
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# MANAGEMENT INFORMAČNÍ BEZPEČNOSTI V PODNIKU
THE INFORMATION SECURITY MANAGEMENT IN COMPANY

**DIPLOMOVÁ PRÁCE**
MASTER'S THESIS


**AUTOR PRÁCE** — **Bc. Petr Kalabis**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR


**BRNO 2016**

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

# ZADÁNÍ DIPLOMOVÉ PRÁCE

**Kalabis Petr, 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:

**Management informační bezpečnosti v podniku**

v anglickém jazyce:

**The Information Security Management in Company**

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 2015/2016.

L.S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>Ředitel ústavu | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>Děkan fakulty |

V Brně, dne 29.2.2016

**Abstrakt**

Tato diplomová práce je zaměřena na návrh zavedení systému řízení bezpečnosti informací v určitém podniku podle souboru norem ISO/IEC 27000. Nejprve byl teoreticky popsán systém řízení bezpečnosti informací a byly vysvětleny relevantní pojmy a další náležitosti k dané problematice. Práce obsahuje analýzu současného stavu podniku a návrhy, které vedou ke snížení zjištěných rizik a k zvýšení celkové bezpečnosti informací.

**Abstract**

This master thesis is focused on the design of implementation the information security management system in the company according to standards ISO/IEC 27000. First of all, it was described the theory of information security management system and it was explained the relevant terms and other requirements in the context of this issue. This assignment involves analysis of the current situation of the company and suggestions that lead to reducing discovered risks and bring improvement of the general information security.

**Klíčová slova**

ISMS, systém řízení bezpečnosti informací, ISO/IEC 27000, aktiva, hrozby, zranitelnost, riziko, dopad, opatření, bezpečnost

**Key words**

ISMS, information security management system, ISO/IEC 27000, assets, threats, vulnerability, risk, impact, countermeasure, security

**Bibliografická citace práce:**

KALABIS, P. *Management informační bezpečnosti v podniku*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 88 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

**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 10. května 2016

……..…….

Petr Kalabis

**Poděkování**

Tímto bych chtěl poděkovat vedoucímu mé práce panu Ing. Viktoru Ondrákovi, Ph.D. za odborné vedení a cenné připomínky a panu Ing. Petru Sedlákovi za odborné rady během psaní této diplomové práce. Také bych chtěl poděkovat svým rodičům za podporu po celou dobu mého studia.

# Obsah

# ÚVOD

V dnešní době by měla být bezpečnost informací v rámci podnikatelských aktivit základním kamenem pro každou organizaci (podnik), která si je vědoma hodnotou svých informací a možných ztrát v případě nedostatečně nastavených bezpečnostních procesů, nebo dokonce v případě jejich absence. Prvním krokem k úspěšnému zvládnutí bezpečnosti informací by mělo být uvědomění si, že bezpečnost informací je nedílnou součástí téměř všech podnikových procesů. Dalším krokem by mělo být zvolení sofistikovaného přístupu, který povede k zvýšení bezpečnosti informací.

V této diplomové práci je přikročeno k navrhnutí takového přístupu, který povede ke zvýšení bezpečnosti informací v konkrétním podniku s důrazem na zavedení určitých bezpečnostních opatření a současně vycházejí ze souboru norem ISO/IEC 27000, ke kterým je po celou dobu tvorby návrhu systému řízení bezpečnosti informací přihlíženo. Bezpečnostní opatření v rámci tohoto přístupu vycházejí z analýzy současného stavu.

V teoretické části této práce jsou popsána východiska a pojmy, které úzce souvisí se systémem řízení bezpečnosti informací. Jsou charakterizovány postupy, které vedou k hodnocení aktiv podniku, k posouzení hrozeb a řízení rizik. V rámci řízení rizik jsou popsány metody zvládání rizik, které jsou nezbytné ke snížení identifikovaných rizik. Dále je představen kybernetický zákon, soubor norem ISO/IEC 27000 a normy vydané organizací NIST.

Praktická část se skládá ze dvou dílčích částí, a to z analýzy současného stavu podniku a z vytvořeného návrhu řešení na základě výsledků této analýzy. V první části je formou analýzy vymezena současná bezpečnostní situace. Jako jedna z množných forem předložené analýzy byla použita maticová metoda. Ve druhé části jsou navržena jednotlivá bezpečnostní opatření odpovídající výsledkům analýzy. Zavedení navrhnutých opatření by mělo být realizováno v rámci tří etap. Na základě finančních nákladů a předpokládaných přínosů finanční i nefinanční povahy bylo vytvořeno ekonomické hodnocení návrhu.

# CÍLE PRÁCE

Cílem této diplomové práce je vytvoření návrhu systému řízení bezpečnosti informací v daném podniku na základě provedené analýzy současného stavu. Vytvořený návrh vychází z požadavků uvedených v normě ISO/IEC 27001 a ze souboru postupů uvedených v normě ISO/IEC 27002. Zmíněný podnik v současné době neusiluje o udělení certifikace systému řízení bezpečnosti informací, z toho důvodu jsou tyto normy brány jako doporučení. Případ, že podnik vytvořený návrh využije jako podporu k získání certifikace, není do budoucna vyloučen. Záměrem této diplomové práce je prostřednictvím návrhu systému řízení informací zvýšit bezpečnost informací s důrazem na aspekt bezpečnostních opatření. Jejich zavádění proběhne v časovém horizontu s ohledem na priority dle zjištěných rizik či požadavků podniku.

# 1. TEORETICKÁ VÝCHODISKA PRÁCE

V úvodu této diplomové práce jsou definovány pojmy a jednotlivé fáze PDCA cyklu, které jsou vztaženy na realizaci systému řízení bezpečnosti informací. Následuje vymezení procesů, které jsou pro realizace tohoto systému nezbytné, mezi tyto procesy patří stanovení působnosti ISMS, prohlášení o politice ISMS a zavedení metrik. Součástí této části je teoretický popis hodnocení aktiv, posouzení hrozeb a řízení rizik. V závěru teoretické části jsou představeny normy řady ISO/IEC 27 000, kybernetický zákon a normy vydané organizací NIST.

## 1.1. Systém řízení bezpečnosti informací

V rámci této diplomové práce je běžně používána zkratka ISMS, která je zkratkou anglického termínu Information Security Management System. Tento termín je ekvivalentní českému překladu systém řízení bezpečnosti informací. Znalost základních pojmů, s kterými se často v ISMS pracuje, je nezbytnou podmínkou pro pochopení a porozumění této oblasti.

Přehled nejčastější pojmů v rámci ISMS je sepsán níže:

- **Bezpečnost informací** nastává v okamžiku zajištění důvěrnosti, integrity a dostupnosti informací. Při tomto zajištění bezpečnosti informací mohou být také kladeny nároky na vlastní informace např. autentičnost, odpovědnost, nepopiratelnost. Důležité je si uvědomit, že bezpečnost informací se také vztahuje na informace, které se vyskytují v nedigitální podobě (1).
- **Důvěrnost informace** je splněna v okamžiku, kdy informace jsou přístupné nebo sdělené pouze oprávněným uživatelům (1).
- **Integrita informace** nastává, pokud informace je nezměněná a úplná (1).
- **Dostupnost informace** nastává v okamžiku zajištění, že oprávněný uživatel má přístup k informaci v okamžiku jeho potřeby (1).
- **Bezpečnost organizace** zajišťuje zabezpečení majetku a objektů organizace např. hlídání přístupů do objektů. Tím zároveň dochází k zabezpečení IS/ICT a k zabezpečení informací (1).

- **Bezpečnost IS/ICT** zajišťuje ochranu aktiv, která se nachází v informačním systému organizace (1).

  Vztah mezi bezpečnostní organizace, bezpečností informací a bezpečností IS/ICT je zobrazen na obrázku č. 1.


**Obr. č. 1: Vztahy bezpečností v organizaci** (Zdroj: Vlastní zpracování dle (2))

- **Aktivum** je cokoliv v organizaci, co má nějakou cenu. Aktiva rozdělujeme na hmotná a nehmotná. Do hmotných aktiv patří veškeré technické prostředky, jako jsou servery, PC, tiskárny, kabelové rozvody, aktivní prvky a další. Do nehmotných aktiv patří pracovní postupy organizace, data, se kterými organizace pracuje, veškeré používané programové vybavení, komunikační a počítačové služby (1).
- **Hrozba** je akce nebo událost, která zneužívá zranitelnost a může ohrozit bezpečnost. Hrozby rozdělujeme na přírodní, fyzické, technické, technologické a lidské. Lidské hrozby se dále dělí na neúmyslné a úmyslné, které mohou působit zvenčí nebo zevnitř organizace. Většina hrozeb, které ohrozily bezpečnost IS/ICT, byly neúmyslné hrozby. Dalším důležitým faktem je, že drtivá většina hrozeb pochází právě zevnitř organizace, např. opuštění svého PC bez odhlášení (1).
- **Zranitelnost** je jakékoliv slabé místo aktiva, které může vést k neautorizovaným přístupům k těmto aktivům. Rozlišujeme několik druhů zranitelnosti např.: fyzická zranitelnost zahrnuje budovy a počítačové místnosti organizace, technická a softwarové zranitelnost nastává v případě poruchy nebo chyby. U nosičů dat a

elektromagnetických zařízení je zranitelnost chápána jako možnost smazání dat. Komunikační systémy a kabelové rozvody jsou zranitelné v případě jejich přerušení nebo odposlechu. A také jde o personální zranitelnost, která pramení z úmyslného nebo neúmyslného chování osob v rámci organizace (1).

- **Opatření** je jakákoliv aktivita, zařízení nebo postup, díky kterým se snižuje síla hrozby nebo se jí úplně zabrání. Opatření se dělí na administrativní, fyzické, technické a technologické. Administrativním opatřením jsou např. směrnice pro práci s IS/ICT, které mohou sloužit k přesně stanoveným postupům při zálohování dat. Do fyzických opatření patří uzamykatelné prostory či čipové karty pro oprávněný přístup. Do technických a technologických opatření spadá např. autorizace a autentizace uživatelů pomocí bezpečnostních hesel. Každé opatření má za cíl předcházet a odhalovat možnosti hrozeb. V případě proniknutí hrozby by mělo správně zavedené opatření zajistit minimalizaci vzniklých škod (1).
- **Riziko** je kombinací hrozby a zranitelnosti aktiva, která může mít za následek poškození aktiva, tj. má určitý dopad na aktivum (1).
- **Dopad** je výsledkem efektivního působení hrozby na aktivum s výsledkem škody. Samostatné dopady jsou různého charakteru, ať už jde o okamžité finanční ztráty nebo postupné snižování důvěryhodnosti organizace, vždy jde o škody negativní. Dopady se převádějí na finanční hodnoty, a to proto, aby bylo možné porovnat náklady na opatření s finanční hodnotou aktiva a hodnotou možného dopadu hrozby na aktivum nebo celou organizaci (1).
- **ISMS** je podle ČSN ISO/IEC 27001 definováno následovně: „*Systém řízení bezpečnosti informací zachovává důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik a dává jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena. Je důležité, že systém řízení bezpečnosti informací je součástí procesů a celkové struktury řízení organizace a je do nich integrován. Je také důležité, že bezpečnost informací je zvažována při návrhu procesů, informačních systémů a opatření. Očekává se, že implementace systému řízení bezpečnosti informací bude nastavena v souladu s potřebami organizace.*“ (3, str. 6).

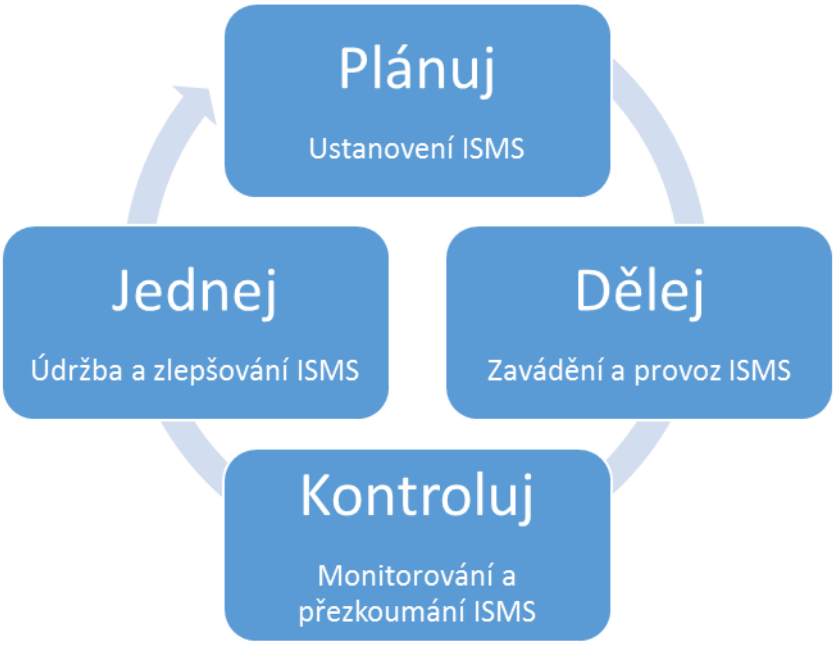
## 1.2. PDCA model

PDCA model bývá také nazýván jako Demingův model, diagram nebo cyklus. William Edwards Deming je nejznámějším průkopníkem přístupu řízení kvality, a to díky představení procesních kontrolních technik pro výrobu v Japonsku, kde byly úspěšně použity. Věřil, že klíčem kvality produkce je mít jasně definované a opakovatelné procesy. PDCA model vychází z těchto čtyřech fází: Plan, Do, Check, Act (4). Do češtiny tyto fáze může přeložit jako: plánuj, dělej, kontroluj a jednej.

PDCA model v rámci systému řízení bezpečnosti informací probíhá následujícími čtyřmi etapami (1):

- **Ustanovení ISMS –** v první etapě se upřesňuje rozsah, kterého se řízení bezpečnosti týká a musí být schválen vedením společnost. Provést ohodnocení rizik a vybrat vhodná bezpečnostní opatření.
- **Zavádění a provoz ISMS –** v druhé etapě dochází k efektivnímu a systematickému prosazení bezpečnostních opatření.
- **Monitorování a přezkoumání ISMS –** v třetí etapě se zajišťuje zpětná vazba a sleduje se, jak je systém řízení bezpečnostních informací úspěšný, či neúspěšný.
- **Údržba a zlepšování ISMS –** v poslední etapě nastává možnost zlepšování systému řízení bezpečnosti informací.

Grafické znázornění PDCA modelu je zachyceno na obrázku č. 2, který zachycuje stále opakující se všechny čtyři etapy.




**Obr. č. 2: PDCA model pro systém řízení bezpečnosti informací** (Zdroj: Vlastní zpracování dle (1))

### 1.2.1. Ustanovení ISMS dle ČSN ISO/IEC 27001

V rámci ustanovení ISMS by měla každá organizace provést následující kroky (3):

- Stanovit hranice a rozsah ISMS. Toto stanovisko provádí na základě prozkoumání specifických rysů činností organizace, uspořádání, struktury atd.
- Definovat politiku ISMS, která obsahuje stanovení cílů, směr řízení a zásad činností, které se týkají bezpečnosti informací. Politika musí obsahovat dále vazby systému managementu bezpečnosti informací na strategii organizace, stanovuje kritéria pro hodnocení rizik a je schválena vedením organizace.
- Stanovit přístup k hodnocení rizik, kde je vybrána metodika hodnocení rizik a vytvořená kritéria pro akceptaci rizik. Výsledky metodiky hodnocení rizik musí být porovnatelné a reprodukovatelné.
- Provést identifikaci rizik. Abychom mohli provést identifikaci rizik, musíme identifikovat aktiva organizace, hrozby vůči nim, zranitelnost a jaké dopady by mohly nastat v případě ztráty důvěrnosti, integrity a dostupnosti.

- Vytvořit analýzu rizik a následné vyhodnocení rizik, které umožní posoudit dopady na činnost organizace v případě selhání bezpečnosti, a zjistit reálnou pravděpodobnost vzniku toho selhání. Odhadnout úroveň rizik a určit, zda jsou tyto rizika akceptovatelná.
- Zvládnout identifikovaná rizika může několika způsoby např.: vytvořením vhodného opatření, vědomě a objektivně akceptovat identifikované riziko, vyhnout se rizikům nebo přenést riziko na třetí strany (pojišťovna).
- Vybrat cíle opatření a vhodná opatření pro zvládnutí rizik ze seznamu opatření uvedeného v normě ISO/IEC 27001, kde výběr musí být zohledněn na základě výsledků analýzy rizik. Berme v úvahu, že cíle opatření a jednotlivá opatření nejsou v této příloze vyčerpávající, tudíž mohou být zavedeny i další postupy.
- Mít souhlas vedení organizace s navrhovanými zbytkovými riziky.
- Mít povolení od vedení organizace k zavedení a provozu ISMS.
- Připravit prohlášení o aplikovatelnosti, které obsahuje cíle opatření a bezpečnostní opatření, která chce vybrat a odůvodnění proč byla vybrána právě tato opatření. Prohlášení o aplikovatelnosti můžeme chápat jako souhrn rozhodnutí, kterými organizace říká, jak bude zacházet s identifikovanými riziky a slouží jako zpětná vazba, aby nedošlo k vyloučení jednotlivých opatření omylem.

### 1.2.2. Zavádění a provozování ISMS dle ČSN ISO/IEC 27001

Při zavádění a provozování ISMS by měly být naplněny následující body (3):

- Formulovat plán zvládání rizik, který by měl vymezovat odpovědnost, činnost vedení, potřebné zdroje a priority, které mohou být stanoveny v rámci zvládání rizik.
- Zavést plán zvládání rizik, a to tak, aby bylo dosáhnuto identifikovaných cílů a opatření, důležité je nezapomenout na finanční zdroje, přiřazení rolí a odpovědností.
- Zavést bezpečnostní opatření, která byla vybrána v první etapě a docílit jejich naplnění.
- Určit způsob, jak se bude měřit účinnost opatření a stanovit, jak tato měření budou vyhodnocena, aby byla porovnatelná a opakovatelná. Měření účinnosti opatření

slouží ke zpětné vazbě jak organizaci, tak i zaměstnancům. Tato měření informují o tom, zdali jednotlivá opatření jsou plněna.

- Zavést programy školení a programy zvyšování informovanosti, tak aby zaměstnanci, kterých se týkají povinnosti se zavedením a provozováním ISMS, byli dostatečně a odborně informováni.
- Organizace by měla zavést řízení provozu a zdrojů ISMS.
- Zavést postupy a další opatření, které se týkají detekce a reakce na bezpečnostní události a na bezpečnostní incidenty.

### 1.2.3. Monitorování a přezkoumání ISMS dle ČSN ISO/IEC 27001

V této etapě dochází k monitorování a přezkoumání ISMS, aby byla tato etapa správně realizována, musí být dodrženy tyto body (3):

- Monitorovat, přezkoumávat a zavádět další opatření v ISMS, které slouží k detekci chyb zpracování, k identifikaci úspěšných i neúspěšných pokusů o narušení bezpečnosti a detekci incidentů. Vedení organizace může určit, zdali bezpečnostní aktivity fungují podle jejich očekávání. Tato etapa také umožňuje detekovat bezpečnostní události a vyhodnocovat účinnost činností v případě narušení bezpečnosti.
- Pravidelně přezkoumávat účinnost ISMS, a to proto, aby docházelo k ověření, že požadavky na bezpečnost jsou naplněny.
- Provádět přezkoumání hodnocení rizik, zbytkového rizika a úroveň akceptovatelného rizika, a to s ohledem na změny organizace, technologií, cílů organizace, identifikovaných hrozeb, účinnosti zavedených opatření a regulatorního a právního prostředí.
- Provádět interní audity, které mohou být prováděny přímo organizací nebo externími auditory.
- Na úrovni vedení organizace se musí pravidelně přezkoumávat ISMS, aby byl zajištěn odpovídající rozsah a možnost zlepšení.
- Závěry monitorování a přezkoumávání vedou k aktualizaci bezpečnostních plánů.
- Zaznamenávat všechny události, které by mohli ovlivnit účinnost nebo výkon ISMS.

### 1.2.4. Udržování a zlepšování ISMS dle ČSN ISO/IEC 27001

Poslední etapou je udržování a zlepšování ISMS, která obsahuje následující kroky (3):

- Zavádění identifikovaných zlepšení ISMS, které byly schváleny organizací.
- Vykonávat nápravné a preventivní činnosti, a to s využitím vlastních zkušeností nebo s využitím zkušeností jiných organizací v oblasti bezpečnosti.
- Projednávat činnosti a návrhy na zlepšení se všemi zainteresovanými stranami.
- Zlepšení musí dosáhnout předpokládaných cílů.

## 1.3. Působnost ISMS

Působnost ISMS zahrnuje stanovení rozsahu a hranice ISMS, důležité je mít na vědomí, že právě působnost ISMS vychází z cílů a strategie organizace. Stanovit rozsah můžeme dvěma základními způsoby. První způsob je stanovit rozsah ISMS totožně s rozsahem celé organizace. Výhodou je celkový pohled na bezpečnost informací, naopak nevýhodou jsou vysoké časové a finanční náklady s předpokládanou nízkou návratností. Druhý způsob stanovuje rozsah ISMS pouze na určenou část organizace (pobočka, IS). Výhodou je soustředění vyšší míry úsilí do zvolené části organizace, to napomáhá usnadnění obhájení účelnosti ISMS a zvládnutí všech požadavků ISMS (1).

„*Tato etapa budování má zásadní dopady na fungování ISMS během jeho celého životního cyklu.*“ (1, str. 96)

## 1.4. Prohlášení o politice ISMS

Prohlášení o politice je sestavováno na základě specifických potřeb každé organizace. Jde o důležitý dokument, který odráží představy vedení organizace o řízení bezpečnosti informací a stanovuje podmínky pro ohodnocení rizik. Správně definovaná politika ISMS může usnadnit celý systém řízení bezpečnosti informací (1).

Prohlášení o politice obsahuje několik důležitých bodů (1):

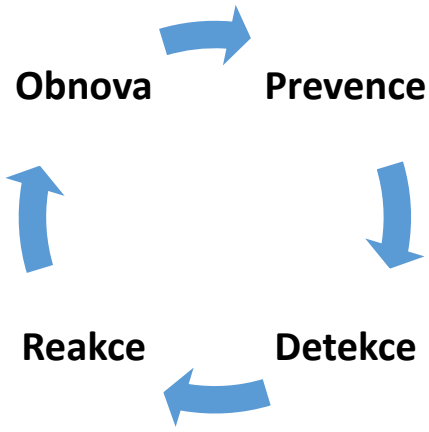
- Stanovení cílů ISMS a základního směru a rámce pro řízení bezpečnosti informací.

- Zohlednění cílů a požadavků organizace, navíc požadavky zákonné, regulativní a smluvní.
- Vytvoření vazeb, které slouží pro vybudování a údržbu ISMS, tak aby byla zohledněna strategie, organizační struktura a procesy organizace atd.
- Stanovení kritérií, která popisují a hodnotí rizika.
- Schválení vedením organizace.

### 1.5. Metriky ISMS

Při sestavení vhodných metrik zaručíme efektivitu bezpečnostních opatření. Definované metriky musíme měřit a následně vyhodnocovat. Metriky můžeme chápat jako ukazatele, které hodnotí efektivitu v oblasti řízení výkonu. V rámci systému řízení bezpečnosti informací se metriky vztahují především k měření efektivity důvěrnosti, integrity a dostupnosti (5).

Na obrázku č. 3 je zobrazen životní cyklus vývoje metrik, který se skládá z prevence, detekce, reakce a obnovy.




**Obr. č. 3: Životní cyklus vývoje metrik v ISMS** (Zdroj: Vlastní zpracování dle (5))

### 1.6. Hodnocení aktiv

Proces hodnocení aktiv musí předcházet identifikování aktiv. Při identifikaci aktiv je v prvním kroku vhodné seskupit všechna aktiva podle stejných logických skupin. Dalším krokem je identifikovat vlastníka aktiva, který je zodpovědnou osobou za dané aktivum a s jeho pomocí lze určit konkrétní hodnotu aktiva (2).

Při hodnocení aktiv se stanovuje stupnice a hodnotící kritéria. Stupnice může být vyjádřena finančními prostředky nebo kvalitativními hodnotami, výběr stupnice záleží na uvážení samotné organizace. Při využití stupnice pomocí finančních prostředků získáme peněžní hodnotu určitého aktiva. Při využití kvalitativní stupnice dostáváme hodnotu v termínech, které si organizace zvolí (např. bezvýznamné riziko, akceptovatelné riziko, nízké riziko, nežádoucí riziko, nepřijatelné riziko). Rozsah a výběr těchto termínů závisí na bezpečnostních potřebách, velikosti organizace atd (2).

Hodnocení aktiv je vhodné provádět s vlastníkem aktiv, ale také s uživatelem daného aktiva. Jde o formu křížové kontroly, která vede k upřesnění hodnoty aktiva a je vhodné ji provádět u všech aktiv, které mají vysoké přínosy pro organizaci. Princip hodnocení aktiv spočívá v odhadu vzniklých nákladů v důsledku porušení důvěrnosti, integrity a dostupnosti. Nejčastěji se výpočet hodnoty aktiv provádí pomocí tzv. součtového algoritmu, který je také nejjednodušší a nejrychlejší. Tento algoritmus můžeme vyjádřit jako podíl, kde v čitateli je součet dostupnosti, důvěryhodnosti a integrity a ve jmenovateli je hodnota tři (2).

### 1.7. Posouzení hrozeb

Seznam možných hrozeb, které mohou negativně ovlivnit bezpečnost aktiva je uveden v normě ISO/IEC 27005 v příloze C. V této příloze jsou uvedeny relevantní zdroje hrozeb a platí, že jednotlivé hrozby mohou mít více zdrojů (6).

Typy těchto zdrojů jsou popsány v následujících bodech (6):

- A (accidental) je označení náhodné činnosti, které mohou poškodit aktivum (vyvolaná hrozba - např. selhání zařízení)

- D (deliberate) je označení úmyslné činnosti zaměřené na poškození aktiva (vyvolaná hrozba - např. krádež zařízení)
- E (environmental) je označení činnosti, které nejsou založeny na lidských činnostech, (vyvolaná hrozba - např. povodeň)

Při hodnocení hrozeb musíme brát v úvahu, jaké veškeré události či akce mohou poškodit bezpečnost aktiv. Hrozby posuzujeme podle závislosti ke ztrátě důvěrnosti, ztrátě integrity, ztrátě dostupnosti, ztrátě individuální odpovědnosti, ztrátě autentičnosti a ztrátě spolehlivosti. Důležité je brát v úvahu veškeré možné dopady hrozeb (2).

### 1.8. Řízení rizik

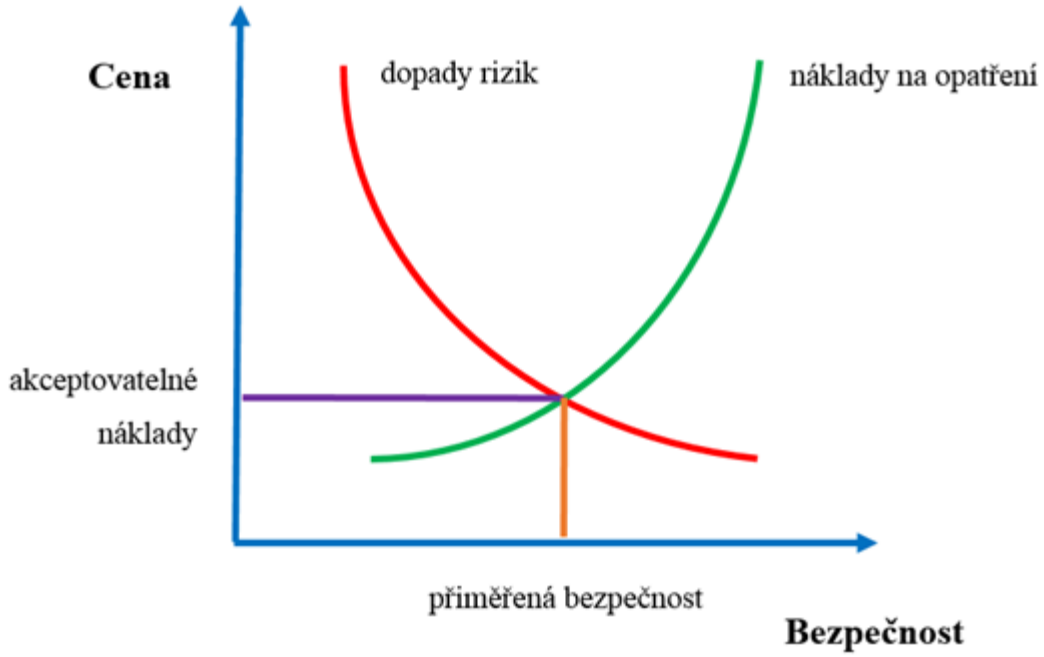
Jeden ze základních nástrojů managementu organizace by mělo být řízení rizik. Tímto nástrojem dochází k ochraně investic, které byly vynaloženy do všech aktiv organizace a současně i do hlavních procesů společnosti (1).

Řízení rizik je východiskem a základem pro systém řízení bezpečnosti informací a také ovlivňuje velkou mírou efektivitu jeho celého fungování. Řízení rizik je možné rozdělit na zvládání rizik, akceptace rizika a hodnocení rizik, které obsahuje analýzu a vyhodnocení rizik (1).

Vztah mezi těmito jednotlivými částmi řízení rizik je zobrazena na obrázku č. 4.


**Obr. č. 4: Řízení rizik** (Zdroj: Vlastní zpracování dle (1))

V rámci řízení rizik dochází k provedení analýzy rizik, která slouží jako podklad pro výběr příslušných opatření. Výběr vhodného opatření a jeho realizace je součástí bezpečnosti organizace. U výběru opatření hrají důležitou roli vzniklé náklady na opatření. Tento ekonomický aspekt je znázorněn na obrázku č. 5. U přiměřené bezpečnosti hledáme bod, kde se protnou křivky nákladů na opatření a dopady rizik. V tomto bodě dochází k přiměřené bezpečnosti za akceptovatelné náklady (1).




**Obr. č. 5: Přiměřená bezpečnost** (Zdroj: Vlastní zpracování dle (2))

### 1.8.1. Analýza rizik

Přístup organizace k analýze rizik je individuální a závisí na podnětu této činnosti. Podle jednotlivých přístupů řešení procesu analýzy rizik rozlišujeme následující přístupy (1):

- Nedělat nic – v případě, že vedení organizace zvolí tento druhy přístupu procesu analýzy rizik, volí variantu, kde plně akceptuje veškerá rizika, které mohou být různého rozsahu a různé síly.
- Neformální přístup – je přístup, kdy dochází k analýze rizik avšak bez jakékoliv dokumentace.
- Základní přístup – analýza rizik je provedena a zdokumentována, management organizace má vizi pro řešení bezpečnosti informací.

- Detailní přistup – je definovaná metodika, podle které dochází k analýze rizik.
- Přístup kombinovaný – provádí se podrobná analýza rizik, ale management organizace některá rizika záměrně nesleduje

V rámci této diplomové práce bude při analýze rizik využita maticová metoda analýzy rizika. Při použití této metody analýzy rizik vycházíme z ohodnocení aktiv, z pravděpodobnosti vzniku hrozby a ze stanovené zranitelnosti ohodnocených aktiv vůči identifikovaným hrozbám. Výpočet míry rizika je definován jako součin těchto tří veličin. Míru rizika můžeme následně převést podle stanovené hodnotící tabulky na kvalitativní hodnocení (2).

Výpočet míry rizika je vyjádřeno pomocí vztahu (2):

$$R = T \times A \times V,$$

kde

R = míra rizika,

T = pravděpodobnost vzniku hrozby,

A = hodnota aktiv,

V = zranitelnost aktiva.

### 1.8.2. Zvládání rizik

Zvládání rizik může být realizováno několika metodami, které vedou ke snížení nebo eliminaci konkrétního rizika. Tyto metody by měly vést k nejvýhodnějším a nejméně finančně náročným postupům v rámci charakterizovaného rizika. Mezi tyto metody patří transfer (přesun), retence (zadržení), vyhnutí a redukce (zmírnění) rizika (7).

Jednotlivé metody zvládání rizik jsou popsány v následujících bodech (8):

- Metoda redukce rizika je založena na aplikování efektivních opatření, která mohou riziko úplně eliminovat nebo snížit na akceptovatelnou úroveň.
- Metoda transferu rizika vychází z přenesení rizika na třetí stranu, např. pojišťovnu.

- Metoda vyhnutí se riziku by měla být provedena v případě, že není možné zavést jiné metody vedoucí ke snížení daného rizika, výsledkem je např. ukončení určité aktivity organizace.
- Metoda retence nastává v případě, že organizace příjme dané riziko.

Volba metody zvládání rizik závisí na konkrétním riziku, obecný přístup k výběru vhodných metod je zobrazen v tabulce č. 1. Tento přístup je založen na pravděpodobnosti výskytu rizika a případného dopadu (7).

**Tab. č. 1: Přístupy zvládání rizik**
(Zdroj: Vlastní zpracování dle (7))

| | **Vysoká pravděpodobnost** | **Nízká pravděpodobnost** |
|---|---|---|
| **Vysoký dopad** | vyhnutí, redukce | transfer (pojištění) |
| **Nízký dopad** | retence, redukce | retence |

Jednotlivé přístupy jsou popsány v následujících bodech:

- Při vysoké pravděpodobnosti a vysokému dopadu je vhodné zvolit metodu vyhnutí nebo redukce rizika. V této situaci není možné využít metody retence, neboť by mohlo dojít např. k vysokým finančním ztrátám. Pojištění by bylo v tomto případě finančně velmi náročné, proto se doporučuje metoda vyhnutí se riziku nebo metoda redukce, která se může vztahovat na příčinu vzniku rizika nebo na jeho důsledek (7).
- Kombinace nízké pravděpodobnosti a vysokého dopadu může způsobit existenční ztráty, které avšak nejsou příliš pravděpodobné. V tomto případě je vhodné vybrat metodu transferu, kdy dochází k přesunu rizika z organizace na jiné podnikatelské subjekty. Např. riziko vzniku požáru v organizaci může být řešeno uzavřením pojistné smlouvy (7).
- Vysoká pravděpodobnost rizika a nízký dopad by měl být řešen metodou retence nebo metodou redukce. Metoda retence by měla být zavedena v případě opravdu malých ztrát a nepřiměřených nákladů na snižování takových ztrát. Aplikujeme-li metodu redukce, bude docházet ke snížení pravděpodobnosti rizika (7). Např. riziko zneužívání firemní tiskárny je vhodné zadržovat nebo redukovat povolením využívání tiskárny pro osobní potřeby v definovaném množství.

- V případě malé pravděpodobnosti rizika a malého dopadu je vhodné zvolit metodu retence, kdy ostatní metody by byly zbytečně nákladné (7). Např. riziko odcizení pracovní židle není třeba řešit jinými metodami než metodou retence.

Plán zvládání rizik je dokument, který obsahuje seznam zvolených metod, které vedou k zvládání identifikovaných rizik. Pořadí realizace jednotlivých činností zvládání rizik se může odvíjet od klasifikace rizik nebo od provedení analýzy nákladů a výnosů. Každá činnost je vymezena z hlediska personální odpovědnosti a časového horizontu (9).

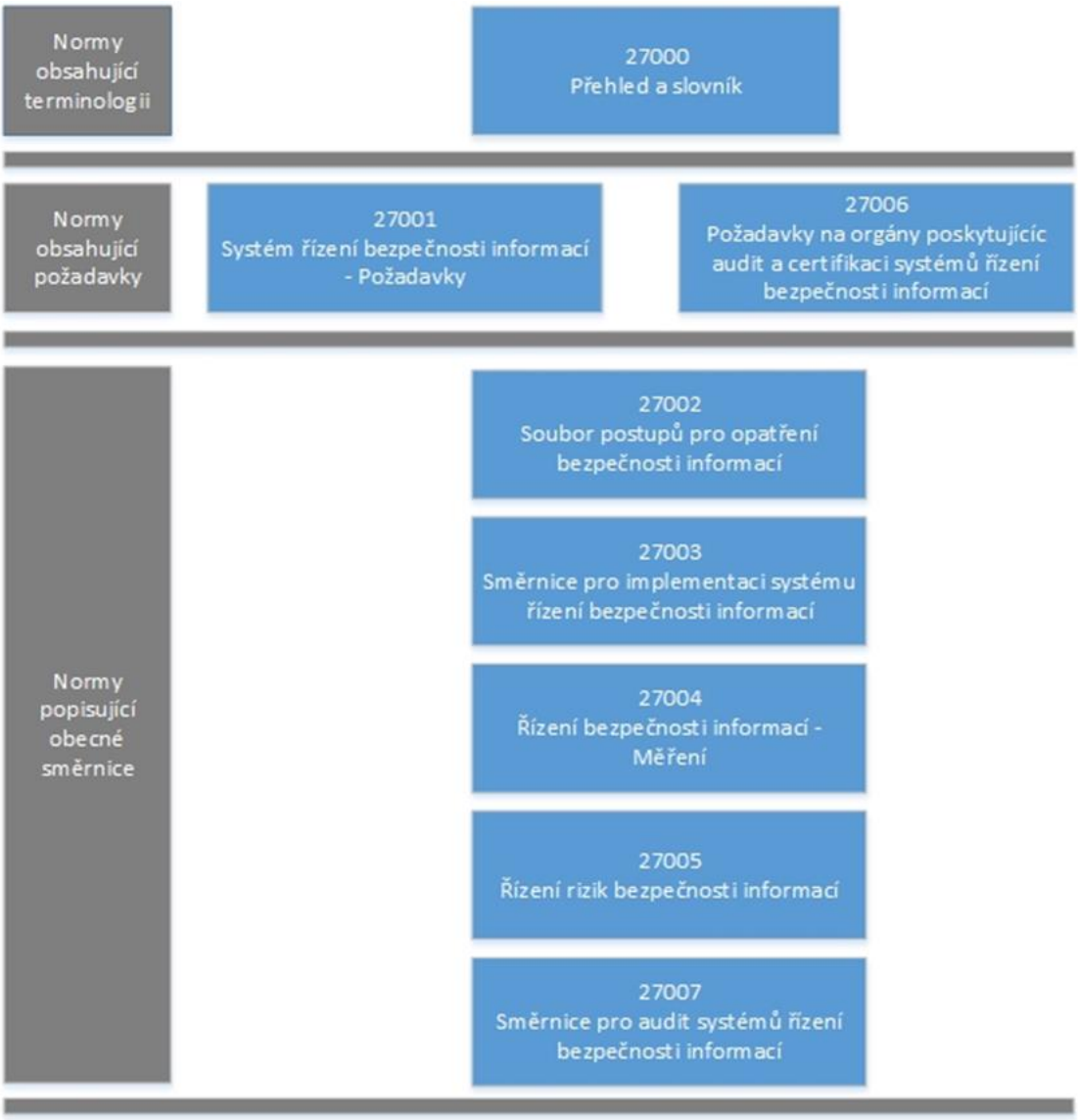
### 1.8.3. Akceptace rizika

Akceptace rizika je posledním krokem v procesu řízení rizik. V tomto kroku dochází k souhlasu vedení organizace s přijetím rizik, která nebyla úplně eliminována v rámci plánu zvládání rizik. Tato rizika se nazývají zbytková a organizace je o těchto rizicích informována a akceptuje je (9).

## 1.9. Normy řady ISO/IEC 27 000

Řada norem je detailně popsána v normě ISO/IEC 27000, kde jsou veškeré normy rozděleny do pěti hlavních skupin. Jde o skupiny norem obsahující terminologii, normy obsahující požadavky, normy popisující obecné směrnice, normy popisující směrnice specifické pro odvětví a normy popisující směrnice specifické pro opatření (10).

V rámci této diplomové práce je nezbytné mít povědomí o normách, které jsou graficky zobrazeny na obrázku č. 6.




**Obr. č. 6: Vztahy norem řady ISMS** (Zdroj: Vlastní zpracování dle (10))

- ČSN ISO/IEC 27000 – předmětem normy je přehled všech norem vztahující se k systému řízení bezpečnosti informací. Norma také obsahuje úvod do ISMS a vysvětluje důležité pojmy a definice, které jsou pro porozumění systému řízení bezpečnosti informací nezbytné (10).
- ČSN ISO/IEC 27001 – norma stanovuje požadavky, které jsou kladeny na ustavení, implementování, udržování a neustálé zlepšování ISMS. Tyto požadavky můžeme považovat jako obecné a aplikovatelné pro jakoukoliv společnost. Pro dodržení této normy nesmí být vyloučeno žádné opatření (3).

- ČSN ISO/IEC 27002 – norma doporučuje postupy, které vedou k výběru vhodných opatření v případě zavádění ISMS, při zavádění obecných opatření nebo k vypracování vlastních směrnic v rámci bezpečnosti informací (11).
- ČSN ISO/IEC 27003 – „*mezinárodní norma poskytuje praktický návod pro implementaci a dále informace pro ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování ISMS*„ (10, str. 25)
- ČSN ISO/IEC 27004 – norma obsahuje rámce měření, pomoci kterých můžeme posoudit efektivnost ISMS a dosažených cílů opatření v rámci řízení bezpečnosti informací (10).
- ČSN ISO/IEC 27005 – norma doporučuje jak zvládnout řízení rizik bezpečnosti informací. Obsahem této normy nejsou žádné konkrétní metodiky, jde o přístup organizace, která si zvolí, jaký bude mít přístup v závislosti na požadavcích a rozsahu ISMS (6).
- ČSN ISO/IEC 27006 – norma je především určena pro certifikační orgány, které poskytují audit a certifikaci ISMS (10).
- ČSN ISO/IEC 27007 – tuto normu můžeme brát jako návod na provádění auditů v rámci ISMS. Norma popisuje návod k interním a externím auditům nebo k auditům, které vychází ze stanovených požadavků (10).

### 1.10. Zákon o kybernetické bezpečnosti

Podoba zákona o kybernetické bezpečnosti se začala tvořit již v roce 2012, a to národním bezpečnostním úřadem. Během roku 2014 byl návrh zákona schválen Vládou České republiky, Poslaneckou sněmovnou a také Senátem. V srpnu roku 2014 byl tento zákon podepsán prezidentem České republiky. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti nabyl účinnosti k 1. 1. 2015. S účinností tohoto zákona přibyly povinnosti osobám a orgánům, které musí dodržovat stanovený souhrn úkonů, které vedou k zajištění kybernetické bezpečnosti (12).

Předmět úpravy tohoto zákona je v následujícím znění: „*Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.*“ (13)

Pro pochopení tohoto zákona je důležité si vymezit následující pojmy (13):

- **Kybernetický prostor** je digitální prostředí, které umožňuje vznik, zpracování a výměnu informací, které jsou tvořeny informačními systémy, službami a sítěmi elektronických komunikací.
- **Kritická informační infrastruktura** je prvek nebo systém prvků v odvětví komunikačních a informačních systémů spadající pod oblast kybernetické bezpečnosti.
- **Významný informační systém** je systém, který je spravovaný orgánem veřejné moci. Významný informační systém není kritickou informační infrastrukturou, ale při narušení bezpečnosti informací ve významném informačním systému může dojít k omezení nebo k výraznému ohrožení výkonu působnosti orgánu veřejné moci.
- **Správce informačního systému** je orgán nebo osoba, která vymezuje záměr zpracování informací a podmínky, které se vztahují k provozování informačního systému.
- **Správce komunikačního systému** je orgán nebo osoba, která vymezuje záměr komunikačního systému a podmínky, které se vztahují k jeho provozování.
- **Významná síť** je síť elektronických komunikací, které zajišťují přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

Orgány a osoby, kterým vznikají povinnosti v rámci tohoto zákona podle §3, jsou (13):

- Poskytovatelé služeb elektronických komunikací a subjekty, které zajišťují síť elektronických komunikací, pokud není orgánem nebo osobou v následujícím bodě.
- Orgány nebo osoby, které zajištují významnou síť, pokud nejsou správcem komunikačního systému kritické informační infrastruktury.
- Správce informačního systému a správce komunikačního systému kritické informační infrastruktury. Kritéria pro kritickou infrastrukturu jsou stanovena v předpise č. 432/2010 Sb.

- Správci významného informačního systému, kritéria pro stanovení významného informačního systému jsou popsány v předpisu č. 317/2014 Sb.

K zákonu o kybernetické bezpečnosti se také vztahují následující předpisy, které blíže popisují opatření v rámci kybernetické bezpečnosti, kritéria pro určení významných informačních systémů a kritéria pro stanovení kritické infrastruktury.

- Předpis č. 316/2014 Sb. vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Tato vyhláška obsahuje strukturu bezpečnostní dokumentace, která je nutná pro organizace, které spadají pod zákon o kybernetické bezpečnosti. Vyhláška obsahuje organizační opatření, která se vztahují ke konkrétním opatřením organizace a technická opatření, které se vztahují k bezpečnosti technických prostředků (14).
- Předpis č. 317/2014 Sb. vyhláška o významných informačních systémech a jejich určujících kritérií. Tato vyhláška stanovuje, které informační systémy patří do skupiny významných informačních systémů, a to přímo nebo podle určujících kritérií. Tato kritéria jsou rozdělena na dopadová určující kritéria a oblastní určující kritéria. Na základě této vyhlášky může správce informačního systému posoudit, zdali patří do skupiny významných informačních systémů (15).
- Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury je důležitým dokumentem. Nařízení, které slouží k určení prvku kritické infrastruktury, obsahuje kritéria průřezová, která se vztahují na zdravotní dopady osob, ekonomický dopad a omezení základních životních potřeb obyvatel. Dále jsou obsažena kritéria odvětvová, která obsahují seznam odvětví, které spadají do kritické informační infrastruktury (16).

## 1.11. NIST normy

Instituce NIST byla založena již v roce 1901 v USA. Cílem této instituce je podporovat inovace a průmyslovou konkurenceschopnost díky pokročilým vědeckým měřením, zavedením standardů a technologiím takovým způsobem, který zlepší ekonomickou bezpečnost a zlepší kvalitu života. NIST zaměstnává přibližně 3400 vědců, inženýrů, techniků a administrativních pracovníků (17).

Řady norem NIST SPECIAL PUBLICATIONS (NIST SP) obsahují průvodce, doporučení a materiály vzhledem k počítačové, kybernetické a informační bezpečnosti. Tyto NIST SP normy jsou vhodné využít v kombinaci s normami řady ISO/IEC 27 000 (18).

Rozdělení norem NIST SP je následující (18):

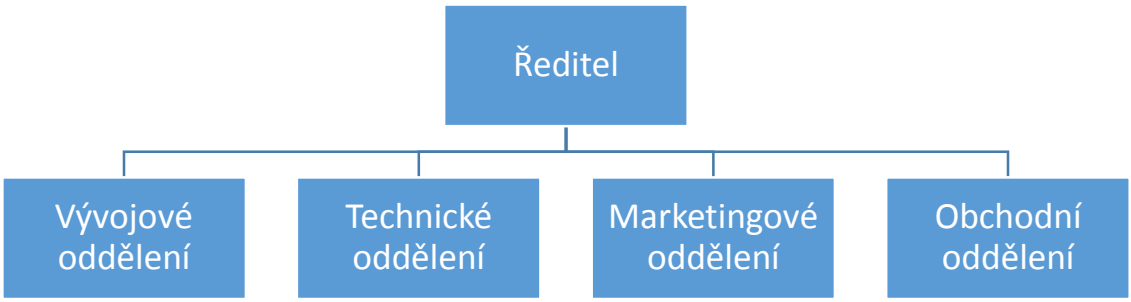
- NIST SP 800 (Computer Security) je řada norem vztahující se k počítačové bezpečnosti, která obsahuje téměř 200 dokumentů. První normy řady SP 800 vznikly již v roce 1990 a neustále nové normy vznikají.
- NIST SP 1800 (NIST Cybersecurity Practice Guides) řada norem, která vznikla jako doplnění norem SP 800. Obsahuje praktické a uživatelsky přijatelné postupy, které vedou k zavedení standartních přístupů ke kybernetické bezpečnosti.
- NIST SP 500 (Computer Systems Technology) je řada norem obsahující širší popis bezpečnosti v informačních technologiích.

# 2. ANALÝZA SOUČASNÉHO STAVU

V této části diplomové práce je nejprve předložena charakteristika analyzované společnost a vymezení její současné bezpečnostní situace, která se vztahuje na informační a komunikační technologie, na bezpečnost v prostředí lidských zdrojů a na procesy vývoje softwaru. Poté byla provedena analýza rizik pomocí maticové metody, která vychází z analýzy aktiv, hrozeb a zranitelností.

## 2.1. Charakteristika společnosti

Reálně existující společnost si nepřála být jmenována, proto v této práci je použit název X.Y.Z. Hlavní podnikatelskou činností společnosti X.Y.Z. je tvorba softwaru a jeho následný prodej. Uživatele tohoto softwaru můžeme najít především v České republice. Společnost v současné době zaměstnává přibližně 20 zaměstnanců. Z organizačního hlediska se ve společnosti X.Y.Z. nachází čtyři oddělení, tj. vývojové oddělení, technické oddělení, marketingové oddělení a obchodní oddělení, v čele organizace je ředitel společnosti, který je zároveň vlastníkem.




**Obr. č. 7: Organizační struktura společnosti X.Y.Z.** (Zdroj: Vlastní zpracování)

Ředitel společnosti si přeje zvýšit bezpečnost informací, neboť ví, že bezpečnost informací je velmi důležitá. Je si také vědom rizik, které se objevují v současné době napříč celou společností. Z toho důvodu chce mít vypracovaný návrh zavedení ISMS, který povede ke snížení vysokých rizik a zvýšení celkové bezpečnosti informací v podniku. Ředitel společnosti nyní neuvažuje podstoupení certifikace, ale chce mít seznam všech opatření a postupů, které by usnadnily certifikaci společnosti v budoucnu.

## 2.2. Popis budovy

Společnost sídlí v administrativní budově, kde sídlí i další organizace, které ale nemají žádný partnerský vztah k analyzované společnosti. Vstup do budovy je střežen vrátným v čase od 7:00 do 19:00 v pracovních dnech. V jiném časovém intervalu je nutné k otevření hlavních dveří použít přístupovou kartu, kterou má každý zaměstnanec. Vstup do budovy je monitorován dvěma bezpečnostními kamerami. Záběry se nahrávají na SD kartu, kde jsou tyto záběry uloženy po dobu 24 hodin, po té dochází k jejich přemazání. Přístupovou kartou se otevírají vstupní dveře do prostor společnosti, které jsou po prvním použití karty ponechány nezajištěné až do konce pracovní doby. Následně tedy není nijak omezen ani monitorován průchod dalších zaměstnanců nebo uživatelů a partnerů společnosti.

## 2.3. Popis ICT

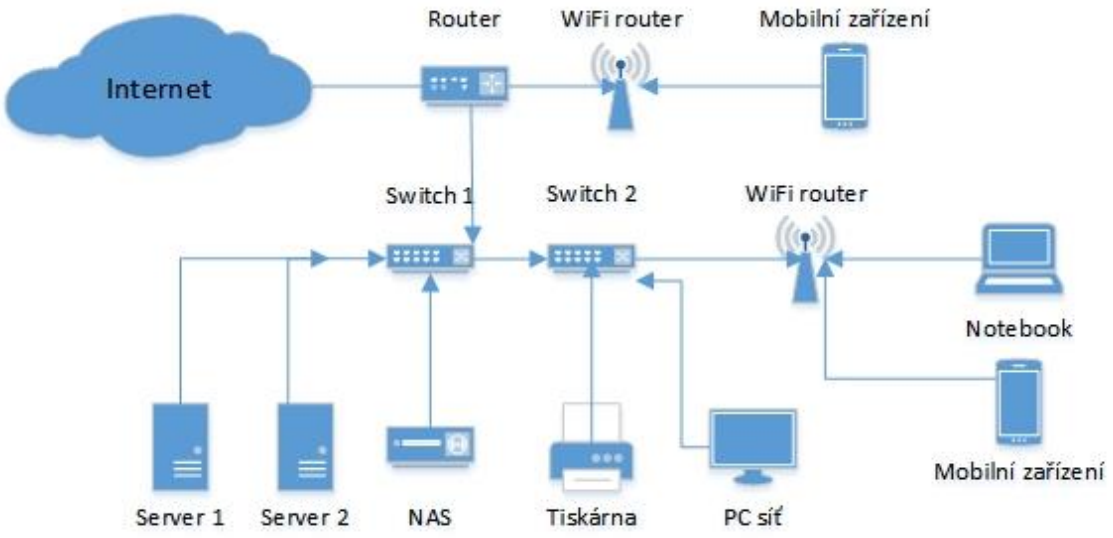
Ve společnosti X.Y.Z. má každý zaměstnanec svůj pracovní notebook, někteří zaměstnanci využívají dokovací stanice s připojenou klávesnicí a monitorem. V případě konzultací u zákazníka nebo práce z domu si mohou zaměstnanci připojit svůj notebook a připojit se k firemní síti přes VPN. Na pracovních noteboocích je nainstalován operační systém Windows 8.1 Enterprise. Ve společnosti se nachází síťová multifunkční tiskárna, ke které mají přístup všichni zaměstnanci.

Důležitým softwarem je informační systém, ke kterému má každý zaměstnanec přístup. Tyto přístupy jsou přiděleny podle potřeb jednotlivých zaměstnanců. Zaměstnanci nemohou na svůj pracovní notebook instalovat jakýkoliv software. Po konzultaci se správcem IT, který se také stará o hardwarové vybavení je možné se individuálně domluvit na instalaci dalšího nezbytně nutného software.

Společnost má k dispozici dva servery, na obou serverech je naistalován operační systém Windows Server 2012. Oba servery využívají diskové pole RAID 1, tedy zrcadlení. Každý server obsahuje dvě disková pole o kapacitě 1 TB a oba servery jsou připojeny k záložním zdrojům UPS, které chrání chod serverů v případě výpadku elektrického proudu. Server 1 je využíván jako databázový server pro provozní databázi informačního systému společnosti. Na tomto serveru je naistalován Microsoft SQL Server 2014, tento

databázový server je spravován správcem IT. Server 2 slouží k účelům vývoje a testování vyvíjeného softwaru. Na tomto serveru běží služba DNS a adresářová služba Active Directory, která umožňuje řídit přístupy uživatelských účtů. Společnost disponuje 2 TB síťovým uložištěm NAS, který slouží jako FTP server a je určen pro zálohu obou serverů.

Počítačová síť je tvořena strukturovanou kabeláží z metalických prvků. Kvalita rozmístěné kabeláže je velmi dobrá, každý zaměstnanec má možnost připojení u svého stolu pomocí UTP kabelu. Všechny metalické kabely jsou schovány do lišt a vedou do uzamykatelného síťového rozvaděče. V prostorách společnosti jsou dvě Wi-Fi sítě, první je určena pouze pro zaměstnance a druhá pro zákazníky, partnery a další návštěvníky, kteří společnost mohou navštívit. Obě tyto Wi-Fi sítě jsou zaheslovány dvěma různými hesly. Je využit typ zabezpečení WPA2 s šifrováním AES, kde délka hesla je nastavena na osm znaků.




**Obr. č. 8: Zjednodušené schéma počítačové sítě** (Zdroj: Vlastní zpracování)

Analyzovaná společnost nepodléhá zákonu č. 181/2014 Sb. o kybernetické o bezpečnosti, protože společnost není orgánem, který je uveden v §3. Informační systém ve společnosti není významný informační systém, neboť není uveden v příloze č. 1 ve vyhlášce č. 317/214 Sb. a nesplňuje žádná dopadová určující kritéria, která jsou uvedena v této vyhlášce. Z nařízení vlády č. 432/2010 sb., které obsahuje průřezová kritéria, vyplývá, že

společnost nedisponuje systémem kritické informační infrastruktury, protože narušení bezpečnosti informací v této společnosti nesplňuje ani jedno z těchto průřezových kritérií. V současné době analyzovaná společnost není dodavatelem informačního systému pro žádné zákazníky se systémem kritické informační infrastruktury. V případě, že některý zákazník by tímto systémem disponoval, analyzované společnosti nastane povinnost splňovat nároky kladené na kybernetickou bezpečnost. Proto, je vhodné o certifikaci ISMS dle normy ISO/IEC 27001 v budoucnu uvažovat, neboť doložení této certifikace a doplněním další nezbytných požadavků by měly být jednodušeji splněny všechny náležitosti, které plynou ze zákona o kybernetické bezpečnosti.

## 2.4. Bezpečnost v prostředí lidských zdrojů

Zaměstnanci této společnosti jsou chápáni jako nezbytná opora pro rozvoj a zlepšování výsledků této společnosti. Z toho důvodu je nastavena přívětivá firemní kultura, která podmiňuje zvyšování kvality práce.

Analyzovaná společnost má zavedenou směrnici, která popisuje způsoby a postupy při výběrovém řízení nových zaměstnanců. Do současné doby nebyl zaznamenán žádný únik informací ze společnosti. Výběrová řízení probíhají ve dvou kolech. Vybraný kandidát podepisuje pracovní smlouvu, která obsahuje detailně popsané kroky, jak zacházet s firemním tajemstvím. Každý zaměstnanec má vytvořeny přístupy a přístupová hesla pouze v rámci své typové pozice v této organizaci. Navýšení počtu přístupových práv nebo jejich rozšíření podle potřeby může zaměstnanec dosáhnout podáním žádosti. V analyzované společnosti je zavedena poměrně nedostatečná politika hesel. Hesla, která jsou přidělena zaměstnanci při nástupu, není nutné aktualizovat ani měnit. Nutné je zmínit, že někteří zaměstnanci nedodržují zásadu čistého stolu ani zásadu čisté obrazovky.

## 2.5. Bezpečnost vývoje software

Společnost se zabývá vývojem software řadu let, za tu dobu vytvořila několik postupů v rámci vývoje software. Žádný z těchto postupů nebyl vytvořen tak, aby splňoval nároky na bezpečnost v rámci ISMS. Dalším zjištěným problémem je nedodržování těchto

postupů, čímž občas dochází k nekontrolovatelným krokům zaměstnanců, které mohou ohrozit celý cyklus vývoje softwaru.

### 2.6. Analýza aktiv

Při procesu analýzy aktiv jsem nejdříve provedl identifikaci aktiv. V tomto kroku jsem čerpal z normy ISO/IEC 27005 z přílohy B. 1, kde jsou uvedeny příklady identifikace aktiv. Následně jsem tento seznam aktiv doplnil dalšími aktivy a stanovil jednotlivé váhy aktiv, a to ve spolupráci se správcem IT.

Hodnocení dopadů bylo sestaveno podle následující klasifikace:

- **Žádný dopad** – nedochází k žádnému ovlivnění společnosti.
- **Zanedbatelný dopad –** částečné omezení chodu společnosti a malé finanční potíže.
- **Potíže a finanční ztráty –** dochází k omezení chodu společnosti v přijatelné míře, ale k citelným finančním ztrátám.
- **Vážné potíže a velké finanční ztráty –** dochází k omezení chodu společnosti v nepřijatelné míře a k velkým finančním ztrátám.
- **Existenční potíže –** dochází k finančním ztrátám a to v takové výši, že společnost nemusí schopná pokračovat ve své podnikatelské činnosti.

Klasifikační schéma hodnocení aktiv zobrazuje jednotlivé váhy aktiva, které jsou ohodnoceny stupnicí 1-5. U tohoto ohodnocení platí, že čím vyšší hodnota váhy aktiva, tím se zvyšuje výše možného dopadu v případě hrozby. Každá váha aktiva má přiřazenou slovní hodnotu dopadu.

**Tab. č. 2: Klasifikační schéma hodnocení aktiv**
(Zdroj: Vlastní zpracování)

| Váha aktiva | Hodnocení dopadu |
|---|---|
| 1 | žádný dopad |
| 2 | zanedbatelný dopad |
| 3 | potíže a finanční ztráty |
| 4 | vážné potíže a velké finanční ztráty |
| 5 | existenční potíže |

Seznam ohodnocených aktiv je rozdělen podle druhů aktiva. U každého aktiva byla stanovena hodnota důvěrnosti, integrity a dostupnosti. Z těchto hodnot byla vypočítána váha aktiva s využitím součtového algoritmu.

**Tab. č. 3: Seznam ohodnocených aktiv**
(Zdroj: Vlastní zpracování)

| Druh aktiva | Aktivum | Důvěrnost | Integrita | Dostupnost | Váha aktiva |
|---|---|---|---|---|---|
| **Informace** | Smlouvy | 5 | 5 | 4 | 5 |
| | Osobní údaje | 4 | 3 | 3 | 3 |
| | Informace o zákaznících | 4 | 3 | 3 | 3 |
| | Informace o partnerech | 4 | 3 | 3 | 3 |
| | Zálohy dat | 5 | 5 | 4 | 5 |
| **Hardware** | Notebook | 5 | 3 | 3 | 4 |
| | Mobilní telefon | 5 | 3 | 3 | 4 |
| | Server | 5 | 4 | 4 | 4 |
| | UPS | 3 | 3 | 3 | 3 |
| | Tiskárna | 2 | 2 | 2 | 2 |
| | Datový projektor | 2 | 2 | 2 | 2 |
| **Software** | Operační systém | 3 | 2 | 3 | 3 |
| | Podnikové aplikace | 4 | 5 | 5 | 5 |
| **Síťě** | Router | 3 | 3 | 3 | 3 |
| | Switch | 4 | 3 | 3 | 3 |
| | Pasivní infrastruktura | 3 | 3 | 4 | 3 |
| | Připojení k internetu | 3 | 4 | 4 | 4 |

## 2.7. Analýza hrozeb

Při analýze hrozeb jsem nejdříve identifikoval samotné hrozby a při jejich výběru jsem přihlížel k tzv. typickým hrozbám, které jsou uvedeny v normě ISO/IEC 27005 v příloze C, a to v počtu více jak 40. Z této přílohy jsem vybral řadu hrozeb, které se vztahují ke zkoumané společnosti. Klasifikační schéma pravděpodobnosti hrozeb jsem sestavil podle míry četnost výskytu těchto hrozeb. Přičemž každá pravděpodobnost hrozby má přiřazenou svoji váhu.

**Tab. č. 4: Klasifikační schéma pravděpodobnosti hrozeb**
(Zdroj: Vlastní zpracování)

| Váha hrozby | Pravděpodobnost |
|---|---|
| 1 | velmi nízká |
| 2 | nízká |
| 3 | střední |
| 4 | vysoká |
| 5 | velmi vysoká |

Seznam hrozeb jsem rozdělil podle druhu hrozby na fyzické poškození, přírodní události, ztrátu základních služeb, ohrožení informací, technické selhání, neoprávněné činnosti a ohrožení funkčnosti. Toto rozdělení vychází z normy ISO/IEC 27005 příloha C. Každá hrozba má přidělenu váhu, která vychází z klasifikačního schématu pravděpodobnosti hrozeb. U každé hrozby je také definován zdroj hrozby písmeny A, D, E, které jsou blíže popsány v teoretické části této práce.

**Tab. č. 5: Seznam ohodnocených hrozeb**
(Zdroj: Vlastní zpracování)

| Druh hrozby | Zdroj hrozby | Váha hrozby |
|---|---|---|
| **Fyzické poškození** | | |
| Požár | A, D, E | 2 |
| Znečištění zařízení | A, D, E | 3 |
| **Přírodní události** | | |
| Povodeň | E | 1 |
| **Ztráta základních služeb** | | |
| Výpadek internetového spojení | A, D | 3 |
| Přerušení dodávky elektřiny | A, D, E | 3 |
| **Ohrožení informací** | | |
| Vzdálená špionáž | D | 2 |
| Krádež | D | 3 |
| **Technická selhání** | | |
| Selhání zařízení | A | 4 |
| Chybné fungování software | A | 3 |
| **Neoprávněné činnosti** | | |
| Neoprávněné použití zařízení | D | 3 |
| Poškození dat | D | 4 |
| **Ohrožení funkčnosti** | | |
| Chyba v používání | A | 3 |
| Zneužití oprávnění | A, D | 3 |

## 2.8. Analýza zranitelnosti

Matice zranitelnosti vyjadřuje vztah mezi aktivy podniku a hrozbami, které na podnik působí. Tato matice zranitelnosti nám tedy zobrazuje, jaká je pravděpodobnost, že uvedená hrozba způsobí škodu u vybraných aktiv. Pravděpodobnost je vyjádřena hodnotami 1 – 5, kde 1 je pravděpodobnost nejnižší a 5 je nejvyšší.

**Tab. č. 6: Matice zranitelnosti**
(Zdroj: Vlastní zpracování)

| ***Zranitelnost*** | **HROZBY** | Požár | Znečištění | Povodeň | Výpadek internetového připojení | Přerušení dodávky elektřiny | Vzdálená špionáž | Krádež | Selhání zařízení | Chybné fungování software | Neoprávněné použití zařízení | Poškození dat | Chyba v používání | Zneužití oprávnění |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **AKTIVA** | | | | | | | | | | | | | | |
| Smlouvy | | 4 | | 1 | | | 2 | 3 | | | | 4 | 2 | 4 |
| Osobní údaje | | 3 | | 1 | | | 2 | 3 | | | 4 | 4 | | 4 |
| Informace o zákaznících | | 3 | | 1 | | | 3 | 3 | | | 4 | 4 | 4 | 4 |
| Informace o partnerech | | 3 | | 1 | | | 3 | 3 | | | 4 | 4 | 4 | 4 |
| Zálohy dat | | 3 | 4 | 1 | 3 | 3 | 3 | 4 | 5 | 4 | 4 | 5 | 5 | 4 |
| Notebook | | 3 | 3 | 1 | 2 | 2 | 1 | 4 | 2 | 2 | 3 | 3 | 4 | 3 |
| Mobilní telefon | | 3 | 3 | 1 | 2 | 2 | 1 | 4 | 2 | 2 | 3 | 2 | 4 | 3 |
| Server | | 4 | 3 | 1 | 5 | 5 | 2 | 2 | 5 | 3 | 4 | 2 | 4 | 3 |
| UPS | | 3 | 4 | 1 | | | | 1 | 4 | | 3 | | 4 | 2 |
| Tiskárna | | 2 | 2 | 1 | 2 | 2 | | 2 | 2 | | 2 | | 2 | 1 |
| Datový projektor | | 2 | 3 | 1 | | 2 | | 3 | 2 | | 2 | | 2 | |
| Operační systém | | | | | 1 | 1 | | | | 3 | | 4 | 4 | 4 |
| Podnikové aplikace | | | | | 2 | 2 | 3 | | | 5 | | 4 | 5 | 4 |
| Router | | 2 | 3 | 1 | 2 | | | 2 | 4 | | 3 | | 3 | 2 |
| Switch | | 2 | 3 | 1 | 2 | | | 2 | 4 | | 3 | | 3 | 2 |
| Pasivní infrastruktura | | 2 | 3 | 1 | 2 | | | 2 | 4 | | 3 | | 3 | |
| Připojení k internetu | | 2 | 2 | 2 | | 3 | | | | | 4 | | 3 | 2 |

## 2.9. Analýza rizik

Analýzu rizik jsem provedl maticovou metodou. U této metody analýzy rizik je důležité mít provedenu analýzu aktiv, hrozeb a zranitelnosti, z kterých maticová metoda vychází. Tato metoda je blíže popsána v teoretické části v kapitole s názvem analýza rizik. Hodnocení míry rizik jsem sestavil po konzultaci s vedením organizace. Zvolené hodnocení je zobrazeno v tabulce č. 7, které bylo po uvážení rozděleno do tří úrovní.

**Tab. č. 7: Hodnocení míry rizik**
(Zdroj: Vlastní zpracování)

| Hodnoty míry rizika | Hodnocení |
|---|---|
| <0 - 40) | Nízké |
| <40- 80) | Střední |
| <80 - 125) | Vysoké |

Z tabulky matice rizik můžeme identifikovat barevně odlišená hodnocení, která hodnotí míru rizika na vysoká, střední a nízká. Celkem bylo pomocí této metody identifikováno 8 vysokých, 35 středních a 111 nízkých hodnot míry rizik.

**Tab. č. 8: Matice rizik**
(Zdroj: Vlastní zpracování)

| ***Míra rizika*** | | **HROZBY** | Požár | Znečištění | Povodeň | Výpadek internetového připojení | Přerušení dodávky elektřiny | Vzdálená špionáž | Krádež | Selhání zařízení | Chybné fungování software | Neoprávněné použití zařízení | Poškození dat | Chyba v používání | Zneužití oprávnění |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 2 | 3 | 1 | 3 | 3 | 2 | 3 | 4 | 3 | 3 | 4 | 3 | 3 |
| ***AKTIVA*** | | | | | | | | | | | | | | | |
| Smlouvy | 5 | | 40 | | 5 | | | 20 | 45 | | | | 80 | 30 | 80 |
| Osobní údaje | 3 | | 18 | | 3 | | | 12 | 27 | | | 36 | 48 | | 48 |
| Informace o zákaznících | 3 | | 18 | | 3 | | | 18 | 27 | | | 36 | 48 | 36 | 48 |
| Informace o partnerech | 3 | | 18 | | 3 | | | 18 | 27 | | | 36 | 48 | 36 | 48 |
| Zálohy dat | 5 | | 30 | 60 | 5 | 45 | 45 | 30 | 60 | 100 | 60 | 60 | 100 | 75 | 80 |
| Notebook | 4 | | 24 | 36 | 4 | 24 | 24 | 8 | 48 | 32 | 24 | 36 | 48 | 48 | 48 |
| Mobilní telefon | 4 | | 24 | 36 | 4 | 24 | 24 | 8 | 48 | 32 | 24 | 36 | 32 | 48 | 48 |
| Server | 4 | | 32 | 36 | 4 | 60 | 60 | 16 | 24 | 80 | 36 | 48 | 32 | 48 | 48 |
| UPS | 3 | | 18 | 36 | 3 | | | | 9 | 48 | | 27 | | 36 | 24 |
| Tiskárna | 2 | | 8 | 12 | 2 | 12 | 12 | | 12 | 16 | | 12 | | 12 | 8 |
| Datový projektor | 2 | | 8 | 12 | 2 | 12 | 12 | | 18 | 16 | | 12 | | 12 | |
| Operační systém | 3 | | | | | 9 | 9 | | | | 27 | | 48 | 36 | 48 |
| Podnikové aplikace | 5 | | | | | 30 | 30 | 30 | | | 75 | | 80 | 75 | 80 |
| Router | 3 | | 12 | 27 | 3 | 18 | | | 18 | 48 | | 27 | | 27 | 24 |
| Switch | 3 | | 12 | 27 | 3 | 18 | | | 18 | 48 | | 27 | | 27 | 24 |
| Pasivní infrastruktura | 3 | | 12 | 27 | 3 | 18 | | | 18 | 48 | | 27 | | 27 | |
| Připojení k internetu | 4 | | 16 | 24 | 8 | | 36 | | | | | 48 | | 36 | 32 |

## 2.10. Zhodnocení analýzy

Z analýzy současného stavu, kterou jsem provedl v rámci této kapitoly, vyplývá několik bezpečnostních aspektů, na které bude brán ohled v rámci návrhu bezpečnostních opatření. Důležité je ještě jednou připomenout, že ředitel společnosti v současné době neuvažuje o získání certifikace ISMS. Přesto si přeje mít návrh opatření, která povedou k zvýšení bezpečnosti informací.

Z popisu administrativní budovy je zřejmé, že bezpečnost fyzického vstupu do prostor společnosti je řešena nedostatečně. Současný stav zavedeného přístupového systému není nijak kritický, ale obnáší vyšší pravděpodobnost hrozeb, např. krádež aktiv, zneužití oprávnění přístupu do prostor společnosti, úmyslné přerušení dodávky proudu atd.

Analyzovaná společnost se zabývá vývojem softwaru, proto by měl být kladen důraz právě na bezpečnost informací v rámci tohoto procesu. Z analýzy bezpečnosti vývoje softwaru je patrné, že společnost nemá pevně definované postupy, které by zajišťovali bezpečnost vývoje softwaru v celém jeho cyklu.

Bezpečnost informací je také negativně ovlivněna lidskými faktory. Za velké riziko považuji nedodržování zásady prázdné obrazovky a zásady prázdného stolu, tyto poměrně jednoduché a ekonomicky nenáročné zásady mohou snížit pravděpodobnost výskytu hrozeb, např. zneužití přístupu, smazání dat atd. Další problém je se současně platná nedostatečná politika hesel.

Pomocí maticové metody analýzy rizik byla odkryta další rizika, která nebyla při analýze v běžném provozu zřejmá. Nejvyšší míra rizika byla zjištěna u aktiv, jako např. smlouvy, zálohy dat obsahující zdrojové kódy, server a podnikové aplikace a z nich především informační systém. Na aktiva, na která působí vysoká míra rizika, musí být brán ohled při navrhování vhodných opatření, stejně tak na rizika s hodnotou střední míry rizika.

# 3. NÁVRH ŘEŠENÍ

Tato kapitola je zaměřena na tvorbu návrhu zavedení ISMS, který obsahuje seznam opatření, která budou zaváděna v analyzované společnosti. Výběr opatření vychází z provedené analýzy současného stavu, uvedené v kapitole č. 2. V závěru této kapitoly je vytvořen harmonogram vlastního zavedení, provedeno ekonomické zhodnocení včetně vyhodnocení nákladů a přínosů vytvořeného návrhu.

## 3.1. Plán zvládání rizik a akceptace rizika

Plán zvládání rizik je v této diplomové práci realizován převážně metodou redukce, tedy snížení rizika pomocí aplikování efektivních opatření. Opatření, která jsou aplikována, jsou různého charakteru, např. postupy a pravidla ve formě firemních směrnic, nákup hardwarového a softwarového vybavení, firemní školení aj.

Tento plán zvládání rizik se opírá o opatření, která jsou uvedeny v normě ISO/IEC 27002 v kapitole 5 až 18. Označení těchto opatření je v této diplomové práci značeno velkým písmenem A a dalším znakem je číslo kapitoly daného opatření.

Po konzultaci s ředitelem společnosti bylo rozhodnuto, že zavádění opatření proběhne ve třech etapách. První etapa bude obsahovat stanovení politiky bezpečnosti informací a zavedení opatření, která se vztahují k bezpečnosti vývoje softwaru. Ve druhé etapě by měla být zavedena opatření, která se vztahují k fyzické bezpečnosti a k bezpečnosti v prostředí lidských zdrojů. V této etapě by také mělo dojít k zavedení opatření, která budou primárně určena ke snížení vysoké a střední míry rizika.

Ředitel společnosti akceptuje nízké hodnoty míry rizika, které vycházejí z metody maticové analýzy rizik. Pro tato rizika nebudou aplikována žádná opatření. Předpokladem ale je, že dojde k určitému snížení těchto rizik v rámci účinnosti opatření, která budou realizována v první a ve druhé etapě zavádění ISMS.

### 3.2. Výběr a zavedení opatření

Výběr opatření byl proveden na základě normy ČSN ISO/IEC 27002. Tato norma obsahuje celkem 14 kapitol, které dohromady vymezují více než 100 opatření. V této diplomové práci byla opatření vybrána na základě provedené analýzy současného stavu v kapitole č. 2.

Zavedení bude provedeno ve třech etapách, první dvě etapy budou dále detailně popsány, ekonomicky i časově vyhodnoceny. Tato opatření by měly vést ke snižování rizik vyplývající z analýzy současného stavu. Ve třetí etapě by mělo dojít k zavedení všech zbylých opatření, která jsou nezbytná pro dosažení certifikace systému řízení bezpečnosti informací. Seznam všech opatření je uveden v příloze č. 1, tento seznam obsahuje celkem 14 kapitol, které jsou rozděleny podle charakteru opatření.

Každé opatření bylo přezkoumáno a následně byly stanoveny postupy výběru konkrétních opatření, a sice tyto:

- Zavést – opatření by mělo být zavedeno ve společnosti. Způsob zavedení se vztahuje ke konkrétním opatřením, může jít např. o zavedení nové směrnice, nových postupů, nákupu nutného vybavení atd.
- Aktualizovat – opatření je již ve společnosti zavedeno, avšak současný stav dostatečně nevyhovuje systému řízení bezpečnosti informací, proto je nutné takové zavedené opatření aktualizovat.
- Nezavádět – opatření s tímto označením není potřeba zavádět, protože daná opatření nejsou relevantní k činnostem v analyzované společnosti.
- Zavedeno – opatření není nutné v analyzované společnosti zavádět, neboť je již správně zavedeno.

### 3.3. První etapa

V první etapě by mělo dojít ke stanovení politiky bezpečnosti informací, ve které budou určeny cíle systému řízení bezpečnosti informací, a bude definováno, jak bude docházet k jejich přezkoumávání. Dalším krokem je zavedení opatření vztahující se k bezpečnosti v procesech vývoje a podpory softwaru.

### 3.3.1. Politiky pro bezpečnost informací (A. 5.1.1)

Prvním opatřením analyzované společnosti je stanovení „Politiky bezpečnosti informací“, která zachycuje nejvyšší úroveň firemní strategie v rámci systému řízení bezpečnosti informací. Tato politika by měla být stanovena a schválena ředitelem společnosti, následně přestavena všem zaměstnancům a všem zainteresovaným osobám, na které se tato politika vztahuje. Mezi tyto osoby patří implementační partneři a externí vývojoví inženýři a uživatelé.

Dokument „Politika bezpečnosti informací“ by měla zahrnovat následující body:

- Cíle, kterých má být dosáhnuto v rámci sytému řízení bezpečnosti informací. Mezi hlavní cíle patří zvýšení všeobecné bezpečnosti informací, vytvoření předpisů, které budou respektovány a dodržovány. Dále také přistupovat k bezpečnosti informací tak, aby bylo možné v budoucnu podstoupit certifikaci systému řízení bezpečnosti informací.
- Inovovaná pravidla a postupy budou zaváděna formou firemních směrnic a školení. V rámci společnosti by měly být tyto směrnice dostupné všem zaměstnancům v elektronické i tištěné podobě. Navrhuji umístění směrnic v tištené podobě do kanceláře asistentky a v elektronické podobě na FTP server.
- Zaměstnancům bude představena tato politika ředitelem společnosti na celopodnikové poradě. Zákazníci a partneři budou informování e-mailem o nové bezpečnostní politice. Školení, která budou prováděna na základě zvýšení bezpečnostního povědomí, budou probíhat v budově společnosti a jejich termíny budou oznámeny vždy tři měsíce předem.
- Definice odpovědností osob v rámci systému řízení informací. Odpovědnou osobou za zavedení ISMS je stanoven ředitel společnosti, během tohoto procesu budou stanovení zaměstnanci nést odpovědnost za realizaci přiřazených bezpečnostních opatření. Mezi tyto zaměstnance patří vedoucí vývojového oddělení, vedoucí technického oddělení a správce IT.
- Korektní chování všech zaměstnanců v rámci dané problematiky se stane nedílnou součástí firemní kultury.

Vytvořená „Politika bezpečnosti informací“ by měla být podporována ředitelem společnosti, který svým podpisem potvrzuje, že stanovená politika je v souladu s jeho postojem k řízení bezpečnosti informací. Po představení této politiky jsou povinni všichni zaměstnanci i zainteresované osoby tuto politiku dodržovat. Korektní chování všech zaměstnanců v rámci dané problematiky se tak stane nedílnou součástí firemní kultury.

**Tab. č. 9: Náklady na vytvoření politiky bezpečnosti informací**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření „Politiky bezpečnosti informací” | Ředitel společnosti | 32 hodin |
| Představení „Politiky bezpečnosti informací” na celopodnikové poradě | Ředitel společnosti | 4 hodiny |

### 3.3.2. Přezkoumání politik pro bezpečnost informací (A. 5.1.2)

K zajištění aktuálnosti vytvořené politiky pro bezpečnost informací je nutné přezkoumávat stanovenou politiku bezpečnosti informací a i firemní směrnice ve stanovených intervalech nebo v případě výrazných změn ve společnosti.

Provádění přezkoumání doporučuji pravidelně v intervalu jednoho roku odpovědnou osobou. První provedení přezkoumání ale navrhuji již 6 měsíců po zavedení všech opatření. Pro změnu nebo zlepšení již zavedených opatření, která je třeba zavést v důsledku změn v prostředí společnosti, je důležité, aby mohli mít možnost předložit návrhy změn či aktualizací zaměstnanci, partneři a zákazníci. Tyto návrhy změn jsou předkládány odpovědným osobám a na základě jejich rozhodnutí mohou být tyto změny přijaty a zavedeny. Tyto změny by měly být evidovány ve změnovém listu a následně dány na vědomí všem zainteresovaným osobám (opatření, sdělení atp.). Toto opatření má za úkol zaručit efektivitu a aktuálnost již zavedených předpisů a postupů.

**Tab. č. 10: Náklady na přezkoumání politiky a směrnic**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Přezkoumání „Politiky bezpečnosti informací” a firemních směrnic | Osoby odpovědné za politiku a dané směrnice | 16 hodin / rok |

### 3.3.3. Role a odpovědnosti bezpečnosti informací (A. 6.1.1)

Opatření definuje a přiděluje v rámci společnosti odpovědnost za bezpečnost informací.

V rámci bezpečnostní politiky byly odpovědné osoby stanoveny, tj. ředitel společnosti, vedoucí vývojového oddělení, vedoucí technického oddělení a správce IT. Doporučuji aktualizovat směrnici, která obsahuje identifikovaná aktiva a procesy bezpečnosti informací s přiřazenou odpovědnou osobu ke každému aktivu a procesu. Tento dokument by měl být součástí „Politiky bezpečnosti informací“, aby bylo jasně definováno, která osoba je za co odpovědná. Tyto odpovědné osoby mohou úkoly bezpečnosti delegovat na další osoby, ale zodpovědnost přetrvává u odpovědných osob.

**Tab. č. 11: Náklady na stanovení rolí a odpovědnosti**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice „Role a odpovědnost bezpečnosti informací” | Ředitel společnosti | 16 hodin |

### 3.3.4. Politika bezpečného vývoje (A. 14.2.1)

Aby společnost mohla vyvíjet bezpečně software, musí být správně nastavena a prováděna politika bezpečného vývoje. Do politiky bezpečného vývoje patří i zavedení bezpečnosti vývojového prostředí, které je vyžadováno zavést v rámci opatření Bezpečné vývojové prostředí (A. 14.2.6).

V rámci tohoto opatření doporučuji vytvořit příručku „Bezpečnost v životním cyklu vývoje softwaru“. Tato příručka by se měla skládat ze dvou částí. V první části by měla být popsána samotná metodologie vývoje softwaru. Druhá část by měla obsahovat směrnici bezpečného vývoje pro každý programovací jazyk, který je při tvorbě softwaru použit. S touto příručkou by měli být seznámeni všichni zaměstnanci z vývojového a technického oddělení.

Dále doporučuji vytvořit dokument „Politiku bezpečného vývoje“, jejíž důležitou částí je i stanovení bezpečnostních požadavků, a to již v rámci návrhu, tak aby v průběhu samotného vývoje nedocházelo k neočekávaným změnám, které mohou ohrozit

požadovanou délku vývoje. Aby tato politika byla účinná po dobu celého procesu vývoje, musí být zavedeny kontrolní body bezpečnosti ve stanovených milnících projektu.

Zkoumaná společnost vydává nové aktualizace svého softwaru dvakrát ročně, proto je nutné brát v úvahu i bezpečnost v řízení verzí, které je vyžadováno požadavky v opatření Postupy řízení změn systémů (A. 14.2.2).

Při tvorbě „Politiky bezpečného vývoje“ je také nutné zajistit, aby se softwaroví programátoři snažili vyhýbat vzniku zranitelných míst, popřípadě byli schopni tato zranitelná místa nalézt a eliminovat. Proto navrhuji provádět interní školení u všech zaměstnanců z oddělení vývoje a z technického oddělení jednou ročně a u nových zaměstnanců v rámci jejich zkušební doby. Tato interní školení by měla zajistit dodržování stanovené bezpečnostní politiky.

**Tab. č. 12: Náklady na politiku bezpečného vývoje**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření „Politiky bezpečného vývoje” | Vedoucí vývojového oddělení | 40 hodin |
| Vytvoření příručky „Bezpečnost v životním cyklu vývoje software” | Vedoucí vývojového oddělení | 40 hodin |
| Školení „Bezpečnostní politika vývoje” | Vedoucí vývojového oddělení | 4 hodiny / rok |

### 3.3.5. Postupy řízení změn systémů (A. 14.2.2)

Změny, které mohou nastat v průběhu vývoje softwaru, by měly být řízeny zdokumentovanými postupy a kontrolovány tak, aby docházelo k zajištění integrity vyvíjeného softwaru.

Analyzovaná společnost se standardně setkává se dvěma typy změn v průběhu vývoje softwaru. Prvním typem změny je aktualizace software, které se vydávají ve dvou termínech, a to v měsíci ledu a říjnu, a jsou předem ohlášeny všem uživatelům. Druhým typem změny softwaru jsou opravy chyb nahlášených uživateli. Navrhuji aktualizovat postupy, které jsou nyní nedostatečně popsány ve směrnici „Změny v softwaru“. Tato směrnice bude přesně dokumentovat řízení aktualizací a opravy chyb softwaru.

Tyto postupy by měly obsahovat následující body:

- Definovat postupy při vývoji aktualizací a opravách chyb.
- Vývojový pracovníci mají přístup pouze k těm částem softwaru, které jsou nezbytně nutné pro jejich práci.
- Schválení vedoucího vývojového oddělení k vydání nové aktualizace nebo k provedení opravy.
- Testování změn v samostatném prostředí, odděleném od produkčního a vývojového.
- Vytvořit postupy při provádění záloh všech aktualizací.
- Aktualizace uživatelských postupů, které je nutno provést při změně softwaru.
- Archivace neaktuálních verzí softwaru a uživatelských příruček.

Analyzovaná společnost provádí testování a vývoj softwaru ve stejném prostředí. Navrhuji oddělit vývojové a testovací prostředí zakoupením nového serveru, který bude sloužit pouze pro vývojové procesy. Tím se sníží riziko porušení integrity, které hrozilo v rámci téhož prostředí. Tímto krokem také dojde k jasnému rozdělení přístupů do vývojového, testovací a provozního prostředí a povede k zajištění principu oddělení prostředí, které je vyžadováno v opatření Princip oddělení prostředí vývoje, testování a provozu (A. 12.1.4) a snazšímu zavedení opatření Bezpečné vývojové prostředí (A. 14.2.6).

**Tab. č. 13: Náklady na řízení změn systémů**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice ,,Změny v software” | Vedoucí vývojového oddělení | 16 hodin |
| Aktualizace uživatelských příruček | Vedoucí technického oddělení | 80 hodin / rok |
| Archivace neaktuálních verzí a uživatelských příruček | Vedoucí technického oddělení | 20 hodin / rok |
| Nákup hardwaru:<br>1 x Lenovo ThinkServer TS440<br>1 x WD Red - 2TB | Správce IT | <br>25 040 Kč bez DPH<br>2 142 Kč bez DPH |
| Nákup sofwaru:<br>Windows Server Standard 2012 R2 | Správce IT | <br>15 804 Kč bez DPH |
| Konfigurace a nastavení serveru | Správce IT | 24 hodin |

### 3.3.6. Přezkoumání aplikací po změnách provozní platformy (A. 14.2.3)

Mezi provozní platformy řadíme operační systémy, databáze, software a aplikace, které podporují chod hlavních firemních procesů. V případě změny některých z těchto provozních platforem je nutno následně provést technické přezkoumání a ujistit se, že tyto změny nemají vliv na provoz a bezpečnost společnosti. Z toho důvodu je nutné vytvořit postup, který bude prováděn při změnách provozních platforem.

Před samotnou změnou provozních platforem navrhuji vydat oznámení, které bude včasně informovat všechny zainteresované osoby, jaké změny budou provedeny. Toto oznámení doporučuji vydat správcem IT po dohodě s ředitelem společnosti. Doporučuji toto oznámení vydat nejpozději 1 měsíce před samotnou změnou. Následně po provedení změn by měl správce IT přezkoumat integritu těch aplikací, které by mohly být danou změnou negativně ovlivněny, a tím by mohla být porušena kontinuita hlavních firemních procesů. Tento postup by měl být zaznamenán ve směrnici „Technické přezkoumání aplikací po změnách provozní platformy."

**Tab. č. 14: Náklady na přezkoumání aplikací po změnách**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Technické přezkoumání aplikací po změnách provzní platform" | Správce IT | 24 hodin |

### 3.3.7. Omezení změn softwarových balíků (A. 14.2.4)

V současné době tato společnost žádný modifikovaný software nepoužívá. Veškeré softwarové vybavení je využíváno bez úprav. Toto opatření přesto doporučuji zavést, a to v případě, že by společnost plánovala modifikovat používaný software v budoucnu.

Navrhuji vytvořit směrnici „Změny v softwarovém vybavení", která by měla zahrnovat následující body:

- V případě změn softwarových balíků musí společnost zajistit riziko integrity, tak aby nedošlo k narušení kompatibility s ostatním používaným softwarem.
- Zajistit souhlas dodavatele softwaru, který opravňuje provádět konkrétní změny.

- Před jakoukoliv změnou je nutné určit, zdali se v důsledku změn společnost nestává zodpovědnou za budoucí údržbu softwaru.
- Důležité je také zajistit získání všech aktualizací, jako tomu bylo před samotnou změnou.

**Tab. č. 15: Náklady na omezení změn softwarových balíků**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice ,,Změny v softwarovém vybavení" | Správce IT | 16 hodin |

### 3.3.8. Bezpečné vývojové prostředí (A. 14.2.6)

V rámci tohoto opatření by mělo dojít k vytvoření bezpečného vývojového prostředí, v kterém je nutno pracovat v každé fázi vývoje softwaru.

Zavedení bezpečné vývojové prostředí doporučuji zavést v analyzované společnosti. V současné době bezpečnost vývojového prostředí není žádným způsobem řešena. Bezpečné vývojové prostředí by mělo být definováno pro každý programovací jazyk.

Navrhuji vytvořit směrnici ,,Bezpečné vývojové prostředí", která bude obsahovat následující body:

- Řízení přístupů vývojových pracovníků k vývojovému prostředí.
- Uložení záloh zdrojových kódů na bezpečných externích discích.
- Monitorování změn ve vývojovém prostředí a změny v kódu.
- Kontrola nad přesunem kódu mezi vývojovým, testovacím a produkčním prostředím.

Navrhuji vytvořit přístupy k vývojovému prostředí pouze pro zaměstnance z vývojového oddělení, přístupy jsou vytvořeny na základě schválení vedoucího vývojového oddělení. V současné době provádí společnost zálohy zdrojových kódů na NAS server, kde jsou zálohy i z provozních a testovacích databází. Pro zvýšení bezpečnosti doporučuji zakoupit ještě jeden NAS server, který bude sloužit pouze pro zálohování vývojového serveru obsahující zdrojové kódy. Zálohu dat z vývojového serveru navrhuji provádět

jednou týdně úplnou zálohou a každý den rozdílovou zálohu. Dodržení těchto postupů povede také k naplnění požadavků v rámci opatření Řízení přístupu ke zdrojovým kódům programů (A. 9.4.5).

**Tab. č. 16: Náklady na bezpečné vývojové prostředí**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice ,,Bezpečné vývojové prostředí" | Vedoucí vývojového oddělení | 40 hodin |
| Konfigurace přístupů do vývojového prostředí | Správce IT | 16 hodin |
| Nákup hardware:<br>1 x Synology DS215<br>1 x WD Red - 2TB | Správce IT | <br>7 533 Kč bez DPH<br>2 142 Kč bez DPH |
| Konfigurace a nastavení NAS serveru a vývojového serveru | Správce IT | 16 hodin |

### 3.3.9. Vývoj zajišťovaný externími zdroji (A. 14.2.7)

Toto opatření má za úkol snižovat rizika, která jsou spojena s externím vývojem a zároveň zajistit kvalitu kódu takto vyvíjeným způsobem.

Některé části software jsou vyvíjeny externími partnery, proto je nutno dohlížet na vývoj těchto dílčích částí. Mezi externími partnery a analyzovanou společností v současné době existují licenční smlouvy, které ale přesně nedefinují vlastnická práva a práva k duševnímu vlastnictví. Navrhuji, aby tyto současné smluvní podmínky s externími dodavateli byly upraveny do podoby, kdy bude z pohledu legislativy zcela jasné, kdo je majitelem vlastnických práv a práv duševního vlastnictví. V rámci tohoto opatření by měl vedoucí vývojového oddělení předat externím partnerům model hrozeb, který popisuje hrozby s vlivem na bezpečnost vývoje. Externí vývojoví inženýři by měli dodržovat základní pravidla bezpečného vývoje, která jsou ve směrnici „Politiky bezpečného vývoje".

**Tab. č. 17: Náklady na vývoj zajišťovaný externími zdroji**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Úprava smluv s externími programátory | Ředitel společnosti | 20 hodin |
| Vytvoření modelu hrozeb | Vedoucí vývojového oddělení | 16 hodin |

### 3.3.10. Testování bezpečnosti systému (A. 14.2.8)

Testování softwaru by mělo být prováděno již během vývoje tak, aby byla zajištěna správná funkcionalita a bezpečnosti softwaru.

V současné době analyzovaná společnost nemá zcela zavedeny postupy při testování softwaru. Odpovědnost za testování má ředitel technického oddělení. Navrhuji rozdělit testování softwaru mezi vývojové a technické oddělení. Vývojové oddělení bude mít povinnost provádět tzv. assembly testy a testy jednotkové, které jsou prováděny samotnými programátory. Technické oddělení bude provádět integrační testy, systémové a akceptační testy. Integrační testy a jejich scénáře budou připravované zaměstnanci k tomu určenými - testery. Systémové testy budou prováděny jako funkční celek, ve kterém bude testování prováděno v širším rozsahu než v integračních testech. Poslední fází testování jsou akceptační testy, které budou zavedeny opatřením Testování akceptace systému (A. 14.2.9).

Výše uvedené postupy by měly být zavedeny do směrnice „Testování softwaru“. Do této směrnice doporučuji zavést i následující kroky:

- Stanovení předmětu testování.
- Definování odpovědné osoby za provedení testu.
- Určení typu testu.
- Použití vhodných testovacích dat.
- Sestavení časového plánu testování.
- Zhodnocení výsledků testování.

**Tab. č. 18: Náklady na testování bezpečnosti systému**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Testování softwaru” | Vedoucí vývojového a technického oddělení | 40 hodin |

### 3.3.11. Testování akceptace systému (A. 14.2.9)

V procesu testování softwaru je posledním testem akceptační test. Tyto testy jsou poslední fází testování před ostrým provozem. V současné době společnost v určité míře akceptační testy provádí, avšak tyto testy nejsou pevně stanoveny.

Akceptační testy budou prováděny na úrovni technického oddělení. Tyto akceptační testy budou zaměřeny na oblasti systému, které v průběhu integračních a systémových testů vykazovaly chybové chování. Akceptační testy by měly být prováděny v prostředí, které má reálně stejný charakter, jako prostředí zákazníka, a tím dochází k zajištění spolehlivosti testů. Veškeré postupy v rámci akceptačních testů by měly být součástí směrnice „Testování softwaru“.

**Tab. č. 19: Náklady na testování akceptace systému**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice „Testování software” | Vedoucí technického oddělení | 16 hodin |

### 3.3.12. Ochrana dat pro testování (A. 14.3.1)

Data, která jsou určena pro testování, by měla být vhodně vybrána, chráněna a kontrolována. Společnost ve většině případů používá data, která jsou uměle vytvořena. Ovšem v některých testovacích procesech se pracuje i s daty, které jsou z provozních databází. Žádná testovací data neobsahují osobní údaje ani citlivé informace, přesto je nutné používání provozních dat zabezpečit, aby nedošlo k jejich zneužití.

V analyzované společnosti je nutné s provozními daty zacházet podle pevně stanovených pravidel. Navrhuji vytvořit směrnici „Testovací data“, která přesně definuje jak s těmito daty zacházet. Doporučuji, aby provozní data, která jsou použita v rámci testování, byla na konci testování odstraněna. Kopírování provozních dat do testovacího prostředí by měla předcházet autorizace uživatele, a tato skutečnost by měla být zaznamenána.

**Tab. č. 20: Náklady na ochranu dat pro testování**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Testovací data” | Vedoucí technického oddělení | 16 hodin |

## 3.4. Druhá etapa

Druhá etapa obsahuje zavedení řady opatření, které vychází z analýzy současného stavu, a to především na hodnoty míry rizik, které byly vyhodnoceny jako vysoké a střední, dále budou navrhnuty opatření, která se vztahují k fyzické bezpečnosti a k bezpečnosti v prostředí lidských zdrojů.

### 3.4.1. Princip oddělení povinností (A. 6.1.2)

Snížení rizika, které vzniká neoprávněným užíváním nebo neúmyslným poškozením aktiv společnosti, je možné docílit metodou oddělení povinností a odpovědností.

Proto navrhuji aktualizovat směrnici „Role a odpovědnost bezpečnosti informací“, ve které bude tento princip uveden a jeho dodržování povede k omezení neoprávněných a neúmyslných zneužití aktiv společnosti.

**Tab. č. 21: Náklady na zavedení principu oddělení povinností**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice „Role a odpovědnost bezpečnosti informací” | Ředitel společnosti | 8 hodin |

### 3.4.2. Bezpečnost informací v řízení projektů (A. 6.1.5)

Veškeré projekty by měly být řízeny s ohledem na bezpečnost informací.

Doporučuji dodržovat metody řízení projektů, jejichž předmětem je posuzování rizik především v první fázi projektu. Dále pak vytvořit potřebná opatření. Dodržování bezpečnosti informací by mělo být zajištěno v rámci všech fází projektu a projektové cíle by měly být v korelaci se stanovenými cíli bezpečnosti informací. Odpovědnost za bezpečnost informací v řízení projektů by měla být definována již před zahájením projektu. Výše zmíněná fakta by měla být přidána do již existující směrnice „Řízení projektů“.

**Tab. č. 22: Náklady na bezpečnost informací v řízení projeků**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice „Řízení projektů” | Vedoucí vývojového oddělení | 8 hodin |

### 3.4.3. Politika mobilních zařízení (A. 6.2.1)

Používáním mobilních zařízení vznikají rizika, která je možno snížit vytvořením a přijetím politiky vztahující se na mobilní zařízení. V rámci tohoto opatření mobilními zařízeními rozumíme mobilní telefony, notebooky a tablety.

Kvůli používání firemních mobilních zařízení doporučuji společnosti vytvořit směrnici „Bezpečné použití mobilních zařízení“. Rizika spojená s únikem firemních informací jsou u mobilních zařízení poměrně vysoká. Z toho důvodu je nutné zavést a dodržovat určité postupy, které by měly obsahovat následující body:

- U mobilních zařízení musí být nastaveno automatické zamykání klávesnice (mobilní telefony),
- Mobilní zařízení zbytečně nevystavovat nebezpečí krádeže (neponechávat bez dozoru v autech, na veřejných místech atp.).
- Nepřipojovat se na nechráněné veřejné sítě (např. v obchodních domech, restauracích atp.).
- Soukromé mobilní zařízení nesmí být připojeny k firemní počítačové síti. (připojení je možné k Wi-Fi určené pro zákazníky, partnery a další návštěvníky)

Navrhuji také uspořádat školení, které by zvýšilo znalosti zaměstnanců o možných rizicích plynoucích z nedůsledného zacházení s mobilními zařízeními.

**Tab. č. 23: Náklady na politiku mobilních zařízení**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Bezpečné použití mobilních zařízení“ | Správce IT | 24 hodin |
| Školení „Bezpečné použití mobilních zařízení“ | Správce IT | 3 hodiny / rok |

### 3.4.4. Práce na dálku (A. 6.2.2)

Práce na dálku přináší bezpečnostní rizika, která by měla být snižována pomocí vytvořených postupů, stanovených podmínek a omezení v rámci společnosti.

Analyzovaná společnost v některých případech umožňuje pracovat svým zaměstnancům na dálku. Z toho důvod doporučuji toto opatření zavést a vytvořit směrnici „Práce z domu“. Tato směrnice nebude obsahovat náplň ani rozsah pracovní doby. Během práce na dálku se zaměstnanci společnosti připojují pomocí VPN ze svých firemních notebooků. Pomocí virtuální privátní sítě je možné se bezpečně připojit k informačnímu systému a k serveru.

Do směrnice „Práce z domu“ doporučuji zavést následující body:

- Zakázat připojení zaměstnanců k firemní síti ze svých soukromých stanic.
- Každý zaměstnanec, který může pracovat z domu, musí být evidován a musí dostat schválení od ředitele společnosti.
- Během práce na dálku může dojít k práci s různou úrovní informací, proto musí být dodržovány postupy, které jsou popsány v klasifikačním schématu informací.
- Připojení k virtuální privátní síti je nastaveno správcem IT, hesla k tomuto připojení nesmí být předvyplněná.
- Firemní notebook by měl být chráněn proti odcizení a neměl by být připojován k nechráněným veřejným sítím.
- Každý firemní notebook je chráněn dostatečně silným heslem k operačnímu systému

Vytvořenou směrnici musí podepsat ti zaměstnanci, kteří obdrželi povolení provádět práci z domu. Tím potvrdí, že jsou s těmito nezbytnými postupy seznámeni. Doporučuji také uspořádat školení, které by bylo spojeno se školením „Bezpečné použití mobilních zařízení“.

**Tab. č. 24: Náklady vztahující se k práci na dálku**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Práce na dálku” | Správce IT | 20 hodin |
| Školení „Práce na dálku” | Správce IT | 3 hodiny / rok |

### 3.4.5. Klasifikace informací (A. 8.2.1)

Klasifikace informací by měla být provedena s ohledem na jejich hodnotu, právní požadavky, kritičnost a citlivost v případě neoprávněného úniku.

Klasifikace informací by měla být definována tak, aby název jednotlivých klasifikačních úrovní indikoval, o jaký druh informace jde a jakým způsobem by se mělo s tímto druhem informace zacházet. V analyzované společnosti je klasifikace provedena na informace veřejné a informace neveřejné.

Navrhuji implementovat klasifikaci informací podle klasifikačního schématu informací znázorněného v tabulce č. 25, ve které doporučuji rozdělit informace do čtyř úrovní, tj. veřejné informace, interní informace, osobní údaje a citlivé informace.

**Tab. č. 25: Schéma klasifikace informací**
(Zdroj: Vlastní zpracování)

| Klasifikační úroveň | Popis |
|---|---|
| **Veřejné informace** | **Charakteristika** |
| | Informace, které jsou určeny ke zveřejnění a není potřeba je chránit z pohledu důvěrnosti. Důležitá je integrita, aby nedocházelo k zveřejňování nepravdivých skutečnosti. Např. informace na firemním webu, propagační materiály, inzerce pracovního místa atd. |
| | **Přístup** |
| | Přístup není omezen. |
| | **Zabezpečení** |
| | Informace v listinné ani v elektronické podobě není nutné z pohledu důvěrnosti ochraňovat. |
| **Interní informace** | **Charakteristika** |
| | Informace, které jsou určeny pro využití zaměstnanci a obchodními partnery a nemají charakter veřejné informace, citlivé informace nebo osobních údajů. Např. firemní směrnice, firemní postupy, finanční dokumenty, informace o zákaznících a partnerech (seznamy produktů, ceny produktů, počet licencí) atd. |
| | **Přístup** |
| | Přístup je omezen pouze na zaměstnance a obchodní partnery, kteří tento druh informací potřebují pro splnění pracovních závazků. |
| | **Zabezpečení** |
| | V listinné podobě musí dokumenty obsahující interní informace být zabezpečeny uzamykatelnou kanceláří. U elektronické podoby musí být přístup zajištěn heslem. |

| | |
|---|---|
| **Osobní údaje** | **Charakteristika** |
| | Informace, které vyplývají ze zákona č. 101/2000 Sb., o ochraně osobních údajů. Např. osobní údaje zaměstnanců (rodná čísla) atd. |
| | **Přístup** |
| | Přístup pouze pro zaměstnance, kteří potřebují tyto informace pro výkon své práce. Přistup je povolen konkrétním osobám nebo oddělením. |
| | **Zabezpečení** |
| | Listinná podoba musí být umístěna v uzamykatelných skříních a v uzamykatelné kanceláři. Elektronická podoba těchto dat musí být šifrována. V informačním systému s řízeným přístupem není šifrování vyžadováno. |
| **Citlivé informace** | **Charakteristika** |
| | V případě úniku těchto informací by mohlo dojít k vážnému ohrožení cíle společnosti a k riziku ukončení podnikatelské činnosti. Např. zdrojové kódy, smlouvy se zákazníky, smlouvy s partnery, informace týkající se firemní strategie a obchodního tajemství atd. |
| | **Přístup** |
| | Přístup mají pouze jednoznačně definovaní zaměstnanci. Přístup k citlivým informacím je možný v případě, že zaměstnanec bude souhlasit se závazným režimem a tento souhlas stvrdí podpisem. |
| | **Zabezpečení** |
| | Citlivé informace v listinné podobě musí být umístěny v uzamykatelných skříních a v uzamykatelné kanceláři. Elektronická podoba citlivých informací vyžaduje šifrování se silným heslem. V informačním systému s řízeným přístupem není šifrování vyžadováno. |

Klasifikační schéma by mělo být konzistentní a použito rámci celé společnosti. S novým klasifikačním schématem by měli být seznámeni zaměstnanci společnosti v rámci školení „Klasifikace informací“.

**Tab. č. 26: Náklady na klasifikaci informací**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace klasifikace informací | Ředitel společnosti | 8 hodin |
| Školení „Klasifikace informaci” | Správce IT | 2 hodiny / rok |

### 3.4.6. Označování informací (A. 8.2.2)

Označení u listinných informací je odlišné než u elektronických informací. Vždy by toto označení mělo vycházet z klasifikačního schématu informací.

U veřejných informací nedoporučuji zavádět žádná označení. Pro označení interních, citlivých informací a osobních údajů by měl být dokument označen textem INTERNÍ, CITLIVÉ nebo OSOBNÍ ÚDAJE dle klasifikace. Označení by mělo být umístěno v horní části stránky, aby bylo viditelné a okamžitě rozpoznatelné.

Doporučuji provést úpravu v informačním systému, kde nyní můžeme dokumenty označit pouze veřejné nebo neveřejné. Tato vlastnost je definována atributem „právo“, který by měl být přizpůsoben klasifikaci informací. Po implementaci této změny by bylo možné označit informace jako veřejná, interní, osobní, citlivá. Dále navrhuji úpravu tiskových výstupů, které budou obsahovat popis klasifikace v horní části dokumentu dle zvoleného atributu. Díky úpravě tiskových výstupů je možné neaktuálně označené dokumenty vytisknout znovu.

**Tab. č. 27: Náklady na označování informací**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Změna v IS (rožšíření atributu ,,právo”) | Vedoucí vývojového oddělení | 32 hodin |
| Změna v IS (tiskové výstupy) | Vedoucí vývojového oddělení | 16 hodin |

### 3.4.7. Manipulace s aktivy (A. 8.2.3)

V rámci tohoto opatření je důležité brát v úvahu manipulaci s aktivy, která obsahují různé úrovně informace. Proto by mělo být definováno, jakým způsobem zacházet, zpracovávat, ukládat a předávat tyto informace a také jak bude zacházeno se samotnými aktivy.

Oprávnění k manipulaci a k přemístění jednotlivých aktiv společnosti by měla být udělena pouze vlastníkům daných aktiv. V případě manipulace či přemístění aktiva jinou osobou než vlastníkem aktiva doporučuju zavést evidenci výpůjček s informacemi o začátku a konci výpůjčky a důvodem vypůjčení. Rozhodnutí o výpůjčce provádí vlastník aktiva. Tímto přístupem by měly být splněny požadavky v rámci opatření Přemístění aktiv (A. 11.2.5).

Musí být jasně specifikována manipulace s aktivy, která obsahuje určitou úroveň informace. U veřejných informací není nutné zavádět žádné omezení na jejich manipulaci. U informací, které se nachází v listinné podobě, je nejčastější a nejdůležitější činnosti kopírování, zasílání dokumentů poštou a samotné uložení. Přístup je řešen v klasifikačním schématu v rámci opatření Klasifikace informací (A. 8.2.1).

V tabulce č. 28 je vytvořen návrh, podle kterého by mělo docházet k manipulaci informací v listinné podobě.

**Tab. č. 28: Manipulace s informacemi**
(Zdroj: Vlastní zpracování)

| Klasifikační úroveň | Způsob manipulace s informacemi |
|---|---|
| **Interní informace** | **Kopírování** |
| | Může být provedeno pouze zaměstnancem společnosti nebo obchodním partnerem. |
| | **Posílání poštou** |
| | Zalepená poštovní obálka. |
| | **Ukládání** |
| | Informace jsou uloženy v uzamykatelných prostorech kanceláře. |
| **Osobní údaje** | **Kopírování** |
| | Kopírování pro pracovní účely v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů. |
| | **Posílání poštou** |
| | Posílat jako doporučené psaní. |
| | **Ukládání** |
| | Ukládání je prováděno v uzamykatelné kancelářské skříni a v uzamykatelné kanceláři. |
| **Citlivé informace** | **Kopírování** |
| | Vytvářet kopie mohou definování zaměstnanci po podepsání podpisového archu. |
| | **Posílání poštou** |
| | Citlivé informace se nesmí posílat poštou. |
| | **Ukládání** |
| | Ukládání je prováděno v uzamykatelné kancelářské skříni nebo ve firemním trezoru, vždy v uzamykatelné kanceláři. |

S informacemi v elektronické podobě je důležité brát ohled na úpravu, odstranění a tisk těchto dokumentů, které jsou přístupné v informačním systému zaměstnancům. Po provedení změn v IS (rozšíření atributu „Právo“ a úprava tiskových výstupů) v rámci opatření Označování informací (A. 8.2.2) lze nastavit omezení těchto činností autorizovaným osobám na základě přístupových práv. Zasílání elektronickou poštou u citlivých a osobních informací musí být šifrováno.

V rámci tohoto opatření doporučuji vytvořit novou směrnici „Manipulace s aktivy“, která bude obsahovat výše uvedené postupy pro ukládání citlivých informací v listinné podobě doporučuji pořídit firemní trezor.

**Tab. č. 29: Náklady na manipulaci s informacemi**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Manipulace s aktivy” | Ředitel společnost | 24 hodin |
| Nákup firemního trezoru:<br>Combi Line CL 40 E FS | Ředitel společnosti | 15 747 Kč bez DPH |

### 3.4.8. Registrace a zrušení registrace uživatele (A. 9.2.1)

Uživatelům systémů a služeb by měl být zajištěn přístup, tak aby nedošlo k ohrožení bezpečnosti informací a zároveň oprávnění uživatelé by měly mít přístup k informacím a službám, které jsou nezbytně nutné ke splnění jejich pracovních povinností.

Navrhuji provádět registraci nově nastupujícího zaměstnance jako nového uživatele nejpozději při zahájení jeho pracovní činnosti a zrušení registrace by mělo být provedeno nejpozději neprodleně po skončení pracovní smlouvy. Každý uživatel by měl mít svoji jedinečnou identifikaci, která bude definovat jeho oprávněné přístupy. Vytvoření oprávněných přístupů nebo jejich zrušení probíhá ve dvou fázích. V první fázi jde o vytvoření nebo zrušení uživatele a v druhé fázi jde o přidělení nebo odebrání přístupových práv. Doporučuji vytvořit směrnici „Řízení přístupů uživatelů“, která bude jasně definovat procesy spojené s uživatelskými přístupy.

**Tab. č. 30: Náklady na registrace a zrušení registrace uživatele**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Řízení přístupů uživatelů” | Správce IT | 24 hodin |

### 3.4.9. Zřízení přístupu uživatele (A 9.2.2)

V následujícím opatření by mělo dojít k definici a přiřazení přístupů již vytvořených uživatelů.

U analyzované společnosti je důležité při vytvoření nového uživatele poskytnout přístupy k informačnímu systému, serveru a zprovoznění e-mailových služeb. Navrhuji vytvořit řadu profilů na základě rolí uživatele, které budou obsahovat sadu přístupových práv k informačnímu systému a k přístupu na určitý server. Vytvoření těchto profilů musí být schváleno vedoucím každého oddělení a popsáno ve směrnici „Řízení přístupů uživatelů“.

V případě nepřiměřené úrovně přístupu mohou být některá přístupová práva odebrána nebo redukována. Zrušení nebo změna přístupových práv by měla být provedena také v případě ukončení pracovního poměru, tento krok musí být schválen vedoucím daného oddělení. Navrhuji do směrnice „Řízení přístupu uživatele“ připsat postup zrušení a změny přístupových práv. Tímto postupem by mělo být řešeny požadavky z opatření Odebrání nebo úprava přístupových práv (A. 9.2.6).

**Tab. č. 31: Náklady na zřízení přístupu uživatele**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice „Řízení přístupu uživatele” kapitola Zrušení a změny přístupových práv | Správce IT | 8 hodin |
| Aktualizace směrnice „Řízení přístupů uživatelů” kapitola Profily uživatel | Vedoucí technického oddělení | 16 hodin |

### 3.4.10. Přezkoumání přístupových práv uživatelů (A 9.2.5)

V pravidelných intervalech by mělo docházet ke kontrole přístupových práv všech uživatelů.

Navrhuji, aby docházelo k přezkoumávání přístupových práv v intervalu jednoho roku a dále v případě změny pozice zaměstnance anebo ukončení pracovního poměru. Tento proces přezkoumání bude popsán ve směrnici „Řízení přístupů uživatelů“ kapitola Přezkoumávání přístupových práv.

**Tab. č. 32: Náklady na přezkoumání přístupových práv**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice „Řízení přístupu uživatelů” kapitola Přezkoumávání přístupových práv | Správce IT | 8 hodin |
| Realizace přezkoumání přístupových práv | Správce IT | 16 hodin / rok |

### 3.4.11. Systém správy hesel (A. 9.4.3)

Systém správy hesel by měl zajistit kvalitu hesel a tím zvýšit bezpečnost informací v analyzované společnosti.

Zaměstnanci na začátku pracovního poměru v současnosti dostávají od správce IT své heslo, které umožňuje přístup k operačnímu systému, k informačnímu systému a k danému serveru. Heslo je doporučeno změnit po prvním přihlášení, ale kontrola změn hesel není důsledně prováděna. Systém správy hesel není analyzovanou společností jednoznačně definován, z toho důvodu navrhuji zavést následující doporučení, která by měla být sepsána ve směrnici „Správa hesel“.

- Heslo obsahuje alespoň 8 znaků.
- Heslo obsahuje alespoň jednu číslici a jedno malé a jedno velké písmeno.
- Heslo neobsahuje osobní údaje uživatele, telefonní čísla apod.
- Heslo nesmí obsahovat slova s obvyklou frekvencí výskytu.
- Změna hesla musí být provedena po prvním přihlášení.

- Heslo nesmí být fyzicky zaznamenáno, hesla mohou být uložena pomocí speciálních šifrovacích programů, které slouží k ukládání hesel. U hesel k těmto programům musí být dodržena stejná doporučení.
- Heslo nesmí být automaticky ukládáno.
- Hesla k různým službám by neměla být stejná.
- V případě ztráty nebo prozrazení hesla neprodleně kontaktovat správce IT (požadavek na obnovu hesla atp.).

Režim vyplývající z nově vytvořeného systému správy hesel by měl být závazný pro všechny zaměstnance. Doporučuji provádět školení, a to při zavedení nové směrnice a jednou ročně.

**Tab. č. 33: Náklady na systém správ hesel**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice ,,Správa hesel" | Správce IT | 8 hodin |
| Školení ,,Správa hesel" | Správce IT | 4 hodiny / rok |

### 3.4.12. Fyzické kontroly vstupu (A. 11.1.2.)

Vstup do prostor kanceláří automaticky by měl být umožněn pouze oprávněným osobám, tj. zaměstnancům společnosti, vstup dalších osob (zákazníci, partneři, návštěvníci) bude spadat do definovaného režimu.

Z analýzy současného stavu vyplývá, že fyzické kontroly jsou částečně zavedeny, ale nejsou dostatečné a reálně by mohlo dojít k neoprávněnému vniknutí do prostor společnosti nebo nekontrolovanému pohybu cizích osob. Z tohoto důvodu navrhuji zabezpečit vstupní dveře do prostor kanceláře novým přístupovým systémem, který bude obsahovat elektromotorický zámek a sadu uživatelských čipů. Výhodou tohoto přístupového systému je nedestruktivní dynamická metoda, automatické uzamykání dveří, malé rozměry čipů a možné připnutí čipu ke svazku klíčů, šifrování čipů algoritmem SHA - 1, evidence příchodu a odchodu zaměstnanců a monitorování vstupů cizích osob.

Pro kontrolu přístupů těchto osob bych doporučil uložení několika čipových klíčů na vrátnici, které vrátný přidělí návštěvě po telefonickém projednání s asistentkou

společnosti. S novým přístupovým systém budou seznámení všichni zaměstnanci společnosti a bude projednán s vlastníkem administrativní budovy v rámci dodavatelskou – odběratelských vztahů.

**Tab. č. 34: Náklady na fyzické kontroly vstupu**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Nákup přístupového systému:<br>1 x Elektromotorický zámek iLoock100<br>1 x Dveřní bateriová sada napájení<br>25 x Uživatelský čip Dallas iButton | Správce IT | <br>22 980 Kč bez DPH<br>490 Kč bez DPH<br>7 000 Kč bez DPH |
| Konfigurace přístupového systému | Správce IT | 20 hodin |
| Představení přístupového systému | Správce IT | 3 hodiny |

### 3.4.13. Údržba zařízení (A. 11.2.4)

Správná údržba zařízení by měla vést k zajištění především dostupnosti a integrity.

V analyzované společnosti má v současné době údržbu zařízení výpočetní techniky na starost správce IT. Důraz na údržbu zařízení není velký a neexistuje žádný ucelený postup, který by tento proces určoval. Navrhuji, aby údržbu zařízení prováděli vlastníci aktiv, kteří jsou zodpovědní za svá aktiva. Frekvence údržby by měla být přiměřená k danému aktivu. Při pořízení nového aktiva by k němu měl být přiřazen i vlastník, v tento okamžik má vlastník v rámci své odpovědnosti na starost i údržbu. V případě nefunkčnosti zařízení musí být zajištěna oprava buď správcem IT, nebo externími autorizovanými pracovníky. Pokud bude prováděn servis externími pracovníky, je nutné z nesprávně fungujícího zařízení odstranit osobní údaje, interní a citlivé informace nebo je jinak zabezpečit. Výše uvedené postupy by měly být popsány ve směrnici „Údržba zařízení“.

**Tab. č. 35: Náklady na údržbu zařízení**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Údržba zařízení” | Správce IT | 8 hodin |

### 3.4.14. Zásada prázdného stolu a prázdné obrazovky monitoru (A. 11.2.9)

Dodržování zásady prázdného stolu a prázdné obrazovky vede k celkovému snížení rizika neoprávněného přístupu, ztrátě nebo poškození informací.

Analyzovaná společnost v současné době ani jednu ze zásad nedodržuje. V případě nepřítomnosti zaměstnanců jsou notebooky často neodhlášeny. Na pracovních stolech některých zaměstnanců je možné najít dokumenty, které nepatří do klasifikace veřejných nebo interních informací, proto navrhuji vytvoření směrnice a prosazování dodržení obou zásad.

Zásada prázdného stolu by měla obsahovat pokyny vztahující se k umístění dokumentů, které obsahují citlivé informace a nebo osobní údaje, a to jak v listinné tak i v elektronické podobě v případě nepřítomnosti zaměstnance. Tyto informace během této doby musí být umístěny v uzamykatelné skříni nebo umístěny ve firemním trezoru a prázdná kancelář by měla být uzamčena. Zásada prázdného obrazovky stanovuje pravidla, která vedou ke snížení rizika neoprávněných přístupů v okamžiku nepřítomnosti oprávněných uživatelů. V rámci této zásady doporučuji odhlašování z operačního systému vždy, když uživatel opustí svoji pracovní stanici. Následné přihlášení by mělo být podmíněno vložením hesla. Obě zmíněné zásady by měly vycházet ze směrnice „Manipulace s aktivy“.

Při tvorbě směrnice „Zásada prázdného stolu a prázdné obrazovky“ navrhuji zahrnout i požadavky z opatření Neobsluhované uživatelské zařízení (A. 11.2.8). Pokud bude uživatel vzdálen od svého notebooku na 30 a více minut, měl by ukončit své aktivní relace ve spuštěných aplikacích, ukončit rozpracované úlohy a uložit je.

V rámci tohoto opatření doporučuji nákup tiskárny k výlučné potřebě ředitele společnosti, asistentky a účetní, která nebude ani síťově ani fakticky sdílena ostatními zaměstnanci. V současné době je pro všechny účely využívána jedna síťová tiskárna. Při tisku dokumentů obsahující citlivé informace nebo osobní data by takto bylo velmi obtížné zajistit ochranu těchto informací.

**Tab. č. 36: Náklady na zásadu prázdného stolu a prázdné obrazovky**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice ,,Zásada prázdného stoulu a prázdné obrazovky" | Správce IT | 16 hodin |
| Školení ,,Zásada prázdného stoulu a prázdné obrazovky" | Správce IT | 3 hodiny / rok |
| Nákup tiskárny:<br>1 x HP LaserJet Pro M225dn | Správce IT | 5 454 Kč bez DPH |
| Konfigurace a nastavení tiskárny | Správce It | 4 hodiny |

### 3.4.15. Zálohování informací (A. 12.3.1)

Zálohování informací je jedním ze základních postupů ochrany dat před jejich ztrátou a poškozením.

Politika zálohování by měla vycházet z požadavků společnosti a z požadavků, které vyplývají z analýzy současného stavu. Mělo by být pevně stanoveno, která data budou zálohována s jakou frekvencí a jakým způsobem. Toto rozhodnutí by mělo plynout z požadavků vlastníků dat.

V současné době společnost disponuje jedním NAS serverem, který slouží k zálohování dvou serverů. V rámci první etapy při opatření Bezpečné vývojové prostředí (A. 14.2.6) doporučuji zakoupit server pro vytvoření odděleného vývojového prostředí a zakoupení druhého NAS serveru, který bude určen pouze pro zálohování dat z vývojového prostředí.

Doporučuji zavést u vývojového a produkčního serveru úplnou zálohu jednou týdně a rozdílovou zálohu jednou denně. U testovacího serveru by měla být prováděna úplná záloha jednou do měsíce a rozdílová záloha každý den. Zálohovací servery by měly být kontrolovány a testovány, aby v případě potřeby byla zajištěna jejich okamžitá možnost obnovy. Tyto kontroly a testy doporučuji provádět správcem IT.

V rámci tohoto opatření doporučuji zavést plán obnovy týkající se obnovy po havárii některého ze serverů. Tento plán bude popsán směrnicí „Plán obnovy", v které by měly být definovány postupy, které je třeba realizovat, a to bezprostředně po zjištění havárie.

Tato směrnice by měla definovat následující body:

- Definování odpovědnosti za spuštění plánu obnovy a jeho provádění (správce IT).
- Činnosti, které budou prováděny během obnovy a jejich jasně definovaném pořadí např. zajištění vytvořených záloh, identifikování jejich druhu, rozbalení úplných a následně rozdílových záloh.
- Stanovení orientační doby obnovení dat, která je nutná pro provedení obnovy.
- Stanovení rozsahu stáří záloh, které jsou vytvářeny během pravidelné zálohy.

Aby tento plán obnovy vedl k efektivnosti a k zajištění kvality při obnově dat je nutné provádět testování tohoto plánu, popřípadě jeho aktualizaci navrhuji provádět testování plánu obnovy dvakrát ročně správcem IT.

Vytváření záloh mimo zálohovací servery je zakázáno, proto by všichni zaměstnanci měli být s touto zálohovací politikou seznámeni. Zálohování informací by mělo být stanoveno ve směrnici „Zálohování informací“

**Tab. č. 37: Náklady na zálohování informací**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Zálohování informací” | Správce IT | 32 hodin |
| Vytvotření směrnice „Plán obnovy” | Správce IT | 32 hodin |
| Testování plánu obnovy | Správce IT | 24 hodin / rok |
| Školení „Zálohování informací” | Správce IT | 4 hodiny / rok |

### 3.4.16. Odpovědnosti a postupy při řízení incidentů (A. 16.1.1)

Reakce na bezpečnostní incidenty by měly být rychlé a efektivní, vedení společnosti by mělo určit odpovědné osoby v rámci řízení vzniklých incidentů.

Postupy by měly zajistit stanovení odpovědnosti kompetentních zaměstnanců a definování kontaktního místa a účinné řízení incidentů bezpečnosti informací.

Postupy, které by měly být dodržovány vzhledem k tomuto opatření podle normy ISO/IEC 27002 jsou následující:

- Postupy pro plánování odezvy na incident.
- Postupy pro monitorování.

- Postupy pro zaznamenání incidentů.
- Postup pro zacházení s důkazy.
- Postupy pro posuzování o událostech bezpečnosti informací.
- Postupy pro odezvu.

Tyto postupy jsou součástí směrnice „Řízení incidentů“, kterou navrhuji vytvořit v rámci požadavků z opatření Podávání zpráv o událostech bezpečnosti informací (A.16.1.2), Rozhodování o událostech bezpečnosti informací (A. 16.1.4), Odezva na incidenty bezpečnosti informací (A. 16.1.5) a Ponaučení z incidentů bezpečnosti informací (A. 16.1.7), které jsou popsána níže. Aby nastalo vyhovující dodržování těchto postupů, navrhuji provést školení pro všechny zaměstnance a informovat zákazníky a partnery, kterých se tato opatření týká e-mailem.

**Tab. č. 38: Náklady postupy a odpovědnosti přiřízení incidentů**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření školení „Řízení incidentů” | Správce IT | 4 hodiny |

### 3.4.17. Podávání zpráv o událostech bezpečnosti informací (A. 16.1.2)

Události, které by mohli ovlivnit bezpečnost informací, musí být neprodleně hlášeny všemi zaměstnanci a zainteresovanými osobami.

Vytvořená směrnice „Řízení incidentů“ v kapitole Události bezpečnosti informací by měla obsahovat seznam událostí, při kterých je nutné podat zprávu odpovědné osobě. V této směrnici musí být uvedeno, kdo je zodpovědnou osobou za příjem těchto oznámení a jakým komunikačním kanálem mají být události hlášeny.

Navrhuji přiřadit zodpovědnost za příjem zpráv o událostech bezpečnosti informací správci IT, v případě jeho nepřítomnosti tuto zodpovědnost přebírá vedoucí technického oddělení. Doporučuji zavést podání zpráv o těchto událostech třemi způsoby, a to osobně, telefonicky nebo e-mailem. Každé podání musí být zaevidováno. Kontaktní údaje odpovědné osoby musí být uvedeny ve směrnici a musí s nimi být seznámeny všechny zainteresované osoby (zaměstnanci, zákazníci, partneři). Přičemž u zákazníků a partnerů

připadá v úvahu řízení incidentů v rámci poskytovaného softwaru. Hlášení by mělo být prováděno na základě zjištění situací, které vychází z normy ISO/IEC 27002:

- Zjištění nefungujícího bezpečnostního opatření.
- Narušení integrity, důvěrnosti, dostupnosti informací.
- Zjištění lidské chyby, která může vést k ohrožení bezpečnosti informací.
- Rozpor s firemními směrnicemi.
- Zjištění prolomení opatření v rámci fyzické bezpečnosti.
- Zjištění neřízené změny systému.
- Nefungující software nebo hardware.
- Nalezení porušení přístupu.

Uvedené situace nemusí znamenat okamžité riziko, ale můžou k němu vést, proto je důležité tyto zprávy o událostech hlásit a prozkoumávat.

**Tab. č. 39: Náklady na řízení kapacit**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Vytvoření směrnice „Řízení incidentů" kapitola Události bezpečnosti informací | Správce IT | 16 hodin |

### 3.4.18. Rozhodování o událostech bezpečnosti informací (A. 16.1.4)

Události ohrožení bezpečnosti informací, které jsou nahlášeny, by měly být posouzeny podle klasifikační stupnice a mělo by být rozhodnuto, zda jde o incident bezpečnosti informací, či nikoliv.

Vytvořený postup pro posuzování a rozhodování, obsahující klasifikační stupnici, by měl být popsán ve směrnici „Řízení incidentů" v kapitole Posouzení událostí bezpečnosti informací. Tyto postupy by měly popisovat následující body:

- Posouzení všech zaevidovaných událostí podle klasifikační stupnice.
- Rozhodnutí, zda se jedná o incident bezpečnosti informací.
- Kompletní výsledky rozhodnutí musí být zaznamenány.

**Tab. č. 40: Náklady na posouzení událostí bezpečnosti informací**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice ,,Řízení incident" kapitola Posouzení událostí bezpečnosti informací | Správce IT | 16 hodin |

### 3.4.19. Odezva na incidenty bezpečnosti informací (A. 16.1.5)

Na základě vzniklých incidentů by měla vzniknout odezva, která zajistí přiměřenou úroveň bezpečnosti a vede k vyřešení vzniklých incidentů.

Postup při vytváření odezvy by měl být formálně zapsán ve směrnici „Řízení incidentů" v kapitole Odezva na incidenty. V prvním kroku procesu odezvy by mělo dojít ke shromáždění všech důkazů (okolností provozní situace), které je možné zaznamenat neprodleně po výskytu incidentu.

Shromažďování důkazů obsahuje následující postupy:

- Identifikaci a dokumentování všech potencionálních důkazů.
- Shromažďování fyzických důkazů.
- Vytváření kopií dat, které jsou chápány jako důkaz.
- Zachování integrity vzniklého stavu.

Dodržením těchto postupů by mělo být zavedeno v rámci požadavků z opatření Shromažďování důkazů (A. 16.1.7).

Ve druhém kroku procesu odezvy na incident je důležité navrhnout řešení, která vedou k vyřešení vzniklých incidentů. Tato řešení mohou být projednána s dalšími zaměstnanci společnosti nebo s osobami, kterých se incident týká. Posledním krokem je formální zápis o provedeném řešení.

**Tab. č. 41: Náklady na odezvy incidentů**
(Zdroj: Vlastní zpracování)

| Doporučení | Odpovědnost | Náklady |
|---|---|---|
| Aktualizace směrnice ,,Řízení incident" kapitola Odezva na incidenty | Správce IT | 16 hodin |

### 3.4.20. Ponaučení z incidentů bezpečnosti informací (A. 16.1.6)

Při analýze incidentů dochází k identifikaci zdrojů těchto incidentů. Na základě této identifikace můžeme zavést nová opatření nebo zvýšit intenzitu stávajících, tak aby byly omezeny dopady a s nimi související náklady v případě budoucích výskytů. Kladen by měl být důraz na incidenty s relativně vysokou frekvencí výskytu a ty, které mají velký dopad na bezpečnost informací.

## 3.5. Třetí etapa

Třetí etapa zavedení systému řízení bezpečnosti informací by měla vést k dosažení certifikace. Tato opatření nejsou detailně popsána, protože společnost v současné době neusiluje o získání certifikace ISMS. Přesto byl vytvořen seznam těchto opatření, který je uveden v příloze č. 1. Na základě tohoto seznamu doporučuji společnosti v následujících letech zavést opatření vztahující se k třetí etapě a požádat o certifikaci ISMS.

## 3.6. Harmonogram realizace

Harmonogram realizace doporučených opatření je podrobně popsán v příloze č. 2. Tato příloha obsahuje Ganttův diagram, který zobrazuje předpokládanou dobu zavedení první a druhé etapy. Ganttův diagram byl sestaven na základě odhadů doby realizace jednotlivých opatření, při reálném zavedení se tato doba může mírně odlišovat od navrhnutého časového plánu.

Začátek zavedení systému řízení bezpečnosti informací byl na základě rozhodnutí ředitele společnosti stanoven na 1. 8. 2016 a předpokládaný konec zavádění byl odhadnut na 28. 11. 2016. Doba trvání první etapy byla odhadnuta na 34 dní a doba trvání druhé etapy na 38 dní. Mezi první a druhou etapou je ponechána časová rezerva 15 pracovních dnů. Celková doba zavedení první a druhé etapy se odhaduje na 86 dní. Po ukončení druhé etapy by měla společnost zvážit zavedení poslední (třetí) etapy, která by vedla k získání certifikace ISMS.

### 3.7. Ekonomické zhodnocení

Ekonomické zhodnocení je rozděleno na náklady a přínosy, které vychází ze zavedení a udržování systému řízení bezpečnosti informací. Náklady jsou rozděleny na náklady na technická řešení, na lidské zdroje a na provoz tohoto systému.

#### 3.7.1. Náklady na technická řešení

Náklady na technické řešení jsou souhrnem všech nákladů vynaložených na hardwarové a softwarové vybavení ostatní bezpečnostní produkty, které jsou nezbytné pořídit pro zavedení určitých opatření.

Tyto náklady jsou hodnotově uvedeny v tabulce č. 42, celkové náklady na technické řešení byly vyčísleny na 104 332 Kč bez DPH.

**Tab. č. 42: Náklady technické řešení**
(Zdroj: Vlastní zpracování)

| Název | Cena bez DPH |
|---|---|
| 1 x Lenovo ThinkServer TS440 | 25 040 Kč |
| 2 x Diskové pole - WD Red - 2TB | 4 284 Kč |
| 1 x Software - Windows Server Standard 2012 R2 | 15 804 Kč |
| 1 x NAS - Synology DS215 | 7 533 Kč |
| 1 x Trezor - Combi Line CL 40 E FS | 15 747 Kč |
| 1 x Elektromotorický zámek - iLoock100 | 22 980 Kč |
| 1 x Dveřní bateriová sada napájení | 490 Kč |
| 25 x Uživatelský čip - Dallas iButton | 7 000 Kč |
| 1 x Tiskárna - HP LaserJet Pro M225dn | 5 454 Kč |
| **Celkem** | **104 332 Kč** |

### 3.7.2. Náklady na lidské zdroje

Vedle nákladu na technické řešení je nezbytné počítat i s náklady na lidské zdroje. Tyto náklady jsou uváděny v tabulce ke každému opatření, souhrn časové náročnosti je zobrazen v tabulce č. 43. Pro zavedení opatření v první a druhé etapě je celkový počet hodin odhadnut na 768, přičemž časová náročnost první etapy je odhadnuta na 376 hodin a náročnost druhé etapy na 392 hodin. Odpovědnost za proces zavedení jednotlivých opatření a z toho vyplývající podíl na celkový odhad časové náročnosti se vztahuje k řediteli společnosti, ke správci IT a k vedoucím technického a vývojového oddělení. Tyto odpovědné osoby mohou jednotlivé úkoly dále delegovat, avšak odpovědnost náleží vždy odpovědné osobě.

**Tab. č. 43: Náklady na lidské zdroje**
(Zdroj: Vlastní zpracování)

| Označení | Řada opatření | Počet hodin |
|---|---|---|
| A.5 | Politiky bezpečnosti informací | 36 |
| A.6 | Organizace bezpečnosti informací | 76 |
| A.8 | Řízení aktiv | 82 |
| A.9 | Řízení přístupu | 64 |
| A.11 | Fyzická bezpečnost a bezpečnost prostředí | 54 |
| A.12 | Bezpečnost provozu | 64 |
| A.14 | Akvizice, vývoj a údržba systémů | 340 |
| A.16 | Řízení incident bezpečnosti informací | 52 |
| **Celkem** | | **768** |

Po konzultaci s ředitelem společnosti byl stanoven odhad, že z celkového počtu 768 hodin je možné přibližně polovinu těchto hodin uvolnit v rámci rezervy pracovních kapacit. Zbytek časového nákladu bude řešen rozšířením pracovních kapacit v průběhu zavádění procesu systému řízení bezpečnosti informací. Rozšíření pracovních kapacit může být provedeno na základě přijmutí nového zaměstnance, a to buď na hlavní pracovní poměr nebo na dohodu o provedení činnosti.

Při kalkulaci nákladů na lidské zdroje byla stanovena hodinová sazba 300 Kč vyplývající ze stanovené superhrubé mzdy. Při této hodinové sazbě a kalkulovaném počtu hodin 384 je odhadovaný náklad na lidské zdroje stanoven na 115 200 Kč.

### 3.7.3. Náklady na provoz ISMS

Systém řízení bezpečnosti informací musí být v rámci PDCA cyklu monitorován, přezkoumáván, udržován a zlepšován. Tyto postupy zajišťují nezbytnou zpětnou vazbu současného stavu systému a v případě potřeby by měla být provedena relevantní zlepšení. Postupy zajišťující provoz ISMS s sebou přináší další náklady, které jsou popsány v tabulce č. 44. Roční náklady vyjádřeny ve spotřebě práce jsou odhadnuty na 227 hodin.

**Tab. č. 44: Roční časové náklady na provoz ISMS**
(Zdroj: Vlastní zpracování)

| Označení | Řada opatření | Počet hodin / rok |
|---|---|---|
| A.5 | Politiky bezpečnosti informací | 64 |
| A.6 | Organizace bezpečnosti informací | 6 |
| A.8 | Řízení aktiv | 2 |
| A.9 | Řízení přístupu | 20 |
| A.11 | Fyzická bezpečnost a bezpečnost prostředí | 3 |
| A.12 | Bezpečnost provozu | 28 |
| A.14 | Akvizice, vývoj a údržba systémů | 104 |
| **Celkem** | | **227** |

Provozní náklady při stanovené hodinové sazbě 300 Kč jsou odhadnuty na 68 100 Kč. Ředitel společnosti předpokládá, že tyto náklady vycházející z provozu ISMS budou pokryty v rámci současné pracovní kapacity společnosti.

### 3.7.4. Přínosy zavedení ISMS

Při zavádění systému řízení bezpečnosti informací vznikají společnosti náklady, které jsou vyčísleny v předchozích kapitolách. Nejmenší požadovaná efektivita zavedení tohoto systému nastává, pakliže bude dosaženo přiměřené bezpečnosti při určitých nákladech. Z toho hlediska je důležité kvantifikovat i přínosy, které pramení ze zavedení systému řízení bezpečnosti informací.

Mezi hlavní přínosy v rámci zavedení nových postupů nebo změn postupů stávajících bych uvedl zvýšení úrovně bezpečnosti informací v rámci hlavních podnikových aktivit, z čehož vyplývá očekáváné snížení finanční ztráty. Těchto přínosů bude dosaženo díky vytvoření nových nebo upravení stávajících firemních směrnic, zavedením nových firemních školení do praxe, úpravou smluv, pořízení nového technického vybavení

společnosti, konfigurace a údržba zařízení. Jednou z podmínek k dosažení očekávaných přínosů je zvýšení kvality některých prvků firemní kultury.

Kalkulace těchto přínosů je velmi složitá, neboť nelze jednoznačně finančně ohodnotit jednotlivé přínosy. Tyto přínosy společnosti nepřináší zisk, ale snižují rizika, která mohou vést ke ztrátám finanční i nefinanční povahy. Seznam odhadovaných finančních ztrát v případě nezavedeného ISMS, který byl vytvořen ve spolupráci s ředitelem společnosti, je uveden v tabulce č. 45.

**Tab. č. 45: Přehled odhadovaných finančních ztrát**
(Zdroj: Vlastní zpracování)

| Hrozby | Finanční ztráta |
|---|---|
| Neoprávněný vstup do prostor společnosti (krádež zařízení) | až 500 000 Kč |
| Kompromitace hesla informačního systému | až 500 000 Kč |
| Odcizení nebo ztráta přenosného zařízení | až 200 000 Kč |
| Nedodržování metody prázdné obrazovky a metody prázdného stolu | až 150 000 Kč |
| Porušení mlčenlivosti ohledně osobních údajů | 100 000 Kč až 5 000 000 Kč |
| Odcizení záloh zdrojového kódu | až 4 000 000 Kč |
| Nedodržení bezpečného vývojového prostředí | až 1 000 000 Kč |
| Kompromitace obsahu smluv | až 2 000 000 Kč |

Příkladů odhadovaných finančních ztrát by mohlo být uvedeno více, ale při prozkoumání těchto uvedených konkrétních hrozeb si je nutné uvědomit, že finanční ztráty mohou dosahovat opravdu vysokých hodnot. Uvedené finanční ztráty v porovnání s náklady, které jsou nutné vynaložit na údržbu ISMS, jsou několika násobně vyšší.

# ZÁVĚR

Cílem mé diplomové práce je vytvoření návrhu systému řízení bezpečnosti informací v konkrétním podniku vycházející z analýzy současného stavu. Při vytvoření tohoto návrhu je přihlíženo k požadavkům a k postupům uvedených v souboru norem ISO/IEC 27000, které jsou brány jako doporučené neboť tento podnik neusiluje o udělení certifikace dle těchto norem.

V teoretické části této práce byly vymezeny východiska a pojmy v rámci systému řízení bezpečnosti informací a teoreticky popsány další nezbytná fakta, která byla následně použita v praktické části práce.

Na začátku praktické části byla provedena analýza současného stavu podniku. Jednou skupinou výstupů této analýzy jsou zjištěná rizika, která je možné zaznamenat díky znalosti a pozorování tohoto podniku. Druhou skupinou jsou zjištěné hodnoty míry rizik, které byly identifikovány pomocí maticové metody analýzy rizik, která vychází z analýzy aktiv podniku, z analýzy působících hrozeb a ze zranitelnosti identifikovaných aktiv.

Při tvorbě návrhu systému řízení bezpečnosti informací bylo nezbytné navrhnout plán zvládání rizik. Ředitelem společnosti byl navržený plán zvládání rizik přijat jako potencionální řešení bezpečnostní situace v podniku s tím, že zavádění jednotlivých opatření bude probíhat ve třech etapách, a to z důvodu odlišnosti charakteru jejich zavedení. V rámci toho návrhu plánu zvládání rizik ředitel společnosti akceptuje nízkou míru rizika stanovenou metodou maticové analýzy rizik.

Spuštění systému řízení bezpečnosti informací nastane v první etapě při zavedení politiky bezpečnosti informací a následného zavedení bezpečnostních opatření, která se vztahují k vývoji softwaru. Druhá etapa obsahuje bezpečnostní opatření, která jsou určena ke snížení vysokých a středních hodnot míry rizika zjištěných při maticové metodě analýzy rizik. Poslední třetí etapa obsahuje seznam doporučených opatření nezbytně nutných k získání zmíněné certifikace.

Celkový návrh zavedení systému řízení bezpečnosti informací obsahuje popis finanční a časové náročnosti provedení navržených opatření, následně byl vytvořen časový harmonogram.

Přijetím navržených opatření lze zřejmě dosáhnout některých přínosů, a sice: snížení neakceptovatelné míry rizika, snížení pravděpodobnosti finančních ztrát, všeobecné zvýšení bezpečnosti informací. Navíc realizací třetí etapy může být dosaženo certifikace dle zmíněných norem.

Domnívám se, že z výše uvedené stručné rekapitulace cílů, východisek, návrhů, jejich zpracování a hodnocení lze usuzovat na splnění stanoveného cíle.

# SEZNAM LITERATURY


(1) DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací*. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

(2) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

(3) ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 36 9797.

(4) Manktelow, James. Plan-Do-Check-Act (PDCA) Implementing New Ideas in a Controlled Way [online]. 2012 [cit. 2016-03-24]. Dostupné z: http://www.mindtools.com/pages/article/newPPM_89.htm

(5) Břicháček, Z. Audit informační bezpečnosti – systém řízení informační bezpečnosti (ISMS). [online]. 2015 [cit. 2016-3-31]. Dostupné z: http://blog.brichacek.net/audit-informacni-bezpecnosti-system-rizeni-informacni-bezpecnosti-isms/

(6) ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informaci.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. Třídící znak 36 9790.

(7) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3. vyd. Praha: Grada, 2010. ISBN 978-80-247-3051-6.

(8) Hujňák, Jaroslav, Petr Hujňák a Michael Motal. *Doporučená praxe Společnosti pro projektové řízení oblast Řízení rizik.* [online]. 2013 [cit. 2016-4-1]. Dostupné z: http://cspr.cz/wp-content/uploads/2014/09/Dobra_praxe_Rizeni_rizik_v1.pdf

(9) Dubec, Radek. *Management kybernetické bezpečnosti* [online prezentace]. [cit. 2016-4-5]. Dostupné z: https://moodle.unob.cz/course/view.php?id=293

(10) ČSN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 36 9790.

(11) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 36 9798.

(12) Peterka, J.: Kdo (a co) bude spadat pod nový zákon o kybernetické bezpečnosti?. *Lupa.cz* [online]. 2014 [cit. 2016-3-31]. Dostupné z: http://www.lupa.cz/clanky/kdo-a-co-bude-spadat-pod-novy-zakon-o-kyberneticke-bezpecnosti/

(13) Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 23. července 2014. Dostupný také z: https://www.zakonyprolidi.cz/cs/2014-18

(14) Vyhláška č. 316/2014 Sb., o bezpečnostních opatření, kybernetických bezpečnostních incidentech, reaktivních opatření a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) ze dne 15. prosince 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-316

(15) Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích ze dne 15. prosince 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

(16) Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ze dne 22. prosince 2010. Dostupné také z: https://www.zakonyprolidi.cz/cs/2010-432

(17) NIST. NIST SPECIAL PUBLICATIONS (SP). *csrc.nist.gov* [online]. 2016 [cit. 2016-4-2]. Dostupné z: http://csrc.nist.gov/publications/PubsSPs.html

(18) NIST. NIST General Information. *nist.gov* [online]. 2016 [cit. 2016-4-2]. Dostupné z: http://www.nist.gov/director/orgchart.cfm

# SEZNAM OBRÁZKŮ, TABULEK

## Seznam obrázků



## Seznam tabulek

# SEZNAM ZKRATEK

ICT – Information and Communication Technology (informační a komunikační technologie)

IS – Information System (informační systém)

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

IEC – International Electrotechnical Commission (mezinárodní elektrotechnická komise)

VPN – Virtual Private Network (virtuální privátní síť)

UTP – Unshielded Twisted Pair (nestíněná kroucená dvojlinka)

UPS – Uniterruptible Power Supply (zdroj nepřerušovaného napájení)

WPA2 – Wi-Fi Protected Access 2 (metoda zabezpečení bezdrátových sítí)

AES – Advanced Encryption Standard (šifrovací standard)

ISMS – Information Security Management System (systém řízení bezpečnosti informací)

NIST – National Institute of Standards and Technology (Národní institut pro standardy a technologie)

RAID – Redundant Array of Independent Disks (vícenásobné diskové pole nezávislých disků)

DNS – Domain Name System (systém doménových jmen)

NAS – Network Attached Storage (síťové datové uložiště)

FTP – File Transfer Protocol (protokol pro přenos souborů)

SHA–1 – Secure Hash Algorithm (kryptografická hashovací funkce)

# SEZNAM PŘÍLOH

Příloha č. 1: Seznam opatření

| Označení | Opatření | Etapa | Postup |
|---|---|---|---|
| **A.5** | **Politiky bezpečnosti informací** | | |
| **A.5.1** | **Pokyny managementu organizace k bezpečnosti informací** | | |
| A.5.1.1 | Politiky pro bezpečnost informací | 1. etapa | zavést |
| A.5.1.2 | Přezkoumání politik pro bezpečnost informací | 1. etapa | zavést |
| **A.6** | **Organizace bezpečnosti informací** | | |
| **A.6.1** | **Interní organizace** | | |
| A.6.1.1 | Role a odpovědnosti bezpečnosti informací | 2. etapa | zavést |
| A.6.1.2 | Princip oddělení povinností | 2. etapa | zavést |
| A.6.1.3 | Kontakt s autoritami | - | nezavádět |
| A.6.1.4 | Kontakt se zvláštními zájmovými skupinami | - | nezavádět |
| A.6.1.5 | Bezpečnost informací v řízení projektů | 2. etapa | zavést |
| **A.6.2** | **Mobilní zařízení a práce na dálku** | | |
| A.6.2.1 | Politika mobilních zařízení | 2. etapa | zavést |
| A.6.2.2 | Práce na dálku | 2. etapa | zavést |
| **A.7** | **Bezpečnost lidských zdrojů** | | |
| **A.7.1** | **Před vznikem pracovního vztahu** | | |
| A.7.1.1 | Prověřování | 3. etapa | aktualizovat |
| A.7.1.2 | Podmínky pracovního vztahu | - | zavedeno |
| **A.7.2** | **Během pracovního vztahu** | | |
| A.7.2.1 | Odpovědnost managementu organizace | 3.etapa | aktualizovat |
| A.7.2.2 | Povědomí, vzdělávání a školení o bezpečnosti informací | - | nezavádět |
| A.7.2.3 | Disciplinární řízení | 3.etapa | aktualizovat |
| **A.7.3** | **Ukončení a změna pracovního vztahu** | | |
| A.7.3.1 | Odpovědnosti při ukončení nebo změně pracovního poměru | - | zavedeno |
| **A.8** | **Řízení aktiv** | | |
| **A.8.1** | **Odpovědnost za aktiva** | | |
| A.8.1.1 | Seznam aktiv | 3. etapa | zavedeno |
| A.8.1.2 | Vlastnictví aktiv | 3. etapa | zavedeno |
| A.8.1.3 | Přípustné použití aktiv | - | nezavádět |
| A.8.1.4 | Navrácení aktiv | - | nezavádět |
| **A.8.2** | **Klasifikace informací** | | |
| A.8.2.1 | Klasifikace informací | 2.etapa | aktualizovat |
| A.8.2.2 | Označování informací | 2.etapa | aktualizovat |
| A.8.2.3 | Manipulace s aktivy | 2.etapa | zavést |
| **A.8.3** | **Manipulace s médii** | | |
| A.8.3.1 | Správa výměnných médií | 3.etapa | zavést |
| A.8.3.2 | Likvidace médií | 3.etapa | zavést |

| | | | |
|---|---|---|---|
| A.8.3.3 | Přeprava fyzických médií | - | nezavádět |
| **A.9** | **Řízení přístupu** | | |
| **A.9.1** | **Požadavky organizace na řízení přístupu** | | |
| A.9.1.1 | Politika řízení přístupu | 3.etapa | aktualizovat |
| A.9.1.2 | Přístup k sítím a síťovým službám | - | zavedeno |
| **A.9.2** | **Správa a řízení přístupu uživatelů** | | |
| A.9.2.1 | Registrace a zrušení registrace uživatele | 2.etapa | zavést |
| A.9.2.2 | Zřízení přístupu uživatele | 2.etapa | zavést |
| A.9.2.3 | Řízení privilegovaných přístupových práv | - | nezavádět |
| A.9.2.4 | Řízení tajných autentizačních informací uživatelů | - | nezavádět |
| A.9.2.5 | Přezkoumání přístupových práv uživatelů | 2.etapa | zavést |
| A.9.2.6 | Odebrání nebo úprava přístupových práv | 2.etapa | zavést |
| **A.9.3** | **Odpovědnost 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 | - | nezavádět |
| A.9.4.2 | Bezpečné postupy přihlášení | - | nezavádět |
| A.9.4.3 | Systém správy hesel | 2.etapa | zavést |
| A.9.4.4 | Použití privilegovaných obslužných programů | - | nezavádět |
| A.9.4.5 | Řízení přístupu ke zdrojovým kódům programů | 1.etapa | zavést |
| **A.10** | **Kryptografie** | | |
| **A.10.1** | **Kryptografická opatření** | | |
| A.10.1.1 | Politika pro použití kryptografických opatření | 3.etapa | zavést |
| A.10.1.2 | Správa klíčů | 3.etapa | zavést |
| **A.11** | **Fyzická bezpečnost a bezpečnost prostředí** | | |
| **A.11.1** | **Bezpečné oblasti** | | |
| A.11.1.1 | Zabezpečené oblasti | 3.etapa | aktualizovat |
| A.11.1.2 | Fyzické kontroly vstupu | 2.etapa | zavést |
| A.11.1.3 | Zabezpečení kanceláři, místností a vybavení | - | zavedeno |
| A.11.1.4 | Ochrana před vnějšími hrozbami a hrozbami prostředí | 3.etapa | zavést |
| A.11.1.5 | Práce v bezpečných oblastech | - | nezavádět |
| A.11.1.6 | Oblasti pro nakládku a vykládku | - | nezavádět |
| **A.11.2.** | **Zařízení** | | |
| A.11.2.1 | Umístění zařízení a jeho ochrana | - | zavedeno |
| A.11.2.2 | Podpůrné služby | - | zavedeno |
| A.11.2.3 | Bezpečnost kabelových rozvodů | - | zavedeno |
| A.11.2.4 | Údržba zařízení | 2.etapa | zavést |
| A.11.2.5 | Přemístění aktiv | 2.etapa | zavést |
| A.11.2.6 | Bezpečnost zařízení a aktiv mimo prostory organizace | - | nezavádět |
| A.11.2.7 | Bezpečná likvidace nebo opakované použití zařízení | - | nezavádět |
| A.11.2.8 | Neobsluhovaná uživatelská zařízení | 2.etapa | zavést |
| A.11.2.9 | Zásada prázdného stolu a prázdné obrazovky monitoru | 2.etapa | zavést |

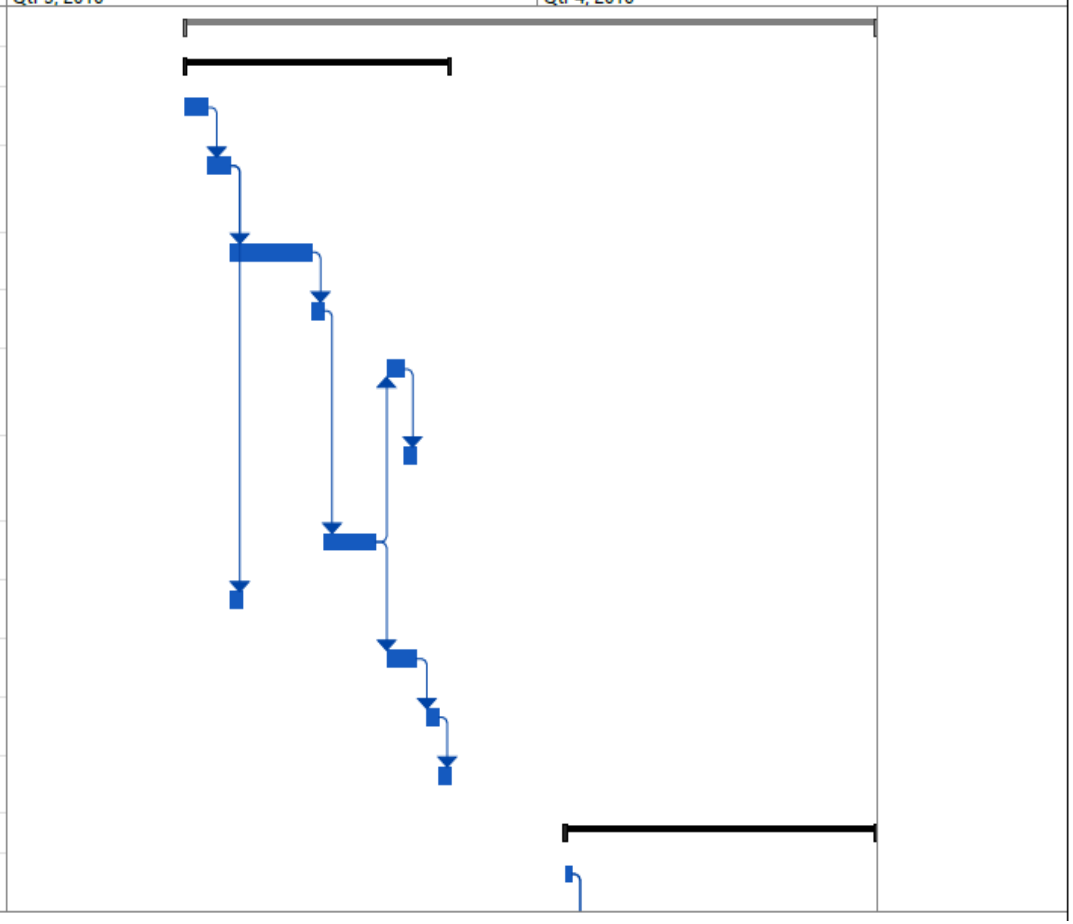
| | | | |
|---|---|---|---|
| **A.12** | **Bezpečnost provozu** | | |
| **A.12.1** | **Provozní postupy a odpovědnosti** | | |
| A.12.1.1 | Dokumentace provozních postupů | - | zavedeno |
| A.12.1.2 | Řízení změn | - | zavedeno |
| A.12.1.3 | Řízení kapacit | 2.etapa | zavést |
| A.12.1.4 | Princip oddělení prostředí vývoje, testování a provozu | 1.etapa | zavést |
| **A.12.2** | **Ochrana proti malwaru** | | |
| A.12.2.1 | Opatření proti malwaru | - | zavedeno |
| **A.12.3** | **Zálohování** | | |
| A.12.3.1 | Zálohování informací | 2.etapa | zavést |
| **A.12.4** | **Zaznamenávání formou logů a monitorování** | | |
| A.12.4.1 | Zaznamenávání událostí formou logů | 3.etapa | aktualizovat |
| A.12.4.2 | Ochrana logů | 3.etapa | aktualizovat |
| A.12.4.3 | Logy o činnosti administrátorů a operátorů | 3.etapa | aktualizovat |
| A.12.4.4 | Synchronizace hodin | 3.etapa | zavést |
| **A.12.5** | **Řízení a kontrola provozního softwaru** | | |
| A.12.5.1 | Instalace softwaru na provozní systémy | - | zavedeno |
| **A.12.6** | **Správa a řízení technických zranitelností** | | |
| A.12.6.1 | Správa a řízení technických zranitelností | 3.etapa | zavést |
| A.12.6.2 | Omezení instalace softwaru | - | zavedeno |
| **A.12.7** | **Hlediska auditu informačních systémů** | | |
| 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 | 3.etapa | zavést |
| A.13.1.2 | Bezpečnost síťových služeb | 3.etapa | aktualizovat |
| A.13.1.3 | Princip oddělení v sítích | - | zavedeno |
| **A.13.2** | **Přenos informací** | | |
| A.13.2.1 | Politiky a postupy při přenosu informací | - | nezavádět |
| 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 | - | nezavádět |
| **A.14** | **Akvizice, vývoj a údržba systémů** | | |
| **A.14.1** | **Bezpečnostní požadavky informančních 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 | - | zavedeno |
| **A.14.2** | **Bezpečnost v procesech vývoje a podpory** | | |
| A.14.2.1 | Politika bezpečného vývoje | 1.etapa | zavést |
| A.14.2.2 | Postupy řízení změn systémů | 1.etapa | aktualizovat |
| A.14.2.3 | Technické přezkoumání aplikací po změnách provozní platformy | 1.etapa | zavést |
| A.14.2.4 | Omezení změn softwarových balíků | 1.etapa | zavést |

| | | | |
|---|---|---|---|
| A.14.2.5 | Principy inženýrství bezpečných systémů | | |
| A.14.2.6 | Bezpečné vývojové prostředí | 1.etapa | zavést |
| A.14.2.7 | Vývoj zajišťovaný externími zdroji | 1.etapa | zavést |
| A.14.2.8 | Testování bezpečnosti systémů | 1.etapa | zavést |
| A.14.2.9 | Testování akceptace systémů | 1.etapa | zavést |
| **A.14.3** | **Data pro testování** | | |
| A.14.3.1 | Ochrana dat pro testování | 1.etapa | zavést |
| **A.15** | **Vztahy s dodavateli** | | |
| **A.15.1** | **Bezpečnost informací ve vztazích s dodavateli** | | |
| A.15.1.1 | Politika bezpečnosti informací pro dodavatelské vztahy | - | nezavádět |
| A.15.1.2 | Řešení bezpečnosti v rámci smluv s dodavateli | - | nezavádět |
| A.15.1.3 | Řetězec dodavatelů informačních a komunikačních technologií | - | nezavádět |
| **A.15.2** | **Řízení dodávky služeb dodavatelů** | | |
| A.15.2.1 | Monitorování a přezkoumávání služeb dodavatelů | - | nezavádět |
| A.15.2.2 | Řízení změn služeb dodavatelů | - | nezavádět |
| **A.16** | **Řízení incidentů bezpečnosti informací** | | |
| **A.16.1** | **Řízení incidentů bezpečnosti informací a zlepšování** | | |
| A.16.1.1 | Odpovědnosti a postupy | 2.etapa | zavést |
| A.16.1.2 | Podávání zpráv o událostech bezpečnosti informací | 2.etapa | zavést |
| A.16.1.3 | Podávání zpráv o slabých místech bezpečnosti informací | - | zavedeno |
| A.16.1.4 | Posouzení a rozhodnutí o událostech bezpečnosti informací | 2.etapa | zavést |
| A.16.1.5 | Odezva na incidenty bezpečnosti informací | 2.etapa | zavést |
| A.16.1.6 | Ponaučení z incidentů bezpečnosti informací | 2.etapa | zavést |
| A.16.1.7 | Shromažďování důkazů | 2.etapa | zavést |
| **A.17** | **Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací** | | |
| **A.17.1** | **Kontinuita bezpečnosti informací** | | |
| A.17.1.1 | Plánování kontinuity bezpečnosti informací | 3.etapa | zavést |
| A.17.1.2 | Implementace kontinuity bezpečnosti informací | 3.etapa | zavést |
| A.17.1.3 | Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací | 3.etapa | zavést |
| **A.17.2** | **Redundance** | | |
| A.17.2.1 | Dostupnost vybavení pro zpracování informací | - | nezavádět |
| **A.18** | **Soulad s požadavky** | | |
| **A.18.1** | **Soulad se zákonnými a smluvními požadavky** | | |
| A.18.1.1 | Identifikace příslušné legislativy a smluvních požadavků | 3.etapa | zavést |
| A.18.1.2 | Práva k duševnímu vlastnictví | 3.etapa | aktualizovat |
| A.18.1.3 | Ochrana záznamů | 3.etapa | zavést |
| A.18.1.4 | Soukromí a ochrana osobních údajů | 3.etapa | aktualizovat |
| A.18.1.5 | Regulace kryptografických opatření | - | nezavádět |
| **A.18.2** | **Přezkoumání bezpečnosti informací** | | |

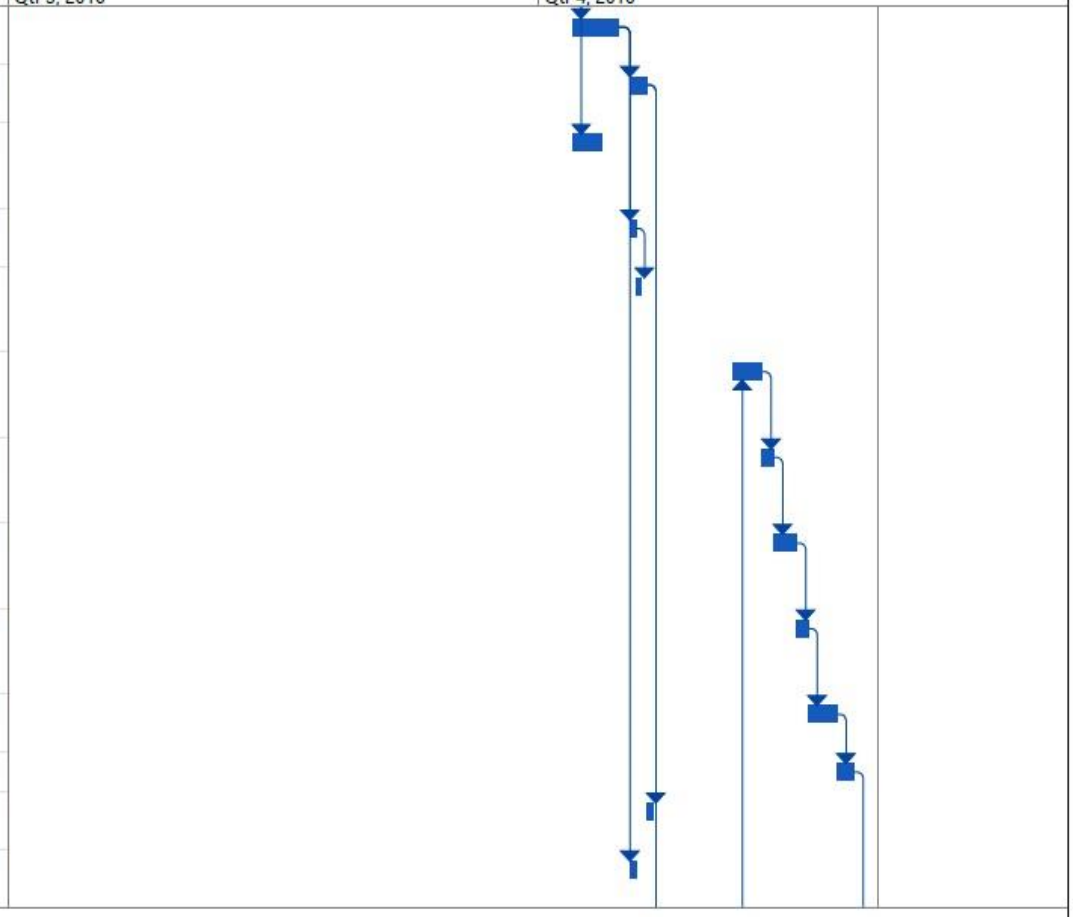
| | | | |
|---|---|---|---|
| A.18.2.1 | Nezávislá přezkoumání bezpečnosti informací | 3 etapa | zavést |
| A.18.2.2 | Soulad s bezpečnostními politikami a normami | 3 etapa | zavést |
| A.18.2.3 | Přezkoumání technického souladu | 3 etapa | zavést |

Příloha č. 2: Časový plán zavedení ISMS

| ID | Task Name | Duration | Start | Finish |
|---|---|---|---|---|
| 0 | **ISMS** | 86 days | Mon 1.8.16 | Mon 28.11.16 |
| 1 | **První etapa** | 34 days | Mon 1.8.16 | Thu 15.9.16 |
| 2 | Politiky pro bezpečnost informací A.5.1.1 | 4 days | Mon 1.8.16 | Thu 4.8.16 |
| 3 | Role a odpovědnosti bezpečnosti informací A.6.1.1 | 2 days | Fri 5.8.16 | Mon 8.8.16 |
| 4 | Politika bezpečného vývoje A.14.2.1 | 10 days | Tue 9.8.16 | Mon 22.8.16 |
| 5 | Postupy řízení změn systémů A.14.2.2 | 2 days | Tue 23.8.16 | Wed 24.8.16 |
| 6 | Přezkoumání aplikací po změnách provozní platformy A.14.2.3 | 3 days | Mon 5.9.16 | Wed 7.9.16 |
| 7 | Omezení změn softwarových balíků A.14.2.4 | 2 days | Thu 8.9.16 | Fri 9.9.16 |
| 8 | Bezpečné vývojové prostředí A.14.2.6 | 7 days | Thu 25.8.16 | Fri 2.9.16 |
| 9 | Vývoj zajišťovaný externími zdroji A.14.2.7 | 2 days | Tue 9.8.16 | Wed 10.8.16 |
| 10 | Testování bezpečnosti systému A.14.2.8 | 5 days | Mon 5.9.16 | Fri 9.9.16 |
| 11 | Testování akceptace systému A.14.2.9 | 2 days | Mon 12.9.16 | Tue 13.9.16 |
| 12 | Ochrana dat pro testování A.14.3.1 | 2 days | Wed 14.9.16 | Thu 15.9.16 |
| 13 | **Druhá etapa** | 38 days | Thu 6.10.16 | Mon 28.11.16 |
| 14 | Klasifikace informací A.8.2.1 | 1 day | Thu 6.10.16 | Thu 6.10.16 |



| ID | Task Name | Duration | Start | Finish |
|---|---|---|---|---|
| 15 | Označování informací A.8.2.2 | 6 days | Fri 7.10.16 | Fri 14.10.16 |
| 16 | Manipulace s aktivy A.8.2.3 | 3 days | Mon 17.10.16 | Wed 19.10.16 |
| 17 | Registrace a zrušení registrace uživatele A.9.2.1 | 3 days | Fri 7.10.16 | Tue 11.10.16 |
| 18 | Zřízení přístupu uživatele A.9.2.2 | 1 day | Mon 17.10.16 | Mon 17.10.16 |
| 19 | Přezkoumání přístupových práv uživatelů A.9.2.5 | 1 day | Tue 18.10.16 | Tue 18.10.16 |
| 20 | Zásada prázdného stolu a prázdné obrazovky monitoru A.11.2.9 | 3 days | Fri 4.11.16 | Tue 8.11.16 |
| 21 | Podávání zpráv o událostech bezpečnosti informací A.16.1.2 | 2 days | Wed 9.11.16 | Thu 10.11.16 |
| 22 | Rozhodování o událostech bezpečnosti informací A.16.1.4 | 2 days | Fri 11.11.16 | Mon 14.11.16 |
| 23 | Odezva na incidenty bezpečnosti informací A.16.1.5 | 2 days | Tue 15.11.16 | Wed 16.11.16 |
| 24 | Politika mobilních zařízení A. 6.2.1 | 3 days | Thu 17.11.16 | Mon 21.11.16 |
| 25 | Práce na dálku A. 6.2.2 | 3 days | Tue 22.11.16 | Thu 24.11.16 |
| 26 | Princip oddělení povinností A. 6.1.2 | 1 day | Thu 20.10.16 | Thu 20.10.16 |
| 27 | Bezpečnost informací v řízení projektů A. 6.1.5 | 1 day | Mon 17.10.16 | Mon 17.10.16 |



| ID | Task Name | Duration | Start | Finish | Qtr 3, 2016 | Qtr 4, 2016 |
|---|---|---|---|---|---|---|
| 28 | Systém správy hesel A.9.4.3 | 1 day | Fri 25.11.16 | Fri 25.11.16 | | |
| 29 | Zálohování informací A.12.3.1 | 8 days | Thu 20.10.16 | Mon 31.10.16 | | |
| 30 | Údržba zařízení A.11.2.4 | 1 day | Mon 28.11.16 | Mon 28.11.16 | | |
| 31 | Fyzické kontroly vstupu (A. 11.1.2) | 3 days | Tue 1.11.16 | Thu 3.11.16 | | |