VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

ZAVEDENÍ ISMS V PODNIKU
IMPLEMENTATION OF ISMS IN A COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Jindřich Pospíchal**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Pospíchal Jindřich, Bc.

Informační management (6209T015)

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

Zavedení ISMS v podniku

v anglickém jazyce:

Implementation of ISMS in a Company

Pokyny pro vypracování:

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

Seznam odborné literatury:

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 P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

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

V Brně, dne 29.2.2016

Abstrakt

Diplomová práce je zaměřená na návrh zavedení systému řízení bezpečnosti informací ve firmě. Obsahuje základní teoretické poznatky a pojmy z bezpečnosti informačních systémů a popisuje normy ČSN ISO/IEC řady 27000. Na základě teoretické části a analýzy současného stavu je zpracován návrh ustanovení ISMS.

Abstract

The master's thesis is aimed at proposing an implementation of information security management system in a company. It covers basic theoretical background and concepts of information system security and describes standards of ČSN ISO/IEC 27000. Specific provisioning of ISMS is then proposed based on the theoretical background and analysis of current state.

Klíčová slova

ISMS, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, bezpečnost informací, management bezpečnosti, návrh informační bezpečnosti

Keywords

ISMS, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, information security, security management, information security design

Bibliografická citace

POSPÍCHAL, J. *Zavedení ISMS v podniku.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 76 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

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

V Brně dne 19. května 2016

…….....

Poděkování

Na tomto místě bych rád poděkoval Ing. Petru Sedlákovi za vedení práce, cenné připomínky a odborné rady, kterými přispěl k vypracování této diplomové práce.

OBSAH

ÚVOD 10

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ 11

1 TEORETICKÁ VÝCHODISKA PRÁCE 12

1.1 Základní pojmy a názvosloví informační bezpečnosti 12

1.2 Zákony a normy v oblasti bezpečnosti IT 13

1.2.1 Legislativa a právní prostředí České republiky 13

1.2.2 Normy ČSN ISO/IEC řady 27000 14

1.3 Analýza rizik 15

1.4 Oblasti opatření podle ČSN ISO/IEC 27001:2013 18

1.5 Management bezpečnosti informačních systémů (ISMS) 23

1.6 Ustanovení ISMS 24

1.7 Zavádění a provoz ISMS 27

1.8 Monitorování a přezkoumání ISMS 28

1.9 Údržba a zlepšování ISMS 30

2 SOUČASNÝ STAV BEZPEČNOSTI 31

2.1 Popis společnosti 31

2.2 Zabezpečení a poloha objektu 31

2.3 Bezpečnost ICT 32

2.4 Zhodnocení současného stavu 34

3 NÁVRH USTANOVENÍ ISMS 35

3.1 Rozsah ISMS 35

3.1.1 Identifikace a ohodnocení informačních aktiv 35

3.2 Politika ISMS 36

3.3 Analýza rizik 37

3.3.1 Identifikace hrozeb 37

3.3.2 Metody analýzy rizik 39
3.4 Soubor opatření podle ČSN ISO/IEC 27001:2013 43
3.5 Plán zavedení opatření 47
3.6 Úpravy lokální sítě a software 47
3.6.1 Úprava lokální sítě 48
3.6.2 Úprava software 51
3.7 Popis bezpečnostních opatření etapy I 52
3.7.1 A.5 Politiky bezpečnosti informací 52
3.7.2 A.6 Organizace bezpečnosti informací 53
3.7.3 A.7 Bezpečnost lidských zdrojů 54
3.7.4 A.8 Řízení aktiv 56
3.7.5 A.11 Fyzická bezpečnost a bezpečnost prostředí 60
3.8 Zdroje a náklady na první etapu 65
3.9 Podíl zavedených opatření na snížení rizika hrozeb 68
ZÁVĚR 69
SEZNAM POUŽITÉ LITERATURY 71
SEZNAM OBRÁZKŮ 73
SEZNAM TABULEK 74
SEZNAM ZKRATEK 75
SEZNAM PŘÍLOH 76

ÚVOD

Bezpečnost je v poslední době velice skloňované téma. Už to není záležitost pouze velkých firem, ale všech firem a domácností. Každá společnost při svém fungování vytváří množství dat a velká část z nich je pro společnost citlivá nebo důvěrná a ohrožení dat s sebou přináší problémy. Proto se bezpečnost řeší i ve firmách, které nejsou technologicky založené a informační a komunikační technologie slouží pouze jako pomocný nástroj pro podporu a ulehčení firemních procesů. Avšak i tyto společnosti potřebují, aby data byla v bezpečí a dalo se na ně spolehnout. Je mnoho hrozeb, které na informace působí a každým dnem se vyvíjejí stále nové a nové. Hrozbami už nejsou ovlivněny pouze počítače, ale i chytré telefony a přenosná média, na kterých se často přenášejí různé škodlivé programy. V této práci se zaměřím na tyto a další hrozby a navrhnu systém, který tato rizika omezuje nebo vyruší.

V první části práce jsou představené teoretické základy a poznatky z oblasti ISMS, které budou využity v návrhové části. Druhá část je věnována rozboru současného stavu informační bezpečnosti v podniku. Třetí, návrhová, část využívá poznatků z teoretické části a analýzy současného stavu k návrhu opatření, aby se současné hrozby omezily nebo vyrušily a společnost byla připravena i na hrozby budoucí.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem práce je analyzovat současný stav informační bezpečnosti a na jeho základě vytvořit návrh opatření pro eliminaci nebo redukci zjištěných nedostatků. V práci bude popsána první etapa zavádění systému řízení bezpečnosti informací, a to ustanovení ISMS, která poslouží jako předloha pro etapy další.

V práci jsou popsány teoretické základy, poznatky a pojmy problematiky informační bezpečnosti včetně popisu důležitých norem ČSN ISO/IEC řady 27000. Ve druhé části je zjištěn současný stav informační bezpečnosti ve firmě. V první části návrhu je zpracována analýza rizik, kde ohodnotíme informační aktiva a hrozby na ně působící. Na základě dat z analýzy se navrhuje bezpečnostní opatření pro ISMS, které se doporučí firmě k přijetí a následně se odhadnou náklady na vypracování první etapy. Poslední část obsahuje zhodnocení přínosů pro společnost a závěr.

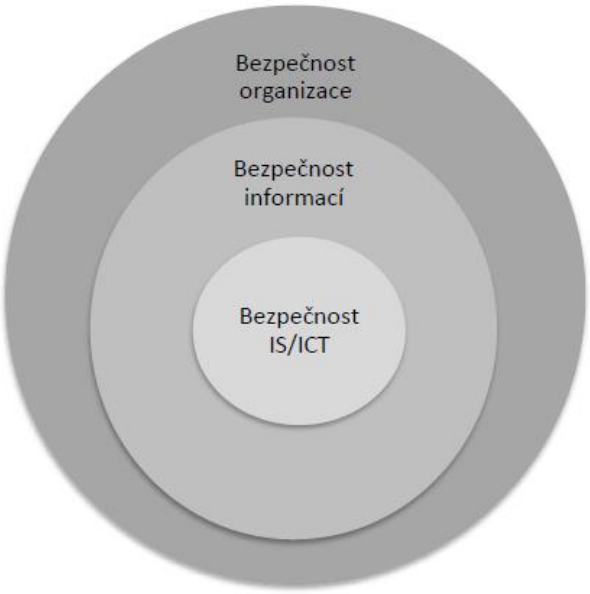
1 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretické části práce jsou vysvětleny základní pojmy a názvosloví z informační bezpečnosti a představeny zákony a normy v oblasti bezpečnosti IT, které souvisí s tématem práce. Na tuto oblast navazuje analýza rizik a bezpečnostní politika a obecná teorie o managementu bezpečnosti informačních systémů.

1.1 Základní pojmy a názvosloví informační bezpečnosti

Tato kapitola definuje základní pojmy a názvosloví, se kterými se při řešení informační bezpečnosti setkáváme.

- *Bezpečnost informací* (Information Security) – spočívá především v ochraně dostupnosti, důvěrnosti a integrity, může však obsahovat i autenticitu, odpovědnost, nepopiratelnost a spolehlivost [1]. Je ve vzájemném vztahu s bezpečností organizace a bezpečností IS/ICT – schéma je vyobrazeno na Obrázek 1
- *Dostupnost* (Availability) – vlastnost dat, kdy jsou informace v požadované době přístupné a pouze oprávněnému uživateli
- *Důvěrnost* (Confidentiality) – přístupnost informací pouze oprávněnému uživateli
- *Integrita* (Integrity) – informace jsou správné a úplné [2]
- *Aktivum* (Asset) – hmotný i nehmotný majetek, který má pro společnost význam a hodnotu
- *Hrozba* (Threat) – možné ohrožení informační bezpečnosti podniku, kdy se využívá zranitelnosti
- *Zranitelnost* (Vulnerability) – slabé místo zabezpečení aktiva
- *Opatření* (Countermeasure) – opatření se zavádějí pro snížení nebo eliminaci hrozeb
- *Riziko* (Risk) – kombinace hrozby a zranitelnosti s dopadem na aktivum
- *Dopad* (Impact) – škoda způsobená v důsledku působení hrozby [2]
- *Bezpečnostní incident* (Security Incident) – proběhlá událost, která vede k narušení pravidel bezpečnosti informací v organizaci



Obrázek 1: Vztah úrovní bezpečnosti v organizaci
Zdroj: [1]

1.2 Zákony a normy v oblasti bezpečnosti IT

Jako pro každou oblast působnosti je i pro bezpečnost informačních systémů a věci s tím souvisejícími v České republice množství zákonů, vyhlášek a předpisů, které ukládají jak s věcmi nakládat, jak je řídit a také ukládají pokuty za nedodržení. Abychom tyto zákony splňovali a i je plnili více, než je ukládáno, můžeme se řídit mezinárodními normami vydávanými organizacemi jako např. ISO (International Organization for Standardization), IEC (International Electrotechnical Comission), IEEE (The Institute of Electrical and Electronics Engineers) apod. Tyto normy jsou jen doporučením pro řešení problematik, avšak je vhodné se jimi řídit, čímž se usnadní mnohé oblasti v řízení bezpečnosti ICT i jiných oblastech.

1.2.1 Legislativa a právní prostředí České republiky

V legislativě České republiky můžeme najít řadu zákonů, které se zabývají nebo mají vliv na otázku bezpečnosti informací nebo informačních systémů. Protože legislativa prostředí bezpečnosti ICT se stále mění, v následujících odstavcích z nich vyberu a velice stručně popíšu pouze několik, které mají souvislost s návrhovou částí této práce.

Zákon č. 101/2000 Sb. – o ochraně osobních údajů – ukládá orgánům (státním i soukromým), právnickým a fyzickým osobám, jak chránit osobní údaje a jak s nimi nakládat

Zákon č. 480/2004 Sb. – o některých službách informační bezpečnosti – *„Tento zákon upravuje v souladu s právem Evropských společenství odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení* [2].

Zákon č. 227/2000 Sb. (101/2010 Sb., 167/2012 Sb.). – o elektronickém podpisu – *Smyslem zákona o elektronickém podpisu je umožnit použití digitálního podpisu v rámci elektronické komunikace jako ekvivalent podpisu vlastnoručního při běžné listinné formě komunikace* [3].

1.2.2 Normy ČSN ISO/IEC řady 27000

Tuto řadu norem vydává Mezinárodní organizace pro normalizaci (ISO) a zabývá se systémy řízení bezpečnosti informací (Information Security Management System – ISMS). Tato řada norem byla zavedena v roce 2005 a poskytuje rámec pro zavedení a řízení ISMS v organizacích všech typů a velikostí. Normy myšlenkově vychází z konceptu PDCA (Plánuj – Dělej – Kontroluj – Jednej) a normy ISO 17799 [1].

ČSN ISO/IEC 27000:2014: *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník* – První norma řady 27000 poskytuje přehled systémů, zavádí pojmy, definice a terminologický slovník systémů řízení bezpečnosti informací **[1]**.

ČSN ISO/IEC 27001:2013: *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky* – Tato norma vychází z normy BS 7799-2, kterou nahradila v říjnu 2005. Norma poskytuje doporučení, jak aplikovat opatření z ISO/IEC 27002 ve všech fázích zavádění ISMS – ustavení, provozu, údržby a zlepšování **[2]**.

ČSN ISO/IEC 27002:2013: *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací* – Norma poskytuje 114 různých oblastí bezpečnosti rozdělených do 13 kapitol, ve kterých je uvedeno mnoho bezpečnostních

opatření. Opatření slouží k dosahování bezpečnostních cílů společnosti, ke kterým je možné přiřadit odpovědnost osobám k tomu vyškoleným [2].

ČSN ISO/IEC 27005:2011: *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací* – Norma poskytuje doporučení pro řízení rizik bezpečnosti informací v organizaci a podporuje implementaci založené na přístupu řízení rizik. Neposkytuje metodiku pro řízení rizik, ale rámec, návod, podle kterého může organizace zvolit přístup, který je pro ni vhodný v závislosti na velikosti společnosti, rozsahu ISMS a dalším. Tato norma je vhodná pro všechny typy organizací, které chtějí řídit rizika **[2]**.

Řada norem 27000 obsahuje mnoho dalších norem, pro další oblasti, např.:

- ČSN ISO/IEC 27003: Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací
- ČSN ISO/IEC 27004: Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření
- ČSN ISO/IEC 27006: Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
- další normy, které nejsou přeloženy z anglického originálu [2]

1.3 Analýza rizik

„Analýza rizik je prováděna za účelem identifikace zranitelných míst informačního systému organizace [2].*“* Je to klíčový dokument, na kterém staví další kroky zavádění systému řízení bezpečnosti informací, proto je přesná znalost rizik důležitá pro následné zavedení vhodných a účinných bezpečnostních opatření. Analýzu můžeme vytvořit čtyřmi různými přístupy – hrubá úroveň, neformální přístup, kombinovaný přístup a podrobný přístup, přičemž poslední jmenovaná je nejdetailnější a zahrnuje hloubkovou revizi v těchto krocích:

- Stanovení hranic revize
- Identifikace aktiv

- Ohodnocení aktiv
- Hodnocení hrozeb
- Odhad zranitelnosti
- Identifikace plánovaných a existujících ochranných opatření
- Výběr ochranných opatření
- Odhad rizik
- Přijetí rizik
- Politika bezpečnosti systému IT
- Plán bezpečnosti IT [2]

Stanovení hranic revize

Jako první krok je potřeba provést stanovení hranic, které nám umožní vyvarovat se provádění zbytečných činností, protože definujeme prvky, kterých se bude analýza rizik týkat [2].

Identifikace aktiv

Aktiva jsou důležité části organizace, mají pro ni hodnotu, a proto organizace požaduje jejich ochranu. Aktiva nemusí být pouze IT charakteru, organizace může definovat vše, co je pro ni cenné [2].

Ohodnocení aktiv

Po identifikaci aktiv následuje jejich ohodnocení. Hodnota aktiva představuje jeho význam (cennost) pro organizaci. Tyto hodnoty jsou definovány vlastníky a uživateli aktiv např. formou dotazníku, rozhovorů nebo nejlepších zkušeností z oboru. Hodnota aktiva není jen otázkou finanční cennosti, ale i například jeho citlivost (např. osobní údaje), křehkost (papírové dokumenty aj.) nebo další hlediska, které mají nepříznivý dopad na organizaci [2].

Hodnocení hrozeb

Hrozba je možnost poškození systému IT a aktiva. Hrozba může být přírodního nebo lidského původu, náhodná nebo úmyslná. Jako základní katalog hrozeb můžeme využít

normu ČSN ISO/IEC 27005, příloha C, která udává příklady typických hrozeb včetně jejich zdroje [4].

Odhad zranitelnosti

Tento odhad odhalí slabá místa ve fyzickém prostředí, organizaci, postupech, personálu, managementu, administraci HW, SW, nebo komunikačním zařízení, která mohou být využita zdrojem hrozby a způsobit tak škodu na aktivech [2].

Identifikace plánovaných a existujících ochranných opatření

Výsledkem identifikace opatření je seznam popisující všechna plánovaná a existující ochranná opatření [2].

Výběr ochranných opatření

Principem ochranných (bezpečnostních) opatření je minimalizace případných rizik. Cíle opatření a jednotlivá opatření jsou popsána v normě ČSN ISO/IEC 27001, podrobný popis je v normě ČSN ISO/IEC 27002. Opatření jsou rozdělena do 13 kategorií:

- Politiky bezpečnosti informací
- Organizace bezpečnosti informací
- Bezpečnost lidských zdrojů
- Řízení aktiv
- Řízení přístupu
- Kryptografie
- Fyzická bezpečnost a bezpečnost prostředí
- Bezpečnost provozu
- Bezpečnost komunikací
- Akvizice, vývoj a údržba systému
- Vztahy s dodavateli
- Řízení incidentů bezpečnosti informací
- Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací
- Soulad s požadavky [5]

Odhad rizik

„Cílem tohoto kroku je identifikovat a odhadnout rizika, kterými jsou aktiva vystavena [2]. Musíme zjistit, co hrozí a proč to hrozí.

Přijetí rizik

Absolutně bezpečný systém neexistuje, proto i po aplikaci opatření na aktiva působí zbytkové riziko. Tato rizika mohou být buď akceptována bez dalších opatření, nebo neakceptována a v tom případě proběhne výběr dalších opatření a odhad rizik. S dalším přijetím rizik však roste riziko vysokých nákladů, které však na bezpečnost nebudou mít téměř vliv [2].

Politika bezpečnosti systému IT

Tato kapitola je více popsána v kapitole 1.6, podnadpis *Prohlášení o politice ISMS.*

Plán bezpečnosti IT

Shrnující dokument, který stručně popisuje všechny akce a činnosti, které se musí uskutečnit před zavedením ochranných opatření [2].

1.4 Oblasti opatření podle ČSN ISO/IEC 27001:2013

„Princip bezpečnostních opatření spočívá v minimalizaci případných rizik [2].

A.5 Politiky bezpečnosti informací

Bezpečnostní politiky jsou pravidla a směrnice v organizaci pro řízení systémů, jejich ochranu a distribuci aktiv včetně citlivých informací. Jsou to základní dokumenty pro veškeré zabezpečení organizace. Zajišťují potřebnou úroveň důvěrnosti, autenticity a integrity informací a zajišťují požadovanou bezpečnost transakcí ve veřejných sítích [2].

A.6 Organizace bezpečnosti informací

Oblast bezpečnosti informací je rozdělena na dvě základní skupiny – interní organizace a mobilní zařízení a práce na dálku. Interní organizace obsahuje 5 opatření, která jsou zaměřená na role a odpovědnosti bezpečnosti informací, oddělení povinností

zaměstnanců, kontakt s příslušnými orgány a autoritami, kontakt se zájmovými skupinami a bezpečnost v řízení projektů. Druhá skupina, mobilní zařízení a práce na dálku, obsahuje 2 opatření – politiku mobilních zařízení a práci na dálku [6].

A.7 Bezpečnost lidských zdrojů

Protože člověk je kritickým a často nejslabším článkem řízení bezpečnosti informací, je tato oblast velmi důležitá. Oblast je zaměřena na životní cyklus pracovníka a dělí se na tři skupiny – před vznikem pracovního vztahu, během pracovního vztahu a ukončení a změna pracovního vztahu. Před vznikem pracovního vztahu je potřeba prověřit uchazeče o zaměstnání podle platných zákonů, předpisů a etiky a na základě pracovního místa, o které se uchazeč zajímá. Uzavření pracovní smlouvy musí obsahovat ustanovení o odpovědnostech zaměstnance a odpovědnostech organizace za bezpečnost informací. Během pracovního vztahu musí vedení organizace požadovat po všech zaměstnancích a smluvních stranách dodržování bezpečnosti informací v souladu s politikami a postupy v organizaci, organizace udržuje povědomí, vzdělává a školí zaměstnance v bezpečnosti informací a v případě přestupku zaměstnance s ním zahájí disciplinární řízení. Ukončení a změna pracovního vztahu nastavuje odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají platné i po ukončení nebo změně pracovního vztahu [6].

A.8 Řízení aktiv

Oblast je rozdělena do 3 skupin – odpovědnost za aktiva, klasifikace informací a manipulace s médii. Odpovědnost za aktiva definuje seznam, vlastnictví, přípustné použití a navrácení aktiv. Klasifikace informací určuje opatření pro klasifikaci a označování informací a manipulaci s aktivy. Manipulace s médii obsahuje správu a přepravu fyzických a výměnných médií a jejich likvidaci [6].

A.9 Řízení přístupu

Řízení přístupu se týká hlavně řízení přístupu k IS/ICT, ale dělí se na 4 skupiny – požadavky organizace na řízení přístupu, řízení přístupu uživatelů, odpovědnosti uživatelů a řízení přístupu k systémům a aplikacím. První skupina, požadavky organizace na řízení přístupu, definuje politiku řízení přístupu a přístup k sítím a

síťovým službám. Řízení přístupu uživatelů ukládá registraci a zrušení registrace uživatele, správu uživatelských přístupů a privilegovaných přístupových práv , správu tajných autentizačních informací uživatelů a přezkoumání, odebrání nebo úpravu přístupových práv uživatelů. Odpovědnost uživatelů vyžaduje používání tajných autentizačních informací a dodržování stanovených postupů při jejich použití. Řízení přístupu k systémům a aplikacím nastavuje omezení přístupu k informacím, definuje bezpečné postupy přihlášení, systém správy hesel, používání privilegovaných programů a řídí přístup ke zdrojovým kódům programů [6].

A.10 Kryptografie

Oblast kryptografie nastavuje politiky pro použití kryptografických opatření a definuje správu kryptografických klíčů [6].

A.11 Fyzická bezpečnost a bezpečnost prostředí

Zabezpečení prostředí organizace ji chrání jako celek – bez zabezpečených oblastí by zavádění dalších bezpečnostních opatření ztrácelo na účinnosti. Dělí se na dvě kategorie – zabezpečení oblastí a zařízení. Zabezpečení oblastí řeší fyzický bezpečnostní perimetr, kontroly vstupu osob, zabezpečení kanceláří, místností a vybavení, ochranu před vnějšími hrozbami a hrozbami prostředí, práci v bezpečných oblastech a oblasti pro nakládku a vykládku. Zabezpečení zařízení řeší umístění zařízení a jeho ochranu, podpůrné služby (např. napájení), bezpečnost kabelových rozvodů, údržbu zařízení, přemístění aktiv, bezpečnost zařízení a aktiv mimo organizaci, likvidaci a opakovaní použití zařízení, uživatelská zařízení bez obsluhy a zásadu prázdného stolu a obrazovky monitoru [6].

A.12 Bezpečnost provozu

Oblast obsahuje 7 skupin opatření pro podporu bezpečného provozu IS/ICT:

- Provozní postupy a odpovědnosti – zajišťují správný a bezpečný provoz vybavení pro zpracování informací, dokumentují provozní postupy, řídí změny a kapacity a oddělují prostředí vývoje, testování a provozu
- Ochrana proti malwaru
- Zálohování

- Zaznamenávání formou logů a monitorování – zaznamenání událostí, ochrana logů, logování činností administrátorů a operátorů a synchronizace hodin
- Správa provozního software - zajišťuje integritu provozních systémů a instalaci softwaru na provozní systémy
- Řízení technických zranitelností – snaží se zabránit využití technických zranitelností jejich řízením a omezením instalace softwaru uživateli
- Hlediska auditu informačních systémů – cílem je minimalizovat dopady auditních činností na provoz systémů [6]

A.13 Bezpečnost komunikací

Obsahuje 2 skupiny – správa bezpečnosti sítě, jejímž cílem je zajištění ochrany informací v sítích a podpůrných prostředcích, přenos informací, který má za cíl zajištění bezpečnosti informací při jejich přenosu. První skupina obsahuje opatření v sítích, bezpečnost síťových služeb a oddělení sítí (skupiny informačních služeb, uživatelů a IS musí být odděleny). Druhá skupina obsahuje politiky a postupy při přenosu informací, dohody i přenosu informací, elektronické předávání zpráv a dohody o utajení nebo mlčenlivosti [6].

A.14 Akvizice, vývoj a údržba systémů

Oblast obsahuje 13 opatření ve 3 skupinách – bezpečnostní požadavky IS, bezpečnost v procesech vývoje a podpory a data pro testování. Bezpečnostní požadavky IS mají za cíl zajistit, aby se bezpečnost informací stala součástí IS v celém jejich životním cyklu. Bezpečnost v procesech vývoje a podpory zaručí, aby bezpečnost informací byla navrhována a implementována do životního cyklu vývoje IS. Data pro testování musí zajistit ochranu dat používaných k testům, jejich kontrolu a pečlivý výběr [6].

A.15 Dodavatelské vztahy

Tato oblast má za cíl ochránit aktiva organizace, ke kterým mají přístup jejich dodavatelé. První skupina ze dvou řeší politiky bezpečnosti a bezpečnostní požadavky pro dodavatelské vztahy a dodavatelská řetězec IS/ICT. Druhý skupina monitoruje,

přezkoumává a řídí změny ve službách dodavatelů s cílem udržet dohodnutou úroveň bezpečnosti informací.

A.16 Řízení incidentů bezpečnosti informací

Cílem je zajištění odpovídajícího a efektivního přístupu ke zvládání bezpečnostních incidentů. Oblast má 7 opatření:

- Odpovědnosti a postupy
- Hlášení událostí bezpečnosti informací
- Hlášení slabých míst bezpečnosti informací
- Posouzení a rozhodnutí o událostech bezpečnosti informací
- Reakce na incidenty bezpečnosti informací
- Ponaučení z incidentů bezpečnosti informací
- Shromažďování důkazů

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

Tato oblast má za úkol zajištění kontinuity bezpečnosti informací a činností organizace v případě bezpečnostního incidentu. Má dvě skupiny – kontinuita bezpečnosti informací a redundance. První skupina obsahuje plánování, implementaci, verifikaci, přezkoumání a vyhodnocení kontinuity bezpečnosti informací, druhá skupina řeší dostupnost redundantního vybavení pro zpracování informací [6].

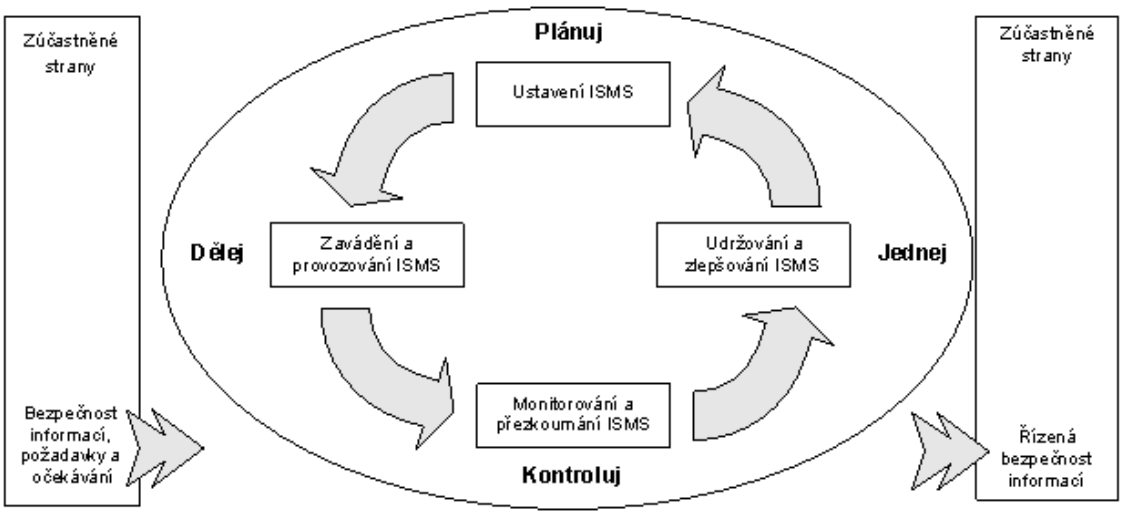
A.18 Soulad s požadavky

Oblast zajišťuje soulad s právními a smluvními požadavky a přezkoumání bezpečnosti informací. Řeší se zde identifikace odpovídající legislativy a smluvních požadavků, ochrana duševního zdraví, záznamům soukromí a osobních údajů, regulace kryptografických opatření, nezávislá přezkoumání bezpečnosti informací a shoda s bezpečnostními politikami a normami a přezkoumání technické shody.

1.5 Management bezpečnosti informačních systémů (ISMS)

Část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací [1]. Podobně jako ostatní modely je i ISMS založeno na modelu PDCA a jsou definovány 4 etapy životního cyklu systému řízení, jak je zachyceno na Obrázek 2:

- Ustanovení ISMS – upřesnění rozsahu a hranic systému řízení bezpečnosti, ohodnocení rizik a výběr nezbytných opatření
- Zavádění a provoz ISMS – prosazení vybraných bezpečnostních opatření do provozu organizace
- Monitorování a přezkoumání ISMS – zpětná vazba a sledování fungujících i nefungujících stránek řízení bezpečnosti informací
- Údržba a zlepšování ISMS – realizace zlepšování systému soustavných zlepšováním nebo odstraňováním zjištěných slabin [1]



Obrázek 2: PDCA model aplikovaný na procesy ISMS
Zdroj: [7]

Norma ČSN ISO/IEC 27001 obsahuje řadu požadavků a v dokumentaci používá výraz „*musí,"* kterým ukazuje závaznost požadavku. Požadavky normy jsou závazné, protože společně utváří celek a pro zajištění shody s touto normou je závazné splnění všech těchto podmínek. Druhá norma, ČSN ISO/IEC 27002, která je souborem postupů,

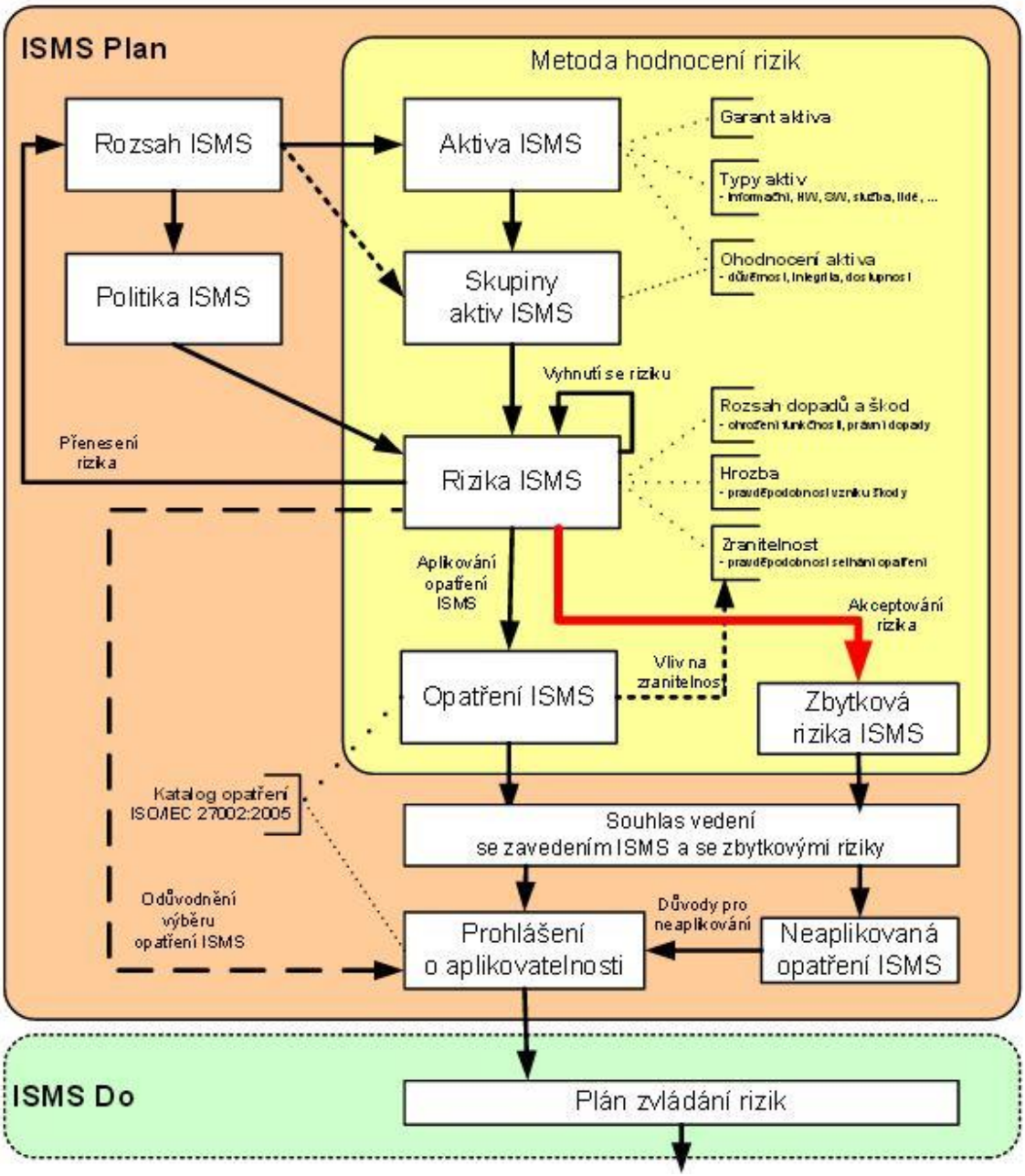
příručkou pro zavádění ISMS, obsahuje výraz *„měl by,“* který značí doporučení a jednotlivé požadavky závazné nejsou [1].

1.6 Ustanovení ISMS

„Cílem této etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření [1]*“.*

Ustanovení je první etapa budování ISMS, jsou zde upřesněny formy řešení bezpečnosti informací. Kromě rozsahu a prohlášení o politice ISMS i analýza rizik a výběr bezpečnostních opatření pro snížení jejich vlivu. Etapa je ukončena souhlasem vedení organizace pro zavedení ISMS a prohlášením o aplikovatelnosti. Přehledný postup ustanovení je zobrazen na Obrázek 3. *„Tato etapa má zásadní dopady na fungování ISMS během jeho celého životního cyklu* [1]*.“* Ustanovení je možné rozdělit do několika činností:

- Definice rozsahu a hranic ISMS
- Prohlášení o politice
- Analýza a zvládání rizik
- Souhlas vedení organizace se zavedením ISMS
- Příprava prohlášení o aplikovatelnosti [1]



Obrázek 3: Přehled činností při ustanovení ISMS
Zdroj: [8]

Definice rozsahu a hranic ISMS

Tato činnost je prvním úkolem při řízení bezpečnosti informací. Na základě činnosti organizace, jejich cílů, organizační struktury apod. se stanoví výchozí rozsah a hranice ISMS, které se však nemusí aplikovat na celou organizaci, ale podle potřeby např. jen na pobočku.

Aplikování na část organizace má výhodu ve vyšším soustředění úsilí na jednotlivou část v porovnání s aplikací ISMS na celou organizaci. Také si můžeme teoretické poznatky vyzkoušet na menším celku a otestovat jejich funkčnost. Při ustanovení se zvládají dva úkoly – obhájení potřebnosti ISMS a zvládnutí všech požadavků. Fungování a kultura organizací je pokaždé jiná a prosazení ISMS může být někdy složité [1].

Prohlášení o politice ISMS

Definice prohlášení o politice ISMS neboli politika ISMS vzniká na základě potřeb organizace a obsahuje:

- Upřesnění cíle ISMS a definice základního směru pro řízení bezpečnosti informací
- Zohlednění cíle a požadavků organizace a související zákonné požadavky
- Potřebné vazby pro vybudování a údržbu ISMS
- Kritéria pro popis a hodnocení rizika
- Schválení vedením organizace

Politika ISMS je krátký, ale důležitý dokument, protože ukazuje zájem vedení společnosti o řízení bezpečnosti informací a stanovuje podmínky pro hodnocení rizik, které jsou základem ISMS. Správná politika může usnadnit budoucí fungování a prosazování pravidel a požadavků na bezpečnost informací [1].

Řízení rizik

Pravidly a postupy řízení rizik se podrobněji zabývá kapitola 1.3.

Prohlášení o aplikovatelnosti

Tento dokument je povinný pro organizace, které usilují o shodu s normou ČSN ISO/IEC 27001. Musí obsahovat cíle opatření a jednotlivá opatření, které byla pro pokrytí rizik vybrána. Dokument je nejčastěji ve formě matice vztahů mezi zjištěnými riziky a vybranými opatřeními. Tato forma je přehledná a je v ní vidět, které opatření jsou aplikována a která jsou vynechána a z jakého důvodu [1].

1.7 Zavádění a provoz ISMS

Druhá etapa životního cyklu ISMS je prosazení bezpečnostních opatření na základě návrhu v předchozí etapě (ustanovení ISMS). Všechna opatření by měla být popsána v příručce bezpečnosti informací a bezpečnostní principy by měly být vysvětleny všem uživatelům. V této etapě se provádí tyto činnosti:

- Plán zvládání rizik a jeho zavedení
- Příručka bezpečnosti informací
- Program budování bezpečnostního povědomí pro všechny uživatele
- Upřesnění způsobu měření účinnosti a sledování stanovených ukazatelů
- Zavedení postupů a opatření pro rychlou detekci a reakci na bezpečnostní incidenty
- Řízení zdrojů, dokumentů a záznamů ISMS [1]

Plán zvládání rizik

Dokument popisuje všechny činnosti, které jsou důležité pro řízení rizik, cíle a priority ISMS, omezující faktory a potřebné zdroje (nejen finanční, ale i personální aj.) V plánu se jednoznačně určí odpovědnosti za prováděné činnosti. Plán vychází především ze dvou zdrojů- výsledků ustanovení ISMS (hodnocení rizik a prohlášení o aplikovatelnosti) a podnětů získaných z přehodnocování ISMS. Je vhodné do plánu začlenit i činnosti, které povedou k postupnému snižování rizik [1].

Příručka bezpečnosti informací

Při prosazování vybraných bezpečnostních opatření je třeba stanovit bezpečnostní pravidla a odpovědnosti. Ty jsou zpracovány ve formě dokumentů, které můžeme rozdělit do tří úrovní důležitosti.

- Povinné podle požadavků ISMS
- Dokumentace sloužící k prosazování ISMS
- Pracovní postupy

Příručka bezpečnosti informací se řadí do kategorie druhé, tedy dokumentace sloužící k prosazování ISMS. *„Důležitým prvkem při tvorbě této dokumentace je definice dílčích*

procesů a postupů, které zajišťují efektivní prosazení dílčích bezpečnostních opatření. Proto je důležité definovat kdo, co, kdy, kde a jak má učinit [1].*“*

Prohlubování bezpečnostního povědomí

Velmi důležitou činností v ISMS je prohlubování bezpečnostního povědomí a tedy promítnutí definovaných pravidel a opatření do každodenních pracovních postupů zaměstnanců. Je to jeden z nejtěžších úkolů a vyžaduje veliké úsilí, protože uživatelé čelí změnám, které se jim ne vždy líbí a protože člověk je nejslabší částí pomyslného řetězce ISMS. Uživatelům je potřeba srozumitelně vysvětlovat bezpečnostní pravidla a rizika, aby byli schopni na ně patřičně reagovat [1].

Měření účinnosti ISMS

Abychom věděli, zda zavedená opatření správně fungují, je nutné zavést měření účinnosti. Objektivní údaje je třeba definovat a pravidelně sledovat informace o fungování systému řízení bezpečnosti informací. Na základě získaných dat se poté budou provádět rozhodnutí o dalších opatřeních [1].

Řízení provozu, zdrojů, dokumentace a záznamů ISMS

Posledním bodem je provádění činností řízeným způsobem. V této části se nejen postupuje podle pravidel, ale shromažďují se i podklady pro další monitorování. Pro kontrolu správnosti fungování ISMS je nutné vytvořit pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace řízení bezpečnosti. Zároveň je nutné vytvářet záznamy o provedených úkonech se základními informacemi o provedené činnosti. Kvalitně vytvořené záznamy umožní snadné dohledání přesně definovaných činností [1].

1.8 Monitorování a přezkoumání ISMS

„Hlavním úkolem této etapy zavádění ISMS je zajistit účinné zpětné vazby [1].*“* V souvislosti s tím dochází i k prověření již zavedených opatření a jejich důsledků na ISMS. To probíhá od kontroly odpovědných osob např. bezpečnostním manažerem až po nezávislé posouzení fungování pomocí interních nebo externích auditů. Obecným cílem je zajistit podklady ohledně fungování ISMS, které se za účelem přezkoumání

souladu s potřebami organizace představí vedení společnosti. V této části se provádí následující činnosti:

- Monitorování a ověření účinnosti bezpečnostních opatření
- Interní audit ISMS
- Zpráva o stavu ISMS [1]

Provádění kontrol

Základní zpětnou vazbou je provádění kontrol ze strany všech osob odpovědných za fungování ISMS. Tyto osoby by měly dohlížet na plnění bezpečnostních požadavků, a zda opatření naplňují očekávání, kterých měla dosáhnout. Součástí je i včasná detekce chyb, úspěšných i neúspěšných pokusů o narušení bezpečnosti nebo sledování událostí a detekce bezpečnostních incidentů – souhrnně označované jako zvládání bezpečnostních incidentů. Další kontrolní činností je vyhodnocení měření účinnosti ISMS a aplikovaných opatření. Výsledky z těchto měření jsou podnětem pro další kontrolu, kterou je přehodnocení ohodnocení rizik [1].

Interní audity

Další zpětnou vazbou je provádění interních auditů ISMS, které poskytují nezávislý pohled na fungování ISMS. Audity by se měly rozložit na celý rozsah ISMS podle cílů, priorit a rizikových oblastí. Řeší dva aspekty – dodržování procesních pravidel (ČSN ISO/IEC 27001) a prověřování fungování jednotlivých bezpečnostních opatření (ČSN ISO/IEC 27002) [1].

Přezkoumání ISMS vedením organizace

„Podněty a připomínky k ISMS, získané při jeho monitorování, jsou důležitými informacemi, které slouží pro objektivní a účinné přezkoumání ISMS vedením organizace [1]. Přezkoumání by mělo probíhat pravidelně podle nastaveného plánu minimálně jednou ročně, u nově zavedených ISMS se může tento interval zkrátit. Vstupem pro přezkoumání jsou všechny podstatné informace o fungování ISMS, a to především:

- Výsledky auditů

- Zpětná vazba uživatelů
- Existující slabiny a hrozby
- Výsledky měření účinnosti ISMS
- Změny ovlivňující ISMS
- Doporučením pro zlepšování

Na základě těchto podnětů se zpracuje SWOT analýza k posouzení silných a slabých stránek ISMS [1].

1.9 Údržba a zlepšování ISMS

Poslední etapou ISMS je jeho udržování a zlepšování. V této fázi dochází ke sběru podnětů ke zlepšení a k nápravě nedostatků. V této části se provádí následující činnosti:

- Zavádění identifikovaných možností zlepšení ISMS
- Provádění opatření k nápravě nedostatků a preventivní opatření [1]

Soustavné zlepšování

Jelikož v praxi dokonalý systém neexistuje, soustavné zlepšování je nutné pro udržení bezpečnosti informací. Důležité je využití pozitivní zpětné vazby pro zlepšení fungování ISMS. Odpovědné osoby zváží dopad řešení a související rizika a podnět poté schválí nebo zamítnou [1].

Odstraňování nedostatků

Odstranění nedostatků probíhá dvěma způsoby – opatření k nápravě a preventivní opatření. Opatření k nápravě je reaktivní forma řešení nedostatku, který se již projevil. Preventivní (proaktivní) opatření je řešení nedostatku, který se ještě neprojevil, ale je jistá možnost, že nastane a může způsobit problémy. Důležitým krokem při odstraňování nedostatků je zjištění příčiny, které k nedostatku vedly, abychom mohli posoudit, zda je opatření relevantní, zamezí opakování a pokryje jeho příčiny. Všechny postupy k nápravě nedostatku jsou zdokumentovány a zaznamenány [1].

2 SOUČASNÝ STAV BEZPEČNOSTI

V této kapitole je analyzován současný stav informační bezpečnosti ve společnosti, na základě kterého se v návrhové části stanoví opatření pro zvýšení bezpečnosti.

2.1 Popis společnosti

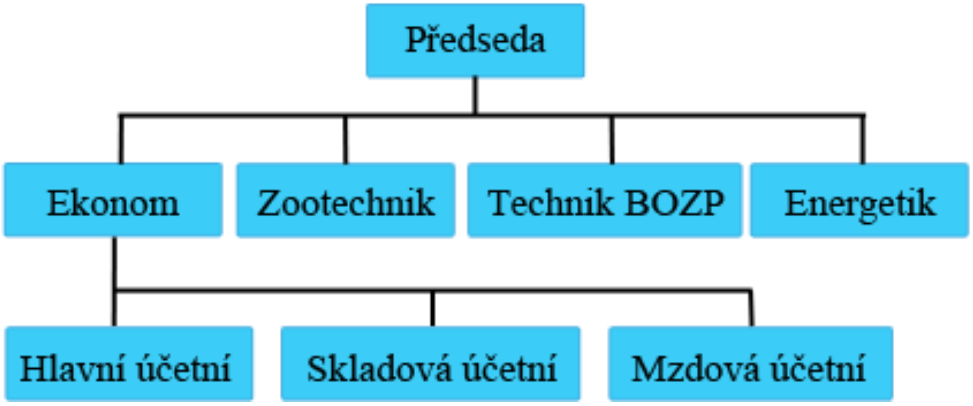
Tato zemědělská společnost sídlí v kraji Vysočina a vznikla na základě původní firmy založené v roce 1956. Společnost se zabývá především prodejem zemědělské rostlinné a živočišné výroby. V současné době zaměstnává 70 pracovníků v několika provozovnách.

2.2 Zabezpečení a poloha objektu

Společnost hospodaří v hornatém kraji Vysočina. Víceúčelová budova, ve které má společnost hlavní kancelářské zázemí, se nachází v malé obci v blízkosti vodních toků. Rozdíl hladiny vody a budovy je několik metrů a je postavena tak, že téměř není možné, aby nárůst hladiny vody ohrozil budovu.

Kanceláře společnosti se nacházejí v nejvyšším, třetím, patře této budovy. Vstup do budovy a jednotlivých pater není kontrolovaný nebo monitorovaný, ve druhém patře se nachází uzamykatelné mříže s kódovým zabezpečením, které se zapíná v době nepřítomnosti zaměstnanců. Neoprávněné vniknutí, případně špatné zadání kódu, se signalizuje hlasitým alarmem. Ve třetím patře má společnost vlastní zamykatelné mříže bez dodatečného zabezpečení.

Prostory jsou rozděleny slabými zděnými příčkami podle oddělení, kde každý zaměstnanec má vlastní kancelář, což odpovídá organizačnímu schématu v budově kanceláří (Obrázek 4).



Obrázek 4: Organizační schéma v budově kanceláří
Zdroj: vlastní zpracování

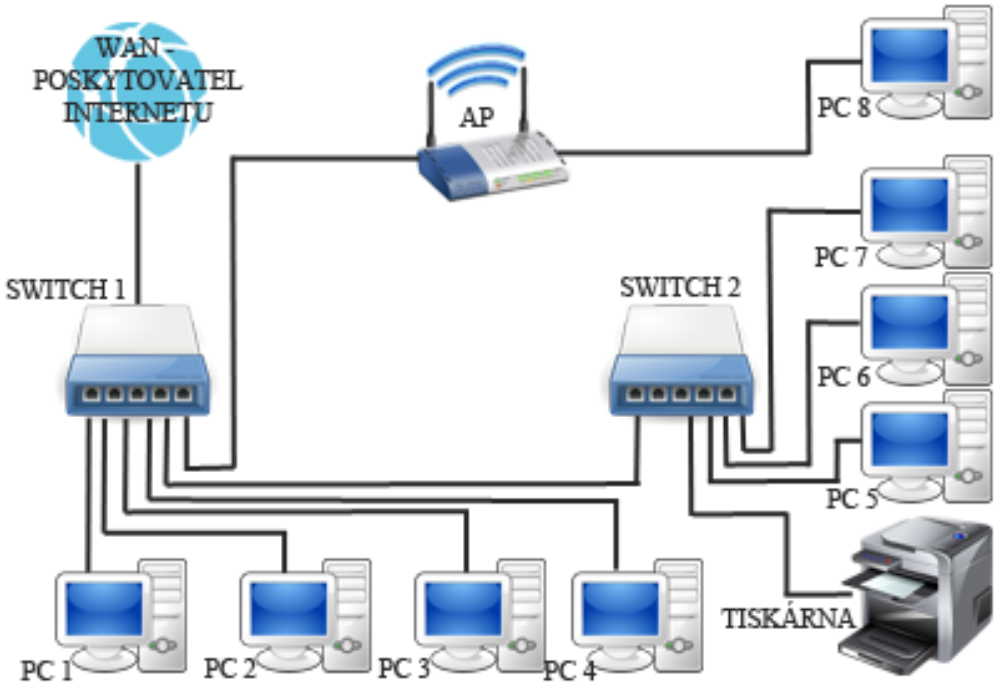
2.3 Bezpečnost ICT

Protože společnost podniká v netechnickém odvětví, informační technologie ve firmě slouží pouze pro usnadnění podpůrných procesů, jako např. vedení účetnictví, část skladové evidence apod. Kultura společnosti je založena na neformálním prostředí s přátelskými vztahy a důvěrou, které také nepomáhá řešení informační bezpečnosti. Z těchto důvodu a z důvodu absence stálé technické podpory je informační bezpečnost na téměř nulové úrovni a pro budoucí fungování je důležité zavedení bezpečnostních pravidel pro práci s informačními aktivy. Protože ve firmě není technická podpora, v případě poškození nebo nefunkčnosti zařízení se volá externí technik, nebo se častěji celé zařízení odveze do servisu, takže firemní data na pevném disku jsou nechráněna.

Zaměstnanci pracují na počítačích typu PC, notebook nebo AiO PC (All-in-One) různých konfigurací a stáří dvou let a více. Většina pracovních stanic má výkon dostačující pro kancelářské využití. Zařízení nejsou mechanicky zabezpečena proti krádeži nebo poškození. U každé pracovní stanice (kromě notebooků, které mají vlastní baterii) je záložní napájecí jednotka UPS, která vydrží napájet zařízení přibližně po dobu 10 až 15 minut, což postačuje pro uložení rozpracovaných materiálů a vypnutí zařízení.

Počítačová síť LAN ve společnosti je vytvořena svépomocí, kabeláž je vedena v elektroinstalačních lištách nebo je pomocí plastových příchytek přibita na zeď. Aktivní prvky nejsou umístěny ve vlastní místnosti a ani v rozvaděči, takže jsou volně přístupné. Ty zahrnují dva osmiportové nespravovatelné komerční přepínače (TP-LINK

TL-SF1008D a Level-One FSW-0507TX) a víceúčelové zařízení (router, přístupový bod, switch, firewall) Zcomax WA-2204A, který pracuje v režimu AP. Aktivní prvky nemají záložní napájení, takže v případě výpadku napájení nebude lokální síť funkční. Nevyužité síťové porty na aktivních prvcích nebo v zásuvkách nejsou klíčované. Schéma současného stavu sítě je na Obrázek 5 níže. V síti je připojeno 8 počítačů a jedno multifunkční zařízení (tiskárna), které je pro úsporu nákladů sdílené pro všechny kanceláře. Každé oddělení (= každý zaměstnanec) má vlastní počítač.



Obrázek 5: Logické schéma zapojení stávající sítě
Zdroj: vlastní zpracování

Zabezpečení lokální sítě není na žádné úrovni řešeno. Router/AP (které je v síti zapojeno) má i funkci firewall, ale protože konektivita od poskytovatele internetu je přivedena nejdříve do přepínače (SWITCH 1) a až poté do AP, nastavení pravidel by omezilo pouze uživatele WiFi a počítače připojené k tomuto zařízení, ne celou síť. Na AP je nastavena bezdrátová síť se jménem společnosti se zabezpečením WPA2 s AES šifrováním a se sdíleným klíčem (PSK). Klíč k síti se nemění, od prvotního nastavení je stejný. Protože síťové IP adresy přiřazuje DHCP server poskytovatele internetu všem připojeným zařízením automaticky a v síti není zařízení pro oddělení provozu (firewall), po připojení do sítě LAN nebo WLAN získáme přístup nejen na internet, ale i do celé lokální sítě a ke sdíleným souborům.

Z hlediska softwarového zabezpečení koncových stanic je na tom společnost o trochu lépe. Ochranu proti škodlivým kódům zajišťuje antivirový program AVG v různých verzích s denně aktualizovanou virovou databází v kombinaci s personálním firewallem Windows Firewall. Informační systémy pro účetnictví, skladové hospodářství apod. jsou udržované na aktuální verzi, ostatní programy jsou zpravidla kvůli chybějící počítačové podpoře neaktualizované.

Přihlášení k uživatelským profilům operačního systému Windows není podmíněné zadáním hesla nebo jinou autentizací a účty jsou typu *administrator*, takže každý uživatel má neomezený přístup k nastavení a souborům v počítači. Jako operační systém se využívá Microsoft Windows 7 ve verzi Home Edition. Tato verze není určena pro nasazení do firemního prostředí, proto jí chybí některé důležité funkce, např. možnost připojení účtu do domény nebo zálohování na síťové uložiště.

Nejdůležitější data a dokumenty jsou zálohována na externí pevné disky nebo flash disky nebo nejsou zálohována vůbec. Zálohovací média mají zaměstnanci umístěné na pracovním stole a zálohy provádí manuálně a v náhodný čas. Zálohovací média, zálohy ani pevné disky v počítačích nejsou šifrované.

Veškeré papírové dokumenty, které jsou zvlášť zranitelné, jsou uloženy v šanonech ve skříních nebo policích v kancelářích jednotlivých oddělení, část z nich je dostupná i v digitální podobě. Dokumentů je velké množství a část z nich je nenahraditelná.

2.4 Zhodnocení současného stavu

Z předchozí analýzy je jasné, že ve společnosti neexistuje řízení informační bezpečnosti a povědomí o možných incidentech. U všech úrovní zabezpečení je nutné zavést opatření pro zamezení zranitelnosti dat, uživatelů a společnosti. Mezi největší nedostatky patří zálohování, ochrana a správa sítě a informační vzdělanost uživatelů. Ti mohou kvůli nedostatku znalostí a neomezenému přístupu ke všem datům a v síti snadno poškodit nebo smazat důležitá data. V návrhové části na základě zjištěných problémů navrhneme opatření a nastavíme bezpečnostní pravidla pro užívání informačních technologií tak, aby se zjištěné nedostatky eliminovaly nebo snížily na úroveň, která nepředstavuje pro společnost ohrožení.

3 NÁVRH USTANOVENÍ ISMS

V předchozí části jsme zhodnotili současné řešení informační bezpečnosti a analyzovali hrozby, zranitelnosti, rizika a nejdůležitější aktiva společnosti. V návrhové části je cílem připravit takové řešení informační bezpečnosti, aby řešilo zjištěné nedostatky a dalším předcházelo nebo na ně dokázalo rychle reagovat. Společnost neuvažuje o certifikaci podle normy ČSN ISO/IEC 27001:2013, ale při řešení informační bezpečnosti se z této normy bude vycházet, aby společnost měla kvalitně nastavená pravidla pro bezpečnost a byla tak chráněná proti napadení útočníkem nebo měla plán pro případ nenadálých událostí a ochránila tak svá aktiva. Ustanovení je první etapa zavádění ISMS. Jsou zde definovány klíčové prvky, které mají vliv na realizaci.

3.1 Rozsah ISMS

Přestože společnost neplánuje certifikaci, kvůli současnému stavu informační bezpečnosti se rozsah opatření bude řídit normami řady ČSN ISO/IEC 27000. Systém nebude aplikován na celý podnik, ale především na kancelářské zázemí, kde sídlí celé vedení společnosti a jednotlivá oddělení a přínos tohoto řešení bude nejvyšší. Při zavedení systému ISMS na celý podnik by náklady byly mnohem vyšší a přínos by neodpovídal vynaloženým prostředkům.

3.1.1 Identifikace a ohodnocení informačních aktiv

Tabulka 1: Stupnice hodnocení aktiv
Zdroj: vlastní zpracování

Hodnota aktiva	Popis
1 - Velmi nízká	Aktivum má zanedbatelnou či žádnou důležitost pro společnost
2 - Nízká	Aktivum s nízkou důležitostí; malý dopad na organizaci
3 - Střední	Aktivum se střední důležitostí; při poškození či ztrátě hrozí potíže či menší finanční ztrátu společnosti; je nahraditelné
4 - Vysoká	Důležité aktivum; při poškození hrozí vážné potíže či střední finanční ztráta společnosti; obtížně nahraditelné
5 - Velmi vysoká	Velmi důležité aktivum; vysoká finanční ztráta; až existenční potíže pro společnost; velmi obtížně nahraditelné nebo nenahraditelné

Tabulka 2: Hodnocení aktiv
Zdroj: vlastní zpracování

	Aktivum	Hodnota
1.	Firemní účetnictví	5
2.	Dokumenty v papírové podobě	5
3.	Zálohy	4
4.	Informační systémy	4
5.	Smlouvy	4
6.	Projektové dokumentace	3
7.	Tiskárna	2
8.	Pracovní stanice	2
9.	Aktivní síťové prvky	2
10.	Operační systém	1
11.	Programové vybavení	1

Všechna identifikovaná aktiva budou obsažena v návrhu ISMS. Aktiva doposud nemají jednoznačného vlastníka a jsou využívána a rozprostřena po celém podniku. Zodpovědnost je určena pouze u aktiva 1, kde je zodpovědná hlavní účetní. Papírové dokumenty i smlouvy má každé oddělení a není tedy určena jednoznačná odpovědnost.

3.2 Politika ISMS

Základní dokument obsahující podrobnosti požadovaných ochranných opatření a jejich popis. Je to rozsahem krátký, ale důležitý dokument, protože prezentuje zájem vedení společnosti, a to dává na vědomí, že chápe význam zavedení tohoto systému a že je připraveno uvolnit potřebné zdroje k jejímu uskutečnění. Správně definovaná politika usnadní budoucí prosazování změn, pravidel a požadavků ISMS. Dokument obsahuje tyto zásady:

- Podnik klade důraz na bezpečnost informací, jejich ochranu v souladu se zákony a požadavky zainteresovaných stran

- Základem bezpečnosti informací je spolehlivý a účinný ISMS a společnost zajistí jeho udržování a bezpečné nakládání s daty
- ISMS je součástí řídících činností společnosti a jeho cílem je eliminovat nebo snížit rizika, která na ni působí
- Systém je vybudován v souladu s normou ČSN ISO/IEC 27001:2013
- Společnost bude hodnotit plnění cílů vycházejících z politiky ISMS a analýzy rizik
- Společnost bude uplatňovat zásady informací bezpečnosti vůči všem zaměstnancům a zainteresovaným stranám

Cílem bezpečnosti informací ve společnosti je zajištění přiměřené ochrany informací, které společnost využívá, a neoprávněné manipulace s daty.

3.3 Analýza rizik

Analýza rizik je základní a důležitý dokument pro zpracování návrhu řízení bezpečnosti informací. Z analýzy vychází a čerpá samotný návrh tak, aby se redukovala nebo úplně vyloučila zjištěná rizika. Analýza rizik je zpracována v souladu s metodikou normy ČSN ISO/IEC 27005:2011 zabývající se řízením rizik bezpečnosti informací a obsahuje identifikaci hrozeb a zranitelností a matici zranitelnosti a rizika.

3.3.1 Identifikace hrozeb

Identifikace hrozeb a zranitelností proběhla na základě konzultace se zastupiteli společnosti a dále vychází z přílohy C normy ČSN ISO/IEC 27005:2011, která uvádí příklady typických úmyslných, náhodných, živelných nebo jiných hrozeb. Z přílohy jsou vybrány pouze relevantní hrozby, které mohou omezit chod společnosti. Dále vychází z přílohy D, která uvádí příklady zranitelností.

Tabulka 3: Stupnice hodnocení pravděpodobnosti hrozby
Zdroj: vlastní zpracování

Pravděpodobnost hrozby	Význam hrozby
1 – Velmi malá	Velmi malý až nulový dopad
2 – Malá	Malý dopad
3 – Střední	Střední dopad
4 – Velká	Velký dopad
5 – Velmi velká	Velmi velký dopad

Tabulka 4: Identifikace hrozeb a zranitelností
Zdroj: vlastní zpracování podle **[4]**

Hrozba	Pravděpodobnost	Příklad zranitelnosti
Fyzické poškození		
Požár	2	Závada elektroinstalace
Poškození vodou	1	Závada vodoinstalace
Přepětí v síti	2	Zásah blesku
Selhání hardware	3	Stáří součástky, poškození
Zničení médií nebo zařízení	2	Neodborná manipulace
Chyba údržby	4	Nedostatečné školení
Dostupnost služeb		
Porucha sítě LAN nebo WAN	3	Závada u poskytovatele
Výpadek elektřiny	3	Porucha el. vedení
Selhání komunikace	1	Nedostatečná ochrana
Ohrožení informací		
Krádež médií nebo dokumentů	1	Nízké zabezpečení objektu a pracovních stanic
Krádež zařízení	1	Slabé zabezpečení objektu
Škodlivé programy	4	Neaktualizovaný antivirový program
Ohrožení funkčnosti		
Poškození uživatelem	5	Nedostatečné školení
Selhání software	3	Napadení škodlivým programem

3.3.2 Metody analýzy rizik

Analýza rizik bude vypracována podle dvou základních metod, a to maticová metoda a metoda pomocí pravděpodobnosti incidentu a jeho dopadu.

Maticová metoda analýzy rizik

Prvním ze základních přístupů k analýze rizik je analýza využívající tři parametry - aktivum, hrozba a zranitelnost. Matice zranitelnosti se vytvoří spojením tabulky hodnocení aktiv (Tabulka 2) a tabulky hrozeb a zranitelností (Tabulka 4). Poté se jednotlivé zranitelnosti aktiv posoudí a doplní do matice. Poté se pomocí vzorce $R = T * A * V$ vypočítá míra rizika a zanese se do nové matice rizik a podle stanovených hranic rizika se stanoví jeho závažnost. Matice zranitelností je zobrazena v Tabulka 5.

Tabulka 5: Matice zranitelností
Zdroj: vlastní zpracování

	V zranitelnost	*Popis aktiva*	Účetnictví	Zálohy	Papírové dokumenty	Projektové dokumentace	Smlouvy	IS	Tiskárna	PC	Síťové prvky	OS	Programy
		A *hodnota aktiva*	5	4	5	3	4	4	2	2	2	1	1
	Popis hrozby	**T** *pravděpo-dobnost*											
Fyzické poškození	Požár	2	5	5	5	5	5	5	5	5	5	5	5
	Poškození vodou	1	5	5	5	5	5	5	5	5	5	5	5
	Přepětí v síti	2							5	4	5		
	Selhání hardware	3		5					3	4	5		
	Zničení médií nebo zařízení	2	2	5	5	3	5	2	2	2	5	1	1
	Chyba údržby	4	1	5	3	3	3	3	2	3	4	2	2
Dostupnost Matice služeb	Porucha sítě LAN nebo WAN	3		3					1	1	2		
	Výpadek elektřiny	3	2	3		1		2	1	1	1	2	2
	Selhání komunikace	1	3	3				3	1	1	2	2	2
Ohrožení informací	Krádež médií nebo dokumentů	1	5	5	5	5	5	4					
	Krádež zařízení	1		5		5			3	4	4		
	Škodlivé programy	4	5	5		3		5		3	5	5	5
Ohrožení funkčnosti	Poškození uživatelem	4	4	5	3	2	3	5	2	4	5	3	3
	Selhání software	3	5	5		2		5		1	2	5	5

Pro vypracování matice rizik si musíme stanovit hranice pro hodnocení rizik – bezvýznamné, nízké, střední a vysoké riziko.

Tabulka 6: Hodnocení rizik
Zdroj: vlastní zpracování podle [2]

Označení	**Riziko**	**Hranice rizika**
	Bezvýznamné	0 - 10
	Nízké	11 - 30
	Střední	31 - 60
	Velké	61 - 125

Následně můžeme zpracovat matici rizik, ze které vidíme, že největší riziko představuje poškození uživatelem (ať úmyslné nebo neúmyslné) a napadení škodlivým programem.

Tabulka 7: Matice rizik
Zdroj: vlastní zpracování

	R riziko	*Popis aktiva*	Účetnictví	Zálohy	Papírové dokumenty	Projektové dokumentace	Smlouvy	IS	Tiskárna	PC	Síťové prvky	OS	Programy
		A *hodnota aktiva*	5	4	5	3	4	4	2	2	2	1	1
	Popis hrozby	**T** *pravděpo-dobnost*											
Fyzické poškození	Požár	2	50	40	50	30	40	40	20	20	20	10	10
	Poškození vodou	1	25	20	25	15	20	20	10	10	10	5	5
	Přepětí v síti	2	0	0	0	0	0	0	20	16	20	0	0
	Selhání hardware	3	0	60	0	0	0	0	18	24	30	0	0
	Zničení médií nebo zařízení	2	20	40	50	18	40	16	8	8	20	2	2
	Chyba údržby	4	20	**80**	60	36	48	48	16	24	32	8	8
Dostupnost služeb	Porucha sítě LAN nebo WAN	3	0	36	0	0	0	0	6	6	12	0	0
	Výpadek elektřiny	3	30	36	0	9	0	24	6	6	6	6	6
	Selhání komunikace	1	15	12	0	0	0	12	2	2	4	2	2
Ohrožení informací	Krádež médií nebo dokumentů	1	25	20	25	15	20	16	0	0	0	0	0
	Krádež zařízení	1	0	20	0	15	0	0	6	8	8	0	0
	Škodlivé programy	4	**100**	**80**	0	36	0	**80**	0	24	40	20	20
Ohrožení funkčnosti	Poškození uživatelem	4	**80**	**80**	60	24	48	**80**	16	32	40	12	12
	Selhání software	3	**75**	60	0	18	0	60	0	6	12	15	15

Analýza rizik pomocí pravděpodobnosti incidentu a jeho dopadu

Druhým přístupem k analýze rizika je vyhodnocení pravděpodobnosti incidentu a jeho dopadu. Tato metoda má parametry pouze dva - pravděpodobnost a dopad incidentu. K již vytvořené tabulce hrozeb a zranitelností se doplní existující opatření a odhadne se pravděpodobnost incidentu. Parametr *dopad* využívá z již vytvořené tabulky aktiv

parametry *hodnota* (viz Tabulka 2). Výpočet míry rizika se provede vztahem $R = PI * D$, kde R je riziko, PI pravděpodobnost incidentu a D dopad. Protože jsme rizika ohodnotili už metodou se třemi parametry, analýzu touto metodou nepoužijeme.

3.4 Soubor opatření podle ČSN ISO/IEC 27001:2013

Tabulka 8: Soubor bezpečnostních opatření podle ČSN ISO/IEC 27001:2013 příloha A
Zdroj: Upraveno dle [6]

Označení	Opatření	Stav
A.5 Politiky bezpečnosti informací		
A.5.1 Směřování bezpečnosti informací vedením organizace		
A.5.1.1	Politiky pro bezpečnost informací	zavést
A.5.1.2	Přezkoumání politik pro bezpečnost informací	zavést
A.6 Organizace bezpečnosti informací		
A.6.1 Interní organizace		
A.6.1.1	Role a odpovědnosti bezpečnosti informací	zavést
A.6.1.2	Princip oddělení povinností	zavést
A.6.1.3	Kontakt s příslušnými orgány a autoritami	zavedeno
A.6.1.4	Kontakt se zájmovými skupinami	x
A.6.1.5	Bezpečnost informací v řízení projektů	zavést
A.6.2 Mobilní zařízení a práce na dálku		
A.6.2.1	Politika mobilních zařízení	zavést
A.6.2.2	Práce na dálku	x
A.7 Bezpečnost lidských zdrojů		
A.7.1 Před vznikem pracovního vztahu		
A7.1.1	Prověřování	aktualizovat
A7.1.2	Podmínky pracovního vztahu	aktualizovat
A.7.2 Během pracovního vztahu		
A.7.2.1	Odpovědnosti vedení organizace	aktualizovat
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	zavést
A.7.2.3	Disciplinární řízení	zavést
A.7.3 Ukončení a změna pracovního vztahu		
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	aktualizovat
A.8 Řízení aktiv		
A.8.1 Odpovědnost za aktiva		
A.8.1.1	Seznam aktiv	zavést
A.8.1.2	Vlastnictví aktiv	zavést
A.8.1.3	Přípustné použití aktiv	zavést
A.8.1.4	Navrácení aktiv	zavedeno
A.8.2 Klasifikace informací		
A.8.2.1	Klasifikace informací	aktualizovat

A.8.2.2	Označování informací	zavést
A.8.2.3	Manipulace s aktivy	zavést
A.8.3 Manipulace s médii		
A.8.3.1	Správa výměnných médií	zavést
A.8.3.2	Likvidace médií	zavést
A.8.3.3	Přeprava fyzických médií	zavést
A.9 Řízení přístupu		
A.9.1 Požadavky organizace na řízení přístupu		
A.9.1.1	Politika řízení přístupu	zavést
A.9.1.2	Přístup k sítím a síťovým službám	aktualizovat
A.9.2 Řízení přístupu uživatelů		
A.9.2.1	Registrace a zrušení registrace uživatele	zavést
A.9.2.2	Správa uživatelských přístupů	zavést
A.9.2.3	Správa privilegovaných přístupových práv	zavést
A.9.2.4	Správa tajných autentizačních informací uživatelů	zavést
A.9.2.5	Přezkoumání přístupových práv uživatelů	zavést
A.9.2.6	Odebrání nebo úprava přístupových práv	zavést
A.9.3 Odpovědnosti uživatelů		
A.9.3.1	Používání tajných autentizačních informací	x
A.9.4 Řízení přístupu k systémům a aplikacím		
A.9.4.1	Omezení přístupu k informacím	zavést
A.9.4.2	Bezpečné postupy přihlášení	zavést
A.9.4.3	Systém správy hesel	zavést
A.9.4.4	Použití privilegovaných programových nástrojů	x
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	x
A.10 Kryptografie		
A.10.1 Kryptografická opatření		
A.10.1.1	Politika pro použití kryptografických opatření	x
A.10.1.2	Správa klíčů	x
A.11 Fyzická bezpečnost a bezpečnost prostředí		
A.11.1 Bezpečné oblasti		
A.11.1.1	Fyzický bezpečnostní perimetr	aktualizovat
A.11.1.2	Fyzické kontroly vstupu	zavést
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	aktualizovat
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	zavedeno
A.11.1.5	Práce v bezpečných oblastech	x
A.11.1.6	Oblasti pro nakládku a vykládku	x
A.11.2 Zařízení		
A.11.2.1	Umístění zařízení a jeho ochrana	zavést
A.11.2.2	Podpůrné služby	aktualizovat
A.11.2.3	Bezpečnost kabelových rozvodů	zavedeno
A.11.2.4	Údržba zařízení	aktualizovat
A.11.2.5	Přemístění aktiv	zavedeno

A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	x
A.11.2.7	Bezpečná likvidace nebo opakované použití	zavést
A.11.2.8	Uživatelská zařízení bez obsluhy	zavést
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	zavést
A.12 Bezpečnost provozu		
A.12.1 Provozní postupy a odpovědnosti		
A.12.1.1	Dokumentované provozní postupy	zavést
A.12.1.2	Řízení změn	zavést
A.12.1.3	Řízení kapacit	zavést
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	x
A.12.2 Ochrana proti malwaru		
A.12.2.1	Opatření proti malwaru	zavedeno
A.12.3 Zálohování		
A.12.3.1	Zálohování informací	zavést
A.12.4 Zaznamenávání formou logů a monitorování		
A.12.4.1	Zaznamenávání událostí formou logů	zavést
A.12.4.2	Ochrana logů	zavést
A.12.4.3	Logy o činnosti administrátorů a operátorů	zavést
A.12.4.4	Synchronizace hodin	zavést
A.12.5 Správa provozního softwaru		
A.12.5.1	Instalace softwaru na provozní systémy	zavést
A.12.6 Řízení technických zranitelností		
A.12.6.1	Řízení technických zranitelností	zavést
A.12.6.2	Omezení instalace software	zavést
A.12.7 Hlediska auditu informačních systémů		
A.12.7.1	Opatření k auditu informačních systémů	x
A.13 Bezpečnost komunikací		
A.13.1 Správa bezpečnosti sítě		
A.13.1.1	Opatření v sítích	zavést
A.13.1.2	Bezpečnost síťových služeb	zavést
A.13.1.3	Princip oddělení v sítích	zavést
A.13.2 Přenos informací		
A.13.2.1	Politiky a postupy při přenosu informací	zavést
A.13.2.2	Dohody o přenosu informací	x
A.13.2.3	Elektronické předávání zpráv	aktualizovat
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	x
A.14 Akvizice, vývoj a údržba systémů		
A.14.1 Bezpečností požadavky informačních systémů		
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	aktualizovat
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	zavedeno
A.14.1.3	Ochrana transakcí aplikačních služeb	zavedeno
A.14.2 Bezpečnost v procesech vývoje a podpory		
A.14.2.1	Politika bezpečného vývoje	x

A.14.2.2	Postupy řízení změn systémů	x
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	zavést
A.14.2.4	Omezení změn softwarových balíků	x
A.14.2.5	Principy budování bezpečných systémů	x
A.14.2.6	Prostředí bezpečného vývoje	x
A.14.2.7	Outsourcovaný vývoj	x
A.14.2.8	Testování bezpečnosti systémů	x
A.14.2.9	Testování akceptace systémů	zavést
A.14.3 Data pro testování		
A.14.3.1	Ochrana dat pro testování	x
A.15 Dodavatelské vztahy		
A.15.1 Bezpečnost informací v dodavatelských vztazích		
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	x
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	zavést
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	zavést
A.15.2 Řízení dodávek služeb dodavatelů		
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	zavést
A.15.2.2	Řízení změn ve službách dodavatelů	zavést
A.16 Řízení incidentů bezpečnosti informací		
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování		
A.16.1.1	Odpovědnosti a postupy	zavést
A.16.1.2	Hlášení událostí bezpečnosti informací	aktualizovat
A.16.1.3	Hlášení slabých míst bezpečnosti informací	aktualizovat
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	zavést
A.16.1.5	Reakce na incidenty bezpečnosti informací	zavést
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	aktualizovat
A.16.1.7	Shromažďování důkazů	zavést
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací		
A.17.1 Kontinuita bezpečnosti informací		
A.17.1.1	Plánování kontinuity bezpečnosti informací	zavést
A.17.1.2	Implementace kontinuity bezpečnosti informací	zavést
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	zavést
A.17.2 Redundance		
A.17.2.1	Dostupnost vybavení pro zpracování informací	zavést
A.18 Soulad s požadavky		
A.18.1 Soulad s právními a smluvními požadavky		
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	zavedeno
A.18.1.2	Ochrana duševního vlastnictví	zavedeno
A.18.1.3	Ochrana záznamů	aktualizovat
A.18.1.4	Soukromí a ochrana osobních údajů	zavedeno
A.18.1.5	Regulace kryptografických opatření	x
A.18.2 Přezkoumání bezpečnosti informací		

A.18.2.1	Nezávislá přezkoumáni bezpečnosti informací	x
A.18.2.2	Shoda s bezpečnostními politikami a normami	x
A.18.2.3	Přezkoumání technické shody	x

Soubor opatření obsahuje celkem 114 jednotlivých opatření rozdělených do 13 oblastí. Společnost má v současné době 11 opatření zavedených, 16 je potřeba aktualizovat, 60 nezavedených a 27 společnost nebude zavádět.

3.5 Plán zavedení opatření

Protože podnik nemá stálé IT zaměstnance a podpora se musí řešit externě, bude vhodné rozdělit opatření, která budou zaváděna nebo aktualizována, do několika fází. Rozdělení se provede také z důvodu, aby nedošlo k narušení firemních procesů - pro zaměstnance, kteří mají pouze základní IT znalosti, bude změna zavedených a naučených postupů složitá a při příliš náročné změně by mohlo docházet k chybám zaměstnanců a snížené produktivitě práce.

Rozdělení opatření proběhne na 3 časové etapy podle následujícího rozdělení:

- *Etapa I* – září 2016 – leden 2017 – zajištění IT správce a manažera bezpečnosti, úprava aktivních prvků a síťové infrastruktury, instalace OS a software, nastavení přístupových práv, opatření A.5 Politiky bezpečnosti informací, A.6 Organizace bezpečnosti informací, A.7 Bezpečnost lidských zdrojů, A.8 Řízení aktiv, A.11 Fyzická bezpečnost a bezpečnost prostředí
- *Etapa II* – únor 2017 – červenec 2017 – opatření A.9 Řízení přístupu, A.12 Bezpečnost provozu, A.13 Bezpečnost komunikací
- *Etapa III* – srpen 2017 – prosinec 2017 - A.14 Akvizice, vývoj a údržba systémů, A.15 Dodavatelské vztahy, A.16 Řízení incidentů bezpečnosti informací, A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací, A.18 Soulad s požadavky

3.6 Úpravy lokální sítě a software

Před zahájením opatření musí společnost provést několik změn v lokální síti a správě software, aby zavedení systému řízení bezpečnosti mělo smysl. Pokud by lokální síť a

stav software zůstal v současném stavu, zavádění ISMS by nebylo účinné, protože zde nejsou nastavena ani nejzákladnější pravidla bezpečnosti. V následující části stručně popíši úpravy, které by se měly provést. Aby společnost měla síť kvalitně provedenou, měla by si najmout externí firmu, aby síť zpracovala. Při výběru kvalitní firmy a dobře nastavenému zadání se zaručí kvalitní návrh a zpracování tak, aby síť odpovídala normám.

3.6.1 Úprava lokální sítě

Prvním krokem úprav jsou změny v prostředí lokální sítě. Tyto změny nastaví základy pro vyšší vrstvy bezpečnosti a ISMS. Do sítě budou zapojeny nové aktivní a jiné prvky, nastavena pravidla provozu a přístupu do sítě WAN i LAN. Společnost vyčlenila 100 000 Kč na výstavbu nové sítě a využije se externí firmy, která návrh a instalaci provede. Výběr externí firmy se nesmí řídit nejnižší cenou, ale kvalitou a službami společnosti. Společnost připravila následující zadání:

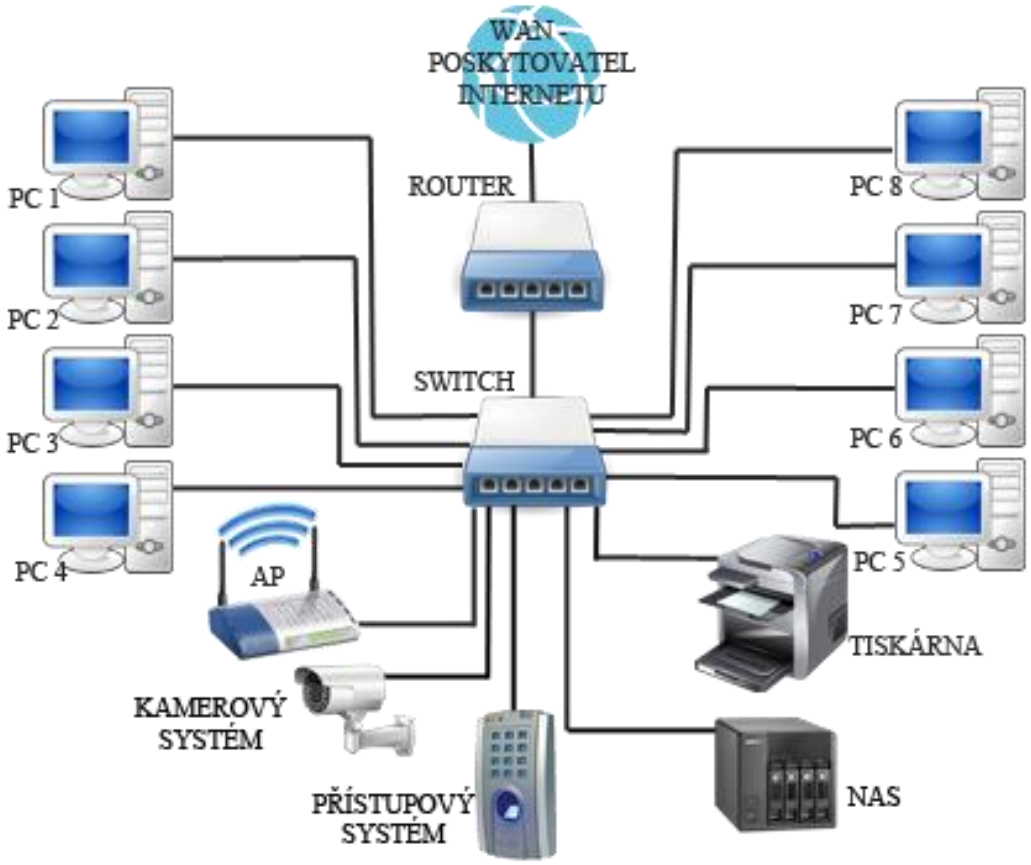
Bezpečnostní prvky

Dodavatel podle zadání dodá kamerový a přístupový systém, na toto zabezpečení společnost vyčlenila 55 000 Kč. Kamerový systém bude obsahovat dvě kamery, obě namířené na vstup do kanceláří (schodiště). Jedna kamera bude umístěna na schodech (až za vstupní mříží), druhá kamera na chodbě namířená na schodiště, jak je zobrazeno v Příloha 3, záznamový systém v datovém rozvaděči. Přístupový systém bude mít snímač v mezipatře schodiště a bude otevírat vstupní mříže.

Topologie

Stávající zapojení aktivních prvků (Obrázek 5) bude zjednodušeno do topologie hvězda s jedním centrálním uzlem, což usnadní správu a uložení prvků, protože aktivní prvky budou uloženy v novém rozvaděči. Společnost není závislá na lokální síti nebo přístupu na internet a výpadek i v řádu hodin nezpůsobí společnosti problémy, tak pro společnost není důležité redundantní zapojení aktivních prvků.

Návrh logického uspořádání:



Obrázek 6: Logické schéma zapojení nové sítě
Zdroj: vlastní zpracování

Uložení kabeláže

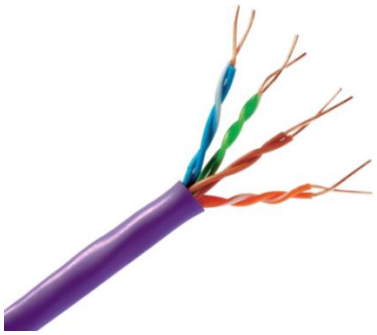
V zadání pro zpracování kabeláže má společnost požadavek na co nejmenší zásahy do zdí. Z toho důvodu chce vedení kabeláže uložené v plastových elektroinstalačních profilech. Příklad takové lišty je na Obrázek 7.

Obrázek 7: Příklad plastových elektroinstalačních profilů
Zdroj: [9]

Pokud to bude možné, trasa kabeláže by měla kopírovat původní trasy kabeláže. Obrázek původního vedení kabeláže a požadovaných nových zásuvek se nachází v Příloha 3.

Strukturovaná kabeláž

Na firemní síti není velký provoz, ale z budoucích důvodů má společnost v zadání kabeláž schopnou rychlosti Gigabit Ethernet. V blízkosti se nenachází žádné zdroje rušení, proto postačí nestíněná kabeláž, ale protože to bude v interiéru, je požadavek na kabel s pláštěm typu LS0H (Low Smoke Zero Halogen), který je vhodný do vnitřního prostředí, protože při hoření produkuje méně kouře a škodlivých halogenů. Z důvodu vysoké kvality společnost požaduje použít kabeláž a další prvky strukturované kabeláže od výrobce Belden nebo Panduit.



Obrázek 8: UTP kabel Belden
Zdroj: [10]

Společnost v zadání specifikuje, aby v každé kanceláři byla jedna zásuvka se dvěma porty a v zasedacích místnostech dvě zásuvky po dvou portech. V Příloha 3 jsou červenou barvou zobrazeny stávající zásuvky, modrou barvou požadované zásuvky. Nové zásuvky, které v současnosti nejsou, jsou K1, K6, K7, K8, K13 a K17. Zásuvky K1 a K17 jsou jednoportové, do K1 bude zapojeno AP, do K17 kamera. Ostatní zásuvky budou dvouportové a budou se nacházet v kancelářích. Zásuvka K8 je umístěna u vstupu do patra a do ní bude zapojena kamera a přístupový systém.

Aktivní prvky budou uloženy v datovém rozvaděči, který by měl mít dostatek místa pro budoucí vylepšení, takže společnost žádá rozvaděč s výškou alespoň 22U. Ten se umístí na místo současných aktivních prvků. Protože rozvaděč v samostatné zabezpečené místnosti, společnost požaduje uzamykatelný rozvaděč, volitelně i s dalším zabezpečením.

Aktivní prvky

Do rozvaděče se uloží aktivní prvky, kdy externí firma musí dodat dostatečně výkonný router s pokročilou administrací a kvalitním firewallem. Dále v rozvaděči bude uložený i switch, který by měl mít alespoň tolik portů, kolik je portů v zásuvkách. Switch nemusí nepodporovat PoE (napájení po ethernetovém kabelu), protože v síti nejsou prvky, které to využijí.

Protože společnost chce funkční a bezpečnou WiFi, musí dodavatel dodat i přístupový bod, který zvládne obsloužit 7 připojených uživatelů a pokročilou správu přístupu.

3.6.2 Úprava software

Instalaci, změnu a nastavení software na pracovních stanicích ve společnosti už zařídí zaměstnanec společnosti – správce IT. Nejdůležitější částí je změna a nastavení operačního systému, poté instalace ostatního software.

Operační systém

V současné době je na všech počítačích nainstalovaný operační systém Microsoft Windows 7 Home, který je určený do domácností a proto mu chybí pro firemní prostředí několik zásadních funkcí. Mezi nejdůležitější se řadí nemožnost zálohování do síťového uložiště a nemožnost nastavení skupinových politik (anglicky Group Policy). Skupinové politiky jsou důležité pro omezení přístupových práv uživatelů a povolení nebo zakázání jednotlivých funkcí systému. V rámci instalace software bude prvním krokem instalace operačního systému do firemního prostředí – Windows 7 Pro nebo Windows 10 Pro, ale všechny počítače budou mít stejnou verzi. Následně budou všem počítačům nastavena přístupová práva podle jejich odpovědností a pracovní pozice a nainstalovaný software nezbytný k výkonu povolání.

Ostatní software

Instalace jakéhokoliv software bude uživatelům zakázána, tuto možnost bude mít pouze správce IT. Základní programy, např. Microsoft Office, prohlížeč PDF, speciální programy pro práci apod. se nainstalují hned po instalaci operačního systému. Instalace dalších programů proběhne na základě požadavků pro výkon povolání. Na jednotlivých stanicích bude nastavené zálohování celého systému podle stanoveného plánu.

3.7 Popis bezpečnostních opatření etapy I

Tato kapitola poskytuje podrobný popis opatření uvedených v kapitole 3.4. Ta jsou vypracována tak, aby eliminovala nebo redukovala zjištěné nedostatky. Opatření vycházejí z normy ČSN ISO/IEC 27002:2014, ve které se nachází soubor postupů pro opatření bezpečnosti informací.

3.7.1 A.5 Politiky bezpečnosti informací

Cílem opatření je poskytnout podporu pro bezpečnost informací ze strany vedení společnosti v souladu s požadavky společnosti, zákony a předpisy.

A.5.1.1 Politiky pro bezpečnost informací

Odpovědná osoba: Předseda společnosti

Opatření: Definování sady politik pro bezpečnost informací a její schválení vedením společnosti. Politiky musí být zveřejněny pro zaměstnance a být přístupné zainteresovaným stranám. Tato politika je na nejvyšší úrovni definované informační bezpečnosti. Měla by řešit požadavky dle podnikatelské strategie, legislativy a hrozeb současných i očekávaných. V politice jsou definovány cíle a principy bezpečnosti a související činnosti, přiřazení odpovědnosti k rolím v podniku a postupy pro zacházení s výjimkami a odchylkami.

Zdroje opatření: Vytvoření politik – 24 hodin
Seznámení zaměstnanců – 2 hodiny

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Odpovědná osoba: Manažer bezpečnosti

Opatření: Politiky definovány v A.5.1.1 by měly být v pravidelných intervalech přezkoumávány, aby byla zajištěna neustálá aktuálnost a efektivnost. V přezkoumání je zahrnuto posouzení možností pro zlepšování politik a přístupu k bezpečnosti. Protože bude bezpečnost ve společnosti nový prvek a odhadnutí správného fungování je obtížné, počáteční přezkoumání by mělo být nejpozději po půl roce od zavedení, později bude

stačit roční revize. V případě hrozeb nebo při zjištění nepoužitelnosti politik je možné politiky přezkoumat mimo plán.

Zdroje opatření: Vytvoření plánu – 6 hodin
Přezkoumání politiky a úpravy – 10 hodin/přezkoumání

3.7.2 A.6 Organizace bezpečnosti informací

Cílem je stanovení rámce pro zahájení, řízení a zachování bezpečnosti informací ve společnosti.

A.6.1.1 Role a odpovědnosti bezpečnosti informací, A.6.1.2 Princip oddělení povinností

Odpovědná osoba: Vedení společnosti, manažer bezpečnosti

Opatření: Ve společnosti je potřeba nastavit přidělení odpovědností, které bude v souladu s politikou bezpečnosti informací (A.5.1.1). Povinnosti odpovědných zaměstnanců mohou být delegovány na ostatní, ale zůstává jim odpovědnost a rozhodnutí o správném provedení úkolu. Konfliktní povinnosti by měly být rozděleny mezi zaměstnance tak, aby se zamezilo neoprávněným změnám aktiv ve společnosti. Je třeba nastavit, aby zaměstnanci nemohli využívat a měnit aktiva společnosti bez patřičného oprávnění. V této společnosti toto může být problematické z důvodu nedostatku personálu a místo zvláštních pracovníků může být vhodné zavedení monitorování činností a dohled nad úkony.

Zdroje opatření: Vytvoření rolí a odpovědností – 20 hodin

A.6.1.5 Bezpečnost informací v řízení projektů

Odpovědná osoba: Předseda společnosti

Opatření: Bezpečnost informací musí být řešena bez ohledu na typ projektu nebo důležitost projektu (IT, služby, výstavba, dodávka materiálu) a měla by být začleněna do řízení jako součást projektu.

Zdroje opatření: Pravidla pro řízení projektů – 8 hodin

A.6.2.1 Politika mobilních zařízení

Odpovědná osoba: Vedení společnosti, manažer bezpečnosti

Opatření: Při používání mobilních zařízení musí být věnována pozornost jejich zabezpečení při používání v nechráněných prostředích, riziko práce a musí se zamezit úniku informací spojených se společností. Firemní mobilní zařízení musí být chráněna bezpečným heslem, softwarem proti škodlivým kódům a majitel zařízení nesmí nechávat zařízení bez dozoru.

Zdroje opatření: Politika mobilních zařízení – 8 hodin
Ověření zabezpečení – 2 hodiny/měsíc

3.7.3 A.7 Bezpečnost lidských zdrojů

Cílem je pochopení povinností zaměstnanců a zainteresovaných stran a zajištění, aby měli vhodnou klasifikaci pro zamýšlenou pozici.

A.7.1.1 Prověřování, A.7.1.2 Podmínky pracovního vztahu

Odpovědná osoba: Předseda společnosti

Opatření: U uchazeče o zaměstnání se v souladu se zákony a etikou musí prověřit minulost, které by mělo být úměrné pozici a požadavkům společnosti. Uchazeč dodává osobní údaje, dosaženou kvalifikaci, výpis z rejstříku trestů a jiné podrobnější ověření, u kterých společnost kontroluje věrohodnost. Pokud se uchazeč zajímá o pozici, kde má přístup k citlivým datům společnosti, musí se společnost ujistit, že má potřebnou kvalifikaci, je seznámený s principem bezpečnosti informací a lze mu důvěřovat. Součástí pracovní smlouvy jsou prověřené informace, popis práce a podmínky pracovního vztahu, odpovědnost za poskytnutá aktiva a dohoda o zachování důvěrnosti nebo mlčenlivosti, kdy při porušení nastane disciplinární řízení (A.7.2.3)

Zdroje opatření: Podmínky pracovního vztahu – 16 hodin
Prověřování uchazeče – 4 hodiny

A.7.2.1 Odpovědnosti vedení organizace

Odpovědná osoba: Vedení společnosti

Opatření: Vedení společnosti musí vyžadovat od všech zaměstnanců a smluvních stran (u kterých je to vyžadované), aby aplikovali bezpečnost informací v souladu s nastavenými politikami společnosti. V dokumentu bude zajištěné, že zaměstnanci a smluvní strany:

- Jsou informované o rolích a odpovědnostech v bezpečnosti informací
- Obdrží směrnice společnosti, přizpůsobí se jim a jsou motivovány k dodržování stanovených politik

Zdroje opatření: Směrnice odpovědnosti – 16 hodin

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Odpovědná osoba: Předseda společnosti, manažer bezpečnosti

Opatření: Všichni zaměstnanci a relevantní smluvní strany musí mít povědomí o informační bezpečnosti, kterého dosáhnou pravidelným vzděláváním a školením. Program školení musí být v souladu s politikami organizace a je zaměřen na zvýšení povědomí o bezpečnost informací a odpovědnosti za ni. Školení by mělo být nastaveno s ohledem na role zaměstnanců a jejich přístup k informačním aktivům společnosti.

Zdroje opatření: Vytvoření programu školení zaměstnanců – 24 hodin
Školení zaměstnanců – 2 hodiny/měsíc

A.7.2.3 Disciplinární řízení

Odpovědná osoba: Vedení společnosti

Opatření: Zavedení disciplinární řízení se zaměstnanci, kteří se dopustili narušení bezpečnosti informací. Řízení může začít až po ověření, že skutečně došlo k ohrožení informací (např. z logů, řeší A.16.1.7). Může být také použito jako motivace k udržování bezpečnosti a pořádku na pracovišti. Výsledek a opatření disciplinárního řízení musí odpovídat závažnosti ohrožení informační bezpečnosti – napomenutí, finanční sankce, ukončení pracovního vztahu nebo právní kroky.

Zdroje opatření: Směrnice pro disciplinární řízení – 16 hodin

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu

Odpovědná osoba: Předseda společnosti

Opatření: Odpovědnosti a povinnosti, které zůstávají v platnosti po ukončení nebo změně pracovního vztahu by měly být definovány, sděleny zaměstnancům a následně prosazovány. Tyto odpovědnosti mohou být zakotveny už v pracovní smlouvě (A.7.1.2).

Zdroje opatření: Směrnice o odpovědnosti – 12 hodin

3.7.4 A.8 Řízení aktiv

Cílem je identifikace aktiv společnosti, definice odpovědnosti za jejich ochranu a jejich klasifikace.

A.8.1.1 Seznam aktiv

Odpovědná osoba: Vedení společnosti, manažer bezpečnosti

Opatření: Základní dokument, společnost musí identifikovat aktiva, která jsou důležitá pro její fungování – aktiva, která slouží k vytvoření, zpracování, ukládání, přenosu, vymazání a zničení informací. Seznam aktiv musí být přesný a aktuální, každé aktivum by mělo mít přiřazeného vlastníka (podle A.8.1.2) a být klasifikováno (podle A.8.2). Aktiva jsou identifikována v Tabulka 2.

Zdroje opatření: Evidence aktiv – 16 hodin
Přezkoumání – 2 hodiny/rok

A.8.1.2 Vlastnictví aktiv

Odpovědná osoba: Vedení společnosti

Opatření: Aktiva definovaná v seznamu aktiv by mělo mít definováno vlastníka. Určení zaměstnanci musí být kvalifikovaní pro správu a řízení daného aktiva. Jako vlastníka je vhodné stanovit zaměstnance, který má svým zaměřením logicky nejblíže. Přidělení odpovědností stanovuje vedení společnosti a musí dotyčného řádně informovat o této

skutečnosti. Aktiva 2, 5, 6 jsou využívány více odděleními, proto jako vlastník je stanoveno vedení společnosti. Revize vlastnictví probíhá zároveň s A.8.1.2 nebo při odchodu odpovědného zaměstnance.

Tabulka 9: Vlastníci aktiv
Zdroj: vlastní zpracování

	Aktivum	**Vlastník**
1.	Firemní účetnictví	Hlavní účetní
2.	Dokumenty v papírové podobě	Vedení společnosti
3.	Zálohy	Správce IT
4.	Informační systémy	Správce IT
5.	Smlouvy	Vedení společnosti
6.	Projektové dokumentace	Vedení společnosti
7.	Tiskárna	Správce IT
8.	Pracovní stanice	Správce IT
9.	Aktivní síťové prvky	Správce IT
10.	Operační systém	Správce IT
11.	Programové vybavení	Správce IT

Zdroje opatření: Stanovení vlastnictví – 8 hodin
Změny vlastnictví – 1h/změna

A.8.1.3 Přípustné použití aktiv

Odpovědná osoba: Vedení společnosti, manažer bezpečnosti

Opatření: Identifikovaná aktiva a informace by měla mít nastavená pravidla pro jejich přípustné použití. Zaměstnanci a zainteresované strany pracující s aktivy společnosti musí být řádně seznámeni s těmito pravidly. Podrobnější pravidla jsou v oblasti A.9.

Pravidla pro využívání informačních aktiv a ostatního vybavení:

- Firemní účetnictví, dokumenty v papírové podobě, smlouvy, projektové dokumentace – zpracování, tisk a úprava je možná pouze pro potřeby společnosti a není možné je používat mimo prostory společnosti, pokud k tomu není uděleno oprávnění od vedení společnosti
- Zálohy – manipulace se zálohami není přípustná, pokud nedojde k havárii zařízení a je nutné data obnovit ze zálohy

- Informační systémy – využití infomačních systému je přípustné pouze pro oprávněné uživatele a data se využívají pouze pro potřeby společnosti
- Tiskárna – není přípustné tisknutí soukromých dokumentů nebo využívání zařízení k soukromým účelům
- Pracovní stanice – zákaz přenášení, úpravy, úpravy, opravy nebo odpojování bez vědomí správce IT coby vlastníka aktiva
- Aktivní síťové prvky – úprava síťových prvků je přípustná pouze vlastníkem aktiva, správcem IT, úprava bezpečnostních pravidel je možná pouze po konzultaci s vedením společnosti a manažerem bezpečnosti
- Operační systém – zaměstnanci musí k přístupu využívat bezpečná hesla, při odchodu od pracovní stanice uzamknout operační systém, využití pouze k pracovním povinnostem
- Programové vybavení – využívání pouze k povaze aplikace a firemnímu využití, programy jsou instalovány a spravovány správcem IT, uživatelé nemají oprávnění ke změnám

Zdroje opatření: Směrnice pro přípustné použití aktiv – 12 hodin
Revize použití aktiv – 2 hodiny/měsíc

A.8.2.1 Klasifikace informací, A.8.2.2 Označování informací

Odpovědná osoba: Manažer bezpečnosti, vedení společnosti

Opatření: Informace by měly být klasifikovány z hlediska zákonů, hodnoty, kritičnosti nebo citlivosti k úpravě a prozrazení. Z hlediska hodnoty pro společnost můžeme klasifikovat 3 druhy informací – účetní, o zaměstnancích, firemní. Účetní informace jsou utajované a mají pro společnost velkou hodnotu, ale případné zneužití by nemělo firmu ohrozit nebo na ni mít dopad. Druhý typ jsou informace o zaměstnancích, které chráněné podle zákona o ochraně osobních údajů a jejich zpracování musí být omezeno. Pokud by byl porušen tento zákon, mohlo by to mít pro společnost právní následky a následně i finanční náklady. Třetím druhem informací jsou informace firemní, mezi které se řadí skladové evidence, objednávky a další. Jejich prozrazení by mohlo mít dopad na společnost, protože to jsou utajované nebo citlivé informace.

Pro klasifikované druhy informací budou vypracovány soubory postupů pro jejich označování. Při tištění dokumentů s citlivými informacemi je doporučeno opatřit dokument vodoznakem. Uživatelé, kteří nepotřebují tisk k výkonu svého zaměstnání, by měli mít znemožněný přístup k tisku. Uložené informace je také nutné opatřit přístupovými právy, aby se zamezilo kopírování neoprávněným uživatelem (A.8.2.3).

Zdroje opatření: Klasifikace informací – 2 hodiny/rok
Nastavení práv – 12 hodin

A.8.2.3 Manipulace s aktivy

Odpovědná osoba: Manažer bezpečnosti

Opatření: V souladu se schématem klasifikace informací se vypracují postupy pro zacházení s aktivy. Všechna podniková data musí mít nastavena přístupová práva, aby k nim nemohli přistupovat neoprávnění uživatelé – omezí se veškeré operace se složkami a zamezí se zobrazení obsahu složek. Aktiva, která nejsou informační povahy (tiskárna, pracovní stanice apod.) budou zřetelně označeny a zaznamenány, jejich skladování musí probíhat dle pokynů výrobce. Manipulace s aktivy proběhne také v souladu s přístupným použitím aktiv (A.8.1.3).

Zdroje opatření: Manipulace s aktivy – 16 hodin

A.8.3.1 Správa výměnných médií, A.8.3.3 Přeprava fyzických médií

Odpovědná osoba: Manažer bezpečnosti

Opatření: Pro vyměnitelná média je třeba zavést postupy pro jejich správu a přepravu. Uložení médií musí být v bezpečném prostředí a musí souhlasit se specifikacemi výrobce. Přenosná média, která se vynáší mimo prostředí společnosti, by měly být zabezpečeny proti neoprávněnému přístupu a neměly by obsahovat citlivé firemní informace. Dále se musí dodržovat předepsaná životnost média, kdy se ke konci doby životnosti musí data přenést na nové médium a staré zlikvidovat (podle A.8.3.2). Kopírování na vyměnitelná média musí být monitorováno, u uživatelů, kde to není vyžadováno, je doporučený zákaz připojení výměnných médií nebo fyzické blokování USB portů a odstranění optické mechaniky. Médium smí přepravovat pouze odpovědná

osoba, média, které pro to nejsou určeny, nesmí opustit prostory společnosti. Při přepravě se musí přijmout taková opatření, aby se zamezilo ztrátě a neoprávněné manipulaci.

Zdroje opatření: Politika výměnných médií – 12 hodin

A.8.3.2 Likvidace médií

Odpovědná osoba: Manažer bezpečnosti

Opatření: Pokud vyměnitelné médium překoná svou životnost, je poškozeno nebo zničeno, je nutné ho bezpečně zlikvidovat podle nastavených postupů nebo ho zaslat k opravě, pokud médium neobsahuje citlivá data a riziko je nízké. Papírové dokumenty se skartují s bezpečnostním stupněm skartování podle citlivosti dokumentu a nastavených politik nebo se spálí. Ostatní média (flash disky, optické disky) je doporučeno zlikvidovat odbornou firmou, která má certifikát bezpečnostního opatření a zkušenosti s provedením likvidace. Likvidace všech médií by se měla zaznamenávat.

Zdroje opatření: Pravidla nakládání s médii – 4 hodiny

3.7.5 A.11 Fyzická bezpečnost a bezpečnost prostředí

Cílem fyzické bezpečnosti je zabránění neoprávněného přístupu, poškození nebo narušení informací a vybavení.

A.11.1.1 Fyzický bezpečnostní perimetr

Odpovědná osoba: Vedení společnosti, manažer bezpečnosti

Opatření: Ve společnosti existuje pouze jeden perimetr a tím je celé patro kanceláří společnosti. To by se mělo rozdělit a společnost by měla definovat bezpečnostní perimetry k ochraně oblastí s citlivými daty a informacemi.

Zóna 1 – Celé patro - Vstup do patra kanceláří je možný pouze jednou cestou – po schodech. U vchodu není recepční, kamerový systém či jiné opatření, takže riziko vstupu neoprávněných osob je vysoké. V první fázi by u vchodu měl být zavedený kamerový systém a systém přístupových karet, návštěvníci by využili zvonek a pověřený zaměstnanec by přišel otevřít. Dále zaznamená jméno osoby, čas a důvod

návštěvy a doprovodí návštěvníka až k zaměstnanci, ke kterému přišel na schůzku. Tím se zamezí volnému pohybu osob.

Zóny 2 – Kanceláře – jednotlivé kanceláře budou spadat do zóny 2, takže kanceláře, kde není zaměstnanec, se musí zamykat. Za klíče od kanceláří mají odpovědnost jednotliví zaměstnanci, předseda společnosti a manažer bezpečnosti budou mít univerzální klíče s přístupem do všech kanceláří.

Zóna 3 – datový rozvaděč – společnost nemá samostatnou místnost s rozvaděčem, proto jsou prvky uloženy v zasedací místnosti. Ta zůstane stále zamčená, mimo doby schůzí. Schůzí se účastní pouze vedení společnosti. Aktivní prvky budou nyní uložené v uzamykatelném datovém rozvaděči, ke kterému bude mít přístup pouze správce IT. V rozvaděči bude uloženo NAS, na které se budou zálohovat data z počítačů.

Zdroje opatření: Dokumentace perimetrů – 8 hodin
Přístupový systém – 25000 Kč
Kamerový systém – 20000 Kč

A.11.1.2 Fyzické kontroly vstupu

Odpovědná osoba: odpovědný pracovník

Opatření: A.11.1.1 tento problém řeší zavedením systému přístupových karet, knihou návštěv a kamerovým záznamem.

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Odpovědná osoba: manažer bezpečnosti

Opatření: Jak bylo zmíněno v A.11.1.1, zabezpečení kanceláří a ostatních místností se bude řešit stálým zamykáním v nepřítomnosti pracovníka, aby se zabránilo vstupu neoprávněné osoby. Vybavení (počítače, tiskárna apod.) se opatří zámkovou sadou proti krádeži nebo neoprávnění manipulaci. Zároveň je možné zabezpečit i periferní zařízení jako monitor, klávesnici nebo myš. Ocelové lanko se zámkem se následně připoutá k pevné věci, např. k topení. Zámkové sady se dodávají s více klíči nebo s jedním hlavním klíčem, který bude uschovaný ve firemním trezoru.

Zdroje opatření: Zámkové sady pro stolní počítače 9ks á 700 Kč – 6300 Kč
Zabezpečení zařízení – 8 hodin

A.11.2.1 Umístění zařízení a jeho ochrana

Odpovědná osoba: Vedení společnosti, manažer bezpečnosti

Opatření: Společnost musí zabezpečit, aby byla aktiva chráněna proti nepřízni životního prostředí a možnosti neoprávněného přístupu. Proti neoprávněnému přístupu jsou učiněna opatření v A.11.1.1, kdy pro přístup do budovy budou použity čipové karty a nevyužívané místnosti budou uzamčeny. Dále podle A.11.1.3 jsou zařízení připevněna ocelovým zámkem a lankem k topení. Proti živelným katastrofám je budova chráněna dobře a kanceláře se nachází až ve třetím poschodí, takže z této strany nehrozí reálné nebezpečí. Proti havárii vodovodního potrubí jsou počítače umístěny vždy ve stole ve výši alespoň 20 cm nad zemí. V místnostech, kde je vodovodní baterie je možné instalovat čidlo zaplavení. Hrozba zatopení z vyššího patra nehrozí, protože kanceláře jsou v nejvyšším patře. V důsledku použití většího množství elektronických zařízení může být v objektu zvýšené riziko požáru. Riziko se sníží pravidelnými revizemi (dále v A.11.2.4) a použitím detektorů kouře. Ty je vhodné umístit do každé kanceláře a místnosti s výjimkou toalet, kde nejsou hořlavé materiály.

Zdroje opatření: Detektory kouře 16 ks á 1000 Kč – 16000 Kč
Další zdroje popsány v A.11.1.1 a A.11.1.3
Čidlo zaplavení 4ks á 800 Kč – 3200Kč

A.11.2.2 Podpůrné služby

Odpovědná osoba: Správce IT

Opatření: Zařízení by měla být chráněna proti výpadku napájení a selháním podpůrných systémů. Společnost u každého zařízení využívá nepřerušitelné zdroje napájení (UPS) v dostatečné kapacitě, aby zaměstnanci stihli uložit rozdělanou práci a zařízení řádně vypnout. UPS nemají ovládací software, takže výpadek napájení je oznámen zvukovým projevem a zaměstnanec musí vypnout zařízení sám. Pro vyšší bezpečnost je možné před zdroj UPS zapojit přepěťovou ochranu. Proti zamezení přepětí v datové síti je možné zapojit před router bleskojistku nebo zařízení galvanicky oddělit použitím

převodníku z metalického na optické vedení a zpět. Společnost však nemá vlastní anténu a konektivita jde přímo od poskytovatele internetu, který je proti tomuto chráněn.

Zdroje opatření: Přepěťová ochrana 10 ks á 1000 Kč – 10000 Kč

A.11.2.4 Údržba zařízení

Odpovědná osoba: Správce IT

Opatření: Je třeba zavést plán pravidelných revizí a kontrol elektrických zařízení s cílem odhalit a zamezit chybám. Energetik ve společnosti, který je proškolený podle vyhlášky 50, bude revize pravidelně provádět a podávat hlášení vedení společnosti. Čistění zařízení od prachu a vizuální kontrolu obstará správce IT.

Zdroje opatření: Plán kontrol – 8 hodin
Revize – 1 hodina/zařízení
Čištění zařízení – 3 hodiny/měsíc

A.11.2.7 Bezpečná likvidace nebo opakované použití

Odpovědná osoba: manažer bezpečnosti

Opatření: Bezpečností při likvidaci zařízení se zabývá odstavec A.8.3.2. Pro opakované použití pro jiné než dosavadní úkoly je nutné paměťové médium přepsat náhodnými daty s počtem průchodů podle citlivosti uložených informací. V pokynech se určí nástroj pro smazání dat a nastavení.

A.11.2.8 Uživatelská zařízení bez obsluhy

Odpovědná osoba: Uživatel zařízení

Opatření: Pokud zaměstnanec odchází od pracoviště, je nutné, aby zajistil přiměřenou ochranu zařízení. Nejsnáze se toho dosáhne uzamčením uživatelského profilu klávesovou zkratkou „*Win+L*“ (platí pro OS Windows).

Zdroje opatření: Návod pro užívání zařízení – 4 hodiny

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Odpovědná osoba: Uživatel zařízení

Opatření: V návaznosti na A.11.2.8 výše musí uživatel dodržovat zásadu prázdného stolu a obrazovky monitoru. Pokud uživatel nevyužívá papírové dokumenty nebo paměťová média, uklidí je do bezpečného prostředí, např. zamčené skříně nebo trezoru, zejména jedná-li se o informace citlivé nebo kritické pro společnost. K zásadě prázdné obrazovky patří, že pokud spuštěné aplikace a programy nejsou využívány, je nutné je vypnout.

Zdroje opatření: Uvedeny v A.11.2.8

3.8 Zdroje a náklady na první etapu

První etapa zavádění bezpečnosti informací zahrnuje kapitoly A.5 Politiky bezpečnosti informací, A.6 Organizace bezpečnosti informací, A.7 Bezpečnost lidských zdrojů, A.8 Řízení aktiv, A.11 Fyzická bezpečnost a bezpečnost prostředků z normy ČSN ISO/IEC 27001:2013, přílohy A.

Tabulka 10: Zdroje a náklady na první etapu
Zdroj: vlastní zpracování

Označení	Činnost	Počáteční nastavení [h]	Ročně [h]	Měsíčně [h]	Událost [h]	Peněžní náklady [odhad Kč]
A.5.1.1	Vytvoření politik	24				
	Seznámení zaměstnanců	2				
A.5.1.2	Vytvoření plánu	6				
	Přezkoumání politiky a úpravy				10	
A.6.1.1	Vytvoření rolí a odpovědností	20				
A.6.1.5	Pravidla pro řízení projektů	8				
A.6.2.1	Politika mobilních zařízení					
	Ověření zabezpečení			2		
A7.1.1, A.7.1.2	Podmínky pracovního vztahu	16				
	Prověřování uchazeče				4	
A.7.2.1	Směrnice o odpovědnosti	16				
A.7.2.2	Vytvoření programu školení zaměstnanců	24				
	Školení zaměstnanců			2		
A.7.2.3	Směrnice pro disciplinární řízení	16				
A.7.3.1	Směrnice o odpovědnosti	12				
A.8.1.1	Evidence aktiv	16				
	Přezkoumání		2			
A.8.1.2	Stanovení vlastnictví	8				
	Změny vlastnictví				1	

A.8.1.3	Směrnice pro přípustné použití aktiv	12				
	Revize použití aktiv			2		
A.8.2.1, A.8.2.2	Klasifikace informací		2			
	Nastavení práv	12				
A.8.2.3	Manipulace s aktivy	16				
A.8.3.1	Politika výměnných médií	12				
A.8.3.2	Pravidla nakládání s médii	4				
A.11.1.1	Dokumentace perimetrů	8				
	Přístupový systém					25 000 Kč
	Kamerový systém					20 000 Kč
A.11.1.3	Zámkové sady pro stolní počítače					6 300 Kč
	Zabezpečení zařízení	8				
A.11.2.1	Detektory kouře					16 000 Kč
	Čidlo zaplavení					3 200 Kč
A.11.2.2	Přepěťová ochrana					10 000 Kč
A.11.2.4	Plán kontrol	8				
	Revize				1	
	Čištění zařízení			3		
A.11.2.8	Návod pro užívání zařízení	4				
		252 h	**4 h**	**9 h**	**16 h**	**80500 Kč**

Součet zdrojů v posledním řádku tabulky ukazuje celkový odhad nákladů na první etapu. Připravení úvodní dokumentace a počáteční nastavení potrvají odhadem 252 hodin. Činnosti, které se opakují ročně, budou trvat pouze 4 hodiny, měsíčně 9 hodin a jednorázové, které se zpracovávají náhodně, 16 hodin. Společnost hodinovou práci bezpečnostního konzultanta odhaduje na 1000 Kč a náklady tedy budou následující:

- Úvodní dokumentace a nastavení – 252 hodin á 1000 Kč = 252 000 Kč
- Ročně opakované činnosti - 4 hodiny á 1000 Kč = 4000 Kč
- Měsíčně opakované činnosti – 9 hodin á 1000 Kč = 9000 Kč
- Náklady na události – 16 hodin á 1000 Kč = 16 000 Kč

Tabulka 11: Orientační tabulka nákladů
Zdroj: vlastní zpracování ke dni 16. 5. 2016

Název	Počet ks	Cena bez DPH za m.j.	Cena celkem
Dokumentace a nastavení ISMS	1	252 000 Kč	252 000 Kč
Přístupový systém	1	25 000 Kč	25 000 Kč
Kamerový systém	1	20 000 Kč	20 000 Kč
Zámková sada pro stolní PC	9	700 Kč	6 300 Kč
Detektor kouře	16	1 000 Kč	16 000 Kč
Čidlo zaplavení	4	800 Kč	3 200 Kč
Přepěťová ochrana	10	1000 Kč	10 000 Kč
Vyčleněné prostředky pro výstavbu lokální sítě	1	100 000 Kč	100 000 Kč
OS Microsoft Windows 10 Professional	8	3 300 Kč	26 400 Kč
NAS + pevné disky	1	20 000 Kč	20 000 Kč
		Celkem:	**478 900 Kč**

Odhad celkových nákladů na první etapu včetně výstavby lokální sítě a software je 478 9000 Kč bez DPH. Tento odhad je pouze orientační a může se měnit v závislosti na časové náročnosti prováděné dokumentace, nastavení, ceně jednotlivých prvků a jejich konfiguraci.

3.9 Podíl zavedených opatření na snížení rizika hrozeb

Tabulka 12 níže ukazuje, že již první etapa opatření řeší většinu hrozeb. Hrozby se však stále objevují nové nebo se odhalují stávající a proto je důležité se zaváděním informační bezpečnosti pokračovat i v dalších etapách.

Tabulka 12: Podíl zavedených opatření na snížení rizika hrozeb
Zdroj: Vlastní zpracování

	Hrozba	Řešení
Fyzické poškození	Požár	Řeší A.11.2.1
	Poškození vodou	Řeší A.11.2.1
	Přepětí v síti	Řeší A.11.2.2
	Selhání hardware	Částečně řeší A.11.2.4, selhání se nedá zabránit, ale opatřením se pravděpodobnost hrozby sníží.
	Zničení médií nebo zařízení	Zařízení jsou chráněna proti neodborné manipulaci. Média se zálohují.
	Chyba údržby	Řeší A.11.2.4
Dostupnost služeb	Porucha sítě LAN nebo WAN	Částečně řeší A.11.2.2 a A.11.2.4. Proti výpadku sítě WAN musí být zajištěný poskytovatel.
	Výpadek elektřiny	Řeší A.11.2.2. Záložní zdroje UPS vydrží napájet zařízení po dobu nezbytnou k uložení a ukončení práce.
	Selhání komunikace	Pro případ nefunkčnosti telefonní sítě nebo VoIP jsou ve firmě k dispozici mobilní telefony.
Ohrožení informací	Krádež médií nebo dokumentů	Řeší A.11.1
	Krádež zařízení	Řeší A.11.1
	Škodlivé programy	Řeší již zavedené A.12.2.1
Ohrožení funkčnosti	Poškození uživatelem	Částečně řeší A.7.2.2, A.8.1.3, A.8.2.3, A.11.1.3. Je nutné provádět školení uživatelů pro budování bezpečnostního povědomí
	Selhání software	Částečně řeší A.12.2.1. Jakékoliv nečekané změny v chování software musí uživatel oznámit správci IT.

Pokud společnost zavede systém řízení bezpečnosti informací, již po první etapě opatření řeší většinu hrozeb, které na aktiva působí. Při správné aplikaci bude mít ISMS pro společnost přínos v podobě mnohem vyšší informační bezpečnosti než doposud a společnost bude mít přehled o dění na lokální síti a o svých zaměstnancích.

ZÁVĚR

Tato diplomová práce se zabývala ustanovením systému řízení bezpečnosti informací. Analýza současného stavu informační bezpečnosti odhalila, že se společnost téměř vůbec nezabývá bezpečností informací a oblasti, které jsou řešené, nejsou zdokumentované.

Teoretická část práce popisovala poznatky ze základních pojmů, procesů, norem ČSN ISO/IEC řady 27000 a hlavně obecných poznatků ze systémů řízení bezpečnosti informací.

Praktická část se zaměřila na návrh ustanovení ISMS. Protože řízení bezpečnosti informací je nikdy nekončící proces, je nutné stále sledovat vývoj, trendy v bezpečnosti, nově vyskytnuté hrozby a přizpůsobit jim úroveň ochrany. Analýza současného stavu, která odhalila velké nedostatky v oblasti bezpečnosti informací, je důležitý krok před začátkem návrhu ISMS. Prvním krokem v ISMS, analýzou rizik, jsme zjistili hrozby, které působí na informační bezpečnost podniku. Pokud by se hrozby naplnily, mohlo by to mít vážné následky na fungování společnosti, proto na základě zjištěných hrozeb je vypracován návrh ustanovení ISMS, ve kterém jsou vybrány jednotlivá opatření z normy ČSN ISO/IEC 27001 pro vyřešení nebo zmírnění zjištěných hrozeb. Protože je opatření velké množství, zavedení najednou by přineslo společnosti zátěž nejen finanční, ale i časovou. Opatření jsem rozdělil do tří etap. V práci je popsána první etapa těchto opatření. Ještě před zahájením první etapy je nutné aktualizovat využívaný software a instalovat novou lokální síť, aby splňovala normy a provoz na ni byl bezpečný a spolehlivý. V práci je popsáno zadání pro vypracování sítě, které dodá externí firma. Toto řešení bude mít výhodu v dodávce profesionálního řešení s kvalitními prvky a podle platných norem.

Výsledné finanční zhodnocení odhaduje náklady na přibližně 479 tisíc korun, které zahrnují náklady na bezpečnostního konzultanta (53%), návrh a instalaci lokální sítě (21%), prostředky pro zajištění fyzické bezpečnosti (17%) a software (9%). Nová lokální síť pro společnost bude mít přínos v podobě bezpečného a spolehlivého provozu, který poskytne základy pro další vrstvy bezpečnosti. Na novém software můžeme nastavit přístupová práva pro oprávněné uživatele a z důvodu bezpečnosti

omezit jejich aktivity jen na nezbytně nutné a tím zabránit neoprávněným přístupům a bezpečnostním incidentům. Prostředky pro fyzickou bezpečnost umožní vstup pouze povolaným osobám a i tyto vstupy jsou kontrolovány a zaznamenávány.

Tato práce splňuje stanovený cíl, kterým byla analýza současného stavu a návrh opatření pro eliminaci zjištěných hrozeb. Mým největším přínosem této práce je začlenění bezpečnosti do každodenního firemního fyzického i informačního prostředí a zadání pro budování nové lokální sítě. Bezpečnost dat i ostatních firemních aktiv bude po zavedení opatření vysoká a opatření budou bránit útočníkům v získání důvěrných dat (osobní údaje) a poškození společnosti a tím ji ušetří finanční výdaje, které by vynaložila za právní služby, pokuty a další následky. Druhý přínosem je zadání pro stavbu bezpečné, funkční a spolehlivé lokální sítě a instalaci nového operačního systému, který s sebou přináší nastavení uživatelských přístupových práv a tím vyšší informační bezpečnost.

SEZNAM POUŽITÉ LITERATURY

[1] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[2] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

[3] *Zákon č. 227/2000 Sb., o elektronickém podpisu* [online]. 2012 [cit. 2016-05-17]. Dostupné z: http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

[4] *ČSN ISO/IEC 27005:2011: Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013, 64 s.

[5] *ČSN ISO/IEC 27002:2013: Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. 1.vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[6] *ČSN ISO/IEC 27001:2013: Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. 1.vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[7] *ČSN ISO/IEC 27001 - Náhled* [online]. 2006 [cit. 2016-05-18]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/36/76533/76533_nahled.htm

[8] NOVÁK, Luděk a Josef POŽÁR. *Systém řízení informační bezpečnosti* [online]. b.r., , 10 [cit. 2016-05-22]. Dostupné z: http://www.cybersecurity.cz/data/srib.pdf

[9] Elektroinstalační profily - katalog. *Polyprofit* [online]. 2010 [cit. 2016-05-16]. Dostupné z: http://www.polyprofil.cz/file/elektroinstalacni_profily.pdf

[10] BELDEN 1583ENH. *Asit.it* [online]. b.r. [cit. 2016-05-16]. Dostupné z: http://www.asit.it/wp-content/uploads/2015/05/1583ENH_02-1000x757.png

SEZNAM OBRÁZKŮ

OBRÁZEK 1: VZTAH ÚROVNÍ BEZPEČNOSTI V ORGANIZACI 13
OBRÁZEK 2: PDCA MODEL APLIKOVANÝ NA PROCESY ISMS 23
OBRÁZEK 3: PŘEHLED ČINNOSTÍ PŘI USTANOVENÍ ISMS 25
OBRÁZEK 4: ORGANIZAČNÍ SCHÉMA V BUDOVĚ KANCELÁŘÍ 32
OBRÁZEK 5: LOGICKÉ SCHÉMA ZAPOJENÍ STÁVAJÍCÍ SÍTĚ 33
OBRÁZEK 6: LOGICKÉ SCHÉMA ZAPOJENÍ NOVÉ SÍTĚ 49
OBRÁZEK 7: PŘÍKLAD PLASTOVÝCH ELEKTROINSTALAČNÍCH PROFILŮ 49
OBRÁZEK 8: UTP KABEL BELDEN 50

SEZNAM TABULEK

TABULKA 1: STUPNICE HODNOCENÍ AKTIV 35
TABULKA 2: HODNOCENÍ AKTIV 36
TABULKA 3: STUPNICE HODNOCENÍ PRAVDĚPODOBNOSTI HROZBY 38
TABULKA 4: IDENTIFIKACE HROZEB A ZRANITELNOSTÍ 38
TABULKA 5: MATICE ZRANITELNOSTÍ 40
TABULKA 6: HODNOCENÍ RIZIK 41
TABULKA 7: MATICE RIZIK 42
TABULKA 8: SOUBOR BEZPEČNOSTNÍCH OPATŘENÍ PODLE ČSN ISO/IEC 27001:2013 PŘÍLOHA A 43
TABULKA 9: VLASTNÍCI AKTIV 57
TABULKA 10: ZDROJE A NÁKLADY NA PRVNÍ ETAPU 65
TABULKA 11: ORIENTAČNÍ TABULKA NÁKLADŮ 67
TABULKA 12: PODÍL ZAVEDENÝCH OPATŘENÍ NA SNÍŽENÍ RIZIKA HROZEB 68

SEZNAM ZKRATEK

ISMS	Information Security Management Systém – Systém řízení bezpečnosti informací
PDCA	Demingův cyklus: Plánuj – Dělej – Kontroluj - Jednej
ISO	Mezinárodní organizace pro normalizaci
IEC	Mezinárodní úřad pro elektrotechniku
ICT	Informační a komunikační technologie
IS	Informační systém
UPS	Nepřerušitelný zdroj napájení
Wi-Fi	Bezdrátová síť
VPN	Virtuální privátní síť
NAS	Datové uložiště připojené do sítě
LAN	Lokální síť
WAN	Rozsáhlá síť
ISP	Poskytovatel internetu
PoE	Power over Ethernet - Napájení po datovém kabelu

SEZNAM PŘÍLOH

PŘÍLOHA 1: SEZNAM OPATŘENÍ FÁZE II PODLE ČSN ISO/IEC 27001:2013 I
PŘÍLOHA 2: SEZNAM OPATŘENÍ FÁZE III PODLE ČSN ISO/IEC 27001:2013 III
PŘÍLOHA 3: TRASY KABELÁŽE A UMÍSTĚNÍ ZÁSUVEK V

Příloha 1: Seznam opatření fáze II podle ČSN ISO/IEC 27001:2013

Označení	Opatření	Popis opatření
A.9 Řízení přístupu		
A.9.1 Požadavky organizace na řízení přístupu		
A.9.1.1	Politika řízení přístupu	Společnost nastaví bezpečnostní politiky pro řízení přístupu k aktivům - fyzickým (PC) i logickým (software).
A.9.1.2	Přístup k sítím a síťovým službám	Pravidla síťového provozu zajistí, že uživatel bude mít přístup pouze k těm službám, ke kterým je autorizován.
A.9.2 Řízení přístupu uživatelů		
A.9.2.1	Registrace a zrušení registrace uživatele	Registrace a zrušení registrace uživatelů bude postupovat podle schválených pravidel.
A.9.2.2	Správa uživatelských přístupů	Na základě registrace (A.9.2.1), jeho pracovní pozici a odpovědnostem, bude uživateli poskytnut přístup k jednotlivým systémům a službám.
A.9.2.3	Správa privilegovaných přístupových práv	Správa privilegovaných přístupových práv bude probíhat v souladu s politikou řízení přístupu (A.9.1.1). Přidělené bude probíhat prostřednictvím formálního procesu.
A.9.2.4	Správa tajných autentizačních informací uživatelů	Přidělení autentizačních informací získá uživatel po registraci (A.9.2.1). Po prvním přihlášení je uživatel nucen změnit heslo podle pravidel tvorby hesla (velikost písmen, čísla, ostatní znaky) a heslo musí udržovat v tajnosti.
A.9.2.5	Přezkoumání přístupových práv uživatelů	Po změně pracovní pozice, odchodu ze společnosti apod. je vyžadováno přezkoumání přístupových práv uživatele s cílem zvýšení, snížení nebo zrušení práv. Přezkoumání probíhá v pravidelných intervalech. Opatření souvisí s A.9.2.1, A.9.2.2 a A.9.2.6.
A.9.2.6	Odebrání nebo úprava přístupových práv	Neprodleně po ukončení zaměstnaneckého poměru se uživateli odeberou přístupová práva ke službám a systémům společnosti.
A.9.3 Odpovědnosti uživatelů		
A.9.3.1	Používání tajných autentizačních informací	Uživatelé musí dodržovat postupy společnosti pro uchování tajných autentizačních informací.
A.9.4 Řízení přístupu k systémům a aplikacím		
A.9.4.1	Omezení přístupu k informacím	V souladu s politikou řízení přístupu (A.9.1.1) je nutné omezení přístupů k informačním systémům a dalším zdrojům podle pracovní pozice uživatele.
A.9.4.2	Bezpečné postupy přihlášení	Přístup k aplikacím je podmíněn přihlášením bezpečným heslem. Pro přístup ke kritickým aplikacím je možné zvolit jiné autentizační postupy - tokeny, čipové karty apod.
A.9.4.3	Systém správy hesel	Uživatel musí zvolit jedinečné a dostatečně bezpečné heslo, které splňuje pravidla pro tvorbu hesla. Heslo je doporučeno v pravidelných intervalech měnit a nové heslo nesmí být podobné, jako původní.
A.12 Bezpečnost provozu		
A.12.1 Provozní postupy a odpovědnosti		
A.12.1.1	Dokumentované provozní postupy	Provozní postupy pro zpracování informací a nakládání s komunikačním vybavením jsou zdokumentované a dostupné všem uživatelům společnosti.
A.12.1.2	Řízení změn	Změny v procesech, službách a systémem, které ovlivňují bezpečnost informací, musí být řízeny a kontrolovány.

A.12.1.3 Řízení kapacit	Využití informačních zdrojů by mělo být monitorováno, optimalizováno a plánováno, aby nenastal nedostatek např. výpočetního nebo diskového prostoru.
A.12.3 Zálohování	
A.12.3.1 Zálohování informací	Je nutné pravidelně pořizovat zálohy souborů a bitové kopie systémů. Záložní kopie je nutné v pravidelných intervalech testovat na čitelnost.
A.12.4 Zaznamenávání formou logů a monitorování	
A.12.4.1 Zaznamenávání událostí formou logů	Monitorované aktivity, výjimky, selhání a události systémů musí být monitorovány a přezkoumávány s cílem vylepšení bezpečnosti.
A.12.4.2 Ochrana logů	Vybavené pro pořízení logů a uložené logy musí být chráněny proti falšování a neoprávněnému přístupu.
A.12.4.3 Logy o činnosti administrátorů a operátorů	Nejen aktivita běžných uživatelů, ale i aktivita administrátorů by měla být zaznamenávána a pravidelně kontrolována.
A.12.4.4 Synchronizace hodin	Všechny systémy společnosti by měly mít čas synchronizovaný podle jednoho referenčního zdroje.
A.12.5 Správa provozního softwaru	
A.12.5.1 Instalace softwaru na provozní systémy	Instalace provozních systémů bude probíhat podle nastavených postupů - aktualizace systémů podle administrátorem, implementace systémů až po důkladném testování, archivace starých verzí apod.
A.12.6 Řízení technických zranitelností	
A.12.6.1 Řízení technických zranitelností	Administrátor musí udržovat přehled o zranitelnostech použitých informačních systémů a zajišťovat potřebné aktualizace nebo přijmout jiná opatření k řešení rizik.
A.12.6.2 Omezení instalace software	Software může instalovat pouze administrátor, za předpokladu schválení vedením a pokud je v souladu s nastavenými politikami společnosti.
A.13 Bezpečnost komunikací	
A.13.1 Správa bezpečnosti sítě	
A.13.1.1 Opatření v sítích	Provoz na síti musí být řízen a kontrolován v zájmu zachování bezpečnosti. Je nutné přijmout opatření, která zajistí bezpečnost přenášených dat a nemožnost jejich změny.
A.13.1.2 Bezpečnost síťových služeb	Síťové služby musí obsahovat mechanismy pro zajištění bezpečného provozu.
A.13.1.3 Princip oddělení v sítích	Skupiny informačních systémů, služeb a uživatelů (např. s rozdílnými právy nebo podle oddělení) musí být v síti odděleny.
A.13.2 Přenos informací	
A.13.2.1 Politiky a postupy při přenosu informací	Pro přenos informací (dovnitř i vně společnosti) by se měly zavést politiky, aby se informace zajistily proti změně, odposlechnutí nebo neoprávněnému použití.
A.13.2.3 Elektronické předávání zpráv	Informace předávané prostřednictvím elektronických zpráv musí být přiměřeně chráněny - např. použitím elektronického podpisu. Pro předávání zpráv je zakázáno použití jiných kanálů než elektronických zpráv (e-mail), např. sociálních sítí.

Příloha 2: Seznam opatření fáze III podle ČSN ISO/IEC 27001:2013

Označení	Opatření	Popis opatření
A.14 Akvizice, vývoj a údržba systémů		
A.14.1 Bezpečností požadavky informačních systémů		
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	Při požadavku na nový IS nebo vylepšení stávajícího je nutné zahrnout do požadavků bezpečnost informací.
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	Pokud probíhá komunikace přes veřejné sítě, informace obsažené v aplikačních službách musí být chráněny.
A.14.1.3	Ochrana transakcí aplikačních služeb	Informace transakcí aplikačních služeb musí být chráněny, aby se zabránilo chybnému přenosu nebo neoprávněné změně.
A.14.2 Bezpečnost v procesech vývoje a podpory		
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	Pokud dojde ke změně provozních platforem, kritické aplikace pro činnost společnosti by měly být přezkoumány a otestovány, aby se zajistilo, že aplikace jsou stabilní a nebudou mít nepříznivý dopad na společnost.
A.14.2.9	Testování akceptace systémů	Při aktualizaci IS na novou verzi by mělo proběhnout testování IS na správnou funkčnost a bezpečnost.
A.15 Dodavatelské vztahy		
A.15.1 Bezpečnost informací v dodavatelských vztazích		
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	Pokud dodavatel získává přístup k informacím společnosti (správa, ukládání, přenos), smluvně se musí zajistit požadavky na bezpečnost informací.
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	Smlouvy s dodavateli IS a ICT musí zahrnovat požadavky na řešení rizik v oblasti bezpečnosti informací.
A.15.2 Řízení dodávek služeb dodavatelů		
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	Společnost by měla monitorovat a zkoumat kvalitu služby od dodavatele. Tu by mělo zajistit dodržování smluvních podmínek a bezpečnosti informací.
A.15.2.2	Řízení změn ve službách dodavatelů	Pokud ze strany dodavatele dochází ke změně poskytované služby, v zájmu bezpečnosti informací by změna měla být řízena s ohledem na kritičnost souvisejících informací a systémů.
A.16 Řízení incidentů bezpečnosti informací		
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování		
A.16.1.1	Odpovědnosti a postupy	Měly by být zavedeny postupy pro rychlou a efektivní odezvu na incident v bezpečnosti informací.
A.16.1.2	Hlášení událostí bezpečnosti informací	Hlášení bezpečnostní události musí být pomocí určených kanálů učiněno bezprostředně po incidentu.

A.16.1.3	Hlášení slabých míst bezpečnosti informací	Zaměstnanci společnosti jsou povinni upozornit na slabá místa nebo chyby v zabezpečení.
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	Na základě politiky a rizika je nutné klasifikovat bezpečnostní incident a rozhodnout o dalším postupu.
A.16.1.5	Reakce na incidenty bezpečnosti informací	V souladu s bezpečnostní politikou a postupy společnosti je nutné reagovat na bezpečnostní incident.
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	Znalosti z analýz a řešení incidentů se musí použít pro zlepšení bezpečnosti a tím snížení pravděpodobnosti nebo dopadu incidentů budoucích.
A.16.1.7	Shromažďování důkazů	Pro případ cíleného útoku je nutné stanovit postupy pro shromažďování a uchovávání informací, které mohou sloužit jako důkaz pro následující právní kroky.
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	Společnost by měla zavést směrnici pro požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací v nepříznivých situacích.
A.17.1.2	Implementace kontinuity bezpečnosti informací	V případě bezpečnostního incidentu, katastrofy nebo nepříznivé situace by se společnost měla řídit podle stanovených směrnic pro kontinuitu bezpečnosti informací (A.17.1.1).
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	Opatření zavedená v A.17.1.1 by měla být pravidelně ověřovat zavedená opatření pro efektivnost v případě nepříznivé situace.
A.17.2 Redundance		
A.17.2.1	Dostupnost vybavení pro zpracování informací	Společnost by měla mít v záloze základní vybavení nebo náhradní díly pro zařízení ke zpracování informací. V této společnosti to není kritické, takže stačí např. záložní pevné disky, myši, klávesnice apod.
A.18 Soulad s požadavky		
A.18.1 Soulad s právními a smluvními požadavky		
A.18.1.3	Ochrana záznamů	Záznamy společnosti musí být chráněny před ztrátou, zničením, falšováním a neoprávněnému přístupu v souladu s bezpečnostními požadavky organizace.

Příloha 3: Trasy kabeláže a umístění zásuvek