VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

ZAVEDENÍ ISMS DO PODNIKU PODPORUJÍCÍHO KRITICKOU INFRASTRUKTURU

PROPOSAL FOR THE ISMS IMPLEMENTATION IN COMPANY WITH CI SUPPORT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Petr Šebrle
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Petr Šebrle**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Zavedení ISMS do podniku podporujícího kritickou infrastrukturu

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Závěr
Seznam použité literatury

Cíle, kterých má být dosaženo:

Cílem této práce je zanalyzovat současný stav bezpečnosti informací v podniku a navrhnout nápravná opatření v souladu a s využitím metodik popsaných v ČSN ISO/IEC 27000. V rámci této práce své návrhy zaměřuji pouze na první fázi implementace. Soubor opatření, který obsahuje tato fáze, byl vybrán vedením podniku jako akceptovatelný při zachování podnikem stanovených přiměřených nákladů.

Základní literární prameny:

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

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Obsahem této závěrečné práce je návrh zavedení managementu informační bezpečnosti ve středně velkém podniku podporujícím kritickou infrastrukturu. V úvodní části jsou shrnuty teoretické poznatky z této oblasti. Praktická část obsahuje analýzu současného stavu podniku, analýzu rizik a dále návrh na zavedení opatření dle přílohy A normy ČSN ISO/IEC 27001:2014. Implementace ISMS je rozdělena do čtyř etap, přičemž tato práce podrobně popisuje pouze první dvě.

Klíčová slova

ISMS, systém řízení bezpečnosti informací, normy řady ISO/IEC 27000, analýza rizik, bezpečnost ICT

Abstract

This diploma thesis deals with the methodology of Management of Information Security in a medium size company supporting critical infrastructure. The first part is focused on the theoretical aspects of the topic. Practical part consists of analysis of the current state, risk analysis and correction arrangements according to the attachment A of standard ČSN ISO/IEC 27001:2014. Implementation of ISMS is divided into four phases. This thesis however covers the first two phases only.

Keywords

ISMS, information security management system, ISO/IEC 27000 standards, risk analysis, ICT security

Bibliografická citace

ŠEBRLE, P. *Zavedení ISMS do podniku podporujícího kritickou infrastrukturu*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 78 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

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

V Brně 21.5.2017

……

Poděkování

Tímto bych rád poděkoval vedoucímu závěrečné práce panu Ing. Petrovi Sedlákovi za jeho cenné rady a připomínky.

1 Úvod

Rychlý rozmach výpočetní techniky, který nastartoval v polovině minulého století, vyžaduje shromaždování stále většího a většího množství dat. Tyto data jsou shromaždována na různých lokálních úložištích a v posledních deseti letech se s rozšířením rychlého internetu začaly tyto data skladovat také v datových centrech a to především při využití outsorcingu a cloudových služeb. Takto uložená data jsou pak lehce dostupná třetím stranám a náchylná na zneužití. Další možností, jak může dojít ke kompromitaci dat je útok pomocí různého malwaru anebo neoprávněným použitím zařízení.

Nejčastějším cílem útočníků jsou osobní data, informace o technologiích, obchodní informace podniků, přístupové údaje a podobně. V případě, že podnik nemá tyto data dostatečně zabezpečena, může dojít až k likvidaci podniku v důsledku zneužití ukradených dat.

Povinností každého podniku je zavést taková opatření, které by minimalizovaly možnosti útočníků a vliv úniku informací na chod podniku. V praxi se využívá velké množství různých způsobů zabezpečení a to od zamezení fyzického přístupu až po smluvní ošetření formou SLA.

Každý podnik by se měl aktivně zabývat identifikací aktiv a možných rizik, aby se mohl účinně bránit proti možným dopadům hrozeb.

2 Vymezení problému a cíle práce

Práce je zaměřena na problematiku řešení managementu informační bezpečnosti ve středně velkém podniku podporující kritickou infrastrukturu. V rámci své běžné činnosti přichází podnik do kontaktu s citlivými informacemi, které jsou uloženy v databázích účetního, rozpočtového a zakázkového programu a dále různých typech neelektronických dokumentů jako jsou faktury, smlouvy a rozpočty.

V minulosti tento podnik opakovaně nesplnil podmínky veřejné soutěže, když jedna z podmínek byly definované bezpečnostní politiky podniku. Odhadnutý ušlý zisk se za poslední dva roky pohybuje mezi osmi až devíti milióny korun. To byl hlavní důvod rozhodnutí vedení, že zavést ISMS alespoň v základním měřítku je nezbytnost.

Cílem této práce je návrh zavedení ISMS do společnosti dle metodik popsaných v sérii ČSN ISO/IEC 27000:2014. Své návrhy zaměřuji pouze na první dvě fáze implementace a to jak z rozsahových důvodů samotné práce, tak kvůli náročnosti implementace a možných nepřesností plánování časově vzdálených úkonů. Soubor opatření, které obsahují tyto fáze, byl vybrán vedením podniku jako akceptovatelný při zachování podnikem stanovených přiměřených nákladů.

3 Teoretická východiska práce

3.1 Základní pojmy

- **Informace** - údaj o prostředí, jeho stavech a procesech v něm probíhajících. Informace snižuje nebo odstraňuje množství entropie v systému. Množství informace je rozdíl mezi neurčitostí informace před a po zprávě. (1)
- **Aktivum** - je jakýkoliv hmotný nebo nehmotný majetek. (2)
- **Informační systém** - lze chápat jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují (1)
- **Síťová infrastruktura** - soubor všech síťových prvků a zařízení použitých při realizaci ICT prostředí.
- **Bezpečnost informací** - zabývá se ochranou (zachování důvěrnosti a integrity) a dostupností informací. Nezahrnuje pouze IS/ICT práci s informacemi, ale i informace v nedigitální podobě. Nejvýše je položená bezpečnost organizace s úkolem zajištění objektu a tím také majetku organizace. (1)

Obrázek 1: Princip bezpečnosti informací (3)

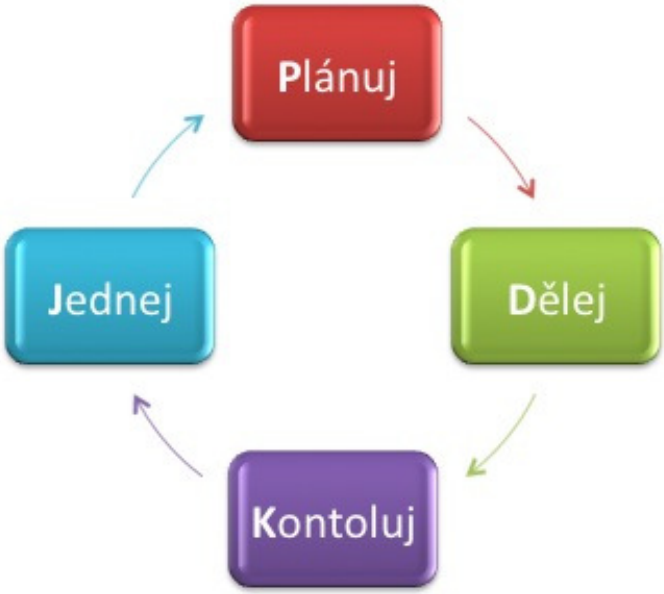
- **Dostupnost** - zajištění dostupnosti informací oprávněným uživatelům v požadovaný okamžik (2)
- **Důvěrnost** - informace jsou přístupné pouze těm, kteří mají patřičná oprávnění (2)
- **Integrita** - zajištění úplnosti a správnosti informace (2)
- **Hrozba** - je událost nebo činnost ohrožující bezpečnost. Jedná se o zneužití zranitelnosti. Zdrojem hrozeb můžou být např. přírodní události nebo lidé. Ti pak mohou vytvářet hrozby neúmyslně nebo s úmyslem poškodit danou organizaci.
- **Zranitelnost** - slabé místo aktiva. Působením hrozby může dojít ke zničení nebo poškození hodnoty daného aktiva.
- **Opatření** - opatření umožňující snížení hrozby
- **Riziko** - jako kombinace hrozby a zranitelnosti poukazuje na dopad na aktivum
- **Dopad** - vznik škody v důsledku působení hrozby (1)

3.2 Demingův model

Cyklus zlepšování PDCA je nazývá podle svého tvůrce jako Demingův cyklus. Je založen na čtyřech fázích, ve kterých by mělo docházet ke zlepšování jakosti nebo realizace změn.

Uvedený cyklus nemá konce a měl by se neustále opakovat a zajišťovat tak systém neustálého zlepšování. Tento cyklus je součástí každého procesu, který se plánuje, realizuje nebo kontroluje.

Cyklus PDCA je základem procesu neustálého zlepšování (základní požadavek normy ISO 9001).



Obrázek 2: Demingův cyklus (3)

Význam jednotlivých fází cyklu PDCA:

P = plan (plánuj) – sestavení plánu, který přinese maximální hodnotu (zvýšení zisku, zvýšení hodnoty pro zákazníka…)

D = do (konej) – realizace plánu, zavedení do praxe.

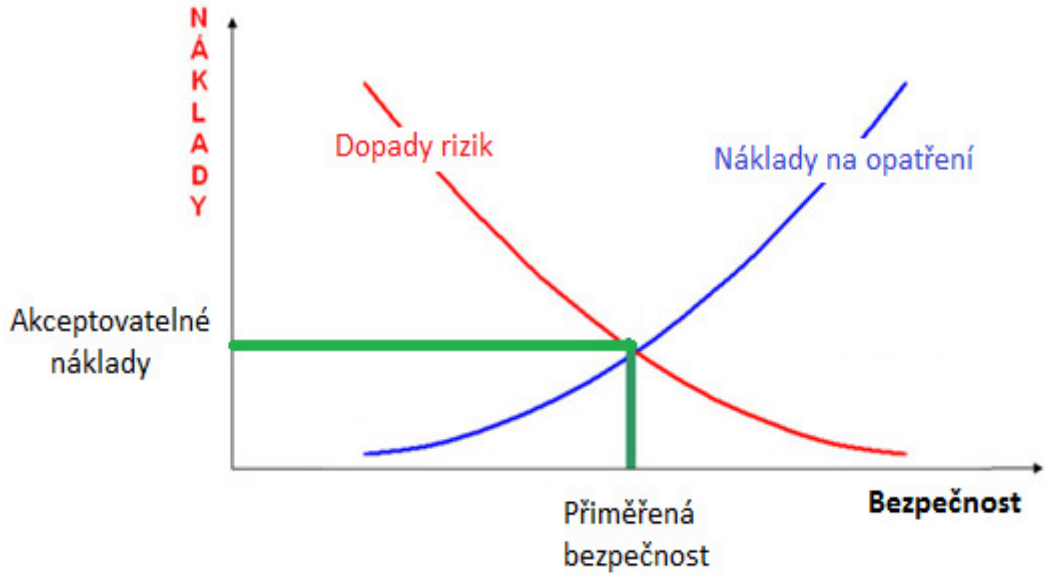
C = check (ověř) – monitorování, analýza a přezkoumání, zda podnik dosahuje vytyčených cílů a zda dosahuje požadovaných výsledků.

A = act (reaguj) – vyhodnocení a provedení opatření reagujících na dosažené výsledky a vedoucích ke zlepšení (zda setrvat v plánu nebo změnit směr) (4)

3.3 Přiměřená bezpečnost

Přiměřená bezpečnost definuje hranici nákladů na snížení nebo odstranění rizika, která je akceptovatelná s ohledem na možnou výši způsobené škody. V praxi to pak znamená, že není nutné úplně odstraňovat všechna možná rizika a používat na ně nepřiměřené zdroje, které by ve výsledku mohly mít vyšší náklady, jak výsledná způsobená škoda při dopadu rizika.

Je tedy třeba definovat přiměřenou bezpečnost za akceptovatelných nákladů. (1)



Obrázek 3: Přiměřená bezpečnost (vlastní zpracování na základě (1))

3.4 Základní normy řady 27000

ČSN ISO/IEC 27000:2014 / Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník

Norma poskytuje přehled systémů řízení bezpečnosti informací, které tvoří předmět rodiny norem ISMS a termíny a definice obecně používané v řadě norem ISMS. Tato mezinárodní norma je použitelná pro všechny typy a velikosti organizací (například pro vládní úřady, obchodní podniky i neziskové organizace). Organizace mohou použitím rodiny norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých aktiv a připravit nezávislé ohodnocení svých ISMS týkající se ochrany informací (např. finančních, duševního vlastnictví, podrobnosti o zaměstnancích atd.). (5)

ČSN ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky

Tato mezinárodní norma specifikuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací v rámci kontextu rizik činnosti organizace. Zahrnuje také požadavky na posouzení a ošetření rizik

bezpečnosti informací, přizpůsobené potřebám organizace. Norma prosazuje přijetí procesního přístupu k řešení ISMS a zavádí model známý jako Plánuj-Dělej-Kontroluj-Jednej (PDCA).

Příloha A této normy obsahuje cíle a jednotlivá opatření, které jsou přímo odvozeny a propojeny s těmi, které jsou uvedeny v ČSN ISO/IEC 27002:2014 a musí být použity v kontextu požadavků procesu ošetření rizik bezpečnosti informací. V příloze B je uveden vztah mezi principy OECD pro bezpečnosti informačních systémů a sítí a fázemi PDCA cyklu. Požadavky této mezinárodní normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. (6)

ČSN ISO/IEC 27002:2014 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací

Tato mezinárodní norma je určena pro organizace k použití jako doporučení pro výběr opatření v rámci procesu zavádění systému řízení bezpečnosti informací (ISMS), založeného na normě ISO/IEC 27001, nebo jako pokyny pro organizace, implementující obecně přijatá opatření bezpečnosti informací. Tato norma je rovněž určena pro použití při vyvíjení směrnic pro řízení bezpečnosti informací specifických pro průmysl a organizace, s přihlédnutím k jejich konkrétnímu prostředí rizik pro bezpečnost informací. Bezpečnostní opatření podporující dosahování podnikatelských cílů, kdy odpovědnost za ně je možné jednoduše přiřadit osobám s odpovídajícími funkcemi. Bezpečnost informací je dosažena zavedením vhodné sady opatření, včetně politik, procesů, postupů, organizačních struktur a softwarových a hardwarových funkcí. Tato opatření je třeba stanovit, implementovat, monitorovat, přezkoumávat a zlepšovat tam, kde je to nutné, aby bylo zajištěno, že jsou splněny specifické cíle bezpečnosti a podnikatelské činnosti organizace. (7)

ČSN ISO/IEC 27003:2011 Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací

Tato norma poskytuje doporučení pro ustanovení a implementaci systému řízení bezpečnosti informací (ISMS) v souladu s požadavky normy ISO/IEC 27001. Norma je použitelná pro všechny typy organizací, které zavádějí ISMS. Norma vysvětluje proces návrhu a implementace ISMS pomocí popisu zahájení, definování a plánování projektu

implementace ISMS. Výsledkem tohoto procesu je finální plán implementace projektu ISMS. Na základě tohoto plánu lze v organizaci realizovat projekt implementace ISMS. Norma popisuje proces plánování implementace ISMS v pěti etapách:

1. získání souhlasu vedení organizace se zahájením projektu ISMS;
2. definování rozsahu, hranic a politiky ISMS;
3. provedení analýzy požadavků bezpečnosti informací;
4. provedení hodnocení rizik a plánování zvládání rizik;
5. návrh ISMS.

Konkrétní finální plán implementace projektu ISMS organizace je hlavním výstupem 5. etapy. Zahrnuje návrh organizace bezpečnosti informací, bezpečnosti ICT, fyzické bezpečnosti a návrh dalších opatření naplňujících specifické požadavky ISMS (normy ISO/IEC 27001) jako je například plán přezkoumání ISMS vedením organizace nebo návrh programu vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací.

V přílohách této normy jsou pak uvedeny kontrolní seznam činností potřebných k ustanovení a implementaci ISMS, popis rolí a odpovědností bezpečnosti informací, informace o interním auditování, struktury politik a informace o monitorování a měření bezpečnosti informací. (8)

ČSN ISO/IEC 27004:2011 Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací – Měření

Tato norma poskytuje doporučení pro vývoj a používání metrik a pro měření účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a účinnosti opatření nebo skupin opatření, jak je uvedeno v ISO/IEC 27001. Program měření bezpečnosti informací zahrnuje procesy rozvoje metrik a měření, provádění měření, analýzu dat a hlášení výsledků měření a dále proces vyhodnocení a zlepšování programu měření bezpečnosti informací. V příloze normy jsou pak uvedeny příklady konceptů měření pro určitá opatření nebo procesy ISMS. (9)

ČSN ISO/IEC 27005:2013 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací

Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecný koncept specifikovaný v ISO/IEC

27001 a je strukturována, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. V souladu s přístupem k řízení rizik popsaným v této normě lze pro implementaci požadavků ISMS použít některou z celé řady existujících metodik pro řízení rizik. Norma je určená manažerům a pracovníkům, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací a tam, kde je to relevantní, také externím subjektům. Je aplikovatelná na všechny typy organizací (např. komerční společnosti, vládní organizace, neziskové organizace), které mají v úmyslu řídit rizika, která mohou narušit bezpečnost informací organizace. (2)

ČSN ISO/IEC 27006:2013 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Tato norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací (ISMS) a doplňuje tak požadavky obsažené v ČSN ISO/IEC 17021 a ISO/IEC 27001. Norma je primárně určená k podpoře procesu akreditace certifikačních orgánů poskytujících certifikace ISMS. (10)

ČSN ISO/IEC 27007:2013 Informační technologie - Bezpečnostní techniky - Směrnice pro audit systémů řízení bezpečnosti informací

Tato mezinárodní norma poskytuje doporučení pro řízení auditů systému řízení bezpečnosti informací (ISMS) a provádění interních nebo externích auditů v souladu s ISO/IEC 27001:2005. Zároveň dává návrhy na odbornou způsobilost a kvalifikaci auditorů ISMS. Norma ČSN ISO/IEC 27007 neuvádí požadavky ale doporučení pro všechny uživatele, včetně malých a středních organizací. Příloha A normy poskytuje všeobecné doporučení, jak provádět audit procesů ISMS tak, jak to požaduje norma ISO/IEC 27001, bez ohledu na konkrétní požadavky v oblasti ISMS, které by jednotlivá organizace mohla mít. (11)

3.5 Aktiva

Aktivum znamená v překladu majetek. V našem případě budeme toto označení používat pro veškerý hmotný a nehmotný majetek podniku.

3.5.1 Definice a klasifikace aktiv

Před ohodnocením aktiv je třeba tyto aktiva identifikovat. To se provádí tak, že se všechna aktiva, která mají nějakou logickou souvislost, seskupí. Dalším důležitým krokem je identifikovat vlastníka, který je za aktiva odpovědný. Ten následně určuje hodnotu daného aktiva. (1)

3.5.2 Hodnocení aktiv

K určení hodnoty aktiv je vhodné využít vhodný softwarový nástroj (např. metodika CRAMM) nebo je možné pro základní výpočet použít libovolný tabulkový editor (např. MS Excel).

Nutnost je vytvořit stupnici pro hodnocení a k ní hodnotící kritéria. Stupnice může být kvantifikována v libovolných vhodných jednotkách. Ve většině případů je vhodné použít bodovou škálu se stupnicí 1 až 5, kde 5 znamená nejvyšší stupeň rizika, popř. stupnici peněžní, kdy se používá hodnota aktiva v místní měně. (1)

Příklad tabulky sloužící k hodnocení aktiv:

Tabulka 1: Příklad ohodnocení aktiv (vlastní zpracování dle (1))

Hodnota aktiva	Ohodnocení dopadu	Hodnota rizika
5 Velmi vysoká	Existenční potíže organizace	Nepřijatelné riziko
4 Vysoká	Vážné potíže či podstatné finanční ztráty	Nežádoucí riziko
3 Střední	Potíže či finanční ztráty	Nízké riziko
2 Nízká	Zanedbatelný dopad na organizaci	Akceptovatelné riziko
1 Velmi nízká	Žádný dopad na organizaci	Bezvýznamné riziko

Hlavním principem při hodnocení aktiv jsou náklady vzniklé v důsledku porušení důvěrnosti, integrity a dostupnosti. Toto ohodnocení je nutné provádět s majitelem aktiva a je vhodné následně konzultovat s jeho uživateli.

Samotný výpočet hodnoty aktiva se pak může provádět různými způsoby. Nejčastěji používaný je tzv. součtový algoritmus. Využívá se vztahu:

Hodnota aktiva (A) = (Dostupnost + Důvěrnost + Integrita) /3. (1)

3.6 Analýza rizik

Analýza rizik je nutná k identifikaci zranitelných míst. Následně zachycuje seznam hrozeb působících na organizaci a stanovuje rizika příslušná každému zranitelnému místu a hrozbě. Účelem výsledného dokumentu je snížení rizik na přijatelnou úroveň a akceptaci zbytkových rizik tam, kde je jejich minimalizace neefektivní. (1)

Normy týkající se analýzy rizik:

- Metodika hodnocení rizik - ISO/IEC 27001:2014 -4.2.1 c
- Zprávy o hodnocení rizik - ISO/IEC 27001:2014 -4.2.1 d-g

3.6.1 Metodiky analýzy rizik

Metodiky analýzy rizik se rozdělují na:

- Analýza rizik - hrubá úroveň

  - bere v úvahu hodnotu systému IT pro činnost organizace a zpracování informací a rizika z pohledu činnosti organizace.
- Analýza rizik - neformální přístup

  - využívá se znalosti a zkušenosti jednotlivců
  - je časově nenáročná, má vysoké riziko opomenutí důležitých detailů
- Analýza rizik - kombinovaný přístup

  - provede se počáteční analýza rizik na hrubé úrovni
  - IT systémy, které jsou označeny jako kritické pro chod organizace nebo jsou vystaveny vysokým rizikům, se přednostně provede detailní analýza
- Analýza rizik - podrobný přístup

  - obsahuje hloubkovou revizi v každém z těchto kroků: stanovení hranic revize, identifikace aktiv, ohodnocení aktiv, hodnocení hrozeb, odhad zranitelnosti, identifikace plánovaných a existujících ochranných kroků

Doporučuje se použít kombinace neformální a detailní analýzy rizik. Nejčastější průběh analýz je popsán v ČSN ISO/IEC 27005.

Analýza rizik na hrubé úrovni bere v úvahu hodnotu systému IT pro činnost organizace a zpracování informací a rizika z pohledu činnosti organizace. (1)

3.6.2 Řízení rizik

Cílem řízení rizik je identifikace a kvantifikace rizik, která organizaci hrozí a následné rozhodnutí o jejich zvládnutí. Jednou z nejčastěji používaných metod je snížení rizika.

Řízení rizik je komplexní proces, který se skládá ze čtyř po sobě jdoucích fází, které tvoří smyčku.

Obrázek 4: Fáze řízení rizik (12)

Stanovení kontextu

Tato fáze vymezuje oblasti řízení rizik, popisuje proces řízení rizik a definuje role a odpovědnosti v rámci procesu, vybírá metodiku pro analýzu rizik, stanovuje referenční úrovně, kritéria a způsoby hodnocení a zvládání rizik.

Analýza rizik

V této fázi dochází k identifikaci a kvantifikaci aktiv, hrozeb a zranitelností. Dále se stanovují míry rizika.

Vyhodnocení rizik

Zde dochází k prioritizaci rizik a výběru optimálních opatření ke snížení rizika. Je považována za kritickou fázi procesu řízení.

Zvládání rizik

V této fázi se rozhoduje o vhodném způsobu zvládání rizik.

Možnosti jsou např.:

- Retence
- Redukce
- Transfer
- Pojištění
- Sdílení
- Vyhnutí se riziku

Jako součást řízení rizika bývá chápáno:

- šíření informací o riziku
- vnímání rizika
- akceptování rizika (1)

3.7 Opatření

Cílem je stanovit úroveň základní ochrany, která by definovala minimální sadu bezpečnostních opatření k ochraně všech nebo některých IT systémů. Základní rozlišení bezpečnostních opatření je:

- preventivní
- detekce a reakce
- podpůrná

3.7.1 Výběr opatření

Výběr opatření se podle přílohy A normy ČSN ISO/IEC 27001:2014 dělí na:

- Opatření související s organizací
  - A.5 Politiky bezpečnosti informací
  - A.6 Organizace bezpečnosti informací
  - A.8 management aktiv

- A.15 Vztahy s dodavateli

- nesouvisející s ICT
  - A.7 Bezpečnost lidských zdrojů
  - A.11 Fyzická bezpečnost a bezpečnost prostředí
- související s ICT
  - A.9 Řízení přístupu
  - A.10 Kryptografie
  - A.12 Bezpečnost provozu
  - A.13 Bezpečnost komunikací
  - A.14 Akvizice, vývoj a údržba systémů
- související s podporou ISMS
  - A.16 Management incidentů bezpečnosti informací
  - A.17 Aspekty bezpečnosti informací managementu kontinuity
  - A.18 Soulad s požadavky (6)

3.8 Síťová bezpečnost

Tento pojem označuje soubor norem obsahující doporučení pro implementaci opatření, která se vztahují k bezpečnosti sítí.

3.8.1 Referenční model ISO/OSI

Tento model, známý pod zkratkou OSI (Open Systems Interconnection), je nejčastěji používaný k popisu síťových technologií a zařízení. Je důležitý zejména pro výrobce síťových komponent, umožňuje pochopit principy práce síťových prvků a patří k základům terminologií sítí. Organizace International Standards Organization (ISO) jej definovala v roce 1983 a rok později byl přijat za mezinárodní normu ISO 7498. Rozděluje síťovou komunikaci do sedmi různých vrstev a zavádí používání těchto vrstev v procesu výměny dat. (13)

Princip spočívá v tom, že vyšší vrstva převezme úkol od podřízené vrstvy, zpracuje jej a předá vrstvě nadřízené. Model ISO/OSI doporučuje, jak mají vrstvy spolupracovat horizontálně. (14)

Tabulka 2: ISO/OSI Model (14)

	Jednotka dat	Vrstva	Funkce
Host layers	Data	7. Aplikační	Určitá aplikace zpřístupňující uživatelům síťové služby. Např. vzdálený přístup k tiskárnám, sdílení souborů,správa sítě...
		6. Prezentační	Vrstva zabezpečuje konverzi dat. Zajišťuje sjednocení formy vzájemně přenášených údajů. Vrstva data komprimuje, popř. šifruje. V praxi často splývá s relační vrstvou.
		5. Relační	Navazuje a po skončení přenosu ukončuje spojení. Může také provádět ověřování uživatelů a zabezpečení přístupu k zařízením.
	Segmenty	4. Transportní	Vrstva dělí přenášené zprávy na packety a přijaté packety skládá do zpráv.
	Packet/Datagram	3. Síťová	Je zodpovědná za spojení a směrováni mezi dvěma počítači, zajišťuje volbu trasy při spojení.
Media layers	Rámec	2. Linková	Uskutečňuje přenos údajů po fyzickém médiu, pracuje s fyzickými adresami síťových karet, odesílá a přijímá rámce…
	Bit	1. Fyzická	Popisuje elektrické (či optické), mechanické a funkční vlastnosti: jakým signálem je reprezentována logická jednička, jak přijímací stanice pozná začátek bitu, k čemu je který vodič v kabelu použit...

ISO/OSI model dává přehled o tom, co vše je třeba zajistit pro úspěšnou komunikaci v síti. Už první tři vrstvy bezprostředně zajišťují komunikaci. Část z nich je integrovaná do elektroniky síťové karty. Ale výběr trasy, kontrola správnosti packetů nebo kudy má packet projít, musí provádět další prvky vložené do kabeláže. Tyto prvky se nazývají aktivní, protože aktivně ovlivňují dění v síti. Pasivní prvky, např. kabely se na přenosu dat aktivně nepodílejí. Společně se tak první čtyři vrstvy starají o přenos dat v síti. Zbývající vrstvy jsou pak zaměřeny na potřeby síťových aplikací, které využívají přenosové možnosti transportní vrstvy. (13)

3.8.2 Management bezpečnosti fyzické vrstvy

Opatření na úrovni fyzické vrstvy se dělí do tří kategorií.

Stupeň bezpečnosti 0 - identifikace

Tento stupeň neposkytuje žádnou fyzickou ochranu, pouze ulehčuje orientaci správce. (15)

Obrázek 5: Barevné odlišení kabeláže (15)

Stupeň bezpečnosti 1 - blokace

Tento stupeň používá fyzické blokování portů a blokování přístupů do kabelových tras a datových boxů. (15)

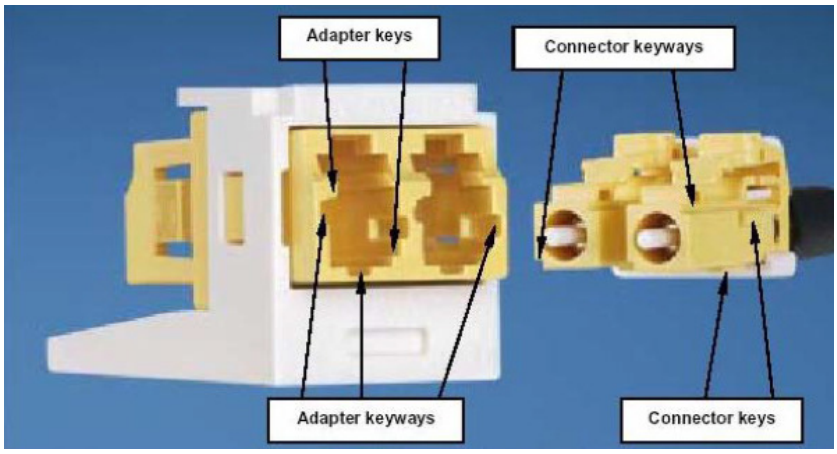
Obrázek 6: Datová zásuvka s omezenou přístupností portů (15)

Obrázek 7: Prvek sloužící k blokování portu RJ45 (15)

Stupeň bezpečnosti 2 - klíčování

Jedná se o klíčované koncovky kabeláže a klíčované porty datových zásuvek. Klíčování funguje na principu:

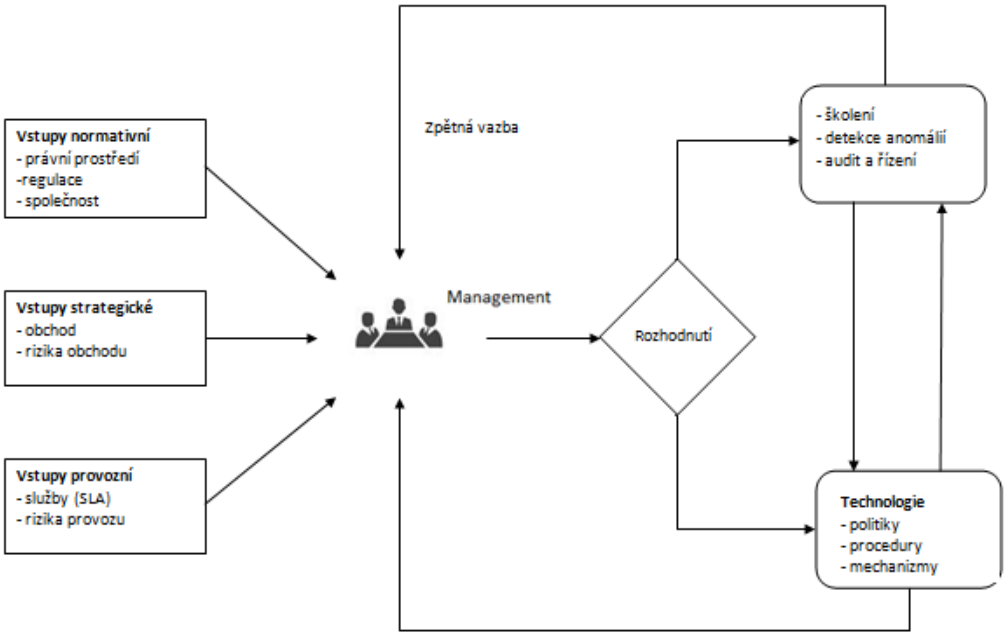
- neklíčovaný plug nelze zasunout do žádného klíčovaného jacku
- klíčovaný plug nelze zasunout do žádného neklíčovaného jacku ani do jacku s jiným klíčováním
- princip platí i pro FO LC Duplex adaptery a LC konektory (15)



Obrázek 8: Klíčované řešení v LC adapterech a konektorech (15)

3.9 Systém řízení informační bezpečnosti (ISMS)

ISMS je zkratka tvořená prvními písmeny anglických slov Information Security Management System, tedy v překlady Systém řízení informační bezpečnosti. Jedná se tedy a řízení informační bezpečnosti se všemi aspekty, které to přináší. V podniku, kde je ISMS naimplementováno, se stává součástí celkového řízení organizace.

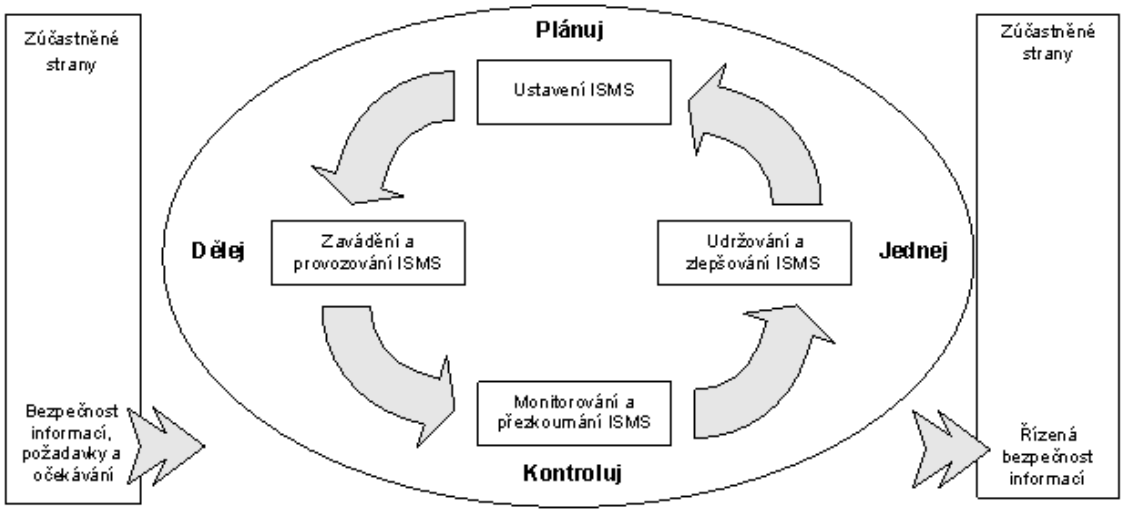


Obrázek 9: Struktura ISMS (1)

3.9.1 Požadavky

ISMS je založen na principu Demingova modelu postupného zlepšování kvality a má 4 etapy:

- **Ustavení ISMS (Plánuj):** Vytvoření politiky ISMS, definice cílů, procesů a postupů, které souvisí s řízením rizik a zlepšováním vlastní ochrany informací takovým způsobem, aby byly splněny cíle stanovené ve vytvořené politice ISMS a to v souladu s cíli organizace. (1)
- **Zavádění a provoz ISMS (Dělej):** Zavedení a provedení stanovené podnikové politiky ISMS, postupy, opatření a procesy soužící ke splnění cílů. (1)
- **Monitorování a přezkoumání ISMS (Kontroluj):** Posouzení a měření výkonu vzhledem k politice ISMS, definovaným cílům a praktickým zkušenostem s pravidelným hlášením výsledků vedení podniku. Toto hlášení slouží k přezkoumání postupu plnění ISMS. (1)
- **Údržba a zlepšování (Jednej):** Přijmutí nezbytných opatření k nápravě identifikovaných problémů a vytváření preventivních opatření, která jsou založena na výsledcích interního podnikového auditu ISMS. (1)



Obrázek 10: Demingův model aplikovaný na ISMS (6)

Základní požadavek je zavedení všech etap uvedených výše. Tyto činnosti musí být dokonale dokumentovány a to v kontextu všech činností a identifikovaných rizik.

Procesy ISMS musí být navrhovány takovým způsobem, aby byla zajištěna přiměřená ochrana, jejímž cílem je chránit informační aktiva podniku. Současně musí tyto opatření poskytovat odpovídající jistotu i dalším zúčastněným stranám. (1)

3.10 Požadavky na dokumentaci

Dokumentace musí obsahovat evidenci o rozhodnutích učiněných vedením organizace a to tak, aby byly všechny činnosti zpětně identifikovatelné při auditech a aby se zajistila jejich opakovatelnost. (1)

Doporučené dokumenty:

- Rozsah a hranice ISMS

  Popisuje dotčené části systému určené k implementaci ISMS, popř. vyjmutí některých částí z ISMS.
- Politika ISMS

  Stručný základní dokument, kterým vedení společnosti deklaruje plnou připravenost a odpovědnost k prosazení cílů při zavádění ISMS. Management se zavazuje, že uvolní potřebné personální a ekonomické zdroje.
- Definice přístupu k hodnocení rizik

  Definice systematického přístupu k hodnocení rizik. Stanovuje, jaká metodika bude použita při hodnocení rizik. Akceptuje normativní a legislativní požadavky.
- Identifikace a ohodnocení aktiv

  Popisuje aktiva vlastněná organizací, jejich majitele, definuje aktiva určená k ohodnocení a identifikaci.
- Analýza rizik

  Popisuje princip analýzy rizik, aktiva, rizika a výsledky analýzy.
- Návrh opatření

  Popisuje způsob minimalizace zjištěných rizik a obsahuje konkrétní návrhy nebo návrhy v obecné rovině. Dále definuje akceptovaná rizika.
- Cíle opatření a bezpečnostní opatření pro zvládání rizik

Popisuje implementaci vhodných opatření dle přílohy A normy ČSN ISO/IEC 27001 a jednotlivá bezpečnostní opatření.

- Akceptace rizik

  Obsahuje stručně formulovaná akceptovaná rizika.

- Získání povolení k provozování ISMS v rámci organizace

  V tomto dokumentu vedení organizace deklaruje svoji vůli k ustanovení, zavedení, monitorování, přezkoumání, udržování a zlepšování ISMS.

Seznam povinných kapitol:

- Zajištění stanovených cílů ISMS a plánů jejich dosažení
- Stanovení role, povinnosti a odpovědnosti v oblasti bezpečnosti informací
- Propagace (v rámci organizace) významu plnění cílů bezpečnosti informací, jejich soulad s politikou bezpečnosti informací, plnění povinností vyplývajících ze zákona a potřebu soustavného zlepšování
- Zajištění dostatečných zdrojů pro ustanovení, zavedení, provoz, monitorování, přezkoumání, údržbu a zlepšování ISMS
- Stanovení akceptovatelné úrovně rizika
- Zajištění provádění interních auditů ISMS
- Provádění přezkoumání ISMS

- Prohlášení o aplikovatelnosti

  Prohlášení popisující cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS.

  Povinně obsahuje následující kapitoly:

  - Cíle opatření a jednotlivá bezpečnostní opatření vybrané a důvody pro jejich výběr
  - Cíle opatření a jednotlivá bezpečnostní opatření, která jsou již v organizaci implementována

- Vyřazené cíle opatření a jednotlivá vyřazená bezpečnostní opatření uvedená v příloze A, včetně zdůvodnění pro jejich vyřazení (1)

4 Požadavky investora

Majitel firmy klade na zavedení ISMS následující požadavky:

- Celková doba implementace nepřesáhne 2 roky.
- Bude rozdělena na 4 fáze z důvodu možnosti časově oddálit zavádění jednotlivých fází z finančních nebo provozních důvodů.
- Náklady na první dvě fáze nepřesáhnou 500 000 Kč včetně práce zaměstnanců. Rozpočet na další fáze bude stanoven až po zavedení prvních dvou a to dle aktuální ekonomické situace podniku.
- Majitel podniku bude do aktivit zahrnut v nejmenší možné míře. Za vše bude zodpovědný bezpečnostní technik, který ho bude o aktuálním stavu a požadavcích informovat na pravidelních dvoutýdenních schůzkách.
- Konečným výstupem implementace bude audit a certifikát ISO/IEC 27001.

5 Analýza současného stavu

5.1 Identifikace společnosti

Z důvodu možnosti zneužití dat uvedených v diplomové práci si společnost nepřeje být jmenována. Dále bude uváděna jako Xyz s.r.o.

5.2 Profil společnosti

Jedná se o stavební společnost se specializací na kanalizace a pokládku živičných povrchů.

5.3 Řídící orgány společnosti

- organizační struktura firmy vychází z potřeb a přání zákazníků,
- v čele stojí ředitel společnosti, který spolu se čtyřmi odbornými řediteli tvoří řídící tým,
- kvalita a rychlost stavebních prací, zejména v inženýrské výstavbě, je založena na dlouholetých zkušenostech pracovníků firmy ve všech úrovních.

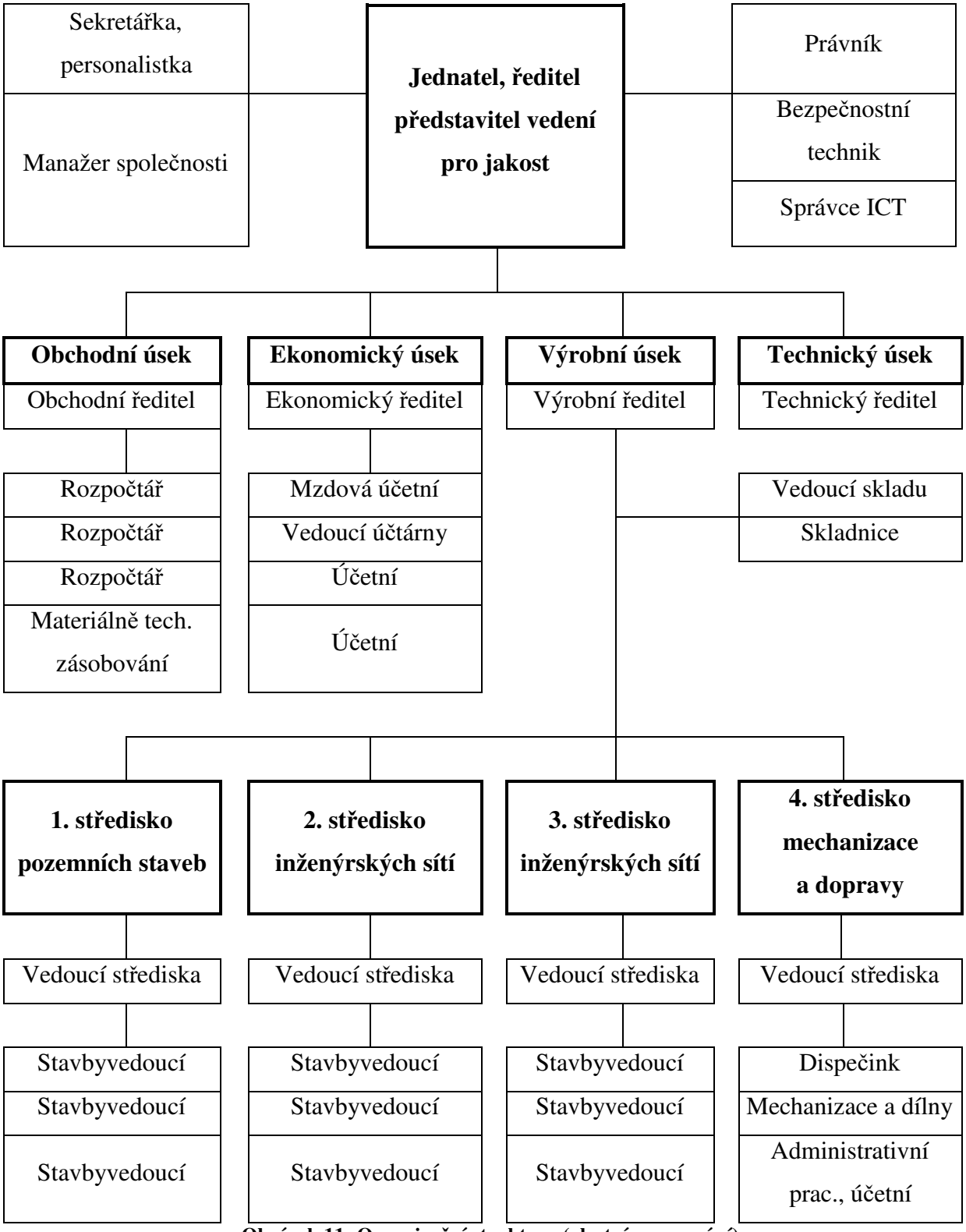
Profesní členění pracovníků je zcela přizpůsobeno výrobnímu programu společnosti. Kromě mechanizace a dopravy jde především o zedníky, tesaře, dlaždiče, montéry kanalizačního a vodovodního potrubí a pracovníky pokládky živičných směsí.

5.4 Skladba pracovníků v roce 2016

Pracovníci celkem:	**189**
– THP	23
– mechanizace, doprava	45
– dělníci základní stavební výroby	121

5.5 Organizační uspořádání společnosti

Organizační uspořádání společnosti je uvedeno v následující tabulce:



Obrázek 11: Organizační struktura (vlastní zpracování)

5.6 ICT infrastruktura

Společnost využívá 2 budovy od sebe vzdálené cca 12 metrů. Sítě obou budov jsou spojeny optickým kabelem, který je ukryt u tunelu propojujícím budovu administrativní s budovou dopravy a mechanizace.

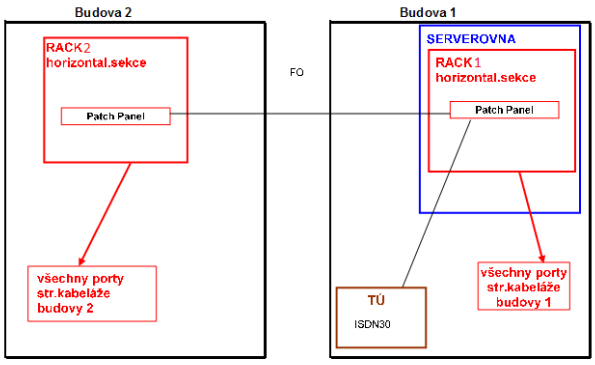
LAN síť byla v administrativní budově zřízena již při stavbě a je tudíž do ní přímo zakomponovaná. V místnostech jsou kabely rozvedeny převážně parapetními kanály a dále kabelovými žlaby umístěnými v podhledech. Instalační šachtou jsou pak kabely svedeny do serverovny, která je umístěna v prvním podzemním podlaží. Datové zásuvky jsou neklíčované, volně přístupné a to i na chodbách. Serverovna je uzamčena a přístupná pouze proškoleným pracovníkům s patřičnými znalostmi, dále jsou záložní klíče uzamčeny v trezoru na klíče na recepci budovy.

V budově dopravy a mechanizace byla LAN síť zřízena před třemi lety, kdy nahradila podomácku vytvořenou síť skládající se pouze z routeru a několika připojených počítačů, převážně sloužících k soukromým účelům. Nyní má budova vlastní datový rozvaděč a je zbudována dle platných norem. Rozvody UTP kabelů jsou opět realizované převážně parapetními kanály. Datový rozvaděč je umístěn v prvním nadzemním podlaží při ústí tunelu.

Obě budovy jsou vybaveny taktéž WIFI routery. Jsou zde zřízeny 2 sítě pomocí technologie VLAN a zaměstnanců a hostům jsou viditelné s rozlišným SSID. Síť určená zaměstnancům je zabezpečená a pro připojení do ní je nezbytné získat certifikát od správce sítě. Tato síť je připojena do intranetu a umožňuje připojení na firemní server. Síť určená hostům není zabezpečena a umožňuje pouze přístup na internet a to omezenou rychlostí.

K lokální síti se lze také připojit i přes VPN tunel. Tuto možnost využívají převážně developeři účetního programu.

Připojení k externím sítím je realizováno optickým kabelem o rychlosti 100/40Mbit, dále je zde ADSL připojení 20/2Mbit jako záložní řešení v případě výpadku.



Obrázek 12: Logické schéma počítačové sítě budov (vlastní zpracování)

Budovy jsou dále vybaveny systémem na bázi RFID. Tento systém je využíván k vytváření docházky jednotlivých zaměstnanců, která slouží jako podklad pro mzdové oddělení. V administrativní budově je využití rozšířeno na řízení přístupů do jednotlivých pater a to jak výtahem, tak po schodech.

5.6.1 Server

Rack v serverovně je, kromě síťových prvků, osazen serverem Lenovo System x3250 M5. Jedná se o 1U server s procesorem Intel Xeon E3-1241 v3, 4GB DDR3 UDIMM. Externí diskové pole je osazeno čtyřmi 2TB disky v konfiguraci RAID10. Využité místo na discích se neustále pohybuje kolem 95% celkové kapacity.

5.6.2 Osobní počítače

Jedná se především o novější modely stolních počítačů a notebooků různých značek a parametrů. Počítače jsou nakupovány postupně dle potřeby, takže zde není mnoho modelů zastoupeno vícekrát.

Hardware

Notebooky jsou ve většině případů vybaveny procesorem Intel Core i5 o taktu 2,5 GHz, 4-8 GB RAM a 300GB HDD.

Pracovní stanice jsou nejčastěji osazeny procesorem Intel Core i3 o taktu 3,3 GHz, 4GB RAM, 500GB HDD. Starší stanice pak mají konfiguraci: Intel Celeron Core 2,2 GHz, 2GB RAM, 120 GB HDD. Ty jsou však postupně nahrazovány a vyřazené stanice jsou přesouvány na třetí patro budovy dopravy a mechanizace, kde se nachází pokoje pro přespání mimobrněnských sezónních pracovníků. Ti využívají vyřazené počítače k soukromým účelům.

Jako příslušenství jsou pak 17 palcové LCD monitory, které mají rozlišení 1280x1024.

Software

Téměř všechny notebooky mají Windows 7 nebo 8, pracovní stanice pak Windows 7. Počítače jsou chráněny softwarem AVG Internet Security. Společnost využívá účetní program, který byl navržený na zakázku. Na tvorbu rozpočtů, kalkulaci stavebních prací a sledování stavebních zakázek se využívá Kros od společnosti ÚRS Praha a.s. a BUILDpower od společnosti RTS.

5.7 Bezpečnostní situace

Podnik Xyz s. r. o. sídlí v odlehlé části Brna, kde okolí tvoří především odstavné koleje Hlavního nádraží Brno a plochy, které sousedící podniky využívají jako parkoviště pro technická vozidla a jako skládky hlíny a štěrku.

Parkovací plochy pro zaměstnance jsou přímo před administrativní budovou.

5.7.1 Fyzická bezpečnost

Při vjezdu do areálu je potřeba projet vrátnicí opatřenou závorou. Ovládána je z prostoru vrátnice. Hlídač, který je zde v pracovní dny od 6:00 do 20:00, dohlíží na průjezd nákladních vozů a zapisuje do informačního systému jejich SPZ a množství a druh materiálu, který převáží. Dále kontroluje pohyb osob do venkovního areálu a do budovy dopravy a mechanizace.

Dále v areálu se pak nachází skládka štěrků a dalších stavebních materiálů a parkoviště pro technická vozidla.

Administrativní budova má jedno podzemní a 6 nadzemních podlaží. Firma Zyx s. r. o. využívá pouze 1. podzemní, 1., 5. a 6. nadzemní podlaží. Ostatní podlaží společnost pronajímá. Do budovy se vchází z parkoviště. Vchodové dveře jsou skleněné, automaticky otvírané, pokud je na recepci přítomná recepční. V případě její nepřítomnosti si zaměstnanci mohou otevřít svou osobní čipovou kartou. Čtečka je umístěna na vnějších vchodových dveřích. V prostoru mezi vchodovými dveřmi se nachází čtečka karet sloužící k evidenci docházky. Zde mají zaměstnanci možnost si při opouštění areálu vybrat důvod odchodu. Např. lékař, dovolená, osobní důvody atd. Za

vchodem se nachází recepce. Recepční je přítomna v pracovní dny od 7:30 do 16:30. V případě návštěvy recepční ověří telefonátem s dotyčným zaměstnancem, zda osoba může získat přístup do areálu. Zapíše návštěvu do IS a vydá návštěvě čipovou kartu, která umožní přístup pouze do daného patra. Kartu je nutno použít buď ve výtahu, nebo u schodišťových dveří v jednotlivých patrech. Celý prostor vstupu do budovy a recepce je monitorovaný množstvím kamer. Záznam sleduje vrátný, popř. hlídací služba a je dlouhodobě uchovávaný. Kanceláře v 5. a 6. nadzemním podlaží jsou v nepřítomnosti zaměstnanců uzamčené a každý zaměstnanec má přístup pouze do své kanceláře. Výjimku tvoří pouze majitel podniku a uklízecí služba, kteří mají univerzální klíč. Dále se 2 kopie tohoto klíče nachází v trezoru na recepci a jeden klíč má také hlídací služba.

Budova dopravy a mechanizace je přes den volně přístupná všem zaměstnancům a není zabezpečena žádným opatřením bránícím vstupu neoprávněných osob. Za vstupem se nachází čtečka karet, ta však slouží pouze k zaznamenávání pracovní doby zaměstnanců. Budova má tři nadzemní podlaží. Většina prostor slouží jako výrobní haly a sklady. V třetím nadzemním podlaží jsou však prostory, které slouží k ubytování sezónních zaměstnanců se vzdáleným místem pobytu.

V nočních hodinách, o víkendech a ve dnech pracovního klidu slouží vrátnice jako stanoviště hlídací služby a je opatřena množstvím monitorů, pomocí kterých lze sledovat dění po celém areálu podniku. Po odchodu posledního zaměstnance z jednotlivých budov dochází k aktivaci alarmu v dané budově. Hlídací služba provádí obhlídky areálu a budov v intervalech danými vnitřním předpisem. V areálu se taktéž nachází hlídací pes.

5.7.2 Bezpečnost informací

V podniku pochází k šíření informací všemi dostupným způsoby. Verbálně, telefonicky, přes IS, elektronickou i klasickou poštou atd. Vzhledem k vyššímu věkovému průměru zaměstnanců, se upřednostňuj neelektronická komunikace a osobní kontakt. Velké množství informací je uchováváno v tisknuté verzi. Vytisknuté dokumenty lze pak ve zvýšeném množství nalézt na všech pracovních stolech a každá kancelář má mnoho skříní na uchovávání vytištěných materiálů. Tyto skříňky mají zámky s universálním klíčem, ale až na výjimky zůstávají odemčené.

Všichni zaměstnanci managementu mají podepsaný dodatek ke smlouvě, obsahující podmínku jejich mlčenlivosti. Fragmentace přístupu k obchodním

informacím a know-how podniku je zavedena, každý zaměstnanec má přístup pouze k informacím, které potřebuje k výkonu svého zaměstnání. Vlivem neformální atmosféry v podniku, však mohou být tyto požadované informace lehko získány.

5.7.3 Síťová bezpečnost

Serverovna se nachází v podzemním podlaží administrativní budovy a je k ní omezen přístup pouze proškoleným zaměstnancům, kteří mají ICT v podniku na starost. V serverovně se také nachází telefonická ústředna. Serverovna je chlazena klimatizační jednotkou s výměníkem v místnosti stropu, umístěným nad rackem serveru. Všechny síťové kabely jsou označeny a kabelové trasy a jejich schéma je dostupné jak v elektronické, tak tištěné verzi, umístěné v pořadači na stěně serverovny.

V racku serveru se také nachází zálohovací server a záložní napájení těchto serverů.

5.7.4 Aplikační bezpečnost

Pracovní stanice jsou chráněny hesly na lokálních účtech, není zde však nastaven interval pro změnu hesla. Zaměstnanci tak mají stejné heslo i několik let. Během prohlídky ve firmě jsem našel i několik lístečků s heslem nalepených na monitorech a počítače, které nebyly po opuštění pracovního místa odhlášeny.

Počítače jsou chráněny antivirovým programem AVG Internet Security, který má nastavený pravidelné týdenní testy s heuristickou analýzou a denní automatickou aktualizaci. Zaměstnanci mohou instalovat jakýkoli software a navštěvovat všechny internetové stránky bez omezení.

Připojení z externích lokací je pomocí zabezpečeného VPN tunelu, ke kterému je nutno se přihlásit pomocí uživatelského účtu a heslo, které má exspiraci nastavenou na tři měsíce. Dále je pak přístup k datům uloženým na serveru bez omezení.

Přístup do informačního systému je omezen pouze na ověřené uživatele, kteří se musí prokázat platným heslem. Tito uživatelé pak mají přístup pouze do modulů, které jsou potřebné pro jejich práci.

5.8 Zhodnocení současného stavu

Řízení bezpečnosti v tomto podniku téměř neexistuje. Hrozí zde únik informací a to jak elektronickou cestou, tak i při vniknutí neoprávněné osoby do objektu. Vypracovány nejsou ani postupy pro zvládání bezpečnostních incidentů, což může dopad úniku informací ještě zhoršit, pokud se na něj vůbec nepřijde.

V dalších kapitolách této práce se zaměřím na analýzu rizik a popíši návrhy opravných opatření, se zaměřením na ošetření smluvních vztahů s externími subjekty.

6 Vlastní návrhy řešení

6.1 Analýza rizik

V této kapitole se věnuji analýze rizik, jak je popsána v ISMS. Tato analýza je dále použita k výběru nápravných opatření, která dané riziko snižuje, popř. eliminuje úplně a to vždy v závislosti na ceně a náročnosti vypracování opatření a hodnotě chráněného aktiva.

Metodika analýzy rizik vychází z normy ISO/IEC 27005:2011.

6.1.1 Hodnocení dopadu

Pro stanovení hodnoty aktiv musí být vytvořeno klasifikační schéma, které jednoznačně určuje náklady v důsledku porušení integrity, důvěrnosti a dostupnosti.

Tabulka 3: Klasifikační schéma pro hodnocení aktiv (vlastní zprac.dle (1))

Hodnota aktiva	**Dopad**
4 Velmi vysoká	**Dopad na aktivum je velmi vážný** - negativní publicita - ztráta důvěry obchodních partnerů - finanční postih nad 5 000 000 Kč - vážná zranění, ohrožení života
3 Vysoká	**Dopad na aktivum je vážný** - interní negativní vliv na organizační celky, projevující v poskytovaných službách - finanční postih nad 500 000 Kč - újma na zdraví způsobena jedné nebo více osobám
2 Střední	**Dopad na aktivum je malý** - finanční postih do 100 000 Kč - interní negativní vliv na organizační celky, neprojevující se navenek

1 Nízká	**Dopad na aktivum je zanedbatelný** - neporušené právní normy - náklady na nápravy nepřesáhnou 50 000 Kč - žádný dopad na okolí podniku
1 Velmi nízká	**Žádný dopad na organizaci**

6.1.2 Identifikace aktiv

V podniku je možné identifikovat aktiva dle Tabulky 4. Klasifikační kritéria pro zařazení do jednotlivých klasifikačních stupňů jsem navrhl pro daný podnik s respektováním jejich podmínek.

Tabulka 4: Seznam identifikovaných aktiv (vlastní zpracování)

Druh aktiv	Aktivum	Hodnota aktiva
Data	Firemní účetnictví	5
	Zdrojové kódy účetního systému	2
	Výrobní postupy	3
	Databáze klientů	4
	Rozpočty, kalkulace	4
	Zálohovaná data	3
Software	VPN server	3
	Účetní SW Faust	3
	Rozpočtový SW	2
Hardware	Server	4
	Zálohovací server	3
	Síťová infrastruktura	3
	Pracovní stanice	2
Budovy	Administrativní budova	5
	Budova dopravy a mechanizace	4
Stroje	Vozidla	2
	Výrobní stroje	4

6.1.3 Definice úrovně hrozeb

Tabulka 5: Klasifikační schéma pro určení úrovně hrozby (vlastní zpracování)

Pravděpodobnost scénáře incidentu	Hodnocení úrovně hrozby
5 - Velmi vysoká (VV)	○ Téměř jistě dojde k vážnému dopadu na činnost podniku nebo oddělení. ○ Riziko se musí řešit s nejvyšší prioritou
4 - Vysoká (V)	○ Je velmi pravděpodobné, že dojde k vážnému dopadu na činnost podniku nebo oddělení. ○ Riziko se musí řešit s vysokou prioritou
3 - Střední (S)	○ Může dojít k dopadu na činnost podniku nebo oddělení. ○ Riziko musí být řešeno.
2 - Nízká (N)	○ Může dojít s nízkou pravděpodobností k zanedbatelnému dopadu na podnik či oddělení. ○ Akceptovatelné riziko.
1 - Velmi nízká (VN)	○ Může dojít s velmi malou pravděpodobností k zanedbatelnému dopadu na podnik či oddělení. ○ Akceptovatelné riziko.

6.1.4 Uvažované hrozby

Seznam typických hrozeb lze nalézt v příloze C normy ISO/IEC 27005:2011. V tabulce níže jsou mnou uvažované hrozby. Ty jsou vybrány po konzultaci s firemními pracovníky. Důležitý je také původ těchto hrozeb. Ten může být nahodilý (A - accidental), přírodní (E - enviromental) anebo úmyslné (D - deliberate).

Tabulka 6: Uvažované hrozby (vlastní zpracování)

Hrozba	Pravděpodobnost jevu	Původ
Fyzické poškození		
Požár	N	A, E, D
Poškození vodou	N	A, E, D
Znečištění	N	A,D,E
Závažná nehoda	N	A,D,E
Zničení zařízení nebo médií	N	A,D,E
Přírodní události		
Meteorologický jev	VN	E
Ztráta služeb		
Selhání klimatizace	N	A,D
Přerušení dodávky elektřiny	VN	A,D,E
Výpadek telefonického připojení	N	A,D,E
Výpadek internetového připojení	S	A,D,E
Výpadek SW Faust	N	A,D
Výpadek serveru	N	A,D
Ohrožení informací		
Neoprávněné získání informací	N	D
Neoprávněné získání přístupových údajů	N	D
Škodlivý software	VV	A,D
Neoprávněný přístup do účetního systému	N	D
Krádež médií nebo dokumentů	S	D
Krádež technického vybavení	N	D
Technická selhání		
Selhání pracovní stanice	S	A, D
Selhání serveru	S	A, D
Selhání zálohovacího serveru	N	A, D
Neoprávněné činnosti		
Neoprávněné použití zařízení	V	D
Zneužití přístupových práv	N	D
Hrozba	**Pravděpodobnost jevu**	**Původ**

Záměrné poškození dat	N	D
Neoprávněný přístup do budovy	S	D
Porušení závazku mlčenlivosti zaměstnance	VN	A, D
Lidské selhání		
Nedostatečná dokumentace	S	A, D
Chyba údržby	N	A, D
Ohrožení funkčnosti		
Chyba v používání	S	A

6.1.5 Výpočet míry rizika

Pravděpodobnost scénáře incidentu je dána hrozbou využívající zranitelnost s určitou pravděpodobností. Tabulka níže propojuje tuto pravděpodobnost s dopadem vztahující se ke scénáři incidentu. Výsledná míra rizika se měří na stupnici 0-8 a jeho hodnota je klíčová při zavádění opatření nutných k odstranění hrozeb a rizik.

Tabulka 7: Přehled míry rizika (vlastní zpracování)

		Pravděpodobnost scénáře incidentu				
		VV	V	S	N	VN
Dopad	5	8	7	6	5	4
	4	7	6	5	4	3
	3	6	5	4	3	2
	2	5	4	3	2	1
	1	4	3	2	1	0

6.1.6 Matice zranitelnosti

Matice zranitelnosti se vytváří spojením tabulky ohodnocení aktiv a tabulky hrozeb a zranitelností. Dále je třeba posoudit zranitelnost jednotlivých aktiv a doplnit ji do tabulky.

Tabulka 8: Matice zranitelnosti (vlastní zpracování)

V Zranitelnost	Popis aktiva	Firemní účetnictví	Zdrojové kódy účetního systému	Výrobní postupy	Databáze klientů	Rozpočty, kalkulace	Zálohovaná data	VPN server	Účetní SW Faust	Rozpočtový SW	Server	Zálohovací server	Síťová infrastruktura	Pracovní stanice	Administrativní budova	Budova dopravy a mechanizace	Vozidla	Výrobní stroje
	A Hodnota aktiva	5	2	3	4	4	3	3	3	2	4	3	3	2	5	4	2	4
Popis hrozby	**T** Pravděpodobnost																	
Fyzické poškození																		
Požár	2	3		2	3	3	2				3	3	3	4	4	4	1	4
Poškození vodou	2			2		1	2				2	2	2		2	2	1	3
Znečištění	2			1							1	1	2	3				
Závažná nehoda	2	3	1	3	4	4	5				3	3	4		3	3	4	4
Přírodní události																		
Meteorologický jev	1										3	3	1		2	2	2	
Ztráta služeb																		
Selhání klimatizace	3										5	5						2
Přerušení dodávky elektřiny	1	2					2				5	5	5	5		2		2
Výpadek telefonického připojení	2	1		2														
Výpadek internetového připojení	3	2		2				3			3		2	2				
Výpadek SW Faust	2	5	1	2	4	3			5	2								
Výpadek serveru	2	5	1	3	5	5	3	5	5	4	5	2	4	3				1

Ohrožení informací																		
Krádež dokumentů	2	4		5	5	5												
Neoprávněné získání přístupových údajů	2	5	1	4	5	4	2	2	4	4	4	4	2	4	2	2		2
Škodlivý software	5	5	3	3	4	4	3	3	4	4	2	2	2	5				
Neoprávněný přístup do účetního systému	2	5	3	1	5	3			5									
Krádež technického vybavení	2	3		3	3	3	4				4	4	5	5	3	3	4	4
Technická selhání																		
Selhání pracovní stanice	3	3			2	2	1	1	3	3	2	1	3	5				1
Selhání serveru	3	5	2	4	5	5	5	5	5	2	5	3	5	3				2
Selhání zálohovacího serveru	2	2					5				3	5		1				
Neoprávněné činnosti																		
Neoprávněné použití zařízení	4	5	2	3	5	5	3	1	3	3	5	3	4	5				3
Zneužití přístupových práv	2	5	2	4	5	5	3	2	3	3	4	2	3	4				
Záměrné poškození dat	2																	
Neoprávněný přístup do budovy	3	3		5	4	4	1				2	2	3	5	3	3	4	4
Porušení závazku mlčenlivosti zaměstnance	1	3		5	5	2												
Lidské selhání																		
Nedostatečná dokumentace	3	3		4	1	1	2	3	2	2	4	1	3	2			3	3
Chyba údržby	2										1	1	2	2	2	2	3	4
Ohrožení funkčnosti																		
Chyba v používání	3	2		2	2	2	1	1	2	2	2	1	2	3	1	1	2	4

6.1.7 Matice rizik

Matice zranitelnosti se dále použije při výpočtu míry rizika. Využívá se vztah R=T*A*V, kde R = míra rizika, T = pravděpodobnost hrozby, A = hodnota aktiva a V = zranitelnost aktiva

Tabulka 9: Matice rizik (vlastní zpracování)

R Riziko	Popis aktiva	Firemní účetnictví	Zdrojové kódy účetního systému	Výrobní postupy	Databáze klientů	Rozpočty, kalkulace	Zálohovaná data	VPN server	Účetní SW Faust	Rozpočtový SW	Server	Zálohovací server	Síťová infrastruktura	Pracovní stanice	Administrativní budova	Budova dopravy a mechanizace	Vozidla	Výrobní stroje
	A Hodnota aktiva	5	2	3	4	4	3	3	3	2	4	3	3	2	5	4	2	4
Popis hrozby	**T** Pravděpodobnost																	
Fyzické poškození																		
Požár	2	30	0	12	24	24	12	0	0	0	24	18	18	16	40	32	4	32
Poškození vodou	2	0	0	12	0	8	12	0	0	0	16	12	12	0	20	16	4	24
Znečištění	2	0	0	6	0	0	0	0	0	0	8	6	12	12	0	0	0	0
Závažná nehoda	2	30	4	18	32	32	30	0	0	0	24	18	24	0	30	24	16	32
Přírodní události																		
Meteorologický jev	1	0	0	0	0	0	0	0	0	0	12	9	3	0	10	8	4	0
Ztráta služeb																		
Selhání klimatizace	3	0	0	0	0	0	0	0	0	0	60	45	0	0	0	0	0	16
Přerušení dodávky elektřiny	1	10	0	0	0	0	6	0	0	0	20	15	15	10	0	8	0	8
Výpadek telefonického připojení	2	10	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Výpadek internetového připojení	3	30	0	18	0	0	0	27	0	0	36	0	18	12	0	0	0	0
Výpadek SW Faust	2	50	4	12	32	24	0	0	30	8	0	0	0	0	0	0	0	0
Výpadek serveru	2	50	4	18	40	40	18	30	30	16	40	12	24	12	0	0	0	8

Ohrožení informací																		
Krádež dokumentů	2	40	0	30	40	40	0	0	0	0	0	0	0	0	0	0	0	0
Neoprávněné získání přístupových údajů	2	50	4	24	40	32	12	12	24	16	32	24	12	16	20	16	0	16
Škodlivý software	5	125	30	45	80	80	45	45	60	40	40	30	30	50	0	0	0	0
Neoprávněný přístup do účetního systému	2	50	12	6	40	24	0	0	30	0	0	0	0	0	0	0	0	0
Krádež technického vybavení	2	30	0	18	24	24	24	0	0	0	32	24	30	20	30	24	16	32
Technická selhání																		
Selhání pracovní stanice	3	45	0	0	24	24	9	9	27	18	24	9	27	30	0	0	0	12
Selhání serveru	3	75	12	36	60	60	45	45	45	12	60	27	45	18	0	0	0	24
Selhání zálohovacího serveru	2	20	0	0	0	0	30	0	0	0	24	30	0	4	0	0	0	0
Neoprávněné činnosti																		
Neoprávněné použití zařízení	4	100	16	36	80	80	36	12	36	24	80	36	48	40	0	0	0	48
Zneužití přístupových práv	2	50	8	24	40	40	18	12	18	12	32	12	18	16	0	0	0	0
Záměrné poškození dat	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Neoprávněný přístup do budovy	3	45	0	45	48	48	9	0	0	0	24	18	27	30	45	36	24	48
Porušení závazku mlčenlivosti zaměstnance	1	15	0	15	20	8	0	0	0	0	0	0	0	0	0	0	0	0
Lidské selhání																		
Nedostatečná dokumentace	3	45	0	36	12	12	18	27	18	12	48	9	27	12	0	0	18	36
Chyba údržby	2	0	0	0	0	0	0	0	0	0	8	6	12	8	20	16	12	32
Ohrožení funkčnosti																		
Chyba v používání	3	30	0	18	24	24	9	9	18	12	24	9	18	18	15	12	12	48

Nyní je potřeba stanovit hranice míry rizika:

Tabulka 10: Stanovené hranice rizika (1)

Stupeň rizika	Bodová hranice
Nepřijatelné riziko	60 a více
Nežádoucí riziko	30 až 59
Mírné riziko	20 až 29
Akceptovatelné riziko	10 až 19
Bezvýznamné riziko	0 až 9

Míra rizika je s ohledem na stupeň rizika barevně rozlišena v matici rizik výše.

6.1.8 Vyhodnocení rizik

Hodnoty vypočítané v matici rizik ukazují, že podnik má největší slabinu v možném selhání serveru, neoprávněném použitím zařízení a působením škodlivého softwaru. To se projevilo i při konzultacích těchto výsledků s osobou odpovědnou za ICT. Budovy jsou sice osazeny novou síťovou infrastrukturou, serverem a zálohovacím serverem, chybí zde však řešení pro případ poruchy serveru. Dlouhodobější výpadek by mohl pro podnik znamenat vážné existenční problémy. Ty mohou být způsobeny především ušlým ziskem nebo platbou smluvních sankcí.

6.2 Návrh opatření

V této kapitole se budu zabývat návrhem opatření, které je nutné zavést nebo revidovat. Tyto opatření vycházejí ze seznamu opatření, který je definován v příloze A normy ISO/IEC 27001:2014.

Na závěr této kapitoly zhodnotím navrhovaná opatření po finanční stránce. Vzhledem k tomu, že se momentálně podnik nachází v nepříznivé situaci, tak se bude návrh opatření vztahovat pouze na kritické oblasti a nezbytná opatření.

6.2.1 Soubor opatření dle přílohy A normy ISO/IEC 27001:2014

Zavádění opatření bude rozděleno do tří fází na základě velikosti rizika z předchozí kapitoly a konzultace s majitelem podniku.

Tabulka 11: Seznam opatření (Vlastní zpracování dle (6))

ID opatření	Opatření dle přílohy A normy ISO/IEC 27001	Stav
A.5	Politiky bezpečnosti informací	
A.5.1	Směřování bezpečnosti informací vedením organizace	
A.5.1.1	Politiky pro bezpečnost informací	Zavést 1. etapa
A.5.1.2	Přezkoumání politik pro bezpečnost informací	Zavést 1. etapa
A.6	Organizace bezpečnosti informací	
A.6.1	Interní organizace	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	Zavést 1. etapa
A.6.1.2	Princip oddělení povinností	Zavést 1. etapa
A.6.1.3	Kontakt s příslušnými orgány a autoritami	Zavedeno
A.6.1.4	Kontakt se zájmovými skupinami	Žádné kontakty se zájmovými skupinami
A.6.1.5	Bezpečnost informací v řízení projektů	Zavést 2. etapa
A.6.2	Mobilní zařízení a práce na dálku	
A.6.2.1	Politika mobilních zařízení	Zavést 2. etapa
A.6.2.2	Práce na dálku	Zavést 2. etapa
A.7	Bezpečnost lidských zdrojů	
A.7.1	Před vznikem pracovního vztahu	
A.7.1.1	Prověřování	Zavést 2. etapa
A.7.1.2	Podmínky pracovního vztahu	Zavést 2. etapa
A.7.2	Během pracovního vztahu	
A.7.2.1	Odpovědnost vedení organizace	Zavést 1. etapa
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	Zavést 1. etapa
A.7.2.3	Disciplinární řízení	Zavést 1. etapa
A.8	Řízení aktiv	
A.8.1	Odpovědnost za aktiva	
A.8.1.1	Seznam aktiv	Zavést 1. etapa
A.8.1.2	Vlastnictví aktiv	Zavést 1. etapa
A.8.1.3	Přípustné použití aktiv	Zavést 1. etapa
A.8.1.4	Navracení aktiv	Zavést 1. etapa
A8.2	Klasifikace informací	
A.8.2.1	Klasifikace informací	Zavést 1. etapa
A.8.2.2	Označování informací	Zavést 1. etapa
A.8.2.3	Manipulace s aktivy	Zavést 1. etapa
A.8.3	Manipulace s médii	
A.8.3.1	Správa výměnných médií	Zavést 1. etapa
A.8.3.2	Likvidace médií	Zavést 1. etapa
A.8.3.3	Přeprava fyzických médií	Zavést 1. etapa

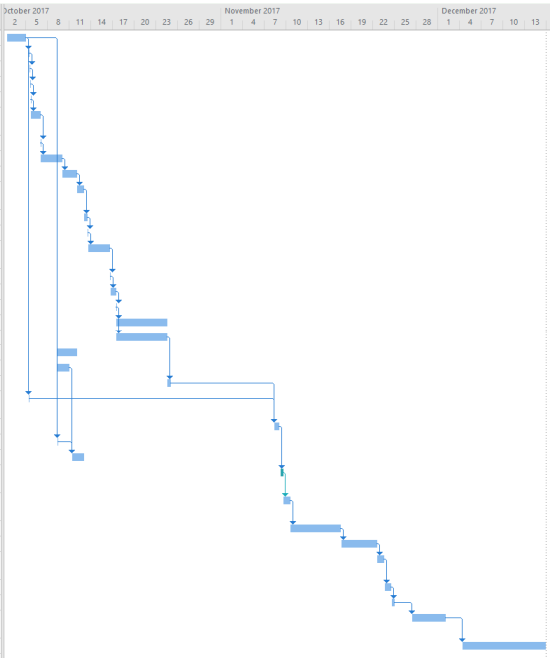
A.9	Řízení přístupu	
A9.1	Požadavky organizace na řízení přístupu	
A.9.1.1	Politika řízení přístupu	Zavést 2. etapa
A.9.1.2	Přístup k sítím a síťovým službám	Zavést 2. etapa
A.9.2	Řízení přístupu uživatelů	
A.9.2.1	Registrace a zrušení registrace uživatele	Zavést 2. etapa
A.9.2.2	Správa uživatelských přístupů	Zavést 2. etapa
A.9.2.3	Správa privilegovaných přístupových práv	Zavést 2. etapa
A.9.2.4	Správa tajných autentizačních práv	Zavést 3. etapa
A.9.2.5	Přezkoumání přístupových práv uživatelů	Zavést 2. etapa
A.9.2.6	Odebrání nebo úprava přístupových práv	Zavést 2. etapa
A.9.3	Odpovědnost uživatelů	
A.9.3.1	Používání tajných autentizačních informací	Zavést 2. etapa
A.9.4	Řízení přístupů k systémům a aplikacím	
A.9.4.1	Omezení přístupu k informacím	Zavedeno
A.9.4.2	Bezpečné postupy přihlášení	Zavedeno
A.9.4.3	Systémy správy hesel	Zavést 1. etapa
A.9.4.4	Použití privilegovaných programových nástrojů	Zavedeno
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	Zavedeno
A.10	Kryptografie	
A.10.1	Kryptografická opatření	
A.10.1.1	Politika pro použití kryptografických opatření	Zavedeno
A.10.1.2	Správa klíčů	Zavedeno
A.11	Fyzická bezpečnost a bezpečnost prostředí	
A.11.1	Bezpečné oblasti	
A.11.1.1	Fyzický bezpečnostní perimetr	Zavést 1. etapa
A.11.1.2	Fyzické kontroly vstupu	Zavedeno
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	Zavést 1. etapa
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	Zavést 3. etapa
A.11.1.5	Práce v bezpečných oblastech	Zavést 3. etapa
A.11.1.6	Oblasti pro nakládku a vykládku	Zavést 3. etapa
A.11.2	Zařízení	
A.11.2.1	Umístění zařízení a jeho ochrana	Zavést 1. etapa
A.11.2.2	Podpůrné služby	Zavést 3. etapa
A.11.2.3	Bezpečnost kabelových rozvodů	Zavedeno
A.11.2.4	Údržba zařízení	Zavést 3. etapa
A.11.2.5	Přemístění aktiv	Zavést 3. etapa
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	Zavést 3. etapa
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	Zavést 3. etapa
A.11.2.8	Uživatelská zařízení bez obsluhy	Zavést 3. etapa
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	Zavést 1. etapa
A.12	Bezpečnost provozu	
A.12.1	Provozní postupy a odpovědnost	
A.12.1.1	Dokumentované provozní postupy	Zavést 3. etapa
A.12.1.2	Řízení změn	Zavést 3. etapa

A.12.1.3	Řízení kapacit	Zavést 3. etapa
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	Zavést 3. etapa
A.12.2	Ochrana proti malwaru	
A.12.2.1	Opatření proti malware	Zavést 1. etapa
A.12.3	Zálohování	
A.12.3.1	Zálohování informací	Zavedeno
A.12.4	Zaznamenávání formou logů a monitorování	
A.12.4.1	Zaznamenávání událostí formou logů	Zavedeno
A.12.4.2	Ochrana logů	Zavedeno
A.12.4.3	Logy o činnosti administrátorů a operátorů	Zavedeno
A.12.4.4	Synchronizace hodin	Zavedeno
A.12.5	Správa provozního softwaru	
A.12.5.1	Instalace softwaru na provozní systémy	Zavést 3. etapa
A.12.6	Řízení technických zranitelností	
A.12.6.1	Řízení technických zranitelností	Zavést 3. etapa
A.12.6.2	Omezení instalace softwaru	Zavést 3. etapa
A.12.7	Hlediska auditu informačních systémů	
A.12.7.1	Opatření k auditu informačních systémů	Zavést 3. etapa
A.13	Bezpečnost komunikací	
A.13.1	Správa bezpečnosti sítě	
A.13.1.1	Opatření v sítích	Zavedeno
A.13.1.2	Bezpečnost síťových služeb	Zavedeno
A.13.1.3	Princip oddělení v sítích	Zavedeno
A.13.2	Přenos informací	
A.13.2.1	Politiky a postupy při přenosu informací	Zavést 4. etapa
A.13.2.2	Dohody o přenosu informací	Zavést 4. etapa
A.13.2.3	Elektronické zpracování zpráv	Zavést 4. etapa
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	Zavést 4. etapa
A.14	Akvizice, vývoj a údržba systémů	
A.14.1	Bezpečnostní požadavky informačních systémů	
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	Zavést 4. etapa
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	Zavést 4. etapa
A.14.1.3	Ochrana transakcí aplikačních služeb	Zavést 4. etapa
A.14.2	Bezpečnost v procesech vývoje a podpory	
A.14.2.1	Politika bezpečného vývoje	Zavést 4. etapa
A.14.2.2	Postupy řízení změn systémů	Zavést 4. etapa
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	Zavést 4. etapa
A.14.2.4	Omezení změn softwarových balíků	Zavést 4. etapa
A.14.2.5	Principy budování bezpečných systémů	Zavést 4. etapa
A.14.2.6	Prostředí bezpečného vývoje	Zavést 4. etapa
A.14.2.7	Outsourcovaný vývoj	Zavedeno
A.14.2.8	Testování bezpečnosti systémů	Zavést 4. etapa
A.14.2.9	Testování akceptace systémů	Zavést 4. etapa
A.14.3	Data pro testování	

A.14.3.1	Ochrana dat pro testování	Zavést 4. etapa
A.15	Dodavatelské vztahy	
A.15.1	Bezpečnost informací v dodavatelských vztazích	
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	Zavést 3. etapa
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	Zavést 3. etapa
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	Zavést 3. etapa
A.15.2	Řízení dodávek služeb dodavatelů	
A.15.2.1	Monitorování a přezkoumání služeb dodavatelů	Zavést 3. etapa
A.15.2.2	Řízení změn ve službách dodavatelů	Zavést 3. etapa
A.16	Řízení incidentů bezpečnosti informací	
A.16.1	Řízení incidentů bezpečnosti informací a zlepšování	
A.16.1.1	Odpovědnost a postupy	Zavést 4. etapa
A.16.1.2	Hlášení událostí bezpečnosti informací	Zavést 4. etapa
A.16.1.3	Hlášení slabých míst bezpečnosti informací	Zavést 4. etapa
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	Zavést 4. etapa
A.16.1.5	Reakce na incidenty bezpečnosti informací	Zavést 4. etapa
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	Zavést 4. etapa
A.16.1.7	Shromažďování důkazů	Zavést 4. etapa
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	Zavést 4. etapa
A.17.1.2	Implementace kontinuity bezpečnosti informací	Zavést 4. etapa
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	Zavést 4. etapa
A.17.2	Redundance	
A.17.2.1	Dostupnost vybavení pro zpracování informací	Zavést 1. etapa
A.18	Soulad s požadavky	
A.18.1	Soulad s právními a smluvními požadavky	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	Zavést 3. etapa
A.18.1.2	Ochrana duševního vlastnictví	Zavést 3. etapa
A.18.1.3	Ochrana záznamů	Zavést 3. etapa
A.18.1.4	Soukromí a ochrana osobních údajů	Zavést 3. etapa
A.18.1.5	Regulace kryptografických opatření	Zavést 3. etapa
A.18.2	Přezkoumání bezpečnosti informací	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	Zavést 3. etapa
A.18.2.2	Shoda s bezpečnostními politikami a normami	Zavést 3. etapa
A.18.2.3	Přezkoumání technické shody	Zavést 3. etapa

6.2.2 Časový plán implementace

Název úkolu	Duration	Start	Finish	Predecessors	Resource Names
A.5.1.1 Vytvoření dokumentu bezpečnostní politiky	3 days	Mon 2.10.17	Wed 4.10.17		
A.5.1.1 Seznámení zaměstnanců s politikou	0,2 days	Thu 5.10.17	Thu 5.10.17	1	
A.5.1.1 Informování externích stran	0,3 days	Thu 5.10.17	Thu 5.10.17	2	
A.5.1.2 Vytvoření plánu revize	0,1 days	Thu 5.10.17	Thu 5.10.17	3	
A.6.1.1 Vytvoření dokumentu rolí a odpovědnosti	0,2 days	Thu 5.10.17	Thu 5.10.17	4	
A.6.1.2 Vytvoření dokumentu neslučitelných povinností a odpovědností	1,08 days	Thu 5.10.17	Fri 6.10.17	5	
A.7.2.2 Vytvoření plánu školení	0,1 days	Fri 6.10.17	Fri 6.10.17	6	
A.7.2.3 Vypracování procesu disciplinárního řízení	1 day	Fri 6.10.17	Mon 9.10.17	7	
A.8.1.1 Vytvoření seznamu aktiv a jejich vlastníků	2 days	Mon 9.10.17	Wed 11.10.17	8	
A.8.1.3 Vytvoření pravidel pro přípustné použití aktiv v podniku	1 day	Wed 11.10.17	Thu 12.10.17	9	
A.8.1.4 Vypracování seznamu aktiv a směrnice	0,5 days	Thu 12.10.17	Fri 13.10.17	10	
A.8.2.1 Vytvoření klasifikace informací	0,1 days	Fri 13.10.17	Fri 13.10.17	11	
A.8.2.1 Vytvoření dokumentu o nakládání s jednotlivými informací	1 day	Fri 13.10.17	Mon 16.10.17	12	
A.8.2.2 Nastavení tiskáren	0,2 days	Mon 16.10.17	Mon 16.10.17	13	
A.8.2.3 Nastavení pracovních stanic	0,4 days	Mon 16.10.17	Tue 17.10.17	14	
A.8.2.3 Proškolení zaměstnanců	0,2 days	Tue 17.10.17	Tue 17.10.17	15	
A.8.3 Vytvoření směrnic pro manipulaci s výměnnými médii	5 days	Tue 17.10.17	Tue 24.10.17	16	
A.8.3.2 Vybrat smluvní společnost k likvidaci médií	5 days	Tue 17.10.17	Tue 24.10.17	16	
A.11.1.1 Čipový systém pro budovu dopravy a mechanizace	3 days	Mon 9.10.17	Wed 11.10.17		
A.11.2.1 Přesun výparníku klimatizace	2 days	Mon 9.10.17	Tue 10.10.17		
A.11.2.9 Vytvoření směrnice Zásada prázdného stolu	0,5 days	Tue 24.10.17	Tue 24.10.17	18	
A.12.2.1 Nákup 30x licence Symantec Endpoint Protection Small Business Edition	0,2 days	Thu 5.10.17	Thu 5.10.17	1	
A.12.2.1 Školení zaměstnanců	1 day	Wed 8.11.17	Wed 8.11.17	21;22	
A.17.2.1 Nákup Lenovo System x3250 M5	0,2 days	Mon 9.10.17	Mon 9.10.17	1	
A.17.2.1 Práce správce ICT	2 days	Wed 11.10.17	Thu 12.10.17	24;20	
A.6.2.1 Vypracování prohlášení o odpovědnosti za mobilní zařízení	0,5 days	Thu 9.11.17	Thu 9.11.17	23	
A.6.2.1 Vypracování postupu pro zvládání bezpečnostního incidentu	1 day	Thu 9.11.17	Fri 10.11.17	26	
A.6.2.2 Vypracování bezpečnostních pravidel	5 days	Fri 10.11.17	Fri 17.11.17	27	
A.6.2.2 Školení zaměstnanců	3 days	Fri 17.11.17	Wed 22.11.17	28	
A.7.1.1 Vytvoření dokumentu s požadavky na prověření uchazečů	1 day	Wed 22.11.17	Thu 23.11.17	29	
A.7.1.2 Vytvoření vzoru dodatků ke smlouvě	1 day	Thu 23.11.17	Fri 24.11.17	30	
A.9.1.1 Definování přístupových skupin	0,5 days	Fri 24.11.17	Fri 24.11.17	31	
A.9.1.2 Bezpečnostní nastavení pracovních stanic, serveru, aktivních síťových prvků a	5 days	Mon 27.11.17	Fri 1.12.17	32	
A.9.2 Řízení přístupu uživatelů	10 days	Mon 4.12.17	Fri 15.12.17	33	



Obrázek 13: Časový plán implementace I. a II. fáze (vlastní zpracování)

6.2.3 I. Etapa – opatření

6.2.3.1 A.5 Politiky bezpečnosti informací

Vzhledem k tomu, že v minulosti nebyla bezpečnost informací v podniku řešena, je nezbytné, aby management podniku vyjádřil podporu projektu dříve, než se začnou implementovat jiná opatření. Nezbytné je také zřídit roli bezpečnostního manažera, který bude za implementaci ISMS zodpovědný.

6.2.3.1.1 **A.5.1 Směřování bezpečnosti informací vedením organizace**

Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi. (6)

6.2.3.1.1.1 A.5.1.1 Politiky pro bezpečnost informací

Odpovědná osoba: majitel podniku

Opatření: Vedení podniku vytvoří bezpečnostní politiku, kterou nechá schválit managementem, vydá ji a dá ji na vědomí všem zaměstnancům a relevantním externím stranám. Zaměstnanci (s výjimkou dělníků) budou povinni podepsat, že se s touto politikou seznámili. V politice se podnik zaváže k následujícímu:

- Bude trvale vytvářet podmínky k zajišťování všech zdrojů potřebných k zavedení, udržování a soustavnému zlepšování systému managementu bezpečnosti informací v celé organizaci.
- Bude uplatňovat politiku založenou na principech důvěrnosti, dostupnosti a úplnosti informací, na požadavcích právních a normativních předpisů a na požadavcích zainteresovaných stran.
- Bude pravidelně hodnotit plnění cílů a cílových hodnot vycházejících z analýzy rizik a této politiky.
- Bude soustavným prosazováním programu zvyšování informovanosti a právního povědomí zaměstnanců udržovat vysokou úroveň informační bezpečnosti.
- Bude pevně a přesvědčivě prosazovat uplatňování zásad informační bezpečnosti vůči smluvním partnerům a třetím stranám prezentovat profesionální přístup a postavení organizace na současném trhu.
- Bude zavedeným systémem managementu informační bezpečnosti informací poskytovat zákazníkům a smluvním partnerům, ale i svým zaměstnancům dostatečnou míru podpory a jistoty při nakládání s jejich informacemi a daty. (6)

Zdroje na opatření:

Vytvoření dokumentu bezpečnostní politiky	3 čd
Seznámení zaměstnanců s politikou	0,2 čd lektor+5čd zam
Informováni externích stran	0,3 čd

6.2.3.1.1.2 A.5.1.2 Přezkoumání politik pro bezpečnost informací

Odpovědná osoba: Bezpečnostní manažer

Opatření: Z důvody zajištění aktuálnosti a souladu s právními normami je nezbytné nastavit pravidelný interval revize dokumentu bezpečnostní politiky. Součástí této revize je také přezkoumání účinnosti této politiky. Doba je nyní stanovena na 1 rok, ale po implementaci ISMS do organizace bude vhodné tuto dobu zkrátit, aby včas přijala opatření k odvrácení nových hrozeb.

Zdroje na opatření:

Vytvoření plánu revize	0,1 čd
Pravidelné přezkoumání politiky a úpravy	3 čd

6.2.3.2 A.6 Organizace bezpečnosti informací

6.2.3.2.1 A.6.1 Interní organizace

Cíl: Ustanovit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci. (6)

6.2.3.2.1.1 A.6.1.1 Role a odpovědnosti bezpečnosti informací

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečnostní manažer vytvoří směrnici, ve které budou definované všechny role z oblasti bezpečnosti informací a odpovědnosti jednotlivých rolí.

Zdroje na opatření:

Vytvoření dokumentu rolí a odpovědnosti	0,2 čd

6.2.3.2.1.2 A.6.1.2 Princip oddělení povinností

Odpovědná osoba: Bezpečnostní manažer

Opatření: Pro vyloučení možnosti manipulace s aktivy z důvodu střetu zájmů, je nezbytné vytvořit směrnici, která bude definovat neslučitelné povinnosti a odpovědnosti. A to jak na úrovni jednotlivých oddělení, ale i všech rolí podniku a jednotlivých aktivit. Tento dokument musí být revidován každé 3 měsíce.

Zdroje na opatření:

Vytvoření dokumentu neslučitelných povinností a odpovědností	1 čd
Revize dokumentu	0,1 čd

6.2.3.3 A.7 Bezpečnost lidských zdrojů

6.2.3.3.1 A.7.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací. (6)

6.2.3.3.1.1 A.7.2.1 Odpovědnost managementu organizace

Odpovědná osoba: Bezpečnostní manažer

Opatření: Management bude od všech zaměstnanců a smluvních stran vyžadovat, aby aplikovali bezpečnost informací v souladu se zavedenými politikami a postupy organizace (viz opatření A.5.1.1)

Zdroje na opatření:

Zahrnuto v A.5.1.1

6.2.3.3.1.2 A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečností manažer vytvoří plán úvodních školení a dále pravidelných přeškolování na roční bázi. Dále vytvoří komunikační kanál, pomocí kterého budou zaměstnanci pravidelně informováni o změnách v politikách a postupech bezpečnosti informací.

Zdroje na opatření:

Vytvoření plánu školení	0,1 čd
Úvodní zaškolení	v rámci A.5.1.1
Pravidelné přeškolení	0,2 čd lektor+5čd zam

6.2.3.3.1.3 A.7.2.3 Disciplinární řízení

Odpovědná osoba: Bezpečnostní manažer, právní zástupce, manažer oddělení

Opatření: Bezpečnostní manažer vytvoří ve spolupráci s právním zástupcem proces disciplinárního řízení vůči zaměstnancům, kteří dopustili narušení bezpečnosti informací. Proces bude obsahovat udělení vytýkacího dopisu při porušení pracovní kázně, popř. okamžité zrušení pracovního poměru při dlouhodobém porušování povinností souvisejících s ochranou informací.

Manažer oddělení bude důsledně následovat tento proces.

Zdroje na opatření:

Vypracování procesu disciplinárního řízení 1 čd

6.2.3.4 A.8 Řízení aktiv

6.2.3.4.1 A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnost k jejich přiměřené ochraně (6)

6.2.3.4.1.1 A.8.1.1 Seznam aktiv

Odpovědná osoba: Bezpečnostní manažer

Opatření: Je třeba zaevidovat aktiva identifikovaná ve fázi ustanovení ISMS. Jako další opatření je třeba zavést pravidelnou revizi těchto aktiv. Revizní interval je stanoven na 1 rok vzhledem k nízké pravděpodobnosti změny ve struktuře aktiv. Součást revize bude posouzení aktuálnosti seznamu aktiv, identifikace a přidání aktiv nových a odstranění neaktuálních aktiv. Revize je nutná i při jakékoliv zaznamenané změně aktiv.

Zdroje na opatření:

Posouzení aktuálnosti seznamu aktiv a jeho aktualizování 0,2 čd/revize

6.2.3.4.1.2 A.8.1.2 Vlastnictví aktiv

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečností manažer přidělí aktivům vlastníka. V našem případě bude vlastnictví aktiv přiděleno vedoucím oddělení. Nezbytným krokem je vlastníka aktiva informovat o jeho právech a povinnostech a vyžádat si potvrzení, že jim rozumí.

Tabulka 12: Vlastnictví aktiv (vlastní zpracování)

Aktivum	Vlastník aktiva
Firemní účetnictví	Ekonomický ředitel
Zdrojové kódy účetního systému	Správce ICT
Výrobní postupy	Výrobní ředitel
Databáze klientů	Obchodní ředitel
Rozpočty, kalkulace	Obchodní ředitel
Zálohovaná data	Správce ICT

VPN server	Správce ICT
Účetní SW Faust	Ekonomický ředitel
Rozpočtový SW	Obchodní ředitel
Server	Správce ICT
Zálohovací server	Správce ICT
Síťová infrastruktura	Správce ICT
Pracovní stanice	Správce ICT
Vozidla	Vedoucí střediska mechanizace a dopravy
Výrobní stroje	Vedoucí střediska mechanizace a dopravy

Zdroje na opatření:

V rámci opatření A.8.1.1 Seznam aktiv

6.2.3.4.1.3 **A.8.1.3 Přípustné použití aktiv**

Odpovědná osoba: Bezpečnostní manažer

Opatření: Je třeba stanovit pravidla pro využívání informací v informačních aktivech a využívání technických prostředků podniku. Musí být vypracována dokumentace, která bude obsahovat povolený software, který lze instalovat na pracovní stanice a odpovědnost jednotlivých pracovníků za data na nich uložená.

Dokumentace bude dále obsahovat informace o nakládání s důvěrnými informacemi. Důvěrné informace a informace, u kterých hrozí zneužití třetí stranou, nesmí být sdíleny jak mimo podnik samotný, tak ani s odděleními, která tyto informace nepotřebují ke svojí pracovní činnosti. Tato pravidla budou revidována v ročním intervalu.

Zdroje na opatření:

Vytvoření pravidel pro přípustné použití aktiv v podniku	1čd
Revize pravidel	0,1 čd / rok

6.2.3.4.1.4 **A.8.1.4 Vrácení aktiv**

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečnostní manažer s vlastníky aktiv vypracuje seznam všech aktiv, která jsou dostupná k zapůjčení. Následně vypracuje směrnici, která bude udávat povinnost zaměstnance před posledním pracovním dnem zaměstnance ve výpovědní lhůtě nebo před odchodem na mateřskou dovolenou, získat písemné potvrzení o navrácení aktiv od všech jejich vlastníků. Toto potvrzení bude předáno odpovědnému manažerovi a uschováno v osobní složce.

Zdroje na opatření:

Vypracování seznamu aktiv a směrnice	0,5 čd

6.2.3.4.2 **A8.2 Klasifikace informací**

Cíl: Zajistit, aby informace dostaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.

6.2.3.4.2.1 **A.8.2.1 Klasifikace informací**

Odpovědná osoba: Bezpečnostní manažer

Opatření: V podniku bude zavedena klasifikace informací podle jejich povahy a to na důvěrné a tajné. Mezi důvěrné informace bude patřit:

- Interní informace o podniku
- Informace o lidských zdrojích
- Informace, které jsou určeny pouze příjemci

Mezi tajné informace bude patřit:

- Informace, které musí být chráněny dle právních předpisů (např. informace o klientech)
- Informace, které mohou podnik poškodit, popř. dát někomu konkurenční výhodu (rozpočty, know-how)
- Účetní informace

Zdroje na opatření:

Vytvoření klasifikace informací	0,1 čd
Vytvoření dokumentu o nakládání s jednotlivými informacemi	1 čd

6.2.3.4.2.2 **A.8.2.2 Označování informací**

Odpovědná osoba: Bezpečnostní manažer

Opatření: Všechny výše uvedené tištěné i elektronické dokumenty musí obsahovat vodoznak "Důvěrné" nebo "Tajné" dle jejich klasifikace. Tištěné dokumenty pak budou obsahovat úvodní stránku s označením klasifikace a jménem osoby, která materiály vytiskla.

Zdroje na opatření:

Nastavení tiskáren	0,2 čd

6.2.3.4.2.3 **A.8.2.3 Manipulace s aktivy**

Odpovědná osoba: Bezpečnostní manažer

Opatření: Tiskárny budou přepnuty do důvěrného režimu, což znamená, že se dokumenty vytisknou až po zadání čtyřmístného kódu na klávesnici tiskárny. Žádné důvěrné informace nesmí být ponechány na přístupném místě bez dozoru.

Zdroje na opatření:

Nastavení tiskáren v rámci A.8.2.2	
Nastavení pracovních stanic	0,4 čd
Proškolení zaměstnanců	0,2 čd

6.2.3.4.3 **A.8.3 Manipulace s médii**

Cíl: Zabránit neoprávněnému prozrazení, modifikaci, odstranění nebo zničení informací uložených na médiu. (6)

6.2.3.4.3.1 **A.8.3.1 Správa výměnných médií**

Odpovědná osoba: Bezpečnostní manažer, Správce ICT

Opatření: Bezpečností manažer analyzuje nutnost použití výměnných médií jednotlivými zaměstnanci. Dále vytvoří směrnici pro nakládání s výměnnými médii. Ta bude obsahovat seznam zaměstnanců, popř. jejich skupin, s možností tato média používat. Ostatní zaměstnanci budou mít jejich používání zakázané jak vnitropodnikovou směrnicí, tak nastavením operačního systému. Všechna média budou zašifrována pomocí Symantec Drive Protection PGP, pokud je to možné. Bude naprogramován skript, který bude minimálně jednou za tři měsíce poskytovat seznam

připojených médií. Jednotlivé detekce se budou individuálně diskutovat se zaměstnanci. Směrnice bude obsahovat sankce pro případné nedodržení směrnice zaměstnanci.

Zdroje na opatření:

Vytvoření směrnice	2 čd
Nastavení OS	1 čd
Zaškolení zaměstnanců	v rámci A.5.1.1
Licence Symantec Drive Protection PGP	v rámci A.6.2.2

6.2.3.4.3.2 A.8.3.2 Likvidace médií

Odpovědná osoba: Bezpečnostní manažer

Opatření: CD a DVD budou skartovány, HDD a flash disky budou fyzicky zničeny nebo demagnetizovány odbornou firmou. Bezpečností manažer zajistí výběr firmy a případné svozy. Likvidace těchto médií bude zaznamenána pro případ nutnosti auditu. Bude součástí směrnice dle A.8.3.1.

Zdroje na opatření:

Vytvoření směrnice	v rámci A.8.3.1
Zaškolení zaměstnanců	v rámci A.5.1.1
Likvidace médií	dle smlouvy

6.2.3.4.3.3 A.8.3.3 Přeprava fyzických médií

Odpovědná osoba: Bezpečnostní manažer

Opatření: Přeprava fyzických médií bude zakázána. Výjimky bude udělovat bezpečnostní manažer po konzultaci s nadřízeným žadatele o výjimku.

Zdroje na opatření:

Vytvoření směrnice	v rámci A.8.3.1

6.2.3.5 A.11 Fyzická bezpečnost a bezpečnost prostředí

6.2.3.5.1 A.11.1 Bezpečné oblasti

Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.

6.2.3.5.1.1 A.11.1.1 Fyzický bezpečnostní perimetr

Odpovědná osoba: Bezpečnostní manažer

Opatření: Je nutné vytvoření dokumentu se seznamem a popisem jednotlivých fyzických bezpečnostních perimetrů. Tyto perimetry budou rozděleny na základě jednotlivých pater a dále středisek, která sídlí v oddělených kancelářích.

Administrativní budova je vybavena čipovým systémem, který umožňuje definovat přístupy do budovy a dále na jednotlivá patra a to jak pomocí výtahu, tak po schodech. Budova dopravy a mechanizace je volně přístupná a je tudíž nezbytné ji tímto systémem vybavit a definovat tak přístup do budovy, na patra a do jednotlivých dílen a skladů na základě nutnosti k výkonu práce.

Zdroje na opatření:

Vytvoření dokumentace perimetrů	1 čd
Čipový systém pro budovu dopravy a mechanizace	27 000 Kč bez DPH
Dohled nad přístupem do perimetrů	0,1 čd / měsíc

6.2.3.5.1.2 A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Odpovědná osoba: Bezpečnostní manažer, odpovědný manažer

Opatření: Bezpečnostní manažer vypracuje směrnici, která bude nařizovat uzamykání kanceláří při opuštění zaměstnanci a definované sankce při porušení nařízení.

Zdroje na opatření:

Vypracování nařízení	0,1 čd

6.2.3.5.2 A.11.2 Zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace.

6.2.3.5.2.1 A.11.2.1 Umístění zařízení a jeho ochrana

Odpovědná osoba: Bezpečnostní manažer

Opatření: Toto opatření je z převážné části již zavedeno. Nutná je úprava chlazení serverovny, kde je výparník částečně umístěn nad rackem, ve kterém je

umístěn server a síťové prvky. Výparník bude přemístěn mimo serverovnu a to tak, aby při poškození klimatizačního potrubí nedošlo k poškození aktiv tekutinou.

Zdroje na opatření:

Přesun výparníku klimatizace	3500 Kč bez DPH
Stavební práce	500 Kč

6.2.3.5.2.2 A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečnostní manažer vypracuje směrnici zakazující ponechávat citlivé nebo kritické informace bez dozoru. Tyto informace, a to jak v tištěné formě, tak na paměťovém médiu, musí být uzamčeny ve skříňce nebo trezoru. Počítače musí být při opuštění pracovního místa odhlášeny nebo uzamčeny. Nastavení tiskáren do "důvěrného režimu" v opatření A.8.2.2.

Zdroje na opatření:

Vytvoření směrnice Zásada prázdného stolu	0,5 čd

6.2.3.6 A.12 Bezpečnost provozu

6.2.3.6.1 A.12.2 Ochrana proti malwaru

Cíl: Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru. (6)

6.2.3.6.1.1 A.12.2.1 Opatření proti malwaru

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečnostní manažer vypracuje směrnici zakazující používání neschváleného softwaru (omezení instalace v A.12.6.2). Směrnice bude obsahovat seznam povoleného softwaru, zákaz používání jakýchkoliv datových médií, pokud nejsou nezbytné k pracovnímu úkonu, interval provádění pravidelných přezkoumání softwaru (každé 3 měsíce) a datového obsahu pracovních stanic. Přítomnost jakéhokoli neschváleného softwaru bude formálně vyšetřena. Bude nainstalován Symantec Endpoint Protection Small Business Edition k detekci a odstranění malwaru. Bude zaveden filtr webových stránek (součást instalace Symantec Endpoint Protection Small Business Edition). Bude vypracován plán proškolení zaměstnanců zabývající se

ochranou před malwarem na systémech a podáváním zpráv o útocích. Zálohování dat k obnovení při bezpečnostním incidentu je popsáno v A.12.3.1.

Zdroje na opatření:

Nákup 30x licence Symantec Endpoint Protection Small Business Edition	27530,1 Kč bez DPH / 3 roky
Instalace Symantec Endpoint Protection Small Business Edition	2 čd
Školení zaměstnanců	15 čd

6.2.3.7 A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

6.2.3.7.1 A.17.2 Redundance

Cíl: Zajistit dostupnost vybavení pro zpracování informací (6)

6.2.3.7.1.1 A.17.2.1 Dostupnost vybavení pro zpracování informací

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bude vytvořen serverový cluster, který v případě výpadku serveru přepojí zdroje na server záložní bez dopadu na uživatele. Diskové pole bude změněno na konfiguraci RAID5, čímž dojde k navýšení místa na discích o 2TB při odolnosti proti výpadku jednoho disku.

Zdroje na opatření:

Nákup Lenovo System x3250 M5	29440Kč bez DPH
Práce správce ICT	2 čd

6.2.4 Zdroje a náklady na I. etapu

Tabulka 13: Tabulka nákladů I. etapy zavedení ISMS (vlastní zpracování)

ID opatření	Popis	Jednorázově v čd	Ročně v čd	Kvartálně v čd	Měsíčně v čd	Jednorázově v Kč bez DPH
A.5.1.1	Vytvoření dokumentu bezpečnostní politiky	3				
A.5.1.1	Seznámení zaměstnanců s politikou	5,2				
A.5.1.1	Informováni externích stran	0,3				
A.5.1.2	Vytvoření plánu revize	0,1				
A.5.1.2	Pravidelné přezkoumání politiky a úpravy		3			
A.6.1.1	Vytvoření dokumentu rolí a odpovědnosti	0,2				
A.6.1.2	Vytvoření dokumentu neslučitelných povinností a odpovědností	1				
A.6.1.2	Revize dokumentu			0,1		
A.7.2.2	Vytvoření plánu školení	0,1				
A.7.2.2	Pravidelné přeškolení		5,2			
A.7.2.3	Vypracování procesu disciplinárního řízení	1				
A.8.1.1	Posouzení aktuálnosti seznamu aktiv a jeho aktualizování		0,2			
A.8.1.3	Vytvoření pravidel pro přípustné použití aktiv v podniku	1				
A.8.1.3	Revize pravidel		0,1			
A.8.1.4	Vypracování seznamu aktiv a směrnice	0,5				
A.8.2.1	Vytvoření klasifikace informací	0,1				
A.8.2.1	Vytvoření dokumentu o nakládání s jednotlivými informací	1				
A.8.2.2	Nastavení tiskáren	0,2				
A.8.2.3	Nastavení pracovních stanic	0,4				
A.8.2.3	Proškolení zaměstnanců	0,2				
A.8.3.1	Správa výměnných médií	3				
A.9.4.3	Nastavení aplikací a OS	3				
A.11.1.1	Vytvoření dokumentace perimetrů	1				
A.11.1.1	Čipový systém pro budovu dopravy a mechanizace					27000
A.11.1.1	Dohled nad přístupem do perimetrů				0,1	
A.11.1.3	Vypracování nařízení	0,1				
A.11.2.1	Přesun výparníku klimatizace					3500
A.11.2.1	Stavební práce					500
A.11.2.9	Vytvoření směrnice Zásada prázdného stolu	0,5				
A.12.2.1	Nákup 30x licence Symantec Endpoint Protection Small Business Edition					27530,1

A.12.2.1	Instalace Symantec Endpoint Protection Small Business Edition	2				
A.12.2.1	Školení zaměstnanců	15				
A.17.2.1	Nákup Lenovo System x3250 M5					29440
A.17.2.1	Práce správce ICT	2				

Odhad nákladů spojených s implementací opatřených vybraných pro první etapu je 40,9 člověkodnů jednorázově při zavádění a dále 0,1 člověkodne měsíčně a kvartálně a 8,5 ročně na revizi opatření.

Tabulka 14: Sumarizace nákladů na I. etapu (vlastní zpracování)

Jednorázové náklady 55,9 člověkodnů á 350 Kč / hod v Kč	**114520**
Roční náklady 8,5 člověkodnů á 350 Kč / hod v Kč	**23800**
Kvartální náklady 0,1 člověkodnů á 350 Kč / hod v Kč	**280**
Měsíční náklady 0,1 člověkodnů á 350 Kč / hod v Kč	**280**
Jednorázové finanční náklady v Kč bez DPH	**87970**

Finanční náklady na první etapu jsou odhadnuty na 226 850 Kč.

Náklady na lidskou práci jsou pouze informativní a budou zahrnuty v pracovním fondu zaměstnanců. Tyto náklady jsou tvořeny převážně prací bezpečnostního manažera, kterému bude rozšířen pracovní úvazek z částečného na plný.

6.2.5 II. Etapa – opatření

6.2.5.1 A.6 Organizace bezpečnosti informací

6.2.5.1.1 A.6.1 Interní organizace

Cíl: Ustanovit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci. (6)

6.2.5.1.1.1 A.6.1.5 Bezpečnost informací v řízení projektů

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečností manažer vytvoří plán školení všech zaměstnanců podílejících se na projektové činnosti. Důraz bude kladen na zahrnutí bezpečnostních cílů do samotných projektů, identifikaci a posuzování bezpečnostních rizik již v rané fázi projektů a implementaci bezpečnosti informací do použité projektové metodiky.

Taktéž zajistí vyškolení nových zaměstnanců a přeškolení v maximálně ročním intervalu.

Zdroje na opatření:

Vytvoření plánu školení	0,1 čd
Vytvoření školení	2 čd
Úvodní zaškolení	0,2 čd lektor+5čd zam
Pravidelné přeškolení	0,1 čd lektor+3čd zam

6.2.5.1.2 A.6.2 Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost při užívání mobilních zařízení a pro práci na dálku. (6)

6.2.5.1.2.1 A.6.2.1 Politika mobilních zařízení

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečnostní manažer vytvoří směrnici pro využívání mobilních zařízení. Každý zaměstnanec podepíše při převzetí zařízení, že je zodpovědný za jeho případné poškození nebo odcizení a že je seznámen s bezpečnostními zásadami pro práci s mobilními zařízeními (viz A.6.2.2 Práce na dálku).

Bezpečnostní manažer vypracuje postup při bezpečnostním incidentu jako je ztráta nebo krádež mobilního zařízení a při podezření na kompromitaci dat.

Zdroje na opatření:

Vypracování prohlášení o odpovědnosti za mobilní zařízení	0,5 čd
Vypracování postupu pro zvládání bezpečnostního incidentu	1 čd

6.2.5.1.2.2 A.6.2.2 Práce na dálku

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečnostní manažer vypracuje směrnici, která bude obsahovat seznam nastavení zařízení a opatření, který je každý zaměstnanec povinen dodržovat. To bude obsahovat prohlášení, že zaměstnanec je zodpovědný za přidělené zařízení a bude podepsáno zaměstnancem při převzetí zařízení. Dále, že každé mobilní zařízení, které je využívané k firemním účelům, musí splňovat danou úroveň zabezpečení. Zařízení musí být chráněné silným heslem s exspirací 3 měsíce, musí mít zašifrované datové úložiště, spořič obrazovky musí být nastaven na méně než 10 minut a musí být chráněn heslem. K zařízením se nesmí připojovat USB zařízení, pokud to není

nevyhnutelné k výkonu práce, povinnost mít zapnutou historii ve webových prohlížečích a podobně.

Všechny přenosné počítače ponechané bez dozoru musí být zabezpečeny uzamykatelným kabelem tak, aby nedošlo k jejich odcizení. Každé 3 měsíce bude provedena náhodná kontrola 10% zaměstnanců využívající mobilní zařízení a striktně uplatněny kázeňská opatření při nedodržení směrnice.

Zdroje na opatření:

Vypracování bezpečnostních pravidel	5 čd
Nákup zabezpečovacích kabelů	12 x 417 Kč bez DPH
Školení zaměstnanců	3 čd
Symantec Drive Protection PGP	22226,4 Kč bez DPH (12x licence na 3 roky)

6.2.5.2 A.7 Bezpečnost lidských zdrojů

6.2.5.2.1 A.7.1 Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybíráni vhodní kandidáti. (6)

6.2.5.2.1.1 A.7.1.1 Prověřování

Odpovědná osoba: Bezpečnostní manažer

Opatření: Bezpečnostní manažer vypracuje ve spolupráci s právním zástupcem seznam prověření, na každou pozici v organizaci, které musí uchazeč dodat před uzavřením pracovní smlouvy. A to s přihlédnutím ke klasifikaci informací, ke kterým by měli uchazeči získat přístup a také z hlediska potencionálních rizik. Požadavky musí být dle platných zákonů a v souladu s etikou.

Zdroje na opatření:

Vytvoření dokumentu s požadavky na prověření uchazečů	1 čd

6.2.5.2.1.2 A.7.1.2 Podmínky pracovního vztahu

Odpovědná osoba: Bezpečnostní manažer

Opatření: Ve spolupráci s právním zástupcem bude vypracován dodatek k pracovní smlouvě, který bude obsahovat ustanovení o jejich odpovědnosti za bezpečnost informací.

Zdroje na opatření:

Vytvoření vzoru dodatků ke smlouvě 1 čd

6.2.5.3 A.9 Řízení přístupu

6.2.5.3.1 A9.1 Požadavky organizace na řízení přístupu

Cíl: Omezit přístup k informacím a vybavení pro zpracování informací. (6)

6.2.5.3.1.1 A.9.1.1 Politika řízení přístupu, A.9.1.2 Přístup k sítím a síťovým službám

Odpovědná osoba: Bezpečnostní manažer, Správce ICT

Opatření: Definování rolí v rámci organizace z pohledu přístupu k informacím a síťovým zdrojům (Např. správce, účetní, stavbyvedoucí atd.) a přiřazení úrovně přístupu pro jednotlivou skupinu.

Zdroje na opatření:

Definování přístupových skupin 0,5 čd

Bezpečnostní nastavení pracovních stanic, serveru, aktivních síťových prvků a dalších prostředků 5 čd

6.2.5.3.2 A.9.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám. (6)

6.2.5.3.2.1 A.9.2.1 Registrace a zrušení registrace uživatele

Odpovědná osoba: Bezpečnostní manažer, ICT manažer

Opatření: Bezpečností manažer vypracuje směrnici, která definuje správu a řízení ID uživatelů. Směrnice bude obsahovat následující body:

- Zákaz používání sdílených ID
- Okamžité zablokování ID zaměstnanců, kteří opustili organizaci – viz A.9.2.6
- Zavedení pravidelné revalidace s cílem eliminace duplicitních uživatelských ID

Zdroje na opatření:

Vytvoření směrnice	0,1 čd
Vytvoření procesu revalidace	2 čd ICT manažer

6.2.5.3.2.2 A.9.2.2 Správa uživatelských přístupů, A.9.2.5 Přezkoumání přístupových práv uživatelů, A.9.2.6 Odebrání nebo úprava přístupových práv

Odpovědná osoba: Bezpečnostní manažer, odpovědný manažer

Opatření: Vypracování procesu přidělování a odebírání přístupových práv. Přístup musí být schválen odpovědným vedoucím a správcem aktiva. Dále je důležité vypracovat proces pro odejmutí přístupových práv a ten zakotvit i do procesu ukončování pracovního poměru. Bude zavedena pravidelná kontrola platnosti práva na přístupové účty a to v intervalu 3 měsíce. Odpovědný manažer potvrdí trvání práva na přístup, popř. neprodleně zahájí nezbytné kroku k deaktivaci přístupového účtu.

Zdroje na opatření:

Vypracování procesu pro přidělování a odebírání přístupových práv	1 čd

6.2.5.3.2.3 A.9.2.3 Správa privilegovaných přístupových práv

Odpovědná osoba: Bezpečnostní manažer, ICT manažer, vlastníci aktiv

Opatření: Bezpečností manažer vytvoří proces pro přidělování privilegovaných uživatelských práv. Tyto práva budou přidělována na dobu určitou a to maximálně na dobu jednoho roku a pouze po odsouhlasení vlastníka aktiva a odpovědného manažera zaměstnance. V ročním intervalu proběhne revalidace, při které se odstraní již nepotřebné přístupy. Bude udržován seznam těchto přístupů pro účely auditu.

Zdroje na opatření:

Vytvoření směrnice	1 čd
Vytvoření procesu revalidace	2 čd
Pravidelná revalidace	0,1 čd/ročně manažeři a vlastníci aktiv

6.2.5.3.3 A.9.4 Řízení přístupu k systémům a aplikacím

6.2.5.3.3.1 A.9.4.3 Systém správy hesel

Odpovědná osoba: Bezpečnostní manažer

Opatření: Aplikace budou nastaveny, aby:

- Vyžadovaly změnu hesla po prvním přihlášení
- Vyžadovaly kvalitní heslo - minimálně 8 znaků, 1 číslo a 1 velké písmeno
- Vyžadovaly pravidelnou změnu hesla každé 2 měsíce
- Zabránily opakovanému použití hesla
- Nezobrazovaly heslo během zadávání
- Ukládaly data a hesla odděleně
- Ukládaly a přenášely hesla v chráněné podobě

Zdroje na opatření:

Nastavení aplikací a OS 3 čd

6.2.5.3.4 A.9.3 Odpovědnost uživatelů

Cíl: Učinit uživatele odpovědné za ochranu svých autentizačních informací. (6)

6.2.5.3.4.1 A.9.3.1 Používání tajných autentizačních informací

Odpovědná osoba: Bezpečnostní manažer, ICT manažer

Opatření: Bezpečností manažer vytvoří směrnici, která bude obsahovat zásady a postupy pro používání tajných autentizačních informací:

- Zaměstnanci budou udržovat tajnou autentizační informaci jako důvěrnou
- Tajná autentizační informace nesmí být uchovávaná v tištěné ani elektronické podobě, vyjma případů, kdy je zabezpečena
- V případě náznaku kompromitace tuto skutečnost zaměstnanec neprodleně oznámí bezpečnostnímu manažerovi a kompromitovanou informaci změní
- Zaměstnanci obdrží školení na tvorbu hesel: ty budou snadno zapamatovatelná, nebudou založena na osobních informacích, nebudou

sestavena ze slov, které obsahuje slovník a neobsahují po sobě jdoucí znaky

Zdroje na opatření:

Vytvoření směrnice	0,5 čd
Nastavení OS a aplikací	2 čd ICT manažer
Školení	5 čd

6.2.6 Zdroje a náklady na II. Etapu

Odhad nákladů na zavedení druhé fáze je uveden v následující tabulce:

Tabulka 15: Tabulka nákladů II. etapy zavedení ISMS (vlastní zpracování)

ID opatření	Popis	Jednorázově v čd	Ročně v čd	Kvartálně v čd	Měsíčně v čd	Jednorázově v Kč bez DPH
A.6.1.5	Bezpečnost informací v řízení projektů	7,3	3,1			
A.6.2.1	Vypracování prohlášení o odpovědnosti za mobilní zařízení	0,5				
A.6.2.1	Vypracování postupu pro zvládání bezpečnostního incidentu	1				
A.6.2.2	Vypracování bezpečnostních pravidel	5				
A.6.2.2	Nákup zabezpečovacích kabelů					5004
A.6.2.2	Školení zaměstnanců	3				
A.6.2.2	Symantec Drive Protection PGP					22226,4
A.7.1.1	Vytvoření dokumentu s požadavky na prověření uchazečů	1				
A.7.1.2	Vytvoření vzoru dodatků ke smlouvě	1				
A.9.1.1	Definování přístupových skupin	0,5				
A.9.1.2	Bezpečnostní nastavení pracovních stanic, serveru, aktivních síťových prvků a	5				
A.9.2.2	Vypracování procesu pro přidělování a odebírání přístupových práv	1				
A.9.2.5						
A.9.2.6						

Odhad nákladů spojených s implementací opatření vybraných pro druhou etapu je 25,3 člověkodnů jednorázově při zavádění a dále 3,1 ročně na revizi opatření.

Tabulka 16: Sumarizace nákladů na II. etapu (vlastní zpracování)

Jednorázové náklady 55,9 člověkodnů á 350 Kč / hod v Kč	**70840**
Roční náklady 8,5 člověkodnů á 350 Kč / hod v Kč	**8680**
Kvartální náklady 0,1 člověkodnů á 350 Kč / hod v Kč	**0**
Měsíční náklady 0,1 člověkodnů á 350 Kč / hod v Kč	**0**
Jednorázové finanční náklady v Kč bez DPH	**27230**

Finanční náklady na zavedení druhé fáze jsou odhadnuté na 106 750 Kč. Konečná cena bude záviset na aktuálních platech zaměstnanců, kteří se budou na jednotlivých úkolech podílet. Dá se předpokládat, že bude nižší.

7 Přínos práce

Přínosem této práce je objasnění komplexnosti problematiky a nutnosti zavedení ISMS majiteli podniku. Práce bude dále sloužit jako podklad pro zavádění jednotlivých nápravných opatření.

Nabyté vědomosti a zkušenosti použiji v zaměstnání, kde jsem se stal kontaktní osobou naší lokální organizace pro audity dle této normy.

S využitím těchto znalostí jsem již v průběhu tohoto roku odhalil několik bezpečnostních incidentů, které mohly potenciálně skončit útokem na spravovaná aktiva, což by mělo za následek velkou finanční škodu jak na straně mého zaměstnavatele, tak našeho zákazníka. A to jak přímou škodu finanční v důsledku uzavřených SLA, tak i nepřímou škodu vzniklou poškozením dobrého jména podniku a negativních referencí.

8 Závěr

Cílem této závěrečné práce bylo zanalyzovat rizika související s řízením informační bezpečnosti a navrhnout nápravná opatření pro první dvě etapy dle přílohy A normy ČSN ISO/IEC 27001:2014.

Vzhledem k tomu, že v současnosti jsou v podniku zavedeny pouze základy ISMS, bude implementace velmi časově i finančně náročná. Majitel podniku si však uvědomuje nutnost zavedení alespoň základních opatření vzhledem k zvyšujícím se nárokům třetích stran na management řízení informací a legislativním požadavkům. Finanční nároky prvních dvou etap jsou odhadnuty na 333 600 Kč, což splňuje podmínku majitele, který stanovil finanční limit, pro nápravná opatření do nich vybraná, na 500 000 Kč.

V této práci jsem vytvořil návrh nápravných opatření pro první dvě etapy implementace dle přílohy A normy ČSN ISO/IEC 27001:2014 a přání investora, čímž jsem splnil cíl práce.

Seznam použité literatury

1. **Ondrák, V., Sedlák, P. a Mazálek, V.** *Problematika ISMS v manažerské informatice.* Brno : Akademické nakladatelství CERM, s.r.o., 2013. ISBN 978-80-7204-872-4.

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

3. **Mitáček, M.** Informační bezpečnost. *Vlastní cesta.* [Online] 23. 11. 2011. [Citace: 1. 5. 2017.] http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/.

4. **Střelec, J.** PDCA cyklus. *vlastnicesta.cz.* [Online] 2008. [Citace: 2. 5 2017.] http://www.vlastnicesta.cz/metody/pdca-cyklus-1/.

5. *ČSN ISO/IEC 27000 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. str. 32.

6. *ČSN ISO/IEC 27001 (36 9797) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. str. 28.

7. *ČSN ISO/IEC 27002 (36 9798) Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. str. 76.

8. *ČSN ISO/IEC 27003 (36 9790) Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. str. 60.

9. *ČSN ISO/IEC 27004 (36 9790) Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. str. 60.

10. *ČSN ISO/IEC 27006 (36 9790) Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. str. 36.

11. *ČSN ISO/IEC 27007 (36 9790) Informační technologie - Bezpečnostní techniky - Směrnice pro audit systémů řízení bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. str. 28.

12. **Čermák, M.** Řízení rizik: Jemný úvod do řízení rizik. *Clever and smart.* [Online] 13. 6. 2010. [Citace: 1. 6. 2016.] http://www.cleverandsmart.cz/rizeni-rizik-jemny-uvod-do-rizeni-rizik/.

13. **Dostálek, A., Dostálek, L.** *Velký průvodce protokoly TCP/IP a systémem DNS.* Brno : Computer Press, 2008. str. 488. ISBN 978-80-251-2236-5.

14. **Horák, J., Keršláger, M.** *Počítačové sítě pro začínající správce.* Brno : Computer Press, 2001. str. 165. ISBN 80-7226-566-0.

15. **Sedlák, P.** NISS: Network Network Infrastructure Infrastructure Security. [Online] [Citace: 14. 6. 2016.] Přednáška, VUTBR FP. https://www.vutbr.cz/www_base/priloha.php?dpid=75253.

16. Člověkoden - Wikipedie. *Wikipedie.* [Online] 17. 5. 2013. [Citace: 2. 6. 2016.] https://cs.wikipedia.org/wiki/%C4%8Clov%C4%9Bkoden.

17. Rack Unit - Wikipedie. *Wikipedie.* [Online] 20. 3. 2013. [Citace: 1. 6. 2016.] https://cs.wikipedia.org/wiki/Rack_unit.

18. ČSN - Wikipedie. *Wikipedie.* [Online] 10. 12. 2014. [Citace: 29. 5. 2016.] https://cs.wikipedia.org/wiki/%C4%8CSN.

19. Veřejný rejstřík a sbírka listin - Ministerstvo spravedlnosti České republiky. *Justice.cz.* [Online] 2012-2016. [Citace: 12. 11. 2016.] https://or.justice.cz/ias/ui/vypis-vypis?subjektId=isor%3a274149&typ=full&klic=358dyl.

20. Veřejný rejstřík a sbírka listin - mMinisterstvo spravedlnosti České republiky. *Justice.cz.* [Online] 2012-2016. [Citace: 12. 11. 2016.] https://or.justice.cz/ias/ui/vypis-vypis?subjektId=isor%3a274149&typ=full&klic=358dyl.

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek a symbolů

ISMS	Systém řízení informační bezpečnosti (z angl. Information Security Management System) (1)
ICT	Informační a komunikační technologie (z angl. Information and Comunication Technology) (1)
čd	člověkoden - čas odpovídající práci jedné osoby po dobu jednoho pracovního dne (16)
1U	je jednotka míry používaná v informačních technologiích k popisu výšky zařízení určeného pro upevnění v racku šíře 19 nebo 23 palců. Jedna racková jednotka je 1,75 palce (44.45 mm) (17)
SLA	Smlouva mezi odběratelem a dodavatelem, která sjednává jistou úroveň služeb. (z angl. Service Level Agreement)
ČSN	chráněné označení českých technických norem. Tvorbu a vydávání ČSN v současné době zajišťuje Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (18)
ISO	Mezinárodní organizace pro normalizaci (z angl. International Organization for Standardization
IEC	Mezinárodní elektrotechnická komise (z angl. International Electrotechnical Commission)
SSID	Identifikátor bezdrátové sítě Wi-Fi, který je periodicky vysílám v tzv. majákovém rámci. Na základě informací které obsahuje, si klienti vybírají síť, do které se chtějí připojit (z angl. Service Set Identifier).
VLAN	Logicky definovaná síť v rámci fyzické sítě(z angl. Virtual Local Area Netowork)
OS	Operační systém (z angl. Operation System).
THP	Technicko-hospodářský pracovník