vzhledem k rozsahu jeho práce plně dostačující.

Požár

Požár je jednou z nejvážnějších hrozeb pro bezpečnost informací ve firmě B4B INKASSO s.r.o. Pokud k požáru dojde, mohou být zničeny fyzické nosiče dat, jako jsou pevné disky, servery, zálohovací zařízení a další zařízení pro ukládání dat. Tyto ztráty dat představují významné riziko pro funkčnost organizace, jelikož by mohly způsobit vážné dopady na provozu společnosti. V případě, že by ke ztrátě dat opravdu došlo, můžou být narušeny obchodní procesy a společnost by mohla čelit značné finanční ztrátě. Požár může ovlivnit funkčnost organizace i nepřímo, a to přerušením dodávky elektrické energie, což může mít za následek nemožnost přístupu k důležitým informacím.

Firma B4B INKASSO s.r.o. má zpracovaný plán v případě požáru, zaměstnanci pravidelně absolvují školení o bezpečnosti a na chodbách se nachází hasící přístroje. Serverovna je oddělena ve speciální místnosti, kde má přístup pouze provozní ředitel a technik ICT. Firma, avšak nedisponuje záložním serverem nebo cloudovým úložištěm a v případě vyhoření serveru by všechna data byla ztracena.

Zneužití systémových zdrojů a chyba operátora

Zneužití systémových zdrojů je riziko, které může být způsobeno interními nebo externími útočníky. Ve firmě B4B INKASSO s.r.o. představují zejména toto riziko vlastní zaměstnanci firmy, neboť vnější útočníci mají minimální možnost proniknout do interního prostředí společnosti.

Jedná se o menší riziko než rizika předešlé z důvodu dobrých bezpečnostních opatření firmy. Riziko představuje práce zaměstnanců s citlivými a osobními informacemi klientů a dlužníků. Zaměstnanci call centra mají přístup k citlivým informacím, jako jsou například adresa a rodné číslo dlužníka. Pokud je tento přístup zneužit, může dojít k odcizení dat, neoprávněnému využití dat nebo jejich šíření. Naplnění tohoto rizika by mělo při firmu značné negativní dopady včetně pokut od klientů a zhoršení image firmy.

Chyba operátora je riziko velmi podobné riziku zneužití systémových zdrojů. Toto riziko představuje chybu operátora, která může být způsobena například neznalostí procesů, nedostatečnou kvalifikací nebo neopatrností při manipulaci s daty. Tato chyba může mít za následek ztrátu dat, porušení zákonných povinností, například v oblasti ochrany osobních údajů nebo finanční ztráty pro firmu.

Firma B4B INKASSO s.r.o. má zavedená pravidla a opatření pro minimalizace rizika zneužití systémových zdrojů a chyb operátora. Patří sem například školení zaměstnanců, pravidelná aktualizace softwaru a hardwaru, monitorování aktivit zaměstnanců v systému a zavedení bezpečnostních opatření, jako jsou například hesla a šifrování.

4.5. Návrh opatření

Po provedení identifikace rizik ve společnosti B4B INKASSO s.r.o. je následně možné navrhnout opatření, jejichž cílem je minimalizovat negativní dopady rizik a předcházet jim. Tento proces má za úkol zajistit, že společnost bude schopna adekvátně reagovat na nečekané situace a minimalizovat případné škody.

Ztráta dat a dokumentace

Ztráta dat a dokumentace představují pro firmu značné riziko, jelikož je chod firmy na datech závislý. Firma B4B INKASSO s.r.o. má riziko ztráty dat a dokumentace ošetřené skrze zálohování na interní server firmy, který je umístěn ve speciálně zabezpečené místnosti s omezeným přístupem pro dané osoby. Kromě toho je také server vybaven UPS zařízením, což zajišťuje neustálou dodávku energie v případě výpadku a chrání server před nečekanými výboji elektřiny. Tyto opatření jsou bezpochyby důležitými opatřeními pro minimalizaci rizika ztráty dat, ovšem je nutné si uvědomit, že i přes tyto kroky mohou nastat nečekané události jako například selhání hardwaru, škodlivý software, hackerský útok nebo požár, které mohou způsobit ztrátu dat nebo dokumentace.

Z toho důvodu je pro vyšší míru zabezpečení dat a dokumentace firmě B4B INKASSO s.r.o. doporučeno zvážit následující opatření: zavedení externí serverovny nebo cloudového úložiště. Toto opatření by firmě umožnilo bezpečné uložení či zálohu informací a přístup k nim v případě nechtěné nebo nečekané ztráty dat na interním serveru firmy, což by přispělo k vyššímu zabezpečení dat a dokumentace. Samostatné rozhodnutí o tom, zda zvolit externí serverovnu nebo cloudové úložiště, závisí na konkrétních potřebách firmy, jako jsou přístupnost nebo finanční náklady.

Náhle snížení počtu pracovníků, zastupitelnost

Problém složité zastupitelnosti zaměstnance, konkrétně provozního ředitele, představuje značné riziko pro fungování společnosti. Momentální opatření firmy B4B INKASSO s.r.o. spočívá v důkladné dokumentaci procesů, postupů a náplně práce provozního ředitele, v případě potřeby jeho zastoupení. Chod firmy B4B INKASSO s.r.o. je z velké části závislý na práci provozního ředitele. Ten zastává klíčové pozice, pravomoci a odpovědnosti, které ovlivňují výkonnost celé firmy. Z tohoto důvodu je důležité brát riziko složité zastupitelnosti velmi vážně a zvážit přijmutí opatření k minimalizaci dopadu na provoz firmy v případě jeho nepřítomnosti.

Návrh opatření na minimalizaci rizika složité zastupitelnosti provozního ředitele spočívá v zavedení opatření jako je rozšíření pravomocí a kompetencí dalších klíčových pracovníků a zaměstnanců, aby byli schopni plnit úkoly provozního ředitele v případě jeho nepřítomnosti. Je možné také zvážit nábor nebo povýšení zaměstnanců na post „Vedoucí It“ a „Manažer kvality nebo Bezpečnostní manažer“, kteří by mohli převzít některé zodpovědnosti a úkoly, které nyní spadají na provozního ředitele, čím by se snížila závislost chodu firmy na provozním řediteli.

Požár

Hlavním rizikem, které přináší požár, je zejména možnost zničení serverovny, což by v důsledku vedlo k nevratné ztrátě dat a informací. Vzhledem k povaze činnosti firmy B4B INKASSO s.r.o. požár nepředstavuje významné riziko, avšak tento fakt nesmí být důvodem k podceňování bezpečnostních opatření, neboť i malý požár by mohl mít v následků katastrofální důsledky na provoz firmy. Momentální opatření firmy spočívá v umístění hasících přístrojů na jednotlivých odděleních firmy a v pravidelném školení BOZP zaměstnanců.

Riziko požáru tedy spočívá především ve zničení serverovny a následné ztrátě dat. Z toho důvodu návrh opatření je totožný jako u rizika ztráty dat a dokumentace, a to v zavedení externí serverovny nebo cloudového úložiště, čímž by se toto riziko minimalizovalo.

Zneužití systémových zdrojů a chyba operátora

Toto riziko spočívá zejména ve zneužití citlivých dat klientů a dlužníků zaměstnancem firmy. Firma B4B INKASSO s.r.o. si je vědoma vážnosti tohoto rizika a z toho důvodu má zavedené interní mechanismy, které minimalizují šanci zneužití systémových zdrojů zaměstnancem a chyby operátora. Mezi tato opatření patří pravidelné školení zaměstnanců, pravidelné aktualizace softwaru, monitorování kroků zaměstnanců na počítačích a zavedení bezpečnostních opatření jako je šifrování dat, silná hesla a nemožnost použití externích USB zařízení.

S ohledem na uvedené faktory lze konstatovat, že firma disponuje adekvátními prostředky k minimalizaci rizika zneužití lidských zdrojů a chyby operátora. Proto by se firma měla nadále držet svých osvědčených postupů a bezpečnostních opatření, aby zajistila jejich efektivní implementaci a maximalizovala ochranu svých dat a aktivit.

Závěr

Cílem této bakalářské práce bylo analyzovat rizika bezpečnosti informací ve vybrané společnosti a navrhnout opatření, jak těmto rizikům předcházet. Analýza rizik bezpečnosti informací je klíčovým procesem, který umožňuje firmám identifikovat a vyhodnotit potenciální hrozby pro bezpečnost informací. Zároveň umožňuje vyvinout a implementovat preventivní opatření pro minimalizaci rizik.

První kapitola bakalářské práce se zaměřuje na terminologii a definici rizika. Kromě samotné definice rizika je zde popsáno, jak probíhá identifikace rizika a jaké nástroje jsou k tomu použity, dále je zde vysvětlena klasifikace rizika a teorie řízení rizik.

Další kapitola se zaobírá analýzou rizik. Tato kapitola začíná charakteristikou analýzy rizik a jsou v ní popsány základní pojmy analýzy rizik, se kterými se můžeme běžně setkat. Velké část této kapitoly je věnována obecnému postupu analýzy rizik a metodám, které se při analýze rizik mohou použít, jako například brainstorming, metoda „What – If“ a metoda Delphi.

Třetí kapitola se věnovala problematice bezpečnosti informací. Byl kladen důraz na vysvětlení pojmu bezpečnost informací a co si pod tím čtenář může představit.

Další velká část nebo kapitola bakalářské práce je praktická část. Tato kapitola se zaměřuje na analýzu rizik bezpečnosti informací ve vybraném podniku B4B INKASSO s.r.o. Nejdříve je zde uvedena charakteristika firmy a její současný stav. Po charakteristice firmy již následuje samostatná analýza bezpečnosti informací, která identifikovala několik potencionálních rizik, jako například ztrátu dat serverů, ztrátu dat a dokumentace a náhlé snížení počtu zaměstnanců či jejich složité zastoupení. Pro minimalizaci rizik bylo navrženo několik preventivních opatření, jako je pořízení externího serveru nebo cloudového úložiště a předání části zodpovědnosti provozního ředitele na vícero zaměstnanců.

Je potřeba zdůraznit, že analýza rizik bezpečnosti informací je dynamický proces, který vyžaduje pravidelné aktualizace a revize, aby firma mohla přizpůsobit své

bezpečnostní opatření novým hrozbám. Výsledky této analýzy by měly být pravidelně aktualizovány a využívány jako základ pro další opatření ke zlepšení bezpečnosti informací ve firmě. Na závěr lze říci, že analýza rizik bezpečnosti informací je nezbytným procesem, který by měl být součástí bezpečnostní strategie každé firmy.

Seznam použité literatury

Knižní zdroje:

ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.

ČSN EN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

ČSN ISO 31000. *Management rizik — Směrnice.* Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

ČSN EN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. Praha: Český normalizační institut, 2014.

FOTR, Jiří a Jiří HNILICA. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada). ISBN 978-80-247-5104-7.

FOTR, Jiří. *Jak hodnotit a snižovat podnikatelské riziko*. Praha: Management Press, 1992. ISBN 80-85603-06-3.

MERNA, Tony a Faisal F AL-THANI. *Risk management: řízení rizika ve firmě*. Vyd. 1. Brno: Computer Press, 2007, xii. ISBN 978-80-251-1547-3.

NEUGEBAUER, Tomáš. *Vyhledání a vyhodnocení rizik v praxi*. 2., aktualiz. a rozš. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-458-3.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada). ISBN 978-80-247-3051-6.

VAJDOVÁ, Eva. *Analýza týmové práce v inkasní firmě.* Ostrava, 2008, 49 s. Diplomová práce. Vysoká škola Báňská, Fakulta metalurgie a materiálového inženýrství, Katedra ekonomiky a managementu v metalurgii. Vedoucí práce Ing. Andrea Samolejová, Ph.D.

Elektronické zdroje:

Inkaso pohledávek | B4B INKASSO. Inkaso pohledávek | B4B INKASSO [online]. Copyright © 2022 B4B INKASSO. Všechna práva vyhrazena. [cit. 15.04.2023]. Dostupné z: https://b4b-inkasso.com/

Metody a způsoby hodnocení rizik na pracovišti | BOZP.cz. Dokumentace BOZP a PO | BOZP.cz [online]. Copyright © 2023 CRDR spol. s r.o. [cit. 06.03.2023]. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/

Risk Analysis (Definition, Methods) | Qualitative & Quantitative. Investment Banking, Financial Modeling & Excel Blog [online]. Copyright © 2023 . CFA Institute Does Not Endorse, Promote, Or Warrant The Accuracy Or Quality Of WallStreetMojo. CFA [cit. 04.03.2023]. Dostupné z: https://www.wallstreetmojo.com/risk-analysis/

The 12 Elements of an Information Security Policy. Exabeam - Cybersecurity & Compliance with Security Log Management and SIEM [online]. Copyright © 2023 Exabeam [cit. 15.04.2023]. Dostupné z: https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/

What is Information Security (Infosec)? – TechTarget Definition. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/information-security-infosec

Seznam použitých symbolů a zkratek

s.r.o.	Společnost s ručeným omezeným
SWOT	Analýza silných a slabých stránek
PEST	Analýza politicko-právního, ekonomického, sociálně-kulturního a technologického prostředí
EU	Evropská unie
ČR	Česká republika
ISO	Mezinárodní organizace pro standardizaci
ČSN	Česká technická norma
ALE	Očekávaná roční ztráta
SLE	Ztráta při jednom výskytu hrozby
ARO	Pravděpodobnost výskytu hrozby za rok
HAZOP	Analýza nebezpečnosti a provozuschopnosti
FMEA	Analýza způsobů a důsledků selhání
FMCEA	Analýza kritičnosti způsobů a účinků poruch
IR	Index rizika
PV	Pravděpodobnost výskytu rizika
N	Následek rizika
ICT	Informační a komunikační technologie
UPS	Zdroj nepřerušovaného napájení

Seznam obrázků

Seznam tabulek