Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Katedra systémové analýzy

Studijní program: Aplikovaná informatika
Obor: Informatika

Název bakalářské práce:

Bezpečnost a analýza rizik v praxi

Vypracoval: Filip Calta
Vedoucí práce: Ing. Ladislav Luc
Rok vypracování: 2016

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 Praze dne …….

Filip Calta

Poděkování:

Tímto bych rád poděkoval svému vedoucímu bakalářské práce Ing. Ladislavu Lucovi za odborné vedení a dohled při zpracování této studie.

Velmi děkuji společnosti Disk Mlutimedia, s.r.o., především finanční ředitelce Ing. Evě Braunšlegerové a Liboru Dvořáčkovi, kteří mi umožnili tuto studii zpracovat.

A v neposlední řadě své přítelkyni, která mi byla podporou a motivovala mě v průběhu dokončování mé bakalářské práce.

Název bakalářské práce:

Bezpečnost a analýza rizik v praxi

Abstrakt:

Tato bakalářská práce seznamuje s problematikou analýzy rizik a bezpečností aktiv podniku. Teoretická část práce přibližuje terminologii dané problematiky a blíže seznamuje s obecně využívanými postupy při řešení návrhu analýzy rizik s informační bezpečností společnosti. Praktická část práce se zaměřuje na aplikaci analýzy rizik po vzoru ISO/IEC 27005 na konkrétním subjektu, jehož oblast působnosti se soustřeďuje na distribuční a poradenskou činnost v oblasti audio a video techniky. V analýze rizik je využito kvalitativních metod hodnocení. Výstupy analýzy je možné sledovat v přílohách studie. Cílem práce je návrh opatření zabraňujících vzniku analyzovaných rizik, která byla zjištěna z předem vyrozuměné oblasti zkoumání stanovené subjektem. Oblast zkoumání je soustředěna na oblast nákupu a prodeje.

Klíčová slova:

Riziko, hrozba, následek, ošetření, aktivum, analýza rizik, zranitelnost, COBIT, ITIL, ISO/IEC 27005

Title of the bachelor's thesis:

Security and Risk Analysis in Practice

Summary:

This thesis describes issues of risk analysis and security of company assets. Theoretical part of the thesis looks into the terminology of the topic with closer familiarization of procedures that are commonly used in risk analysis solutions and in company information security. Practical part of the thesis is focused on application of risk analysis using ISO/IEC 27005 methods on a concrete company, which is focused on distribution and consultation in the field of audio and video technology business. In risk analysis qualitative methods of valuation are used. An output of the analysis could be seen in added annex. The output of this thesis should be a treatment that shall prevent creation of risks, which had been found in previously defined area. Scope of the study is focused on purchase and sale.

Keywords:

Risk, threat, consequence, treatment, asset, risk analysis, vulnerability, COBIT, ITIL, ISO/IEC 27005

Obsah

Úvod bakalářské práce

V průběhu dvacátého století se začíná uvažovat, že současné postavení a konkurenceschopnost podniků nestojí již pouze na hmotném zajištění společnosti, ale na informacích nebo také znalostech. O informacích se přestává hovořit jako o abstraktním pojmu a začíná se více chápat jako zboží [3], které může nabývat rovnocenného postavení stejně jako tradiční ekonomické zdroje.

Souběžně s tímto faktem začíná vnikat nová manažerská disciplína, jež má za úkol informace chránit. Hovoříme o informační bezpečnosti a jejím řízení. Tento obor koncem dvacátého století zaznamenal velký rozmach a v současnosti se těší výsadnímu postavení u velkých korporátních společností a stejně tak nabývá na svém významu u menších společností, které tvoří základnu ekonomiky většiny evropských zemí.

Paradoxně jsou to menší podniky, jež z většiny případů bezpečnostní politiku neuplatňují a považují řízení bezpečnosti informací za přebytečné zlo, nebo řízení bezpečnosti u těchto podniků bývá nedostatečné. Je tomu často z toho důvodu, že společnost odmítá vynaložit finanční prostředky na oblast řízení, jíž nepovažuje pro předmět svého podnikání za kritický, a operuje pouze povrchově na základě zákonných ustanovení dané země. Avšak je to právě informační bezpečnost s bezpečností aktiv, která zajišťuje společnostem dostatečnou důvěryhodnost a konkurenceschopnost na poli tržního prostředí.

Je však nutné brát v potaz skutečnost, že metodiky nabízené pro řešení informační bezpečnosti tvoří převážně větší podniky a menší společnosti jsou v tomto ohledu čistými příjemci nových trendů. Což staví menší ekonomické subjekty do nesnadného postavení. Otázku informační bezpečnosti je pak nutné řešit individuálně.

V minulosti vzniklo mnoho metodik, norem a doporučení, jakým způsobem s informační bezpečností v podniku nakládat. Ve většině případů tato doporučení nabízí vlastníkům i budoucí certifikaci a ověření informační bezpečnosti. Těmto normám a metodikám bude v této práci věnována samostatná kapitola, kde jsou popsány jejich charakteristiky.

Cílem této bakalářské práce je blíže se seznámit s menším ekonomickým subjektem, který bude podroben analýze rizik, v níž se prakticky ověří jedna z metodik, a ověřit zajištění řízení bezpečnosti menšího subjektu v českém prostředí, na základě dříve získaných teoretických znalostí.

Ve vymezené oblasti analýzy budou stanovena rizika. Tato rizika budou klasifikována a budou pro tuto oblast navrhnuta patřičná opatření.

Opatření vycházející z hodnocení rizik budou dále konzultována s vedením společnosti, jež má za úkol rozhodnout, zda nová opatření pro minimalizaci rizik jsou dostačující.

Teoretická část

1. Terminologie

Pro bližší pochopení této bakalářské práce je žádoucí blíže specifikovat termíny a výrazy, které běžnému čtenáři nemusí být zcela zřejmé. Proto následující kapitola bude věnována teorii, která má za úkol seznámit čtenáře s problematikou bezpečnosti informací a analýzou rizik. Tato část práce bude doplněna i o subjektivní názor autora.

1.1 Bezpečnost

Pod pojmem „bezpečnost“ můžeme sledovat mnoho definic osvětlujících danou problematiku. Můžeme však tvrdit, že v obecné rovině se bezpečností nejčastěji rozumí soubor opatření a soustavných činností vedoucí k zamezení neoprávněného nakládání s aktivy společnosti. Tuto skutečnost nejlépe vystihuje následující definice.

„Pod pojmem bezpečnosti v prostředí IT rozumíme soubor opatření, aktiv a pravidel, které mají zabránit neoprávněnému použití těchto technologií jak na straně uživatele tak na straně provozovatelů.“ [1]

V současné době získává nejvíce na svém významu informační bezpečnost. Tento fakt lze sledovat na základě světové globalizace pomocí informačních a komunikačních technologií (ICT). Díky neustálému vývoji informačních technologií se řadí informační bezpečnost mezi jednu z nejrychleji se vyvíjejících disciplín.

„Informační bezpečnost je multidisciplinární obor, usilující o komplexní pohled na problematiku ochrany informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace. Je tak možné chápat odvětví, zabývající se snižováním rizik, vztahujících se k fenoménu informací a navrhující opatření, vztahující se k příslušným organizačním, řídícím, metodickým, technickým, právním a dalším otázkám, které s touto problematikou souvisí.“[2]

Nejčastějšími důvody zavádění informační bezpečnosti v podnicích je fakt, že světová globalizace vede k digitalizaci většiny informací, rozvoje nových metodik přenosu dat, vzájemné ovlivňování ekonomik pomocí ICT, což má za následek vznik nového druhu kriminální činnosti spojené s odcizením, popřípadě rizikem znehodnocení informačních aktiv společnosti. Na základě těchto informací lze usuzovat důležitost informační bezpečnosti a její význam i v budoucnosti.

1.2 Informace

„Poznatek týkající se jakýchkoliv objektů, například fakt, událostí, věcí, procesů nebo myšlenek včetně pojmů, který má v daném kontextu specifický význam (podle ČSN ISO/IEC 2382-1, s. 7).“[3]

Informace se může vyskytovat v nesčetných podobách. Nejčastěji v tištěné, psané či elektronické podobě. V současné době se často hovoří o informaci jako o nejcennějším aktivu společností. Napovídá tomu fakt, že informace mohou být nositeli kritických znalostí, které mohou společnostem přinést užitek a v případě neoprávněného nakládání ztrátu. Informace tak podporují konkurenceschopnost organizací se schopností přežití na dnešních trzích. Z toho důvodu musí společnosti ochraně informací věnovat obzvláštní pozornost.

1.3 IT, IS, ICT

IT je všeobecně uznávaná zkratka pro informační technologie. Často se označuje jako nauka o zpracování informací. V praxi se toto označení týká veškerých technologií, které se zabývají automatizací shromažďování informací, jejich zpracováním a mnohým dalším.

IS je zkratkou užívanou pro informační systém. Informační systém lze pak definovat jako *„soubor lidí, technologických prostředků a metod, které zabezpečují sběr, přenos, zpracování a uchování dat za účelem tvorby prezentace informací pro potřeby uživatelů.“* [1]

ICT označuje zkratku pro informační a komunikační technologie. Podle [1] tento termín nahrazuje dříve používaný termín IT. V případě ICT moderní informační produkty mají schopnost komunikace jako předpoklad k vzájemné integraci a zabezpečení tak konkurenceschopnosti.

1.4 Řízení bezpečnosti informací

Řízení bezpečnosti informací můžeme definovat jako oblast řízení, která se výlučně věnuje informačním aktivům podniku a jejich bezpečnosti. Podle pole působnosti lze členit řízení bezpečnosti na bezpečnost organizace, bezpečnost informací a bezpečnost IS/ICT, jak uvádí [10]. Můžeme dále tvrdit, že řízení bezpečnosti informací vytváří repetitivní proces, jehož cílem je neustálé zlepšování bezpečnosti. Blíže nám definuje tento proces definice z ČSN ISO/IEC 27001:2005.

„Systém řízení bezpečnosti informací – ISMS (Information Security Management System) – část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.“ [8]

Před samotným řízením bezpečnosti informací musí společnost vydat ustanovení v podobě politiky ISMS, která stanovuje rozsah řízené oblasti s hranicemi pro následnou analýzu rizik, na jejímž základě se stanovují soubory postupů a technik pro zajištění bezpečnosti.

Řízení bezpečnosti se podle [8] skládá z doporučených etap, jež tvoří opakující se cyklus:

- ustanovení ISMS
- zavádění a provoz ISMS
- monitorování a přezkoumání ISMS
- údržba a zlepšování ISMS

Existuje více metodik, jež nám nabízí řešení informační bezpečnosti s analýzou rizik. A řadíme je stejně jako ISO normy mezi „best practices" metodiky. Jedná o soubory postupů a doporučení jako například COBIT, ITIL a další, jimž je věnována druhá kapitola této práce.

1.5 Riziko

Pokud bychom se měli ohlédnout za historickým významem tohoto pojmu, dojdeme závěru, že neexistuje jednotná definice, která by dokázala spolehlivě vyjádřit úplný význam daného slova. V našem případě však bude nejvhodnější uvažovat následující vysvětlení.

„Z hlediska problematiky řízení podnikatelských rizik bude užitečné vnímat jako možnosti, že s určitou pravděpodobností dojde k události, jež se liší od předpokládaného stavu či vývoje. Riziko by nicméně nemělo být směšováno, respektive redukováno na pouhou pravděpodobnost, neboť zahrnuje jak samotnou pravděpodobnost, tak kvantitativní rozsah dané události." [17]

Ačkoliv by se z této definice na první pohled mohlo zdát, že riziko je těsně spjato pouze s ekonomickými procesy, opak je pravdou. Riziko lze kategoricky členit do skupin dle témat, kterých se riziko týká. Můžeme pak například hovořit o politickém, bezpečnostním či právním riziku. Těchto skupin může být nesčetné množství, ale ať už hovoříme o kterékoliv zkoumané oblasti, riziko provádí dva stavy, jež definují podstatu rizika. Jedná se o neurčitost výsledku a skutečnost, že jeden z výsledků bude nežádoucí. Nežádoucí výsledky můžeme definovat jako odchylku od požadovaného stavu. Tedy stavu, který očekáváme a doufáme v něj.

Stupně rizika je možné měřit a stanovit tak míru pravděpodobnosti, s níž dojde k nežádoucím výsledkům. Nejedná se však o podmínku. Velmi často dochází k situacím, kdy subjekty se musí rozhodovat pouze na základě hůře kvantifikovatelných a kvalifikovatelných informací, což vede k rozvoji subjektivních postojů k riziku. Nejčastěji jsou pak skloňovány přístupy jako averze, sklon k riskování a v neposlední řadě neutrální postoj. Tyto postoje definují manažerské přístupy a

predikují, jakým způsobem budou subjekty s největší pravděpodobností postupovat v případě rozhodovaní. Avšak nejedná se pouze o subjektivní postoj. Subjekty svá rozhodnutí musí částečně podřídit i předchozí analýze daného rizika, která poskytuje dostatečnou informační základnu pro zkoumání určitého jevu.

1.6 Analýza rizik

Podle zkoumané oblasti lze analýzu rizik chápat vícero způsoby. V případě bezpečnosti informačních a komunikačních zařízení nám definuje vyhláška NBÚ č. 523/2011 Sb. pojem následovně:

„…proces, během něhož jsou zjišťována aktiva informačního systému, hrozby působící na aktiva informačního systému, jeho zranitelná místa, pravděpodobnost realizace hrozeb a odhad jejich následků,“ [4]

Podle [5] lze analýzu rizik vysvětlovat jako:

„Systematické používání informací k odhadu míry rizika a k určení jeho významu.“

Zobecňující definice analýzy rizik podle [3], nám pojem vykládá následovně:

„Analýza rizik je obvykle chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti.“

Pro větší proniknutí do teoretické podstaty a postupů analýzy rizik se může zdát tato definice jako nejvhodnější. Je nutné uvědomit si, že analýza rizik je velice komplexní disciplínou a pro zajištění zdravé bezpečnosti a snižování rizikovosti je žádoucí zkoumat danou problematiku z více úhlů pohledu. Aby byla zajištěna dostatečná informační základna pro pozdější řízení bezpečnosti podniku.

Postup analýzy lze podle [3] zpravidla shrnout do následujících bodů:

- Identifikace aktiv
- Stanovení hodnoty aktiv
- Identifikace hrozeb a slabin
- Stanovení závažnosti hrozeb a míry zranitelnosti

1.7 Kvantitativní analýza rizik

Analýzu rizik můžeme členit podle formy zkoumání rizik a jejich hodnocení. Podle [9] se kvantitativními metodami můžeme setkat od počátku 70. let minulého století. Metody vznikaly v reakci na požadavky formalizace procesu analýzy rizik IS. Tyto metody mají silnou matematickou podporu, jsou snadno pochopitelné a jejich výsledky jsou jednoznačné. Výsledky metod jsou vyjádřeny na spojité číselné škále a lze je vyjádřit v penězích. Nevýhodou těchto metod je náročnost provedení, časová a informační.

1.8 Kvalitativní analýza rizik

Podle [9] se můžeme s kvalitativními metodami setkávat od počátku 80. let. Tyto metody využívají pro popis výše dopadu, hrozeb, zranitelností a výsledného rizika diskrétní škály. Nejčastěji se pak jedná o škály od jedné do deseti, případně využívají slovní popis výsledného rizika. Tyto metody jsou oproti kvantitativním metodám časově mnohem méně náročné. Nicméně výsledky metody mohou být zatížené o subjektivní odhad, který nemusí být vždy zcela přesný.

1.9 Aktivum

Podle [3] lze aktivum vnímat jako vše, co má pro subjekt určitou hodnotu, která může být však zmenšena negativním působením hrozby. Aktiva můžeme základně členit podle jejich charakteristických vlastností na hmotná a nehmotná.

Další možností, jak lze aktiva rozlišovat, je doporučené členění v souladu s [6]. Tato norma doporučuje členit aktiva na primární a podpůrná. Kdy na straně primárních aktiv stojí obchodní činnosti, procesy, informace. A na straně podpůrných aktiv vše, co slouží k zajištění aktiv primárních.

Nejpodstatnější charakteristikou aktiva se pak jeví jeho hodnota, která lze vyjádřit mnoho způsoby. Z pravidla se uvažuje objektivní a subjektivní vyjádření hodnoty.

Objektivní hodnocení aktiva vychází z cenového ohodnocení, kdežto subjektivní ohodnocení hodnotí aktivum na základě kritičnosti k činnostem subjektu.

1.10 Hrozba

Hrozbou můžeme označovat cokoliv, co může svou podstatou ohrozit žádoucí stav bezpečnosti aktiv společnosti. Může se jednat o fyzické osoby, přírodní katastrofy, nepovolené nakládání s aktivy, působení ekonomických sil. Tuto skutečnost nám nejlépe shrnuje definice:

„Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu.“ [3]

Závažnost hrozby lze kategorizovat podle [3] do úrovní:

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

1.11 Dopad hrozby

Tímto pojmem označujeme míru následků, které mohou působením hrozby nastat. Nejčastěji se hodnotí pomocí absolutní hodnoty ztrát, popřípadě náklady na odstranění následků škod, [3].

1.12 Zranitelnost

„Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.“ [3]

1.13 Protiopatření

„Protiopatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby.“ [3]

2. Metodiky, metody a normy pro zpracování analýzy rizik

V případě, že se podnik rozhodne pro uplatňování řízení bezpečnosti informací a na tomto základě bude chtít vypracovat analýzu rizik, bude postaven před nelehký úkol výběru toho nejvhodnějšího postupu. Skutečnost, že se na trhu vyskytuje nesčetné množství metodik, doporučení, metod, postupů, tuto situaci může velmi ztěžovat. Stejně tak jako otázka volby subjektu zhotovení. Ale ať už se bude jednat o externího či interního zhotovitele analýzy, dostatečná znalost podniku s jeho procesy a kontextem bude hrát zásadní roli.

Díky těmto znalostem jsou zhotovitelé schopni velikost výběru zredukovat a případně dané metodiky upravit pro potřeby společnosti. V mnoha případech se tyto metodiky objevují ve formách doporučení a návodů a nevyžaduje se jejich striktní dodržování. Metodiky mohou nabízet úplné řešení, případně se problematikou mohou zabývat pouze jako podkapitolou celkového řízení IT/ICT ve společnosti.

2.1 Metodiky zahrnující analýzu rizik s řízením bezpečnosti informací

V následujících podkapitolách budou vystihnuty nejznámější a nejužívanější metodiky, metodami, technikami a patřičnými normami, které bývají nejčastěji skloňovány s problematikou analýzy rizik a bezpečností informací.

2.1.1 COBIT

Metodika COBIT je zkratkou anglického „Control Objectives for Information and Related Technology“. První verze této metodiky vznikla v roce 1996 pod záštitou agentury ISACA[1]. Cílem této metodiky bylo vytvořit sadu procesů, ukazatelů, návodů, které měly za úkol vytvořit všeobecně uznávaný rámec řešení pro správu IT společností a maximalizovat z nich plynoucí prospěch.

Podle [10] základní princip metodiky COBIT je postaven na cílech organizací, zdrojích informačních technologií a procesech. Tyto základní komponenty vytváří tzv. COBIT kostku. Zdroje informatiky jsou řízeny procesy tak, aby bylo dosaženo stanovených cílů informatiky, které odpovídají strategickým požadavkům.

[1] Zkratka slov: Information Systems Audit and Control Association

Oddíl plánování a organizace obsahuje položky týkající se procesů, odkazujících se na řízení bezpečnosti a řízení rizik. Jedná se o proces Určení a řízení rizik. Tomuto procesu podléhají mnohé další procesy, jež dohromady vytváří komplexní řešení pro ISMS.

Pokud se budeme zabývat formální stránkou metodiky, v [11] je COBIT popsán jako velmi dobře strukturovaná metodika, v níž se snadno orientuje díky své tabelární formě s pevně danou strukturou. Nicméně terminologické zatížení psaného slova může ve čtenáři vyvolat dojem, že v praxi se může spíše stát nástrojem auditorů nežli firemním nástrojem.

2.1.2 ITIL

„Information Technology Infrastructure Library“ je souborem knih tvořící výčet způsobů procesního řízení služeb a infrastruktury IT. Podle [10] můžeme říci, že cílem metodiky je poskytnout ucelený soubor tzv. nejlepších zkušeností pro oblast řízení služeb IT a souvisejících procesů.

ITIL vznikl v 80. letech minulého století jako reakce britské vlády na nedostatky v oblasti řízení informatiky ve státním sektoru. K vytvoření této metodiky byla pověřena vládní agentura CCTA (Central Computer and Telecomunications Agency), která vytvořila daný soubor postupů.

V minulosti došlo k přepracování této metodiky tak, aby mohla být využívána i soukromým sektorem a to na základě studií z praxe. Avšak prvotní vydání nebyla schopna naplnit očekávání zadavatelů. A to zejména díky postupnému doplňování svazků, jež nestačily svým postupným vydáváním reagovat na potřeby soukromého sektoru. Obrat k lepšímu u této metodiky můžeme sledovat až počátkem 90. let dvacátého století.

Od vzniku ITILU verze 2, můžeme sledovat zakomponování řízení bezpečnosti do samotné knihy. Tato kniha však neobsahuje přesný postup při analýze rizik. Naopak je tato část velmi stroze definována. Tento fakt bývá odůvodněn tím, že vedení každé společnosti využívá jiných praktik a dokáže odhadnout, které způsoby budou nejlépe vyhovovat podniku.

Ve třetí verzi ITILU lze vysledovat výrazné zlepšení ve smyslu propojení řízení bezpečnosti informací s ostatními procesy, což bylo velmi pozitivně přijímáno uživateli metodiky. Avšak detailnější řešení analýzy rizik nepřináší.

Oproti metodice COBIT se dá říci, že ITIL je v mnohých ohledech více flexibilní a nabízí spíše výčet doporučení nežli komplexní řešení.

Mnohá tato doporučení však bývají detailněji specifikována a jejich nasazení je mnohem lépe proveditelné u většiny podniků, bez ohledu na jejich velikost či organizační strukturu.

Podle [12], pokud se podnik rozhodne pro užití metodiky ITIL a následnou certifikaci, musí se připravit na nemnohá úskalí. Ačkoliv se na první pohled může zdát, že detailní popis postupů může vést k úspěšnému pochopení jednotlivých doporučení, což by mělo k úspěšné implementaci s certifikací stačit, opak je pravdou. Pro certifikaci je důležitá znalost definic, jak je v [12] uvedeno. Některé definice zde však bývají hůře srozumitelné pro běžného uživatele a vedou tak k nedorozuměním, ačkoliv je to paradoxně ITIL, který se snaží o zjednodušení a unifikaci terminologie.

2.1.3 CRAMM

CRAMM (CCTA Risk Analysis and Management Method) je další z metodik, která pochází původem z Velké Británie a za jejímž vznikem stojí vládní agentura. Od roku 1985 sloužila k zajišťování bezpečnosti informačních systémů pro státní sektor. Jedná se o metodu využívající formy kvalitativní analýzy rizik. Díky své oblibě a rychlé adaptaci na soukromý sektor se rychle rozšířila v povědomí velkého množství uživatelů a v současnosti se řadí mezi jednu z nejoblíbenějších metodik.

Je tomu především z toho důvodu, že tato metodika se snaží komplexně pokrýt všechny fáze řízení rizik, a to od analýzy až po samotný návrh protiopatření. Součástí této metodiky jsou i nástroje pro tvorbu dokumentace zajišťující havarijní plány, jejichž účelem je zajištění kontinuity provozu. V současnosti metodika na trhu nabízí i několik aplikací, které mají svým uživatelům napomoci při výpočtech, zpracování reportů a se shromažďováním informací.

Velkou výhodou této metodiky je i fakt, že je kompatibilní a částečně obsahuje prvky norem ISO řady 27000, jež jsou považovány za standard v oblasti řízení bezpečnosti a jsou celosvětově uznávány a těší se velké oblibě.

„Použití metodiky CRAMM umožňuje také připravit organizaci na certifikaci podle ISO 27001. Je také v souladu s dalšími ISO normami (ISO 9001 a ISO 14001).“[13]

2.2 Podpůrné metody a techniky užívané analýzou rizik

V následujícím výčtu této podkapitoly bude představeno několik nejznámějších technik, s nimiž se můžeme setkat při analýze rizik. Tyto metody slouží jako podpůrný nástroj při jejím zpracování a mnohé z nich jsou v současné době hojně využívané při zpracování analýzy a stejně tak v jiných oblastech zajišťující zdravý chod společnosti.

2.2.1. DELPHI

Podle [14] se tato metoda zakládá na principech bainstormingu[2] nezávislých expertů, jejichž účelem je zajistit objektivní odhad vývoje či stavu dané problematiky. Metoda se často využívá současně s jinými kvalitativními metodami, které jsou určené pro analýzu rizik. Stejně často bývá využívaná při řízení projektů.

Pro využití této metody se uvažuje skupina osmi a více osob, které se v jednotlivých kolech diskuse snaží o generování otázek na dané téma. Otázky jsou tvořeny takovou formou, aby na ně bylo možné kvalifikovaně odpovídat. V průběhu kol mohou účastníci své názory na problematiku pozměňovat a mají přístup i názorům ostatních. S přibývajícími koly dochází k zpřesnění odhadu. Odhad je zaznamenán s výsledným kolem, v němž je i statisticky zaznamenán.

2.2.2 CLA

Technika CLA neboli Check List Analysis je velmi jednoduchou metodou, která využívá seznamu položek, podle něhož lze kontrolovat postup analýzu rizik. Velmi často se také užívá obecně v souvislosti bezpečnosti informací a řízení kvality.

Technika stanovuje seznam kontroly, který je založen na předchozích zkušenostech s danou problematikou. A podle fáze postupu lze v tomto seznamu odpovídat formou ano/ne, zda je daný bod seznamu splněn.

2.2.3 ETA

Event tree analysis je metoda, která vznikla po roce 1979 v reakci na havárii elektrárny v Three Mill Island. Stejně jako předchozí metody nachází uplatnění v oblasti řízení kvality, rizik a bezpečnosti.

[2] *„Brainstorming je skupinová kreativní technika. Cílem je generování co nejvíce nápadů na dané téma.“ [15]*

„Metoda ETA je založená na rozboru sekvence činností a událostí v procesu vedoucí k nehodě, kterou zobrazuje pomocí grafického logického modelu. ETA zvažuje také případné odezvy bezpečnostního systému a lidské obsluhy (operátorů). Výsledkem analýzy ETA jsou různé scénáře nehody.“ [16]

2.2.4 FTA

Technika Fault Tree Analysis je metoda, jež se zakládá na zpětném rozboru událostí, které vedou k možné příčině problému. Technika byla vyvinuta společností Bell Telephone Laboratories v roce 1962.

Metoda využívá grafického zpracování problému, kdy vrcholem stromu je zkoumaný problém, od něhož se větví jednotlivé možné příčiny, jež mohou problém způsobit. Možné příčiny jsou analyticky vyhodnocovány a tvoří se statistický odhad pro pravděpodobnost výskytu s využitím jednotlivých příčin.

2.2.5 Safety Audit

Technika bezpečnostní metody neboli Safety audit je metoda, která systematicky vyhledává potencionální rizika, která mohou zapříčinit nežádoucí stav. Tato metoda slouží především jako preventivní kontrola zvýšení bezpečnosti.

Metoda postupuje pomocí předem připraveného seznamu otázek, které mají za úkol odhalit potencionální riziko. Otázky vychází především ze zkušeností a praxe. A na základě odpovědí se zaznamenávají výsledky do skórovací matice.

2.2.6 QRA

Quantitative Risk Analysis je technika založená na kvantitativním posuzování potenciálních rizik, jehož cílem je tvorba predikce odhadu, četností a dopadů. Metoda je doporučována jako vhodné rozšíření kvalitativních analýz.

Společně s využitím jiných nástrojů podporuje QRA proces rozhodování. Výstup této metody umožňuje lépe analyzovat zkoumaný problém. Její nevýhodou může být náročnost na softwarovou podporu při složitějších analýzách.

2.3 Příslušné normy

Následující podkapitola bude pojednávat o normalizaci bezpečnosti informací, kterou zajišťuje nadvládní mezinárodní organizace pro normalizaci „International Organisation for Standardization“, nesoucí označení ISO. Zmíněná část práce se bude více věnovat normám, konkrétně normám řady ISO/IEC 27000. A blíže bude specifikován postup analýzy rizik podle normy ČSN ISO/IEC 27005, jež je součástí rodiny norem 27000.

Organizace ISO vznikla roku 1947 a v současné době má sídlo v Ženevě. Organizace zaštituje standardy přibližně 161 zemí. A do dnešní doby publikovala více než 21000 standardů, které pokrývají téměř všechny oblasti technologií a výroby.

2.3.1 ISO/IEC 27000 - Systém řízení bezpečnosti informací - Přehled a slovník

Za páteř této normy se považuje ISMS, jenž norma staví na principech cyklického PDCA modelu, na jehož základě i stojí převážná část normy. Zkratka vychází z anglického překladu slov „Plan-Do-Check-Act“, tedy „Plánuj-Konej-Kontroluj-Jednej“.

První část normy se věnuje především stanovení předmětu normy, definici pojmů a termínu, s nimiž norma pracuje. Následující část popisuje systémy řízení bezpečnosti informací a nabízí nám kratší přehled řady norem z rodiny ISMS. Za touto částí následuje obsah normy, na nějž navazují doplňující přílohy.

2.3.2 ISO/IEC 27001 - Systém řízení bezpečnosti informací – Požadavky

Norma 27001 vychází z britského standardu BS-7799-2 z roku 2005, avšak oproti svému předchůdci odstraňuje několik bezpečnostních opatření a nahrazuje je mnohými novými, které považuje za v praxi lépe fungující.

Cílem této normy je specifikovat veškeré požadavky na ISMS, jež musí společnost splňovat před jeho implementováním. Jedná se především o dělby rolí, organizace a hodnocení výkonosti.

Přílohou této normy je specifikovaný seznam bodů, které by měla společnost splnit pro úspěšné zavedení zdravého systému řízení bezpečnosti informací. Pokud společnost není schopna splnit požadavky této normy, není možné systém implementovat a norma nás od toho odrazuje.

2.3.3 ISO/IEC 27002 – Soubor postupů pro opatření informační bezpečnosti

Původní verze této normy vyšla v průběhu roku 2005, kdy ještě nesla označení ISO/IEC 17799:2005. Tato norma prochází pravidelnými revizemi. [10] Společně s normou ISO/IEC 27000 je tato norma považována za jednu z nejdůležitějších norem rodiny 27000.

Úvodní část normy poskytuje objasnění pojmu informační bezpečnost a vysvětlení důležitosti této disciplíny pro společnost. Obsahem kapitol normy ISO/IEC 27002 jsou bezpečnostní opatření s kroky, které jsou nutné pro úspěšné implementování ISMS. Díky bezpečnostním opatřením jsou společnosti schopné dosáhnout i na certifikaci podle ISO/IEC 27001, avšak bez uplatňování doporučení dle ISO/IEC 27001 se stávají postupy této normy neúčinné.

2.3.4 ISO/IEC 27003 - Směrnice pro implementaci systému řízení bezpečnosti informací

Oproti svým předchůdcům se až teprve tato norma stává praktickým návodem, jak vytvořit plán a zavést ISMS. Norma se odvolává na normy předchozí, a to především na normu ISO/IEC 27001.

V první části norma přináší přehled užívané terminologie a popisuje postup komunikace přípravných kroků s vedením společnosti. V následujících krocích vysvětluje norma sestavení politiky ISMS s analýzami prostředí podniku. Přílohy obsahují informativní materiál týkající se rozdělení rolí, zodpovědností atd. Výsledkem normy je plán implementace ISMS.

2.3.5 ISO/IEC 27004 – Měření

Poslední normou, která se přímo vztahuje k řízení systému bezpečnosti, je norma ISO/IEC 27004. Tato norma stanovuje přesné metriky k hodnocení ISMS v podniku, díky nimž by měl podnik vykazovat lepší výsledky v implementaci ISMS. Norma se odkazuje na porozumění problematiky řízení a hodnocení rizik ISO/IEC 27005.

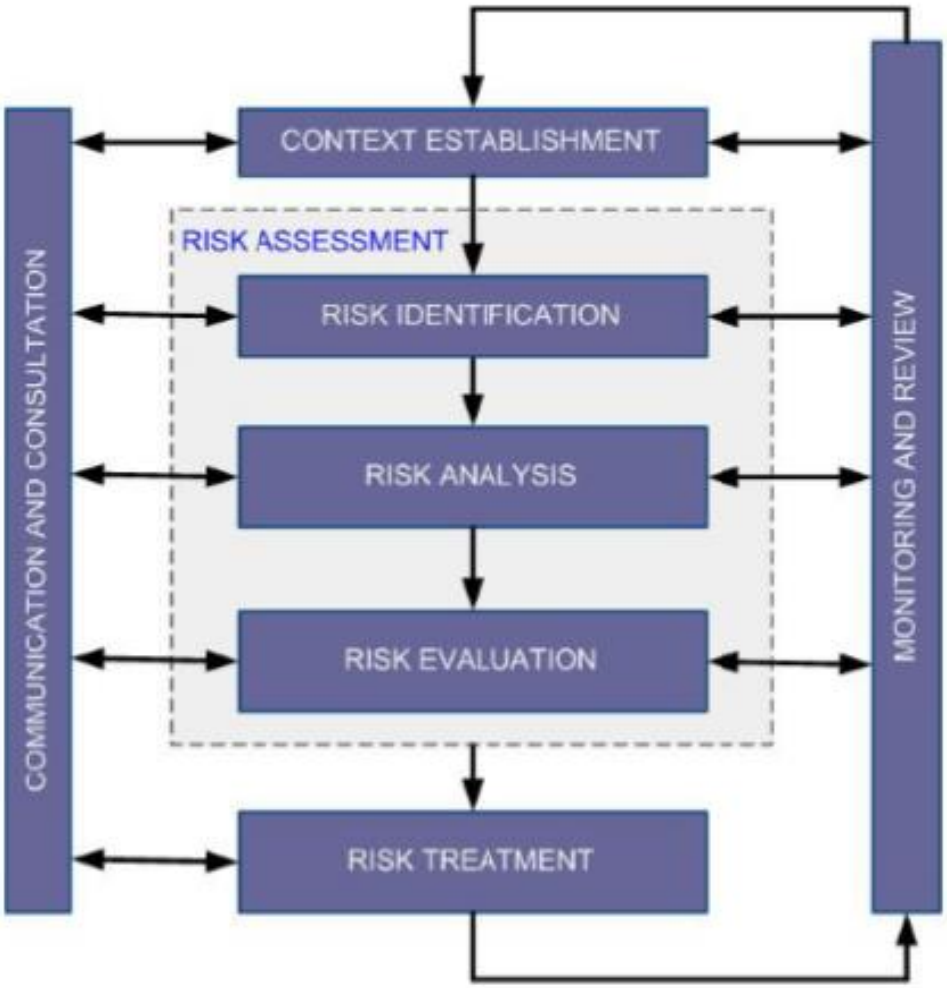
2.3.6 ISO/IEC 27005 – Informační technologie – Bezpečnostní techniky – Řízení rizik a bezpečnosti informací

Norma byla vydána roku 2008. Cílem bylo nahradit již zastaralou normu ISO/IEC TR 13335-3:1998, která již nedokázala dostatečně pokrýt současné potřeby uživatelů. Stejně tak nově vzniklá norma kladla důraz na kompletní revizi všech pravidel a postupů, jež by dokázaly vystihnout dnešní nároky na oblast řízení rizik.

Nutno dodat, že norma od svého počátku nabízela rozsáhlý katalog hrozeb a zranitelností, s nimiž se může společnost setkat a díky častým revizím se tento katalog dále rozšiřuje, jak je popsáno v [10].

Stejně jako jiné normy se i ISO/IEC 27005 odkazuje na definice a požadavky na ISMS normy ISO/IEC 27001, ačkoliv norma ve svém úvodu nabízí uživateli přehledný výčet definic termínů, s nimiž se v normě pracuje.

Norma poskytuje grafický náhled celého procesu analýzy, na nějž navazuje neustále opakující se subproces monitorování a přezkoumávání pro dosažení těch nejlepších výsledků. V popředí stojí proces stanovení kontextu, který doplňují procesy identifikace rizik, analýzy rizik, vyhodnocení rizik a v neposlední řadě zvládání rizik, na nějž navazuje proces monitorování a spouští celý model znovu, podle [18].



Obr. 1: Proces řízení rizik

3. Postup analýzy rizik – ISO/IEC 27005

V následující kapitole bakalářské práce bude popsán postup analýzy rizik podle normy ISO/IEC 27005:2001(E). Tato kapitola čerpá informace z [18], které jsou doplněny o subjektivní chápání autora.

3.1 Stanovení kontextu

V úvodní části modelu nás norma nabádá k získání dostatečné informační základny, tedy kontextu celé společnosti, což tvoří vstup pro celý proces. Správné pochopení společnosti, její vnitropodnikové fungování a vazby s okolím jsou pro nás nezbytné.

Kontext společnosti je důležité také chápat z více úhlů pohledu. Skutečnost, že podnik působí na trhu od určitého okamžiku, nám dává možnost se seznámit i s jeho minulou činností a stejně tak i s jeho budoucí představou, plány a cíli.

Nesmíme dále opomenout fakt, že je nutné znát i důvod, pro který se podnik rozhodl aplikovat model řízení bezpečnosti. Nejčastějšími důvody bývá podpora systému řízení bezpečnosti, soulad s právními předpisy, příprava „business continuity[3]“ plánu, příprava plánu protiopatření, popis požadavků na zabezpečení informací produktu, služby nebo mechanismu, podle [18].

3.1.1 Základní kritéria

V této fázi je nutné zvolit nejvhodnější přístup pro aplikaci řízení rizik, neboť různé přístupy mohou přicházet v úvahu a každý z těchto přístupů využívá jiné formy hodnocení pro kritéria, dopady i akceptaci rizik.

Současně je také nutné zjistit, zda společnost vlastní, nebo má přístup k takovým zdrojům, které by dokázaly zajistit dostatečnou podporu a informační základnu pro jednotlivé fáze postupu analýzy rizik.

3.1.2 Rozsah a hranice

Cílem stanovení rozsahu a hranic je vymezit ta aktiva, která budou subjektem brána v potaz při analýze a stejně tak vymezit oblast zkoumání, v níž bude analýza prováděna, zvážit všechny aspekty tohoto rozhodnutí, stejně jako odůvodnění, proč některá aktiva nebudou do oblasti zahrnuta.

[3] Výstup Řízení kontinuity činností organizace, plán zachování činnosti

3.1.3 Organizace řízení rizik bezpečnosti informací

V tomto kroku se zvažuje rozdělení rolí a zodpovědností pro osoby pověřené analýzou rizik, jejichž úkolem je vyvinout vhodný systém řízení bezpečnosti informací pro společnost, nastavení povinností a vztahů pro interní a externí část společnosti a specifikace dokumentace, jež se bude k dané problematice vztahovat.

3.2 Identifikace rizik

Cílem této fáze je odhalení možných příčin, které mohou způsobit potenciální ztrátu ve zkoumané oblasti. Nejčastěji se pak hledají odpovědi na otázky, které se ptají na to, kde ztráta může nastat a proč může nastat. Za vstup se považují základní informace, které jsou poskytnuty subjektem.

3.2.1 Identifikace aktiv

Identifikace aktiv se zaměřuje na členění zjištěných aktiv z oblasti zkoumání na primární a podpůrná. Přičemž vytváří jejich podrobný katalog. V tomto katalogu můžeme sledovat detailní popis vlastností aktiv s jejich ohodnocením.

3.2.1.1 Primární aktiva:

Mezi primární aktiva řadíme nejčastěji procesy, které mají kritický vztah k předmětu podnikání, a informace s nimi spojené.

a) Obchodní procesy a činnosti

Neexistence těchto procesů ve své podstatě znemožní plnit předmět podnikání společnosti. Tato skupina obsahuje činnosti, které do jisté míry nesou know-how procesů. Jejich změna by měla dopad na plnění cílů podnikání, stejně jako smluvních a regulačních nastavení.

b) Informace

Jedná se o informace kritické pro předmět podnikání; soukromé informace, informace náročné na zpracování.

3.2.1.2 Podpůrná aktiva

Tato aktiva jsou zranitelná a jsou zneužívána hrozbami, jejichž cílem je skrze tato aktiva poškodit, případně jiným způsobem znehodnotit aktiva primární. Do podpůrných aktiv řadíme:

a) Hardware

Obsahuje všechny fyzické prvky, zajišťující správný chod procesů.

b) Software

Skládá se ze všech programů aplikací, které slouží ke zpracování dat.

c) Sítě

Jedná se o telekomunikační zařízení využívaných k propojení fyzicky vzdálených počítačů, nebo propojení prvků IS.

d) Personál

Personál se skládá ze všech osob, které jsou zapojené do IS.

e) Umístění

Obsahuje všechny lokality, vlastní i externí, které jsou ve vztahu k činnostem společnosti, a zdroje nutné pro jejich provoz.

f) Organizace

Popisuje organizační rámec, který obsahuje veškeré personální struktury nutné k zajištění úkolů.

3.2.1.3 Hodnocení aktiv

Dalším krokem je volba správné škály a metody ohodnocení aktiv. Tento krok probíhá za souhlasu se subjektem hodnocení a musí se brát ohled na složitost a druh aktiv, která se rozhodujeme ohodnotit.

Z důvodu různorodosti a často také nemožnosti kvantitativního ohodnocení se využívají kvalitativní metody, jež přisuzují aktivům slovní ohodnocení, jak už bylo dříve řečeno. Případně lze zvolit kombinaci obou metod. Problém ohodnocení aktiva může nastat ve chvíli, kdy dané aktivum může mít dva způsoby ohodnocení, v nichž je možné sledovat různé druhy nákladů s aktivem spojené. Obecně se však uvažuje maximální hodnota zkoumaného aktiva s ohledem na kritičnost aktiva k danému procesu se závislostí procesu na tomto aktivu. Blíže nám popisuje hodnocení aktiv anexe B z [18].

3.2.2 Identifikace hrozeb

V tomto oddíle je doporučováno se zaměřit na hrozby a jejich členění. Důležité je identifikovat původ těchto hrozeb a jejich typ. Rozlišuje se původce hrozby, neboť hrozby mohou mít jak lidského původce, tak jiná zapříčinění. Případně mohou mít tyto hrozby více původců a těmto aktivům je třeba věnovat zvýšenou pozornost. Stejně tak mohou být hrozby způsobeny záměrně, nebo naopak náhodně. Anexe C doporučuje následující členění:

a) *A – Accidental (Náhodné); Způsobené neúmyslnou činností personálu*
b) *D – Deliberate (Úmyslné); Úmyslné činnosti cílené na informační majetek*
c) *E – Environmental (Environmentální); Způsobené činnostmi nemající lidského původce*

Ve všech případech je nutné hrozby dobře specifikovat a snažit se nalézt všechny možné hrozby, s ohledem na jejich vývoj, který se v čase mění. Nejčastěji nám k tomu dopomáhá konzultace s vlastníkem daného aktiva, neboť se předpokládá, že vlastník bude nejlépe seznámen s funkčností a vlastnostmi. Při prvotní katalogizaci se doporučuje užívat základního členění na fyzické poškození s technickými poruchami a podle potřeby toto členění dále rozvádět.

Jako detailní příklad nám může sloužit katalog hrozeb v anexi C. V tomto katalogu je možné nalézt množství příkladů hrozeb, které jsou rozděleny podle typu a svého původu. V této příloze je dále doporučováno věnovat i zvýšenou pozornost hrozbám s lidským původcem. V ukázkovém katalogu jsou tyto hrozby členěny podle konkrétního typu původce, motivace a možných následků.

Možné následky lze hodnotit kvalitativně nebo kvantitativně. Oba způsoby jsou přípustné a jsou na volbě hodnotitele, která se zakládá na domluvě se subjektem analýzy.

3.2.3 Identifikace stávajících opatření

Tento krok nám doporučuje zjistit veškerá bezpečnostní opatření, jež v minulosti firma vytvořila pro ochranu svých aktiv. Díky této předběžné kontrole je možné předejít duplikování práce a opatření. Důležité je se také soustředit na funkčnost daných opatření. Některá z opatření nemusí správně fungovat a jejich korekce je nutná. K tomuto šetření se norma odkazuje na ISO/IEC 27001, v níž je stanoven systém měření efektivnosti ISMS.

Kontrola stávajících opatření vychází především z kontroly minulých auditů, konzultace s pracovníky, bezpečnostní dokumentace a kontroly podle listu požadovaných opatření pro danou oblast.

3.2.4 Identifikace zranitelností

Určení zranitelností se rozumí nalezení těch slabých míst, jež mohou být využita hrozbami k způsobení nežádoucího stavu. V tomto ohledu se ISO/IEC 27005 opět odkazuje na normu ISO/IEC 27001.

Norma definuje nejčastější místa, kde je možné zranitelnosti identifikovat:

a) *Organizace*
b) *Procesy a postupy*
c) *Běžná praxe*
d) *Personál*
e) *Fyzické prostředí*
f) *Konfigurace informačního systému*
g) *Hardware, Software, ICT*
h) *Závislost na externích stranách*

Zranitelnosti mývají určitý vztah k aktivům a jejich existence může vycházet z toho, jakým způsobem s daným aktivem nakládáme a za jakým účelem. Díky tomuto pochopení jsme schopni přiřadit dané zranitelnosti hrozbu z ní vyplývající. Podrobný seznam možných zranitelností s jejich katalogizací lze naleznout v anexi D.

3.2.5 Identifikace následků

Následkem se v této podkapitole rozumí ztráta efektivity, zhoršené operační podmínky, narušení či ztráta předmětu podnikání, poškození reputace a další. Identifikace následků doplňuje předchozí katalogy a vytváří k jednotlivým položkám scénáře incidentu, které mohou nastat.

Aby mohl být sestaven incidentní scénář, je nutné uvažovat hrozbu, její aktivum, zranitelnost a dřívější opatření, z jejichž charakteristik lze odvodit daný následek. Následky se pak člení podle dopadu – na přímé a nepřímé následky. Detailní rozbor nám poskytuje anexe B.

Výsledná škoda způsobená incidenty se může lišit od ceny aktiva, neboť následek nemusí být vztahován na pouze jedno aktivum. Podle úspěšnosti naplnění nežádoucího incidentu lze odvodit rozsáhlejší následky, které výsledné hodnoty mohou radikálně navýšit.

Příkladem nám může být proces evidence transakcí v informačním systému. Pakliže nebudou z důvodu působení hrozby informace patřičně evidovány, bude to mít za následek neúplnost informací o platbách v systému.

Tímto způsobem lze pozorovat, jak se následek jedné hrozby na jedno konkrétní aktivum přesouvá na aktivum další. Toto však nemusí být konečný stav. Dopad se může dále šířit o dalších několik aktiv, případně se může řetězit napříč celým spektrem.

Díky této skutečnosti jsem dále schopni pozorovat jednotlivé souvislosti a vazby mezi následky hrozeb a lépe tak definovat nová opatření pro jejich zabránění.

3.3 Analýza rizik

3.3.1 Posuzování následků

Vstupem pro posuzování následků jsou předchozí katalogy. Metoda hodnocení je volena na základě dostupných informací a konzultace se subjektem. Můžeme tak volit mezi kvantitativním a kvalitativním hodnocením.

Jak už bylo dříve řečeno. Následek může mít mnohem širší dopad než na jedno aktivum společnosti a jeho hodnotu. Z toho důvodu se uvažuje při hodnocení maximální možná ztráta při naplnění incidentu, neboť dopad aktiva se nemusí vztahovat pouze na majetek hmotný, ale jeho rozsah může zasahovat i do obchodní činnosti společnosti.

Z toho důvodu má samotné hodnocení počátek v členění aktiv podle kritičnosti k daným činnostem společnosti. Při hodnocení se uvažují dva faktory, kdy na jedné straně stojí hodnota výměny, případně hodnota obnovy, na straně druhé hodnota dopadu na obchodní činnost zapříčiněný nedostupností, poškozením, vyzrazením, modifikací, zničením informačních aktiv.

3.3.2 Posuzování pravděpodobnosti incidentů

Dalším navazujícím krokem je určení pravděpodobnosti incidentů. V tomto kroku je možné, stejně jako v kroku předchozím, volit mezi kvantitativní či kvalitativní metodou hodnocení. Měl by se však brát především ohled na zkušenosti s pravděpodobností výskytu z minulosti, zdroje motivace záměrného ohrožení, zdroje náhodných hrozeb, zranitelnosti a existující opatření.

Výstupem jsou pravděpodobnosti jednotlivých incidentů ve vztahu k jednotlivým aktivům. Při posuzování pravděpodobnosti incidentů je možné využít agregace aktiv a řešit posuzování skupinově.

3.3.2.1 Stanovení míry rizik

V této fázi procesu analýzy rizik jsou vstupem scénáře incidentů, jejich následky na aktiva společnosti a obchodní činnost s pravděpodobností výskytu. Analýza přisuzuje jednotlivým scénářům hodnoty rizika a jejich pravděpodobnost v kvalitativním či kvantitativním vyjádření, ve vztahu k zainteresovaným osobám, jiným proměnným, které mají vypovídající hodnotu pro analýzu rizik.

Volba metody je opět na zhotoviteli. Existuje více přístupů pro zpracování tohoto úkolu. Z toho důvodu nám norma ve své anexi E poskytuje podrobný přehled možných zpracování.

a) Přehledové posouzení rizik bezpečnosti informací

Tato forma posuzování rizik nám umožňuje stanovit prioritu s chronologií v jednotlivých fázích analýzy. K tomu přístupu se nejčastěji společnosti přiklánějí z různých důvodů. Nejčastěji jsou to důvody jako rozpočet, nemožnost aplikování všech opatření zároveň, nemožnost ošetření všech rizik, případně chce společnost vypracovat předběžné posouzení nejkritičtějších míst z důvodu budoucích změn.

Toto posouzení pak přináší společnosti pouze obecný pohled na jednotlivé incidenty a může zapříčinit, že jednotlivé procesy a systémy nebudou identifikovány. Z toho důvodu musí být později aplikováno druhotné posouzení rizik.

b) Detailní posouzení rizik bezpečnosti informací

Proces detailního posouzení rizik hloubkově identifikuje a hodnotí aktiva, hrozby s aktivy spojené a zranitelnosti. Toto posouzení vyžaduje dostatek času se snahou a znalostmi. Tato metoda nejčastěji využívá tabulkového zpracování v podobě matic, přičemž je možné aplikovat kvalitativní i kvantitativní hodnocení, případně kombinaci obou přístupů.

Metody zpracování blíže specifikuje anexe E. Mezi tyto metody patří:

- *Matice s předem definovanými hodnotami*

Tato metoda ohodnocuje při posuzování rizik aktiva a jejich cenu, respektive cenu za jejich nahrazení či opravu. Tyto ceny jsou dále převedeny do kvalitativní stupnice. Stejný princip oceňování je dodržen pro software a informace. Hodnoty jsou nejčastěji získávány na základě komunikace s vlastníky aktiv.

Metodu lze však zpracovat dvěma způsoby. První možností je k předem ohodnoceným aktivům vypracovat úroveň jednotlivých hrozeb a zranitelností, která se k aktivům vztahují. Tyto ohodnocené zranitelnosti a hrozby se za použití stejné kvalitativní škály zpracovávají do matice, v níž se následně riziko posuzuje. Viz tabulka 3.3.3.1 na straně 24.

V případě, že pro dané aktivum neexistuje hrozba nebo pro aktivum neexistuje zranitelnost, uvažuje se nulové riziko. Úroveň rizika lze určit dle příkladu.
Za předpokladu, že hodnota aktiva je 3 (Asset Value), hrozba pro dané aktivum je vysoká (High) a zranitelnost aktiva je nízká (L), výsledná úroveň rizika bude na škále od 0 do 8 ohodnocena hodnotou 5.

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	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 3.3.3.1:Matice s předem definovanými hodnotami 1

Druhým možným způsobe zpracování je porovnávání úrovně rizika podle pravděpodobnosti scénáře incidentů s jejich dopady na obchodní činnost. Pravděpodobnost scénářů je determinována hrozbou, která může využít zranitelnost s určitou pravděpodobností (viz tabulka 3.3.3.2). Opět uvažujeme hodnocení na škále od 0 do 8.

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Tabulka 3.3.3.2: Matice s předem definovanými hodnotami 2

- *Třídění hrozeb pomocí míry rizika*

Metoda hodnotí výši rizika za pomocí hodnoty následku hrozby pro dané aktivum s pravděpodobností výskytu dané hrozby. Součin těchto hodnot nám pak udává míru rizika. Míry rizika jsou podle své závažnosti dále tříděny v posledním sloupci. Viz tabulka 3.3.3.3 na straně 25.

Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

Tabulka 3.3.3.3: Třídění hrob pomocí míry rizika

- *Stanovení hodnoty pravděpodobnosti a možných následků rizik*

Tato metoda se zaměřuje především na dopady informačně bezpečnostních incidentů a určuje, kterému systému by měla být přisouzena priorita. Posuzují se dvě hodnoty, jak pro aktivum, tak pro riziko, jejichž kombinace udává výslednou hodnotu aktiva.

Aktivům jsou přiřazovány hodnoty na základě nepříznivých následků, které mohou nastat v případě ohrožení aktiva. Pravděpodobnostní hodnota je závislá na zranitelnosti daného aktiva v ohledu na určitou hrozbu. K tomuto hodnocení jsou již zapotřebí scénáře incidentů.

Hodnota aktiva je sečtena s hodnotami všech hrozeb, které s aktivem souvisí, čímž získáme výslednou hodnotu aktiva. Výsledné hodnoty se dále dají sečíst a porovnávat s výsledky jiných systémů (viz tabulka 3.3.3.4).

Asset Value	0	1	2	3	4
Likelihood Value					
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 3.3.3.4: Stanovení hodnoty pravděpodobnosti a možných následků

3.3.3 Hodnocení rizik

S ohledem na posouzení rizik předchozími metodami se v tomto kroku musí zhotovitel rozhodnout, která kritéria budou řešena primárně a která lze řešit druhotně. Stejně tak je nutné brát v potaz skutečnost, že agregace některých rizik může mít mnohem větší následky. Z toho důvodu se doporučuje tato rizika řešit přednostně. Rizika, jež budou řešena druhotně, musí být stále monitorována. V této fázi se musí brát ohled na všechny zainteresované strany společnosti a cíle společnosti. Výstupem tohoto kroku je seznam seřazených rizik podle závažnosti, který nám udává pořadí, v jakém je dobré rizika řešit.

3.4 Ošetření rizik a akceptace rizik bezpečnosti informací

Vstupem pro ošetření rizik je výstup z hodnocení rizik. Na základě seznamu seřazených rizik se vybírá nejvhodnější metoda ošetření, podle předem stanovených kritérií pro uspokojivé řešení. Norma nám nabízí čtyři možné způsoby, jakým lze daná rizika ošetřit:

1) *Modifikace rizika*
2) *Podstoupení rizika*
3) *Vyhnutí se riziku*
4) *Sdílení rizik*

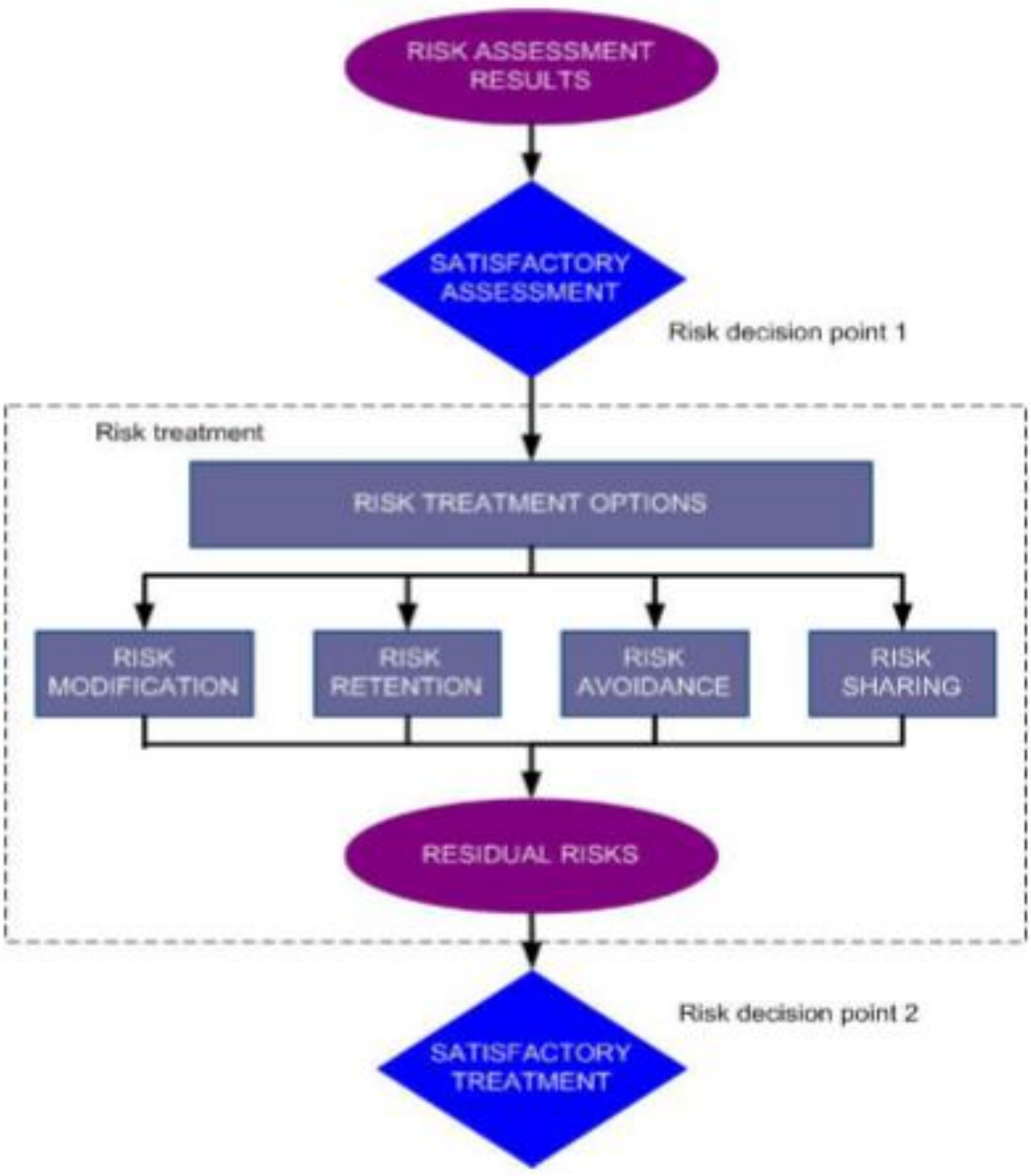
Při ošetřování rizik se především uvažují náklady spojené s aplikací daných metod při ošetřování daného rizika. Obecně platí, že čím větší část jsme schopni metodou pokrýt a ošetřit při relativně nižších nákladech, tím víc bude daná metoda upřednostňována. Oproti této skutečnosti se zvažují benefity plynoucí z ostatních možností.

Cílem volby vhodné metody ošetření je maximální snížení vyhodnocených rizik dle incidentních scénářů při různé pravděpodobnosti výskytu. Nutno dodat, že volba se nemusí vztahovat pouze na jednu metodu ošetření. Společnost se může rozhodnout pro volbu více metod současně. Vhodná kombinace metod může přinést výhody, plynoucí z jejich aplikace, ať už se jedná o snížení nákladů pro danou oblast či zvýšení příjmů díky redukování rizika.

Tento fakt lze pozorovat i při volbě jedné metody. Některé metody jsou schopné ošetřit více rizik zároveň. Avšak benefity jako snížení nákladů, případně zvýšení příjmů, nejsou přímo závislé na počtu ošetřených rizik, nýbrž na povaze daného rizika s jeho vlastnostmi.

Po volbě vhodné metody se sestavuje plán implementace, při němž se klade důraz na znalost veškerých omezení společnosti – jak finančních, časových, organizačních, tak legislativních a mnohých dalších. Tyto faktory nám determinují vývoj plánu implementace s jeho zavedením.

S dokončením plánu ošetření je nutné vyhodnotit, zda ošetření minimalizovala rizika v celém rozsahu. Metody mohou i nemusí riziko ošetřit úplně a je nutné určit zbytková rizika a jejich řešení. V této fázi se doporučuje opětovná aktualizace posouzených rizik s přihlédnutím k řešení daného rizika. V případě, že riziko nesplňuje kritéria přijatelnosti, stanovená společností, je nezbytné další ošetření. V opačném případě bude riziko akceptováno. Výstupem celého procesu je uspokojivé ošetření rizika, viz přiložený Obr. 2.



Obr. 2: Ošetření rizik

3.5 Metody ošetření rizik

V následující podkapitole budou blíže popsány metody ošetření rizik. Stejně jako celá třetí kapitola budou veškeré informace čerpány z [18].

3.5.1 Modifikace rizika

Cílem této metody je změna úrovně rizika. Toho lze dosáhnout pomocí zavedení druhotných opatření, odstranění nefungujících opatření či úpravou stávajících opatření tak, aby úroveň rizika spadala do kategorie akceptovatelných rizik.

V případě volby nových opatření s patřičnou kontrolou, která budou upravovat míru rizika, je důležité dbát na to, aby zvolená opatření splňovala kritéria pro jejich zavedení. Zejména pak časová, finanční, technická provozní, kulturní, etická, legislativní.

Implementace nového nebo modifikovaného opatření musí být důkladně konzultována s vedením společnosti či odpovědnými osobami. V případě, že danou modifikaci není možné jednoduše implementovat, je vhodné provést opětovné šetření jednou z metod ošetření rizik při typovém členění rizika. Riziko pak může být podle typu označeno jako:

a) *Inherentní riziko*
b) *Residuální riziko*
c) *Cílové riziko*

Inherentním rizikem rozumíme riziko bez ošetření. Residuální riziko je takové riziko, které bylo ošetřeno všemi předchozími opatřeními. Cílové riziko je stav, jehož chceme dosáhnout. Jedná se o riziko, jež dosahuje výše, která je společnost akceptovatelná.

3.5.2 Podstoupení rizika

V případě podstoupení rizika se jedná spíše o přístup k výslednému riziku. Jedná se o stav, v němž společnost dané riziko přijme. Nejčastějšími důvody k akceptaci bývá časová a finanční náročnost na zavedení nových opatření.

Podstoupená rizika v tomto případě většinou oscilují okolo hranice přijatelnosti. Může se stát, že podstoupené riziko nabývá vyšších hodnot, toto podstoupení je pak zapříčiněno výše zmíněnými důvody. Důvodů může být i více, nicméně společnost, která se rozhodla akceptovat dané riziko, si musí být vědoma možných následků.

3.5.3 Vyhnutí se riziku

Tento přístup skýtá určitou podobnost s přístupem podstoupení. Především v oblasti nákladů. Společnost si z důvodu nedostatku zdrojů na vývoj či modifikaci opatření pro ošetření daného rizika nemůže dovolit další šetření. Avšak oproti podstoupení rizika sahá tento přístup po radikálním řešení. Aby se společnost vyhnula danému riziku, zastaví veškeré činnosti, které mohou riziko způsobovat. Důvodem bývá fakt, že rizika podléhající tomuto přístupu mnohem více přesahují hranici akceptovatelnosti a jejich následky mohou být kritické.

3.5.4 Sdílení rizik

Tato metoda poskytuje subjektu jistou podporu při zvládání rizik. Část odpovědnosti za zvládání rizika bývá přenesena na jiný subjekt, který se snaží rizika minimalizovat. Toto řešení však nepřináší odklonění dopadu následků rizik. Nicméně existují formy sdílení rizik, kdy je přenesena část zodpovědnosti za následky na dílčí účastníky, kdy výše následku je rozmělněna mezi subjekty dohody. Toto sdílení se však nevztahuje na regulaci a velkou část právních ustanovení. Jedná se spíše o pokrytí finančních ztrát z následků dopadu rizik.

Praktická část

4. Případová studie

Pro praktickou část této práce byla zvolena případová studie společnosti Disk Multimedia, s.r.o. Společnost souhlasila s vypracováním analýzy rizik a zpracováním poskytnutých informací, které budou použity a publikovány v této bakalářské práci.

Veškeré informace budou získány na základě telefonických a osobních schůzek, které bude zprostředkovávat finanční ředitelka Ing. Eva Braunšlegerová, za souhlasu majitele společnosti Libora Dvořáčka.

Analýza rizik bude postupovat podle [18]. Společnost projevila zájem o tuto normu z důvodu porovnání stávajících bezpečnostních opatření s praktikami ISO. Pro případné zvažování budoucí implementace normy ISO 27005.

Společnost je evidovaná v obchodním rejstříku vedeným Krajským soudem v Brně, kde lze o ní získat základní informace, nebo také z [19]:

Datum zápisu: 11. ledna 1999

Obchodní firma: Disk Multimedia, s.r.o.

Sídlo: Boskovice, Sokolská 221/13, PSČ 68001

4.1 Představení a historie společnosti – Disk Multimedia, s.r.o.

Firma DISK Multimedia, s.r.o. působí na českém a slovenském trhu již 17 let. Za tuto dobu si vybudovala rozsáhlou distribuční síť pro prodej audiovizuálních technologií. Společnost zastupuje řadu významných značek. Jejich výrobky dováží z různých zemí nejen v rámci EU. Zabývá se také využitím audiovizuálních technologií a prodejem produktů v rámci větších funkčních celků a systémů, jako jsou nahrávací studia, televizní studia, vysílací místnosti rádií, učebny, soudní síně, divadla apod.

Současně s prodejní činností se zabývá již 14 let vývojem vlastního softwaru na zpracování audia pro hudebníky, divadla, soudy, parlament a další instituce.

Výsledky zmíněného vývoje již byly zúročeny. Software byl rozdělen na několik produktů, které firma DISK Multimedia, s.r.o. prodává jak v tuzemsku, tak v zahraničí.

Úspěchem v rámci vývojově-prodejní činnosti firmy jsou uzavřené kontrakty na dodávky vlastních, zatím softwarových, technologií, několika zahraničním firmám. Vzhledem k dosaženému postavení na trhu, znalosti tržního prostředí, orientaci na poli audiovizuálních produktů a technickým znalostem se firma rozhodla maximálně využít potenciálu vlastního vývojového oddělení a zahájit vývoj, výrobu a prodej vlastních hardwarových zařízení.

V roce 2014 byl dokončen vývoj hardwarového procesoru SceneBox. Nyní se firma zaměří na jeho uvedení do prodeje.

Další aktivitou firmy je vzdělávací činnost. Kurzy společnosti DISK Multimedia s.r.o., v rámci vzdělávací sekce nazvané Deccart, jsou akreditované MŠMT[4] a v rámci jejich konání se mohou klienti naučit lépe využívat prodávaný hardware či software a orientovat se na trhu audiovizuálních technologií.

4.2 Strategie a obchodní cíle

Společnost DISK Multimedia, s.r.o. si klade za cíl nasytit světový trh audiovizuálních technologií kvalitními produkty. V oblasti audia se tedy rozhodla přistoupit také k vývoji nových softwarových i hardwarových produktů.

Strategie výroby nových zařízení je založena na špičkových znalostech pracovníků firmy v oblasti softwarových technologií. Současný prodej softwarových řešení však podstatně ztěžuje fakt, že softwary mohou být napadeny internetovými piráty a snadno nelegálně šířeny. Na základě rozboru trhu bylo nově přistoupeno k vývoji vlastního specializovaného hardwaru, bez něhož není možné software využívat.

Kooperace s renomovanými zahraničními firmami dokládají skutečnost, že software, vyvinutý v rámci vývojového oddělení firmy, dosahuje vysokých kvalit. Výhodou bude cena specializovaného zařízení, která by měla být mnohem nižší než cena kompletního řešení s počítačem.

V zásadě si firma nejvíce zakládá na postupném obsazení větší části zahraničního trhu touto novinkou. Nutné tedy je, aby se prodejci naučili velmi plynule a účinně přesunout z českého trhu na trhy zahraniční a připravit pro produkt nejlepší možnou startovací pozici. Pakliže budou prodeje

[4] MŠMT - Ministerstvo školství mládeže a tělovýchovy

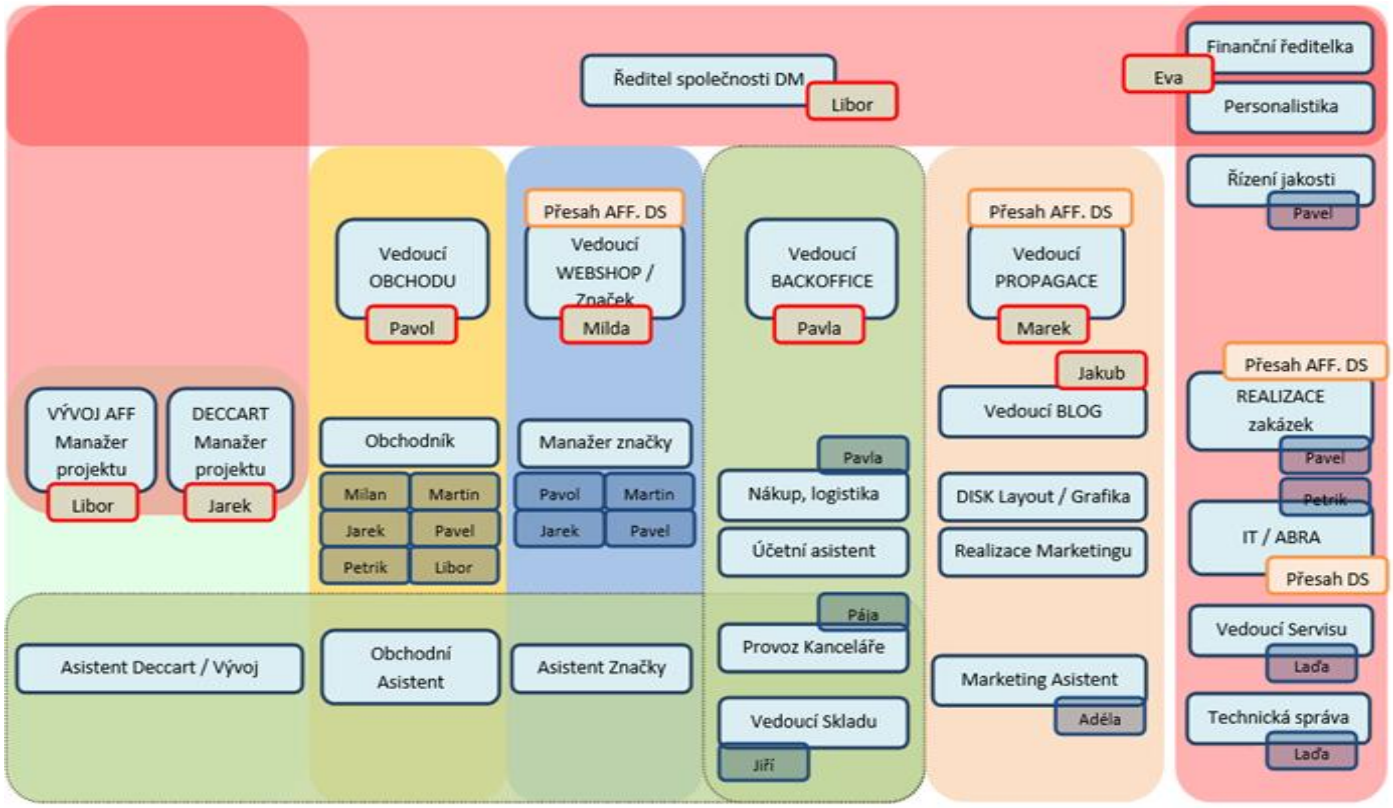
dosahovat dostatečné kapacity, plánuje vedení společnosti vytvoření nových pracovních míst. Firma má tedy jasně stanovený cíl podnikání, ke kterému stabilně směřuje.

Výroba hardwaru bude probíhat v rámci Jihomoravského kraje, tedy v České republice. Konkrétně se jedná o firmy z Brna, Boskovic a Jedovnic. Blízkost měst, v jejichž rámci budou vyráběny části hardwaru, umožňuje osobní kontrolu výroby a případné flexibilní úpravy výrobních procesů či jednotlivých detailů na vyráběných částech. Jedním z cílů je dlouhodobá spolupráce firem v regionu.

4.3 Organizační struktura společnosti

Každý výše uvedený pracovník může nařídit či vyžadovat práci od podřízeného kolegy či činnosti jím vykonávané uvedené níže. Hodnotí jeho práci, předložené výsledky a může se vyjadřovat k jeho odměnám. Všichni se vyjadřují k procesům a podílí se na jejich nápravě.

Jména pracovníků jsou uváděna tak, jak byla poskytnuta společností, a pro zachování jejich soukromí a totožnosti jsou uváděna pouze křestní jména. Žlutá pole s vysvětlivkami „*Přesah*“ chápejme jako propojení činností s dceřinou společností.



Obr. 3: Stručný popis organizační struktury Disk Multimedia, s.r.o.

4.4 Zaměstnanci

V současné době společnost zaměstnává 15 pracovníků na HPP, 5 pracovníků na DPP a 5 externích pracovníků na základě mandátní smlouvy. Jejich jednotlivé funkce a pozice budou popsány níže v následujícím výčtu, který čerpá z job listů poskytnutých generálním ředitelem Liborem Dvořáčkem. Názvy pozic jsou upraveny dle potřeb firmy, jejich podoba nebyla upravována.

- *Ředitel společnosti:*

Ředitel zodpovídá za veškerou obchodní strategii společnosti, stanovuje rozpočty na nadcházející období, upravuje interní procesy a hledá nové klíčové partnery.

- *Vedoucí obchodu:*

Zodpovídá za realizaci obchodní strategie a vytváří návrhy, které slouží jako podpora rozhodování ředitele společnosti. Současně zodpovídá za činnost obchodníků.

- *Vedoucí webshopu:*

Tato pozice zodpovídá a má na starost chod internetového obchodu a kvalitu obsahu webshopu.

- *Vedoucí backoffice:*

Zodpovídá za veškeré kancelářské činnosti a procesy. Současně zodpovídá za nákup spojený s touto pozicí a dohlíží na asistenty.

- *Vedoucí propagace:*

Vedoucí propagace se stará o kvalitní prezentaci společnosti a realizaci marketingu.

- *Vedoucí blogu:*

Tento vedoucí zodpovídá za obsah internetových blogů firmy a navazuje na marketingovou činnost.

- *Obchodník:*

Nejdůležitější pozice. Firma klade největší důraz na tyto pracovníky. Jejich úkolem je zajištění stálého prodeje se ziskem.

- *Manažer značky:*

Tato pozice má zodpovědnost za veškerou agendu spojenou s přidělenou značkou. Zodpovídá za zisk z přidělených značek, spolupracuje s obchodníky.

- *Realizace:*

Realizace má zodpovědnost za realizaci zakázek a projektů s nimi spojených.

- *Deccart:*

Pracovník v této pozici je zodpovědný za vzdělávání v oblasti nových produktů a současně je projektovým manažerem stejnojmenné značky.

- *Vývoj:*

Zodpovídá za vývoj nových produktů a prodej produktů vývojového střediska. Kooperuje s ostatními pozicemi.

- *Vedoucí servisu:*

Vedoucí zodpovídá za činnost servisních služeb a zpracovává reklamace.

- *Nákupčí/Logistika:*

Tato pozice v sobě kloubí zodpovědnost za nákup zboží a dohlíží na logistiku. Současně dochází ke kooperaci s manažery značek.

- *Vedoucí skladu:*

Vedoucí skladu zodpovídá za stav skladových zásob a veškeré procesy spojené s příjmem a expedicí.

- *Backoffice:*

Touto pozicí se rozumí veškerá kancelářská, účetní, personální, správní a IT činnost.

4.5 Produkty a služby

Společnost se zaměřuje na nákup a distribuci zboží zahraničních značek spojených s audiovizuální technikou. Jedná se především o značky: RODE, AKAI, M-AUDIO, PRESONUS, GIBSON, YAMAHA, NUMARK, NATIVE INSTRUMENT a SIBELIUS.

Současně společnost nabízí služby spojené s instalací, vybavováním studií a nahráváním, na které navazuje školení v oblasti záznamu a zpracování zvuku. Mimo jiné společnost nabízí servisní služby spojené s prodávanými značkami.

Nově se společnost zaměřuje i na prodej licencí k softwarové podpoře v podobě licenčních čísel, přičemž společnost soustavně vyvíjí nové softwarové produkty a hardwarové doplňky k těmto produktům, jež se snaží dostat do povědomí jak na českém, tak i zahraničním trhu.

4.6 Dodavatelé a outsourcing

Dodavatelé produktů v podstatě kopírují názvy značek, jež společnost distribuuje. Tyto značky byly již zmíněny v předchozí podkapitole (4.5).

Společnost využívá externích služeb obchodních pracovníků, kteří slouží společnosti jako podpora prodeje. Tito pracovníci pracují na základě mandátní smlouvy s podepsanou dohodou o zákazu úniku informací.

Pro zajištění logistiky využívá společnost služeb externích dopravců, jejichž úkolem je přeprava zboží k zákazníkům a dodávka zboží s celním odbavením do skladových prostor společnosti.

Další skupinou externích služeb jsou lektoři, vývojáři a antipirátské společnosti. Lektoři zajišťují podporu střediskům školení. Vývojáři, pracující na dohodu o provedení práce, jejíž část zahrnuje zákaz úniku informací, vypomáhají na projektu DECCART. Antipirátské společnosti se zaměřují na kontrolu využití prodaných licencí k softwarové podpoře.

Společnost využívá externích služeb pro dodávky plynu, elektřiny, pojištění podnikatelských rizik, zpracování elektroodpadu, o němž pravidelně společnost informuje ve formě výkazů.

4.7 Obchod a zákazníci

Prodejní činnost společnosti se soustřeďuje na maloobchodní a velkoobchodní řetězce, přičemž prodej drobným zákazníkům je lokalizován v e-shopu společnosti, kde je možné skrze katalog a objednávkový formulář nakoupit zboží. Internetový obchod zákazníkům poskytuje možnost výběru platby a doručení. Zákazník může využít platby předem, přičemž zboží je zasláno na dobírku či dodavatelskou službou bez dobírky, nebo osobní odběr s platbou na pokladně.

Hlavními zákazníky Disk Multimedia jsou dealerské společnosti, pro něž je určený objednávkový dealerský systém. Přepravu objednaného zboží těmto zákazníkům zajišťují smluvní přepravní společnosti. Mezi hlavní dealerské odběratele patří: Alza.cz a.s., AUDIO PARTNER s.r.o., AudioMaster s.r.o., Profi-DJ s. r. o. a MUZIKER s.r.o.

Zvláštní skupinou zákazníků jsou zahraniční klienti, kteří vesměs využívají e-shop pouze k nákupu licencí softwarové podpory produktů distribuovaných značek. Nákup licence pro zahraniční klienty je zprostředkován pomocí služby PAYPAL.

V uplynulých letech společnost prodejem audiovizuálních produktů vykázala následující obraty: 2013 - 56.507 tis. Kč, 2014 - 62.572 tis. Kč, 2015 - 65.344 tis. Kč

4.8 Konkurence

Vzhledem k tomu, že společnost dováží k prodeji zahraniční značky na základě dohody o výhradním zastoupení na českém a slovenském trhu, tak je konkurence velmi omezená. Exkluzivita od výrobce ale není nikdy jistá. Může přijít distribuční firma, která dosud od společnosti Disk Multimedia odebírala určitou značku a nabídne dodavateli, jehož zboží Disk Multimedia distribuuje, vyšší objem prodeje nebo jinou výhodu prodeje na českém trhu a tím získá exkluzivitu tato firma.

Dá se tedy říct, že potencionálními konkurenty jsou vlastně nejsilnější odběratelé: Alza.cz a.s., AUDIO PARTNER s.r.o., AudioMaster s.r.o., Profi-DJ s. r. o. a MUZIKER s.r.o.

Významným konkurentem do budoucna jsou mezinárodní obchodní domy a e-shopy typu Thomann Musikhaus, které vynechávají dealerskou složku prodejního systému, a prodávají přímo koncovému uživateli. V tomto případě ztrácí velkoobchod téměř smysl.

4.9 Kritické procesy společnosti

4.9.1 Nákup zboží

Proces nákupu zboží na sklad začíná ve chvíli, kdy informační systém upozorní na nedostatečný stav zboží na skladě. Informace o stavu skladu jsou aktualizovány vedoucím skladu na základě průběžného monitorování a inventarizace. Hranice pro upozornění je stanovená obchodním plánem a strategií společnosti.

Existují však i další možnosti, popisující zvláštní situace, za kterých může docházet k nákupu. Jedná se o zavádění novinky na trh nebo koupě specifického zboží dle zakázky. Ve všech případech o nákupu rozhodují obchodníci, kteří se starají o jednotlivé značky či zakázky a sledují stav jejich zásob.

Proces je lokalizován v prostorách kanceláří společnosti v Sokolské ulici v Boskovicích, případně může být ve zvláštních případech přenesen na homeoffice díky možnosti vzdáleného přístupu do systému. Proces se dále přesouvá na dodavatele, který zajišťuje přepravu zboží, případně je přeprava přenesena na přepravní partnery společnosti. Doručené zboží je dále vyskladněno do skladu ve Svěrákově ulici v Boskovicích, kde vedoucí skladu zodpovídá za převzetí a kontrolu. Uskladnění zajišťují podřízení pracovníci vedoucího skladu.

Platba dodavatelům může probíhat dvěma způsoby. Pro zahraniční dodavatele je typická platba na fakturu s 30denní splatností, kdy uhrazení faktury je zajištěno bankovním převodem. Druhou možností je platba doplňkové objednávky na fakturu s platbou předem, dobírkou či převodem.

K tomuto procesu jsou nutné informace jako: stav zásob v informačním systému, stav zásob na skladě (inventarizace), identifikace dodavatele (adresa, mail, telefon, bankovní údaje), hodnota dodávky, termíny odeslání a dodání zboží, dostupnost a nabídka dodavatele, ceníky přepravy, informace o přepravních společnostech.

Za specifikaci objednávky je zodpovědný obchodník dané značky, za doručení objednávky nese zodpovědnost asistentka obchodu, za přepravu zboží je zodpovědná asistentka prodeje, za propuštění zboží do volného prodeje celní správou v případě nákupu zboží z třetích zemí nese odpovědnost asistentka prodeje, za správné naskladnění do systému nese odpovědnost asistentka obchodu, za správné přijetí a zaúčtování dodavatelské faktury do systému nese odpovědnost ekonom a za včasnou a správnou úhradu faktury nese odpovědnost také ekonom společnosti.

Proces může skončit několika možnými způsoby:

a) *Dodavatel dodá zboží v požadovaném množství, ceně a kvalitě*
b) *Dodavatel je schopný pokrýt objednávku jen částečně*
c) *Dodavatel dodá zboží nekompletně chybou expedice u dodavatele*
d) *Přepravní služba předá zboží ve správném termínu a v odpovídající kvalitě*
e) *Přepravní služba předává zboží s poškozenými obaly a s poškozeným zbožím*
f) *Přepravní služba dodá jen část dodávky*
g) *Dodavatel dodá zboží s nesprávnou cenou*

4.9.2 Prodej zboží

Proces prodeje zboží zahajuje poptávka zákazníka. Případně může prodej zahájit obchodník přímou komunikací s klientem. Zákazník či dealer, nejčastěji skrze e-shop nebo dealerský systém, vytvoří objednávku na základě katalogu zboží, ceny, slevových akcí. V objednávce u specifikace zboží zvolí způsob přepravy a platby. Položky přepravy nabízí možnosti jako: pošta, PPL, DHL, osobní odběr. Možnosti úhrady zahrnují: dobírku, platbu předem, platební kartou, hotově. Hlavní dealeři mají podmínky ošetřené smluvně, dodání přepravní službou a platbu převodem s třicetidenní splatností. Menší dealeři bez smlouvy musí využít platby předem nebo dobírku. Podmínky plateb a dodání se zadávají do systému ABRA, konkrétně do adresy zákazníka. Ve výjimečných situacích je možné objednávku řešit telefonicky, přímým kontaktem či emailově.

Načtení objednávky zákazníka do systému zajišťuje asistentka obchodu u koncových zákazníků a obchodník u dealerů. V objednávce v systému je důležité vedle specifikace zboží a adresy zákazníka zadat i správnou cenovou hladinu a podmínky plateb a dodání. Z objednávky se pak tyto údaje automaticky generují do dodacího listu a faktury. V adrese zákazníka je povinný údaj telefonický kontakt, který požadují přepravní služby.

Z objednávky obchodník nebo jeho asistentka vygeneruje dodací list, který vytiskne na tiskárnu ve skladě ve Svěrákové ulici. Dodací list slouží skladovému pracovníkovi k přípravě konkrétního zboží k zaslání za podmínek uvedených na dodacím listě, které se automaticky vygenerovaly z objednávky. Z vybraného zboží načte čárový kód a zadá sériová čísla do systému. Zboží zabalí do krabice. V systému vygeneruje fakturu. Fakturu zašle elektronickou cestou zákazníkovi.

V systému vygeneruje skladový pracovník z naimplementované aplikace přepravní služby průvodní přepravní doklady buď s dobírkou, nebo bez dobírky. Systém zásilce vygeneruje číslo, pod kterým je pak zásilka sledována. Zboží vyzvedne přepravní služba, která do firmy jezdí denně objednávky vyzvedávat.

Přepravní služba zásilku předá zákazníkovi. V případě dobírky řidič vyzvedne hotovost, předá na centrále přepravky a z centrály se peníze posílají na bankovní účet společnosti.

Pokud si zákazník zvolí osobní odběr, tak skladový pracovník připraví zboží dle dodacího listu, vygeneruje fakturu a po příchodu zákazníka na ul. Svěrákova mu předá zboží, doklady a převezme hotovost nebo využije bankovní terminál umístěný ve skladových prostorech a provede úhradu platební kartou. Hotovost vybranou ve skladových prostorech předává skladový pracovník do centrální pokladny na ul. Sokolská a poté vkládá do banky asistentka obchodu.

Konkrétní větší zakázky se řeší specificky a individuálně. Osobní kontakt při tvorbě nabídky, po potvrzení zájmu od zákazníka se sepíše obchodní smlouva, která obsahuje specifikaci zboží, platební a dodací podmínky. Z této smlouvy konkrétní pracovník, který má tuto zakázku na starosti, vygeneruje objednávku v systému, kam zanese všechny podmínky smlouvy.

Z objednávky se vygeneruje dodací list, podle kterého skladník nachystá zboží, čtečkou převede čárové kódy, sériová čísla do systému a vygeneruje fakturu zákazníkovi. Dále všechny doklady a zboží předá obchodníkovi, ten zboží naloží do firemního automobilu a zaveze k instalaci na adresu zakázky. Zboží tam vyloží, nainstaluje a předá doklady k podpisu o převzetí. U zakázek je

smluvně sjednaná určitá výše zálohy na účet a pak splatnost faktury, většinou 14denní, na účet společnosti.

V tomto procesu především figurují informace jako stav zásob a dostupnost zboží v informačním systému, identifikace zákazníka (adresa, email, telefon), ceník a cenové podmínky, specifikace zboží na e-shopu, podmínky a možnosti nákupu na e-shopu. Kooperuje se zákazníkem, přepravní službou, s bankami, s finančním úřadem, s externím právníkem pro vymáhání pohledávek a přihlašováním do insolvenčního řízení.

Úhradu zboží sleduje ekonomické oddělení i obchodníci. Po 4 dnech po splatnosti systém ABRA automaticky zasílá upomínky zákazníkům s neuhrazenými fakturami. Po 10 dnech po splatnosti asistentka obchodu zasílá dvě až tři upomínky na e-mail. Dále se zasílá doporučený dopis s dodejkou s upozorněním pro obchodníka.

Průměrně se naleznou 3 neplatiči za rok, jejichž případy jsou předány právníkovi společnosti. Úspěšnost vymáhání pohledávek se v těchto případech odhaduje na 30 %.

Proces může skončit několika možnými způsoby:

a) *Zákazník obdrží zboží v požadovaném množství, ceně, kvalitě a zboží uhradí*
b) *Zákazník obdrží zboží v požadovaném množství a ceně, ale zboží vrátí ve čtrnáctidenní lhůtě*
c) *Zákazník obdrží zboží nekompletně chybou logistiky – tedy skladového pracovníka*
d) *Zákazník obdrží zboží poškozené vinou přepravní služby*
e) *Zákazník obdrží zboží v požadovaném množství, ceně a kvalitě, ale zboží neuhradí*
f) *Zákazník obdrží zboží s nesprávnou cenou*

5. Analýza rizik – Disk Multimedia, s.r.o.

Tato část práce bude vytvářet tabulkové a seznamové výstupy, které jsou dostupné z přílohy této práce. Jednotlivé texty se odkazují na přílohy, kde je vysvětlený i jejich obsah a postup tvorby. Pro správné porozumění této kapitoly je vhodné využít těchto výstupů.

5.1 Stanovení kontextu

Pro porozumění fungování společnosti se v této práci bude uvažovat základní představení společnosti, které předchází této kapitole. Dodatečně budou získávány informace na základě potřeby analýzy, která si klade za cíl minimalizaci rizik a soulad navrhnutých opatření s požadavky společnosti.

5.1.1 Základní kritéria, rozsah a hranice

Společnost se v současné době zaměřuje především na distribuční činnost a obchod z ní plynoucí. Z toho důvodu se společnost vyslovila, že by ráda oblast zkoumání zaměřila především na nákup a prodej zboží společnosti Disk Multimedia. V práci nebude uvažována činnost dceřiné společnosti Disk Systems, která se zaměřuje výhradně na vývoj a distribuci softwaru. Dále se nebudou uvažovat pozice ani lokality, jež přímo nesouvisí s distribucí a prodejem Disk Multimedia.

Pomyslnou hranicí a zkoumání bude stav, kdy procesy s touto oblastí spojené budou ohroženy na své funkčnosti, což může vést ke ztrátě ve smyslu finanční újmy či narušení plnění cílů, závazků, chodu společnosti a poškození dobrého jména firmy. Základní kritéria pro hodnocení byla vybrána z návrhů, které jsou doporučeny v [18] a mají pro společnost význam.

5.1.2 Organizace řízení rizik bezpečnosti informací

Konzultační činnost a zodpovědnost za řízení je delegována na finanční ředitelku Ing. Evu Braunšlegerovou, která bude v průběhu analýzy poskytovat potřebné informace k analýze a dále informovat o průběhu generálního ředitele Libora Dvořáčka a stejně tak pracovníky společnosti, již budou specifikovat informace o svých činnostech a dále spolupracovat při postupu analýzy.

Zodpovědnost za akceptaci a zvážení postupů s využitými metodami je také delegována na finanční ředitelku Ing. Braunšlegerovou, která bude přebírat výstup z analýzy rizik a dále hodnocení konzultovat s Liborem Dvořáčkem.

Výsledné rozhodnutí o akceptaci opatření ve smyslu ošetření rizik bude mít generální ředitel, jenž bude výstupy analýzy hodnotit a na základě nich se rozhodovat o modifikaci či zavedení opatření ve stávajících procesech, pročež rozhodovací kompetence má výhradně on.

5.2 Identifikace Rizik

5.2.1 Identifikace aktiv a jejich hodnocení

K identifikaci sloužily především popisy dvou kritických procesů, z nichž se vycházelo. Na základě prvotního porozumění procesů byl vypracován seznam všech aktiv, která v procesech mohou vystupovat. Tento seznam byl dále upraven podle potřeby společnosti. Aktiva, která společnost považovala za nejméně důležitá pro analýzu, byla vyřazena a chybějící aktiva doplněna. U každé položky byla konzultována její důležitost, funkčnost a ostatní vlastnosti.

Následně byla aktiva rozčleněna do podskupin. Členění vycházelo z [18] na primární a podpůrná. Forma hodnocení byla zvažována dle časových možností a účelu. Z těchto důvodů vedení společnosti přistoupilo na kvantitativní hodnocení využívající následující stupnice:

1) *Velmi nízké - Minimální závislost, nenaruší chod procesů, náhrada možná do několika dnů*
2) *Nízké - Existence závislosti, částečně naruší chod procesů, náhrada možná do jednoho týdne*
3) *Střední - Přímá závislost, naruší chod procesů, náhrada možná do dvou týdnů*
4) *Vysoké - Vysoká závislost, silně naruší chod procesů, náhrada možná do měsíce*
5) *Kritické - Extrémní závislost, ochromí procesy*

Pro určení hranic bylo využito kritérií nabídky ISO 27005, kdy jednotlivé body byly konzultovány a rozhodovalo se o jejich výběru, podle nichž byl sestaven i výsledný katalog aktiv:

1) *Porušení právních předpisů, nařízení*
2) *Snížení hodnoty výkonnosti procesů*
3) *Ztráta dobrého jména, negativní vliv na pověst společnosti*
4) *Porušení spojená s důvěrnými informacemi*
5) *Ohrožování osobní bezpečnosti*
6) *Finanční ztráta*
7) *Narušení obchodních aktivit*
8) *Neschopnost poskytovat službu*
9) *Narušení vnitřního provozu*
10) *Neschopnost plnit zákonné povinnosti*
11) *Neschopnost plnit smluvní závazky*
12) *Ztráta zboží*
13) *Ztráta konkurenční výhody*
14) *Oslabení vyjednávací schopnosti*

Podle součtů kritérií, do nichž aktiva zasahovala, byla stanovena stupnice hodnocení o stejném počtu stupňů, jako tomu bylo u hodnocení aktiv:

a) *Velmi nízké – 0 až 1 kritérium*
b) *Nízké – 2 až 3 kritéria*
c) *Střední – 4 až 5 kritérií*
d) *Vysoké – 6 až 7 kritérií*
e) *Kritické – 8 až 14 kritérií*

Na základě získaných informací a ohodnocení byl poté vytvořen prvotní katalog aktiv, který v sobě zahrnoval členění aktiv podle typu, kategorie, názvu aktiva s příslušným hodnocení, podle zvolené číselné škály a s ohodnocením dle kritérií.

5.2.2 Identifikace hrozeb

Následně bylo nutné katalog doplnit o seznam hrozeb, jež aktivům hrozí. Předlohou nám byl výčet z anexe C, z [18]. Jednotlivé hrozby byly modifikovány podle potřeby tak, aby nejvíce odpovídaly společnosti a jejím aktivům. Hrozby byly rozčleněny do základních kategorií:

1) *Fyzické poškození*
2) *Přírodní události*
3) *Ztráta základních služeb*
4) *Ohrožení informací*
5) *Technická selhání*
6) *Neoprávněná činnost*
7) *Ohrožení funkčnosti*

Po rozdělení hrozeb do kategorií bylo potřeba určit původ hrozby. Z důvodu předchozího kvalitativního hodnocení bylo potřeba zvolit takový způsob třídění, který by odpovídal potřebám kvalitativní metody. K tomu nám posloužilo jednoduché základní značení pomocí písmen:

1) *A = Náhodný – Vznik hrozby je náhodný*
2) *D= Úmyslný – Hrozba vznikla úmyslnou činností*
3) *E= Přírodní – Hrozba vznikla působením přírodních vlivů*

5.2.3 Identifikace stávajících opatření

Pro identifikaci stávajících opatření pro zamezení hrozeb byla nutná konzultace. Aby se zamezilo nejasnostem a zajistila se dostatečná efektivita práce při zkoumání stávajících opatření, byl vytvořen modifikovaný katalog hrozeb, na nějž budou opatření navazovat.

Při tvorbě tohoto katalogu byla využita agregace. Ke skupinám hrozeb byly přiřazeny skupiny aktiv, jež mohou být ohroženy hrozbami z dané kategorie. Pro jednotlivé skupiny aktiv byla nalezena stávající opatření, která společnost aplikuje. Účelem tohoto katalogu bylo přezkoumání stávajících opatření a zabránění redudance při tvorbě nových opatření v pozdější fázi analýzy.

Jednotlivá opatření byla dále ohodnocena na základě kvalitativního hodnocení, pomocí písmen V, Z a N, vycházející z doporučení [18]:

a) *V= Vyhovující opatření*
b) *Z= Opatření je třeba zlepšit*
c) *N= Opatření je nevyhovující*

Výstupem byl katalog opatření, který je možné nalézt v příloze pod stejnojmenným názvem. Katalog v sobě slučuje vlastnosti předchozích výstupů.

5.2.4 Identifikace zranitelností

Při identifikaci aktiv jsme normou ISO 27005 nabádáni k zvážení zranitelností, jež daná aktiva mohou mít. V tomto kroku je třeba využít předchozích katalogů a dřívějších zamyšlení k sestavení výčtu zranitelností ve vztahu k aktivům, hrozbám a opatřením. Z toho důvodu došlo k rozhodnutí, že nejlepším možným způsobem sestavení seznamu zranitelností bude další modifikace předchozích katalogů s přihlédnutí k výčtu zranitelností, jenž nám je nabízen v [18].

Výstupem tohoto kroku je modifikovaný katalog zranitelností navazující na předchozí katalog opatření. A druhý přehledový katalog kategorizovaný podle své povahy, využívající doporučené členění podle oblastí dle [18].

5.2.5 Identifikace následků

Pro identifikaci následků jednotlivých hrozeb bylo nutné sestavit nové katalogy. Katalogy využily předchozích modifikací. Výčty aktiv byly převzaty z katalogu opatření, kde byla aktiva tříděna podle kategorie hrozeb, jež na ně mohou působit. Aktiva byla dále agregována podle typu, abychom usnadnili identifikaci.

K těmto podskupinám byly ve sloupcích přiřazeny hrozby z jednotlivých kategorií hrozeb. Na závěr byl přiřazen i sloupec opatření, pro lepší určení souvislostí.

Pro každou kategorii hrozeb byl vytvořen samostatný katalog následků pro lepší orientaci a jednoduší sestavování scénářů. Jednotlivé katalogy nesou v názvu označení kategorie hrozeb.

Ve chvíli, kdy byly dokončeny katalogy, bylo nezbytné diskutovat nad scénáři, které odpovídaly naplnění jednotlivých hrozeb. Z těchto scénářů se odvodily následky pro každou agregovanou skupinu aktiv.

Při posuzování následků se zjistilo, že dopad jedné hrozby bude mít mnohem větší rozsah, než se zpočátku předpokládalo. Byla tak odhalena silná závislost s vazbami mezi jednotlivými aktivy. Můžeme tedy tvrdit, že dopad na jednu skupinu aktiv ohrozí i ostatní skupiny z většiny případů. Tento jev lze objasnit velkou koncentrací aktiv na jednom místě a nedostatku náhradních řešení.

Díky podobnosti následků při posuzování scénářů v tuto chvíli není možné zcela jednoznačně určit, která z hrozeb bude pro společnost představovat největší ohrožení. Pro lepší porozumění bude potřeba následná analýza doposud zformulovaných výstupů.

5.3 Analýza rizik

Po seznámení se se společností, pochopení jejich procesů a sestavení jednotlivých katalogů je možné přejít k samotné analýze výstupů. V souvislosti s nemožností jednoznačného určení nejkritičtějších míst bude nutné další zkoumání a hodnocení.

V tuto chvíli je nutné zvolit nejvhodnější metodu stanovení míry rizik a posuzování následků s pravděpodobností incidentů. Vzhledem k rozsáhlosti katalogů, záměru společnosti s analýzou by se mohlo zdát, že nejvhodnější volbou metody bude přehledové posouzení. Avšak z důvodu podobnosti dosavadních výstupů musíme volit takovou metodu, která dokáže identifikovat ty nejzávažnější rizika s ohledem na současné výstupy.

Z toho důvodu jsme se s vedením společnosti shodli na volbě detailního posouzení rizik pomocí matice s předem definovanými hodnotami. Forma tabulkového zpracování vycházela z ukázky uvedené v této práci, viz *Tabulka 3.3.3.2*.

Při sestavování nových katalogů pro posouzení míry rizik bylo domluveno, že míra rizika bude stanovená pro jednotlivá aktiva, abychom tak docílili lepšího pochopení vztahů mezi aktivy a hrozbami na ně působícími.

5.3.1 Posuzování následků a pravděpodobnosti incidentů

Nežli však bylo možné začít s posuzováním míry rizik, bylo potřeba zvolit nové stupnice pro hodnocení pravděpodobnosti incidentů a jejich následků. Stejně jako v předchozích hodnoceních jsme užili kvalitativního přístupu, abychom zachovali strukturu analýzy a mohli jsme maximálně využít předchozích výstupů.

Při identifikaci aktiv byla využita pětistupňová škála. Z důvodu zachování podobnosti hodnocení, sestavili jsme stupnici o stejném počtu stupňů. Nově vzniklá stupnice pravděpodobnosti byla opatřena stručným popisem, jenž nám ulehčoval chápání pravděpodobnosti výskytu. Popis udává pravděpodobnost, s níž se daný incident teoreticky uskuteční v určitém časovém intervalu. Při usuzování tak bylo možné vycházet z předchozích zkušeností společnosti. Výsledná stupnice měla tuto podobu:

- *1 – Velmi nízká - Pravděpodobnost výskytu v intervalu 4 a více let*
- *2 – Nízká – Pravděpodobnost výskytu v intervalu jednoho roku*
- *3 – Střední – Pravděpodobnost výskytu v intervalu jednoho měsíce*
- *4 – Vysoká – Pravděpodobnost výskytu v intervalu jednoho týdne*
- *5 – Extrémní – Pravděpodobnost výskytu v intervalu několika dnů*

V tuto chvíli zbývalo sestavit ještě stupnici hodnocení následků na daná aktiva, abychom dosáhli sestavení matice s předem definovanými hodnotami, kterou nám předkládá [18] ve své anexi. Rozhodli jsme se sestavit matici o stejném rozsahu, z toho důvodu naše stupnice měla tuto podobu:

- *1 – Velmi nízký*
- *2 – Nízký*
- *3 – Střední*
- *4 – Vysoký*
- *5 – Extrémní*

Po sestavení těchto stupnic bylo již možné sestavit matici a katalog pro posuzování míry rizik. Pro sestavení katalogu jsme užili třídění hrozeb podle jejich charakteru. Každý list katalogu obsahuje všechny hrozby, jež mohou z dané skupiny působit na aktiva. Výčet aktiv byl použit z původního katalogu i s jejich hodnocením, což nám umožnilo pozorovat při posuzování rizik, zda se jedná o kritická aktiva společnosti, či nikoliv. K hodnocení aktiv byly dále přidány sloupce hodnocení následku, pravděpodobnosti incidentu a výsledné hodnocení rizika.

5.3.2 Stanovení míry rizik

Abychom mohli posuzovat jednotlivé míry rizika, bylo zapotřebí sestavit již dříve zmíněnou matici s předem definovanými hodnotami. Naším cílem bylo sestavit matici, která by odpovídala ukázce z ISO/IEC 27005.

Díky volbě stejného počtu stupňů hodnocení bylo sestavení naší matice velmi jednoduché. Horní okraj matice tvoří pravděpodobnost s jejím počtem stupňů. Její levý okraj byl doplněn o stupně hodnocení následků, které označujeme v naší matici jako dopad.

V matici tak existuje 0 až 8 stupňů pro posouzení míry rizika. Tyto stupně nám protkali celou síť matice a utvořili hranice pro rozlišení závažnosti rizik. Hranice rozčlenily matici na tři části. Tyto části jsme definovali jako:

- **Pole (0-2) – Nízká míra rizika:**
  Tyto hrozby nemají větší následky a jejich výskyt je velmi nepravděpodobný.
- **Pole (3-5) – Střední míra rizika:**
  Tyto hrozby mohou ohrozit procesy, jejich výskyt není nepravděpodobný.
- **Pole (6-8) – Vysoká míra rizika:**
  Tyto hrozby mohou kriticky ohrozit procesy, jejich výskyt je pravděpodobný.

Naší cílovou skupinou se tak stala rizika, která se nacházela v poli 6-8. Tedy všechna rizika hodnocena číslem 6 a více. Tato rizika považujeme za kritická, a proto se budeme snažit je nalézt a vytvořit pro ně patřičná opatření, jež by dokázala těmto rizikům předcházet a žádoucím způsobem je ošetřit. Naše výsledná matice má tuto podobu:

	Pravděpodobnost	Velmi nízká	Nízká	Střední	Vysoká	Extremní
Dopad	Velmi nízký	0	1	2	3	4
	Nízký	1	2	3	4	5
	Střední	2	3	4	5	6
	Vysoký	3	4	5	6	7
	Extrémní	4	5	6	7	8

Tabulka 5.3: Matice s předem definovanými hodnotami

Při posuzování rizik jsme postupovali následovně. Nejprve se určila pravděpodobnost, s jakou se naplní hrozba. Tato pravděpodobnost se posuzovala na základě předchozích znalostí společnosti. Abychom zabránili větší míře subjektivity, konzultovali jsme hodnoty s osobou, jež byla pověřená řízením analýzy rizik ve společnosti. Při hodnocení se bral především ohled na minulé zkušenosti firmy.

Následně se ohodnotily následky na dané aktivum. Následek byl často nutný vnímat v širších souvislostech. Z toho důvodu se stávalo, že následek jedené hrozby markantně navyšoval hodnoty následku jiných aktiv. Vycházeli jsme především z incidentních scénářů. V tuto chvíli už bylo možné pomalu pozorovat širší souvislosti.

Po získání těchto hodnot zbývalo pouze vypočítat z matice s předem definovanými hodnotami výsledek. Postup si uvedeme na příkladu.

Uvažujme hrozbu „*Krádež informačních zařízení a dokumentů*“ z čtvrtého listu přílohy posuzování míry rizika. Pravděpodobnost, že se tato hrozba naplní, je stanovena s hodnotou 3. Aktivum „Know-how“ v případě naplnění této hrozby ponese následek v uvažované hodnotě 4.

Od uvažované hodnoty pravděpodobnosti 3 nalezneme v horním okraji odpovídající popis. Hodnota tři je ve stupnici pravděpodobnosti definována jako *„Střední“*. Pro hodnotu následku 4 najdeme v levém sloupci matice odpovídající popis. V stupnici hodnocení následků je hodnota 4 označena jako „Vysoký“. Pokud tyto dva body spojíme pomocí vertikální a horizontální přímky, jejich průsečík bude udávat výslednou hodnotu rizika. Tento postup lze sledovat na níže přiloženém obrázku.

	Pravděpodobnost	Velmi nízká	Nízká	Střední	Vysoká	Extremní
Dopad	Velmi nízký	0	1	2	3	4
	Nízký	1	2	3	4	5
	Střední	2	3	4	5	6
	Vysoký	3	4	5	6	7
	Extrémní	4	5	6	7	8

Obr. 4: Postup určení rizika z matice s předem definovanými hodnotami

Výsledné hodnoty byly následně zaznamenány do katalogu. Tento postup se opakoval u všech aktiv a hrozeb z dané kategorie. Výstupem byl přehledný katalog míry rizik, v němž bylo možné sledovat jednotlivá hodnocení a rizika. U rizik přesahující námi zvolenou hranici byla použita červená výplň pro snadnější orientaci v katalozích.

5.4 Hodnocení rizik

Stanovení míry rizika nám přineslo překvapivé výsledky. Byly jsme schopní nově rozeznat působení daných hrozeb na jednotlivá aktiva. Přičemž se odhalily rizika, která přesahovaly námi předem definovanou hranici a spadaly do skupiny s vysokou mírou rizika.

Tuto hranici nám přesáhly téměř všechny skupiny hrozeb, až na výjimku, kterou tvořila skupina hrozeb spadající do kategorie přírodních událostí. Bylo tomu dáno především pravděpodobností naplnění jednotlivých hrozeb z této kategorie.

V následujícím výčtu budou shrnuty výsledky našeho hodnocení, přičemž bude kladen důraz na opodstatnění námi zjištěných skutečností. Výčet bude pro lepší orientaci členěn podle skupiny hrozeb, stejně jako tomu je v našem katalogu stanovení míry rizik, aby bylo čtenáři usnadněno pochopení výsledků hodnocení:

1) *Fyzická poškození*

Skupina fyzických poškození naši pomyslnou hranici přesáhla celkem sedmkrát, ačkoliv se tak stalo pouze u hrozby *„Prach, koroze, zamrznutí“*. Z toho důvodu usuzujeme, že věnování větší pozornosti této hrozbě bude na místě.

Pravděpodobnost výskytu hrozby nese hodnotu 3. Výskyt se dá očekávat v intervalu jednoho měsíce. Tato hodnota byla přisouzena hrozbě z důvodu jejího původu. Jedná se o environmentální hrozbu a její existence není podmíněna motivací jedince, nýbrž působením přírodních vlivů.

Dopad této hrozby podobně jako v celé skupině je kritický na mnohá aktiva. Především na její informační složku. Za předpokladu, že informační zařízení nejsou spravována v pravidelných intervalech, dá se očekávat vyvození závažných následků.

V případě koroze či prachu může dojít k znehodnocení veškerých serverů, služeb využívající těchto zařízení a následek této hrozby by mohl být katastrofický, neboť veškerá činnost spojená s námi zkoumanými procesy je silně závislá na užívání systému a všech činností s ním spojených.

U ostatních hrozeb této kategorie lze sledovat pouze střední hodnoty nebo hodnoty hraniční. Ohodnocení jejich rizik bylo rapidně snižováno pravděpodobností jejich výskytu nebo dopady těchto hrozeb nenesly větší následky.

2) Přírodní události

V této skupině nebyla nalezena žádná rizika, jež by přesahovala hranici hodnocení. U bouře, která sice měla vyšší míru pravděpodobnosti, se bral především ohled na klimatické podmínky daného regionu a situování míst vykonávání činností. Z toho důvodu nemohla rizika nabývat vyšších hodnot.

V případě povodně byla rizika snížena výškou budov, v níž procesy probíhají. Kdyby povodeň skutečně nastala, aktiva by prakticky nemohla být ohrožena. Nicméně v případě následku se uvažovala maximální hodnota.

3) Ztráta základních služeb

V této skupině bylo možno sledovat tři výskyty rizik s vysokým ohodnocením míry. Tato tři překročení se vztahovala na skupinu *„Selhání klimatizace a dodávky vody“*. Kritická oblast této hrozby zahrnovala skupinu aktiv z kategorie umístění. Zde můžeme pozorovat, jak se hodnota následku přenáší na další aktiva. Především skupina zahrnující veškerý personál. Selhání těchto služeb by mělo za následek možné zdravotní problémy a díky čemuž by mohlo docházet s nížení efektivity daných procesů.

Zbylé hrozby dosahovaly pouze hraničních, středních a nízkých hodnot. Tato skutečnost lze opět odůvodnit nízkou hodnotou pravděpodobnosti s kontextem společnosti.

4) Ohrožení informací

Díky neexistenci řízení informační bezpečnosti se v této skupině hrozeb dalo očekávat velké množství kritických rizik. Skupina hrozeb dokázala naší pomyslnou hranici překročit celkem třicet sedmkrát.

Z toho kategorie *„Krádež informačního zařízení dokumentů“* obsahovala více jak dvacet výskytů. Střední hodnota pravděpodobnosti a vysoká hodnota následků zapříčinila takové množství kritických rizik.

Díky předpokladu velkého množství informačního zařízení a závislosti na těchto aktivech se daly kritické hodnoty předpokládat. Situaci dále ztěžují časté služební cesty a homeoffice mnohých zaměstnanců.

Skupina s druhým výskytem se týkala informací z nedůvěryhodných zdrojů. Jelikož předmět podnikání je především závislý na tržních informacích, dá se předpokládat, že při nedostatku relevantních informací, případně užívání neověřených informací, by jakýkoliv postup mohl být kritický ve vztahu k podnikání.

5) *Technická selhání*

Hrozby technického selhání dosáhly kritických hodnot více než třicetkrát. Kritické hodnoty se vyskytovaly u hrozeb selhání operačního systému a selhání internetového připojení. Ačkoliv se zpočátku předpokládalo, že kritické hodnoty budeme moci nalézt především u selhání informačního systému, po konzultaci s IT oddělením společnosti jsem byl nucen přehodnotit pravděpodobnost naplnění této hrozby.

V případě selhání operačního systému u informačních zařízení v prostorách kanceláří se dá očekávat, že toto selhání povede k snížení či ochromení procesů prodeje a nákupu. Tuto skutečnost podporuje i fakt, že pracovníci využívají pro práci i vlastní přenosné počítače, na něž může působit mnohem větší počet hrozeb, než je tomu u stolních počítačů kanceláří.

Pokud však budeme hovořit o operačním systému, který slouží pro provoz informačního systému ABRA G3, budeme hovořit o riziku s katastrofickými následky. Pokud by skutečně došlo k takovému ohrožení a naplnění hrozby, veškeré procesy by byly ochromeny.

Kritické hodnoty v oblasti selhání internetového připojení jsme mohli odůvodnit díky provázaností poskytování služeb informačního systému a ostatních činností procesu. Bez internetového připojení by nebylo možné poskytovat službu skrze vzdálené plochy na jednotlivých zařízeních a procesy nákupu a prodeje by byly dočasně ochromeny.

Stejně tak nás k tomu může vést především fakt, že společnost svůj prodej koncentruje výhradně na e-shopu společnosti, který bez internetového připojení není možné provozovat.

6) *Neoprávněná činnost*

U neoprávněné činnosti jsme mohli zaznamenat také více než třicet překročení hranice pro hodnocení. Překročení byla možná sledovat ve skupinách poškození dat a virové infekce.

Virová je hrozba, jež spadá do skupiny náhodného a úmyslného původu. Ačkoliv společnost při činnostech procesů využívá především ověřené stránky vlastního původu a stránky dodavatelů, neexistují jiná pravidla užívání internetových služeb, což nás vede k přesvědčení, že tato hrozba může využít této zranitelnosti. Virová nákaza může zapříčinit snížení efektivity procesů, nebo procesy úplně ochromit.

Poškození dat může mít také původ v náhodě či úmyslu. Ve chvíli, kdy dojde k nenávratnému poškození dat, se může stát, že poškozené informace budou kritické k předmětu podnikání. Zaměstnanci jsou sice vybízeni k pravidelnému zálohování, avšak neexistuje opatření, které by této hrozbě dokázalo účinně zamezit.

7) Ohrožení funkčnosti

Poslední hodnocenou skupinou a zároveň nejkritičtější skupinou, co se rizik týče, je skupina ohrožení funkčnosti. Podařilo se nám nalézt více než padesát hodnot vstupujících do pole kritičnosti. Je tomu dáno hlavně charakterem hrozeb, které jsme do této skupiny zahrnuly.

Hrozba *„Špatná rozhodnutí“* vede, podobně jako hrozba informací z nedůvěryhodných zdrojů, k špatné obchodní strategii, obchodnímu plánu a výrazně tak dokáže ovlivnit tržní postavení společnosti. Absence podpůrných rozhodovacích nástrojů či metod k tomu silně napomáhá.

Druhé tři skupiny s kritickými hodnotami jsou hrozby spadající do kategorie ztráta zákazníků, ztráta konkurenční výhody a nevymahatelné pohledávky. Pokud společnost ztratí veškeré své zákazníky, můžeme očekávat i ztrátu veškerých aktiv z důvodu ztráty předmětu podnikání. Stejný scénář lze očekávat i u ztráty konkurenční výhody. Tyto dvě hrozby se stávají kritickými z důvodu možného nástupu nové konkurence na poli distribuce audiovizuální techniky. V případě nevymahatelných pohledávek přestává mít podnikání smysl, neboť nebude z čeho platit současné náklady.

Jiný případ je hrozba popisující nedostatek finančních zdrojů. Dalo by se předpokládat, že tato hrozba bude mít stejné následky a výši míry rizika jako předchozí skupiny, nicméně je nutné rozlišovat hrozby jako takové.

Pokud společnost bude trpět nedostatkem finančních zdrojů, má možnost situaci řešit. Nevnímáme hrozbu jako dlouhodobou událost. Stejně tak bereme hrozbu jako jev nevztahující na výše zmíněné hrozby, neboť bychom se dopustili duplicity při hodnocení rizik. Proto se míra rizik hrozby stále pohybuje pod hranicí kritičnosti a její pravděpodobnost je o řád nižší.

5.5 Akceptace a ošetření rizik

Výsledky analýzy byly vedením společnosti přijaty. Po odevzdání hodnocení se vedla diskuse nad výslednými hodnotami rizik a bylo rozhodnuto, že společnost bude v současné době věnovat pozornost především nejkritičtějším oblastem.

Ostatní oblasti hodnoceny jako hraniční, tedy s ohodnocením 5, budou monitorovány s tím, že do budoucna budou dále zkoumána a podrobena detailnější analýze pro návrh nových opatření. Společnost se rozhodla daná rizika dočasně podstoupit.

5.5.1 Ošetření rizik

Pro rizika s ohodnocením 6-8 byla navržená následující doporučení pro ošetření. Ošetření jsou tříděna dle skupiny hrozeb a v jejich popisu je věnována pozornost jednotlivým skupinám. Tento výčet byl přijat společností a nebyla vyžadována další modifikace. Můžeme tedy tvrdit, že navrhnutá ošetření se stávajícími opatřeními snížila rizika hrozeb na úroveň akceptovatelnosti.

- **Fyzická poškození**

Pro tuto oblast navrhujo zajištění pravidelné údržby serverů a veškerých informačních zařízení. Servery situovány v budově musí být v uzamykatelné místnosti opatřené bezpečnostními prvky jako bezpečnostní zámek či kód, omezený přístup všem osobám s výjimkou správy, ventilační zařízení zajišťující správnou teplotu a sucho v místnosti, prvky zabraňující proniknutí vody do místnosti, impregnace zařízení a kamerový systém.

Kontroly serverů by měly probíhat minimálně jednou týdně, přičemž bude zajištěno odstranění prachu a výměna filtrů chladících zařízení. Zároveň se důrazně doporučuje změna lokace druhého serveru. V případě působení hrozeb ve stejné lokalitě může dojít k nenávratné ztrátě. Ostatní stávající opatření společnosti jsou vyhodnoceny jako dostatečné.

- **Selhání dodávek základních služeb**

Pro selhání dodávek vody a klimatizace doporučuji tvorbu náhradního řešení. Pokud teplota na pracovišti přesáhne vyšší teploty než teploty stanovené zákoníkem práce, je nutné mít na pracovišti uskladněné náhradní ventilační zařízení, které dokáže teploty snížit, nebo naopak zvýšit, v závislosti na ročním období.

Pro udržování stálého pitného režimu a hygieny musí být zajištěna druhotná sociální zařízení a dostupnost nápojů zaměstnancům na pracovišti.

V opačném případě může být zaměstnancům doporučeno práci vykonávat z domova, pokud se jejich činnost nevztahuje přímo na místo výkonu práce.

- **Ohrožení informací**

Jako opatření navrhuji zavedení systému řízení informační bezpečnosti. Společnost může po splnění náležitých podmínek implementovat systém řízení ISO či jiného systému podle možností. Dále doporučuji změnu způsobu zálohování informací v podobě dat.

Veškerá činnost před svým ukončením musí být podmíněna zálohou na záložní disky. Ostatní kritická data, nevyužívající informačního systému, musí být uložena na sdíleném síťovém disku. Data na sdíleném disku sloužící vícero uživatelům mohou mít nastavena možnost úpravy, avšak dostupnost ukládání bude povolena po ukončení činnosti prvního uživatele.

Současně doporučuji navrhnout fyzické zálohování nejkritičtějších informací. Nově vzniklé fyzické zálohy a stávající musí být dostatečně zabezpečené proti odcizení nepovolaných osob a musí být dostupné pouze na vyžádání s dohledem odpovědné osoby.

Informace ukládané do systému či shromážděné informace musí být ověřovány a před ukládáním prověřeny dle více zdrojů.

Školení o informační bezpečnosti by se mělo stát pravidelnou rutinou pro všechny zaměstnance v případě, že nedojde k zavedení systému řízení bezpečnosti. Stejně tak je nutné zvážit držení informačních zařízení obsahující kritické informace mimo místo výkonu práce.

Zařízení by měla být opatřena bezpečnostními prvky jako: autentizaci, autorizaci, pravidla užívání. Mezi tato zařízení zahrnujeme veškeré mobilní telefony, notebooky, stolní počítače a jiné. Dodržování informační bezpečnosti musí být vyžadováno po všech zaměstnancích. Ostatní stávající opatření společnosti jsou považována za dostačující.

- **Technická selhání**

Pro selhání operačního systému navrhuji jako opatření zavedení nových bezpečnostních prvků pro systém Debian Linux. Tento operační systém je klíčový pro provoz informačního systému, v případě jeho ochromení dojde k vyřazení provozu celého systému. Volba bezpečnostních prvků je ponechána na místním IT oddělení. Nové bezpečnostní prvky by měly být řešeny s dodavatelem informačního systému.

V případě selhání telekomunikačních služeb navrhuji zvážení nového dodavatele, který by byl schopný zajistit dodatečnou podporu, pokud selže první dodavatel.

U volby nového dodavatele doporučuji zvážit i náklady. Nový dodavatel by mohl nabídnout službu levněji. V případě že dojde k výpadku služby, bude ohrožený veškerý prodej zboží.

Současně důrazně doporučuji revizi zálohování kamerového systému. Ačkoliv pravděpodobnost hrozby selhání nenabývá vysokých hodnot, její dopad ve vztahu s ostatními hrozbami může být kritický. Ostatní opatření společnosti jsou považována za dostačující.

- **Neoprávněná činnost**

Proti virové infekci navrhuji zavedení systému oprávnění k užívání internetu. Uživatelé by měli být omezeni na užívání pouze nezbytných stránek. Ostatní přístupy pro pevná zařízení by měly být odepřeny, až na povolené výjimky.

Proti poškození dat vycházejme z předchozích opatření, viz opatření proti ohrožení informací. Ostatní opatření společnosti jsou považována za dostačující.

- **Ohrožení funkčnosti**

Pro hrozbu špatného rozhodování navrhuji zavést podpůrné metody či aplikace rozhodování, které usnadní tento proces. Díky současně dostupným metodám může společnost zefektivnit proces rozhodování a směřovat své úsilí na jiné oblasti. Jako například na budování přidané hodnoty pro zákazníka, díky čemuž by si mohla společnost vytvořit pevnou základnu věrných zákazníků. Ostatní stávající opatření společnosti jsou považována za dostačující.

Závěr

Cílem této práce bylo seznámit čtenáře s problematikou řízení bezpečnosti aktiv a analýzou rizik. Přičemž mělo dojít mimo jiné k praktickému ověření řízení bezpečnosti na menším ekonomickém subjektu pomocí analýzy rizik jedné z norem.

Praktické ověření normy ISO/IEC 27005 nám potvrdilo, že tato norma je aplikovatelná na různé druhy subjektů. Její aplikace není nutně vázaná na větší podniky, jako tomu může být u jiných metodik. Struktura i obsah této normy jsou snadno pochopitelné a její aplikace zjednodušená díky detailním popisům doporučení. Analýza rizik podle této normy nám přinesla překvapivé výsledky a subjekt analýzy byl spokojen s jejím průběhem a stejně tak i s navrhnutými opatřeními.

Opatření byla navržena pro hrozby z těchto oblastí: fyzická poškození, selhání dodávek základních služeb, ohrožení informací, technická selhání, neoprávněná činnost a ohrožení funkčnosti. Přičemž největší počet nalezených rizik, námi definovaných jako kritické, byl ve skupině hrozeb ohrožení funkčnosti.

Jak už bylo v úvodu řečeno, většina menších firem považuje řízení informační bezpečnosti za nutné zlo a z toho důvodu většina společností neaplikuje žádný systém řízení bezpečnosti informací. Tuto skutečnost jsme si mohli ověřit na námi zvoleném subjektu. Společnost v současné době neaplikuje žádný konkrétní ucelený systém opatření pro eliminaci rizik spojených s informační bezpečností.

Nicméně v mnohých ohledech si společnost Disk Multimedia je vědoma svých zranitelností, které mohou napomáhat hrozbám k znehodnocení primárních aktiv, a z toho důvodu pracuje na neustálém zlepšování všech svých procesů s opatřeními, které se snaží pokrýt veškeré činnosti společnosti, aby těmto hrozbám zabránila.

Jako příklad nám může posloužit riziko spojené s nástupem nové konkurence, z oblasti ohrožení funkčnosti, na trh v podobě internetových velkoobchodů Thomann Musikhaus, které vynechávají dealerskou složku prodejního systému, a prodávají přímo koncovému uživateli. Společnost vědoma si tohoto rizika v současné době přesměrovává předmět svého podnikání na vývoj softwarových a hardwarových komponent a poskytování služeb, aby tak do budoucna zajistila zdravé fungování podniku.

Současně můžeme na příkladu této případové studie tvrdit, že ačkoliv menší podniky mají sklony vyhýbat se systémům řízení bezpečnosti, společnosti jsou schopné mnohdy napříč svých organizací zavádět kvalitní opatření, která do jisté míry dokáží potlačit míru rizika spojených s různými druhy hrozeb, bez aplikace systému řízení bezpečnosti.

Cíle této studie byly splněny dle zadání díky dostupné literatuře, jež dopomohla ke zpracování teoretického základu a výbornému přístupu námi analyzované společnosti, pro niž výsledky této studie mohou v budoucnu sloužit jako podněty pro zavedení systému řízení bezpečnosti.

Zdroje

Citovaná literatura

[1] GALBA Alexander a Antonín PAVLÍČEK. Moderní informatika. Praha : Professional Publishing, 2012. 184 str. ISBN: 978-80-743-1095-9.

[2] POŽÁR, Josef: Informační bezpečnost v organizaci, In: Bezpečnostní teorie a praxe 1/2005

[3] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 3., aktualiz. a rozš. vyd. Praha: Grada Publishing, a.s., 2010, 354 str., ISBN 978-80-247-3051-6

[4] ČESKO. Vyhláška č. 523/2005 Sb., ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor, ve znění vyhlášky č. 453/2011 Sb. In: Sbírka zákonů České republiky. 2005, částka: 179/2005. Praha 2005 Dostupná také z: http://www.epravo.cz/vyhledavani-aspi/?Id=60721&Section=1&IdPara=1&ParaC=2

[5] BS ISO/IEC 73: 2002 Risk Management - Vocabulary - Guidelines for use in standards. Londýn: BSI, 2002, 24 s. ISBN 0-580-40178-2.

[6] ROSICKÝ, Antonín. Informace a systémy, Základy teorie pro úspěšnou praxi. Praha : Nakladatelství Oeconomica, 2009. 200 str. ISBN 978-80-245-1629-5.

[8] ČSN ISO/IEC 27001:2005. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Poţadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2005, 35 s. Třídící znak 369790.

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

[10] Doucek, Petr. NOVÁK, Luděk. NEDOMOVÁ, Lea. SVATÁ, Vlasta. Řízení bezpečnosti informací. Druhé rozšířené vydání o BCM. Praha: Professional Publishing, 2011, 286 str.., ISBN 978-80-7431-050-8

[11] ČERMÁK, Miroslav.COBIT tajemství zbavený. In: Clever and Smart [online]. Poslední aktualizace 30.10.2010 [cit. 19.04.2016]. Dostupné z: http://www.cleverandsmart.cz/cobit-tajemstvi-zbaveny/

[12] ČERMÁK, Miroslav. ITIL tajemství zbavený. In: Clever and Smart [online]. Poslední aktualizace 29.10.2019 [cit. 19.04.2016]. Dostupné z: http://www.cleverandsmart.cz/itil-tajemstvi-zbaveny/

[13] Management mania. Metodika CRAMM (CCTA Risk Analysis and Management Method). In: Management Mania [online]. Poslední aktualizace 26.03.2016 [cit. 19.04.2016]. Dostupné z: https://managementmania.com/cs/metodika-cramm-ccta-risk-analysis-and-management-method

[15] Management mania.Metoda DELPHI. in: Management Mania [online]. Poslední aktualizace 29.07.2015 [cit. 19.04.2016]. Dostupné z: https://managementmania.com/cs/metoda-delphi

[15] Management mania. Brainstorming. in: Management Mania [online]. Poslední aktualizace 16.03.2016 [cit. 19.04.2016]. Dostupné z: https://managementmania.com/cs/brainstorming

[16] Management mania. ETA (Event tree analysis) - analýza stromu událostí. in: Management Mania [online]. Poslední aktualizace 24.07.2015 [cit. 19.04.2016]. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysis-analyza-stromu-udalosti

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

[18] ISO/IEC 27005:2011(E). Second Edition.Information technology – Security techniques – Information security risk Management.Geneva: ISO copyright office, 2011, 68 s. ICS: 35.040

[19] Ministerstvo spravedlnosti České republiky. In: Veřejný rejstřík a Sbírka listin – eJustice [online]. Poslední aktualizace 26.04.2016 [cit 26.04.2016]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=587007&typ=UPLNY

Seznam doplňujících ilustrací, tabulek a příloh

Obrázky:

Tabulky:

Přílohy: