Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky

Bezpečnost a analýza rizik v praxi

Vypracoval: **Jakub Hlahůlek**
Vedoucí práce: **Ing. Ladislav Luc**
Rok vypracování: **2015**

Čestné prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Veškeré použité podklady, ze kterých jsem čerpal informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V..... dne .... Podpis: .....

Poděkování:

Rád bych poděkoval především Pavlovi Kozumplíkovi, majiteli firmy TESLUX Lighting s.r.o., za poskytnutý čas a hodnotné informace, potřebné k realizaci této bakalářské práce. Dále bych chtěl poděkovat svému vedoucímu bakalářské práce Ing. Ladislavu Lucovi.

Abstrakt

Cílem práce bude seznámit se s problematikou bezpečnosti aktiv společnosti. Prakticky ověřit metody řízení bezpečnosti informací ve firmách, pomocí příslušných norem. Poté provést analýzu rizik na konkrétní firmě a vyhodnotit tím nejzávažnější rizika. Na závěr navrhnout v kooperaci s vlastníkem této firmy vytvoření bezpečnostních opatření zabraňujících vzniku analyzovaných rizik.

Klíčová slova

Bezpečnost informací, analýza rizik, identifikace rizik, hodnocení rizik, ošetření rizik, aktivum, hrozba.

Abstract

The aim of this work is getting acquainted with the safety of the companie´s assets. To practicly verify the information methods of security management on companies implemented through adequate standards. Then perform risk analysis on a specific company and assess the most serious risks. In conclusion propose safety measures to prevent risks which have been analyzed in cooperation with the owner of this company.

Keywords

Security of informations, risk analysis, risk identification, risk assessment, treatment of risks, asset, threat.

Obsah

1. Úvod

1.1. Úvod do problematiky

Se stoupající rychlostí, s jakou se technologie i společnost posouvá dopředu, rostou i její nároky. A nejedná se jenom o nároky na kvalitu, rychlost či cenu, ale rostou také nároky na zabezpečení. Jakákoliv práce, ať už jde o pozici zahradníka, či bankovního makléře, se zrychluje, zefektivňuje a automatizuje. Rozhodování na jakémkoliv stupni řízení probíhá v kratším čase a ve větším množství. A i když tyto trendy posouvají naši společnost dopředu, zvyšuje to množství rizik, které mohou nastat. A právě tato rizika jsou tématem této bakalářské práce.

Každá firma či organizace se snaží být tou nejlepší ve svém oboru a posouvat své hranice co nejdále a díky tomu musí řídit i svá rizika, zabezpečit jakékoliv hrozby. V ideálním případě minimalizovat všechna rizika do takové podoby, že nehrozí žádné nebezpečí, které by mohlo ohrozit chod společnosti. Tento cíl je samozřejmě nereálný, vždy budou určitá rizika existovat. Čím blíže se ovšem k tomuto cíli dostaneme, čím více budou tato rizika zanedbatelná, tím většího úspěchu dosáhneme.

1.2. Cíl práce

Jaká rizika můžou ve firmě vzniknout? Jak je rozpoznat? Jak je analyzovat a určit, která jsou závažná a která nikoliv? A nakonec - jak tato rizika minimalizovat?

Na tyto otázky nám pomůže naleznout odpověď analýza rizik. [2] Boudou zde vysvětleny její principy, metody a postupy. Nejdříve se teoreticky proberou všechny podklady, které budou k analýze potřeba, jak tyto podklady získat a ohodnotit. Následně se vypočítá závažnost rizik a na závěr se zváží, jak firmu zabezpečit před těmito riziky.

Pro následující praktickou část byla vybrána firma TESLUX lighting s.r.o., s jejímž majitelem bude probíhat spolupráce, vedoucí k úspěšné aplikaci této analýzy rizik. V závěru budou s majitelem probrány možnosti zabezpečení těchto rizik.

Tato bakalářská práce je neveřejná.

2. Bezpečnost a analýza rizik

2.1. Co to je riziko a analýza rizik?

Samotný pojem riziko sebou nese spoustu významů. Záleží na oboru, ve kterém se tento pojem používá, ale také na konkrétním člověku, jaký význam si osvojí. V oblasti řízení podnikatelských rizik se definuje jako určitá pravděpodobnost toho, že nastane jev, který je různý od jevu předpokládaného. Neměl by být ovšem chápán pouze jako pravděpodobnost, neboť pojem zahrnuje i míru následků, jenž riziko může vyvolat. [1] K lepšímu pochopení může pomoci definice, že riziko je nebezpečí vzniku určité ztráty. [2] V každém případě riziko vždy souvisí s negativní událostí, které se snažíme vyhnout. K tomu aby rizika nenastala, nebo se alespoň minimalizovala, slouží analýza rizik. Jak už název vypovídá, jde o to, že pokud chceme řídit rizika, musíme je nejdříve analyzovat. Tento proces spočívá v definici mnoha pojmů a získávání a analyzování mnoha dat, jenž budou vysvětlena v dalším postupu. Ve stručnosti je potřeba nejprve stanovit kontext, neboli hranice analýzy rizik. Poté identifikovat rizika a jejich složky (aktiva, hrozby, stávající opatření, zranitelnosti, následky). Teprve poté je možné získat množinu rizik, se kterou se dá operovat, čímž se zabývá analýza rizik. Ta se skládá z posouzení následků, určení pravděpodobnosti incidentu a určení úrovně rizik. Na to se naváže ohodnocením rizik a ve finální části bude zpětně posouzeno, která rizika jsou nejzávažnější a měla by se ošetřit. [2]
Analýza rizik se dá provádět na mnoha stupních podrobnosti, závisí to na zvolených kritériích. Na těchto úrovních se musí ohodnocovat a počítat s mnoha daty. Analýza může probíhat kvantitativně, nebo kvalitativně, případně kombinací obou. V praxi se většinou začíná kvalitativní analýzou, kvůli menší náročnosti. [8]

2.1.1. Kvalitativní analýza rizik

U kvalitativní analýzy je zvolena vhodná škála (například 1 - 10, nebo malé, střední, velké). Dle této škály jsou poté hodnoceny rizika, jejich následky a pravděpodobnosti výskytu. Výhodou je větší jednoduchost a snadná pochopitelnost. Nevýhodou je subjektivní ohodnocení, jenž může být někdy zavádějící. Může také nastat problém při následném ošetření rizika, jelikož náklady na něj vynaložené se problematicky srovnávají s kvalitativním ohodnocením. Tato metoda se používá pokud je charakter dat vhodnější pro tuto metodu, nebo pokud jsou údaje nepoužitelné ke kvalitativní analýze, nebo jako předloha k detailnější analýze. [2]

2.1.2. Kvantitativní analýza rizik

Kvantitativní analýza používá číselné hodnocení a výpočty. Je založena na přesnosti ocenění následků a jejich pravděpodobností. Metoda je sice detailnější a poskytuje přesnější informace,

ovšem je také mnohem náročnější ať už na data, tak i na čas. Data jsou využívaná z více zdrojů a je velmi pravděpodobné, že nebude k dispozici dostatek relevantních dat, zejména u nových rizik. [2]

2.2. Základní pojmy

Zde jsou definovány základní pojmy, určující množinu dat, jenž je potřeba nashromáždit k analýze. K tomu existuje mnoho postupů v závislosti na organizaci, na kterou bude daný postup aplikován.

2.2.1. Aktiva

Pod pojmem aktivum si většina lidí, jenž má alespoň základní ekonomické znalosti, představí účetní aktivum, tedy položky majetku, hmotný i nehmotný majetek společnosti. V tomto případě má ale aktivum mnohem širší rozsah. Jedná se o všechno co společnost vlastní, má pro ni určitou hodnotu a tato hodnota může být vlivem negativního jevu snížena. [2]
Určení všech takových aktiv může být velmi obtížné, stačí si uvědomit, co všechno dané firmě hodnotu přináší. Nejedná se pouze o hmotné věci jako jsou peníze, budova nebo hardware, ale také o nehmotné věci jako informace, patenty, pověst apod. K tomu je nutné zahrnout i lidský faktor, zaměstnance, jejich oddanost, loajalitu či morálku. Dalším faktorem jsou externí firmy a dodavatelé. V pozici majitele firmy dokonce i vlastní dispozice, jako je například zdraví a v neposlední řadě se nesmí opomenout naši zákazníci. Zákazník dokonce bývá jedním z klíčových aktiv, na kterých stojí existence firmy. Ale jak tedy neopomenout žádné aktiva? K tomu mohou dopomoci normy, kde se vyskytují seznamy používaných aktiv. Další oblíbenou možností je kategorizace, tedy rozdělení aktiv do skupin, které nejvíce přísluší posuzované firmě.

Dle normy je vhodné rozdělit aktiva na dvě základní skupiny [8]:

Primární aktiva

- Obchodní procesy a činnosti
- Informace

Podpůrná aktiva všech typů

- Hardware
- Software
- Sítě
- Pracovníci
- Lokalita
- Organizace

Co všechno jednotlivé oblasti obsahují je vysvětleno dále v postupu nasazení analýzy.

Další důležitou částí bude ohodnocení aktiv vzhledem k tomu, jakou hodnotu pro naší společnost mají. Ohodnocení může být prováděno buď objektivně dle ceny, nebo subjektivně dle užitku, což může být často velmi zavádějící. K tomuto hodnocení bývá zvolena vlastní škála, jak bude dále, vysvětleno. [8]

2.2.2. Hrozby

Jde o iniciátor výše zmíněného negativního vlivu. To co negativní jev způsobí, ať už jde o věc, sílu, událost či osobu. Hrozba může být úmyslná, nahodilá nebo environmentální (není založena na lidské činnosti) a dle toho by měla být posuzována. Hrozba může působit zvnějšku i uvnitř organizace. Může být přírodního nebo lidského původu [8].

2.2.3. Bezpečnostní opatření (protiopatření)

Jde o postupy, metody, systémy, činnosti, věci a cokoliv dalšího, co slouží k zamezení nebo snížení existence hrozby, jejího dopadu, nebo zranitelností. Jejím účelem je následkům předcházet a vyhnout se tak zbytečným nákladům. Jejich základními vlastnostmi jsou efektivita a náklady. Efektivita sděluje, do jaké míry jsou schopné omezit hrozby a náklady říkají jakou mají hodnotu. Do nákladů se musí započítat nejen náklady na pořízení, ale i náklady na zavedení a provoz. [8]

2.2.4. Zranitelnost

Jde o slabinu, nedostatek nebo jakýkoliv jiný stav aktiva, který může hrozba využít k tomu aby způsobila škodu aktivům organizace. Zranitelnost sama o sobě není nebezpečná. Vyžaduje hrozbu, která této zranitelnosti využije. Pokud taková hrozba neexistuje, nemusí se řešit zabezpečení, ale měla by se sledovat. Stejná vazba platí i naopak, hrozba nemusí nutně představovat riziko, pokud neexistuje zranitelnost, které by využila.

Pro lepší pochopení následuje příklad. Aktivem je budova společnosti, její zranitelností je nedostatečné zabezpečení. Hrozbou jsou například zloději. Tím vzniká riziko, že zloději využijí špatného zabezpečení budovy k jejímu vykradení. Ovšem pokud by bylo zabezpečení v pořádku, samotní zloději by nepředstavovali riziko. Stejně tak pokud by zloději neexistovali, špatné zabezpečení by také nepředstavovalo riziko.

Zranitelnost vzniká při každém střetu hrozby s aktivem. Její základní veličinou je úroveň. Ta je dána citlivostí (náchylnosti aktiva vůči hrozbě) a kritičností (důležitostí aktiva pro analyzovaný subjekt). Zranitelnost může ale i nemusí souviset se základní funkcí aktiva. Musí se proto sledovat, zda zranitelnost vychází ze zdrojů, která jsou pro aktivum hlavní nebo vedlejší.[8].

2.2.5. Následky (dopad)

Následek, jak už název vypovídá, je jev, který následuje po určitém incidentu. Může způsobit například ztrátu účinnosti, zničení pověsti, škodu, nedostupnost atd. Identifikuje dopad na organizaci, způsobený podle scénáře incidentu. Tento scénář popisuje hrozby zneužívající určitou zranitelnost nebo více zranitelností. Následek může ovlivnit jedno, více, nebo jen část aktiva. Následky mohou být dočasné nebo trvalé. Následky by měly být posuzovány z mnoha hledisek a to: vyšetřování a doba nápravy, ztráta času, ztráta příležitosti, zdraví a bezpečnost, finanční náklady na zvláštní dovednosti nutné pro nápravu škody a pověst a důvěryhodnost.[8]

3. Příslušné normy

Analýza rizik bude prováděna na základě norem. Konkrétně norem ČSN ISO/IEC 27000 až ČSN ISO/IEC 27005. Tyto normy patří do kategorie informační technologie, bezpečnostní techniky. Jedná se o řadu norem ISMS, které popisují Systém řízení bezpečnosti informací. Obsah této práce je částí ISMS. Normy vysvětlují jeho účel, termíny, požadavky, postup, metody implementace, výsledky, udržování a aktualizace.
Hlavní normou je ČSN ISO/IEC 27005, která zahrnuje veškerý postup k aplikování analýzy rizik. Informace z této normy jsou detailně popsány v kapitole 4. Zde je stručně shrnut obsah zbylých souvisejících norem.

3.1. ČSN ISO/IEC 27000: Systémy řízení bezpečnosti informací - Přehled a slovník

Norma vysvětluje předmět norem ISMS, určuje, které normy sem patří, jejich základní definici a vysvětluje související termíny.
Struktura začíná předmětem normy, dále pokračuje termíny a definicemi, a následuje kapitola o Systémech řízení bezpečnosti informací. Poté je výčet a základní obsah norem z řady ISMS a na závěr přílohy, které vysvětlují slovesné tvary pro vyjádření ustanovení a definují vlastnosti termínů.

3.1.1. ISMS

ISMS neboli Systém řízení bezpečnosti informací obsahuje soubor metod, praktik a postupů, jak mají organizace řídit a chránit svá informační aktiva. Obsahuje podrobný návod jak, kde a za jakých požadavků tento systém aplikovat a jaké analýzy nám k tomu dopomáhají. Cílem ISMS je aby informační aktiva byly natolik chráněna, aby konala činnost vedoucí k cílům podniku. Pod pojmem informační aktiva rozumíme informace nesoucí určitou hodnotu pro organizaci vedoucí k dosažení sílů podniku. Tyto informace jsou uchovávány buďto v digitální formě (harddisk), materiální formě (papír), nebo v nezapsané formě tj. v myslích majitele či zaměstnanců. Únik, ztráta, nebo zničení takovýchto informací může mít kritické následky pro celou organizaci, proto je tyto informace nutné řídit a zabezpečit.
Důležitost ISMS je dána stále rozvíjejícím, rychlejším a více sofistikovaným hrozbám, vůči kterým musí být společnosti schopny se bránit. Navíc je každá organizace velmi rozdílná a ISMS musí být aplikován na každou organizaci cíleně a v celém rozsahu.

Norma člení zavedení ISMS do následujícího postupu. Identifikace informačních aktiv a jejich bezpečnostních požadavků. Posoudit a ošetřit rizika bezpečnosti informací. Vybrat a implementovat potřebná opatření vůči nejzávažnějším rizikům. Tato opatření sledovat, spravovat a vylepšovat, aby neustále plnily svoji funkci.

I po úspěšném nasazení ISMS práce nekončí. ISMS musí být pravidelně udržován a aktualizován, jinak s neustále se rozvíjejícími hrozbami brzo ztratí smysl.[3]

3.2. ČSN ISO/IEC 27001: Systémy řízení bezpečnosti informací - Požadavky

Tato norma definuje požadavky na zavedení, udržování a aktualizování systému řízení bezpečnosti informací v organizaci. Tyto požadavky musí být splněny v celém rozsahu, pokud chce organizace splňovat podmínky normy. Jednotlivé požadavky se týkají kontextu a organizace, vůdčími rolemi, plánováním, podporou, provozováním, hodnocením výkonnosti a zlepšováním . Norma obsahuje jednu přílohu, která obsahuje rozsáhlou tabulku s cíly, opatřeními a jednotlivými opatřeními, zajišťující bezpečnost informací.[4]

3.3. ČSN ISO/IEC 27002: Soubor postupů pro opatření bezpečnosti informací

Obsahuje postupy a doporučení pro výběr opatření k zavedení v rámci ISMS založeného na ČSN ISO/IEC 27001. Obsahuje 14 kapitol vysvětlujících cíle a pokyny k implementaci jednotlivých opatření. Při analýze rizik nám tato norma může velmi pomoci k porovnávání jednotlivých opatření s realitou a tím ke snadnější identifikaci hrozeb a zranitelností. Jednotlivé kapitoly se zabývají politikou bezpečnosti informací, organizací bezpečnosti informací, bezpečností lidských zdrojů, řízením aktiv, řízením přístupu, kryptografií, fyzickou bezpečností a bezpečností prostředí, bezpečností provozu a komunikací, akvizicí, údržbou a vývojem systému, vztahy s dodavateli, řízením incidentů bezpečnosti informací, aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací a soulady s požadavky. [5]

3.4. ČSN ISO/IEC 27003: Směrnice pro implementaci systému řízení bezpečnosti informací

Tato norma obsahuje postup, jak implementovat systém ISMS v souladu s ISO/IEC 27001:2005. Podporuje přípravu zahájení plánu implementace, definování organizační struktury pro projekt a získání souhlasu vedení organizace. Dále kritické činnosti pro projekt a příklady naplnění

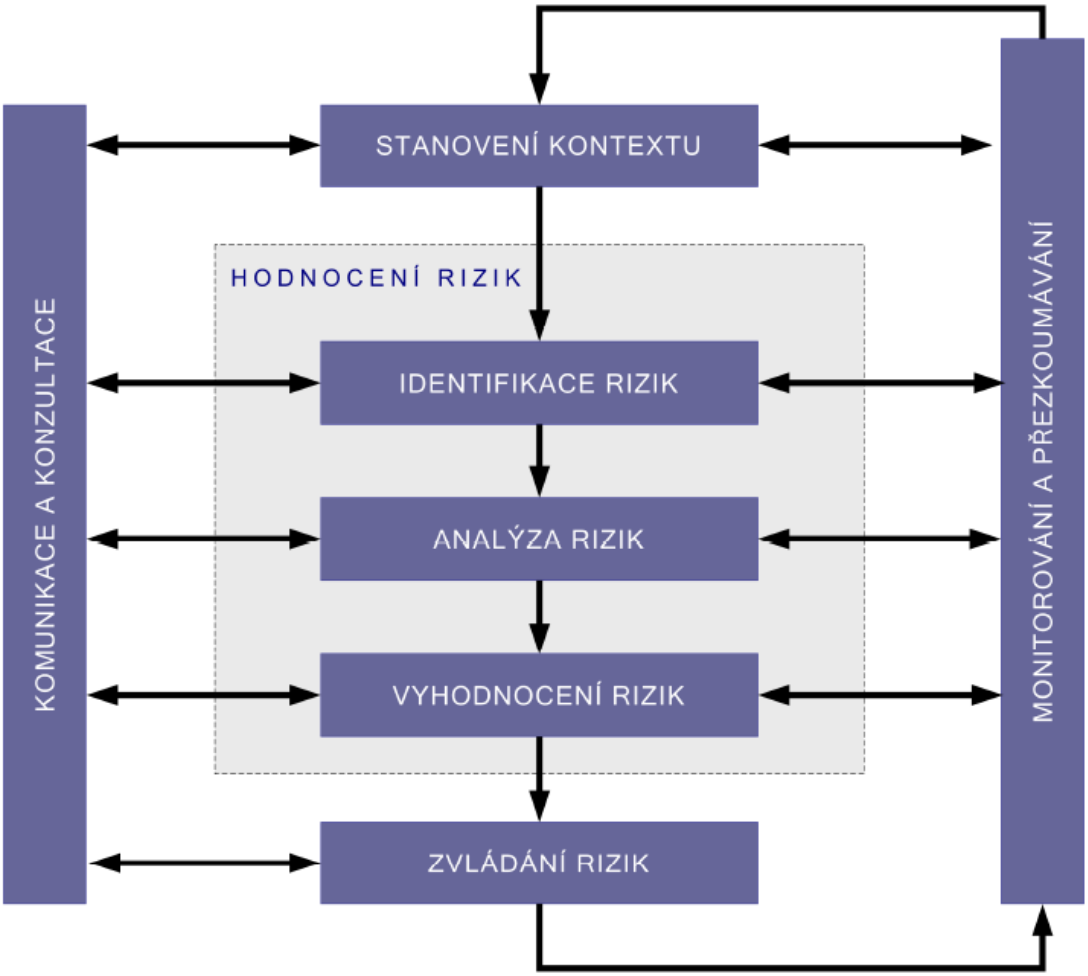
požadavků normy ISO/IEC 27001:2005. Norma neobsahuje návod k provozu ISMS, pouze doporučení k zahájení provozování. Výstupem je finální plán implementace projektu ISMS. Jednou z částí tohoto projektu je i obsah této práce, proto s ní tato norma souvisí. [6]

3.5.ČSN ISO/IEC 27004: Řízení bezpečnosti informací - měření

Norma poskytující doporučení k používání metrik a měření účinnosti zavedeného systému ISMS dle ISO/IEC 27001. Doporučení se zabývají politikou, řízením rizik bezpečnosti informací, opatřeními, procesy a podporou revize změn nebo zlepšení. Toto měření pomáhá organizaci, která řídí ISMS k identifikaci a vyhodnocení nežádoucích procesů a součástí tohoto programu. Tento proces předpokládá porozumění rizikům bezpečnosti informací a správného hodnocení rizik dle normy ISO/IEC 27005, čímž navazuje na tuto práci. [7]

4. Postup analýzy rizik

Tento postup bude vycházet převážně z normy ČSN ISO/IEC 27005 a knihy Řízení rizik ve firmách a jiných organizacích. Ve všech fázích postupu musí být proces neustále přezkoumáván a monitorován, neboť se během jeho průběhu může změnit mnoho podstatných informací, které ovlivní průběh analýzy. Postup začíná stanovením kontextu, poté identifikací, analýzou a vyhodnocením rizik a na závěr ošetřením neboli zvládáním rizik. Viz obr. 4.



Obrázek 4: Postup analýzy rizik

4.1. Určení činností společnosti vedoucí k zisku a základní pochopení firmy

Ke kvalitní analýze je třeba firmu pochopit do hloubky. Proto je potřeba nejen prodiskutovat všechny podstatné záležitosti, ale také firmu navštívit a vidět všechno na vlastní oči. Je nutné probrat základní myšlenku a cíl firmy od základů až po jednotlivé činnosti tvořící celek. Musí se podrobně chápat hlavní činnost firmy nejenom v současnosti, ale i v minulosti (historie) a v

budoucnosti (vize). Důležitá je samozřejmě také celková organizační struktura, i jednotliví zaměstnanci a jejich funkce. Je třeba vymezit místo firmy na trhu, její konkurenci, jednotlivé produkty, dodavatele i odběratele. Čím více je toho o firmě v jednotlivých oblastech zjištěno, tím větší je jistota, že následující postup bude vykonán správně.

4.2.Stanovení kontextu (Určení hranice analýzy rizik)

Před samotnou identifikací rizik je třeba stanovit kontext organizace. To znamená určení jednotlivých kritérií, rozsahu a hranic, a stanovení organizační struktury pro další postup. Je důležité určit účel této analýzy rizik, což může být například podpora ISMS nebo příprava plánu reakce na incidenty apod. [8]

4.2.1. Základní kritéria

Je důležité určit přístup k řízení rizik, který závisí na rozsahu a cílech řízení rizik a který řeší základní kritéria. Musí být také zkontrolováno, zda jsou k dispozici potřebné zdroje pro všechny plánované činnosti.
Musí se stanovit následující kritéria: kritéria hodnocení rizik, kritéria dopadu, kritéria akceptace rizik. [8]

4.2.2. Rozsah a hranice

Rozsah by se měl určit, aby bylo jasné do jaké hloubky brát v potaz aktiva. Hranice se určují aby se vědělo, která rizika řešit a která ne. Při tomto určování by se měly brát v potaz základní informace o firmě uvedené v předchozí kapitole. Pokud jsou některé části organizace vyloučeny, měl by se uvést důvod. [8]

4.2.3. Organizace řízení rizik bezpečnosti informací

Cílem je určit osobu nebo více osob, jenž budou mít na starost celý proces analýzy rizik a budou zodpovídat za jeho jednotlivé části.. Jejich povinností bude řídit a rozvíjet proces řízení rizik, rozdělovat role a určovat vztahy mezi nimi, specifikovat záznamy k uchování. [8]

4.3. Identifikace rizik

4.3.1. Identifikace a ohodnocení aktiv

Jak už bylo u definice aktiv zmíněno, pro jejich základní identifikaci budou rozdělena na dvě základní skupiny a to primární a podpůrná aktiva, které obsahují další složky, jenž budou nyní vysvětleny. [8]

Primární aktiva

Identifikaci zajišťují představitelé hlavních procesů organizace. Jsou to obvykle hlavní procesy, informace o činnosti v rámci rozsahu a organizační procesy.
Dělíme je na:

1) *Obchodní (dílčí) procesy a činnosti:*

Jejich ztráta nebo omezení znemožňuje plnit poslání firmy. Obsahují tajné, patentové nebo jinak chráněné procesy. Jejich změna ovlivní chod celé organizace. Procesy nezbytné pro splnění smluvních, právních nebo regulačních požadavků.

2) *Informace:*

Informace a strategické informace nezbytné pro plnění poslání a cílů organizace. Osobní údaje dle zákona týkající se soukromí. Informace, které jsou časově a nákladově velmi náročné. [8]

Podpůrná aktiva

Obsahují zranitelnosti, které zneužívají hrozby, aby poškodily primární aktiva v rámci rozsahu.
Typy:

1) *Hardware:*

Skládá se ze všech procesů, podporujících fyzické prvky.
Obsahuje: zařízení pro zpracování dat, přenosná zařízení (notebook), pevná zařízení (PC), procesní periferie (tiskárna), nosiče dat, elektronické nosiče (CD ROM), ostatní nosiče (papír, fax)

2) *Software:*

Všechny programy pomáhající hardwaru ke zpracovávání dat.
Obsahuje: operační systém (jádro a základní funkce nebo služby), software pro služby, údržbu nebo správu (doplňuje služby OS a není přímo ve službách uživatelů nebo aplikací), softwarové balíky nebo standardní software (databázový software), podnikové aplikace (účetní software)

3) *Sítě*

Telekomunikační zařízení využívaná k propojení fyzicky vzdálených počítačů nebo prvků informačního systému.

Obsahuje: medium a podpory (ethernet, ADSL), pasivní nebo aktivní přenos (směrovač, rozbočovač), komunikační rozhraní (GPRS, adaptér ethernetu)

4) Pracovníci

Obsahuje: ti, co rozhodují (vedení organizace), uživatelé (management financí), pracovníci provozu/údržby (správce systému), vývojáři (vývojář podnikových aplikací)

5) Lokalita

Všechna místa, která zcela nebo zčásti zasahují do našeho rozsahu činnosti a fyzické prostředky potřebné pro jejich provoz.

Obsahuje: vnější prostředí (domovy pracovníků, městská oblast), areál (budovy), zóna (kanceláře), nezbytné služby (pro provoz zařízení organizace), komunikace (telefonní linka), vybavení (klimatizace)

6) Organizace

Organizační rámec sestávající ze všech struktur pracovníků přidělených k úkolu a postupů kontrolujících tyto struktury.

Obsahuje: řídící orgány (správní orgán), organizační struktura organizace (řízení lidských zdrojů), projektová nebo systémová organizace (projekt vývoje nové aplikace), subdodavatelé/dodavatelé/výrobci (konzultační společnosti). [8]

Ohodnocení aktiv

V této části se musí každému aktivu přiřadit určitá hodnota. Jak již bylo dříve vysvětleno, aktiva se můžou ohodnotit kvalitativně nebo kvantitativně. Kvůli velké různorodosti aktiv je důležité si tento výběr důkladně promyslet. Některá aktiva se můžou ohodnotit přesnou sumou, pro jiné jsou vhodnější slova jako "důležité" či "kritické". Proto se po důkladné konzultaci zvolí vhodné řešení a případně se vytvoří potřebná škála hodnocení. Tato škála má běžně mezi 3 a 10 úrovněmi a pro každou se definují její limity.

Při hodnocení se musí pečlivě dbát na zvolená kritéria. Důležité je snažit se co nejvíce vyhnout subjektivnímu hodnocení a zaměřit se na definovaná kritéria. Těmi může být například původní cena, cena za případné nahrazení nebo ztráty způsobené následky negativních jevů. V potaz se bere také nepopiratelnost, odpovědnost, autentičnost a spolehlivost.

Často se stává, že aktivům je přiřazeno více hodnot v závislosti na pohledu a hodnotícím. V takovém případě se ovšem musí hodnoty zredukovat na jedinou, jelikož tato hodnota ovlivní další postup práce. K volbě kritérií může pomoci jejich seznam v příloze B.2 normy ČSN ISO/IEC 27005.

V neposlední řadě se nesmí zapomenout při hodnocení na závislosti mezi jednotlivými aktivy a procesy. Čím důležitější je proces, který je na aktivu závislý, tím větší je hodnota tohoto aktiva.

Je třeba rozeznávat i více stupňů závislosti, což může pomoci také při identifikaci hrozeb a zranitelností.
Výstupem celé této části by tedy měl být strukturovaný seznam ohodnocených aktiv. [8].

4.3.2. Identifikace hrozeb

Jedná se o velmi široký pojem, zahrnující spoustu oblastí a jejich správné určení, bez opomenutí některých hrozeb může být často problematické. K tomu opět mohou pomoci normy (konkrétně ČSN ISO/IEC 27005 obsahuje v příloze C tabulku typických hrozeb), či katalogy hrozeb, přičemž se nesmí zapomenout na jejich aktualizování. [2] Při jejich identifikaci by se měli nejprve rozlišit hrozby obecně (fyzické zničení, technické poruchy) a poté pokud je potřeba definovat jednotlivé hrozby. Nesmí se opomenout na to, že některé hrozby mohou postihnout více aktiv a tím se jejich závažnost zvyšuje.

Identifikuje se pomocí konzultace s vedením firmy, manažery, s vlastníky aktiv, ale i pomocí právních orgánů, meteorologických stanic, pojišťoven apod. Pomoci může také pohled do historie firmy, jaké incidenty se zde již odehrály a jaké problémy nastávaly nejčastěji. Nesmí se zapomenout na to, že současné hrozby se neustále mění a zdokonalují. [8]

U hrozby se určuje typ zdroje:

- A - accidental - náhodný - lidské činnosti, které mohou náhodně poškodit aktiva
- D - deliberate - úmyslný - lidské úmyslné akce cílené na aktiva
- E - environmental - environmentální - incidenty, které nesouvisí s lidskou činností

Důležitou vlastností hrozby je její dopad, neboli velikost následků, jenž hrozba může způsobit. Její ohodnocení se rovněž může vyjádřit subjektivně nebo objektivně dle zvoleného měřítka hodnocení [2].
Na závěr by se měl získat zhotovený seznam hrozeb, jejich typu a zdroje.

4.3.3. Identifikace stávajících opatření

Bezpečnostní opatření jsou významná v mnoha fázích analýzy. Již na počátku je důležité identifikovat stávající bezpečnostní opatření. Tedy taková, která jsou již ve firmě zavedena a která plní svou funkci. Je to důležité jednak proto, aby firma později nesnažila zavést opatření, které se zde již vyskytuje a jednak proto, aby se brali tato opatření v potaz při určování pravděpodobnosti hrozeb či výši zranitelností. Je ovšem třeba zvážit i současnou funkčnost opatření. Některá mohou být zastaralá, nedostačující, jiná mohou selhat atd. To se dá zjistit kontrolou dřívějších auditů nebo přezkoumáváním vedením organizace. U těchto nefunkčních opatření by se mělo určit, jak s nimi bude dále naloženo. Zda se opraví, nahradí, či zruší. V potaz by měla být také brána opatření, jenž jsou plánovaná.

K identifikaci může pomoci přezkoumávání dokumentů stávajících opatření, kontrola s pracovníky, kteří za ně odpovídají, přezkoumávání fyzických opatření na místě nebo kontrola výsledků auditů [8].

4.3.4. Identifikace zranitelností

K této identifikaci by měl být k dispozici již hotový seznam aktiv, hrozeb i stávajících opatření. Tvoří se vazby mezi seznamem hrozeb a aktiv, které můžou zneužít, právě díky zranitelnosti. Tu ještě může snižovat nebo zcela eliminovat stávající nebo plánované opatření. Oblasti, ve kterých lze aktiva identifikovat, jsou organizace, procesy a postupy, běžné praxe řízení, pracovníci, fyzické prostředí, konfigurace informačního systému, hardware, software nebo komunikační zařízení, závislost na externích stranách.

Zranitelnost se může hodnotit dle scénářů incidentů, kde hrozby zneužívají aktiva, nebo dle příkladů zranitelností přístupného v normě ISO/IEC 27005.

Zde je výsledkem seznam zranitelností vůči aktivům a hrozbám a seznam zranitelností, které se k žádné hrozbě nevztahují [8].

4.3.5. Identifikace následků

V této fázi by již měly být zhotoveny všechny předchozí seznamy (aktiva, hrozby, opatření, zranitelnosti). Je třeba vytvořit seznam scénářů incidentů. To znamená, že ke každé hrozbě se přiřadí aktivum, které může ohrozit, zranitelnost kterou může využít a stávající opatření, které může snížit následek. Poté jsou opět formou rozhovoru a pomocí informací o posouzení technických zranitelností (příloha B, ČSN ISO/IEC 27005) identifikovány následky neboli dopad těchto incidentů, který se může značně lišit oproti hodnotě samotného aktiva. Tím se získá seznam scénářů incidentů s jejich následky vůči procesům a aktivům [8].

4.4. Analýza rizik

4.4.1. Posuzování následků

V této části se musí zhodnotit identifikované scénáře incidentů. Při hodnocení pomáhá již určená hodnota aktiv, ale často může nastat rozdíl mezi hodnotou tohoto aktiva a následkem neboli dopadem na organizaci. Různé hrozby totiž můžou ohrozit jedno, část nebo i více aktiv. Různé hrozby mají na aktiva odlišné dopady.

Při hodnocení se opět volí mezi kvantitativní a kvalitativní metodou. Finanční vyjádření vyjadřuje podrobnější informace potřebné k rozhodnutí, ovšem rozhodnutí o volbě metody opět primárně závisí na dostupnosti potřebných dat, formě organizace a obchodních činnostech.

Při hodnocení následků se bere nejčastěji v úvahu hodnota za náhradu těchto aktiv a obchodní následky ztráty nebo kompromitace aktiva. Přičemž hodnota následků obchodní ztráty bývá většinou vyšší, než náklady na vyměnění, či obnovení tohoto aktiva a pověřená osoba by se měla řídit vyšší hodnotou.
Další pomůckou můžou být informace o již uskutečněných incidentech v minulosti a závažnost jejich následků, ovšem musí se brát v potaz, že hrozby i aktiva se neustále vyvíjejí a dopad může být dnes zcela odlišný než dříve.
Výstupem v této části bude seznam ohodnocených následků scénáře incidentů souvisejících s aktivy a kritérii dopadu. [8]

4.4.2. Určení pravděpodobnosti incidentu

Zde je potřeba ke každému incidentu přiřadit pravděpodobnost jeho výskytu. K tomu slouží opět kvantitativní nebo kvalitativní metody. Například zvolení škály pravděpodobnosti výskytu během jednoho či více let.
Při určování pravděpodobnosti se musí brát v potaz zkušenosti z minulosti a platné statistiky o výskytu hrozeb, motivaci a schopnost uskutečnění hrozby a úmyslných hrozeb, geografické faktory u náhodných hrozeb, zranitelnosti a jejich vazby na aktiva, účinnost stávajících opatření vůči hrozbám.
Pravděpodobnost se může určovat buď zvlášť, nebo je možné některá aktiva spojovat do skupin dle potřeby.
Výstupem zde budou pravděpodobnosti určené u všech incidentů. [8]

4.4.3. Určení úrovně a hodnocení rizik

Zde se volí úroveň rizik u každého podstatného scénáře incidentu. Volba závisí především na již ohodnocené pravděpodobnosti a následcích scénáře. V potaz by se ale měly brát také další proměnné vhodné pro hodnocení rizik (náklady, zainteresované strany). Jde o proces, kdy se již uvažuje o scénářích možných incidentů jako o rizicích.
Existují různé metody k tomuto postupu, jejichž výběr závisí na samotné organizaci.
Úroveň rizik, neboli posouzení rizik provádíme na dvou úrovních podrobnosti. [8]

- **Přehledové posouzení rizik bezpečnosti informací**

Používá se v případech, kdy firma nemá dostatečné prostředky (časové, finanční) k provedení detailní analýzy. Následné ošetření lze omezit pouze na nejkritičtější rizika. Jde o hrubé posouzení následků, namísto detailní analýzy hrozeb, aktiv, zranitelností atd. Používá se také, pokud firma v brzké budoucnosti plánuje zásadní změny (outsourcing) a bylo by neefektivní detailně analyzovat dočasný stav. Jejími hlavními rysy jsou globální pohled na organizaci a její

informační systémy, nezávislost technologie na obchodních záležitostech. Může řešit přímo scénáře možných incidentů a nezabývat se jejími jednotlivými částmi. Díky hrozbám sloučeným do skupin jsou uvažovaná rizika obecnější, s čímž souvisí i jejich ošetření. Vhodné spíše pro organizační a netechnická opatření. Největším nebezpečím je to, že díky menší přesnosti může dojít k opomenutí některých významných rizik. Proto často po tomto posouzení následuje druhé detailní posouzení rizik bezpečnosti informací. [8]

- **Detailní posouzení rizik bezpečnosti informací**

Často následuje po přehledovém posouzení rizik. U detailního posouzení je potřeba nejprve detailně identifikovat a ohodnotit jednotlivá aktiva, hrozby, zranitelnosti a opatření. Tato data poté lze použít k ohodnocení rizik a následnému ošetření. Vyžaduje to mnohem více času, úsilí a informací než u přehledového posouzení. Nejčastější metody jsou založené na tabulkách, které pracují s ohodnocenými následky a pravděpodobnostmi. Tyto metody vysvětlené v příloze E normy ČSN ISO/IEC 27005 jsou zde vysvětleny. [8]

1. *Matice s předem definovanými hodnotami*

Tato metoda se užívá nejčastěji, je také doporučována v knize Řízení rizik ve firmách a jiných organizacích. Aktiva jsou zde hodnocena ve vztahu k nákladům na jejich výměnu nebo obnovu. Tato hodnota je poté převedená na kvalitativní škálu, která je jednotná jak pro fyzická aktiva, tak pro software i informace. Hodnota se určuje pomocí informací od pověřených osob dané společnosti, jež mají v těchto aktivech a incidentech hlavní slovo.

U této metody existují dva typy, přičemž u prvního je potřeba vyhodnotit ještě úroveň hrozby a úroveň zranitelností, rovněž na předem definované škále. Tyto hodnoty spolu s hodnotou aktiva jsou poté porovnány v následující matici, která nám určí výslednou úroveň rizika. Zde uvažujeme úroveň rizika v rozmezí od 0 do 8. [8]

	Úroveň hrozby	Nízká			Střední			Vysoká		
	Úroveň zranitelnosti	N	S	V	N	S	V	N	S	V
Hodnota aktiva	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tabulka 4.4.3.1: Matice s předem definovanými hodnotami 1

Druhý typ porovnává pravděpodobnosti scénáře incidentu s odhadovaným dopadem. Opět v rozmezí od 0 do 8. Tuto hodnotu poté můžeme rozdělit buď dle kritérií akceptace rizik nebo například vytvořit škálu kritičnosti (0-2 nízké, 3-5 střední, 6-8 vysoké). [8] [2]

	Pravděpodobnost scénáře incidentu	Velmi nízká	Nízká	Střední	Vysoká	Velmi vysoká
Dopad	Velmi nízká	0	1	2	3	4
	Nízká	1	2	3	4	5
	Střední	2	3	4	5	6
	Vysoká	3	4	5	6	7
	Velmi vysoká	4	5	6	7	8

Tabulka 4.4.3.2: Matice s předem definovanými hodnotami 2

2. *Třídění hrozeb pomocí míry rizika*

Matice hodnotící jednotlivé hrozby. Závisí zde na sobě hodnota následku (aktiva) a pravděpodobnost výskytu hrozby s ohledem na zranitelnost a opatření. Tyto dvě hodnoty se mezi sebou vynásobí a poté seřadí dle nejvyšší míry rizika. [8]

Popis hrozby (a)	Hodnota následku (aktiv) (b)	Pravděpodobnost výskytu hrozby (c)	Míra rizika (d)	Seřazení hrozeb (e)
Hrozba A	5	2	10	2
Hrozba B	2	4	8	3
Hrozba C	3	5	15	1
Hrozba D	1	3	3	5
Hrozba E	4	1	4	4
Hrozba F	2	4	8	3

Tabulka 4.4.3.3: Třídění hrozeb pomocí míry rizika

3. *Stanovení hodnoty pravděpodobnosti a možných následků rizik*

Největší zřetel je kladen na následky incidentů bezpečnosti informací a na systémy, které by měly být prioritní. Postup začíná určením dvou hodnot pro každé aktivum a riziko, což potom díky matici určí výslednou hodnotu aktiva. Hodnoty všech aktiv v daném systému se sečtou a tím se získá úroveň rizika daného systému. V matici jsou proti sobě postaveny hodnoty aktiva (závislá na nepříznivých následcích) a hodnota pravděpodobnosti (závislá také na zranitelnosti) určitého aktiva a určité hrozby. Tato hodnota se sečte se všemi dalšími hodnotami hrozeb daného aktiva a získá se celková hodnota tohoto aktiva. Nakonec se sečtou všechny hodnoty aktiv v daném systému a tento systém se může porovnávat s dalšími. [8]

Hodnota aktiva	0	1	2	3	4
Hodnota pravděpodobnosti					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Tabulka 4.4.3.4: Stanovení hodnoty pravděpodobnosti a možných následků

4.4.4. Hodnocení rizik

Nakonec, když už je určena celková úroveň u všech rizik, musí se tato rizika posoudit s kritérii hodnocení a akceptace rizik a rozdělit je na kritická rizika, která se musí řešit ihned a ostatní, které zatím stačí pouze monitorovat. Tato kritéria by měla být určena už při stanovení kontextu firmy. Toto rozdělení slouží k následnému separování rizik, jež budou ošetřena, od těch ostatních. [8]

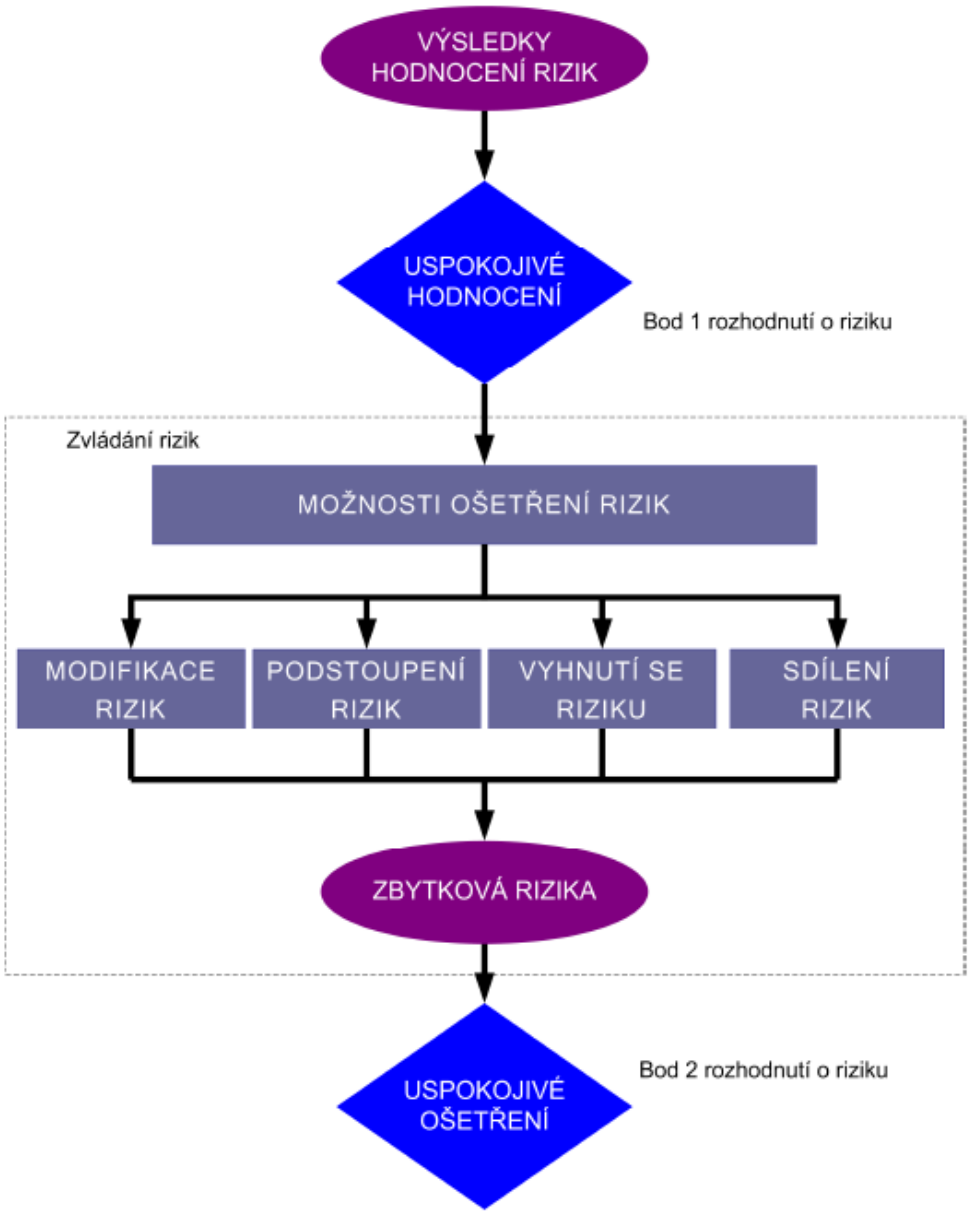
4.5. Akceptace a ošetření rizik bezpečnosti informací

Poslední fáze slouží ke shrnutí výsledků a rozhodnutí o dalším postupu. Vybírají se zde nejzávažnější rizika, určená při hodnocení rizik a u nich se volí způsob opatření. Základní způsoby jsou čtyři. Modifikace, podstoupení, vyhnutí se nebo sdílení rizik. Při volbě způsobu ošetření, by mělo být bráno v potaz mnoho vstupních údajů. Vycházet by se mělo z předchozích kapitol a výsledků hodnocení rizik viz obr. 4.5.. Poté by měla být zvolena jedna z možností ošetření rizik. Tyto možnosti se ovšem nevylučují a můžou být vzájemně kombinovány. Rozhoduje se na základě nákladů spojených se změnou, odstraněním nebo vytvořením nových opatření. Také podle ušetřených nákladů, jež toto ošetření přinese. V některých případech dokonce podle příjmů, které se tím získají. Základní pravidlo je, že čím víc se sníží riziko, při co nejmenších nákladech, tím je opatření přijatelnější.

Některá opatření můžou snížit více rizik (informovanost zaměstnanců o obecných hrozbách) a zároveň ke snížení některých rizik je potřeba více opatření (proti požáru nestačí brát jako opatření dostupnost hasičů, ale i kvalitní pojištění majetku). Může dojít také k volbě odstranění některých stávajících opatření. V takovém případě musíme hledět na to, s kterými opatřeními jsou propojeny a jestli se ekonomicky vyplatí tato opatření rušit.

Musí být sestaven kvalitní plán pro následnou implementaci těchto opatření, zajišťující nejen finanční stránku věci, ale i časovou. Také musí brát v potaz všechna omezení, která se organizace týkají, ať už právní, organizační, regulační, technická či strukturální atd.

Po stanovení plánu je třeba ještě určit zbytkové riziko, k jehož určení může dopomoci opět posouzení tohoto rizika dle matice a finální rozhodnutí, zda je toto zbytkové riziko akceptovatelné. Může nastat zvláštní okolnost, kdy je vhodné riziko akceptovat, i když nesplňuje základní kritéria akceptovatelnosti. Mohou například existovat výnosy z tohoto rizika, které jsou příliš atraktivní, nebo náklady na jeho odstranění jsou příliš vysoké. [8]



Obrázek 4.5: Ošetření rizik

Obsah jednotlivých metod:

- **Modifikace rizika**

Modifikací neboli změnou úrovně rizika, pomocí zavedení, odstranění nebo upravení opatření se docílí snížení rizika na úroveň, která je akceptovatelná. Tato úroveň se musí znovu určit, například podle opětovného detailního posouzení rizika. K volbě a rozsahu opatření může pomoci seznam opatření v normě ISO/IEC 27002. [5] Při volbě opatření se musí také brát v potaz omezení, která tato opatření přinesou, a to zejména: časová, finanční, technická, provozní, kulturní, etická a ekologická, právní, osobní omezení, snadnost použití a omezení při integraci nových a existujících opatření. [8]

Při tomto postupu může být toto opatření zvoleno buď po důkladné konzultaci mezi pověřenými osobami, nebo například opětovným využitím matice s předem definovanými hodnotami. V druhém případě se musí rozdělit riziko do tří fází, dle úrovně zvažovaného opatření. Inherentní riziko znamená, že je vyjádřena úroveň rizika bez jakéhokoliv implementovaného opatření. Reziduální riziko znamená, že se zohlední riziko se všemi stávajícími opatření. Cílové riziko pak znamená, že riziko je vyjádřeno i s novými plánovanými opatřeními v takovém rozsahu, aby se riziko snížilo na akceptovatelnou úroveň. Jak takové zanesení do matice s předem definovanými hodnotami může vypadat je zobrazeno na následující tabulce. [2]

	Pravděpodobnost scénáře incidentu	Velmi nízká	Nízká	Střední	Vysoká	Velmi vysoká
Dopad	Velmi nízká	0	Cílové 1	2	3	4
	Nízká	1	2	3 Reziduální	4	5
	Střední	2	3	4	5	6 Inherentní
	Vysoká	3	4	5	6	7
	Velmi vysoká	4	5	6	7	8

Tabulka 4.5: Využití matice s předem definovanými hodnotami ke snižování rizik

- **Podstoupení rizika**

Rozhodnutí o tom, že se podstoupí, neboli akceptuje toto riziko. Znamená to, že riziko není natolik závažné, nebo se ekonomicky nevyplatí podstupovat další kroky k jeho ošetření. Zde je důležité neopomenout žádný následek tohoto rizika. [8]

- **Vyhnutí se riziku**

Metoda celkově se vyhnout riziku, kvůli velké kritičnosti nebo příliš velkým nákladům na ošetření. Uskuteční se tak, že se zcela přestane vykonávat činnost vedoucí k tomuto riziku, nebo

se natolik upraví podmínky, aby toto riziko nemohlo nastat. Například u přírodních katastrof se přemístí působení firmy na místo, kde toto riziko nehrozí. [8]

- **Sdílení rizik**

Riziko se sdílí, nebo přenese na někoho jiného, což firmě pomůže se s ním vypořádat. Je třeba se zamyslet nad tím, zda toto sdílení nevytvoří nová rizika. Sdílení může být formou pojištění nepříznivých následků, nebo najmutí externí firmy, která se o rizika bude starat. Je ovšem nutné si uvědomit, že je možné sdílet odpovědnost za zvládnutí rizika, ale ne za dopad tohoto rizika. [8]

O všech rizicích a ošetřeních, o všech informacích získaných při analýze a řízení rizik je třeba komunikovat. Je důležité, aby tyto informace byly sdíleny mezi těmi, kteří o nich rozhodují. Obousměrná komunikace poskytne lepší informace pro rozhodnutí, posoudí rizika z více pohledů a umožní pružnější řešení těchto problémů. [8]

5. Představení firmy

K praktickému nasazení analýzy rizik byla vybrána firma TESLUX Lighting s.r.o.. Firma se zabývá prodejem a instalací osvětlení založeném na moderní LED technologii a řízeném stmívání, umožňujícím řídit a šetřit náklady za osvětlení. Nabízí široký sortiment zboží a to například LED diody, LED panely, LED reflektory, LED žárovky či LED svítidla. Provozovna firmy je v Hodoníně, oficiální sídlo firmy je zapsáno v Brně.

Právní formou firmy je společnost s ručením omezeným. Statutárním orgánem je zde jednatel, kterým je Pavel Kozumplík, s nímž bude po celou dobu probíhat spolupráce. Společník firmy je v současnosti jeden a to Pavel Kozumplík, který vlastní 50% obchodního podílu a současně řeší odkoupení zbylých 50% od dědiců po zesnulém druhém společníkovi. Základní kapitál při založení firmy tvořil 200 000,- Kč. V minulém roce se roční obrat pohyboval kolem 25 milionů korun.

5.1. Historie firmy

Majitel firmy Pavel Kozumplík se zabýval činností v oblasti LED technologií od roku 2008. Do roku 2010 byly produkty bez vlastní obchodní značky. V roce 2010 z důvodu rostoucího obchodu a rostoucího potenciálu na trhu založil firmu TESLUX T.S.Trade, která byla zaměřena na tuto činnost. Následně byla zaregistrována ochranná známka TESLUX, pod kterou se začaly uvádět vlastní výrobky na trh. V roce 2012 došlo k přejmenování společnosti na TESLUX Lighting s.r.o., kvůli provázání obchodní známky s firmou. V roce 2012 se z finančních důvodů a důvodu lepšího utužování vztahů s dodavateli a vyjednávání výhodnějších podmínek přidal jako druhý společník k firmě Zhou Chuang, který odkoupil polovinu obchodního podílu. Za dobu své činnosti ve firmě přinesl lepší vyjednávací podmínky s dodavateli v Číně. V prosinci 2013 bohužel Zhou Chuang zesnul a nyní Pavel Kozumplík vyjednal s pozůstalou rodinou odkoupení zbytku firemního podílu zpět. Toto odkoupení nyní probíhá. Od roku 2008 do roku 2010 se činnost firmy zaměřovala spíše na e-shop a mezi lety 2010 až 2011 se k tomu přidaly projekty a maloobchodní prodejny. Od roku 2011 se zaměřují především na velkoobchod, dále na projekty a došlo ke zrušení e-shopu.

5.2. Strategické cíle a vize

V současnosti firma upřednostňuje velkoobchod před koncovými zákazníky. Z tohoto důvodu byl zrušen i e-shop. Firma upřednostňuje vybudování pevných dlouhodobých vztahů s velkými řetězci a odběrateli v sítích velkoobchodů před nejistou poptávkou u koncových zákazníků. Do budoucna se firma snaží upevňovat tyto vztahy, budovat nové s dalšími velkoobchodními řetězci a rozšiřovat své výrobky do co možná nejširšího okolí. Expanze firmy je prioritou. Firma

samozřejmě klade důraz i na inovaci a vývoj svých produktů, šíři jejich nabízeného sortimentu chce ovšem udržet v rozumných mezích.

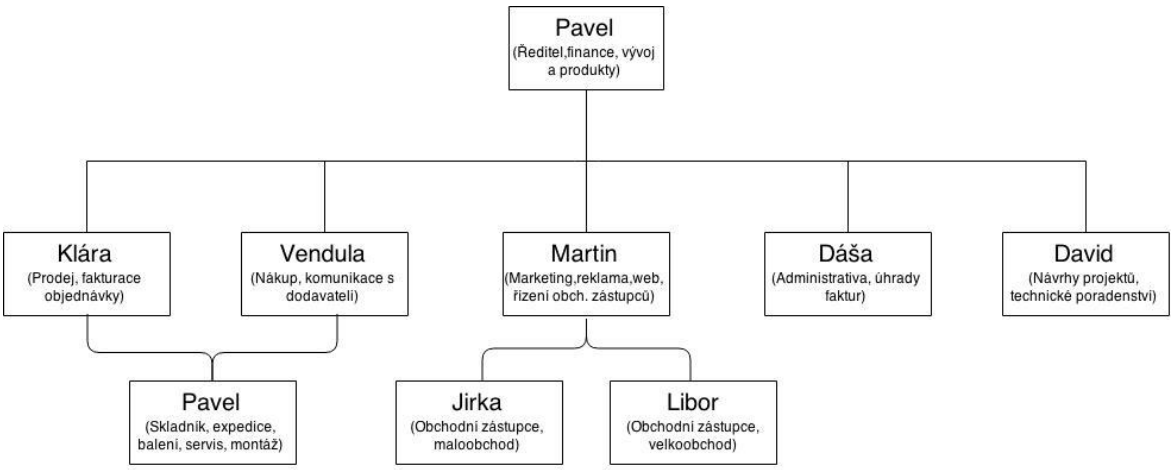
Zároveň si firma uvědomuje velké rizika závislosti na menším počtu klíčových odběratelů a proto se snaží zaměřovat i na menší, například regionální velkoobchodní řetězce. Současně proto začíná rozšiřovat i maloobchodní síť u svých velkoobchodních odběratelů a zároveň u samotných maloobchodů (elektra). Firma najala nového zaměstnance, zaměřeného konkrétně na budování nových vztahů s maloobchody a získávání nových odběratelů.

Zároveň se firma začíná věnovat projektům nejen v oblasti LED žárovek, ale i veřejných osvětlení a svítidel do průmyslového odvětví. Letos proběhla investice do nových modelů pro veřejné osvětlení a průmysl a očekává se výrazný nárůst prodeje. Tímto se firma snaží nabízet jedinečné produkty odlišující se od konkurence. Veškerá tato činnost samozřejmě směřuje k růstu obratů i zisku, což je hlavním cílem firmy do budoucna.

5.3. Organizační struktura

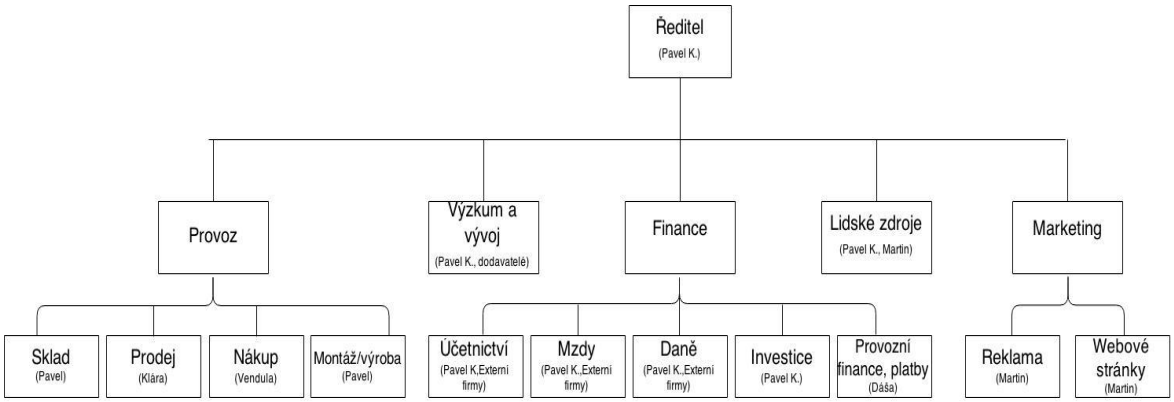
Z důvodu anonymity bude většina zaměstnanců, až na majitele firmy, označena pouze křestním jménem. Firma má v současnosti kromě majitele osm zaměstnanců a plánuje rozšíření o jednoho až dva další.

První schéma jsme rozdělili dle pracovníků a k nim připsali hlavní náplň jejich činnosti. Zároveň jsou seřazeni pod sebou dle odpovědnosti.



Obrázek 5.3.1: Organizační struktura dle zaměstnanců

Druhé schéma rozděluje firmu do základních oddělení, u nichž je vždy připsaný člověk, který za toto oddělení odpovídá.



Obrázek 5.3.2: Organizační struktura dle základních oddělení

5.4.Zaměstnanci

Pavel Kozumplík - v současnosti jediný společník a majitel firmy. Rozhoduje o hlavních událostech firmy, respektive zastává pozici ředitele firmy. Řídí celé finanční oddělení firmy, rozhoduje o investicích a klíčových peněžních tocích. Dále řídí mzdy, účetnictví i daně, které mu provozují externí firmy. Rozhoduje o svých zaměstnancích, podílí se na managementu a vybírá zaměstnance. Komunikuje s klíčovými zákazníky a často jezdí do Číny a Hongkongu jednat se svými obchodními partnery. Díky tomu, že firmu vytvořil a zpočátku zastával všechny současné funkce sám, je schopen řídit veškeré firemní pozice a školit všechny své zaměstnance.

Martin - stará se o marketingovou část firmy. Zařizuje reklamu firmy, stará se o webové stránky (e-shop byl zrušen) a řídí design. Zároveň na pozici lidských zdrojů řídí obchodní zástupce. Udává a kontroluje jejich činnost.

Dáša - zaměstnankyně, která je ve firmě nejdéle, zvládá řídit oblast prodeje i nákupu, ale soustřeďuje se nyní hlavně na administrativní činnost. Stará se o úhrady faktur a jiné provozní platby.

David - návrhář společnosti. Pokud má zákazník zájem o úsporu na osvětlení, David vytvoří návrh projektu. Tyto projekty ovšem samotná firma nerealizuje, ale předává dále svým velkoobchodním řetězcům k realizaci. Také obstarává technické poradenství.

Vendula - řídí nákupní část firmy. To znamená, že zajišťuje nákup potřebných produktů, dílů, součástek. Tím pádem komunikuje s dodavateli z Číny v anglickém jazyce.

Klára - zastává prodejní část. Přijímá faktury a vyřizuje objednávky od odběratelů. Zároveň zadává skladníkovi (Pavlovi), jaké zboží se musí vyskladnit a zabalit. Také vyřizuje dodávky produktů, kontroluje produkty a určuje, kam se budou odvážet.

Pavel - momentálně převážně skladník, zodpovídá za expedici a balení produktů. Vozí produkty ze skladu do provozovny, protože sklad je v jiné části města. Obstarává uskladňování a vyskladňování zásob. Zároveň začal obstarávat i servis a montáž. Do budoucna je úmyslem ředitele firmy, aby se Pavel více soustředil na tuto pozici a na pozici skladníka byl časem nahrazen.

Jirka - první obchodní zástupce. Nově přijatý zaměstnanec, zaměřující se převážně na maloobchodní prodejny. Pokrývá především severní a jižní Moravu a získává nové odběratele pro TESLUX z oblasti maloobchodů, jako jsou například elektra. Zároveň se stará o současné odběratele.

Libor - druhý obchodní zástupce. Také získává a navazuje nové obchodní vztahy, ale v oblasti velkoobchodů. Pokrývá oblast západně od Brna.

Třetí obchodní zástupce - uvažuje se o zaměstnání třetí obchodního zástupce, jenž by měl pokrýt oblast Čech.

5.5. Prodej a zákazníci

Hlavním zákazníkem firmy jsou velkoobchodní řetězce, mezi největší z nich patří BAUMAX ČR s.r.o.. Dále spolupráce s maloobchody jako jsou elektra. Na projekty se firma soustředit nechce, raději poskytuje zboží velkoobchodům, které tyto projekty zprostředkují sami. Krom toho vytváří návrhy projektů, které posílá dále svým velkoobchodním partnerům. V budoucnu firma uvažuje o otevření trhu v Číně. Nyní pokrývá celou oblast České republiky a úzce spolupracuje se slovenskou stranou.

5.6. Dodavatelé

Firma spolupracuje s pěti dodavateli z Číny, od nichž odebírá buď hotové produkty, nebo součástky, jenž následně v ČR montují. Také spolupracuje s univerzitním profesorem ze

Šanghaje, který se stará o velmi kvalitní výzkum a vývoj nových produktů. Zboží je sem dováženo v pravidelných intervalech pomocí lodní, případně letecké dopravy.

5.7.Konkurence

Na našem trhu se vyskytuje mnoho firem nabízejících osvětlení založené na LED technologii. Největším konkurentem v LED žárovkách je společnost EMOS s.r.o., jehož výhodou je větší sortiment zboží (nejenom žárovky a osvětlení) v oblasti elektrotechniky. Jedná se o mnohonásobně větší firmu. Přesto se firmě TESLUX daří úspěšně konkurovat. Dále se na trhu vyskytuje spousta zahraničních firem, zejména z Polska a z Německa.
Konkrétní obavy se vyskytují u důležitého obchodního partnera a to obchodního řetězce BAUMAX, který je již delší dobu ve stavu prodeje a pokud jej odkoupí polská společnost, bude mít zájem dosadit sem své zboží, místo zboží společnosti TESLUX.

5.8.Produkty

Firma nábruse přiklání spíše k orientaci na užší sortiment kvalitních výrobků než širší. Vedou ji k tomu hlavně problémy s uskladňováním mnoha rozdílných produktů. Základním produktem jsou LED žárovky, které nabízí asi v patnácti verzích, dále nabízí LED svítidla a panely a to přisazené nebo vestavné. Nabízí také LED reflektory a LED světelné moduly. Nejnovějšími produkty jsou LED veřejná osvětlení a LED průmyslová osvětlení. Do těchto produktů vkládá firma velké naděje a uvolnila dostatek prostředků na jejich vývoj. Všechny tyto produkty jsou vyrobené pomocí moderní LED technologie, založené na řízeném stmívání, jenž pomáhá šetřit náklady za osvětlení.

5.9.Externí firmy

Externí firmy pro společnost vypracovávají účetnictví a daně.

6. Průběh analýzy

Spolupráce probíhala převážně s majitelem firmy Pavlem Kozumplíkem, s nímž pravidelně probíhalo účelové interview. Na těchto schůzkách jsme získali veškeré potřebné podklady pro analýzu.

6.1.Stanovení kontextu (Určení hranice analýzy rizik)

Hlavním účelem této analýzy rizik je identifikovat, analyzovat a ošetřit rizika této společnosti. Zjistit díky tomuto postupu rizika, o kterých jsme netušili. Uvědomit si, která rizika jsou nejzávažnější a která méně závažná a stanovit si konkrétní plán ošetření nejkritičtějších rizik.

6.1.1. Základní kritéria

Dle majitele jsou nejdůležitějším faktorem firmy jeho klíčoví dodavatelé, konkrétně dva klíčoví dodavatelé z Číny, díky nimž je firma schopná nabízet jedinečné produkty oproti konkurenci.
V oblasti prodeje je nejdůležitější firma s jejíž pomocí dodává firma zboží do řetězce Baumax. Dalším důležitým odběratelem je slovenská firma realizující projekty, se kterou úzce spolupracují a tvořila loni obrat v hodnotě asi 6 milionů korun a letos se čeká až trojnásobek. Důležitými odběrateli jsou také velkoobchody, letos se například navázala spolupráce s řetězcem ELKO EP s.r.o.. Také se firma začíná zabývat maloobchody, protože je u nich možné nasadit větší marži a rozděluje se tím riziko.
Důležitými kritérii tedy bude, jak tyto dodavatele a odběratele může aktivum ovlivnit.

6.1.2. Rozsah a hranice

Rizika i aktiva budeme řešit v takovém rozsahu a od takové hranice, kdy nějakým způsobem dokážou ovlivnit základní cíle a chod firmy, vysvětlený v předchozích krocích. Toto ovlivnění může být buď přímé (ztráta odběratelů), nebo nepřímé (finanční újma).

6.1.3. Organizace řízení rizik bezpečnosti informací

Vzhledem k velikosti firmy a dostatečné znalosti a kompetenci majitele k veškeré činností firmy budou všechny odpovědnosti vůči řízení rizik přiděleny majiteli Pavlovi Kozumplíkovi. S případnými změnami a procesy budou obeznámeni zaměstnanci, kterých se tyto procesy týkají.

6.2. Identifikace rizik

6.2.1. Identifikace a ohodnocení aktiv

Identifikace a ohodnocení aktiv probíhalo s majitelem. Postupně jsme dle normy s majitelem probírali jednotlivé oblasti aktiv a diskutovali o aktivech, které vlastní. Současně jsme probírali i hrozby a zranitelnosti, které se k nim vztahují. Majitel si již před analýzou velmi dobře uvědomuje jednotlivé vazby a závislosti mezi aktivy. Následuje seznam aktiv a jejich ohodnocení v závorce, které je vysvětleno níže.

6.2.1.1. Primární aktiva

Identifikaci zajišťují představitelé hlavních procesů organizace. Jsou to obvykle hlavní procesy, informace o činnosti v rámci rozsahu a organizační procesy.
Dělíme je na:

3) *Obchodní (dílčí) procesy a činnosti:*
   - dva klíčoví dodavatelé (4 - 10),
   - ostatní dodavatelé (3 - 6),
   - klíčoví odběratelé (BAUMAX, Slovensko) (4 - 10),
   - klíčoví odběratelé - velkoobchody (ELKOV) (4 - 8),
   - klíčoví odběratelé - maloobchody (2 - 3),
   - kurz měny (dolar) (3 - 5),
   - certifikace výrobků (3 - 7),
   - cash flow (4 - 10),
   - zboží (4 - 10).

4) *Informace:*
   - know-how (4 - 8),
   - informace o cenách nákupu od dodavatelů (4 -8),
   - informace o cenách prodeje odběratelům (4 - 8),
   - soukromé informace o zaměstnancích (např. plat) (3 -5),
   - obrátkovost skladových zásob (druh a množství uskladňovaných zásob) (4 - 10),
   - informace o investici do vývoje nových produktů (3 - 6).

6.2.1.2. Podpůrná aktiva

Obsahují zranitelnosti, které zneužívají hrozby, aby poškodily primární aktiva v rámci rozsahu.

Typy:

7) Hardware:

- server (obsahuje účetní program, uchovává prodeje a nákupy) (4 - 8),
- počítače (2 - 2),
- notebook majitele (4 - 8),
- notebooky (3 - 5),
- smartphony (2 - 4),
- tiskárny (1 - 0),
- externí disk (k zálohování serveru) (4 - 8),
- flashdisky (2 - 3),
- důležité smlouvy, dokumenty (3 - 6),
- hmotný movitý majetek (vybavení budov, vozidla) (3 - 7).

8) *Software:*

- Money (4 - 8),
- operační systém (2 - 3),
- antivirový program Esset (3 -6),
- externí mailový server na síti (2 - 2),
- program na tvorbu návrhů projektů (2 - 2).

9) *Sítě*

- síť (přes šifrovanou wifi) (1 - 1),
- VPN přístup (3 - 5),
- externí firewall (3 - 6),
- telefonní datové přenosy (2 - 2),
- neomezené psaní a volání z telefonů (1 - 1).

10) Pracovníci

- Pavel - Kozumplík - majitel (5 - 15),
- Martin - stará se o marketingovou část firmy. Zařizuje reklamu firmy (4 - 8),
- Dáša - oblast prodeje i nákupu, ale soustřeďuje se nyní hlavně na administrativní činnost (4 - 8),
- David - návrhář společnosti (3 - 6),

- Vendula - řídí nákupní část firmy (3 - 6),
- Klára - zastává prodejní část (2 - 4),
- Pavel - momentálně převážně skladník, zodpovídá za expedici a balení produktů. (2 - 4),
- Jirka - první obchodní zástupce (3 - 5),
- Libor - druhý obchodní zástupce (4 - 8),
- Vývojář - externí vývoj ve spolupráci s vysokoškolským profesorem ze Šanghaje (3 - 7).

11) Lokalita

- oblast (Hodonín - okraj města) (1 - 1),
- hlavní budova (2 - 2),
- sklad (2 - 4),
- kanceláře (2 - 2),
- externí údržba (vodo-topo, malíři) (1 - 1),
- pevná linka (1 - 0),
- fax (1 - 0),
- bezdrátové internetové připojení (1 - 1),
- záložní zdroj (1 - 1),
- svoz odpadu (externí firma) (1 - 0),
- sběr nebezpečného odpadu (externí firma) (1 - 1).

12) Organizace

- organizační struktura firmy (2 - 4),
- externí bezpečností služba (1 - 1),
- projekční oddělení (projektant navrhující instalaci svítidel v rámci projektů) (3 - 5),
- místní příležitostní dodavatelé (2 - 2).

6.2.1.3. Ohodnocení aktiv

Po diskuzi s majitelem jsme se dohodli na kvalitativní metodě hodnocení. Vedla nás k tomu různorodost aktiv a nedostatečné podklady ke kvantitativnímu ohodnocení některých aktiv.
Proto jsme si museli zvolit škálu, dle které budeme hodnotit. Shodli jsme se na škále od jedné do pěti, jejíž hodnoty jsou zde přesně popsány.

- 1 - velmi nízké - Lehce nahraditelná aktiva, která lze bez problému nahradit do tří dnů. Firma na nich není nijak podstatně závislá.

- 2 - nízké - Aktivum způsobí problém, který lze vyřešit v rámci jednoho týdne a nijak zásadně neohrozí chod firmy.

- 3 - střední - Vzniká problém tato aktiva nahradit. Problém ovšem zásadně neochromí základní činnost společnosti. Aktiva bývají nahraditelná do čtrnácti dnů.

- 4 - vysoké - Velmi obtížně nahraditelné. Firmě nastanou závažné problémy, které je třeba vyřešit. Taková aktiva bývají nahraditelná v časovém úseku až jednoho měsíce a více.

- 5 - kritické - nenahraditelné aktivum. Takové, bez kterého v daném okamžiku firma není schopna vykonávat svou činnost.

Podle čeho ale zařazovat aktiva do jednotlivých skupin? Jak vytyčit hranice kam aktiva zasahují? K tomu nám pomohl seznam kritérií v příloze B.2 normy ČSN ISO/IEC 27005. Z něj jsme si vypsali a dle potřeby upravili patnáct základních kritérií, jenž jsou nejpodstatnější pro tuto firmu.

Kritéria:

- porušení legislativy,
- zhoršení výkonu firmy,
- poškození jména firmy,
- ohrožení osobní bezpečnosti,
- finanční ztráta,
- přerušení obchodní činnosti,
- ztráta důvěry zákazníků,
- narušení vnitřního provozu firmy,
- porušení zákonů, předpisů,
- ztráta zboží,
- ztráta zákazníků, dodavatelů,
- ztráta konkurenční výhody,
- oslabení schopnosti jednání,
- propouštění ze zaměstnání,
- materiální škoda.

Dle počtu splňujících kritérií jsme si zvolili následující *hranice hodnocení*:

- 1 - velmi nízké: 0 - 1 kritérií,
- 2 - nízké: 2 - 4 kritéria,
- 3 - střední: 5 - 7 kritérií,
- 4 - vysoké: 8 - 10 kritérií,
- 5 - kritické: 11 a více kritérií.

Postup si uvedeme na příkladu. První aktivum jsou dva klíčoví dodavatelé. Kdybychom o ně přišli, nastaly by následující situace: zhoršení výkonu firmy, finanční ztráta, přerušení obchodní činnosti, ztráta důvěry zákazníků, narušení vnitřního provozu firmy, ztráta zboží, ztráta zákazníků, dodavatelů, ztráta konkurenční výhody, oslabení schopnosti jednání, propouštění ze zaměstnání. Tím je splněno deset z patnácti kritérií a proto je aktivum ohodnoceno číslem 4 jako vysoké. Zároveň probíhá kontrola majitele, jestli získaný výsledek odpovídá jeho odhadu, kam by aktivum zařadil.
Tímto způsobem jsou hodnocena všechna aktiva a ke každému je doplněno číslo skupiny, do které patří a počet kritérií které splňuje. Tato čísla jsou uvedena v seznamu aktiv. Za každým aktivem se vyskytuje v závorce nejprve hodnocení, poté pomlčka a počet kritérií, které splňuje. Například sklad (2 - 4) má hodnocení dva, protože splňuje čtyři kritéria.

6.2.2. Identifikace hrozeb

Většinu hrozeb jsme vydedukovali již při identifikaci aktiv. Bylo snazší přemýšlet o hrozbách ve spojitosti s aktivy, nežli o hrozbách samotných. Zbylé hrozby se měly identifikovali dle příkladů typických hrozeb v příloze C normy ČSN ISO/IEC 27005. Vybrali jsme pouze ty hrozby, které jsou pro naši firmu reálné. Za každou hrozbou je v závorce její původ (A,D,E). Hrozby jsou rozděleny stejně jako v normě dle typu hrozby a jednotlivých hrozeb a podle zdroje hrozby a jejich důsledků. Přičemž zdroje a hrozby a jejich důsledky jsme vyjádřily tabulkou z normy ČSN ISO/IEC 27005, která zahrnuje vše podstatné.

I. Typ hrozby

1. *Fyzické poškození*
   - požár (A,D,E),
   - poškození vodou (A,D,E),
   - zničení zařízení nebo médií (A,D,E).

2. *Přírodní události*

- povodeň (E),
- zemětřesení (E),
- klimatický jev (E).

3. *Ztráta základních služeb*
   - selhání klimatizace nebo dodávky vody (A,D),
   - přerušení dodávky elektřiny (A,D,E),
   - selhání telekomunikačního zařízení (A,D),
   - výpadek internetového spojení (A,D),
   - porucha vytápění (A,D,E).

4. *Ohrožení informací*
   - odposlech (D),
   - krádež dokumentů (D),
   - krádež zařízení a médií (D),
   - zprovoznění recyklovaných nebo vyřazených médií (D),
   - vyzrazení (A,D):
     - vyzrazení know-how,
     - vyzrazení informací o cenách nákupu od dodavatelů,
     - vyzrazení informací o cenách prodeje odběratelům,
     - vyzrazení soukromých informací o zaměstnancích,
     - vyzrazení informací o obrátkovosti skladových zásob,
     - vyzrazení informací o investici do vývoje nových produktů,
   - data pocházející z nedůvěryhodných zdrojů (A,D),
   - falšování pomocí technického vybavení (D),

5. *Technická selhání*
   - selhání zařízení (A),
   - chybné fungování zařízení (A),
   - přetížení informačního systému (A,D),
   - chybné fungování aplikačního programového vybavení (A),
   - chyba údržby (A,D).

6. *Neoprávněné činnosti*
   - neoprávněné použití zařízení (D),
   - podvodné kopírování aplikačního programového vybavení (D),

- poškození dat (D),
- poškození serveru (D),
- nezákonné zpracování dat (D),
- zavirování systému (A,D),
- napadení mailového serveru (D),
- prolomení firewallu (D),
- zneužití internetového bankovnictví (D).

7. *Ohrožení funkčnosti*
   - chyba v používání (A),
   - špatné rozhodnutí (A,D),
   - odepření činností (D),
   - nečinnost zaměstnanců (například počítání množství potřebných zásob) (A,D),
   - nedostatek personálu, ztráta zaměstnanců (A,D,E),
   - nemožnost vykonávání činnosti majitele (A,D,E),
   - rozpad, nefunkčnost organizační struktury (A,D),
   - nefunkčnost projekčního oddělení (A,D,E).

8. *Ostatní (odvozené z identifikovaných aktiv)*
   - ztráta klíčových dodavatelů (A,D,E),
   - ztráta místních příležitostných dodavatelů (A,D,E),
   - ztráta klíčových odběratelů (BAUMAX, Slovensko) (A,D,E),
   - ztráta klíčových odběratelů - velkoobchody (ELKO EP) (A,D,E),
   - ztráta klíčových odběratelů - maloobchody (A,D,E),
   - zneužití chybějící ochranné známky (D),
   - výkyv kurzu dolaru (A,D),
   - udání nedostatečné kvality výrobku (D),
   - nefunkčnost softwaru Money (A),
   - nefunkčnost antiviru Esset (A),
   - ukončení spolupráce s vývojářem (A,D,E),
   - změna oblasti sídla firmy (A,D,E),
   - ztráta hlavní budovy (A,D,E),
   - ztráta skladu (A,D,E),
   - nárůst oblastních cen (A,D),

- pokuty, penále (A,D),
- nevymahatelnost pohledávek (nezaplacené faktury) (A,D).

II. Zdroj hrozby

Tabulka zachycuje základní zdroje hrozeb, jejich motivaci a důsledky.

Zdroj hrozby	Motivace	Možné důsledky
Hacker, cracker	Výzva Ego Rebelie Prestiž Peníze	• Hacking • Sociální inženýrství • Narušení a prolomení systému • Neoprávněný přístup do systému
Počítačová kriminalita	Zničení informací Nezákonné prozrazení informací Finanční prospěch Neoprávněné vyzrazení dat	• Počítačový zločin (např. kybernetické pronásledování) • Podvodné jednání (např. odpovídání, imitace, zachycení) • Získání informace za úplatu • Spoofing • Průnik do systému
Terorismus	Vydírání Zničení Vykořisťování Odplata Politický prospěch Zviditelnění v médiích	• Bombové útoky/Terorismus • Informační válka • Útok na systém (např. útok odmítnutí služby, DoS) • Průnik do systému • Porušení systému
Průmyslová špionáž (zpravodajské služby, společnosti, zahraniční vlády, ostatní vládní zájmy)	Konkurenční výhoda Ekonomická špionáž	• Vojenské zvýhodnění • Politické zvýhodnění • Ekonomické zneužití • Krádež informací • Průnik do soukromí • Sociální inženýrství • Průnik do systému • Neoprávněný přístup do systému (přístup ke klasifikovaným aktivum a technologickým informacím
Interní pracovníci (špatně zaškolení, nespokojení, škodolibí, nedbalí, nečestní nebo zaměstnanci s ukončeným pracovním poměrem)	Zvědavost Ego Vyzvědačství Finanční prospěch Odplata Neúmyslné chyby a opomenutí (např. chybné vložení dat, chyba při programování)	• Napadení zaměstnance • Vydírání • Prohlížení chráněných informací • Zneužití počítačů • Podvod a krádež • Získání informace za úplatu • Vložení falešných nebo upravených dat • Narušení komunikace • Škodlivý kód (např. virus, logická bomba, trojský kůň) • Prodej osobních údajů • Chyby systému • Průnik do systému • Sabotáž systému • Neoprávněný přístup do systému

Tabulka 6.2.2: Seznam hrozeb dle typu hrozby

6.2.3. Identifikace stávajících opatření

Při identifikaci jsme se zaměřili na cíle, opatření a jednotlivá opatření shrnutá v příloze A normy ČSN ISO/IEC 27001. Mnohem více nám ovšem pomohlo, uvědomit si stávající opatření, již při identifikaci aktiv. U každého zvažovaného aktiva jsme se zároveň snažili určit, jak je zabezpečeno.
V - vyhovuje
Z - potřeba zlepšit
N - nevyhovuje

- snaha o stálé dodavatele, vyhnutí se nebezpečí nekvalitních výrobků (V,Z),
- kontrola kvality zboží (Z),
- získávání maloobchodních zákazníků, rozdělení rizika ztráty odběratelů (Z),
- omezení informování zaměstnanců o klíčových informacích (know-how, ceny) na nezbytnou úroveň (V),
- nezveřejňování soukromých informací o zaměstnancích pokud to není nezbytné (V),
- ověřování přístupu zvenku i zevnitř (V,Z),
- antivir (V),
- firewall (V),
- omezení přístupu uživatelů jen k potřebným datům (V,Z),
- data nejsou uložena v přenosných zařízeních, ale na serveru (V),
- šifrované spojení (V),
- záloha dat ze smartphonů na google účtech (V),
- zálohy na serveru (V),
- externí zálohy serveru (na externí disk mimo prostor serveru) (V,Z),
- zabezpečovací, výjezdová služba (V),
- aktualizace a kontrola softwaru Money (V),
- aktualizace operačních systémů (V,Z),
- záloha mailového serveru (V),
- externí zálohy (V),
- server chráněn proti výpadku elektřiny záložní energií (V),
- pojištění rizik firmy na majetek a proti poškození vlastním zařízením (V),
- externí zálohy notebooků (včetně majitele) (N),
- informovanost zaměstnanců o obecných potencionálních hrozbách (Z,N),
- jazykové vzdělávání zaměstnanců (V,Z),
- ostatní vzdělávání zaměstnanců (N,Z),
- hasiči (V)
- zabezpečovací, výjezdová služba (V),

- řízení a kontrola lidských zdrojů (Z),
- nastavování pravidel a kompetencí (V,Z),
- dostatečné podklady k rozhodnutí (Z),
- kontrola kvality zboží (V,Z),
- loajalita (V),
- dodržování certifikací (V),
- prověřování odběratelů (V,Z),
- snaha o dostatek finančních prostředků (Z),
- snaha vybudovat vlastní nemovitosti (Z),
- budování vztahů (V,Z),
- zajištění externí IT firmou (V).

6.2.4. Identifikace zranitelností

Zde bylo opět prvním krokem určení zranitelnosti již při identifikaci aktiv. Druhým krokem bylo postupovat dle příkladů zranitelností z přílohy D normy ČSN ISO/IEC 27005. Z této normy byly vypsány zranitelnosti vyskytující se nebo hrozící v dané firmě a rozděleny dle daných skupin.

1. *Hardware*
   - nekontrolované kopírování,
   - nezabezpečené smartphony,
   - nedostatečná údržba,
   - zastaralé nevyhovující zařízení.

2. *Software*
   - nedostatečná aktualizace softwarového vybavení.

3. *Sítě*
   - nechráněné komunikační linky,
   - nedostatečné ověřování posílání a přijímání zpráv,
   - automatické programy snažící se nabourat do systému,
   - nedostatek pokrytí,
   - nestabilní připojení k internetu,
   - přístup více uživatelů,
   - špatná identifikace podvodných emailů.

4. *Zaměstnanci*
   - veškerá činnost firmy závisí na majiteli,

- loajalita,
- nedostatečné proškolení,
- nedbalost zaměstnanců,
- problematické nahrazení,
- sdílení soukromých informací o zaměstnancích.

5. *Lokality*
   - nepřiměřená nebo nedbalá kontrola fyzického přístupu do budov, místností a kanceláří,
   - veškeré nemovitosti jsou v pronájmu,
   - hlavní vchod při odemčení je volně přístupný,
   - chybí záložní zdroj energie pro případ výpadku elektrického proudu,
   - závada na klimatizaci nebo na topení,
   - výkyvy trhu,
   - špatný technický stav nemovitosti.

6. *Organizace*
   - nedostatečné popisy jednotlivých funkcí a činností.

7. *ostatní*
   - ochranná známka pouze pro ČR,
   - velká část odběru závisí na několika klíčových odběratelích,
   - jedinečnost produktů závisí převážně na dvou dodavatelích,
   - pohyblivost kurzu,
   - riziko udání kontrole kvůli konkurenci,
   - sdílení informací o cenách nákupu od dodavatelů,
   - sdílení informací o cenách prodeje odběratelům,
   - sdílení know-how,
   - sdílení informací o obrátkovosti zásob,
   - sdílení informací o investici do vývoje nových produktů,
   - špatné plánování a informace,
   - špatný výběr dodavatele,
   - špatná kvalita nebo nákupní cena,
   - vzdálenost dodavatele,
   - náchylnost udání kontrole kvůli konkurenci,
   - použití špatných součástek.

6.2.5. Identifikace následků

Jako nejjednodušší cesta byla zvolena zprvu identifikace následků pomocí základních skupin hrozeb. U každé skupiny byly prokonzultovány pravděpodobné scénáře. Vytiskly jsme si seznamy aktiv, hrozeb a zranitelností. Poté jsme si je zobrazili vedle sebe a přiřazovali jsme hrozby k aktivům a zranitelnostem. Následují obecné následky, dle základních skupin hrozeb.

- Zneužití, ohrožení informací například kvůli nedostatečné loajalitě vůči firmě, nekontrolovanému kopírování, špatným aktualizacím softwaru, či úniku informací z firmy, může mít za následek ztrátu odběratelů, dodavatelů, zhoršení pověsti firmy, ztráta pozice na trhu, prozrazení know-how nebo zvýhodnění konkurence.

- Nedostatečně proškolení zaměstnanci můžou způsobit zničení zařízení hardwaru (server, počítače), softwaru (Money), sítě či lokality (budova). Může také vzniknout požár nebo únik vody a to vše má za následek ohrožení chodu firmy nebo neschopnost dodávat zboží, což vede ke ztrátě odběratelů a zhoršení pověsti.

- Přírodní události dokážou poškodit nejen vybavení firmy, ale hlavně i skladové zásoby, což opět vede k neschopnosti dodávat zboží zákazníkům. Vzniká také majetková škoda, která při absenci kvalitního pojištění může způsobit závažné finanční problémy.

- Přerušení dodávky elektřiny může kvůli absenci generátorů elektřiny ochromit na určitou dobu firmu.

- Chyba údržby technického vybavení, selhání zařízení, přetížení informačního systému nebo chybné fungování může kvůli nedostatečné aktualizaci způsobit, že zaměstnanci nebudou schopni konat svou činnost, čímž opět dojde paralyzování firmy, což může vést ke ztrátě zákazníků.

- Nedostatečná loajalita, či proškolení zaměstnanců může vést ke zneužití dat, což má za následek propuštění zaměstnance, kvůli jeho pochybení. To opět postihne chod firmy, kvůli absenci zaměstnanců.

- Nedostatečnou organizací práce nebo špatným popisem práce může dojít ke špatným rozhodnutím, neefektivním činnostem zaměstnanců což může ohrozit chod firmy, vztahy mezi zaměstnanci a může vést ke ztrátě zaměstnanců.

- Špatné rozdělení práce, špatná evidence, špatný odhad evidence zásob může vést k finanční újmě.

Poté jsme měli zhruba ucelenou představu o následcích a nastala druhá fáze a to sepsání seznamu scénáře možných incidentů. Vycházeli jsme z jednotlivých hrozeb. První sloupec označoval skupinu hrozeb. Druhý sloupec obsahoval jednotlivé hrozby, přičemž každé aktivum související s jednou hrozbou tvořilo jeden řádek a proto se každá hrozba vyskytla v tabulce tolikrát, kolik aktiv ohrožovala. Třetí sloupec představoval zranitelnost vůči této hrozbě. Čtvrtý sloupec aktivum, se kterým hrozba souvisela, přičemž se často stávalo, že hrozba ohrožovala celou skupinu aktiv. Například požár mohl ohrozit veškerý hardware společnosti a počet řádků by tak markantně vzrostl. Proto jsme v těchto případech na místo aktiva vložili celou skupinu aktiv, kterou hrozba ohrožovala. V pořadí pátý sloupec obsahoval stávající opatření vůči hrozbě vztahující se na dané aktivum. Ze všech těchto sloupců jsme poté vyvodili poslední sloupec následek.
Jako příklad scénáře incidentu uvedu hrozbu selhání klimatizace nebo dodávky vody na aktivum zaměstnance. Zranitelností zde je možná závada na klimatizaci. Stávajícím opatřením je informovanost zaměstnanců o obecných potencionálních hrozbách, jak se v takových situacích chovat. A následkem tohoto incidentů je dehydratace, vyčerpání zaměstnanců. V extrémních případech může být druhotným následkem i neschopnost zaměstnanců vykonávat svoji činnost nebo zdravotní problémy.
Celá tabulka je uvedena v příloze A této bakalářské práce.

6.3. Analýza rizik

V této části, která je nejrozsáhlejší a zároveň nejdůležitější nás zpočátku čekalo důležité rozhodnutí, jakou metodu si k určení míry a posouzení rizik vybereme. Již v této fázi jsme si byli jisti, že se vydáme cestou detailního posouzení rizik bezpečnosti informací, tak jak jsme postupovali doposud. Přehledové posouzení by v tomto případě bylo silně nedostačující a hrozilo by opomenutí některých klíčových rizik, která je třeba ošetřit.
Další volba nás čekala mezi jednotlivými metodami detailního posouzení, kdy jsme vycházeli opět z normy ČSN ISO/IEC 27005 a knihy Řízení rizik ve firmách a jiných organizacích. Mohli jsme volit mezi čtyřmi metodami. Poté jsme vyřazovací metodou zhodnotili, že poslední metoda stanovení hodnoty pravděpodobnosti a možných následků rizik pro nás není vůbec vhodná. Důvodem bylo, že rizika posuzuje v rámci celých systému a ne jednotlivých aktiv, což by v naší firmě bylo neefektivní. Metoda třídění hrozeb pomocí míry rizika pro změnu nehodnotí celková rizika vycházející ze scénářů incidentů, ale jednotlivé hrozby, což nám také nevyhovovalo. U první tabulky matice s předem definovanými hodnotami, bychom museli volit úroveň hrozby a

zranitelnosti, což by mohlo v našem případě být zavádějící. Autoři knihy doporučovali pouze jednu metodu a to druhou tabulku u matice s předem definovanými hodnotami v normě a i my jsme se nakonec shodli na této metodě.U tohoto typu bylo třeba posoudit následky, neboli dopad a určit pravděpodobnost incidentů. Tyto hodnoty jsme poté vložili do matice, kde nám vyšla výsledná hodnota úrovně rizik.

Detailní postup byl následující. Nejprve jsme si museli zvolit škálu hodnocení dopadu a pravděpodobnosti. Tu jsme ponechali stejnou, jako v ukázkové matici a to o pěti hodnotách:

- Velmi nízká - 0,
- Nízká - 1,
- Střední - 2,
- Vysoká - 3,
- Velmi vysoká - 4.

Tato škála je rovněž shodná se škálou u hodnocení aktiv, což nám práci usnadnilo. Jelikož dopad byl na aktivum, kterého se scénář incidentu týkal, vycházelo určení dopadu z velké části z hodnoty tohoto aktiva. I tak avšak nebyla hodnota vždy stejná, různé hrozby totiž můžou aktivum poškodit různým způsobem, přináší to rozdílné následky a tuto skutečnost jsme vždy museli bedlivě posoudit.

Při určení pravděpodobnosti jsme se snažili upřesnit si každou hodnotu škály. K tomu nám pomohlo zvolit si časové rozmezí, v jakém je pravděpodobné, že se scénář uskuteční. Časové úseky sice vždy zcela neodpovídaly realitě, ale výrazně nám pomohly objektivně určit tuto pravděpodobnost.

- Velmi nízká - 5 let a více,
- Nízká - 1 rok,
- Střední - měsíc,
- Vysoká - týden,
- Velmi vysoká - 0 až 3 dny.

Když jsme měli určenou pravděpodobnost i dopad scénářů incidentů, pustili jsme se do samotného určování úrovně rizik. U každého scénáře opět tento proces probíhal samostatně. A to zanesením těchto dvou hodnot do vybrané matice s předem definovanými hodnotami. V této matici vybereme nejdříve první až pátý řádek, podle závažnosti dopadu (velmi nízká, nízká, střední, vysoká, velmi vysoká). Poté vybereme první až pátý sloupec, tentokrát dle pravděpodobnosti scénáře incidentu (velmi nízká, nízká, střední, vysoká, velmi vysoká). V místě

matice, kde se tyto hodnoty střetnou nakonec získáme výslednou hodnota, která udává úroveň neboli míru rizika.

V této matici úroveň rizika nabývá hodnot 0 až 8 a je rozdělena do tří skupin dle závažnosti. Tyto skupiny jsme ponechali.

- 0 - 2,
- 3 -5,
- 6 -8.

Postup si uvedeme opět na příkladu. Jako scénář incidentu zvolíme hrozbu nevymahatelnost pohledávek (nezaplacené faktury), ohrožující aktivum cash flow. Zranitelností je zde špatný výběr odběratele, ošetřením prověřování odběratele a následkem finanční újma. Dopad jsme si zhodnotili jako velmi vysoký, tudíž v tabulce číslem čtyři a pravděpodobnost jako vysokou, tudíž v tabulce číslem 3. Při zanesení do matice tedy zvolíme poslední pátý řádek, kvůli velmi vysokému dopadu a čtvrtý sloupec, kvůli vysoké pravděpodobnosti. Tím se dostaneme k buňce s hodnotou 7, což je výsledná úroveň rizika. Pro lepší znázornění si to představíme na obrázku.

	Pravděpodobnost scénáře incidentu	Velmi nízká	Nízká	Střední	Vysoká	Velmi vysoká
Dopad	Velmi nízká	0	1	2	3	4
	Nízká	1	2	3	4	5
	Střední	2	3	4	5	6
	Vysoká	3	4	5	6	7
	Velmi vysoká	4	5	6	7	8

Tabulka 6.3: Postup určení úrovně rizik

Seznam všech scénářů možných incidentů s určenou úrovní rizika se nachází v příloze B. U scénářů incidentů, kde hrozba neohrožuje jedno aktivum, ale celou skupinu (hardware, informace), se v kolonkách hodnocení dopadu, pravděpodobnosti i rizik vyskytuje více hodnot. Tyto hodnoty patří jednotlivým aktivům z dané skupiny, tak jak jsou seřazeny zde v seznamu aktiv.

6.4. Hodnocení rizik

V této fázi již nemluvíme o scénářích možných incidentů jako takových, ale o rizicích s určenou úrovní. Tato rizika nyní musíme seřadit a zhodnotit. Nejprve tedy seřadíme rizika dle hodnoty úrovně rizika. Poté si tato rizika rozdělíme do skupin. K tomu nám pomůže rozdělení v matici

při určování úrovně rizik. Zde byly hodnoty rozděleny do tří skupin, přičemž hodnoty od 6 do 8 patřili do skupiny nejvyšší. S přihlédnutím na hranice akceptace rizik a kritéria, tuto skupinu budeme i my považovat za hraniční a jednotlivá rizika v ní budeme považovat za kritická a nutné k ošetření. Tato rizika jsou vyznačena červeně v příloze B.

6.5. Akceptace a ošetření rizik bezpečnosti informací

Dostáváme se tedy k závěru, jehož výstupem je seznam nejzávažnějších rizik. Tato rizika byla opět důkladně probrána s majitelem firmy a bylo navrhnuto řešení ke snížení těchto rizik na akceptovatelnou úroveň. Bylo vybráno jedno ze čtyř řešení, modifikace, podstoupení, vyhnutí se nebo sdílení rizika. Následuje seznam těchto rizik a způsob jejich řešení.

a) Selhání zařízení, například kvůli použití špatných komponent, poškodí zboží, což může mít za následek vadné zboží a následně ztrátu odběratelů a finanční újmu. Stávajícím opatřením je kontrola kvality zboží. Firma by se měla snažit co nejvíce kontrolovat příchozí zboží od dodavatele a nekvalitní zboží hlásit a posílat zpět. Nejdůležitější je ale kontrola zboží na vstupu ve výrobě, což je starost dodavatelů. Proto se toto riziko dá částečně modifikovat zvýšením kontroly příchozího zboží, ale riziko se také musí sdílet s dodavateli.
b) Poškození dat, serveru, nezákonné zpracování dat nebo zavirování systému například vlivem automatických programů snažících se nabourat do systému, špatnou identifikací podvodných emailů, nezabezpečenými smartphony apod., může poškodit ať už informace (know-how, informace o cenách nákupu od dodavatelů, informace o cenách prodeje odběratelům, obrátkovost skladových zásob, informace o investici do vývoje nových produktů), software (Money, operační systém, antivirový program Esset, externí mailový server na síti) nebo hardware (server, notebook majitele, notebooky, externí disk). Stávající opatřeními jsou firewall, antivir, ověřování přístupu zevnitř i zvenku, data nejsou uložena v přenosných zařízeních, ale na serveru, záloha dat ze smartphonů na google účtech, zálohy na serveru, záloha mailového serveru, externí zálohy, školení zaměstnanců. Následkem může být ztráta nebo znehodnocení informací, nefunkčnost softwaru nebo hardwaru. Řešením zde může být kombinace podstoupení a sdílení rizika. Současné opatření jsou v maximální výši a není možné ovlivnit chybu lidského faktoru, například při otevření škodlivého emailu. Riziko se sdílí s externí IT firmou, která má tyto hrozby na starost.
c) Prolomení firewallu opět například vlivem automatických programů snažících se nabourat do systému může poškodit informace jako know-how, informace o cenách nákupu od dodavatelů, informace o cenách prodeje odběratelům, obrátkovost skladových zásob, informace o investici do vývoje nových produktů. Stávajícím opatřením je funkční firewall. Následkem je napadení sítě a znehodnocení nebo únik těchto informací. Jediným řešením je

toto riziko podstoupit, neboť firewall je využit v nejvyšší možné míře. Tím že je hardwarový a ne softwarový poskytuje nadstandardní míru ochrany.

d) Zneužití internetového bankovnictví může nastat kvůli špatné identifikaci podvodných emailů, nebo nezabezpečeným smartphonům, či krádeži a může to přinést značné problémy s cash flow. Zde byla navržena modifikace rizika, nastavením přístupu přes čipovou kartu. Tím se zvýší zabezpečení a zbytkové riziko je akceptovatelné.

e) Špatné rozhodnutí, kvůli nedostatečnému proškolení zaměstnanců, nebo třeba špatnému plánování může způsobit ztrátu odběratelů. Nyní se firma snaží tomuto zamezit nastavením přesných pravidel a kompetencí. Do budoucna se firma bude snažit modifikovat toto riziko větším proškolováním zaměstnanců a ještě lepším vytyčováním pravidel a kompetencí.

f) Špatné rozhodnutí, kvůli špatnému plánování nebo informacím může poškodit také cash flow a způsobit finanční újmu. Zde řešení závisí pouze na majiteli. Špatné rozhodnutí vznikají hlavně kvůli nezbytným dlouhodobým objednávkám zboží. Majitel se snaží získávat dostatek podkladů pro správné rozhodnutí. Tyto informace mu poskytují především jeho obchodní zástupci a je si vědom toho, že toto informování se musí zlepšit. Další plánovanou modifikací je držení větší finanční rezervy. Toho se docílí sjednáním revolvingového úvěru v bance. Dále se bude firma snažit získávat dostatečné zálohy při objednávkách zboží, čímž lépe kontroluje cash flow. Všechny tyto modifikace by měly vést ke snížení rizika na akceptovatelnou úroveň.

g) Špatné rozhodnutí majitele, kvůli špatnému plánování nebo informacím může přinést finanční újmu také v souvislosti se změnou kurzu měny. Nejefektivnějším řešením je mít dostatečné množství finančních prostředků, aby bylo i v případě nepříznivé změny kurzu možné splatit své závazky. Toto riziko závažně postihlo firmu v minulosti, a proto si na něj firma bude dávat velký pozor a bude se snažit disponovat dostatkem finančních prostředků. Další zvažovanou možností je sdílení rizika pomocí uzavření forwardového kontraktu.

h) Nečinnost zaměstnanců, ať už kvůli jejich nedbalosti nebo nedostatečnému popisu jejich funkcí může způsobit finanční újmu a tím poškodit cash flow. Firma se tomu snaží zabránit řízením a kontrolou lidských zdrojů a všeobecným vzděláváním. Řešením je modifikace zvýšením kontroly činnosti zaměstnanců. Toho je v plánu docílit přenesením kompetencí z majitele, který nemá na tuto činnost dostatek času, na zaměstnance Martina, který již nyní dohlíží na obchodní zástupce. Touto změnou se zlepší kontrola zaměstnanců a poskytne to majiteli více času na zásadní rozhodování.

i) Ztráta klíčových odběratelů (BAUMAX, Slovensko) a velkoobchodů, může způsobit velké problémy kvůli tomu, že velká část odběru závisí na těchto několika klíčových odběratelích. Doposud se tomu firma snažila bránit získáváním odběratelů, v poslední době nově i maloobchodních, čímž toto riziko rozdělí. Navrženo je lepší vzdělávání obchodních zástupců, zlepšování jejich schopností a vyvíjení tlaku na to, aby získávali nové odběratele.

Problémem je, že se spíše starají o současné zákazníky, než získávají nové. Proto jsou zavedeny reporty, které by měli tuto situaci do budoucna zlepšit.

j) Zneužití chybějící ochranné známky může poškodit know-how firmy a tím zvýhodnit konkurenci a způsobit ztrátu trhu. Ochranná známka je zavedena pouze pro Českou republiku. Zde je tedy jednoznačné řešení modifikace rizika. Náklady na rozšíření jsou zde mnohonásobně nižší než případné ztráty. Ochranná známka proto bude v co nejbližší době rozšířena i na ostatní země.

k) Udání nedostatečné kvality výrobku může vést ke ztrátě dodavatelů. Toto riziko je závažné hlavně kvůli vzdálenosti dodavatelů (Čína). Současná opatření jsou snaha o stálé dodavatele a kontrola kvality výrobků. Také je nutné mít v pořádku všechny potřebné certifikace a tím dávat co nejmenší šanci k takovému udání. Majitel považuje současné dodavatele za dostatečně kvalitní a věrohodné. Spolupracuje nově pouze s jedním menším dodavatelem, u nějž tuto jistotu nemá. Proto je v plánu modifikace v podobě změny tohoto dodavatele za věrohodnějšího.

l) Velmi závažným rizikem je ukončení spolupráce s vývojářem, neboť tento vysokoškolský profesor ze Šanghaje je velmi těžce nahraditelný. Může to způsobit neschopnost vytvářet nové produkty a zastavení výzkumu a mít dopad na know-how. Proto se firma snaží budovat dobré vztahy a být k tomuto vývojáři loajální. Majitel uvažuje o závažnějším smluvním spojení, které lépe zajistí spolupráci do budoucna. Hledají se i další cesty a noví případní vývojáři. V tomto okamžiku byla, vzhledem k tomuto vysokému riziku zahájena jednání s jinou společností.

m) Nárůst oblastních cen, kvůli výkyvům trhu může způsobit finanční újmu a tím poškodit cash flow. Toto rizika se bohužel nedá nijak ovlivnit, jedinou snahou majitele je mít dostatek podkladů ke správnému rozhodnutí. Toto riziko ale z trhu nikdy nezmizí a týká se všech. Proto bylo rozhodnuto, že bude toto riziko podstoupeno.

n) Nevymahatelnost pohledávek, kvůli špatnému výběru dodavatele může způsobit také finanční újmu a tím poškodit cash flow. Firma se brání prověřováním odběratelů. Toto závisí opět na obchodních zástupcích. Je potřeba, aby se toto prověřování zlepšilo, a firma na to kladla důraz. Například je nutné hlídat si zálohy a mít v pořádku veškeré objednávky. Toto riziko je také sdíleno s právní firmou, která se o tyto problémy stará.

o) Posledním závažným rizikem, které sice nespadá dle hodnocení do kritické oblasti je riziko trvalé nemožnosti vykonávání činnosti majitele. Toto riziko má sice nízkou pravděpodobnost, ale dopad největší ze všech rizik. Důvodem je, že veškerá podstatná činnost firmy doposud závisí pouze na majiteli. Majitel je současně jediným jednatelem společnosti a v případě úmrtí by ho neměl kdo nahradit. Jednou možností je nechat do firmy vstoupit dalšího člověka, nebo firmu transformovat na akciovou společnost. První možnost sebou nese příliš nových rizik a druhá možnost se zatím finančně nevyplatí. Do úvahy sice

připadá jeden kandidát na možného spolumajitele, nicméně prozatím majitel firmy raději podstoupí toto riziko.

7. Závěr

7.1. Shrnutí a dosažení cílů práce

Práce se dělí na praktickou a teoretickou část. V teoretické části bylo nejprve vysvětleno, co to vlastně analýza rizik je a jaké jsou její základní termíny. Dále je uveden základní obsah souvisejících norem. V další části se věnuji podrobnému teoretickému popisu celého průběhu oblasti řízení rizik, která je realizována v praktické části.

Následuje praktická část, která začíná základním představením firmy, její historie, organizační struktury, cílů a vizí firmy atd.. Poté je podrobně popsaný průběh realizace celého procesu, začínající identifikací rizik, poté analýzou rizik a na závěr akceptací a ošetřením rizik bezpečnosti informací.

Cílem práce bylo seznámit se v teoretické části s problematikou bezpečnosti aktiv společnosti. Tento cíl byl splněn a byla osvojena znalost metodologie identifikace, analýzy a ošetření rizik. Také byly osvojeny znalosti celkové oblasti bezpečnosti aktiv a terminologie. Cíl byl dosažen i v praktické části, kde byla tato metodologie realizována. S majitelem firmy probíhala bezproblémová spolupráce a byly úspěšně dokončeny všechny potřebné kroky. Bylo dosaženo plánovaných výsledků a byly zjištěny nejzávažnější rizika společnosti. Úspěšně byla identifikována veškerá potřebné aktiva, hrozby, zranitelnosti, stávající opatření i následky. Poté byla tato data ohodnocena a analyzována dle vhodné metody. Na závěr byla dle plánu v kooperaci s majitelem firmy prodiskutována a naplánována bezpečností opatření k ošetření těchto rizik.

Všechny cíle byly tedy úspěšně dosaženy a firma je do budoucna lépe zabezpečena.

7.2. Závěrečné slovo majitele

Původně měl majitel obavy ze zveřejnění příliš velkého množství informací. Po několika úvodních konzultacích se však tyto obavy rozptýlily. Díky tomu, že majitel má na starosti stále veškerou hlavní činnost firmy, měl již před začátkem analýzy velmi dobrý přehled o stavu a rizicích této firmy. I když si tedy většinu rizik již před analýzou uvědomoval, největším přínosem pro něj bylo, uvědomit si jejich dopad. Dále pro něj byla cenná možnost prodiskutovat všechna rizika s nezaujatým, ale informovaným externistou, rizika systematicky ohodnotit a získat tím přehled o tom, která rizika je nutné neodkladně řešit.

Sám majitel Pavel Kozumplík uvedl:

"Díky analýze jsem si v hlavě více urovnal, co je pro firmu opravdu důležité a na co bych se měl zaměřit. A ne jen o problémech tušit a odkládat je kvůli nedostatku času."

Po analýze má proto v plánu tato rizika co nejdříve ošetřit.

7.3.Závěrečné slovo autora

Tahle práce mě mnohému naučila. Pohled do problematiky bezpečnosti a analýzy rizik je velmi komplexní. Jeho aplikace byla realizovatelná v daném časovém horizontu, hlavně díky výborné spolupráci s majitelem. Důležitým faktorem bylo, že firma není přespříliš rozsáhlá a všechny důležité podklady, bylo možné získat od jednoho člověka, majitele firmy. U větších firem, by bylo nezbytně nutné využít podporujících softwarů, více lidí a větší množství času.

Jsem pevně přesvědčen, že proces analýzy a řízení rizik je ve firmách velmi důležitým krokem. Vhodný je zejména pro začínající a rozsáhlé firmy, kde rizika nejsou zcela zřejmá, ale důležitý je v jakékoliv firmě či organizaci. Vždyť co je pro firmu důležitější, než zabezpečit její rizika a zajistit tím svou existenci do budoucna?

Prostor pro navázání, se zde nachází v dlouhodobém monitorování zde dosažených výsledků, realizování plánovaných ošetření a udržování celkového povědomí o rizicích firmy. Touto bakalářskou prací proces řízení rizik tedy rozhodně nekončí.

8. Seznam použité literatury

[1] PEARCE, D. W.. *Macmillanův slovník moderní ekonomie*. Victoria Publishing, Praha 1995, s. 361, ISBN 80-85605-42-2

[2] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 9788024746449.

[3] *ČSN ISO/IEC 27000 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010, 23 s.

[4] *ČSN ISO/IEC 27001 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Český normalizační institut, 2006, 35 s.

[5] *ČSN ISO/IEC 27002 (36 9790) Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 76 s.

[6] *ČSN ISO/IEC 27003 (36 9790) Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací*. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011, 59 s. Česká technická norma.

[7] *ČSN ISO/IEC 27004 (36 9790) Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření*. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011, 59 s. Česká technická norma.

[8] *ČSN ISO/IEC 27005 (36 9790) Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013, 63 s. Česká technická norma.

[9] *Slovník ekonomických pojmů* [online]. [cit. 2015-17-4]. Datum zveřejnění neznámý. Dostupný z World Wide Web: http://www.zalozit-firmu.cz/slovnik-ekonomickych-pojmu/

9. Seznam obrázků a tabulek

10. Přílohy

Příloha A: Seznam scénářů incidentů a jejich následků (Tabulka)

Příloha B: Seznam rizik s určenou úrovní (Tabulka)