VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATICS

ZAVEDENÍ ISMS V PODNIKU

ISMS IMPLEMENTATION IT THE ENTERPRISE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — BC. ET BC. JAN PAWLIK
AUTHOR

VEDOUCÍ PRÁCE — ING. VIKTOR ONDRÁK PH.D.
SUPERVISOR

BRNO 2015

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2014/2015
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Pawlik Jan, Bc. et Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Zavedení ISMS v podniku

v anglickém jazyce:

ISMS Implementation in the Enterprise

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.
ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.
DOBDA L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.
DOUCEK P., L. NOVÁK a V. SVATÁ Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.
POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2014/2015.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 28.2.2015

Abstrakt

Diplomová práce se věnuje implementaci systému řízení bezpečnosti informací dle normy ČSN ISO/IEC 27 001 v reálném prostředí malé obchodní společnosti. V první části práce jsou přiblížena teoretická východiska z oblasti bezpečnosti informací. V druhé části je zpracována analýza společnosti a proveden návrh opatření zvyšujících bezpečnost informací v dané společnosti.

Abstract

This master thesis deals with the implementation of the information security management system according to the standard ISO/IEC 27 001 in the environment of a small company. In the first part, it focuses on the theoretical background of the information security. The second part deals with the analysis of the company and concept of a company's measures to increase the security of information within the selected company.

Klíčová slova

ČSN ISO/IEC 27 001, ČSN ISO/IEC 27 002, Systém řízení informační bezpečnosti, ISMS, PDCA, příručka bezpečnosti, analýza rizik

Keywords

ISO/IEC 27 001, ISO/IEC 27 002, Information Security Management System, ISMS, PDCA, security manual, risc analysis

Bibliografická citace

PAWLIK, J. Zavedení ISMS v podniku. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. 77 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 24. 5. 2015

……

Jan Pawlik

Poděkování

Děkuji panu Ing. Petru Sedlákovi za cenné připomínky a rady při tvorbě mé diplomové práce a panu Ing. Viktoru Ondrákovi Ph.D. za odborné vedení. Chci také poděkovat svým rodičům, kteří mi umožnili vysokoškolské studium. V neposlední řadě děkuji také své ženě za její podporu a trpělivost.

Obsah

Úvod

V dnešní době se informační bezpečnost stává stále aktuálnějším tématem, které je ale často podceňováno, zejména v menších obchodních společnostech. Největším bohatstvím, kterým společnosti disponují, je know-how, které je obsaženo rovněž v datech a informacích.

S rozvojem informačních technologií zvyšují společnosti svou závislost na informačních technologiích. Často převádějí většinu důležitých informací do digitální podoby z důvodu snadnější manipulace, vyhledávání, ale i zálohování a správy. Často si však majitelé společností neuvědomují, že s příchodem nových technologií se objevují také nové hrozby, které je nutno ošetřit vhodnými opatřeními.

Pokud není tato oblast dostatečně ošetřena, může dojít ke ztrátě dat a ta může způsobit citelné existenční problémy. Další významnou hrozbou je oblast průmyslové špionáže, která může mít ještě horší následky než prostá ztráta dat.

Menší společnosti často nepřikládají bezpečnosti informací dostatečnou důležitost. Další překážkou pro ně může být finanční náročnost zavádění opatření a následného auditu. Pomocí implementace norem řady ISO 27 000 však je možné zvýšit úroveň zabezpečení informací bez výrazných finančních výdajů. Rovněž je možné zavádět tyto normy vlastními silami a následně neprovádět certifikaci dle odpovídajících norem, která může být pro některé společnosti finančně neúnosná.

Tato diplomová práce si klade za cíl navrhnout systém řízení bezpečnosti informací v malé obchodní společnosti, která má zájem chránit svá informační aktiva. První část práce bude věnována teoretickým východiskům informační bezpečnosti, ve druhé provedu analýzu vybrané společnosti. Cílem třetí části je sestavení směrnic, které budou odpovídat normám z rodiny ISO 27 000 a připraví společnost na ochranu proti ztrátě informací a rovněž případné požadavky dle zákona o kybernetické bezpečnosti. Práce bude zakončena ekonomickým zhodnocením aplikace navržených směrnic.

1 Cíle práce, metody a postupy zpracování

Cílem práce je pomocí norem řady ISO 27 000 provést návrh zavedení systému řízení bezpečnosti informací (dále také „ISMS“) v malé společnosti. Tyto normy obsahují řadu doporučení, které je nutné implementovat při snaze získat certifikát bezpečnosti informací, ale v této práci jsou normy využívány spíše jako doporučení, protože společnost v nejbližší době certifikaci neplánuje. Cílem je tedy zvýšit úroveň zabezpečení informací v dané společnosti pomocí návrhu příslušných opatření a směrnic. Mezi dílčí cíle patří alespoň přibližné ekonomické zhodnocení a návrh časového plánu zavedení nejdůležitějších opatření.

Pokud by se analyzovaná společnost rozhodla v budoucnu pro certifikaci dle normy ISO 27 001, tato diplomová práce by měla být základním dokumentem pro tuto certifikaci.

V práci budou popsána nejprve teoretická východiska pro následující analýzu společnosti. Budou zde zmíněny vazby na jednotlivé normy i české zákony a popsán obecný způsob analýzy rizik a návrhu opatření v souladu s normou ČSN ISO/IEC 27 001. Následovat bude část uvádějící informace o společnosti, kde bude zpracována analýza aktiv a s nimi souvisejících rizik. Poslední a klíčová část práce bude obsahovat návrh opatření dle příslušných norem, náklady na jejich zavedení a rámcový časový plán.

2 Teoretická východiska

2.1 Informace

„Informace o nějakém jevu, procesu, události je jistá veličina, která snižuje nebo částečně odstraňuje dosavadní neurčitost, neznalost právě o tomto jevu, události.“[1]

Informace je dnes jedním z hlavních faktorů podmiňujících pokrok ve všech oborech lidské činnosti. Informace o stavech, jevech a procesech představuje schopnost tyto procesy ovlivňovat. Schopnost manažera a jeho spolupracovníků se správně rozhodovat vždy záleží na informacích. Při jejich nedostatku je nutné vydávat subjektivní, intuitivní a nepodložená rozhodnutí.

Rozlišujeme několik výkladů informace:

- Ve všeobecném významu sdělení, zprávy apod.,
- Distribuované působení na jedince i společnosti (hromadné sdělovací prostředky, reklama apod.),
- V obecném kybernetickém významu pro řízení a sdělování v živých organismech a ve strojích, včetně ekonomických systémů.[2]

2.1.1 Cíle informační bezpečnosti

Základní cíle informační bezpečnosti dle normy [3] lze rozdělit na:

- Důvěrnost – zajištění, že informace jsou přístupné nebo sděleny pouze těm, kdo jsou k tomu oprávněni,
- Dostupnost – zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby,
- Integrita – zajištění správnosti a úplnosti informací.

Není možné zajistit absolutní bezpečnost. Vždy kalkulujeme s mírou rizika, která je akceptovatelná. Označujeme to jako zbytkové riziko (= riziko zbývající po uplatnění zvládání rizik).

[1] POŽÁR, J. *Informační bezpečnost*, s.39
[2] Tamtéž, s. 39 – 40.
[3] ISO 27 001:2006, s. 2.

2.2 Integrovaný systém řízení (IMS)

IMS (Integrated Management System) představuje komplexní pohled na problematiku řízení v organizaci. Řízení organizace je nutné vnímat jako řešení komplexního problému, v jehož rámci je nutné řídit každý dílčí aspekt.[4]

„IMS je filosofie komplexního řízení organizací“[5]

Mezi komponenty IMS řadíme

- QMS (Quality management System)
    - Představuje základ pro trvalé zlepšování jakosti a procesů s ní spojených. Za následek má zvýšení produktivity práce díky zavedení vnitřního řádu.
- EMS (Environmental Management System)
    - Jedná se o řízení lidských aktivit a jejich dopadů na okolní prostředí s důrazem na ochranu životního prostředí. Cílem je neustálé zlepšování environmentálního profilu organizací.
- OHSAS (Occupational Health and Safety)
    - Systém řízení bezpečnosti a ochrany zdraví při práci umožňuje rozpoznávat a řídit bezpečnostní a zdravotní rizika a snižovat pravděpodobnost nehod a úrazů.
- ISMS (Information Security Management System)[6]
    - Řízení bezpečnosti informací se věnuji v podkapitole 2.4.

[4] DOUCEK, P. *Řízení bezpečnosti informací*, s.19 - 27.
[5] ONDRÁK, V. *Problematika ISMS v manažerské informatice*. s. 13.
[6] DOUCEK, P. *Řízení bezpečnosti informací*, s.27.

Obr. č. 1 - IMS (Zdroj: AFOES CONSULATNTS, Integrated Management System (IMS))

Tato diplomová práce je zaměřena na Management informační bezpečnosti, proto se blíže budu zabývat pouze ISMS

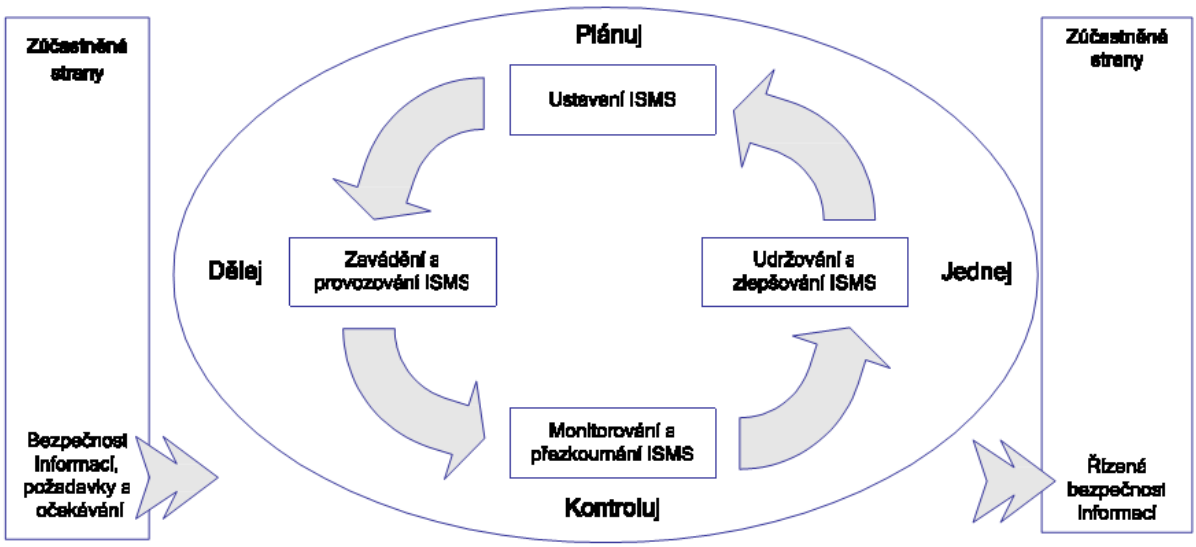
2.3 Model PDCA

Model PDCA poskytuje tematické vyjádření životního cyklu IMS nebo jeho komponenty a také obsahuje zpětnou vazbu.[7] Díky tomuto modelu je možné konstantní zlepšování kvality výrobků, služeb, procesů, aplikací, dat atd. Model se skládá ze čtyř etap.[8]

1. Plan (Plánuj)
    - V této etapě probíhá ustavení politiky ISMS, cílů, procesů a postupů související s managementem rizik a zlepšování bezpečnosti informací, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
2. Do (Dělej)
    - Zavedení a využívání politiky ISMS, opatření, procesů a postupů.

[7] DOUCEK, P. *Řízení bezpečnosti informací*, s. 20.
[8] ONDRÁK, V. *Problematika ISMS v manažerské informatice*, s. 24.

3. Check (Kontroluj)
    - Posouzení, případně měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
4. Act (Jednej)
    - Přijetí opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.[9]



Obrázek 1- PDCA model aplikovaný na procesy ISMS

Obr. č. 2 - PDCA model aplikovaný na procesy ISMS (Zdroj: ISO 27 001:2006, s ix.)

2.4 ISMS

„Systém managementu bezpečnosti informací ISMS je část celkového systému managementu organizace založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací“[10]

[9] ISO 27 001:2006, s. ix.
[10] Tamtéž, s. 3.

2.4.1 Základní pojmy

Pro porozumění ISMS a jejím normám je dále nutné stanovit a vysvětlit základní pojmy, které se ho týkají. Jejich definice stanovuje norma ISO 27 001:

Aktivum – cokoliv, co má pro organizaci nějakou hodnotu.

Dostupnost – zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

Bezpečnost informací – zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

Bezpečnostní událost – identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací.

Bezpečnostní incident – jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací.

Integrita – zajištění správnosti a úplnosti informací.

Zbytkové riziko – riziko zbývající po uplatnění zvládání rizik.

Akceptace rizik – rozhodnutí přijmout riziko.

Analýza rizik – systematické používání informací k odhadu rizika a k identifikaci jeho zdrojů.

Hodnocení rizik – celkový proces analýzy a vyhodnocení rizik.

Vyhodnocení rizik – proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu.

Management rizik – koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika.

Zvládání rizik – proces výběru a přijímání opatření ke změně rizika.

Prohlášení o aplikovatelnosti – dokumentované prohlášení popisující cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace.[11]

Informační systém – soubor prvků spojených vzájemnými vztahy, vazbami. Prvky IS tvoří místa transformace dat a informací (hardware, software, lidé atp.). Vazby jsou tvořeny především spojování kanály, vzájemné působení mezi prvky.

Zranitelnost – nedostatek nebo slabina bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv.

Zranitelné místo – slabina IS, využitelná ke způsobení škod nebo ztrát útokem na IS.

Útok nebo **Bezpečnostní incident** – úmyslné využití zranitelného místa IS ke způsobení škod/ztrát na aktivech nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Útočit lze přerušením, odposlechem, změnou či přidáním hodnoty k datu.[12]

2.4.2 ISMS

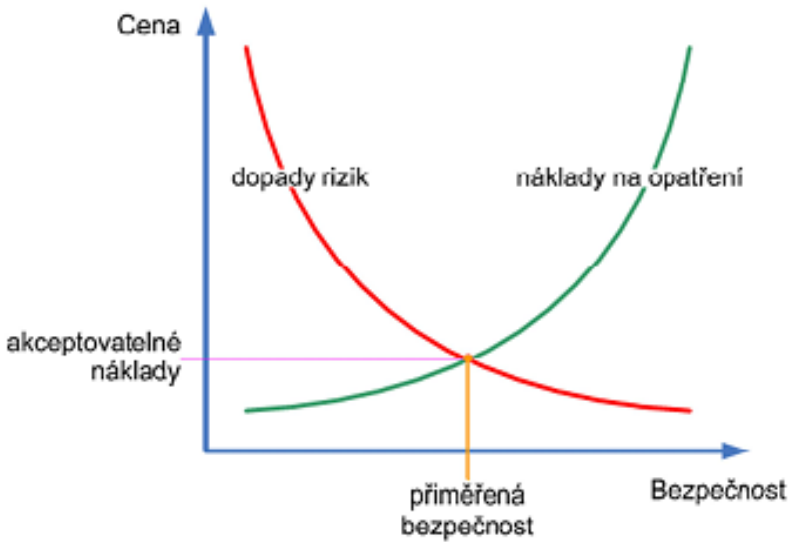
ISMS postihuje několik základních okruhů:

- Bezpečnosti IT,
- Bezpečnost komunikace,
- Personální bezpečnost,
- Administrativní bezpečnost,
- Fyzickou bezpečnost,
- Dokumentaci,
- Bezpečnostní funkce a mechanismy.[13]

2.4.3 Přiměřená bezpečnost

Velikost prostředků vložených do bezpečnosti ICT musí odpovídat hodnotě aktiv a míře rizik. Představu u této problematice vidíme v následujícím grafu.

[11] ISO 27 001:2006, s.2 – 4.
[12] POŽÁR, J. *Informační bezpečnost*, s. 98-99.
[13] ONDRÁK, V., *Problematika ISMS v manažerské informatice*, s. 66.



Obr. č. 3 - Graf přiměřené bezpečnosti (Zdroj: ONDRÁK, V., Problematika ISMS v manažerské informatice, s. 36.)

Z grafu tedy vyplývá, že při zavádění systému informační bezpečnosti je cílem najít přiměřenou úroveň bezpečnosti za akceptovatelné základy.

2.4.4 Zavádění ISMS

Cílem zavedení ISMS je řízení a správa informačních aktiv s cílem eliminace jejich možné ztráty nebo poškození na třech úrovních:

1. Určení aktiv, která se mají chránit,
2. Zvolení a řízení možných rizik bezpečnosti informací,
3. Zavedení opatření s požadovanou úrovní záruk a jejich kontrola.[14]

2.4.5 Určení aktiv

Aktivum je majetek společnosti. Aktiva dělíme do několika skupin

- **Hmotná** – technické prostředky výpočetní techniky (počítače, modemy, aktivní prvky počítačových sítí, kabelové rozvody, tiskárny atd.)
- **Nehmotná**
    - Pracovní postupy využívané v oblasti ICT,
    - Data – vytvořená nebo převzatá odjinud, důležitá pro provoz,

[14] ONDRÁK, V., *Problematika ISMS v manažerské informatice*, s. 66.

- Programové vybavení – jakýkoliv software od operačního systému po BI aplikace,
- Služby – počítačové a komunikační služby, ale také základní služby (topení, klimatizace).

Aktiva dělíme také z hlediska ISMS. Aktiva ISMS dělíme do dvou základních skupin

- **Primární** – zejména nehmotná. Jedná se o informace, které jsou organizací využívány, a funkční procesy a aktivity organizace, znalosti a know-how, které mají pro ISMS určitý význam a je tedy potřeba zajistit jejich bezpečnost.
- **Sekundární** – zejména hmotná. Jedná se o technické vybavení, komunikační infrastrukturu, ale také programové vybavení a pracovníky, kteří se na chodu organizace podílejí. Patří sem také prostory organizace apod.[15]

2.4.6 Ohodnocení aktiv

Pokud aktiva určíme, je nutné je dále ohodnotit a vyjádřit míru jeho důvěrnosti, integrity a dostupnosti. K tomu je využívaná např. metodika CRAMM. Ta pokrývá všechny fáze řízení rizik od analýzy aktiv až k návrhu opatření. Pro využití této metodiky je nutné nejdříve stanovit hodnotící kritéria pro posouzení jednotlivých aktiv. Nejčastěji se jedná o peníze nebo kvalitativní hodnoty.

Tab. č. 1- Příklad hodnocení aktiv (Zdroj: ONDRÁK, V., *Problematika ISMS v manažerské informatice*, s.82.)

1	žádný dopad na organizaci	bezvýznamné riziko
2	zanedbatelný dopad na organizaci	akceptovatelné riziko
3	potíže či finanční ztráty	nízké riziko
4	vážné potíže či podstatné finanční ztráty	nežádoucí riziko
5	existenční potíže	nepřijatelné riziko

Hlavním principem při hodnocení aktiv jsou náklady vzniklé v důsledku porušení **důvěrnosti, integrity a dostupnosti.** Tato tři kritéria poskytují podklady pro hodnocení aktiv.[16]

[15] DOUCEK, P., *Řízení bezpečnosti informací*, s. 57.
[16] ONDRÁK, V., *Problematika ISMS v manažerské informatice*, s. 83.

Pro výpočet hodnoty aktiva je více způsobů. Nejčastější je tzv. součtový algoritmus, kde principem je součet (Dostupnost + Důvěrnost + Integrita)/3. Dostupnost, důvěrnost a integritu jednotlivých aktiv můžeme určit na škále 1 až 5 a výsledek zařadíme do tabulky uvedené výše. Výsledná hodnota odpoví na otázku, jaký dopad bude mít poničení daného systému na organizaci.

2.4.7 Analýza rizik

Analýza rizik je prováděna kvůli identifikaci zranitelných míst IS. Zachycuje také seznam hrozeb a stanovuje rizika jednotlivým zranitelným místům a hrozbám. Účelem je snížení rizik na přijatelnou úroveň a také akceptace zbytkových rizik tam, kde je jejich minimalizace neefektivní.[17]

U rizik rozlišujeme pravděpodobnost vzniku a existence rizika (P) a míru rizika (R).

P – pravděpodobnost vzniku a existence rizika nabývá pěti hodnot:

1) Nahodilá,
2) Nepravděpodobná,
3) Pravděpodobná,
4) Velmi pravděpodobná,
5) Trvalá.

R – Míru rizika rozdělujeme také do pěti úrovní

1) 1 – 10: Bezvýznamné riziko
2) 10 – 20: Akceptovatelné riziko
3) 21 – 30: Mírné riziko
4) 31 – 60: Nežádoucí riziko
5) 61 – 120: Nepřijatelné riziko

Bezvýznamné riziko

Není vyžadováno opatření, ale bezpečnost není 100% a je potřeba riziko přijmout a uvést např. výchovná a organizační opatření.

[17] Tamtéž, s 83 – 83.

Akceptovatelné riziko

Je přijatelné se souhlasem vedení. Je nutno zvážit, zda náklady na případné řešení nebo zlepšení jsou přijatelné a pokud se nepodaří provést technická bezpečnostní opatření k jeho snížení, je třeba zavést vhodná a přiměřená opatření organizační.

Mírné riziko

Je zpravidla nutno realizovat bezpečnostní opatření dle zpracovaného plánu podle rozhodnutí vedení firmy. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období.

Nežádoucí riziko

Vyžaduje urychlené provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnější úroveň, musí být přiděleny zdroje k jeho snížení. Je-li riziko spjato se značnými následky, musí se provést další vyhodnocení, aby se co nejpřesněji stanovila pravděpodobnost vzniku úrazu nebo jiné nehody, jako podklad stanovení potřeby dosažení snížení rizika.

Nepřijatelné riziko

Je nepřípustné, značné a kritické, permanentní možnost úrazů, závažné nehody, nutnost okamžitého zastavení činnosti, odstavení z provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik a přijetí opatření. Práce nesmí být zahájena nebo v ní pokračováno, dokud se riziko nesníží.[18]

2.4.7.1 Metodiky

Analýza rizik se rozděluje:

- Hrubá úroveň,
- Neformální úroveň,
- Kombinovaný přístup,
- Podrobný přístup.

[18] ONDRÁK, V., *Problematika ISMS v manažerské informatice*, s. 90 – 91.

Analýza rizik na **hrubé úrovni** bere v úvahu hodnotu systému IT pro činnost organizace. Pro rozhodnutí, který přístup je pro systém IT vhodný, má význam zhodnocení několika skutečností:

- Jakých cílů má být použitím IT systému dosaženo,
- Úroveň investic do tohoto systému,
- Aktiva systému, kterým organizace přiřazuje určitou hodnotu,
- Stupeň činnosti organizace závisící na IT systému (zda klíčové funkce v organizaci jsou na tomto systému závislé).

Neformální přístup je založen na využívání znalostí a zkušeností jednotlivců. Obvykle nevyžaduje mnoho zdrojů, ani není nutné se naučit nové dovednosti a je provedena relativně rychle. Bez detailních seznamů kontrol ale vzrůstá pravděpodobnost opomenutí některých důležitých detailů a je obtížné obhájit implementaci ochranných opatření.

Kombinovaný přístup je další možností. Nejprve se provede analýza rizik na hrubé úrovni. U IT systémů, které jsou identifikovány jako významné pro činnost organizace, by měla být přednostně provedena podrobná analýza rizik. Pro všechny zbývající IT systémy by měl být zvolen základní přístup. Tento přístup umožňuje minimalizaci času a úsilí věnovaného na identifikaci ochranných opatření při zajištění ochrany proti vysokým rizikům.

Podrobný přístup je detailní analýza rizik systému IT. Zahrnuje hloubkovou revizi v každém z těchto kroků:

1. Stanovení hranic revize – bude provedeno ještě před identifikací a ohodnocením aktiv. Umožní vyvarovat se zbytečných činností.
2. Identifikace aktiv – těch, kterým organizace přímo přiděluje hodnotu a pro které požaduje ochranu,
3. Ohodnocení aktiv – identifikovaná aktiva ohodnotíme dle významu pro činnost organizace. Může být určeno nejen finančně, ale také z hlediska dopadu na organizaci atd.,
4. Hodnocení hrozeb – jaká je možnost poškození sledovaného systému IT a jeho aktiv. Jako katalog lze použít seznam v normě ČSN ISO/IEC TR 13335-3 v příloze C,

5. Odhad zranitelnosti – odhalí slabá místa, která mohou být využita zdrojem hrozby.

Identifikace plánovaných a existujících ochranných opatření – součástí analýzy rizik je také identifikace opatření[19]

2.5 Fáze ustavení ISMS

- Ustanovení ISMS (=PLAN),
- Zavádění ISMS (=DO),
- Monitorování ISMS (=CHECK),
- Údržba a zlepšování ISMS (=ACT).[20]

2.6 Ustanovení ISMS

V této fázi probíhá definice rozsahu ISMS, dále odsouhlasení Prohlášení o politice ISMS. Další důležitou činností je výběr vhodných opatření pro snížení vlivu existujících rizik.

Ustanovení ISMS je možné rozdělit na několik skupin činností:

- Definice rozsahu, hranic a vazeb ISMS,
- Definice a odsouhlasení Prohlášení o politice ISMS,
- Analýza a zvládání rizik,
- Souhlas vedení s navrhovanými zbytkovými riziky a zavedení ISMS,
- Prohlášení o aplikovatelnosti.

Tato etapa má zásadní dopad na celý životní cyklus ISMS, proto je nutné ji provést pečlivě.[21]

2.6.1 Definice rozsahu a hranic ISMS

První částí řízení bezpečnosti je upřesnění rozsahu a hranic uplatňování ISMS. ISMS nemusí být vždy zaveden v celé organizaci. Při tomto rozhodování je nutné vzít

[19] ONDRÁK, V., *Problematika ISMS v manažerské informatice*, s. 91 – 95.
[20] ISO 27 001:2006, s. ix.
[21] DOUCEK, P., *Řízení bezpečnosti informací*, s 85.

v úvahu charakteristické činnosti a cíle organizace, organizační strukturu, umístění jednotlivých součástí a také technologie používané pro přenos.[22]

2.6.2 Prohlášení o politice ISMS

To vzniká na základě potřeb organizace. Politika ISMS by měla:

- Upřesnit cíle ISMS a definovat základní směr a rámec pro řízení bezpečnosti informací,
- Zohlednit cíle a požadavky organizace, zákonů a smluv,
- Vytvořit potřebné vazby pro budování a údržbu ISMS v dané organizaci,
- Stanovit kritéria pro popisování a hodnocení rizik,
- Být schválena vedením organizace.[23]

2.6.3 Pravidla a postupy řízení rizik

Řízení rizik je pro řízení informační bezpečnosti klíčovým nástrojem. Blíže je zpracováno v kapitole 2.7**.**

2.6.4 Souhlas vedení se zavedením ISMS a zbytkovými riziky

Je nutné, aby vedení odsouhlasilo návrh bezpečnostních opatření nutných pro snížení bezpečnostních rizik. V souvislosti s tím by se mělo vyjádřit, zda jsou existující zbytková rizika pro chod organizace přijatelná. Pokud vedení zjistí, že výsledky řízení rizik nevedou k požadované úrovní bezpečnosti, je možné upravit návrh bezpečnostních opatření.[24]

2.6.5 Prohlášení o aplikovatelnosti

„Prohlášení o aplikovatelnosti je dokumentované prohlášení popisující cíle opatření a jednotlivý bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace.“[25]

[22] DOUCEK, P., *Řízení bezpečnosti informací*, s 87.
[23] ONDRÁK, V., *Problematika ISMS v manažerské informatice*, s. 105 – 106.
[24] DOUCEK, P., *Řízení bezpečnosti informací*, s. 85 – 88.
[25] ISO 27 001:2006, s. 4.

V praxi se jedná o nejdůležitější dokument, který postihuje systémové vazby ISMS a zobrazuje matici vztahů mezi zjištěnými riziky a vybranými bezpečnostními opatřeními.

Prohlášení o aplikovatelnosti plní i zpětnou vazbu. Pomocí něj můžeme zkontrolovat, zda došlo k pokrytí všech identifikovaných rizik příslušnými opatřeními.[26]

2.7 Zavádění a provoz ISMS

V této etapě se prosazují bezpečnostní opatření tak, jak byla navržena v předchozí. Důležité je upřesnit termíny, odpovědné osoby apod. Vše by mělo být zdokumentováno v Příručce bezpečnosti informací. Během této etapy by měly být provedeny následující činnosti:

- Formulovat dokument Plán zvládání rizik a začít s jeho zaváděním,
- Zavést plánovaná bezpečnostní opatření a vytvořit příručku bezpečnostní informací,
- Definovat program budování bezpečnostního povědomí a provést přípravu a školení uživatelů,
- Upřesnit způsoby měření účinnosti a sledovat vybrané ukazatele,
- Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty,
- Řídit zdroje, dokumenty, záznamy ISMS atd.[27]

2.7.1 Plán zvládání rizik

Popisuje všechny činnosti ISMS, které jsou potřebné pro řízení rizik, stanovené cíle a priority těchto činností, omezující faktory a potřebné zdroje. Důležitým prvkem je také určení odpovědnosti za provádění jednotlivých činností. Plán bývá sestaven dle podkladů získaných při ustanovení ISMS (především ve zprávě o hodnocení rizik a v prohlášení o aplikovatelnosti) a dle podnětů získaných při pravidelném

[26] DOUCEK, P., *Řízení bezpečnosti informací*, s. 101.
[27] DOUCEK, P., *Řízení bezpečnosti informací*, s. 104 - 116.

přehodnocování ISMS vedením organizace. Do plánu je možné zapracovat činnosti potřebné ke snižování bezpečnostních rizik.[28]

2.7.2 Příručka bezpečnosti informací

Bezpečnostní pravidla bývají nejčastěji definována pomocí dokumentů jako bezpečnostní politiky či bezpečnostní principy, pravidla, zásady odpovědnosti a které jsou často nazývány jako příručka bezpečnosti informací. Ta musí být napsána tak, aby byla pro cílové skupiny snadno pochopitelná a srozumitelná.[29]

2.7.3 Prohlubování bezpečnostního povědomí

Jedná se o jeden z nejdůležitějších prvků při prosazování ISMS, protože pokud uživatelé nebudou dodržovat pravidla, pak zabezpečení nebude účinné. Všem pracovníkům je nutné srozumitelně vysvětlovat bezpečnostní principy a pravidla, seznamovat je s bezpečnostními riziky a projednávat s nimi bezpečnostní incidenty, jejich příčiny i následky. Lidský faktor je nejslabším článkem ISMS, proto je nutné na něj dávat velký důraz. Jedině systematickou komunikací s pracovníky lze zajistit větší odolnost lidského faktoru.[30]

2.7.4 Měření účinnosti ISMS

Již v etapě plánování je nutné naplánovat měření účinnosti. Je nutné definovat a pravidelně sledovat objektivní údaje o skutečném fungování systému řízení bezpečnosti informací. Nejdůležitější je z hlediska účinnosti etapa plánování – vstupní analýza rizik, na jejíž kvalitě záleží i kvalita ISMS. V této etapě jsou také nejnižší náklady na odstranění chyby v ISMS.

Ukazatele pro měření bezpečnosti lze rozdělit dle předmětu měření do tří skupin:

- finanční,
- personální,
- technické – ukazatele provozu IS/ICT.[31]

[28] DOUCEK, P., *Řízení bezpečnosti informací*, s. 104.
[29] Tamtéž, s. 105.
[30] Tamtéž, s. 106.
[31] Tamtéž, s. 106.

2.7.5 Řízení provozu, zdrojů, dokumentace a záznamů ISMS

Tato fáze je posledním bodem zavedení ISMS. Nestačí ale pouze postupovat podle dohodnutých pravidel, ale je nutné i shromažďovat podklady pro další fázi monitorování. Pro umožnění kontroly fungování ISMS je podstatné vytvořit definovaná pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace řízení bezpečnosti.

Je také podstatné vytvářet záznamy o jednotlivých provedených úkonech ISMS, sledovat, zda jsou potřeby ISMS pokryty dostatečným množstvím odborných zdrojů a řídit jejich používání. Podstatným požadavkem je definice postupů a opatření pro řízení incidentů.[32]

2.8 Monitorování a přezkoumání ISMS

Hlavním úkolem této etapy je zajištění účinné zpětné vazby. Mělo by proto dojít k prověření všech aplikovaných bezpečnostních opatření jejich důsledků na ISMS. Ověření začíná přímou kontrolou odpovědných osob. Důležitou roli sehrává také nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů. Cílem je připravit dostatek podkladů o fungování ISMS za účelem přezkoumání, zda je realizace ISMS v souladu s obecnými potřebami organizace. Tato část zavádění obsahuje následující činnosti:

- Monitorování a ověření účinnosti prosazení bezpečnostních opatření,
- Provedení interních auditů ISMS, jejichž náplň pokryje celý rozsah ISMS,
- Příprava zprávy o stavu ISMS a následné přehodnocení ISMS na úrovni vedení organizace.[33]

2.8.1 Provádění kontrol ISMS

Zpětná vazby je pro fungování ISMS nezbytná, proto je nutné provádět pravidelné kontroly. Součástí musí být i schopnost včasné detekce chyb a pokusů o narušení bezpečnosti či schopnost sledování bezpečnostních událostí a včasné detekce

[32] DOUCEK, P., *Řízení bezpečnosti informací*, s. 117.
[33] Tamtéž, s. 117.

bezpečnostních incidentů. Podněty je nutné následně promítnout do aktualizace příslušných dokumentů a plánů ISMS.[34]

2.8.2 Přezkoumání ISMS vedením organizace

Přezkoumání by mělo probíhat pravidelně a to nejméně jednou za rok. Mezi vstupy přezkoumání patří informace o fungování ISMS. Pozornost by měla být věnována zvláště následujícím kritériím:

- Výsledkům provedených auditů ISMS,
- Zpětné vazbě od zainteresovaných uživatelů a třetích stran,
- Existujícím slabinám a hrozbám, které mohly být při analýze rizik podceněny,
- Výsledkům měření účinnosti ISMS,
- Změnám, které ovlivňují ISMS,
- Získaným doporučením pro další zlepšování ISMS.

Na základě těchto podnětů by měly být silné a slabé stránky ISMS posouzeny pomocí SWOT analýzy.[35]

2.9 Údržba a zlepšování ISMS

V poslední etapě se jedná především o sběr podnětů ke zlepšení ISMS a nápravě všech nedostatků. Je nutné provést následující činnosti:

- Zavádět identifikované možnosti zlepšení ISMS,
- Provádět odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků.[36]

2.9.1 Soustavné zlepšování ISMS

Zpětná vazba zavedená v systému musí odhalovat nedostatky a jejich příčiny a na tyto podněty reagovat. Podněty by měly pocházet od uživatelů na všech úrovních

[34] DOUCEK, P., *Řízení bezpečnosti informací*, s. 117.
[35] Tamtéž, s. 118.
[36] Tamtéž s. 119 – 121

hierarchie. Důležitá je motivace pracovníků na účasti při všech činnostech spojených s ISMS.[37]

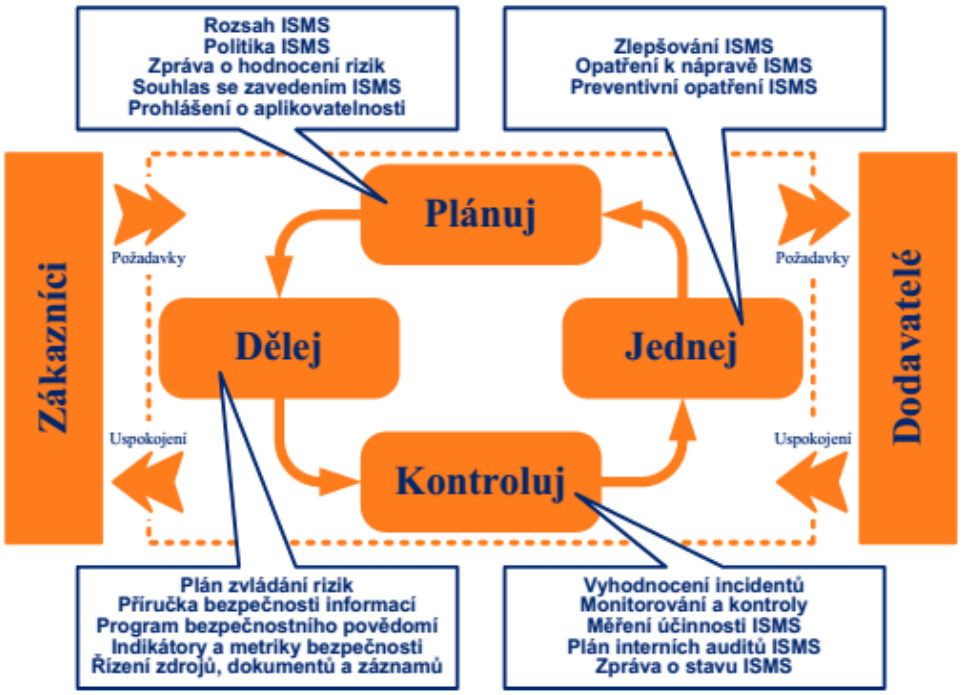
2.9.2 Odstraňování nedostatků ISMS

Nedostatky odstraníme opatřeními k nápravě nebo preventivními opatřeními. Opatření k nápravě reaguje na nedostatek, který se již projevil, naopak preventivní opatření vychází z toho, že se zjištěný nedostatek ještě neprojevil, ale v budoucnu by mohl způsobit vážnější problémy.

Při odstraňování nedostatků je nutné vzít v úvahu všechny souvislosti a opatření realizovat tak, aby se omezily možnosti jejich opakování. Všechny postupy je nutné dokumentovat a po zavedení opatření přezkoumat, zda jsou účinná. [38]

2.10 Shrnutí

Celý cyklus ISMS můžeme shrnout následujícím obrázkem:



Obr. č. 4 - Model PDCA pro řízení bezpečnosti informací (Zdroj: NOVÁK, L, *Systém řízení informační bezpečnosti*, s. 4.)

[37] Tamtéž s. 119 – 121
[38] DOUCEK, P., *Řízení bezpečnosti informací*, s. 114 – 120.

2.11 Bezpečnost

Ve společnosti můžeme bezpečnost vnímat z několika různých hledisek, z nichž každé má různá kritéria. Základní oblasti jsou uvedené v následujících čtyřech podkapitolách.

2.11.1 Personální bezpečnost

„*Největším bohatstvím organizace jsou vzdělaní a výkonní lidé*“[39]

Bezpečnostní hrozbou je v tomto případě pracovník, jehož zájmy nejsou totožné se zájmy organizace. Představuje potenciální hrozbu, jejíž vliv je velmi těžké odhadnout. Pro snížení této hrozby je nutné vždy vyžadovat reference z dřívějších působišť, využívat psychologické testy uchazečů o zaměstnání, testy odbornosti apod. Po přijetí má pracovník omezený přístup k citlivým informacím a postupně získává rozsáhlejší bezpečnostní oprávnění.

Kromě toho je nutné neustále sledovat, jak průběh zpracování uživatelských programů, tak jejich testování i rutinní provoz. Je nutné provádět všechny druhy kontroly od fyzické, personální, softwarové, hardwarové a dalších. [40]

2.11.2 Komunikační bezpečnost

Komunikační cesty IS představují jedno z nejdůležitějších, ale také nejzranitelnějších míst. V počítačových sítích hrozí nebezpečí odposlechu a modifikace odesílaných a přijímaných dat třetí stranou. Je potřeba také dbát na management přístupu k datům na serverech a omezit přístup jednotlivých uživatelů na nutné minimum, které potřebují ke své práci.[41]

[39] POŽÁR, J., *Informační bezpečnost*, s. 147.
[40] Tamtéž, s. 147.
[41] Tamtéž, s. 147 – 148.

2.11.3 Fyzická bezpečnost

„Bezpečnost každého informačního systému začíná u vchodu do objektu“[42]

Je nutné zabezpečit také budovy, ve kterých je IS umístěn, před přírodními vlivy, povodněmi či požáry a proti neoprávněnému vniknutí osob do objektů. Cílem je eliminace případné hrozby ještě dříve, než nastane.

Zaměstnanci by měli mít přístup pouze do prostor, kde pracují a potřebují se pohybovat. To je možné řešit pomocí přístupových karet. Přes vrátnici by neměl nikdo projít bez doprovodu někoho ze zaměstnanců.

Výpočetní techniku je nutné chránit také proti výpadkům proudu či proti přepětí v elektrické síti. To je nelépe proveditelné pomoci on-line UPS s přepěťovou ochranou.[43]

2.11.4 Bezpečnost IS/IT

Bezpečnost IS/IT se je v současnosti jednou z klíčových součástí informační bezpečnosti. Nejčastěji ji má na starosti manažer bezpečnosti, který by měl být v každé společnosti jmenován. Je nutné zajistit zejména dostatečnou ochranu dat v informačních systémech, zejména takových, která by mohla být lehce zneužita.[44]

2.12 Zákonné požadavky

Bezpečnost informací je kromě mezinárodních norem upravena také českými zákony, které požadují ochranu některých druhů informací. Jedná se zejména o Zákon č. 101/2000 Sb. o ochraně osobních údajů a o Zákon č. 89/2012 Sb. občanský zákoník, který upravuje obchodní tajemství.[45]

2.12.1 Zákon o kybernetické bezpečnosti

V roce 2015 vstoupil v platnost zákon č. 181/2014 Sb. o kybernetické bezpečnosti, který je *„milníkem v české legislativě, krokem k vyšší bezpečnosti v digitálním prostředí státních institucí i firem“*. Zároveň může tento zákon sloužit jako

[42] DOBDA, L., *Ochrana dat v informačních systémech*, s. 48.
[43] Tamtéž, s. 50 – 65.
[44] KUNDEROVÁ, L. *Bezpečnsot IS/IT*, s. 1.
[45] DOUCEK, P., *Řízení bezpečnosti informací*, s. 139.

vhodné „*vodítko*“, jak se postavit k problematice bezpečnosti informací. Nabízí kompletní návod na ustavení základů bezpečnosti ve společnosti a jejího následného vylepšování. Můžeme říci, že odpovídá standardu ČSN ISO/IEC 27 001. Tedy pokud společnost má zavedenu tuto normu, je připravena na splnění požadavků zákona. Zákon upravuje následující oblasti:

- systém řízení bezpečnosti informací,
- organizační bezpečnost,
- řízení dodavatelů,
- klasifikace aktiv, která zahrnuje pravidla pro bezpečné nakládání s aktivy,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací,
- řízení přístupu,
- bezpečné chování uživatelů,
- používání kryptografické ochrany,
- nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.

Zákon o kybernetické bezpečnosti se vztahuje pouze na vybrané subjekty, které definuje v §3. Je ale zřejmé, že tento zákon může být využit i ve společnostech, které mu přímo nepodléhají, v rámci zavedení systému řízení bezpečnosti informací.[46]

[46] KRÁTKÝ, Pavel. *Zákon o kybernetické bezpečnosti v praxi*.

3 Analýza současného stavu

3.1 Popis podniku

Vybraná společnost si nepřeje, z důvodu citlivosti informací uvedených v této diplomové práci, být jmenována. Proto uvádím pouze její stručnou charakteristiku.

Jedná se o malou poradenskou agenturu, která se zabývá daňovým zvýhodněním výzkumu a vývoje, dotacemi na investice, inovace, výzkum a vývoj, daňovým poradenstvím, podnikovým poradenstvím a vedením výběrových řízení. Společnost má 16 zaměstnanců a sídlí v Brně. Kromě toho má také z kapacitních důvodů odloučené pracoviště, které je rovněž v Brně.

Správa ICT je zde řešena formou outsourcingu. Všechny ICT prvky spravuje externí pracovník, který je rovněž správcem serveru. V rámci organizačního diagramu spadá správa ICT pod majitele a zároveň ředitele společnosti, který ji dále deleguje na jednoho ze zaměstnanců.

Vedení společnosti zajišťují dva společníci. Dále je stanoven projektový a produktový manažer, obchodní referent. Ve společnosti dále pracuje několik účetních a několik specialistů technické dokumentace.

3.2 Infrastruktura

V sídle společnosti je umístěn server se všemi důležitými daty využívanými pro podnikání. Každý zaměstnanec má své PC, na kterém pracuje. Vzhledem k tomu, že někteří zaměstnanci nepracují na plný úvazek, neodpovídá počet PC počtu zaměstnanců a na některých PC se zaměstnanci střídají. Každý z nich má ale vlastní přístupové údaje a vlastní profil.

Server může využít vlastní záložní zdroj (UPS), který ho udrží v provozu přibližně 30 minut. Server je nastaven tak, aby se v případě výpadku dodávky elektrické energie sám přivedl k bezpečnému ukončení provozu. Úložný prostor serveru je složen ze dvou disků o kapacitě 1 TB zapojených v režimu RAID 1, tedy zrcadlení. Server funguje pod operačním systémem Windows Small Business Server 2011. Je zde instalována serverová verze antiviru ESET a dále je aktivní firewall implementovaný

přímo do OS: Přístup k datům uloženým na serveru je řízen pomocí Group Policy v prostředí Active Directory.

Server je také v pravidelných intervalech zálohován. Každý týden je server zálohován na notebooky vedoucích pracovníků. Zálohy jsou šifrovány pomocí PGP a každý z vedoucích pracovníků má vlastní 256 bitový AES klíč. Kromě toho je jednou měsíčně obsah serveru zálohován na vzdálené úložiště, kde jsou uložená data šifrována stejným způsobem.

Na server je možné přistupovat pomocí VPN. Připojení je zajišťováno bezpečným protokolem PPTP. Na serveru je vytvořena skupina uživatelů VPN, která definuje uživatele s povoleným přístupem pomocí VPN. Autentizace a autorizace probíhá pomocí stejného přihlašovacího jména a hesla, jaké je využíváno pro přihlášení na PC. Přístup pomocí VPN do firemní sítě využívají především vedoucí pracovníci, když jsou mimo prostory sídla společnosti. Přístup je možný z jakékoliv sítě. Dále je tento přístup využíván na odloučeném pracovišti (viz níže).

Síť je řešena pomocí metalického vedení. Kabely jsou uloženy v lištách. V některých místnostech (zejména v zasedací místnosti) nejsou kabely uloženy v lištách, ale pouze přilepeny pod stůl, a končí v přípojném bodě pro notebooky návštěvníků. V sídle společnosti je k dispozici také wi-fi síť. Tu mohou využívat návštěvníci a je oddělena od vnitřní sítě. Kromě toho je zabezpečena heslem a šifrována.

Všechna důležitá data jsou umístěna na serveru a tam s nimi také zaměstnanci pracují. Na jednotlivá PC žádná data ukládána nejsou. Je tam pouze nainstalován OS a podpůrný software.

Dalším PC je firemní notebook, se kterým jezdí zaměstnanci na jednání k jednotlivým klientům. V notebooku rovněž nejsou uložena žádná data, pouze je zde instalován podpůrný software. Před návštěvou klienta jsou do notebooku vždy nakopírována data o daném klientovi a po skončení jednání jsou daná data smazána pomocí běžné funkce pro mazání využitelné v systému MS Windows.

Internet je přiveden poskytovatelem. Hned za modemem / routerem poskytovatele je umístěn switch HP ProCurve (switch s managementem a podporou

VPN), přes který je vedena všechna vstupní i výstupní síťová komunikace. Router poskytovatele (Cisco EPC 3925) obsahuje firewall a zajišťuje NAT.

Ve společnosti je také multifunkční síťová kopírka. Kromě toho mají 2 vedoucí pracovníci k dispozici vlastní barevnou tiskárnu.

Na odloučeném pracovišti jsou prozatím 2 zaměstnanci, ale v budoucnu je plánováno rozšíření počtu zaměstnanců. Tito zaměstnanci potřebují přístup na firemní server, který je řešen pomocí VPN. Ta je zajišťována routerem MikroTik, který přistupuje pomocí protokolu PPTP na server společnosti.

Na modem zajišťující připojení k internetu od jeho poskytovatele je napojen switch společnosti (MikroTik) a od něj vedou síťové kabely k jednotlivým stanicím. Kabely jsou vedeny po zemi bez jakékoliv ochrany. Také switch není žádným způsobem chráněn, ale je položen na vyvýšeném místě pod oknem.

3.3 Bezpečnost podniku

V analyzovaném podniku není bezpečnost informací řešena systematicky. Vedení podniku disponuje základním povědomím o bezpečnosti informací a již zavedlo některá opatření, která tuto bezpečnost zvyšují. Jedná se však spíše o jednotlivé samostatné kroky či opatření, které vznikají nezávisle na sobě dle aktuálních potřeb. Rovněž k těmto opatřením neexistuje téměř žádná dokumentace. Zavedené postupy tedy nejsou dodržovány a ve výsledku je skutečná úroveň zabezpečení nižší, než ta, která byla zavedena managementem společnosti.

3.3.1 Fyzická bezpečnost

Do prostor společnosti mají přístup pouze zaměstnanci. Prostory se nacházejí v rodinném domě, který je celý pronajatý pro účely podnikání. Přístup do budovy mají pouze zaměstnanci. Každý z nich má vlastní klíč k budově, kde se nachází sídlo podnikání společnosti. Do budovy je možné se dostat pouze hlavním vchodem. Pokud přijde do sídla společnosti klient nebo jakýkoliv jiný návštěvník, musí být vpuštěn některým ze zaměstnanců. Zaměstnanci musí každou návštěvu zaznamenat. Pokud přijde např. zaměstnanec pošty, dostane se pouze do tzv. vstupní chodby. Klientům je

dán přístup buď do zasedací místnosti, nebo do kanceláře některého z vedoucích pracovníků.

Pokud v budově žádný ze zaměstnanců není, je zabezpečena elektronickým zabezpečovacím systémem, který je napojen na pult centrální ochrany. Každý zaměstnanec má vlastní kód pro aktivaci a deaktivaci zabezpečovacího systému. Zabezpečovací systém se skládá z pohybových čidel, požárních hlásičů a řídící jednotky s displejem a klávesnicí. Spojení s pultem centrální ochrany je zajišťováno pomocí GSM modulu.

3.3.2 Personální bezpečnost

Zaměstnanci společnosti jsou pečlivě vybíráni v minimálně tříkolovém přijímacím řízení. Přístup k informačnímu systému a datům o zákaznících je jim udělen vždy až po podepsání pracovní smlouvy.

Počítačová gramotnost zaměstnanců je na relativně vysoké úrovni. Každý ze zaměstnanců si pamatuje všechna svá přístupová hesla. Je zakázáno je mít kdekoliv zapsána. Pokud zaměstnanci odcházejí od PC, na které pracují, jsou povinni vždy PC zamknout (pomocí kláves Win + L), aby k němu byl zabráněn přístup neoprávněným osobám.

Kromě předchozích opatření je jednotlivým zaměstnancům poskytován přístup pouze k těm datům, která potřebují ke své práci (pomocí Group Policy v prostředí Active Directory, které běží na serveru společnosti). K dalším datům přístup nemají. Přístup k datům je tedy řízen pomocí přiřazování uživatelů do skupin s různou úrovní přístupu.

Zaměstnanci mají povoleno instalovat na PC volně dostupné programy. Hrozbou by mohla být instalace programu, který není dostatečně zabezpečen nezkušeným zaměstnancem.

3.4 Identifikace aktiv

Informační systém

Společnost používá informační systém pouze pro řízení vztahu se zákazníky. Pomocí IS jsou také řízeny veškeré činnosti související jak s činností podniku, tak s jeho provozem. Pro každodenní fungování podniku je důležitá nepřetržitá dostupnost IS.

Databáze IS je uložena na firemním serveru. Jejich obsluhu zajišťuje informační systém. Klíčová je jak dostupnost dat, tak jejich důvěrnost a integrita. Ztráta nebo kompromitace databáze by měla pro společnost velmi vážné následky, které by mohly vést až k ukončení činnosti.

Všichni uživatelé mají práva pro čtení jakékoliv informace uložené v informačním systému. Pouze k některým projektům je přístup omezen a je umožněn pouze konkrétnímu uživateli. Uživatelé mohou do systému rovněž data přidávat. Pouze vybraným uživatelům je povoleno informace z IS mazat.

Účetní systém

Tento systém je poskytován dodavatelem pomocí vzdálené plochy a pracují s ním účetní podniku. Data obsahují kompletní účetnictví společnosti a rovněž osobní údaje zaměstnanců. Zde by ztráta databáze měla opět velmi vysoký negativní vliv na společnost. Odpovědnost za databázi a bezpečnost dat nese však dodavatel systému.

Sdílené úložiště dat

Sdílené úložiště je umístěno opět na firemním serveru. Je zde uložena veškerá dokumentace zpracovávaná pro klienty od založení společnosti a podklady k této dokumentaci. Jsou zde rovněž uloženy informace o klientech. Kromě toho jsou zde průběžně ukládány dokumenty zpracovávané pro jednotlivé klienty zaměstnanci společnosti. Data jsou na server ukládána do předem dané struktury adresářů. Ty jsou děleny dle jednotlivých oblastí podnikání (např. Daňové poradenství, Dotace) a následně dle jednotlivých klientů. U klientů jsou data dělena dle jednotlivých let. Složka klientů má vždy stejnou závaznou strukturu, na jejíž dodržování je vedením společnosti kladen vysoký důraz.

Některé z těchto dat tvoří součást obchodního tajemství a know-how jednotlivých klientů. Proto by zvláště jejich vyzrazení třetí straně mělo vážné právní

následky pro společnost. Kromě toho by ztráta informací o klientech měla značný dopad na fungování společnosti, protože značnou část dat tvoří dokumenty a soubory poskytnuté klienty a bylo by časové náročné znovu získat všechny dokumenty.

Pracovní PC stanice

Společnost využívá PC Fujitsu řady Esprimo 400, které jsou tvořeny hardwarovou a softwarovou částí. Stanice jsou vybaveny operačním systémem MS Windows 7, na každé stanici je aktivní firewall implementovaný v operačním systému. Každá stanice je rovněž vybavena antivirem od společnosti ESET. Uživatelé mají pravomoci k instalaci jakéhokoliv software a přístup na internet rovněž není žádným způsobem omezen.

Pokud by nastala porucha některé ze stanic, znamenalo by to finanční náklady pro společnost na její opravu, ale vzhledem k tomu, že všechna data jsou ukládána na sdílené úložiště, nemělo by to téměř žádný vliv na činnost společnosti. SW tvoří operační systém a aplikace. Problém se SW by rovněž neměl téměř žádný vliv na činnost společnosti, pouze by bylo nutné znovu zakoupit některé licence, které jsou svázané s danou pracovní stanicí (např. MS Office, OS apod.)

On-line znalostní báze

Společnost využívá pro sdílení znalostí a rovněž pro ukládání veškerých směrnic a doporučených postupů on-line znalostní bázi. Při práci potřebují zaměstnanci mít přístup do této znalostní báze. Její výpadek by měl vliv pouze dlouhodobě. Krátkodobě jsou zaměstnanci schopni pracovat i bez ní. Pokud by došlo ke ztrátě uložených dat, dala by se obnovit, protože vše, co je uloženo v on-line znalostní bázi, je uloženo rovněž na sdíleném firemním serveru, ale bylo by to časově náročné, protože někteří zaměstnanci by se museli věnovat obnově této databáze a došlo by k prodlevám ve zpracovávání některých projektů.

Připojení k internetu

Připojení k internetu je rovněž nezbytné pro zaměstnance, kteří zpracovávají technické dokumenty pro jednotlivé klienty. Pokud by připojení k internetu nefungovalo několik hodin, nebyl by to problém, ale při delším výpadku by to vedlo k opoždění plnění některých termínů.

Výpadek připojení k internetu by rovněž znemožnil jakoukoliv komunikaci, protože by nefungoval e-mail ani VoIP telefony, které jsou ve společnosti využívány.

Kromě předchozích dopadů by výpadek připojení rovněž znemožnil přístup k firemní on-line znalostní bázi.

Dokumenty v papírové podobě

Dokumenty v papírové podobě jsou určeny především pro archivaci dokumentů zpracovávaných pro jednotlivé klienty a také pro archivaci podkladů od klientů získaných. Většina z nich je uložená ve firemním archivu. Ty, které jsou často využívané, jsou uloženy v policích v kancelářích zaměstnanců. Ztráta těchto dokumentů by měla minimální dopad na funkci společnosti, ale problém by mohl nastat, pokud by si klient vyžádal dokumentaci, kterou společnost dle smlouvy musí uchovávat.

Smlouvy

Dalšími ukládanými dokumenty jsou smlouvy. Ty se týkají převážně jednotlivých klientů, ale rovněž jsou obsaženy i smlouvy se zaměstnanci apod. Ty mají mnohem vyšší důležitost nežli ostatní dokumenty, protože z nich vychází všechny obchodní a právní vztahy a v případě právního (nebo i jiného) sporu by při jejich ztrátě hrozily společnosti značné postihy, které by mohly hraničit až s likvidací. Rovněž kdyby se smlouvy dostaly do vlastnictví neoprávněné osoby, hrozilo by jejich zneužití.

3.5 Ohodnocení aktiv

Jednotlivá aktiva byla následně ohodnocena, tedy byly u nich určeny velikosti dopadů při ohrožení jejich důvěrnosti, dostupnosti nebo integrity. Hodnoty byly určeny po konzultaci s vedením společnosti a také jednotlivými zaměstnanci, kteří daná aktiva využívají ke své práci.

Tab. č. 2 - Ohodnocení aktiv (Zdroj: Vlastní zpracování)

aktivum	důvěrnost	dostupnost	integrita	konečná hodnota
IS	5	4	5	5
účetní systém	4	4	4	4
databáze IS	5	5	5	5
dokumenty na sdíleném úložišti dat	5	5	5	5
síťové prvky + kabeláž	5	5	5	5
pracovní PC stanice	3	2	2	2
notebooky vedoucích pracovníků	5	4	4	4
on-line znalostní báze	4	3	3	3
síťová kopírka	2	4	3	3
připojení k internetu	2	2	2	2
vzdálené úložiště pro zálohy	4	4	4	4
www stránky společnosti	2	2	2	2
dokumenty v papírové podobě	3	2	1	2
smlouvy	5	5	5	5

3.6 Identifikace hrozeb

Po konzultaci s vedením společnosti, interním a externím správcem IT byly identifikovány následující hrozby:

Tab. č. 3 - Identifikace hrozeb (Zdroj: Vlastní zpracování)

Popis rizika	Pravděpodobnost
chyby techniky	
selhání HW	3
výpadek připojení k internetu	2
přerušení dodávky elektrické energie	2
Zničení zařízení nebo médií	3
chyby SW	
selhání softwarového vybavení	2
poškození dat	3
chyba zálohování	2
vnější hrozby	
škodlivý software	3
krádež médií	3
krádež dokumentů	3
krádež zařízení	4
útok na webové stránky	2
prolomení nebo odcizení hesla	2
vnitřní hrozby	
chyba údržby	2
zneužití oprávnění	2
chyba uživatele	3
zavlečení škodlivého SW	3
fyzické hrozby	
živelná pohroma	1
vloupání do budovy	1
poškození zařízení zaměstnancem/havárie	2

Nyní jsou identifikována aktiva a hrozby, které by je mohly ohrozit. Na základě konzultace s jednotlivými zaměstnanci a správcem IT byl stanoven dopad, který by mohla mít realizace hrozby, a konečná hodnota úrovně rizik u jednotlivých aktiv byla zanesena do tabulky č. 4.

Tab. č. 4 – Úroveň rizik (Zdroj: Vlastní zpracování)

ÚROVEŇ RIZIKA	Pravděpodobnost/Aktiva	IS	účetní systém	databáze IS	dokumenty na sdíleném úložišti	síťové prvky + kabeláž	pracovní PC stanice	notebooky vedoucích pracovníků	on-line znalostní databáze	síťová kopírka	připojení k internetu	vzdálené úložiště pro zálohy	www stránky společnosti	dokumenty o zakázkách	smlouvy
Hrozby\hodnota aktiva		5	4	5	5	5	2	4	3	3	2	4	2	2	4
chyby techniky															
selhání HW	3	30	24	45	60	45	30	60	18	36					
výpadek připojení k internetu	2		24						18		20	24			
přerušení dodávky elektrické energie	2						16	16			20				
Zničení zařízení nebo médií	3	30	24	45	45	60	24	48		36		48			
chyby SW															
selhání softwarového vybavení	2	40	32	50			12	24	24						
poškození dat	3	30	24	75	75				27			60			
chyba zálohování	2			30	30										
vnější hrozby															
škodlivý software	2	30	24	30	30										
krádež dokumentů	2													20	40
krádež zařízení	2					20	12	32		6					
útok na webové stránky	1												10		
prolomení nebo odcizení hesla	3	60		45	75				27			36			
vnitřní hrozby															
chyba údržby	2						16	24		18	16	24			
zneužití oprávnění	2	40	32	50	50				24			40	16		
chyba uživatele	2	30	24	30	40		16	32	18	12		24			
zavlečení škodlivého SW	3	45	36	60	60		18	36				36			
fyzické hrozby															
živelná pohroma	1			20	20	20	10	20		15	8	16		10	20
poškození zařízení zaměstancem/havárie	2						16	32		24	16				

Jednotlivé úrovně rizik byly následně klasifikovány do tří skupin. Podle toho, do které skupiny jsou daná rizika zařazena, budou k těmto rizikům navrhována opatření. Pro klasifikaci rizik jsou využity tři úrovně (viz tabulka č. 5).

Tab. č. 5 - Úrovně rizik (Zdroj: Vlastní zpracování)

Hodnota rizika	Klasifikace rizika
1 až 20	Nízké
21 až 45	Střední
46 až 75	Vysoké

Bylo identifikováno 15 rizik, u kterých je vysoká úroveň rizika. Po konzultaci s vedením společnosti bylo rozhodnuto, že budou nejprve zavedeny směrnice dle normy ISO 27 001 a následně bude rozhodnuto, zda budou aplikována další opatření ošetřující rizika, která byla zvýrazněna červenou barvou.

4 Návrh řešení

Tato kapitola popisuje postup zavedení systému řízení bezpečnosti informací podle normy ISO 27 001 ve společnosti. Uvádí jednotlivé kroky zavádění normy, opatření proti rizikům a rovněž uvádí plánované náklady. Vše je zpracováno v příručce bezpečnosti informací, která se stane výchozím zdrojem pro zavedení normy ISO 27 001. Při návrhu opatření vycházím z norem ČSN ISO/IEC 27 001 a ČSN ISO/IEC 27 002. Seznam opatření dle normy ISO 27 001 je uveden v příloze č. 1 diplomové práce.

4.1.1 Porozumění organizaci a jejímu kontextu

Navržená opatření budou posuzována interními zaměstnanci, kteří rozumí organizaci velmi dobře a jsou schopni efektivně navrhnout opatření k zajištění odpovídající úrovně bezpečnosti informací. Externí subjekt vstupující do řešení je externí správce IT, který může alespoň částečně nabídnout pohled externího pozorovatele.

4.1.2 Porozumění potřebám a očekáváním zainteresovaných stran

Mezi zainteresované strany můžeme zařadit především vedení vybrané společnosti v osobě jednatele a zároveň majitele firmy, který má nejvyšší zájem na utajení know-how a dalších důležitých informací. Důležitým požadavkem je tedy ochrana proti potenciálnímu úniku informací jakýmkoliv způsobem. Mezi zainteresované strany pak lze řadit i klienty dané společnosti, jejichž citlivá data a v některých případech se týkající i know-how těchto společností má vybraná společnost k dispozici.

4.1.3 Stanovení rozsahu systému řízení bezpečnosti informací

Rozsah ISMS definuje, jak široce bude ISMS v podniku zavedeno. Vedení vybraného podniku stanovilo rozsah ISMS na všechny interní HW i SW systémy, zaměstnance a všechny další osoby, které v rámci vybrané společnosti uskutečňují jakékoliv práce (tzn. údržbář, externí správce IT, mzdová účetní apod.). Jedná se většinou o živnostníky, kteří pracují pod vlastním jménem, ale často pracují s daty nebo

zařízením, které souvisí s činností společnosti. Dále bude nutné zahrnout i prostory podnikání a každého, kdo se v těchto prostorech bude pohybovat.

4.2 Vůdčí role

4.2.1 Vůdčí role a závazek

V rámci zavádění norem pro řízení bezpečnosti informací bude podepsán dokument v následujícím znění:

Vedení společnosti se zavazuje, že bude podporovat zavedení systému pro řízení bezpečnosti informací. Cíle budou podporovány finančně i z hlediska organizačních změn nutných pro zavedení opatření vyžadovaných normou ČSN ISO/IEC 27 001. Dále vedení určí pracovníky pověřené řízením bezpečnosti informací a bude zajišťovat jejich pravidelné školení. V rámci dodržování cyklu PDCA bude vedení společnosti dbát na neustálou kontrolu a zlepšování úrovně řízení bezpečnosti informací.

4.2.2 Politika

Cílem zvýšení bezpečnosti informací je zejména zajištění dostatečné ochrany informací a zabránit neoprávněnému nakládání s informacemi v různých formách.[47] Mezi dílčí cíle politiky ISMS jsou zařazeny následující:

- Systém řízení bezpečnosti informací tvoří součást všech procesů probíhajících ve společnosti a je nutné dodržovat závazky.
- Pomocí systému řízení bezpečnosti informací bude klientům i zaměstnancům společnosti poskytována dostatečná jistota, že jejich osobní informace a know-how nebudou vyzrazeny třetí straně.
- Všechna zavedená opatření budou pravidelné kontrolována a revidována vedením společnosti a pověřenými zaměstnanci.
- Vedení společnosti bude zajišťovat dostatečné proškolení všech zaměstnanců v oblasti informační bezpečnosti.

[47]DOUCEK, P., *Řízení bezpečnosti informací*, s. 88 – 89.

4.2.3 Role odpovědnosti a pravomoci organizace

Odpovědnosti a pravomoci pro:

- Zajištění shody systému řízení bezpečnosti informací s požadavky normy ISO 27 001 budou svěřeny zaměstnanci určenému interní směrnicí jako manažer bezpečnosti.
- Podávání zpráv o výkonnosti systému řízení bezpečnosti informací vedení společnosti bude rovněž zajišťovat zaměstnanec určený interní směrnicí jako manažer bezpečnosti.

4.3 Plánování

4.3.1 Posuzování rizik bezpečnosti informací

Posouzení rizik bezpečnosti informací včetně jejich klasifikace je uvedeno v kapitole 2 této práce.

4.3.2 Ošetření rizik bezpečnosti informací

Analýza rizik je uvedena v kapitole 2.7. K těmto rizikům nyní budou určena opatření, která sníží jejich pravděpodobnost nebo dopad na analyzovanou společnost. V téže kapitole je uvedena tabulka, která klasifikuje rizika do tří úrovní. Vedení společnosti se rozhodlo, že rizika označená jako nízká budou akceptována a nebudou k nim navržena opatření. Rovněž bude u těchto rizik zavedeno jejich sledování, aby mohla být v případě zvýšení jejich hodnoty včas zabráněno nepříznivým následkům. Největší pozornost bude věnována rizikům označeným jako vysoká. Tato rizika budou ošetřena metodou redukce. U rizik označených jako střední bude provedena kontrola po zavedení opatření proti vysokým rizikům a pokud bude shledáno, že opatření proti vysokým rizikům mělo vliv i na některá z těchto rizik, budou přesunuta mezi nízká rizika. Zbylá střední rizika budou ošetřena opatřeními dle uvážení vedení společnosti. Nejprve však budou zavedena opatření popsána

Opatření využitelná pro snížení rizik uvádí norma IS0 27 001 v příloze A. Proto jsem se rozhodl, že nejlepším způsobem pro snížení identifikovaných rizik bude využití této přílohy. Výběr doporučených opatření je uveden v příloze 1 této práce.

Zavádění opatření dle normy ISO 27 001 bude probíhat ve více etapách. Je to způsobeno tím, vedení společnosti není nuceno v brzké době získat certifikát dle této normy. Cílem vedení je zejména pečlivé zavedení normy. Rovněž je však mít na paměti požadavek na přednostní řešení kritických oblastí, jejichž opomenutí by mohlo mít vážné následky v podobě ohrožení bezpečnosti společnosti.

V první fázi zavádění budou zavedena opatření vyhodnocená jako nutná. Jedná se zejména o opatření A.6.2, A.9.1, A.11.2, A.12.3 a A.13.1.

4.3.3 První fáze

A.9.1.1 Politika řízení přístupu

Ve společnosti je řízen přístup jednotlivých uživatelů k různým informacím pomocí Group Policy v adresářové službě Active Directory. Na základě požadavků jednotlivých uživatelů byly stanoveny skupiny uživatelů s různými oprávněními. Stejné skupiny jsou definovány rovněž pro přístup do informačního systému a zaměstnanci mají přístup pouze k informacím, které potřebují. Nastavení skupin probíhá za podpory Group Policy.

Pro přístup budou zaměstnanci zařazení do následujících skupin:

- Technické dokumenty – přístup k dokumentům zpracovávaným pro zákazníky a zdrojům pro zpracování těchto dokumentů. Dále umožňuje přístup ke společným šablonám pro různé dokumenty.
- Kancelář – stejný přístup jako skupina technické dokumenty. Dále má přístup k ekonomickým podkladům týkajícím se jednotlivých klientů společnosti.
- Projektový management – stejný přístup jako skupina kancelář. Dále má přístup k souborům týkajícím se řízení projektů
- Personalistika – speciální skupina, která dává přístup k CV uchazečů výběrových řízení a rovněž aktuálních zaměstnanců.
- Administrátor – uživatelé zařazení do této skupiny mají přístup k heslům jednotlivých zaměstnanců, jejich aktivitám a dalším osobním údajům.
- Vedení – vedení společnosti má přístup ke všem souborům na disku.

Náklady na zavedení tohoto opatření jsou společné s náklady v opatření 13.1.3, proto jsou uvedeny níže.

A.9.1.2 Přístup k sítím a síťovým službám

Všem uživatelům je povolen přístup do sítě internet. Dále přistupují na server společnosti, kde jsou uložena všechna data. Přístup k těmto datům je řízen pomocí Group Policy na základě vytvořených skupin. Rovněž mají přístup k multifunkční tiskárně. Přes síť mohou odesílat e-maily, soubory a stahovat soubory.

Síť umožňuje odesílat emaily pouze z emailových schránek společnosti. Je zakázán přístup k webovým stránkám nesouvisející s pracovní činností (facebook.com, další komunikační stránky, youtube.com apod.). Filtrace těchto stránek je nastavována přímo na routeru.

Uživatelé nemají přístup ke správě sítě ani k zálohování pomocí sítě. Spravovat síť může pouze externí správce IT. Ten rovněž sleduje aktivitu jednotlivých uživatelů v síti. Pokud zjistí podezřelé chování, informuje vedení společnosti, které podnikne další kroky.

Náklady na zavedení tohoto opatření jsou společné s náklady v opatření 13.1.3, proto jsou uvedeny níže.

A.11.2.1 Umístění zařízení a jeho ochrana

Ochrana je nutná zejména pro zařízení poskytující podpůrné služby koncovým zařízením. Jedná se tedy zejména o server společnosti a dále o aktivní síťové prvky. Přístupové body bezdrátové sítě wi-fi jsou přichyceny na zeď, takovým způsobem, aby nebyly ohroženy případnou neodbornou manipulací nebo prostou nepozorností osob pohybujících se v prostorách sídla společnosti, tedy ve výšce minimálně dvou metrů nad zemí.

Router v sídle společnosti i na odloučeném pracovišti je umístěn v uzamykatelném rozvaděči. V sídle společnosti je rozvaděč umístěn v uzamčené místnosti. Na odloučeném pracovišti je přichycen na zeď ve výšce dvou metrů v zadní části místnosti. V obou rozvaděčích je umístěn rovněž modem poskytovatele internetového připojení a další síťové prvky nutné pro provoz sítě. Pokud budou v budoucnosti pořizovány další aktivní prvky, budou rovněž umístěny do rozvaděče.

Tab. č. 6 - Náklady na opatření 11.2.1 (Zdroj: Vlastní zpracování)

Rack Triton 19	1 ks	2 400 Kč	2 400 Kč
Instalace	4 hod	350 Kč/hod	1 400 Kč
Celkem			**3 800 Kč**

A.11.2.2 Podpůrné služby

V sídle společnosti i na odloučeném pracovišti je instalována jednotka UPS, která je napojena na rozvaděč elektrické energie a zajistí běh všech zařízení minimálně 15 minut při výpadku proudu. Tato doba byla vyhodnocena zaměstnanci i vedením společnosti jako dostatečná pro uložení rozdělané práce. Doba 15 minut byla zvolena také z toho důvodu, že zaměstnancům společnosti není znám případ, kdy by ve společnosti proběhl delší výpadek elektrické energie.

Tab. č. 7 - Náklady na opatření 11.2.2 (Zdroj: Vlastní zpracování)

APC Smart-UPS C 1000VA LCD	1 ks	9 300 Kč	9 300 Kč
APC Smart-UPS SC 420VA 230V	1 ks	3 400 Kč	3 400 Kč
Instalace	4 hod	350 Kč/hod	1 400 Kč
Celkem			**14 100 Kč**

A.11.2.3 Bezpečnost kabelových rozvodů

Všechny kabelové rozvody jsou vedeny ve žlabech na omítce. Zakončeny jsou přípojnými místy a druhý konec vede do instalovaného rozvaděče. V případě nutnosti dalších kabelových rozvodů budou rovněž instalovány do žlabů, aby bylo zamezeno neoprávněné manipulaci.

Tab. č. 8 - Náklady na opatření 11.2.3 (Zdroj: Vlastní zpracování)

Žlaby	10 m	150 Kč/m	1 500 Kč
Instalace	2 hod	350 Kč/hod	700 Kč
Celkem			**2 200 Kč**

A.11.2.6 Bezpečnost zařízení mimo prostory organizace

Bezpečnost mimo prostory společnosti je nutné zajistit zejména u notebooků. Další přenosná zařízení jsou mobilní telefony, které jsou ale používány pouze pro komunikaci se zákazníky, nikoliv pro ukládání dat. Práce s přenosnými zařízeními se řídí následujícími pravidly:

- Na přenosný počítač pro služební cesty jsou ukládána pouze nezbytná data,

- Všechna data určená pro podnikání na přenosných počítačích vedení společnosti včetně lokálního serveru informačního systému jsou šifrována,
- Na počítačích nesmí být uložena žádná hesla umožňující přístup k firemním datům (např. heslo pro přístup do IS),
- Všechna data uložená na notebook pro služební cesty budou po ukončení služební cesty bezpečně smazána pomocí programu PGP Shredder.

Všichni zaměstnanci jsou jednou ročně školeni o zacházení s přenosnými zařízeními mimo prostory společnosti a jsou povinni dodržovat směrnice.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Všichni zaměstnanci jsou povinni při jakémkoliv opuštění pracoviště softwarově zamykat počítač pomocí kláves Windows + L. Pokud již daný den nebudou na pracovišti, je nutné odhlásit se z počítače a všechny dokumenty (ne elektronické) uklidit do uzamykatelných zásuvek pracovního stolu. Po vytištění dokumentu označeného jako důvěrný je nutné vymazat paměť tiskárny.

A.12.3 Zálohování

Zálohován je server společnosti, na kterém jsou uložena všechna data včetně databáze informačního systému. Data jsou zálohována na externí server poskytovaný externím správcem IT, který je certifikován podle normy ISO 27 001. Zálohování probíhá automaticky jednou každý pátek ve 21:00 formou úplné zálohy serveru. Ve všední dny probíhá zálohování formou přírůstkové zálohy vždy ve 21:00.

Tab. č. 9 - Náklady na opatření 12.3 (Zdroj: Vlastní zpracování)

Nastavení zálohování	2 hod	400 Kč/hod	800 Kč
Celkem			**800 Kč**

A.13.1.1 Opatření v sítích

Ve všech nevyužívaných portech RJ45 jsou aplikovány blokátory.

Celá síť je monitorována externím správcem IT, který kontroluje podezřelé LOG soubory zaměstnanců. Interní správce IT společnosti provádí pravidelnou vizuální kontrolou všech síťových prvků a vedení jednou měsíčně.

Tab. č. 10 - Náklady na opatření 13.1.1 (Zdroj: Vlastní zpracování)

Aplikace blokátorů	1 hod	250 Kč/hod	250 Kč
Cena za blokátory	40 ks	30 Kč/Ks	1 200 Kč
Celkem			**1 450 Kč**

A.13.1.2 Bezpečnost síťových služeb

Dostupnost připojení k internetu je vyžadována na 99,6 %. Za dostupnost připojení je odpovědný dodavatel tohoto připojení. Při výpadku internetového připojení je možné využít mobilní připojení přes telefon některého ze zaměstnanců, kterým byl poskytnut služební telefon.

Tab. č. 11 - Náklady na opatření 13.1.2 (Zdroj: Vlastní zpracování)

Revize smlouvy s dodavatelem	1 hod	350 Kč/hod	350 Kč
Celkem			**350 Kč**

A.13.1.3 Princip oddělení v sítích

V prostorách sídla společnosti jsou k dispozici dvě bezdrátové wi-fi sítě. Jedna je k dispozici hostům, druhá je určena pro zaměstnance. Každá síť má jiné přístupové heslo a obě sítě jsou šifrovány.

Přístup do vnitřní podnikové sítě je povolen pouze zařízením, jejichž MAC adresa je povolena filtrem routeru. Pokud tedy přístupové body nenaleznou připojené zařízení v tabulce povolených MAC adres, je mu poskytnuto pouze připojení k internetu. Tabulka povolených MAC adres je uložena na centrálním routeru, odkud ji mohou získat i další síťové prvky. Přes tento router prochází veškerá komunikace v podnikové síti a také komunikace z podnikové sítě ven.

Tab. č. 12 - Náklady na opatření 13.1.3 (Zdroj: Vlastní zpracování)

Aplikace nastavení oddělení a filtrace, skupin přístupů	6 hod	400 Kč/hod	2 400 Kč
Celkem			**2 400 Kč**

4.3.4 Druhá fáze

Ve druhé fázi zavádění normy ISO 27 001 budou navrženy obecné směrnice upravující strategickou stránku bezpečnosti informačních technologií. Návrh směrnic bude následován jejich implementací v podniku. Druhá fáze bude tedy zaměřena na opatření související převážně s vnitřním prostředím společnosti. V rámci této fáze budou zavedena zbývající vybraná opatření.

A.5.1.1 Politiky pro bezpečnost informací

Vedoucí pracovníci vyjádřili souhlas se zavedením opatření dle normy ISO 27 001. Pro dodržení směrnice bude tento souhlas zapsán a publikován jako podniková směrnice. Následně s ním budou seznámeni všichni zaměstnanci a rovněž externí subjekty, na které se zavedená opatření vztahují.

Politika bezpečnosti informací se řídí následujícími principy:

- Společnost se zavazuje dodržovat všechny legislativní a smluvní požadavky týkající se oblasti bezpečnosti informací.
- Zaměstnanci i subjekty zajišťující externí služby jsou pravidelně školeni a vzděláváni v oblasti bezpečnosti informací.
- Prevence a detekce virů i ostatního škodlivého softwaru pro zachování bezpečnosti hardware a uchovávaných dat je aktivována na všech zařízeních, která ji podporují.
- Zajištění bezpečnosti informačních aktiv pomocí vhodných opatření.
- Pravidelná kontrola plnění cílů informační bezpečnosti a následné návrhy nových opatření.
- Definování odpovědnosti a postihů v případě porušení norem řízení bezpečnosti.

Po zaměstnancích společnosti je vedením vyžadováno zejména:

- Svědomité dodržování všech pravidel stanovených v souladu se systémem řízení bezpečnosti informací.
- Odpovědnost za vlastní činnost spojenou s prevencí chyb.
- Kontrola své práce a neustálé zlepšování v souladu s cyklem PDCA.

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Politiky bezpečnosti informací budou jednou ročně přezkoumávány vedením společnosti a manažerem bezpečnosti. Pokud bude shledán nějaký nedostatek, manažer bezpečnosti navrhne nové znění politiky bezpečnosti. Pokud jej vedení společnosti schválí, začne se používat. Pokud neschválí, manažer bezpečnosti vypracuje novou verzi, která bude opět muset být schválena vedením.

Tab. č. 13 – Náklady na opatření 5.1.2 (Zdroj: Vlastní zpracování)

Přezkoumání politik	20 hod/rok	250 Kč/hod	5 000 Kč
Celkem			**5 000 Kč**

A.6.1.1 Role a odpovědnost bezpečnosti informací

Manažer bezpečnosti zodpovídá vedení společnosti za dodržování všech postupů a opatření týkajících se společných aktiv společnosti.

Za bezpečnost aktiv užívaných pouze určitým zaměstnancem zodpovídá daný zaměstnanec. Manažer bezpečnosti všechny zaměstnance každé pololetí kontroluje, zda dodržují všechna opatření. Rovněž jsou zaměstnanci jednou ročně školeni a přezkušováni ze směrnic upravujících bezpečnost informací manažerem bezpečnosti. Ten může ale kontaktovat rovněž externí společnost.

V souladu s touto směrnicí budou sestavovány pracovní smlouvy, z nichž vyplývají povinnosti jednotlivých zaměstnanců a do těchto smluv budou zaneseny rovněž sankce při nedodržení těchto povinností. Jedná se zejména o pracovní smlouvu manažera bezpečnosti.

Tab. č. 14 - Náklady na opatření 6.1.1 (Zdroj: Vlastní zpracování)

Kontrola zaměstnanců	30 hod/rok	250 Kč/hod	7 500 Kč
Celkem			**7 500 Kč**

A.6.1.2 Princip oddělení povinností

Princip oddělení povinností je stanoven v úrovních přístupu k aktivům společnosti. Přístup do místnosti, kde je uložen server a důležité informace o obchodních zakázkách, je evidován pomocí podpisového archu. Bez podpisu není přístup k této místnosti povolen.

A.6.1.5 Bezpečnost informací v řízení projektů

Bezpečnost informací je dodržována při řízení všech projektů včetně interních nebo přímo nesouvisejících s předmětem podnikání. Před začátkem projektu je zaměstnanec odpovědný za projekt povinen ve spolupráci s manažerem bezpečnosti analyzovat rizika s daným projektem související a navrhnout vhodná opatření. Pro zahájení projektu je nutné písemné schválení manažerem bezpečnosti.

Tab. č. 15 - Náklady na opatření 6.1.2 (Zdroj: Vlastní zpracování)

Přibližné náklady na 5 projektů/rok	15 hod	300 Kč/hod	4 500 Kč
Celkem			**4 500 Kč**

A.7.1.1 Prověřování

Všichni uchazeči o zaměstnání budou prověřeni dle platných zákonů, předpisů a rovněž v souladu s etikou podnikání. Každý uchazeč o zaměstnání bude prověřován zejména pomocí výpisu z rejstříku trestů. Dále o něm budou vyhledány dostupné informace na internetu. Pokud zaměstnanci mají předchozí pracovní zkušenosti, bude od nich vyžadován kontakt na předchozího zaměstnavatele a budou u něj zjišťovány reference. Rovněž budou požadovány doklady o dosaženém vzdělání. Pro získání údajů pro pracovní smlouvu je uchazeč povinen prokázat se občanských průkazem nebo cestovním pasem.

Výše uvedené kroky provádí v průběhu přijímacího řízení personalista společnosti.

Pokud některý ze zaměstnanců postupuje na vyšší pozici, se kterou je spojen přístup k důvěrným informacím, manažer bezpečnosti je povinen vydat potvrzení, že je daný zaměstnanec dostatečně proškolen v oblasti bezpečnosti informací a dodržuje všechna pravidla týkající se řízení bezpečnosti informací.

Prověřovány budou rovněž smluvní strany všech smluv uzavíraných společností. Zejména bude ověřován zápis společnosti v obchodním a insolvenčním rejstříku. Pokud zde budou objeveny nejasné nebo zavádějící informace, bude smluvní strana prověřována u společností, se kterými spolupracovala (na základě referencí apod.).

Tab. č. 16 - Náklady na opatření 7.1.1 (Zdroj: Vlastní zpracování)

Předpokládané náklady/rok	20 hod	300 Kč/hod	6 000 Kč
Celkem			**6 000 Kč**

A.7.1.2 Podmínky pracovního vztahu

Součástí podmínek pracovního vztahu je bezvýhradný souhlas s dodržováním všech vnitřních směrnic organizace, zejména upravujících bezpečnost informací. Součástí je rovněž dohoda o mlčenlivosti týkající se všech informací, které jsou v průběhu pracovního vztahu zaměstnanci poskytnuty. Dále budou v pracovních smlouvách vymezena přesná práva a povinnosti z pracovně právního vztahu vyplývající. V pracovní smlouvě bude rovněž stanovena role a odpovědnost bezpečnosti informací dle bodu A.6.1.1.

Dohodu o mlčenlivosti podepisují rovněž všechny smluvní strany, se kterými společnost vstupuje do kontaktu v rámci své činnosti.

Tab. č. 17 - Náklady na opatření 7.1.2 (Zdroj: Vlastní zpracování)

Revize pracovních smluv	5 hod	300 Kč/hod	1 500 Kč
Revize dalších smluv	20 hod	300 Kč/hod	6 000 Kč
Celkem			**7 500 Kč**

A.7.2 Během pracovního vztahu

A.7.2.1 Odpovědnost vedení organizace

Vedení organizace vyžaduje po všech zaměstnancích dodržování všech směrnic a nařízení souvisejících se systémem bezpečnosti informací. Se všemi povinnostmi zaměstnance seznámí personalista společnosti v průběhu výběrového řízení. Rovněž současně s předáním pracovní smlouvy k podpisu jsou zaměstnanci předány bezpečnostní směrnice společnosti. Zaměstnanci se zavážou rovněž rozvíjet své znalosti související s informační bezpečností pomocí pravidelných školení a dalších akcí nařízených vedením společnosti.

Zaměstnanci mohou pomocí anonymních dopisů ohlašovat porušení bezpečnosti a rovněž porušování zákonů s bezpečnosti informací souvisejících.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Zaměstnanci jsou seznámeni se směrnicemi již při přijetí do pracovního poměru. Během pracovního vztahu jsou povinni podrobit se pravidelnému školení pověřeným zaměstnancem (manažerem bezpečnosti informací), která probíhají jednou ročně. Pověřený zaměstnanec odpovědný za školení všech zaměstnanců bude pravidelně absolvovat školení zaměřené na informační bezpečnost u externích subjektů (Národní bezpečnostní úřad apod.). Rovněž je manažer bezpečnosti povinen soustavně vyhledávat nové informace o bezpečnosti informací a sledovat aktuální hrozby. K nim navrhuje vhodná opatření.

Tab. č. 18 - Náklady na opatření 7.2.2 (Zdroj: Vlastní zpracování)

Školení pro manažera bezpečnosti	10 hod/rok	1 000 Kč/hod	10 000 Kč
Školení zaměstnanců	45 hod/rok	300 Kč/hod	13 500 Kč
Celkem			**23 500 Kč**

A.7.2.3 Disciplinární řízení

Disciplinární řízení bude vedeno se zaměstnanci, kteří nebudou dodržovat směrnice. Sankce bude stanovována vedením společnosti dle závažnosti prohřešku proti informační bezpečnosti. Méně vážné prohřešky budou vyřešeny napomenutím a případným proškolením a následným přezkoušením zaměstnance ze směrnic ISMS. Vážné prohřešky mohou skončit ukončením pracovního poměru. Pokud zaměstnanec nedodržením směrnic způsobí škodu, bude po něm vymáhána její náhrada v souladu se zákoníkem práce.

V rámci disciplinárního řízení mohou být zaměstnanci, kteří dodržují všechny směrnice zaměstnavatele a díky včasné reakci odvrátili hrozící nebezpeční, oceněni finanční odměnou ve výši až 5000 Kč.

A.7.3.1 Odpovědnost při ukončení nebo změně pracovního vztahu

Při ukončení pracovního vztahu budou zaměstnanci přidělené přihlašovací údaje smazány ze systému. Jeho e-mail bude přesměrován na jeho nadřízeného. Za tyto úkony je odpovědný interní správce IT systémů.

Zaměstnanec bude i po skončení zaměstnaneckého vztahu vázán mlčenlivostí vztahující se na všechny informace, které se v průběhu pracovního vztahu dozvěděl, a

nejsou veřejně známé. Tato mlčenlivost bude zakotvena v pracovní smlouvě, kde budou rovněž stanoveny sankce při jejím nedodržení.

Rovněž další smluvní strany jsou po ukončení spolupráce se společností vázány mlčenlivostí vyplývající ze vzájemné dohody o mlčenlivosti.

Náklady na toto opatření jsou společné s opatřením 7.1.2 – jedná se pouze o náklady na revize smluv.

A.8.1.1 Seznam aktiv

Seznam aktiv, který je uveden v kapitole 2.5 této práce, bude vždy v tříměsíčních intervalech aktualizován pověřeným pracovníkem.

A.8.1.2 Vlastnictví aktiv

Vlastníci aktiv jsou určeni následovně:

Tab. č. 19 - Vlastníci aktiv (Zdroj: Vlastní zpracování)

aktivum	vlastník
IS	interní správce IT
účetní systém	externí správce IT
databáze IS	externí správce IT
dokumenty na sdíleném úložišti dat	interní správce IT
síťové prvky + kabeláž	externí správce IT
pracovní PC stanice	interní správce IT
notebooky vedoucích pracovníků	vedoucí pracovníci
on-line znalostní báze	interní správce IT
síťová kopírka	interní správce IT
připojení k internetu	interní správce IT
vzdálené úložiště pro zálohy	externí správce IT
www stránky společnosti	zaměstnanec prověřený marketingem
dokumenty v papírové podobě	pracovník pověřený prací s těmito dokumety

Vlastník aktiv je povinen aktiva pravidelně inventarizovat, zajistit jejich klasifikaci a ochranu. Vlastník aktiva je povinen ve spolupráci s manažerem bezpečnosti pravidelně jednou za 6 měsíců přehodnotit přístupová práva k aktivům a klasifikaci aktiv. Dále je povinen zajistit správný postup při ničení aktiv.

A.8.1.3 Přípustné použití aktiv

Aktiva společnosti mohou být použita pouze v souladu s plněním pracovních povinností. Žádný se zaměstnanců nesmí používat aktiva pro svou osobní potřebu nebo

pro potřeby třetí strany. Přístup k aktivům může být poskytnut třetí straně pouze se souhlasem nadřízeného zaměstnance nebo vedení společnosti.

A.8.1.5 Navrácení aktiv

Při ukončení pracovního nebo jiného smluvního poměru bude pověřeným pracovníkem zajištěno navrácení zapůjčených aktiv, která jsou majetkem společnosti. Tato aktiva budou předávána oproti podpisu pověřeného pracovníka. Pokud nebudou aktiva vrácena, budou zahájeny příslušné právní kroky. To se týká rovněž přístupových údajů a klíčů k budově.

Tab. č. 20 - Náklady na opatření 8.1.5 (Zdroj: Vlastní zpracování)

Revize aktiv a vlastníků	10 hod/rok	350 Kč/hod	3 500 Kč
Předávací procedury	10 hod/rok	350 Kč/hod	3 500 Kč
Celkem			**7 000 Kč**

A.8.2.1 Klasifikace informací

Informace budou klasifikovány dle následující tabulky:

Tab. č. 21 - Klasifikace informací (Zdroj: DOUCEK, P., *Řízení bezpečnosti informací*, s. 139.)

Klasifikace		Označení		Základní popis	
Veřejné informace		Veřejné informace	VI	Informace, které jsou odpovědnou osobou a v souladu s příslušným postupem schváleny ke zveřejnění	
Neveřejné informace		Neveřejné informace	NI	Informace, jejich ohrožení sice může vést k ohrožení zájmů organizace, ale které nenaplňují požadavky nutné pro ochranu ochodního tajemství dle § 504 zákona č. 89/2012 Sb., občanský zákoník,	
Citlivé informace	Důvěrné informace	Důvěrné informace	DI	Informace, u nichž nutnost ochrany vyplývá z legislativních povinností nebo ze smluvních závazků	
				osobní údaje	Informace, u nichž nutnost ochrany vyplývá ze zákona č. 101/2000 Sb., o ochraně osobních údajů
				obchodní tajemství	Informace, u nichž organizace stanovila nutnost ochrany vyplývající z § 504 zákona č. 89/2012 Sb., občanský zákoník
				informace smluvní strany	Informace, u nichž nutnost ochrany vyplývá ze smluvních závazků nebo jiných požadavků
	Přísně důvěrné	Přísně důvěrné informace	PDI	Informace charakteru obchodního tajemství dle § 504 zákona č. 89/2012 Sb., občanský zákoník, jejichž ohrožení vede k poškození strategických a klíčových zájmů organizace	
				citlivé (osobní) údaje	Informace, u nichž nutnost ochrany vyplývá ze zákona č 101/2000 Sb., o ochraně osobních údajů (§9)

A.8.2.2 Označování informací

Ve společnosti je zaveden systém označování souborů v následujícím formátu: RRRRMMDD – Klient – název dokumentu – verze – autor. Do tohoto systému bude přidána další část, která bude označovat důvěrnost dokumentu. Nový způsob označování bude tedy následující: RRRRMMDD – Klient – název dokumentů – označení – verze – autor.

Například podklady poskytnuté 22. 5. 2015 klientem VUT by byly označeny následovně: 20150522 – VUT – podklady pro dokumentaci – DI – v01 – JNovák.

Dokumenty, které nejsou v elektronické podobě, budou označovány na první straně v hlavičce dokumentů označením dle bodu 8.2.1 této směrnice. Dokumenty, které byly vytištěny před datem implementace směrnice, budou označeny nálepkou určující jejich klasifikaci na první straně v pravém horním rohu.

K označení informací bude najat brigádník, který dané dokumenty označí. Odpovědný za provedenou práci bude manažer bezpečnosti.

Tab. č. 22 - Náklady na opatření 8.2.2 (Zdroj: Vlastní zpracování)

Označení stávajících aktiv	40 hod	150 Kč/hod	6 000 Kč
Označení elektronických aktiv	40 hod	150 Kč/hod	6 000 Kč
Průběžné označování aktiv	20 hod/rok	300 Kč/hod	6 000 Kč
Celkem			**12 000 Kč**
Celkem další roky			**6 000 Kč**

A.8.2.3 Manipulace s aktivy

Pouze s aktivy označenými jako veřejné informace může být volně nakládáno. S důvěrnými informacemi mohou zaměstnanci nakládat pouze v souladu s pracovními povinnosti, v žádném případě je nesmí vynášet nebo odesílat z prostor zaměstnavatele nebo odesílat jakýmkoliv způsobem.

Přísně důvěrné informace mohou být zpřístupněny pouze těm zaměstnancům, kteří je nutně potřebují pro výkon své práce. Ostatní zaměstnanci k nim přístup nemají povolen.

Manipulace s jakýmikoliv aktivy mimo prostory společnosti může být provedena pověřeným zaměstnancem pouze na přímý příkaz jednoho z vedoucích pracovníků.

Pro zajištění vhodné úrovně manipulace s aktivy bude zakoupena uzamykatelná skříň, do které budou ukládány dokumenty označené jako důvěrné. Uzamykatelná skříň bude umístěna v místnosti, kde je umístěn server. Přísně důvěrné dokumenty budou ukládány do trezorů umístěných v kancelářích vedení společnosti. O každém uloženém dokumentu bude veden zápis v elektronickém evidenčním archu.

A.8.3 Manipulace s médii

Společnost žádná výměnná média nepoužívá, proto není nutné se jimi ve směrnici zabývat. Na média využívaná v jednotlivých pracovních stanicích nejsou ukládány žádné klasifikované informace, vše je na serveru.

Likvidaci médií má na starosti externí správce IT. Ten je povinen využít softwarových nástrojů pro mazání a formátování disků, které znemožní obnovu dat.

Dokumenty v papírové formě, které již nejsou potřebné, a není nutné je uchovávat, jsou vždy skartovány.

A.8.3.3 Přeprava fyzických médií

Jediná příležitost, kdy jsou média přepravována, je v případě, že jsou odesílána data některému z klientů a je požadováno jejich odeslání ve formě CD nebo DVD. V tom případě jsou na tato média přenesena požadovaná data, které jsou ale opatřena heslem pro přístup, které je předáno jinou cestou než médium. Média jsou vždy odesílána poštou, pojištěnou zásilkou s garantovaným doručením.

A.9.2.1 Registrace a zrušení registrace uživatele

Přihlašovací jméno a heslo nového uživatele do všech systémů vytvoří pověřený zaměstnanec společnosti (interní správce IT). Tyto údaje společně s údaji o přístupových právech následně předá externímu správci IT, který vytvoří pro nového uživatele účty ve všech systémech. Každému přijatému zaměstnanci budou udělena základní přístupová práva v závislosti na tom, zda je přijat pro vytváření technických dokumentů nebo pro administrativní a účetní činnost. Přidělení dalších uživatelských práv jednotlivým uživatelům musí být schválena vedením společnosti. Skupiny uživatelských práv jsou uvedeny v bodu A.9.1.1.

A.9.2.5, A.9.2.6 Přezkoumání přístupových práv uživatelů, jejich odebrání nebo úprava

Přístupová práva uživatelů budou jednou ročně přezkoumávána pověřeným pracovníkem. Pokud shledá, že uživatelé ke své práci nepotřebují danou úroveň přístupových práv, bude jim snížena.

Pokud některý ze zaměstnanců bude požadovat zvýšení úrovně uživatelských práv, informuje o požadavku pověřeného zaměstnance. Ten po schválení vedením společnosti zajistí úpravu přístupových práv zaměstnance na požadovanou úroveň.

Tab. č. 23- Náklady na opatření 9.2.5 a 9.2.6 (Zdroj: Vlastní zpracování)

Přezkoumání přístupových práv	10 hod/rok	300 Kč/hod	3 000 Kč
Celkem			**3 000 Kč**

A.9.4.3 Systém správy hesel

Všichni uživatelé dostanou pro první přihlášení k počítači, emailu a informačnímu systému jednorázové heslo. To jsou povinni při prvním přihlášení změnit. Nové heslo si nesmí nikam zapisovat ani jej sdělovat jiným osobám. Nastavování prvotního hesla bude s podporou Group Policy.

Uživatelé musí vybrat heslo, které splňuje následující požadavky

- Délka hesla je 8 až 10 znaků,
- Heslo obsahuje alespoň dvě číslice,
- Heslo obsahuje alespoň dvě malá a dvě velká písmena,
- Heslo obsahuje alespoň jeden znak, který není číslice ani písmeno,
- Nesmí obsahovat žádné slovo v jakémkoliv jazyce,
- Nesmí obsahovat znaky po sobě jdoucí na klávesnici,
- Nesmí obsahovat údaje jako datum narození, telefonní číslo, rodné číslo apod.,
- Nesmí obsahovat jméno, přezdívku nebo známý název.

A.10 Kryptografická opatření

Na serveru společnosti je zapnuto šifrování disku pomocí nástroje Bitlocker. Šifrovací certifikát budou mít k dispozici zaměstnanci na svých stanicích a rovněž bude

zálohován. Dále budou šifrovány pevné disky notebooků vedoucích pracovníků pomocí 64 bitového PGP klíče. Jednou ročně budou generovány nové šifrovací klíče, aby byla snížena pravděpodobnost jejich vyzrazení.

Tab. č. 24- Náklady na opatření 10 (Zdroj: Vlastní zpracování)

Nastavení šifrování a klíčů	7 hod	500 Kč/hod	3 500 Kč
Celkem			**3 500 Kč**

A.11.1 Bezpečné oblasti

Všechny osoby, které nejsou zaměstnanci společnosti, se při vstupu do prostor společnosti zapisují do knihy návštěv. Eviduje se čas příchodu, jméno, příjmení, společnost, účel návštěvy a při jejich odchodu je zapsán čas odchodu.

Některé osoby vstupující do společnosti jsou zaměstnancům známé. U těchto osob může zápis do knihy návštěv provést zaměstnanec, který známou osobu vpustí do prostorů společnosti.

Každý zaměstnanec disponuje klíčem od kanceláře, kde se nachází jeho pracovní stůl. Poslední zaměstnanec, který z dané kanceláře odchází, je povinen kancelář zamknout. Dále je povinen zkontrolovat, zda jsou zavřena všechna okna. Každý zaměstnanec rovněž využívá zámek na zásuvkách svého pracovního stolu a při opuštění pracoviště jej vždy zamkne.

Přístup do místnosti, kde je umístěn server a historické dokumenty, má pouze manažer bezpečnosti, který ale může v případě potřeby klíč zapůjčit jinému zaměstnanci. Dále tímto klíčem disponuje jednatel společnosti.

Přírodní katastrofy na místě, kde se nachází sídlo společnosti, nehrozí. Jediná možnost fyzického ohrožení je vloupání. To je ošetřeno alarmem, který je napojen na pult centrální ochrany.

Prostory společnosti budou v ročním intervalu kontrolovány specialistou v oblasti ochrany před přírodními a vnějšími hrozbami.

Je zakázáno pomocí fotografických nebo záznamových zařízení zachycovat dění v prostorách společnosti.

Tab. č. 25- Náklady na opatření 11.1 (Zdroj: Vlastní zpracování)

Kontrola specialistou	1/rok	5 000 Kč	5 000 Kč
Celkem			**5 000 Kč**

A.11.2.4 Údržba zařízení

Server společnosti je měsíčně testován externím správcem IT, zda jsou všechny jeho komponenty plně funkční. Jakákoliv porucha zařízení je ihned hlášena zaměstnancem, který ji zjistí, internímu správci IT. Ten je povinen neprodleně zajistit nápravu.

Servis kopírky probíhá při jakémkoliv problému a je prováděn specializovaným externím pracovníkem, kterého informuje o problému správce kopírky.

Tab. č. 26- Náklady na opatření 11.2.4 (Zdroj: Vlastní zpracování)

Servisní poplatky	20 000 Kč/rok		20 000 Kč
Celkem			**20 000 Kč**

A.12.1.1 Dokumentace provozních postupů

Instalace a konfigurace systémů je prováděna externím správcem IT: Externí správce IT sestavuje a uchovává všechny postupy týkající se instalace a konfigurace systémů.

Pokud nastane chyba při zpracovávání informací, zejména vyznačující se problémy s ukládáním souborů nebo nedostupností serveru, je osoba, která první zjistí tuto chybu, povinna nahlásit ji internímu správci IT, který ji vyřeší sám nebo po konzultaci s externím IT správcem.

Při výskytu jakékoliv chyby je první kontaktní osobou interní správce IT, který bude dále řešit zadaný problém. Pokud interní správce IT není k dispozici, je nutné problém řešit s externím správcem.

A.12.1.2 Řízení změn

Všechny změny ve firemních procesech je nutné projednat s vedením společnosti a manažerem bezpečnosti informací. Po projednání nastane testovací provoz, který bude probíhat po dobu určenou vedením společnosti. Testovací provoz začne po vyhlášení změny zaměstnancům, kterých se změna týká. Během testovacího provozu je ověřováno, zda změna vyhovuje požadavkům na bezpečnost informací.

Pokud testovací provoz proběhne v pořádku, je změna přijata a vyhlášena všem zaměstnancům ve formě vnitropodnikové směrnice.

A.12.2 Ochrana před malwarem

Proti malware je počítačová síť společnosti chráněna firewallem, který automaticky rozpoznává hrozby a pokud je nějaký způsob komunikace podezřelý, ihned jej ukončí. Firewall obsahuje rovněž seznam podezřelých webových stránek, kam je přístup všem zaměstnancům zakázán. Server společnosti je před malwarem chráněn antivirem ESET, který je automaticky aktualizován. Stejným způsobem jsou chráněny jednotlivé počítače využívané ve společnosti.

Zaměstnancům společnosti není povoleno instalovat na využívané stanice jakýkoliv software. Instalace software není na jejich uživatelských účtech povolena vůbec. Pokud potřebují nějaký program instalovat, vznesou požadavek internímu správci IT, který program prověří a následně povolí jeho instalaci.

Pokud je na některém počítači identifikován malware, zajistí správce IT jeho okamžité odpojení od podnikové sítě, na všech ostatních počítačích včetně serveru spustí kontrolu počítače na přítomnost malware. Následně infikovaný počítač vyčistí pomocí antivirového programu.

Tab. č. 27- Náklady na opatření 12.2 (Zdroj: Vlastní zpracování)

Nastavení omezení	10 hod	350 Kč/hod	3 500 Kč
Celkem			**3 500 Kč**

A.12.5. Řízení a kontrola provozního softwaru

Operační systémy, nástroje kancelářského balíků MS Office, informační systém a antivirový program jsou automaticky aktualizovány při vypuštění nové verze daného programu. Aktualizace programů nainstalovaných na vyžádání zaměstnance jsou provedeny pouze na vyžádání zaměstnance po předchozím prověření nové verze manažerem bezpečnosti. Instalace zařízení na více stanic probíhá pomocí Group Policy.

Uživatelé nemají přístup k nastavení informačního systému. Jeho nastavení upravuje pouze interní správce IT, který výraznější změny konzultuje s manažerem bezpečnosti.

A.12.6.2 Omezení instalace softwaru

Zaměstnanci společnosti nemají povoleno instalovat software. Pokud vyžadují instalaci určitého programu, je nutno požádat manažera bezpečnosti, který požadovaný program nejdříve prověří a následně pověří interního správce instalací tohoto programu.

A.13.2.1 Politiky a postupy při přenosu informací

E-maily odesílané klientům obsahující důležité informace, jejichž vyzrazení by znamenalo pro jednu ze stran ztráty, budou šifrovány pomocí veřejného klíče příjemce daného e-mailu. Pokud je příjemcem někdo ze zaměstnanců společnosti, je povinen požadovat, aby druhá strana šifrovala odesílaná data jeho veřejný klíčem.

Tab. č. 28- Náklady na opatření 13.2.1 (Zdroj: Vlastní zpracování)

Nastavení šifrovacích cerifikátů	5 hod	350 Kč/hod	1 750 Kč
Školení uživatelů	1 hod	250 Kč/hod	250 Kč
Celkem			**2 000 Kč**

A.13.2.4 Dohody o důvěrnosti nebo mlčenlivosti

Ve všech smlouvách s externími subjekty jsou vymezeny všechny postupy, metody a dokumenty související s činností společnosti jako součást svého obchodního tajemství, které je tedy nutné chránit. Součástí každé uzavřené smlouvy je dohoda o vzájemné mlčenlivosti (tzv. non disclosure agreement).

Pokud některý ze zaměstnanců získá podezření o nedodržení dohody, je povinen to ihned ohlásit manažerovi bezpečnosti a vedení společnosti. Následně manažer bezpečnosti podezření ověří, a pokud se ukáže jako důvodné, nahlásí vedení společnosti tyto skutečnosti Úřadu pro ochranu hospodářské soutěže.

Tab. č. 29- Náklady na opatření 13.2.4 (Zdroj: Vlastní zpracování)

Revize smluv	5 hod	350 Kč/hod	1 750 Kč
Celkem			**1 750 Kč**

A.15.1.3 Dodavatelský řetězec informačních a komunikačních technologií

Výhradním dodavatelem informačních a komunikačních technologií je externí správce IT, který je certifikován dle normy ISO 27 001. Ten rovněž provádí instalaci technologií a software.

A.16 Řízení incidentů bezpečnosti informací

A.16.1. Řízení incidentu bezpečnosti informací a zlepšování

Po aplikaci všech navrhovaných opatření bude zaveden systém řízení incidentů bezpečnosti informací. Bude určen přesný postup reakce na zjištěné porušení bezpečnosti informací včetně odpovědných osob.

A.16.1.1 Odpovědnosti a postupy

Zaměstnanec je při zjištění bezpečnostního incidentu povinen tento incident okamžitě nahlásit manažerovi bezpečnosti informací. Pokud není manažer bezpečnosti k dispozici, je incident nahlášen internímu správci IT. Hlášení probíhá osobně nebo telefonicky. Povinnost hlásit bezpečnostní incidenty vyplývá z pracovní smlouvy všech zaměstnanců.

Manažer bezpečnosti informací je povinen ihned po nahlášení vyhodnotit incident a aplikovat odpovídající opatření. Tato opatření může konzultovat s vedením společnosti nebo externím správcem IT.

A.16.1.2 Podávání zpráv o událostech bezpečnosti informací

Bezpečnostní incident jsou povinni nahlásit zejména v následujících případech:

- Pokud zjistí, že některé z navržených opatření není dostatečně efektivní.
- Pokud je narušena očekávaná úroveň integrity, dostupnosti nebo důvěrnosti informací.
- Pokud udělá nebo zjistí chybu, která by mohla mít za následek narušení bezpečnosti informací.
- Pokud zjistí nesoulad s vnitřními směrnicemi týkajícími se bezpečnosti informací.
- Pokud zjistí, že byla narušena nebo prolomena opatření fyzické bezpečnosti.
- Pokud zjistí, že některý z informačních systémů se dostal do neočekávaného stavu.
- Pokud zjistí, že hardware nebo software vykazují nedostatečnou nebo špatnou funkčnost.

- Pokud zjistí, že byly porušeny přístupové politiky nebo neadekvátně pozměněna přístupová práva.

A.16.1.3 Podávání zpráv o slabých místech bezpečnosti informací

Pokud některý ze zaměstnanců objeví slabé místo v zabezpečení, je povinen postupovat stejně jako v bodě 16.1.1.

A.16.1.4 Posuzování bezpečnosti informací

Každá událost bezpečnosti informací bude posuzována a bude vyhodnocováno, zda se jednalo o bezpečnostní incident. O incident bezpečnosti informací se bude jednat pouze v případech, že byly ohroženy následující data:

- Finanční výkazy společnosti nebo zákazníků,
- Informace obsahující know-how společnosti nebo zákazníků podléhající ochraně dle občanského zákoníku,
- Osobní informace zaměstnanců nebo externích osob podléhající ochraně podle zákona o ochraně osobních údajů,
- Informace, které jsou klasifikovány jako přísně důvěrné a jejichž ztráta by měla za následek finanční výdaje nebo ztráty převyšující 50 000 Kč.

A.16.1.6 Ponaučení z incidentů bezpečnosti informací

Po každém incidentu bezpečnosti informací manažer bezpečnosti ve spolupráci s interním správcem IT a vedením společnosti vyhodnotí příčiny incidentu a navrhne vhodná opatření, která v budoucnu povedou ke snížení pravděpodobnosti výskytu podobného incidentu.

A.17 Kontinuita řízení bezpečnosti informací

Systém řízení bezpečnosti informací je nikdy nekončící proces. Po vyhlášení bezpečnostní politiky a příručky bezpečnosti informací je nutné neustále postupovat podle PDCA cyklu. Zlepšování systému řízení bezpečnosti úrovně informací záleží zejména na zaměstnancích, kteří jsou v rámci výkonu svých povinností zavázáni rovněž k hlášení bezpečnostních incidentů a potenciálních bezpečnostních problémů. Díky tomu mohou být navrhována nová opatření ošetřující různá rizika. Některá opatření budou přezkoumávána pravidelně manažerem bezpečnosti. Dalším důležitým aspektem

je neustálé vzdělávání manažera bezpečnosti i ostatních pracovníků v oblasti informační bezpečnosti. Tím je zajištěna včasná detekce všech hrozeb a neustálé zlepšování systému řízení bezpečnosti informací.

4.4 Harmonogram zavedení

Zavádění systému řízení bezpečnosti informací započne 1. 6. 2015. Nejprve budou zavedena opatření uvedená v podkapitole 3.3.3. Ta budou zavedena podle následující tabulky.

Tab. č. 30 - Harmonogram zavedení směrnic (Zdroj: Vlastní zpracování)

Opatření	1. - 8. 6.	9. - 18. 6.	19. - 25. 6.	25. - 30. 6.
11.2.1				
11.2.2				
11.2.3				
11.2.6				
9.1.1				
9.1.2				
13.1.1				
13.1.2				
13.1.3				
11.2.9				
12.3.1				

Po dokončení implementace uvedených opatření, která je plánována na konec měsíce června, započne implementace dalších opatření. Ta bude probíhat po zbytek roku 2015. Součástí zavádění mohou být po zvážení managementem také penetrační testy.

4.5 Ekonomické zhodnocení

4.5.1 Reálné náklady

Náklady na zavedená opatření můžeme rozdělit na dva druhy – finanční náklady a pracovní náklady. Finanční náklady jsou přímo vydané peněžní prostředky na zavádění norem a pracovní náklady jsou počítány v hodinách.

Celkové finanční náklady na zavedení navrhovaných opatření byly vyčísleny na 62 250 Kč. V této částce nejsou zahrnuty náklady na vypracování směrnic, neboť ty jsou již součástí této diplomové práce. V nákladech rovněž nejsou zahrnuty penetrační testy. Ty jsou k dispozici v různém rozsahu a různých formách nabízené různými společnostmi. Záleží tedy na rozhodnutí vedení společnosti, jaký rozsah penetračních testů zvolí. V dalších letech budou roční náklady ve výši 87 000 Kč. V těchto nákladech nejsou zahrnuty náklady na opatření proti bezpečnostním incidentům, které reálně nastanou. Podle odhadu by se mohla uvedená částka zvýšit o dalších 10 000 Kč.

Dále společnosti doporučuji provést alespoň vnější penetrační testy, které se pohybují v ceně okolo 3 000 Kč.[48]

4.5.2 Přínosy zavedení ISMS

Vyčíslit přesnou hodnotu přínosů zavedení ISMS je problematickým úkolem, zejména proto, že nelze s dostatečnou přesností určit výši ztrát, která by nastala bez zavedení opatření. Pro alespoň částečné porovnání uvádím tabulku, která vyčísluje ztráty při realizaci některé z hrozeb.

Tabulka 1 - Hrozby a finanční dopad (Zdroj: Vlastní zpracování)

Hrozba	Finanční ztráty/dopad
Vyzrazení důvěrných nebo soukromých informací	až 500 000 Kč, pokuta až 5 000 000 Kč
Vyzrazení smluv a obchodních tajemství	až 1 000 000 Kč
Kompromitace hesla do PC a IS	až 500 000 Kč
Zneužití přístupu k síti, likvidace nebo kompromitace dat	až 500 000 Kč, některá data nenahraditelná
Odcizení přenosného PC - ztráta dat	až 250 000 Kč
Nedostupnost sítě (vnitřní)	až 35 000 Kč/den

V tabulce je uvedena vždy pouze finanční ztráta. Nejsou zde uvedeny ztráty, které by byly spojeny s nedůvěrou stávajících i potenciálních klientů a případné důsledky medializace problémů s bezpečností ve společnosti. Je ale zřejmé, celkové ztráty jsou velmi vysoké a proto je nutné se informační bezpečností zabývat.

[48] AGERIT, S.R.O., *Popis a ceny bezpečnostních testů a služeb*.

Závěr

Cílem této práce bylo provedení návrhu sytému řízení bezpečnosti informací v malé obchodní společnosti. Společnost v nejbližší době neplánuje z různých důvodů certifikaci dle normy ISO 27 001 ani nepodléhá zákonu o kybernetické bezpečnosti, proto bylo možné zaměřit se pouze na některá opatření a jiná upravit pouze obecně a ponechat prostor do budoucna v rámci zlepšování (fáze PDCA Check) systému řízení bezpečností informací.

V diplomové části jsem nejprve shrnul základní poznatky týkající se informační bezpečnosti podle odpovídajících norem a dále zákonné požadavky vyplývající především ze zákona o kybernetické bezpečnosti. Popsal jsem metody, kterých je možno využít při zavádění systému řízení bezpečnosti informací podle normy ČSN ISO/IEC 27 001.

Ve druhé části jsem provedl analýzu vybrané společnosti, jejího ICT zařízení, ale rovněž informačních systémů a některých postupů. Následně jsem identifikoval aktiva, která mají pro společnost nejvyšší důležitost a rizika, kterými by mohla tato aktiva být ohrožena. Výsledkem analýzy bylo stanovení nejvíce ohrožených aktiv.

Třetí část práce obsahuje návrh opatření dle přílohy A normy ČSN ISO/IEC 27 001:2014, které byly vybírány dle normy ČSN ISO/IEC 27 001:2013. Tato opatření bezpečně ošetřila všechna rizika identifikovaná ve druhé části práce a nebylo nutné navrhovat další opatření zaměřená na ochranu nejvíce ohrožených aktiv. Mezi zásadní opatření řadím umístění propojovacích kabelů do žlabů, nutnost změny uživatelských hesel a dále přísnější omezení přístupu jednotlivých zaměstnanců k některým datům.

Součástí poslední části práce je rovněž ekonomické zhodnocení výdajů na aplikaci opatření dle uváděných norem. V prvním roce bude zavedení stát společnost 90 000 Kč a v dalších letech přibližně 60 000 Kč za rok. Může se zdát, že se jedná o vysoké částky, ale pokud vezmeme v úvahu výši ztrát při ohrožení některých informací, již se tato částka jeví jako přijatelné výdaje na prevenci ohrožení informačních aktiv analyzované společnosti a také aktiv zákazníků společnosti, se kterými zaměstnanci rovněž pracují.

Stanovené cíle diplomové práce byly tedy splněny a nyní záleží na vedení společnosti a zaměstnancích, jak navržené směrnice implementují do reálného provozu společnosti. Přestože společnost neplánuje v nejbližší době certifikaci, zavedení ISMS přinese zvýšení zabezpečení a sníží riziko úniku dat. Rovněž již samotná analýza současného stavu je pro společnost přínosem, protože bylo poukázáno na nedostatky v zabezpečení, které nyní budou odstraněny. Po zavedení navržených opatření dojde ke značnému snížení rizik a společnost dosáhne přiměřené bezpečnosti za akceptovatelné náklady. V budoucnosti je důležité důsledné pravidelné přezkoumávání aktiv, rizik i navržených opatření a dále školení všech zaměstnanců společnosti, protože největším nedostatkem v zabezpečení společnosti bývají často zaměstnanci.

Literatura

- AFOES CONSULTANTS. Integrated Management System (IMS), [online], 2012 [cit. 2015-02-14]. Dostupné z: http://www.afoes.ae/solutions/consultancy/management-certification-consulting/integrated-managemement-system/.
- AGERIT, S.R.O., Popis a ceny bezpečnostních testů a služeb, [online], 2015 [cit. 2015-05-13]. Dostupné z: http://test.bezpecnosti.cz/sluzby_ceny.php.
- ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27 001 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2006, 35 s.
- ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27 001. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.
- ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27 002. Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Český normalizační institut, 2013.
- DOBDA, Luboš. Ochrana dat v informačních systémech. Vyd. 1. Praha: Grada, 1998, 286 s. ISBN 80-7169-479-7.
- DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 978-80-86946-88-7.
- HEUREKA.CZ, Porovnání cen a srovnání produktů z internetových obchodů. [online], [cit. 2015-05-12]. Dostupné z: www.heureka.cz.
- KRÁTKÝ, Pavel. Zákon o kybernetické bezpečnosti v praxi. [online]. SystemOnLine, 2014 [cit. 2015-05-13]. ISSN: ISSN 1802-615X. Dostupné z: http://www.systemonline.cz/it-security/zakon-o-kyberneticke-bezpecnosti-v-praxi.htm.
- KUNDEROVÁ, Ludmila. Bezpečnost IS/IT. [online]. Mendelova univerzita, 2014 [cit. 2015-15-11]. Dostupné z: https://akela.mendelu.cz/~lidak/bis/.
- NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti. CyberSecurity.cz - Kybernetická bezpečnost [online]. [cit. 2015-10-28]. Dostupné z: www.cybersecurity.cz/data/SRIB.pdf.

- ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.
- POŽÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, 309 s. ISBN 80-86898-38-5.
- UNICORN SYSTEMS, Bezpečnostní politika informací. [online], Unicorn 2015 [cit. 2015-15-12]. Dostupné z: http://unicornsystems.eu/cz/o-spolecnosti/bezpecnostni-politika-spolecnosti.html.

Seznam tabulek

Seznam obrázků

Seznam zkratek

BI – Business Intelligence

ČSN – Česká státní norma

ICT – informační a komunikační technologie

IEC – International Electrotechnical Comission

IMS – Integrated Management System

IS – informační systém

ISMS – Information security management system (systém řízení informační bezpečnosti)

ISO – International Organization for Standardization (mezinárodní organizace pro standardizaci)

IT – informační technologie

OS – operační systém

PPTP – Point-to-Point Tunneling Protocol (protokol VPN)

VPN – Virtual Private Network (privátní virtuální síť – umožňuje bezpečné spojení neveřejných sítí pomocí sítě veřejné)

Seznam příloh

Příloha 1: Výběr opatření z normy ISO 27 001

A.5	Politiky bezpečnosti informací	Sloupec1
A.5.1	**Směrování bezpečnosti informací vedením organizace**	
A.5.1.1	Politiky pro bezpečnost informací	aplikovat
A.5.1.2	Přezkoumání politik pro bezpečnost informací	aplikovat
A.6	**Organizace bezpečnosti informací**	
A.6.1	**Interní organizace**	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	aplikovat
A.6.1.2	Princip oddělení povinností	aplikovat
A.6.1.3	Kontakt s příslušnými orgány a autoritami	nezavádět
A.6.1.4	Kontakt se zájmovými skupinami	nezavádět
A.6.1.5	Bezpečnost informací v řízení projektů	aplikovat
A.6.2	**Mobilní zařízení a práce na dálku**	
A.6.2.1	Politika mobilních zařízení	aplikovat
A.6.2.2	Práce na dálku	aplikovat
A.7	**Bezpečnost lidských zdrojů**	
A.7.1	**Před vznikem pracovního vztahu**	
A.7.1.1	Prověřování	aplikovat
A.7.1.2	Podmínky pracovního vztahu	revidovat
A.7.2	**Během pracovního vztahu**	
A.7.2.1	Odpovědnost vedení organizace	aplikovat
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	revidovat
A.7.2.3	Disciplinární řízení	aplikovat
A.7.3	**Ukončení a změna pracovního vztahu**	
A.7.3.1	Odpovědnost při ukončení nebo změně pracovního vztahu	aplikovat
A.8	**Řízení aktiv**	
A.8.1	**Odpovědnost za aktiva**	
A.8.1.1	Seznam aktiv	aplikovat
A.8.1.2	Vlastnictví aktiv	aplikovat
A.8.1.3	Přípustné použití aktiv	aplikovat
A.8.1.4	Navrácení aktiv	aplikovat
A.8.2	**Klasifikace informací**	
A.8.2.1	Klasifikace informací	aplikovat
A.8.2.2	Označování informací	aplikovat
A.8.2.3	Manipulaci s aktivy	aplikovat
A.8.3	**Manipulace s médii**	
A.8.3.1	Správy výměnných médií	nezavádět
A.8.3.2	Likvidace médií	nezavádět
A.8.3.3	Přeprava fyzických médií	aplikovat
A.9	**Řízení přístupu**	
A.9.1	**Požadavky organizace na řízení přístupu**	
A.9.1.1	Politika řízení přístupu	revidovat
A.9.1.2	Přístup k sítím a síťovým službám	revidovat

A.9.2	**Řízení přístupu uživatelů**	
A.9.2.1	Registrace a zrušení registrace uživatele	revidovat
A.9.2.2	Správa uživatelských přístupů	nezavádět
A.9.2.3	Správa privilegovaných přístupových práv	nezavádět
A.9.2.4	Správa tajných autentizačních informací uživatelů	nezavádět
A.9.2.5	Přezkoumání přístupových práv uživatelů	aplikovat
A.9.2.6	Odebrání nebo úprava přístupových práv	aplikovat
A.9.3	**Odpovědnosti uživatelů**	
A.9.3.1	Používání tajných autentizačních informací	nezavádět
A.9.4	**Řízení přístupu k systémům a aplikacím**	
A.9.4.1	Omezení přístupu k informacím	revidovat
A.9.4.2	Bezpečné postupy přihlášení	aplikovat
A.9.4.3	Systém správy hesel	aplikovat
A.9.4.4	Použití privilegovaných programových nástrojů	nezavádět
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	nezavádět
A.10	**Kryptografie**	
A.10.1	**Kryptografická opatření**	
A.10.1.1	Politika pro použití kryptografických opatření	aplikovat
A.10.1.2	Správa klíčů	aplikovat
A.11	**Fyzický bezpečnost a bezpečnost prostředí**	
A.11.1	**Bezpečné oblasti**	
A.11.1.1	Fyzický bezpečnostní perimetr	aplikovat
A.11.1.2	Fyzické kontroly vstupu	revidovat
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	revidovat
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	revidovat
A.11.1.5	Práce v bezpečných oblastech	revidovat
A.11.1.6	Oblasti pro nakládku a vykládku	nezavádět
A.11.2	**Zařízení**	
A.11.2.1	Umístění zařízení a jeho ochrana	revidovat
A.11.2.2	Podpůrné služby	revidovat
A.11.2.3	Bezpečnost kabelových rozvodů	aplikovat
A.11.2.4	Údržba zařízení	revidovat
A.11.2.5	Přemístění aktiv	aplikovat
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	revidovat
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	aplikovat
A.11.2.8	Uživatelské zařízení bez obsluhy	nezavádět
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	aplikovat
A.12	**Bezpečnost provozu**	
A.12.1	**Provozní postupy a odpovědnosti**	
A.12.1.1	Dokumentované provozní postupy	aplikovat
A.12.1.2	Řízení změn	aplikovat
A.12.1.3	Řízení kapacit	nezavádět
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	nezavádět
A.12.2	**Ochrana proti malwaru**	

A.12.2.1	Opatření proti malwaru	revidovat
A.12.3	**Zálohování**	
A.12.3.1	Zálohování informací	revidovat
A.12.4	**Zaznamenávání formou logů a monitorování**	
A.12.4.1	Zaznamenávání událostí formou logů	nezavádět
A.12.4.2	Ochrana logů	nezavádět
A.12.4.3	Logy o činnosti administrátorů a operátorů	nezavádět
A.12.4.4	Synchronizace hodin	nezavádět
A.12.5	**Správa provozního softwaru**	
A.12.5.1	Instalace softwaru na provozní systémy	aplikovat
A.12.6	**Řízení technických zranitelností**	
A.12.6.1	Řízení technických zranitelností	nezavádět
A.12.6.2	Omezení instalace softwaru	aplikovat
A.12.7	**Hlediska auditu informačních technologií**	
A.12.7.1	Opatření k auditu informačních systémů	nezavádět
A.13	**Bezpečnost komunikací**	
A.13.1	**Správa bezpečnosti sítě**	
A.13.1.1	Opatření v sítích	aplikovat
A.13.1.2	Bezpečnost síťových služeb	aplikovat
A.13.1.3	Princip oddělení v sítích	revidovat
A.13.2	**Přenos informací**	
A.13.2.1	Politiky a postupy při přenosu informací	aplikovat
A.13.2.2	Dohody o přenosu informací	nezavádět
A.13.2.3	Elektronické předávání zpráv	nezavádět
A.13.2.4	Dohody o utajení nebo mlčenlivosti	aplikovat
A.14	**Akvizice, vývoj a údržby systémů**	
A.14.1	**Bezpečnostní požadavky informačních systémů**	
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	nezavádět
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	nezavádět
A.14.1.3	Ochrana transakcí aplikačních služeb	nezavádět
A.14.2	**Bezpečnost v procesech vývoje a podpory**	
A.14.2.1	Politika bezpečného vývoje	nezavádět
A.14.2.2	Postupy řízení změn systémů	nezavádět
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	nezavádět
A.14.2.4	Omezení změn softwarových balíků	nezavádět
A.14.2.5	Principy budování bezpečných systémů	nezavádět
A.14.2.6	Prostředí bezpečného vývoje	nezavádět
A.14.2.7	Outsourcovaný vývoj	nezavádět
A.14.2.8	Testování bezpečnosti systémů	nezavádět
A.14.2.9	Testování akceptace systémů	nezavádět
A.14.3	**Data pro testování**	
A.14.3.1	Ochrana dat pro testování	nezavádět
A.15	**Dodavatelské vztahy**	

A.15.1	**Bezpečnost informací v dodavatelských vztazích**	
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	nezavádět
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	nezavádět
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	revidovat
A.15.2	**Řízení dodávek služeb dodavatelů**	
A.15.2.1	Monitorování a přezkoumání služeb dodavatelů	nezavádět
A.15.2.2	Řízení změn ve službách dodavatelů	nezavádět
A.16	**Řízení incidentů bezpečnosti informací**	
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**	
A.16.1.1	Odpovědnosti a postupy	zavést
A.16.1.2	Hlášení událostí bezpečnosti informací	zavést
A.16.1.3	Hlášení slabých míst bezpečnosti informací	zavést
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	zavést
A.16.1.5	Reakce na incidenty bezpečnosti informací	zavést
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	zavést
A.16.1.7	Shromažďování důkazů	zavést
A.17	**Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací**	
A.17.1	**Kontinuita bezpečnosti informací**	
A.17.1.1	Plánování kontinuity bezpečnosti informací	zavést
A.17.1.2	Implementace kontinuity bezpečnosti informací	zavést
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	zavést
A.17.2	**Redundance**	
A.17.2.1	Dostupnost vybavení pro zpracování informací	nezavádět
A.18	**Soulad s požadavky**	
A.18.1	**Soulad s právními a smluvními požadavky**	
1.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	revidovat
1.18.1.2	Ochrana duševního vlastnictví	zavést
1.18.1.3	Ochrana záznamů	zavést
1.18.1.4	Soukromí a ochrana osobních údajů	zavést
1.18.1.5	Regulace kryptografických opatření	zavést
A.18.2	**Přezkoumání bezpečnosti informací**	
A.18.2.1	Nezávislé přezkoumání bezpečnosti informací	nezavádět
A.18.2.2	Shoda s bezpečnostními politikami a normami	zavést
A.18.2.3	Přezkoumání technické shody	zavést