VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ ISMS VE FIRMĚ
PROPOSAL FOR THE ISMS IMPLEMENTATION IN THE COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. JAN TRUNKÁT

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. VIKTOR ONDRÁK, Ph.D.

BRNO 2015

Diplomová práce je zpracována na základě reálné firmy. Na základě podstaty práce je upraven název společnosti a některé další dílčí údaje. Práce dále neobsahuje informace, které jsou dle rozhodnutí dotyčného subjektu jeho obchodním tajemstvím či utajovanými informacemi.

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2014/2015
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Trunkát Jan, 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:

Návrh zavedení ISMS ve firmě

v anglickém jazyce:

Proposal for the ISMS Implementation in the Company

Pokyny pro vypracování:

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

Seznam odborné literatury:

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

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

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

L.S.

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

V Brně, dne 28.2.2015

ABSTRAKT

Diplomová práce je zaměřená na návrh zavedení managementu bezpečnosti informací ve firmě. Seznamuje se základními pojmy z oblasti bezpečnosti informací a obsahuje obecné postupy systému řízení informační bezpečností. V rámci práce byla provedena analýza rizik firmy a byla navržena opatření vedoucí ke snížení rizik. Práce je převážně čerpána z řady norem ISO/IEC 27000.

KLÍČOVÁ SLOVA

ISO/IEC 27000, systém řízení bezpečnosti informací, bezpečnost, bezpečnost informací, analýza rizik, bezpečnostní opatření

ABSTRACT

The master´s thesis is aimed at Proposal for the information security management system implementation in the company. It introduces with basic concepts of information security and provides general procedures for information security management system. As part of the work was carried out a risk analysis company and proposed measures to reduce risk. Work is mainly drawn from the series of standards ISO/IEC 27000.

KEYWORDS

ISO/IEC 27000, information security management system, security, information security, risk analysis, security measures

TRUNKÁT, Jan *Návrh zavedení ISMS ve firmě*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky, 2015. 76 s. Vedoucí práce byl Ing. Viktor Ondrák, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Návrh zavedení ISMS ve firmě“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu ing. Viktoru Ondrákovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Dále bych rád poděkoval panu ing. Sedlákovi za srozumitelné vysvětlení látky v rámci předmětu Management informační bezpečnosti a firmě, která se mi plně věnovala a vyhověla všem mým požadavkům.

Brno ....

(podpis autora)

OBSAH

Úvod **10**

1 Cíle práce, metody a postupy zpracování **11**

2 Teoretické východiska práce **12**

2.1 Základní pojmy a názvosloví informační bezpečnosti 12

2.2 Zákony a normy v oblasti bezpečnosti IT 14

2.2.1 Řada norem ISO/IEC 2700x 14

2.2.2 Zákony 17

2.3 Řízení informatiky a bezpečnosti informací v organizacích 18

2.3.1 Koncepce řízení informatiky organizací 18

2.3.2 Metodiky 19

2.4 Bezpečnostní hrozby 21

2.5 Analýza rizik 22

2.5.1 Stanovení hranice analýzy rizik 22

2.5.2 Identifikace aktiv 23

2.5.3 Stanovení hodnoty a seskupování aktiv 23

2.5.4 Identifikace hrozeb 23

2.5.5 Analýza hrozeb a zranitelnosti 23

2.5.6 Pravděpodobnost jevu 23

2.5.7 Měření rizika 23

2.6 Informační systém 24

2.7 Informační bezpečnost 24

2.8 Bezpečnost počítačové sítě 25

2.8.1 Vnější hrozby 26

2.8.2 Vnitřní hrozby 26

2.9 Bezpečnostní politika 26

2.10 Systém řízení bezpečnosti informací 27

2.10.1 Všeobecně 27

2.10.2 Ustavení a řízení ISMS 28

2.10.3 Požadavky na dokumentaci 30

2.10.4 Odpovědnost vedení 31

2.10.5 Interní audity ISMS 32

2.10.6 Přezkoumání ISMS vedením organizace 33

2.10.7 Zlepšování ISMS 33

3 Analýza současného stavu **35**
3.1 Popis firmy . . . 35
3.2 Bezpečnost ve firmě . . . 35
3.2.1 Situační analýza . . . 35
3.2.2 Informační situace v podniku . . . 36
3.3 Analýza rizik a bezpečnostních hrozeb . . . 36
3.3.1 Identifikace a hodnocení aktiv . . . 37
3.3.2 Identifikace hrozeb a zranitelnosti . . . 37
3.3.3 Metoda analýzy rizik . . . 39
3.4 Shrnutí analýzy . . . 44

4 Vlastní návrh řešení **45**
4.1 Zavedení ISMS . . . 45
4.1.1 Soubor opatření . . . 45
4.1.2 Plán zavedení opatření . . . 50
4.2 Popis první etapy zavedení opatření . . . 50
4.2.1 A.5 Politiky bezpečnostní informací . . . 50
4.2.2 A.6 Organizace bezpečnosti informací . . . 51
4.2.3 A.7 Bezpečnost lidských zdrojů . . . 52
4.2.4 A.8 Řízení aktiv . . . 55
4.2.5 A.9 Řízení přístupu . . . 58
4.2.6 A.11 Fyzická bezpečnost a bezpečnost prostředí . . . 59
4.2.7 A.12 Bezpečnost provozu . . . 61
4.2.8 Náklady na první etapu . . . 63
4.2.9 Časový harmonogram první etapy . . . 66
4.3 Provoz, monitorování, přezkoumávání, údržba a zlepšování . . . 70

Závěr **71**

Literatura **72**

Seznam symbolů, veličin a zkratek **74**

ÚVOD

V dnešním digitalizovaném světě se všude nachází spousty elektronických dat a informací. Tak je tomu i ve firmách či různých organizacích a s tím souvisí i otázka bezpečnosti těchto dat a informací, protože každá firma či organizace si chce chránit své know-how a je i ze zákona povinna zabránit úniku informací o osobních údajích ať už dodavatelů, odběratelů či zaměstnanců. Pro stanovení doporučené bezpečnosti se využívají normy řady 27000 a s tím souvisí zavedení systému řízení bezpečnosti informací, který obsahuje nejlepší postupy jak chránit data a informace. Tato práce je zaměřena na návrh zavedení systému řízení bezpečnosti informací ve firmě. V Kapitole 1 jsou sepsány cíle práce, metody a postupy zpracování. V Kapitole 2 bude čtenář seznámen se základními pojmy a názvoslovími z informační bezpečnosti i se souvisejícími zákony a normami v této oblasti a nakonec se všeobecným popisem systému řízení bezpečnosti informací vycházejícího z normy ISO/IEC 27001. V Kapitole 3 bude popsán aktuální stav firmy, pro kterou je ISMS navrhováno, a bude zde nacházet jedna z nejdůležitějších části práce a to je analýza rizik, kde dochází k identifikaci a ohodnocení aktiv, hrozeb a zranitelností. Kapitola 4 bude řešit výsledky rizik, kde dojde k zavedení ISMS a tím pádem navrhování opatření, které by bylo vhodné zavést nebo aktualizovat, a dojde zde k sestavení plánu, kdy budou jednotlivá opatření zaváděna. Předposlední sekce kapitoly se bude věnovat jedné etapě při zavádění, bude zobrazovat náklady na etapu a bude zde i navržen plán jak by se mohlo postupovat při zavádění etapy. Jelikož ISMS je nikdy nekončící proces, jak se čtenář dočte v práci, tak v poslední sekci kapitoly bude náznak jak by se mohlo pokračovat při provozování ISMS.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Hlavním cílem práce je návrh zavedení systému řízení bezpečnosti informací ve firmě. Před zavedením je nejdříve zapotřebí se seznámit s problematikou ISMS, která je popsána v normě ISO/IEC 27001. Není zapotřebí splnit všechny požadavky normy ISO/IEC 27001, jelikož zatím zájem o certifikace není, ale norma bude sloužit jako předloha pro návrh zavedení ISMS. U firmy je nutné zanalyzovat aktuální stav bezpečnosti a to jak z fyzické tak z technologické stránky. Důležitým faktorem úspěchu je podpora ze strany vedení a vycházení vstříc všem dotazům. Dalším důležitou etapou ke správnému návrhu bezpečnostních opatření je analýza rizik. Na rizika, které vzejdou z identifikace a ohodnocení aktiv, hrozeb a zranitelností, jsou navrženy bezpečnostní opatření, které by měla firma přijmout.

2 TEORETICKÉ VÝCHODISKA PRÁCE

V této části práce budou vysvětleny základní pojmy a názvosloví z oblasti informační bezpečnosti a popsány zákony a normy, které se týkají informační bezpečnosti.

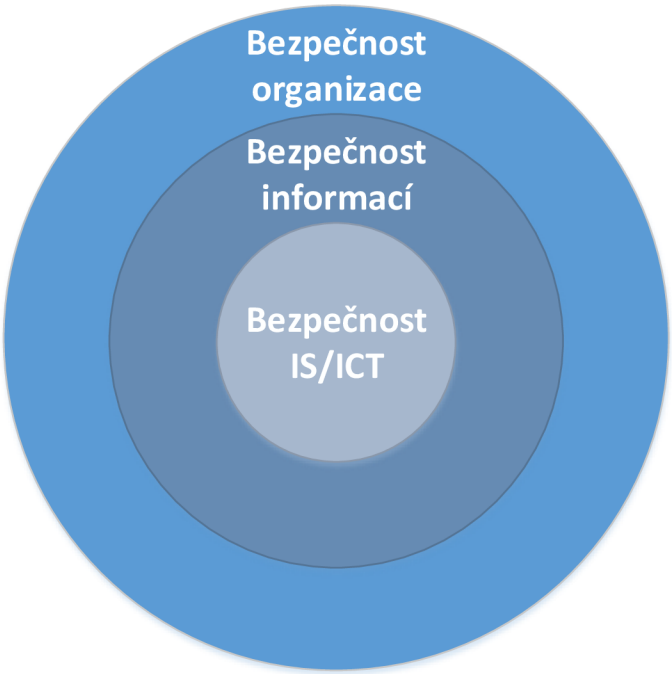
2.1 Základní pojmy a názvosloví informační bezpečnosti

Aby bylo možné přistoupit k zavedení a řízení informační bezpečnosti je nutné si sjednotit pojmy, které se zde vyskytují. V následujících odrážkách jsou tyto pojmy vysvětleny dle [1].

- **akceptace rizik (risk acceptance)** - rozhodnutí přijmout riziko
- **aktivum (asset)** - cokoliv, co má pro organizaci nějakou hodnotu
- **analýza rizik (risk analysis)** - systematické používání informací k odhadu rizika a k určení jeho zdrojů
- **autentičnost (authenticity)** - vlastnost zajišťující, že identita subjektu nebo zdroje je taková, za kterou je prohlašována
- **bezpečností incident, útok (information security incident attack)** - jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti organizace a ohrožení bezpečnosti informací
- **bezpečnost informací (information security)** - zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojení priority např.: autentičnost
- **bezpečnostní politika (security policy)** - celkový záměr a směr dosažení bezpečnosti, formálně vyjádřený vedením organizace
- **bezpečnostní událost (information security event)** - identifikovaný stav systému. služby nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření
- **dostupnost (availability)** - informace je pro oprávněné (autorizované) uživatele přístupná v okamžiku její potřeby
- **důvěrnost (confidentiality)** - informace jsou přístupné nebo sdělené pouze těm, kdo jsou k tomu oprávněni
- **hrozba (threat)** - potencionální příčina nechtěného incidentu, která může vyústit v poškození systému nebo organizace
- **integrita (integrity)** - zajištění správnosti a úplnosti informací a metod zpracování zabráněním neautorizovaným modifikacím
- **nepopiratelnost (non-repudation)** - rozšíření chápaní autentičnosti z pouhé ověřitelnosti původnosti, na nemožnost popření deklarovaného původu

- **odpovědnost (accountability)** - vždy musí být explicitně vyjádřena (kdo, za co...)
- **riziko (risk)** - funkce pravděpodobnosti, že zdroj hrozby využije konkrétní potencionální zranitelnost a způsobí organizaci nepříznivou událost
- **zranitelnost (vulnerability)** - vada nebo slabina v bezpečnostních opatřeních, v návrhu, v implementaci, která může být náhodně či záměrně využita jednou nebo více hrozbami

V souvislostí s bezpečností informací je zapotřebí zmínit i pojmy **bezpečnost organizace nebo firmy** a **bezpečnost IS/ICT**. Vztahy mezi nimi jsou zobrazeny na Obrázku 2.1.



Obr. 2.1: Úrovně bezpečnosti ve firmě [2]

Bezpečnost organizace je na nejvyšší úrovni bezpečnosti. Spadá tady zajištění bezpečnosti objektu nebo majetek organizace. Zároveň může pomoct ostatním úrovním jako například bezpečnosti IS/ICT tím, že se bude kontrolovat fyzický přístup do objektu/budovy. [2]

Bezpečnost informací je součástí bezpečnosti organizace a jejím cílem je shrnutí zásad bezpečné práce s informacemi všech druhů a typů. Navíc se stará nejen o digitální data, ale i o způsob zpracování uložení a správy archive nedigitálních dat,

zásady skartace materiálů, jak nakládat s informacemi při přesunu mimo objekt atd. [2]

Bezpečnost IS/ICT chrání pouze aktiva a to „jen“ ta, která patří k informačnímu systému organizace, podporovaného informačními a komunikačními technologiemi. Tato nejužší oblast pracuje s "neviditelnými"daty, informacemi a službami. [2]

2.2 Zákony a normy v oblasti bezpečnosti IT

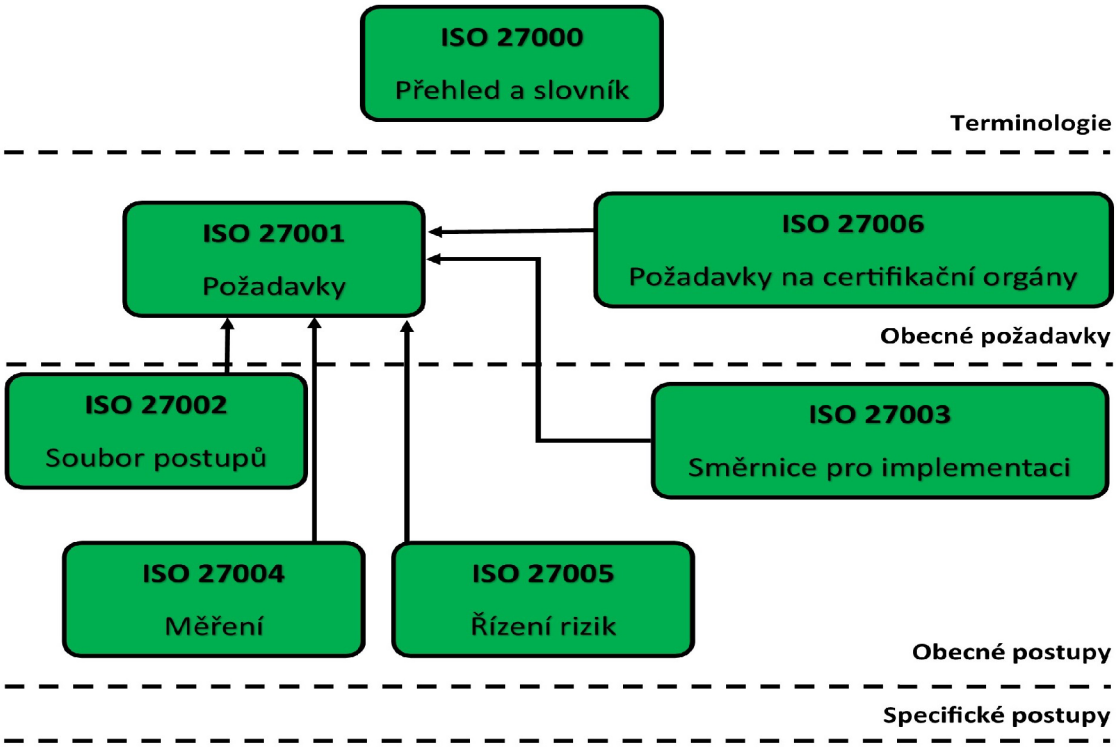
Při budování bezpečnosti IT i řízení je třeba brát v úvahu aktuální zákony a normy (doporučení). ISMS vychází z rodiny norem ISO/IEC 2700x. ISO (International Organization for Standardization) mezinárodní organizace pro normalizaci.

2.2.1 Řada norem ISO/IEC 2700x

Tuto řadu norem rezervovala ISO pro řízení informační bezpečnosti v organizacích. [13]

- **ISO/IEC 27000** - ISMS - přehled a slovník
- **ISO/IEC 27001** - ISMS - požadavky
- **ISO/IEC 27002** - soubor postupů pro opatření bezpečnosti informací
- **ISO/IEC 27003** - směrnice pro implementaci systému řízení bezpečnosti informací
- **ISO/IEC 27004** - ISMS - měření
- **ISO/IEC 27005** - řízení rizik bezpečnosti informací
- **ISO/IEC 27006** - požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
- **ISO/IEC 27007** - směrnice pro audit ISMS
- **ISO/IEC TR 27008** - směrnice pro audit opatření ISMS
- **ISO/IEC 27010** - směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi
- **ISO/IEC 27011** - směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002
- **ISO/IEC 27013** - návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1
- **ISO/IEC 27014** - správa bezpečnosti informací
- **ISO/IEC 27015** - směrnice pro řízení bezpečnosti informací pro finanční služby
- **ISO/IEC 27016** - řízení bezpečnosti informací - organizační ekonomika

Provázanost rodiny norem 2700x je zobrazena na Obrázku 2.2.



Obr. 2.2: Základní struktura norem řady ISO 2700x

Norma ISO/IEC 27000

Předmětem této mezinárodní normy je podání jakého si přehledu systémů řízení bezpečnosti informací a souvisejících termínů a definic. Norma najde využití ve všech typech a velikostech organizací. [13]

Norma ISO/IEC 27001

Norma poskytuje podporu pro ustanovení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací. Spadá do strategických rozhodnutí organizací, které chtějí přijmout systém řízení bezpečnosti informací. Faktory ovlivňující ustavení a zavedení systému řízení bezpečností informací je hned několik a v čase se můžou měnit. Spadají sem např.: potřeby a cíle organizace, požadavky na bezpečnost a podobně. U řízení rizik je důležité zachovat důvěrnost, dostupnost a integritu a toto systém řízení bezpečnosti informací splňuje. V příloze A této normy se nachází tabulka s opatření, které jsou odvozeny a propojeny s normou ISO/IEC 27002. [15]

Norma ISO/IEC 27002

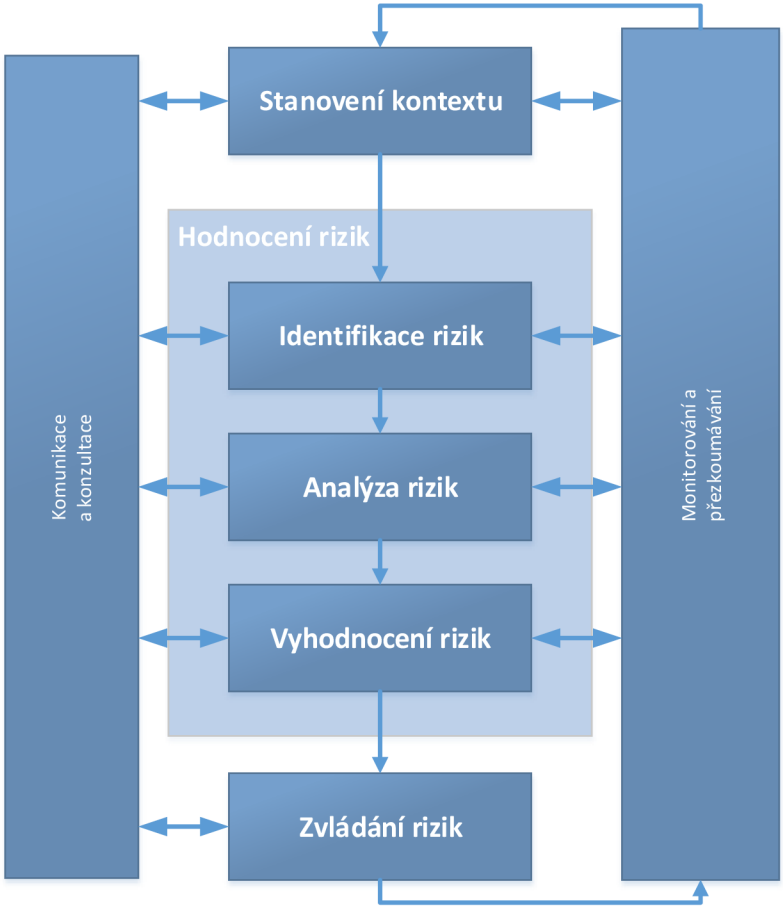
Norma obsahuje výčet opatření a slouží tedy jako doporučení pro výběr opatření při zavádění systému řízení bezpečnosti informaci, který je založen na normě ISO/IEC 27001 a zároveň může sloužit i jako pokyny pro společnosti zavádějící přijaté opatření bezpečnosti informací. Norma může sloužit i při vytváření směrnic pro řízení bezpečnosti informací pro průmysl. Obsahuje celkem 14 kapitol o opatřeních a dohromady mají celkem 35 hlavních kategorií bezpečnosti a 114 kontrol. Kapitoly a kolik obsahují hlavních kategorií a opatření jsou vypsány v Tabulce 2.1. [16]

Označení	**Název kapitoly**	**Počet kategorií**	**Počet opatření**
A.5	Politiky bezpečnosti informací	1	2
A.6	Organizace bezpečnosti informací	2	7
A.7	Bezpečnost lidských zdrojů	3	6
A.8	Řízení aktiv	3	10
A.9	Řízení přístupu	4	14
A.10	Kryptografie	1	2
A.11	Fyzická bezpečnost a bezpečnost prostředí	2	15
A.12	Bezpečnost provozu	7	14
A.13	Bezpečnost komunikací	2	7
A.14	Akvizice, vývoj a údržba systémů	3	13
A.15	Dodavatelské vztahy	2	5
A.16	Řízení incidentů bezpečnosti informací	1	7
A.17	Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací	2	4
A.18	Soulad s požadavky	2	8
	Celkem = 14	**35**	**114**

Tab. 2.1: Hlavní oblasti pro opatření dle normy ISO/IEC 27002 [16]

Norma ISO/IEC 27005

Předmětem normy je poskytnutí doporučení pro řízení rizik bezpečnosti informací. Podporuje obecný koncept, který se nachází v normě ISO/IEC 27001. Je udělána strukturovanou formu pro podporu implementace informační bezpečnosti založené na přístupu řízení rizik. [12]



Obr. 2.3: Proces řízení rizik dle ISO/IEC 27005 [12]

2.2.2 Zákony

V úvahu je třeba brát i zákony týkající se informační společnosti a prosazování ochrany užívání IS/ICT. Při budování bezpečnosti informací je třeba se i těmto zákonům věnovat. V této kapitole budou zmíněny jen ty, které se dotýkají problematiky práce. Popis zákonů vychází z citace uvedených zákonů.

- *zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů* - Tento zákon v souladu s právem Evropské unie, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států
- *zákon č. 106/1999 Sb. o svobodném přístupu k informacím* - Tento zákon za-

pracovává příslušný předpis Evropských společenství a upravuje pravidla pro poskytování informací a dále upravuje podmínky práva svobodného přístupu k těmto informacím

- *zákon č. 227/2000 Sb. o svobodném přístupu k informacím* - Tento zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem
- *zákon č. 480/2004 Sb. o některých službách informační spolehlivosti* - Tento zákon upravuje v souladu s právem Evropských společenství odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení

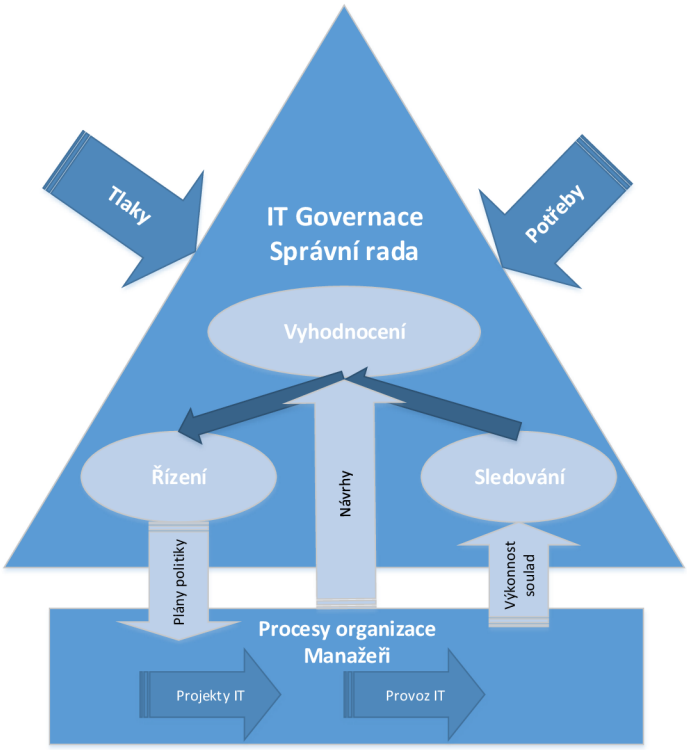
2.3 Řízení informatiky a bezpečnosti informací v organizacích

2.3.1 Koncepce řízení informatiky organizací

V dnešní době se nejvíce využívají dvě koncepce řízení informatiky organizací. První koncepce je **IT Governance**, která vzešla rozšířením koncepce Corporate Governance a Enterprise Governance, a druhou koncepcí potom je **IT Service Management**, která má své pole působnosti na nižší úrovni řízení informatiky a jejím účelem je poskytování služeb informačních technologií. [2]

IT Governance - ITG (IT správa a řízení)

IT Governance se definuje jako struktura řídících vztahů a procesů umožňující dosažení cílů organizace realizací přidané hodnoty ze současného vyrovnání rizika s návratností investic do informačních technologií. Pojem řídící vztah je brán jako vztah mezi vlastníky a vedením organizace a pojem procesy zahrnuje: stanovení cílů, určení návodů, jak jich dosáhnout a měření spotřeby zdrojů při jejich realizaci. Primárním cílem ITG je transparentnost rizik organizací a ochrana hodnot vlastníků. Řízení bezpečnosti informací je založeno na stejných cílech. Používaný model je znázorněn na Obrázku 2.4. [2]



Obr. 2.4: Model IT Governance dle [2]

IT Service Management - ITSM (Řízení služeb IT)

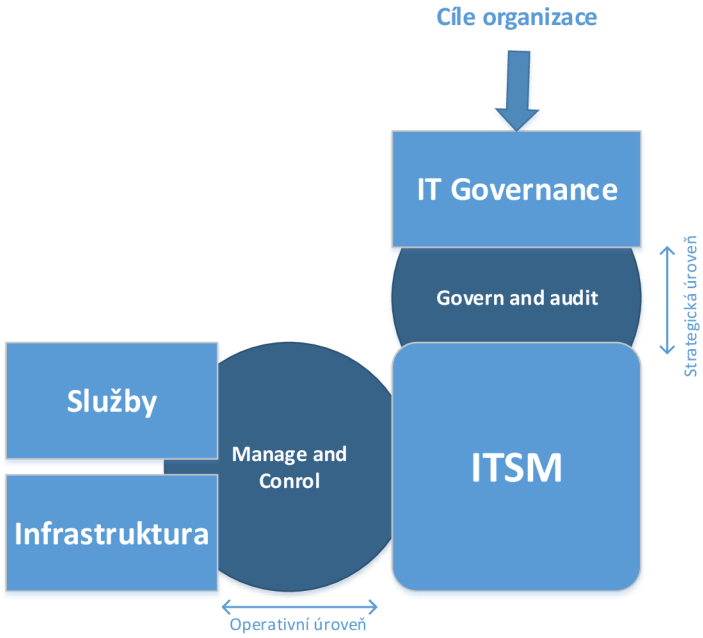
Jedná se o postup, který zohledňuje principy a praktiky pro návrh, dodávku a správu služeb IT v domluvené kvalitě, podporující klíčové aktivity zákazníka. Vztah mezi ITG a ITSM je na Obrázku 2.5. [2]

2.3.2 Metodiky

Aby předešlé koncepce řízení správně fungovaly, je zapotřebí podpory ve formě různých standardů, zkušeností nebo metodik. Budou zde popsány metodiky a knihovna, které se zabývají nejen řízení bezpečnosti, ale i dalšími aspekty řízení informatiky v organizacích. [2]

Knihovna ITIL

ITIL (information technology infrastructure library) je sada publikací s nejlepšími praktikami pro správu služeb IT. Knihovna ITIL poskytuje návod na zajištění kvalitních služeb IT a potřebných podpůrných procesů, funkcí a dalších způsobilostí.



Obr. 2.5: Vztah ITG a ITSM dle [2]

Rámec ITIL je založen na celoživotním cyklu (strategie služeb, návrh služeb, přechod služeb, provoz služeb a neustálého zlepšování služeb), každá z těchto fází má vlastní podpůrnou publikaci. [3]

Metodika COBIT

CobiT (control objectives for information and related technology) je mezinárodně uznávanou metodikou, která má základ v souboru všeobecně uznávaných praktik řízení informačních a komunikačních technologií a to takovým způsobem, aby využití informací a nasazení ICT přispívalo k dlouhodobému rozvoji organizace, prohlubovalo její strategické cíle a snižovalo rizika souvisejících s použitím ICT. Popis os kostky COBIT je následující: informační kritéria (osa x), IT zdroje (osa z) a IT proces (osa y). Mezi požadavky na informační kritéria patří: [4]

- *efektivita* - požadavky na včasné doručování relevantních informací ve správném, konzistentním a použitelném tvaru
- *účinnost* - požadavky na zpracování informací (nejekonomičtějším a nejproduktivnějším způsobem) prostřednictvím optimálního využívání zdrojů informatiky
- *důvěryhodnost* - požadavky zahrnující ochrany důležitých informací proti neautorizovanému použití (prozrazení)

- *integrita* - požadavky týkající se přesnosti a kompletnosti informace ve vztahu k požadavkům podnikání a jeho očekáváním
- *dostupnost* - požadavky týkající se dostupnosti informace pro podnikání a týkající se také ochrany potřebných zdrojů
- *soulad* - požadavky týkající se udržování souladu se zákony, směrnicemi, regulacemi a kontraktačními podmínkami, které se týkají procesů podnikání (hlavních podnikových procesů)
- *spolehlivost* - požadavky vztahující se k přínosu informace pro rozhodování manažerů

Mezi zdroje IT patří: [4]

- *aplikace*
- *informace*
- *infrastruktura*
- *lidé*

Mezi procesy IT patří: [4]

- *domény*
- *procesy*
- *aktivity*

Metodika CRAMM

Je metodika a soubor softwarových nástrojů pro zavádění a podporu systému řízení bezpečnosti informací, pro provádění identifikace a ohodnocení aktiv, analýzy rizik informačních systémů a sítí, k návrhu bezpečnostních opatření, určování havarijních požadavků na informační systém a k návrhům na řešení havarijní situaci. CRAMM se vyskytuje ve dvou formách. První je *CRAMM Express*, která je jednodenní analýzou rizik využívající pouze opatření ze tří kategorií z knihovny opatření, a druhou je *CRAMM Expert*, která je detailní analýzou rizik disponující s plnohodnotnou knihovnou opatření.

2.4 Bezpečnostní hrozby

Definice hrozeb byla zmíněná již výše. Tato podkapitola přináší bližší pohled na hrozby. Dělení hrozeb podle původu: [4]

- přírodní (požár, zemětřesení)
- způsobené lidským faktorem (chyba zaměstnance).

Rozlišení hrozeb podle úmyslu: [4]

- náhodné (zapomenuté dokumenty na veřejném místě s citlivými informacemi)
- úmyslné (krádež).

Úmyslné i náhodné hrozby by kvůli bezpečnosti měly být identifikovány a následně by měla být odhadnuta jejich úroveň a pravděpodobnost výskytu. Hrozby je možné seskupit do skupin podle toho na jaké aktivum působí. Výčet možných skupin: [4].

- operační systém
- aplikace
- databáze
- síť
- klient

Hrozby se nejčastěji posuzují podle otázek: [4]

- ztráta důvěrnosti
- ztráta integrity
- ztráta dostupnosti
- ztráta individuální odpovědnosti
- ztráta spolehlivosti

Mezi nejčastější hrozby patří: [4]

- selhání dodávky energie
- škodlivý software
- selhání hardwaru
- selhání komunikačních služeb

2.5 Analýza rizik

Analýza rizik je jednou z nejdůležitějších etap za účelem zjištění zranitelných míst informačního systému organizace. Na základě této analýzy se zjišťuje seznam působících hrozeb. Výsledkem analýzy je dokument, který má za účel snížení rizik na přijatelnou úroveň. [5]
Obecný postup analýzy rizik je zpracován v následujících podkapitolách dle [6].

2.5.1 Stanovení hranice analýzy rizik

Jedná se o pomyslnou čáru, která nám odděluje zahrnutá aktiva a ostatní aktiva. O tom, která aktiva zahrnout a která ne, rozhoduje management, kdy se vychází z jejich záměrů. [6]

2.5.2 Identifikace aktiv

V tomto kroku jsou vypsána všechna aktiva spadající do zahrnutých aktiv z předešlého kroku. K zahrnutým aktivům se standardně uvádí název a umístění. [6]

2.5.3 Stanovení hodnoty a seskupování aktiv

K aktivům musí být přiřazeny hodnoty a to podle toho jak velkou škodu by způsobili při případné ztrátě nebo zničení. Při sestavování takových hodnot se vychází zejména z nákladových charakteristik. Důležité je i rozlišení aktiv zda se jedná o jedinečné aktivum nebo aktivum jednoduše nahraditelné. Může se využít i seskupování aktiv s podobnými vlastnostmi pro lepší následující manipulaci. Aktivu je přiřazena hodnota (ocenění) a je i zásadní mít pro něj nastavený způsob ochrany. [6]

2.5.4 Identifikace hrozeb

Za hrozbu se považuje cokoliv co může nějakým negativním způsobem ovlivnit aspoň jedno z aktiv. Tyto hrozby se vybírají ze seznamu hrozeb, který je sestaven podle literatury nebo na základě vlastních zkušeností, průzkumů dříve provedených analýz. [6]

2.5.5 Analýza hrozeb a zranitelnosti

Výsledkem tohoto kroku je seznam dvojic aktivum-hrozba. Všechny identifikované hrozby z předešlého kroku se hodnotí vůči všem vybraným aktivům. Pokud hrozba má vliv na konkrétní aktivum tak se určí úroveň hrozby a úroveň zranitelnosti. V tomto kroku se berou v potaz již realizovaná bezpečnostní opatření, které můžou snížit jak úroveň hrozby, tak úroveň zranitelnosti. [6]

2.5.6 Pravděpodobnost jevu

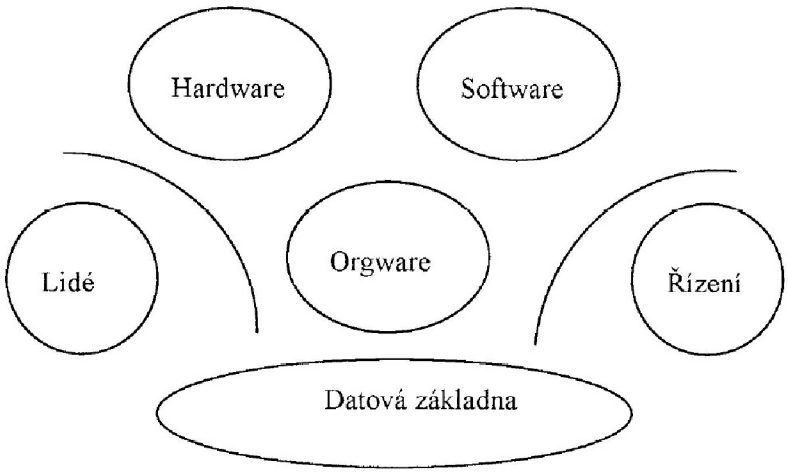
Jak název tohoto kroku napovídá jedná se o to, že nevíme, zda zkoumaný jev nastane. A proto s k popisu jevu ještě připisuje údaj o pravděpodobnosti výskytu jevu. [6]

2.5.7 Měření rizika

Míra rizika je v každé situaci jiná a závisí na hodnotě aktiva, úrovni hrozby a zranitelnosti aktiva. [6]

2.6 Informační systém

Informační systém (IS) můžeme chápat jako systém, kde jsou mezi sebou propojeny informace a procesy, které využívají tyto informace. Procesy lze charakterizovat jako funkce, které zpracují vstupující informace do systému a převedou je na informace, které ze systému vystupují. Jiná teorie definuje informační systém jako soubor lidí (zdrojů, zpracovatelů, uživatelů), technických prostředků a metod, zabezpečujících sběr, přenos, uchování a zpracování dat za účelem tvorby a prezentace informací pro potřeby uživatelů. [7]



Obr. 2.6: Obecné schéma informačního systému [8]

Informační systém se standardně skládá z několika položek jako první máme *data*, která jsou obvykle umístěna nějakém *médiu* (HDD, SSD, CD, DVD, flash disk). Pro práci s médiem je zapotřebí *HW* (PC, server, NAS) a na něm je obvykle nainstalován *SW* (OS, aplikace). K datům, obzvlášť těm na serveru a NASu, je zapotřebí přistupovat skrz *síť* (LAN, WAN, MAN, WiFi). Všechny tyto prvky jsou někde *umístěny* a *někdo* s nimi pracuje. [10]

2.7 Informační bezpečnost

Bezpečnost jako takovou si můžeme uvést jako ochranu něčeho před něčím (poškození, zničení, ztráta nebo zcizení) a informační bezpečnost si potom můžeme uvést jako ochranu informací před těmito hrozbami. S informační bezpečnosti se tedy pojí již zmíněné pojmy jako *narušení integrity*, které nastane když dojde k poškození, dále *narušení dostupnosti*, ke kterému dojde při zničení informace, a v poslední řadě *narušení důvěrnosti* a k tomu dojde v případě ztráty či zcizení informace.

Z čeho se skládá IS již bylo zmíněno o sekci výše a bylo tak i poukázáno na to, co všechno se dá považovat za aktiva společnosti a jestli se tedy mají všechny tyto aktiva chránit je zapotřebí k nim zavést příslušná opatření: [10]

- **personální bezpečnost** - nejčastější riziko pro vytvoření bezpečnostního incidentu tvoří lidi a proto je třeba vybírat kvalifikované a přemýšlející lidi
- **fyzická bezpečnost** - jedná se o zabezpečení místností, kde se nachází HW, média a lidé, a jedná se o ochranu nejen přírodního charakteru (požár), ale i před úmyslným poškozením ze strany lidí
- **technologická bezpečnost** - slouží k zajištění přístupu k SW pro zajištění důvěrnosti, integrity a dostupnosti
- **organizační bezpečnost** - je potřeba zajistit řízení bezpečnosti, ustanovení odpovědnosti a povinnosti jednotlivých skupin a osob v organizaci a to vše směřuje k sestavení bezpečnostní politiky

Etapy procesu informační bezpečnosti jsou znázorněny na Obrázku 2.7 a slouží jako postup řešení informační bezpečnosti v podniku. Výstupem každého procesu je souhrn několika dokumentů. Etapy na sebe navazují a je zde i možnost se vrátit k předešlé etapě. Proces pravidelně cyklí vzhledem, aby bylo možné reagovat na případné změny. [9]

Obr. 2.7: Etapy procesu informační bezpečnosti [9]

2.8 Bezpečnost počítačové sítě

Bezpečnost počítačové sítě je důležitá pro ochranu informací a dat obsažených v počítači v síti či na serveru. Platí tedy čím je síť lépe přístupná, tím méně je zabezpečená. Ochrana dat a informací je problémem každé organizace a je jen na ni jaké

politik či směrnice si tam nastaví. Rizika, kterým čelí počítačová síť, si lze rozdělit na dvě skupiny: **vnější hrozby** a **vnitřní hrozby**. [9].

2.8.1 Vnější hrozby

Můžou se nacházet v několika základních formách: [9].

- *neautorizované použití hesel a klíčů*
- *DoS útok*
- *odposlech IP adres*
- *počítačové viry a červi*
- *trojské koně*

2.8.2 Vnitřní hrozby

V organizacích nejčastěji hrozí ze strany zaměstnanců: [9].

- *krádež*
- *zneužití*
- *zničení dat.*

Zaměstnanci porušují bezpečnostní pravidel nejčastěji z těchto důvodů: [9].

- *průmyslová špionáž*
- *vnitřní politika*
- *rozhněvaní zaměstnanci (i bývalí)*
- *neúmyslné přestupky*
- *vzpurní uživatelé.*

2.9 Bezpečnostní politika

Tvorba bezpečnostní politiky vychází z analýzy rizik a může se dělit na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku. Celková bezpečnostní politika je stručnější a obsahuje: co se bude chránit, kdo za to nese odpovědnost, jakým způsobem se bude postupovat při budování bezpečnosti, kdežto systémová bezpečnostní politika definuje způsob implementace v konkrétním prostředí daného systému. Obě politiky směřují ke stanovení strategických opatření na úrovni IS. Při sestavování bezpečnostní politiky se musí stanovit cíl a rozsah, pro koho je závazná, charakteristika IS, východiska bezpečnosti (zákony, normy) atd. Neexistuje žádná univerzální bezpečnostní politika a to z důvodu, že každá organizace má jinou strukturu, jiný IS atd. Rozsáhlejší politika bývá standardně rozdělena na bezpečnost fyzickou, personální, administrativní a procedurální, bezpečnost IS a komunikační. Další části, které by měla bezpečnostní politika obsahovat, jsou: bezpečnostní řízení

IS (popis rolí, zodpovědnosti, pravomocí), řešení incidentů, testování bezpečnosti, havarijní plán (může být také formou zvláštního dokumentu). Bezpečnostní politika by měla být známa, platnost by měla mít vyhlášenou ke konkrétnímu dni a ve formě vnitřního dokumentu. [11]

2.10 Systém řízení bezpečnosti informací

Systém řízení informační bezpečnosti (ISMS, Information Security Management System) se skládá z pravidel, postupů, pokynů, souvisejících zdrojů a činností společně řízené organizací ve snaze o ochranu svých informačních aktiv. [13]

ISMS je založeno na využití modelu PDCA (Demingův model). Koncept modelu PDCA je znázorněn na Obrázku 2.8, kde i analogicky jsou znázorněny procesy ISMS. PDCA je metoda postupného zlepšování, protože poskytuje i zpětnou vazbu, a zobrazuje životní cyklus ať už jde o vývoj softwaru nebo zlepšování kvality výroby. [13]

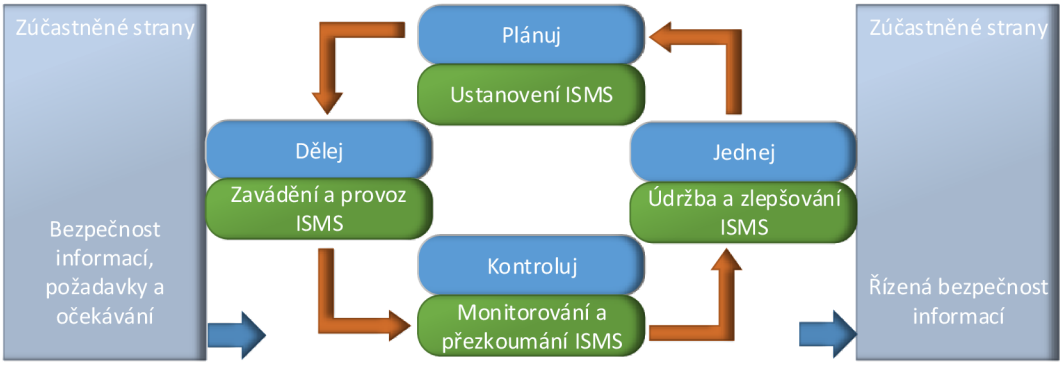
Zavádění ISMS se musí dělat na míru podniku, tzn. že neexistuje jednotné řešení. Na míru hned z několika z důvodů: každý podnik má jiná aktiva, jiné složení zaměstnanců, jiné priority atd. a to dělá z každého podniku podnik jedinečný. Popis postupu zavedení ISMS je popsán následujících v kapitolách převzatých z normy ISO/IEC 27001. [14]

2.10.1 Všeobecně

Přijetí ISMS je možná strategická volba každé organizace. Návrh a zavedení ISMS v organizaci probíhá na základě potřeb a cíli činnosti organizace, ze kterých potom vyplývají požadavky na bezpečnost. Norma prosazuje přijímat procesní přístup pro *ustavení, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti* ISMS v organizaci. Jak již bylo výše zmíněno tak procesy ISMS jsou aplikovány na PDCA model: [14]

- **ustanovení ISMS (plánuj)** - ustavení politiky ISMS, cílů, procesů a postupů souvisejících s řízením rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace
- **zavádění a provoz ISMS (dělej)** - zavedení a využívání politiky ISMS, opatření, procesů a postupů
- **monitorování a přezkoumání ISMS (kontroluj)** - posouzení, kde je to možné i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání

- **údržba a zlepšování ISMS (jednej)** - provedení opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS



Obr. 2.8: PDCA model aplikovaný na procesy ISMS dle [15]

2.10.2 Ustavení a řízení ISMS

Ustavení ISMS

V rámci ustanovení je organizace povinna provést: [14]

- definici rozsahu a hranic ISMS podle konkrétních rysů činností organizace, jejího uspořádání, struktury, lokality, aktiv a technologií
- definici politiky ISMS podle podle konkrétních rysů činností organizace, její struktury, umístění aktiv a technologií zahrnující rámec pro stanovení cílů organizace a ustanovení celkového směru řízení a rámce zásad činnosti týkajícího se bezpečnosti informací. Dále je třeba brát v úvahu: požadavky vyplývající z činnosti organizace a legislativní nebo regulátorní požadavky, stanovení kritérií pro hodnocení rizika, ale hlavně schváleno vedením
- zvolení metodiky pro hodnocení rizik a to takové, která vyhovuje ISMS a stanovené bezpečnosti informací, legislativním a regulatorním požadavkům. Určení kriterií pro akceptaci rizik
- identifikaci rizik což znamená identifikaci aktiv a jejich vlastníků, identifikaci hrozeb pro tato aktiva, identifikace zranitelnosti a identifikace dopadu na aktiva při ztrátě důvěrnosti, integrity a dostupnosti

- analýzu a vyhodnocování rizik, kde se ohodnocují dopady na činnost organizace, které by mohly vyplynout ze selhání bezpečnosti dále ohodnocení pravděpodobnosti selhání bezpečnosti, které by se mohlo objevit působením existujících hrozeb a zranitelností a dopady na konkrétní aktiva s přihlédnutím k aktuálně zavedeným opatřením. Odhadnutí úrovně rizik a určení akceptovatelnosti těchto rizik
- identifikaci a vyhodnocení variant pro zvládání rizik tzn.: aplikace vhodných opatření, vyhnutí se rizikům, akceptace rizik splňující politiku organizace a kritéria pro akceptaci rizik, přenos rizik spojených s činností organizace na třetí stranu
- vybrání cílů opatření a jednotlivých bezpečnostních opatření pro zvládání rizik
- získání souhlasu vedení organizace s navrhovanými zbytkovými riziky
- získání povolení ze strany vedení organizace k zavedení a provozu ISMS
- připravení prohlášení o aplikovatelnosti, které musí obsahovat: cíle opatření a jednotlivá vybraná bezpečnostní opatření a důvody jejich výběru, cíle opatření a jednotlivá bezpečnostní již implementované v organizaci, vyřazené cíle opatření a jednotlivá vyřazená bezpečnostní opatření a jejich důvod vyřazení. Poskytuje souhrn jak bude naloženo s identifikovanými riziky

Zavádění a provozování ISMS

V rámci zavádění a provozování je organizace povinna provést: [14]

- formulaci plánu zvládání rizik, který vymezí odpovídající řídící činnosti, zdroje, odpovědnosti a priority pro řízení rizik bezpečnosti informací
- realizaci plánu zvládání rizik pro dosažení určených cílů opatření i s úvahou na finanční a lidské zdroje a přiřazením rolí a odpovědnosti
- realizaci bezpečnostních opatření zvolených pro naplnění cílů těchto opatření
- určení způsobu, kterým se bude měřit účinnost vybraných opatření případně skupin opatření a stanovení způsobu vyhodnocení těchto měření a to tak, aby závěry hodnocení mohly být porovnány i opakovány
- realizaci programů pro školení a pro zvyšování bezpečnostního povědomí
- řízení provozu ISMS
- řízení zdrojů ISMS
- realizaci kroků a dalších opatření pro rychlou detekci a reakci na bezpečnostní události a kroky reakce na bezpečnostní incident

Monitorování a přezkoumání ISMS

V rámci monitorování a přezkoumání je organizace povinna provést: [14]

- monitorování, přezkoumávání a zavádění dalších opatření např.: pro včasnou detekci chyb zpracování, úspěšných a neúspěšných pokusů o narušení bezpečnosti a detekci bezpečnostních incidentů. Dále umožnit vedení organizace určit lidi, zda bezpečnostní aktivity fungují jak mají, umožnění detekce bezpečnostních událostí a tím zabránění vzniku bezpečnostních incidentů a umožnění vyhodnocení účinnosti kroků podniknutých při narušení bezpečnosti
- pravidelné přehodnocování účinnosti ISMS s ohledem na výsledky bezpečnostních auditů, incidentů, výsledku měření účinnosti opatření, návrhu a podnětu všech zainteresovaných stran
- měření účinnosti zavedených opatření pro ověření naplnění požadavků na bezpečnost
- pravidelné provádění přezkoumání hodnocení rizik a přehodnocování úrovně zbytkového a akceptovaného rizika s ohledem na změny
- provádění pravidelných interních auditů
- vedení organizace by mělo pravidelně přehodnocovat ISMS kvůli zajištění jeho odpovídajícího rozsahu
- aktualizování bezpečnostních plánů s ohledem na nálezy získané z monitorování a přezkoumání
- zaznamenávání všech činností a událostí, které by mohly mít dopad na účinnost nebo výkon ISMS

Udržování a zlepšování ISMS

V rámci udržování a zlepšování je organizace povinna pravidelně provádět: [14]

- zavádění identifikovaných možností vylepšení ISMS
- provádění odpovídajících nápravných a preventivních činností s přihlédnutím nejen z vlastních zkušeností ale i ze zkušeností ostatních organizací v oblasti bezpečnosti
- projednávání činností a návrhů na zdokonalení úrovni detail se všemi zainteresovanými stranami a domluvení dalšího postupu
- zaručení, že navržená zlepšení dosáhnout předpokládaných cílů

2.10.3 Požadavky na dokumentaci

Dokumentace musí obsahovat záznamy o rozhodnutí učiněných vedením organizace. Veškeré činnosti musí být zpětně identifikovatelné v politikách a dohledatelné záznamech o rozhodnutím vedením. Veškeré činnosti musí být zaznamenány, aby se zajistila jejich opakovatelnost. Dokumentace musí obsahovat: [14]

- prohlášení politiky a cílů ISMS
- rozsah ISMS

- postupy a opatření podporující ISMS
- popis použitých metodik hodnocení rizik
- zhodnocení rizik
- plán zvládání rizik
- nezbytné postupy pro zajištění efektivního plánování, provozu a řízení procesů bezpečnosti informací organizace a popis způsobu měření účinnosti realizovaných opatření
- záznamy vyžadované normou ISO 27001
- prohlášení o aplikovatelnosti

Řízení dokumentů

Požadované dokumenty, které jsou v rámci ISMS vytvořeny, musí být chráněny a řízeny. Dokumentovaný postup musí být vytvořen tak, aby ohraničil řídící činnosti potřebné k: [14]

- schválení dokumentů před jejich vydání
- přezkoumání dokumentů, případná aktualizace dokumentů a opakovanému schválení
- zajištění identifikace změn dokumentů a aktuálního stavu revize dokumentů
- zajištění dostupných verzí příslušných dokumentů v místech jejích používání
- zajištění čitelnosti a snadné identifikovatelnosti dokumentů
- zajištění dostupnosti všem, jež je potřebují, zajištění přenášení, ukládání a likvidace v souladu s příslušnými postupy
- zajištění identifikace externích dokumentů
- zajištění řízené distribuce dokumentů
- znemožnění použití zastaralých dokumentů
- aplikování vhodné identifikace pro případné další použití

Řízení záznamů

Záznamy musí být vytvořeny, udržovány, chráněny a řízeny tak, aby poskytovaly důkaz o shodě s požadavky a o efektivním fungování ISMS. Záznamy musí být čitelné, snadno identifikovatelné, lehce dohledatelné. Tyto opatření musí být dokumentované. Musí zohlednit příslušné právní nebo regulátorní požadavky a smluvní závazky. [14]

2.10.4 Odpovědnost vedení

Závazek vedení

Vedení organizace musí deklarovat svoji vůli k procesům ISMS a to následovně: [14]

- ustanovení politiky ISMS
- zajištění stanovení cílů ISMS a plánu pro jejich dosažení
- stanovení rolí, povinností a odpovědností v oblasti bezpečnosti informací
- zajištění dostatečných zdrojů pro procesy ISMS
- stanovení svým rozhodnutím o přijatelné míře rizika
- zajištění interních auditů
- provádění přezkoumání ISMS

Řízení zdrojů

Zajištění zdrojů Potřebné zdroje, které musí organizace zajistit, pro: [14]

- procesy ISMS
- zajištění podpory cílů činnosti organizace
- vybrání a zabývání se příslušnými zákonnými a regulátorními požadavky a smluvních bezpečnostních závazků
- zajištění úrovně bezpečnosti správným zavedením všech opatření
- občasné přezkoumání a případně zajištění příslušné reakce na výsledek
- zlepšení efektivnosti ISMS podle potřeby

Školení, vědomí závažnosti a odborná způsobilost Povinností organizace je zajistit příslušným zaměstnancům kompetenci k výkonu požadovaných úkolů a to pomocí: [14]

- zajištění příslušných školení nebo najmutí kvalifikovaného personálu
- vyhodnotit účinnost školení a realizovaných činností
- udržování záznamů o vzdělání, školení, zkušenostech a kvalifikačních předpokladech

2.10.5 Interní audity ISMS

Pravidelné provádění interních auditů ISMS organizací pro zjištění, jestli cíle opatření, jednotlivá bezpečnostní opatření, procesy a postupy ISMS: [14]

- stále vyhovují požadavkům normy a odpovídají legislativě případně regulátorním požadavkům
- stále vyhovují stanoveným požadavkům na bezpečnost informací
- jsou zavedeny a udržovány efektivně a fungují tak jak se očekává

Každý audit musí být naplánován a to vzhledem ke stavu a významu auditovaných procesů a oblastí a vzhledem k výsledkům předchozích auditů. Audity musí být prováděny lidmi, u kterých jsme schopni zajistit objektivitu a nestrannost. Auditor nesmí prověřovat svou práci.

Pracovníci, kteří jsou odpovědní za oblast, kde se dělá audit, jsou povinni ihned odstranit zjištěné nedostatky. Náprava musí být zpětně zkontrolována a musí se znova vyhodnotit.

2.10.6 Přezkoumání ISMS vedením organizace

Vedení organizace je povinno pravidelně provádět přezkoumání ISMS organizace za účelem zajištění účelnosti, adekvátnosti a efektivnosti, hodnocení možnosti zlepšení a potřebu změn ISMS, včetně bezpečnostní politiky a cílů bezpečnosti. Dokumentace a k nim příslušným záznamů o výsledcích přezkoumání je nutností.

Vstup pro přezkoumání

Vstupy musí mít údaje o: [14]

- výsledcích auditů a přezkoumání ISMS
- údajích od zainteresovaných stran
- technikách vedoucích ke zlepšení výkonnosti a efektivnosti ISMS
- preventivních opatření a opatření k nápravě
- slabinách/hrozbách, kterým doposud nebyla věnována náležitá pozornost
- výsledcích měření účinnosti opatření
- činnostech následujících po předchozích přezkoumáních
- změnách ovlivňující ISMS
- zlepšovacích doporučení

Výstup z přezkoumání

Rozhodnutí a výstupu, které jsou zahrnuty ve výstupech, se vztahují k: [14]

- zvýšení efektivity ISMS
- aktualizování hodnocení a plánu zvládání rizik
- reagování na vnitřní/vnější změny z pohledu bezpečnosti informací
- potřebování zdrojů
- zdokonalování postupů pro měření účinnosti

2.10.7 Zlepšování ISMS

Soustavné zlepšování

Jak už je patrné z modelu PDCA, na který jsou nasazeny procesy ISMS, tak je to nekončící proces a je třeba ho neustále zlepšovat. Zvýšení účinnosti ISMS se děje s využitím politiky bezpečnosti informací, cílů bezpečnosti, výsledků auditu,

analýzy monitorovaných událostí, nápravných a preventivních akcí a přezkoumání prováděných organizací. [14]

Opatření k nápravě

Organizace musí udělat vše proto aby odstranila nedostatky implementace a provozu ISMS, zabránění jejich opětovnému výskytu a vše řádně zdokumentovat. Aplikované postupy opravných aktivit v dokumentaci musí určit požadavky na: [14]

- určení neshod v zavedení a provozu ISMS
- určení příčin neshod
- vyhodnocení opatření takových, aby se už neshody neopakovaly
- vybrání a realizaci potřebných opatření k opravě
- zaznamenání výsledků realizovaných opatřeních
- přezkoumání realizovaných opatření

Preventivní opatření

Pro zamezení opakovaných neshod je organizace povinna vybrat opatření. Pro tyto preventivní opatření vyplývá povinnost být přiměřené závažnosti možných problému. Je nutné provést a vyhodnotit rizika, aby se mohly stanovit priority preventivních opatření. Aplikované postupy preventivních aktivit v dokumentaci musí určit požadavky na: [14]

- určení případných neshod a jejich příčin
- zamezení znovuobjevení neshod vyhodnocením potřeb provedení činností
- vybrání a realizaci potřebných preventivních opatření
- zaznamenání výsledků realizovaných opatření
- přezkoumání realizovaných preventivních opatření

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Popis firmy

Společnost vznikla transformací společnosti Y s.r.o., založené dne X.Y.Z, na akciovou společnost X ke dni X.Y.Z. Zakladatelem firmy je skupina inženýrů se zkušenostmi v oblasti projektování elektrických zařízení a řídicích systémů pro hutní průmysl. Zaměřuje se především na inženýrsko - dodavatelskou činnost v oblasti projektování elektrických zařízení silnoproudu a měření a regulace, na tvorbu systémů kontroly a řízení technologických procesů základní a operativní úrovně řízení a na informační technologie v oblasti výrobních informačních systémů. Hlavními oblastmi působení společnosti jsou zejména hutnictví, vysoké a průmyslové pece, koksárenství, chemický průmysl, ekologie, dopravní a vážní systémy, energetické agregáty, zpracování a distribuce zemních plynů, vodní hospodářství a řada dalších odvětví. Společnost disponuje pracovníky v oblasti projekce elektrických zařízení a v oblasti programování systémů řízení technologických procesů a informačních technologií. Společnost disponuje nejmodernějšími technickými prostředky a systémovým programovým vybavením pro komplexní pokrytí vysokých požadavků kladených na moderní automatizaci výrobních procesů. Společnost disponuje technickým know-how ve speciálních oblastech kvalifikovaných metod číslicové regulace, identifikace řízených soustav, dynamické optimalizace nastavení regulačních okruhů a snižování energetické náročnosti tepelně - teplotních procesů s uplatněním statických a dynamických modelů řízení. Společnost provozuje svou činnost v prostorách budovy ještě se společnosti Z a.s. v Moravské Ostravě.

3.2 Bezpečnost ve firmě

Zavedení ISMS se doposud ve firmě neřešilo.

3.2.1 Situační analýza

Firma se nachází v blízkosti centra Ostravy. Sídlí v budově společnosti Z a.s., kde je v podnájmu. Vstup do budovy je možný pouze přes hlavní dveře, kde se nachází recepce, na které je neustále někdo přítomný. Venkovní obvod budovy je chráněn kamerovým systémem a obraz je přenášen na recepci. Firma se nachází v levém křídle budovy v přízemí. Na oknech firmy jsou zvenku namontovány mříže. Chodby jsou vybaveny alarmem, které reagují na pohyb. Alarmový systém se aktivuje po odchodu posledního zaměstnance. Hned vedle budovy má sídlo městská policie. Není zde žádná fyzická ostraha ani žádný čipový systém pro identifikaci osob. Z hlediska

přírodních katastrof firma nemusí mít strach o zaplavení, jelikož se nenachází v záplavové oblasti a na požár jsou na chodbách budovy připravené hasicí přístroje.

3.2.2 Informační situace v podniku

Každý z pracovníků má svůj stůl, kde se nachází stolní pracovní stanice, na kterém běží operační systém Windows 7 do nějž se přihlašuje pomocí svého ID a hesla. Na každém takovém počítači je nainstalována antivirová ochrana společnosti eset NOD32, kde je pravidelně aktualizována antivirová databáze. Zaměstnanci nejsou nijak kontrolování. Všichni zaměstnanci mají přístup na datový server, kde by měly pracovat s podklady a dokumenty k zakázkám. Překopírování těchto souborů na vlastní počítač či flash disk není nijak kontrolováno. Každá pracovní stanice má své vlastní UPS, které po výpadku elektrického proudu je schopno napájet pracovní stanici ještě 15 minut a tím je umožněno řádné ukončení všech rozpracovaných věcí.

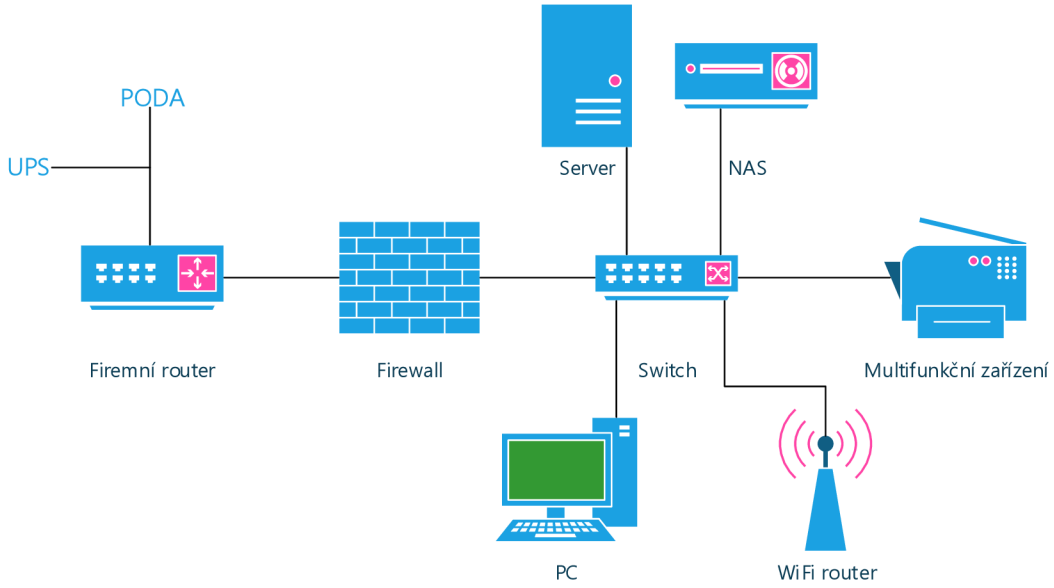
Firma využívá zabudované síťové připojení, které má napojené na svůj router. Topologie sítě je znázorněna na Obrázku 3.1. Všechny stolní pracovní stanice jsou připojeny do sítě přes kabel. Kabely jsou vedené ve zdi a ukončeny zásuvkou na zdi. Programátoři používají jeden wifi router pro multiplikaci LAN portů a pro testování zařízení s WIFI. V případě výpadku energie je v budově napojen zdroj nepřerušovaného napájení (UPS) pro síťové prvky.

Server se skládá ze stanice, která běží pod operačním systémem Windows server 2000 a skládá se z disku o kapacitě 70GB zapojeného v RAID 1. Email a web je řešen externě přes poskytovatele internetového připojení Poda. Dále firma disponuje dvěma síťovými úložišti NAS o velikosti 500GB zapojeného v RAID 1. Jeden se nachází s spolu se serverem v serverové místnosti a druhý na stole v kanceláři. Tyto NAS úložiště slouží pouze pro zálohu serveru. Server je používán pouze pro práci s daty nic jiného se na něm nenachází.

Firma používá i informační systém a to od společnosti Premier system, z kterého využívá pouze modul pro účetnictví, jehož součástí je přehled zakázek, pohledávek nebo správa zákazníků. Informační systém běží

3.3 Analýza rizik a bezpečnostních hrozeb

Co to je analýza rizik a bezpečnostní hrozby již bylo popsáno v teoretické části. Tato kapitola se zabývá už identifikací aktiv firmy a hrozeb, které můžou uškodit aktivům.



Obr. 3.1: Zjednodušená topologie sítě firmy

3.3.1 Identifikace a hodnocení aktiv

Ohodnocení aktiv proběhlo podle Tabulky 3.1.

Následně byly identifikovány důležitá aktiva společnosti a došlo k jejich ohodnocení. Vybrána aktiva určitě nejsou všechny, ale jsou vybrány ty nejdůležitější pro firmu. U každého aktiva se vždy hodnotí dopad na dostupnost, důvěrnost a integritu, kdy sečtením všech tří komponent a následným vydělením jich jejich počtem, dostaneme celkovou hodnotu aktiva. Identifikované aktiva jsou ohodnoceny v Tabulce 3.2 a jejich uvedené hodnoty jsou již souhrnným ukazatelem všech tří komponent.

Z identifikovaných aktiv lze vidět, že pro společnost jsou nejdůležitější data k zakázkám na serveru a jejich zálohy.

3.3.2 Identifikace hrozeb a zranitelnosti

Pro sestavení matice zranitelnosti je třeba nejdřív identifikovat a sepsat hrozby s pravděpodobností jakou mohou nastat. Ohodnocení hrozeb a zranitelnosti proběhlo podle Tabulky 3.3.

Hrozby byly vybrány takové, které by mohly ohrozit aktiva společnosti a tím i chod celé firmy. Jejich výběr vychází z různých doporučení, názorů, zkušeností nebo předpokladů. Standardní hrozby jsou brány taky z přílohy C normy ISO 27005. Identifikované hrozby a jejich ohodnocení jsou vypsány v Tabulce 3.4. Po identifikaci

Hodnota aktiva	Slovní ohodnocení	Význam ohodnocení
1	nevýznamná	žádný dopad na firmu aktiva, která lze lehce nahradit náklady za náhradu jsou malé
2	malá	zanedbatelný dopad na firmu aktiva mající už nějakou hodnotu firma je může chvíli postrádat
3	významná	potíže či finanční ztráta
4	cenná	vážné potíže či podstatné finanční ztráty absence aktiv vede k omezení chodu firmy
5	velmi cenná	existenční potíže firmy klíčová aktiva bez kterých by firma neexistovala

Tab. 3.1: Ohodnocování aktiv

Aktivum	Zdroj	Hodnota
Data	IS - účetníctví	4
	zálohy	5
	data	5
	zdrojové kódy	3
	databáze zákazníků	3
Hardware	server	4
	NAS	4
	PC	2
	síťové prvky	2
Software	operační systém	1
	informační systém	3

Tab. 3.2: Ohodnocená identifikovaná aktiva

hrozeb a jejich pravděpodobností se může sestavit matice zranitelností po spojení tabulky aktiv a hrozeb. Matice zranitelnosti je vidět v Tabulce 3.5, kde v řádcích se nachází hrozby a ve sloupcích aktiva.

Pravděpodobnost hrozby	Slovní ohodnocení	Význam ohodnocení
1	velmi malá	velmi malý dopad
2	malá	malý dopad
3	střední	střední dopad
4	velká	velký dopad
5	velmi velká	velmi velký dopad

Tab. 3.3: Ohodnocování hrozeb

3.3.3 Metoda analýzy rizik

Pro vypočtení míry rizika se používají dvě metody analýzy rizik. První je metoda se dvěma parametry a druhá je maticová metoda se třemi parametry.

Metoda se dvěma parametry

Tato metoda vyhodnocuje pravděpodobnost incidentu a dopadu tohoto incidentu. Nejdříve se identifikují a ohodnotí aktiva společnosti. Následně se vytvoří tabulka hrozeb a zranitelností doplnění o existující opatření. Dalším krokem je odhadnutí pravděpodobnosti incidentu a ohodnocení dopadu, který použije stejných jako jsou ohodnocena aktiva. Potom výpočet míry rizika proběhne vynásobením pravděpodobnosti incidentu a dopadu.

Metoda se třemi parametry

Metoda oproti předchozí metodě využívá tří parametrů a těmi jsou hodnota aktiva, pravděpodobnost hrozby a zranitelnost aktiva. Opět dojde k identifikaci a ohodnocení aktiv, poté dojde k identifikaci a ohodnocení pravděpodobností výskytu hrozeb. Po vytvoření těchto dvou tabulek se sestaví matice zranitelnosti a vyhodnotí se zranitelnost aktiv. Míra rizika se potom spočítá vynásobením hodnoty aktiva, pravděpodobností výskytu hrozby a zranitelnosti aktiva.

	Hrozba	Pravděpodobnost
Fyzické poškození		
1	Požár	2
2	Voda	1
3	Zničení zařízení nebo médií	2
Dostupnost služeb		
4	Výpadek elektřiny	4
5	Výpadek IS	3
6	Výpadek internetu	4
7	Výpadek serveru	3
Důvěrnost služeb		
8	Napadení sítě	3
9	Neoprávněný přístup do IS	3
10	Neoprávněný přístup na server	3
11	Odcizení výpočetní techniky	3
12	odcizení diskových úložišť	4
13	Zisk dat z vyřazených médií	3
Selhání lidského faktoru		
14	Ztráta důvěrných informací	3
15	Fyzické poškození výpočetní techniky	4
16	Nedostatečná dokumentace	3
17	Nedodržování firemních zásad	4
18	Nedbalosti při obsluze zařízení	3
Technická selhání		
19	Selhání diskového úložiště serveru	3
20	Selhání diskového úložiště NASu	3
21	Selhání síťových prvků	2
22	Selhání ostatní výpočetní techniky	2
Neoprávněné činnosti		
23	Neoprávněné vynášení dat	4
24	Neoprávněný přístup do budovy	3

Tab. 3.4: Ohodnocené hrozby

Zranitelnost	**účetnitví**	**data**	**zdrojové kódy**	**zálohy**	**DB zákazníků**	**server**	**NAS**	**PC**	**síťové prvky**	**OS**	**IS**
Fyzické poškození											
Požár	5	5	5	5	5	5	5	5	5	5	5
Voda	3	3	3	3	3	4	4	4	4	3	3
Zničení zařízení nebo médií	2	2	2	2	2	4	4	4	2	2	2
Dostupnost služeb											
Výpadek elektřiny	1	1	1	1	1	1	1	2	1	2	2
Výpadek IS	3	1	1	1	3	1	1	1	1	1	3
Výpadek internetu	1	2	2	2	1	2	2	3	4	1	1
Výpadek serveru	1	4	3	4	1	4	4	2	1	1	1
Důvěrnost služeb											
Napadení sítě	4	3	2	3	4	3	3	2	5	1	3
Neoprávněný přístup do IS	4	1	1	1	4	1	1	1	1	1	4
Neoprávněný přístup na server	1	4	3	4	1	2	2	1	1	1	1
Odcizení výpočetní techniky	2	2	4	1	2	2	2	4	1	1	1
odcizení diskových úložišť	1	3	2	4	1	2	2	2	1	1	1
Zisk dat z vyřazených médií	3	3	2	3	3	1	1	1	1	1	1
Selhání lidského faktoru											
Ztráta důvěrných informací	1	3	3	2	1	1	1	2	1	1	1
Fyzické poškození výpočetní techniky	1	2	3	2	1	3	3	4	3	2	1
Nedostatečná dokumentace	3	3	4	3	4	2	2	2	1	1	1
Nedodržování firemních zásad	1	3	3	2	1	2	2	2	2	1	1
Nedbalosti při obsluze zařízení	1	1	1	1	1	4	3	3	1	1	1
Technická selhání											
Selhání diskového úložiště serveru	1	4	3	2	1	3	1	1	1	1	1
Selhání diskového úložiště NASu	1	2	2	4	1	2	3	1	1	1	1
Selhání síťových prvků	1	2	1	2	1	1	1	1	4	2	1
Selhání ostatní výpočetní techniky	1	1	1	1	1	1	1	3	1	1	1
Neoprávněné činnosti											
Neoprávněné vynášení dat	2	5	5	4	2	2	2	2	1	1	1
Neoprávněný přístup do budovy	1	3	3	3	1	2	2	3	1	2	1

Tab. 3.5: Matice zranitelnosti

Ohodnocení míry rizika

Hranice rizika jsou rozděleny do tří základních skupin: nízké, střední nebo vysoké a jejich ohodnocení se nachází v Tabulce 3.6.

Riziko	Hranice rizika
nízké	0 - 30
střední	31 - 60
vysoké	61 - 125

Tab. 3.6: Ohodnocování rizik

Míra rizika

V této práci byly sestaveny tabulky pro aktiva, hrozby a zranitelnost a tudíž pro výpočet míry rizika je zde využita metoda se třemi parametry. Výsledné hodnoty jsou uvedeny v Tabulce 3.7 a je k nim přiřazena patřičná barva podle hodnoty z Tabulky 3.6.

Riziko	účetnictví	data	zdrojové kódy	zálohy	DB zákazníků	server	NAS	PC	síťové prvky	OS	IS
Fyzické poškození											
Požár	40	50	30	50	30	40	40	20	20	10	30
Voda	12	15	9	15	9	16	16	8	8	3	9
Zničení zařízení/médií	16	20	12	20	12	32	32	16	8	4	12
Dostupnost služeb											
Výpadek elektřiny	16	20	12	20	12	16	16	16	8	8	24
Výpadek IS	36	15	9	15	27	12	12	6	6	3	27
Výpadek internetu	16	40	24	40	12	32	32	24	32	4	12
Výpadek serveru	12	60	27	60	9	48	48	12	6	3	9
Důvěrnost služeb											

Napadení sítě	48	45	18	45	36	36	36	12	30	3	27
Neopráv. přís. do IS	36	15	9	15	36	12	12	6	6	3	36
Neopráv. přís. na server	12	60	27	60	9	24	24	6	6	30	9
Odcizení PC	24	30	36	15	18	24	24	24	6	3	9
odcizení disků	16	60	24	80	12	32	32	16	8	4	12
Zisk dat z vyřaz. méd.	36	45	18	45	27	12	12	6	6	3	9
Selhání lidského faktoru											
Ztráta dův. infor.	12	45	27	30	9	12	12	12	6	3	9
Fyzické poškoz. PC	16	40	36	40	12	48	48	32	24	8	12
Nedostatečná doku.	36	45	36	45	36	24	24	12	6	3	9
Nedodrž. firem. zásad	16	60	36	40	12	32	32	16	16	4	12
Nedbalosti při obsluze	12	15	9	15	9	48	36	18	6	3	9
Technická selhání											
Selhání disků serveru	12	60	27	30	9	36	12	6	6	3	9
Selhání disků NASu	12	30	18	60	9	24	36	6	6	3	9
Selhání síť. prvků	8	20	6	20	6	8	8	4	16	4	6
Selhání PC	8	10	6	10	6	8	8	12	4	2	6
Neoprávněné činnosti											
Neopráv. vynášení dat	32	100	60	80	24	32	32	16	8	4	12
Neopráv. přís. do bud.	12	45	27	60	9	24	24	18	6	6	9

Tab. 3.7: Matice rizik

3.4 Shrnutí analýzy

Přístup do informačního systému mají pouze majitelé. Zaměstnanci nejsou řízeni téměř žádnými bezpečnostními předpisy. Zálohování dat probíhá pravidelně po delších intervalech (jednou za týden), ale zároveň se data i jejich zálohy nacházejí ve stejné budově. Fyzická bezpečnost jako taková je docela kvalitní. Přístup do budovy je hlídán pomocí kamer a recepční. Analýza poukázala na některé nedostatky, kterým by firma měla věnovat pozornost. Řešením těchto nedostatků se zabývá následující kapitola, která se snaží tyto nedostatky eliminovat nebo aspoň srazit na přijatelnou úroveň.

4 VLASTNÍ NÁVRH ŘEŠENÍ

4.1 Zavedení ISMS

Po identifikaci aktiv, bezpečnostních hrozeb a výpočtu míry rizika lze vidět, které bezpečnostní hrozby můžou mít velký dopad na firmu. Účelem této kapitoly je sestavení bezpečnostní příručky, kde budou navrženy příslušná opatření, které by měly případné hrozby a rizika zamezit nebo aspoň eliminovat na přijatelnou úroveň. Výběr opatření vychází z normy normy ISO/IEC 27001:2014 příloha A a z normy ISO/IEC 27002:2014.

4.1.1 Soubor opatření

Firma zatím nemá v nejbližší době v plánu certifikaci, ale jde o zlepšení bezpečnosti ve firmě. Jak již bylo zmíněno v teoretické části práce příloha A normy ISO/IEC 27001 obsahuje 14 hlavních kapitol, 35 hlavních kategorií bezpečnosti a 114 kontrol. V následující Tabulce 4.1 jsou všechna opatření vypsána a k nim stav zda je již opatření zavedeno nebo je potřeba ho zavést nebo aktualizovat (opatření se už v nějaké formě nachází ve firmě, ale je zapotřebí, trochu je upravit nebo něco doplnit). Opatření, které mají ve stavu písmeno *x*, jsou vynechána díky tomu, že se ve firmě nenacházejí.

Označení	**Opatření**	**Stav**
A.5	Politiky bezpečnostních informací	
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.6.1.1	Role a odpovědnosti bezpečnosti informací	aktualizovat
A.6.1.2	Princip oddělení povinností	aktualizovat
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 projektu	zavést
A.6.2.1	Politika mobilních zařízení	zavést
A.6.2.2	Práce na dálku	x
A.7	Bezpečnost lidských zdrojů	
A.7.1.1	Prověřování	zavést
A.7.1.2	Podmínky pracovního vztahu	aktualizovat

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.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	zavést
A.8	Řízení aktiv	
A.8.1.1	Seznam aktiv	zavést
A.8.1.2	Vlastnictví aktiv	zavést
A.8.1.3	Přípustné použití aktiv	aktualizovat
A.8.1.4	Navrácení aktiv	zavedeno
A.8.2.1	Klasifikace informací	zavést
A.8.2.2	Označování informací	zavést
A.8.2.3	Manipulaci s aktivy	aktualizovat
A.8.3.1	Správa výměnných médií	aktualizovat
A.8.3.2	Likvidace médií	zavést
A.8.3.3	Přeprava fyzických médií	x
A.9	Řízení přístupu	
A.9.1.1	Politika řízení přístupu	zavést
A.9.1.2	Přístup k sítím a síťovým službám	zavedeno
A.9.2.1	Registrace a zrušení registrace uživatele	zavedeno
A.9.2.2	Správa uživatelských přístupů	zavedeno
A.9.2.3	Správa privilegovaných přístupových práv	x
A.9.2.4	Správa tajných autentizačních informací uživatelů	zavedeno
A.9.2.5	Přezkoumání přístupových práv uživatelů	zavést
A.9.2.6	Odebrání nebo úprava přístupových práv	zavedeno
A.9.3.1	Používání tajných autentizačních informací	zavedeno
A.9.4.1	Omezení přístupu k informacím	zavedeno
A.9.4.2	Bezpečné postupy přihlášení	zavedeno
A.9.4.3	Systém správy hesel	aktualizovat
A.9.4.4	Použití privilegovaných programových nástrojů	x
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	x
A.10	Kryptografie	

A.10.1.1	Politika pro použití kryptografických opatření	x
A.10.1.2	Správa klíčů	x
A.11	Fyzický bezpečnostní perimetr	
A.11.1.1	Fyzický bezpečnostní perimetr	zavedeno
A.11.1.2	Fyzické kontroly vstupu	aktualizovat
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	zavedeno
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	aktualizovat
A.11.1.5	Práce v bezpečných oblastech	x
A.11.1.6	Oblasti pro nakládku a vykládku	x
A.11.2.1	Umístění zařízení a jeho ochrana	zavést
A.11.2.2	Podpůrné služby	zavedeno
A.11.2.3	Bezpečnost kabelových rozvodů	zavedeno
A.11.2.4	Údržba zařízení	aktualizovat
A.11.2.5	Přemístění aktiv	x
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	aktualizovat
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	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.12.1.1	Dokumentované provozní postupy	zavést
A.12.1.2	Řízení změn	zavést
A.12.1.3	Řízení kapacit	aktualizovat
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	zavedeno
A.12.2.1	Opatření proti malwaru	zavedeno
A.12.3.1	Zálohování informací	zavést
A.12.4.1	Zaznamenávání událostí formou logů	x
A.12.4.2	Ochrana logů	x
A.12.4.3	Logy o činnosti administrátorů a operátorů	x
A.12.4.4	Synchronizace hodin	x
A.12.5.1	Instalace softwaru na provozní systémy	x
A.12.6.1	Řízení technických zranitelností	x

A.12.6.2	Omezení instalace softwaru	zavést
A.12.7.1	Opatření k auditu informačních systémů	x
A.13	Bezpečnost komunikací	
A.13.1.1	Opatření v sítích	aktualizovat
A.13.1.2	Bezpečnost síťových služeb	zavést
A.13.1.3	Princip oddělení v sítích	x
A.13.2.1	Politiky a postupy při přenosu informací	zavést
A.13.2.2	Dohody o přenosu informací	zavést
A.13.2.3	Elektronické předávání zpráv	zavedeno
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	zavést
A.14	Akvizice, vývoj a údržba systémů	
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	aktualizovat
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	x
A.14.1.3	Ochrana transakci aplikačních služeb	x
A.14.2.1	Politika bezpečného vývoje	aktualizovat
A.14.2.2	Postupy řízení změn systémů	zavést
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	x
A.14.2.4	Omezení změn softwarových balíků	zavést
A.14.2.5	Principy budování bezpečných systémů	aktualizovat
A.14.2.6	Prostředí bezpečného vývoje	zavést
A.14.2.7	Outsourcovaný vývoj	x
A.14.2.8	Testování bezpečnosti systémů	zavedeno
A.14.2.9	Testování akceptace systémů	x
A.14.3.1	Ochrana dat pro testování	x
A.15	Dodavatelské vztahy	
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	x
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	x
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	zavést
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.16.1.1	Odpovědnosti a postupy	zavést
A.16.1.2	Hlášení událostí bezpečnosti informací	zavést
A.16.1.3	Hlášení slabých míst bezpečnosti informací	zavést
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	zavést
A.16.1.5	Reakce na incidenty bezpečnosti informací	zavést
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	zavést
A.16.1.7	Shromáždění důkazů	zavést
A.17	Aspekty řízení kontinuity činnosti organizace z hlediska 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.17.2.1	Dostupnost vybavení pro zpracování informací	aktualizovat
A.18	Soulad s požadavky	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	aktualizovat
A.18.1.2	Ochrana duševního vlastnictví	aktualizovat
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.18.2.1	Nezávislá přezkoumání bezpečnosti informací	zavést
A.18.2.2	Shoda s bezpečnostními politikami a normami	zavést
A.18.2.3	Přezkoumání technické shody	zavést

Tab. 4.1: Soubor opatření

4.1.2 Plán zavedení opatření

Jelikož firma momentálně neusiluje o certifikaci ISMS a je menšího charakteru, tak se plán na zavádění opatření může rozdělit na etapy do delších časových úseků. Jednak se tím rozloží finanční výdaje, ale dojde i k rozložení časové náročnosti na zaměstnance a majitele, kterých by se zavádění opatření dotýkalo. V první etapě budou by měla být zavedena nejdřív opatření taková, která eliminují momentální největší hrozby a rizika a sníží je úplně na minimum nebo aspoň na akceptovatelnou úroveň. Ve druhé etapě potom budou následovat zbylá opatření.

- **1.etapa** - opatření: A.5 Politiky bezpečnosti informací, A.6 Organizace bezpečnosti informací, A.7 Bezpečnost lidských zdrojů, A.8 Řízení aktiv, A.9 Řízení přístupu, A.11 Fyzická bezpečnost a bezpečnost prostředí, A.12 Bezpečnost provozu
- **2.etapa** - opatření: A.13 Bezpečnost komunikací, A.14 Akvizice, vývoj a údržba systémů, A.15 Dodavatelské vztahy, A.16 Řízení incidentů bezpečnosti informací, A.17 Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací, A.18 Soulad s požadavky

4.2 Popis první etapy zavedení opatření

V této kapitole bude popsána první etapa zavádění opatření. Nachází se zde taková opatření, které eliminují hrozby a rizika nebo je srazí na přijatelnou úroveň. Opatření vychází z normy ISO/IEC 27002:2014.

4.2.1 A.5 Politiky bezpečnostní informací

Cílem je poskytnutí pokynů a podpory ze strany managementu pro bezpečnost informací v souladu s požadavky podnikatelské činnost firmy a příslušnými zákony a předpisy.

A.5.1.1 Politiky pro bezpečnost informací

Odpovědná osoba: majitelé firmy
Opatření: Vytvořit sady politik pro bezpečnost informací, které budou schváleny majiteli firmy, zveřejněny a dány na vědomí zaměstnancům a relevantním externím stranám. Nejvýše položená politika by měla být *politika bezpečnosti informací*, která stanovuje přístup organizace k řízení svých cílů bezpečnosti informací. Vedení organizace:

- vyjádří cíle a význam bezpečnosti informací

- dojde k definici a stručnému vysvětlení bezpečnostních zásady, principy a pravidla
- určí odpovědnosti a pravomoci pro řízení bezpečnosti informací
- projeví zájem o prohlubování bezpečnosti informací

Doba trvání vytvoření politik: 48h

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Odpovědná osoba: manažer bezpečnosti
Opatření: Vytvořené politiky pro bezpečnost se budou v pravidelných intervalech přezkoumávat nebo když dojde výrazným změnám ve firmě a to kvůli zajištění vhodnosti, přiměřenosti a efektivnosti. Politiky kontrolovat aspoň jednou ročně nebo když dojde k výrazným změnám. Revizi politik budou dělat pověření vlastníci těchto politik a mají za ně odpovědnost. Zrevidované politiky musí opět schválit majitelé.

Doba trvání vytvoření plánu přezkoumání: 8h
Doba pro přezkoumání: 12h/přezkoumání

4.2.2 A.6 Organizace bezpečnosti informací

Z interní stránky je třeba ustanovení řídícího rámce pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace. Z externího hlediska je zapotřebí zajištění bezpečnosti práce na dálku a bezpečnosti mobilních zařízení.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Odpovědná osoba: majitelé firmy
Opatření: V souladu s vytvořenými politikami v opatření A.5.1.1 budou přiděleny odpovědnosti za bezpečnost informací. Firma identifikuje odpovědnosti za ochranu aktiv a za provádění specifických postupů v oblasti bezpečnosti informací. Dále se definují odpovědnosti za činnost v oblasti řízení rizik bezpečnosti informací. Osoby, kterým byla přidělena odpovědnost za bezpečnost informací, mohou delegovat úkoly na ostatní, ale stále zůstávají zodpovědní za správnost provedeného úkolu. Bude zde navržen manažera bezpečnosti informací, který bude mít na starost celkovou odpovědnost za rozvoj a implementaci bezpečnosti informací a podporovat identifikaci opatření. Určení vlastníci aktiv budou zodpovědní za každodenní ochranu aktiva.

Doba trvání vytvoření dokumentu: 24h

A.6.1.2 Princip oddělení povinností

Odpovědná osoba: majitelé firmy
Opatření: Oddělit konfliktní povinnosti a oblasti působnosti kvůli zamezení neoprávněným nebo neúmyslným změnám nebo zneužití aktiv firmy. Je nutné zavést aby žádná osoba nemohla k aktivům přistupovat, upravovat je nebo používat je bez oprávnění. V případě, když by nešlo oddělit povinnosti, tak je zapotřebí aspoň monitorovat činnost.

Doba trvání rozdělení povinností: 16h

A.6.1.5 Bezpečnost informací v řízení projektu

Odpovědná osoba: majitelé firmy
Opatření: V rámci řízení všech projektů se bude řešit bezpečnost informací. Zavést bezpečnost informací do metod řízení projektů pro zajištění identifikace rizik a jejich řešení.

Doba trvání: 8h

A.6.2.1 Politika mobilních zařízení

Odpovědná osoba: majitelé firmy, bezpečnostní manažer
Opatření: Zavést politiku používání mobilních zařízení a podpůrná bezpečnostní opatření, aby nedošlo k kompromitování informací týkající se činnosti organizace. Dávat pozor při používání mobilních zařízení na veřejných místech, v zasedacích místnostech a dalších nechráněných oblastech. Dodržovat bezpečnostní postupy při připojování k bezdrátovým sítím. Zařízení s citlivými informacemi nenechávat bez dozoru. Mobilní zařízení fyzicky chránit. Neponechávat zařízení, které obsahují citlivé informace, bez dozoru a případně uzamknout.

Doba trvání vytvoření politiky: 8h

4.2.3 A.7 Bezpečnost lidských zdrojů

Před vznikem pracovního poměru je důležité, aby zaměstnanci chápali své povinnosti a bylo zajištěno, aby byli vhodní pro úlohy, na které jsou nabírání. Během pracovního poměru potom se ujistit, že každý zaměstnanec si je vědom svých povinností a jejich plnění. Po ukončení nebo změně pracovního poměru ochránit zájmy firmy jako součást procesu změny nebo ukončení pracovního poměru.

A.7.1.1 Prověřování

Odpovědná osoba: majitelé firmy
Opatření: U každého uchazeče o práci prověřit minulost v souladu s příslušnými zákony, nařízeními a etikou. Prověřování bude zahrnovat následující:

- dostupnost uspokojivých osobních posudků
- ověření životopisu žadatele
- potvrzení proklamovaného vzdělání a odborných kvalifikací
- nezávislé ověření totožnosti
- podrobnější ověření, jako jsou posouzení finanční situace nebo výpis z rejstříku trestů

Doba trvání zavedení: 16h

A.7.1.2 Podmínky pracovního vztahu

Odpovědná osoba: majitelé firmy
Opatření: Smlouvy se zaměstnanci nebo smluvními stranami budou odrážet bezpečnostní politiky firmy a navíc všichni zaměstnanci, kteří mají přístup k důvěrným informacím, musí podepsat dohodu o zachování důvěrnosti nebo mlčenlivosti předtím než je jim udělen přístup k vybavení pro zpracování informací. Dále stanovení odpovědnosti za klasifikaci informací a správu aktiv organizace spojených s informacemi, vybavením pro zpracování informací a informačními službami vykonávané zaměstnancem nebo smluvní stranou. Povinnost zaměstnance ve vztahu k zacházení s informacemi získanými od jiných společností nebo externích subjektů. V případě ignorování bezpečnosti zaměstnanci budou mít disciplinární řízení a v případě externích subjektů budou to budou sankce.

Doba trvání vytvoření: 16h

A.7.2.1 Odpovědnosti managementu organizace

Odpovědná osoba: majitelé firmy
Opatření: Majitelé firmy budou požadovat dodržování stanovené bezpečnostní politiky firmy a musí zajistit, aby zaměstnanci:

- byli informování o svých rolí a odpovědnostech v oblasti bezpečnosti informací před tím, než je jim poskytnut přístup k důvěrným informacím
- obdrželi směrnice, které stanovují co se od nich bude požadovat v oblasti bezpečnosti informací a spojená se jejich rolí v rámci organizace
- byli motivováni k plnění politiky bezpečnosti

Majitelé firmy musí jít příkladem a to tak, že dají najevo podporu politik, postupů a opatření bezpečnosti informací.

Doba trvání vytvoření směrnic: 16h

A.7.2.2 Povědomí vzdělávání a školení bezpečnosti informací

Odpovědná osoba: majitelé firmy
Opatření: Zajistit, aby všichni zaměstnanci firmy získali povědomí o bezpečnosti informací v pravidelně se konajících vzdělávání, školení a byli pravidelně seznamování s aktualizacemi politik a postupů ve firmě. Zajistit aby se programu mohli zúčastnit všichni zaměstnanci a to včetně i externích zaměstnanců (recepční, uklízečka). V programu zvyšování povědomí bezpečnosti informací musí být zohledněny role zaměstnanců (programátoři, projektanti, majitelé, externí subjekty) a upravit tak pro každou skupinu lidí jednotlivá školení či vzdělávání. První školení provádět pro nové zaměstnance, ale i pro ty co přestupují na jinou pracovní pozici.

Doba trvání vytvoření programu: 16h
Doba pro přezkoumání: 1h/měsíc

A.7.2.3 Disciplinární řízení

Odpovědná osoba: majitelé firmy
Opatření: Zavedení procesu, který všem bude znám/oznámen, pro podniknutí patřičných kroků v případě narušení bezpečnosti informací ze strany zaměstnanců. Před procesem jak moc byla narušena bezpečnost, zda-li se jedná o první přestupek nebo už opakovaný, zda-li byl zaměstnanec řádně proškolen. Lehčí nebo první přestupky řešit slovním napomenutím nebo výtkou a závažnější nebo opakované přestupky řešit finančními sankcemi nebo ukončení pracovního poměru. V případě, že dojde i k velkému poškození firmy, tak řešit právní cestou.

Doba trvání vytvoření postupů: 24h

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního poměru

Odpovědná osoba: majitelé firmy
Opatření: Sdělit zaměstnanci jeho odpovědnosti při ukončení nebo změně pracovního poměru. Jedná se o povinnosti a odpovědnosti zůstávající v platnosti i po ukončení pracovního poměru, které jsou obsaženy v pracovní smlouvě zaměstnance (viz. A.7.1.2.).

Doba trvání zavedení: 8h

4.2.4 A.8 Řízení aktiv

Nejdřív je zapotřebí aktiva firmy identifikovat a definovat odpovědnosti za přiměřenou ochranu. Dalším důležitým bodem je zde klasifikace informací a k nim přiřazení patřičné ochrany podle důležitosti. Nakonec snažit se zabránit neoprávněnému prozrazení, modifikací, odstranění nebo zničení informací uložených na médiu.

A.8.1.1 Seznam aktiv

Odpovědná osoba: manažer bezpečnosti
Opatření: Aktiva už byly v této práci identifikovány v etapě ustanovení ISMS. Tyto aktiva jsou vypsána jako seznam a udržována. Seznam aktiv by měl být přesný, aktuální, konzistentní a uspořádaný s dalšími inventáři. Každému aktivu je zapotřebí přiřadit vlastníka (viz. A.8.1.2) a identifikovat jeho klasifikaci (viz. A.8.2). Aktiva je nutné pravidelně aktualizovat aspoň jednou za půl roku a i v případě při změně aktiv.

Doba pro přezkoumání: 2h/aktualizaci

A.8.1.2 Vlastnictví aktiv

Odpovědná osoba: manažer bezpečnosti
Opatření: K aktivům uvedených v seznamu musí být přiřazen vlastník. Vlastník aktiv má povinnost:

- zajistit,že aktiva jsou inventarizovaná
- zajisti, že aktiva jsou náležitě klasifikována a chráněna
- stanovit a pravidelně přezkoumávat omezení přístupu k důležitým aktivům a jejich klasifikaci, s přihlédnutím k platným politikám řízení přístupu
- zajistit správné zacházení, když je aktivum vymazáno nebo zničeno

V Tabulce 4.2 jsou k aktivům přiřazení vlastníci a ve většině případů jsou vlastníci majitelé firmy, kteří by si měli stanovit jednoho, kdo se bude o všechna aktiva starat.

Doba pro ověření vlastníků: 4h

A.8.1.3 Přípustné použití aktiv

Odpovědná osoba: manažer bezpečnosti, majitelé
Opatření: Manažer bezpečnosti musí sestavit přípustná pravidla ohledně toho, jakým způsobem se můžou využívat informace v informačních aktivech firmy a ja-

Aktiva	Vlastník
Data informační systém	majitelé
Zálohy	majitelé
Zdrojové kódy	programátoři
databáze zákazníků	majitelé
server	majitelé
NAS	majitelé
PC	majitelé
síťové prvky	majitelé
operační systém	majitelé
informační systém	majitelé

Tab. 4.2: Aktiva a jejich vlastníci

kým způsobem může být využita výpočetní technika ve firmě. Tyto pravidla musí být identifikována, dokumentována, implementována a musí s nimi být seznámeni zaměstnanci a externí strana, která má přístup k nějakým aktivům firmy. Např.: zakázat kopírování citlivých informací firmy na přenosné média.

Doba vytvoření postupů: 16h

A.8.2.1 Klasifikace informací

Odpovědná osoba: manažer bezpečnosti
Opatření: Informace, které se nacházejí ve firmě musí být oklasifikovány z pohledu právních požadavků, hodnoty, kritičnosti a citlivosti ve vztahu k neoprávněnému prozrazení nebo modifikace. Mezi nejcitlivější informace ve firmě patří data uložené na serveru, kde se nachází řešené a rozpracované zakázky, tím pádem know-how firmy a ty budou spadat do *důvěrných informací*. Dalšími informacemi jsou zde databáze klientů. Ty se musí chránit ze zákona a budou spadat tedy do kategorie *soukromých informací*. Jako nejméně citlivé jsou data z účetnictví a ty budou spadat do kategorie *citlivých informací*. Všechny ostatní budou spadat do kategorie *veřejných*.

Doba trvání klasifikace: 16h

A.8.2.2 Označování informací

Odpovědná osoba: manažer bezpečnosti
Opatření: Pro oklasifikované informace se musí vytvořit postupy jak tyto informace označovat a to už jak ve fyzické, tak elektronické podobě. V případě tisku opatřit dokument vodoznakem s klasifikací a elektronické dokumenty taktéž takto označit. Seznámit zaměstnance s postupem označovaní. Dokumenty, které jsou utajované ani neobsahují citlivé informace, není potřeba označovat.

Doba pro vytvoření postupů: 16h

A.8.2.3 Manipulace s aktivy

Odpovědná osoba: manažer bezpečnosti
Opatření: Zavést postupy pro zacházení, zpracování, ukládání a předávání informací v souladu s jejich klasifikací. Zavést přístup pro každou úroveň klasifikace jen oprávněným osobám a vést o tom záznam. Chránit kopie informací jako originál a kopie označovat.

Doba pro vytvoření postupů: 16h

A.8.3.1 Správa výměnných médií

Odpovědná osoba: majitelé
Opatření: Stanovení postupů a pokynů pří správě s médii:

- v případě médií, které mají být odstraněna tak je třeba fyzicky zlikvidovat nebo učinit obsah neobnovitelný
- dělat záznamy po odstranění médií
- ukládat média v podmínkách doporučené výrobcem
- pokud data přesahují životnost média, přenést je na nové médium
- vícenásobné kopie ukládat na oddělené média
- v případě vyměnitelných médii monitorovat přenos informací do těchto médií

Doba pro vytvoření postupů: 16h

A.8.3.2 Likvidace médií

Odpovědná osoba: majitelé, manažer bezpečnosti
Opatření: Bezpečně zlikvidovat již nepotřebná média a to buď skartací nebo spálením, aby došlo k zamezení úniku citlivých informací. O likvidacích vést záznamy.

Návrh likvidace je uveden následující kapitole, kde se nachází ekonomické zhodnocení.

Doba pro vytvoření postupů: 16h

4.2.5 A.9 Řízení přístupu

Cílem je omezit přístup k informacím a k vybavení pro zpracování informací, zajistit oprávněný přístup uživatelů a zabránit neoprávněnému přístupu k systémům a službám. Dále je dobré učinit uživatele odpovědné za ochranu svých autentizačních informací. A v neposlední řadě zabránit neoprávněnému přístupu k systémům a aplikacím.

A.9.1.1 Politika řízení přístupu

Odpovědná osoba: majitelé
Opatření: Vlastníci aktiv stanoví vhodná pravidla řízení přístupu, přístupová práva a omezení pro jednotlivé role (programátoři, projektanti atd.) ve vztahu k jejich aktivům. Přístup k aktivům bude poskytován pouze tehdy pokud to bude opravdu zapotřebí.

Doba pro vytvoření pravidel: 16h

A.9.2.5 Přezkoumání přístupových práv uživatelů

Odpovědná osoba: majitelé, manažer bezpečnosti
Opatření: Vlastníci budou v pravidelných intervalech přezkoumávat přístupová práva uživatelů. Přezkoumávání bude probíhat vždy, když u zaměstnance dojde ke změně pozice ve firmě nebo ukončení pracovního poměru.

Doba pro přezkoumání: 1h/měsíc nebo při změně

A.9.4.3 Systém správy hesel

Odpovědná osoba: majitelé, manažer bezpečnosti
Opatření: Zaměstnanci se přihlašují do systému skrz uživatelské ID a heslo, ale už nejsou nuceni ho pravidelně měnit nebo aby vybírali kvalitní hesla. Zavést pravidelné změny hesel (jednou za 4 měsíce a heslo se nesmí opakovat po dobu 2 cyklů) a minimální požadavky na heslo.

Doba vytvoření pravidla: 16h

4.2.6 A.11 Fyzická bezpečnost a bezpečnost prostředí

Cílem fyzické bezpečnosti je zajistit aby nedocházelo k neoprávněnému fyzickému přístupu, poškození a narušování informací a vybavení pro zpracování informací organizace. Zároveň opatření vedou k ochraně aktiv a snaží se zabránit jejich ztrátě, poškození, odcizení nebo kompromitaci a snaží se zabránit aby nedošlo k přerušení provozu firmy.

A.11.1.2 Fyzické kontroly vstupu

Odpovědná osoba: manažer bezpečnosti
Opatření: Vstupy do oblastí firmy musí být chráněny vhodnými opatřeními, kvůli zajištění přístupu jen oprávněných osob. Firma má fyzickou kontrolu díky recepci, na které se někdo nepřetržitě nachází, zajištěnou. Problém by mohl nastat, kdyby recepční si musel/a na chvíli někam odskočit (např.: na záchod) a tím pádem by nebyl problém do firmy proklouznout. Jelikož firma má pro sebe celé levé křídlo přízemního podlaží, kde vede vstup pouze přes jedny dveře, tak navrhuji tyto dveře zajistit pomocí čipového systému pro fyzickou kontrolu vstupu. Čipový systém je popsán a ohodnocen v Kapitole 4.2.8.

Doba pro zavedení systému: 40h

A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí

Odpovědná osoba: manažer bezpečnosti
Opatření: Jedná se o zabezpečení před přírodními hrozbami. Jelikož budova firmy se nenachází v záplavové oblasti, tak výskyt vody je velmi malý až zanedbatelný. Na hrozbu v podobě požáru je firma připravena v podobě hasících přístrojů umístěných v prostorách firmy. Jako zlepšení pro detekci požáru navrhuji nainstalovat kouřové čidla, které by upozornili v případě, kdy se v prostorách firmy nikdo nenachází. Výběr a popis detektorů se nachází v Kapitole 4.2.8.

Doba potřebná pro zavedení: 40h

A.11.2.1 Umístění zařízení a jeho ochrana

Odpovědná osoba: manažer bezpečnosti
Opatření: Zařízení je třeba chránit, aby se snížily rizika, které plynou z hrozeb, životního prostředí a z možnosti neoprávněnému přístupu a podle toho u umístěna. Všechna zařízení (PC, NAS, síťové prvky) jsou umístěna na stolech, takže jediná

hrozba pro ně je shození ze stolu to bych řešil pomocí pevného připevnění ke stolu a tím by bylo i z velké části vyřešeno odcizení. Pravděpodobnost poškození zatopením je velmi malá, protože sídlo firmy je sice v přízemí ale to je ještě zvednuté nad venkovním okolím a navíc sídlo neleží v záplavové oblasti. Popis a cena ochrany je v Kapitole 4.2.8.

Doba potřebná pro zavedení: 40h

A.11.2.4 Údržba zařízení

Odpovědná osoba: manažer bezpečnosti
Opatření: Je zapotřebí sestavit plán pro pravidelnou revizi serveru, NASu a dalších zařízení, aby byla zajištěna stálá dostupnost a integrita. Doporučuji zařízení jednou za měsíc očistit od prachu a vést záznam o každé údržbě. Údržbu a servis bude provádět autorizovaný pracovník. Pokud se při revizi zjistí problémy, bude zapotřebí je ihned řešit s příslušnými lidmi. Pravidelná revize je u každého zařízení jiná a je stanovená výrobcem, a proto revize dělat podle potřeb zařízení.

Doba pro sestavení plánu: 16h
Revize: 1h/4měsíce

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Odpovědná osoba: manažer bezpečnosti, majitelé
Opatření: Používání aktiv (zařízení, informace nebo software) mimo firmu nelze provést do té doby, dokud nedojde k povolení od vedení. Každý zaměstnanec firmy musí někdy pracovat s aktivem mimo umístění firmy, ale musí o tom patřičně uvědomit některého z majitelů a případně i vlastníka aktiva. Doporučuji vést záznamy o těchto aktivitách mimo prostory firmy. Zaměstnanec nesmí nechat zařízení nebo aktivum firmy bez dozoru.

Doba pro sestavení postupů: 16h

A.11.2.7 Bezpečnost likvidace nebo opakované použití zařízení

Odpovědná osoba: majitelé
Opatření: Je zapotřebí stanovit postupy jak nakládat s médii, které již nejsou zapotřebí a zároveň stanovit zodpovědnou osobu. Na odstranění médií se doporučuje používat buď nějaký speciální software nebo přímo fyzická likvidace. Média musí být zlikvidovány tak, aby nebylo možné z nich získat jakékoliv informace. Návrh jak

likvidaci provádět se nachází v Kapitole 4.2.8.

Doba pro sestavení postupů: 16h

A.11.2.8 Uživatelská zařízení bez obsluhy

Odpovědná osoba: majitelé
Opatření: Uživatel musí zabezpečit neobsluhované zařízení. V případě, kdy zaměstnanec opouští své pracoviště, tak navrhuji, aby byl povinen svůj počítač zabezpečit tak, aby se do něj nikdo nedostal a to buď vypnutím zařízení nebo zabezpečení heslem.

Doba pro sestavení postupů: 8h

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Odpovědná osoba: majitelé
Opatření: Je důležité poučit zaměstnanec se zásadou prázdného stolu, kam spadají papírové dokumenty nebo vyměnitelné paměťové média. Zaměstnanec nebude nechávat volně se válet po pracovním stole zmíněné věci a uzamykat je na příslušné místo.

Doba pro sestavení postupů: 8h

4.2.7 A.12 Bezpečnost provozu

Bezpečnost provozu se stará o správné a bezpečné provozování vybavení pro zpracování informací. S tím souvisí, že je zapotřebí informace i vybavení pro zpracování informací chránit před malwarem, chránit data před ztrátou pomocí zálohování, zaznamenávat události a generovat důkazy, zajistit integritu provozních systémů, zabránit využívání technických zranitelností a minimalizovat dopad auditních aktivit na provozní systémy.

A.12.1.1 Dokumentované provozní postupy

Odpovědná osoba: majitelé, manažer bezpečnosti
Opatření: Firma si musí stanovit, dokumentovat a dát k dispozici provozní postupy, který bude dostupný zaměstnancům. Dokument bude zahrnovat postupy pro:

- vypnutí a zapnutí počítače
- zálohování
- údržbu zařízení
- zacházení s médii

- správu počítačové místnosti
- bezpečnost práce

Doba pro sestavení postupů: 24h

A.12.1.2 Řízení změn

Odpovědná osoba: majitelé
Opatření: Je důležité řídit a kontrolovat změny ve firmě, které se dotýkají podnikových procesů, vybavení pro zpracování informací a systémech, které mají vliv na bezpečnost informací. Majitelé musí určit zda jde o významnou změnu a případně ji zaznamenat. V případě významné změny je zapotřebí stanovit možné dopady, posouzení jich z hlediska bezpečnosti informací a po vykonání změny ověřit zda požadavky na bezpečnost informací byly splněny. Řízení změn je odpovědnost majitelů a tyto postupy by měly formalizovat, aby bylo zajištěno uspokojivé řízení změn.

Doba pro formalizaci: 48h

A.12.1.3 Řízení kapacit

Odpovědná osoba: majitelé
Opatření: Pravidelně hlídána kapacitu disků, aby byl zajištěn požadovaný výkon systému z hlediska budoucích na kapacitu. Je zapotřebí stanovit zodpovědnou osobu (jeden z majitelů), která bude pravidelně monitorovat stav disků na serveru a zálohovacích disků NASu a případě potřeby buď navýšit diskovou kapacitu nebo smazat stará nepotřebná data.

Potřebná doba: 8h

A.12.3.1 Zálohování informací

Odpovědná osoba: majitelé, manažer bezpečnosti
Opatření: Pravidelně pořizovat a testovat záložní kopie informací. Zaměstnanci ve firmě pracují s daty na serveru, který se v delších pravidelných intervalech zálohuje do dvou NAS úložišť, které se nacházejí v jedné budově. Je zapotřebí data zálohovat i na vzdálenější místo než je budova firmy. Navrhuji, aby zálohování probíhalo ještě i do cloudového úložiště. Zálohovací dobu stanovit na jednou denně na všechny média (NAS i Cloud). Popis a zhodnocení navrhovaného vybavení je v Kapitole 4.2.8.

Potřebná doba: 48h

A.12.6.2 Omezení instalace softwaru

Odpovědná osoba: majitelé, manažer bezpečnosti
Opatření: Firma si musí stanovit a prosadit politiku, která bude určovat, který software je přijatelný a zaměstnanec si ho může nainstalovat a který software je zakázaný. Všichni zaměstnanci využívají operační systém Windows, kde se omezí práva uživatelů a tím se tak zamezí instalaci softwaru pro osobní využití nebo ještě hůře instalaci nějakého škodlivého softwaru. Jediný, kdo bude mít právo instalovat software na výpočetní stanice, bude administrátor. Standardně ostatní uživatelé právo pro instalaci mít nebudou.

Potřebná doba: 16h

4.2.8 Náklady na první etapu

Většina opatřeních navržená v první etapě jsou spíše administračního typu, které může firma řešit postupně za provozu. V opatřeních nalezneme i takové, které něco stojí a patří mezi ně: pořízení čipového systému a čipových karet, zámky na stůl pro zařízení, požární signalizace, zařízení sloužící k likvidaci médií a nakonec zálohování do cloudového úložiště.

Čipový systém
Firma Faberasystems byla zvolena jako dodavatel čipového systému a čipů. Firma potřebuje zabezpečit jedny vchodové dveře do prostor firmy a má 18 zaměstnanců včetně majitelů. Jako přístupový systém je zvolen KABA EVOLO LEGIC C-LEVER E300 ÚZKÝ (autonomní přístupová kontrola, Obrázek 4.1), který nezávisí na zámku ani cylindrické složce. Jeho cena je 15 642Kč. Není u něj zapotřebí žádná kabeláž a přístup jak povolený tak nepovolený je indikován opticky i akusticky. Jelikož se dveře nachází hned u recepce, tak akustické ozvučení přijde velmi vhod. Dále zakoupení 25 přívěšků LEGIC (bezkontaktní přístupové médium), kde cena je 291Kč za kus. Ceny jsou brány z eshopu.

Fyzické zabezpečení výpočetní techniky
Jelikož ve firmě se pracuje převážně na stolních počítačích je voleno od společnosti Kensington balíček (Obrázek 4.2), který obsahuje zamykací prostředky pro stolní počítač a zároveň i pro periférie. Cena jednoho takového balíčku činí cca 768Kč.

Požární signalizace
Firma je složena z 5 hlavních kanceláří a do každé takové je zapotřebí zakoupit detektory kouře. Pro tyto účely na základě testů časopisu dTest [17] je vybrán detektor

Obr. 4.1: KABA EVOLO LEGIC C-LEVER E300

Obr. 4.2: Kensington zabezpečení

Jablotron JA–63S bezdrátový (Obrázek 4.3). Cena za kus 1 061Kč.

Obr. 4.3: Detektor Jablotron JA–63S

Likvidace médií

Jelikož ve firmě málo dochází k odstraňování médií, tak by bylo zbytečné zakupovat vlastní stroj a proto se likvidace bude využívat jako služba externí společností Data Labs, která je schopna zajistit dodržení postupů a norem dle NBÚ, ISO 9001, ISO 14001 a ISO 27001. Cena potom závisí na osobní domluvě.

Záloha do cloudového úložiště

Zde se využijí služby společnosti Autocont a jejich služba vBR (virtual Backup & Recovery), která umožňuje zálohovat data z infrastruktury firmy do prostředí AC CLOUD a v případě potřeby je opět obnovit zpět. Data jsou přenášena pomocí bezpečného šifrovaného připojení a jsou ukládána v šifrované podobě. Přístup k těmto datům má pouze vlastník dat. Pro potřeby společnost je vybrán vBR Standard, kde je měsíční poplatek za každý zálohovaný stroj 145Kč a měsíční poplatek za rozsah zálohovacího prostoru je 1,2Kč za 1GB dat, kde se účtuje podle toho kolik se reálně využívá. Pro provoz služby je potřeba zakoupit licenci zálohovacího produktu Veeam Backup & Replication v8 Standard v hodnotě 620eur cca 16 740Kč. Firma momentálně oplývá cca 500GB dat.

Zhodnocení

V Tabulce 4.3 jsou zobrazeny celkové náklady na opatření v první etapě. Celková suma první etapy je odhadnuta na necelých 60 000Kč, což je dle mého názoru na přijatelné úrovni. Modelovým příkladem, že tento finanční obnos za opatření se vyplatí, může být například jakékoliv poškození budovy (požár) nebo úmyslné zničení či odcizení úložných prostor serveru a zálohovacích prostor NASu. Firma skladuje veškeré svá data vesměs na jednom místě, takže například v případě požáru, i když na vrátnici je neustále někdo přítomný, tak než dojde k zjištění, že je něco špatně, může být už pozdě pro data firmy. Tento relativně málo pravděpodobný scénář, ale

Předmět	Počet	Cena
čipový systém	1 Ks	15 642Kč
čipy	25 Ks	7 275Kč
fyzické zabezpečení	18 Ks	13 824Kč
detektor kouře	5 Ks	5 305Kč
licence záloh	1 Ks	16 740Kč
poplatek měsíční		145Kč
zálohovací prostor	500GB	600Kč
Celkem		59 531Kč

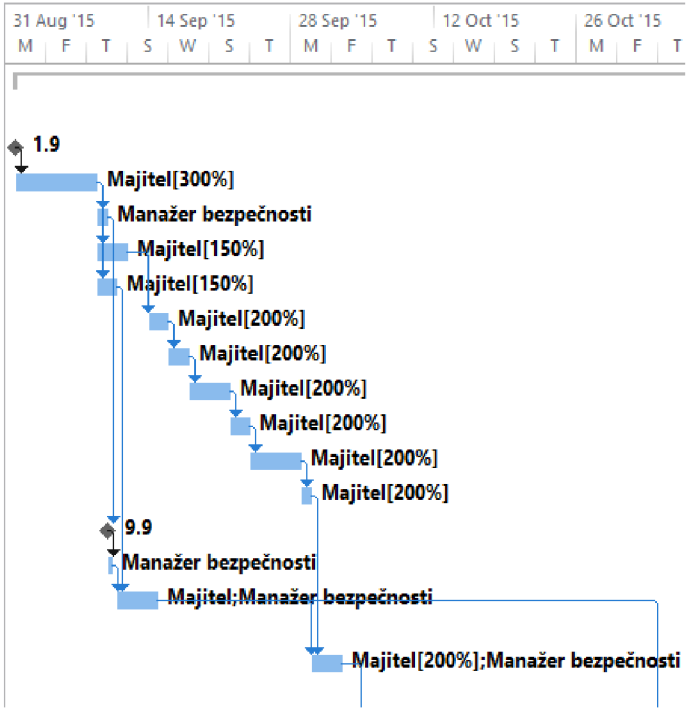
Tab. 4.3: Náklady celkem

ne nemožný, by s největší pravděpodobností ukončilo firemní působnost na trhu. Takže firma by přišla nejen o část fyzického majetku, ale i toho důležitějšího a to jsou data. Bankrot firmy je nevyčíslitelný.

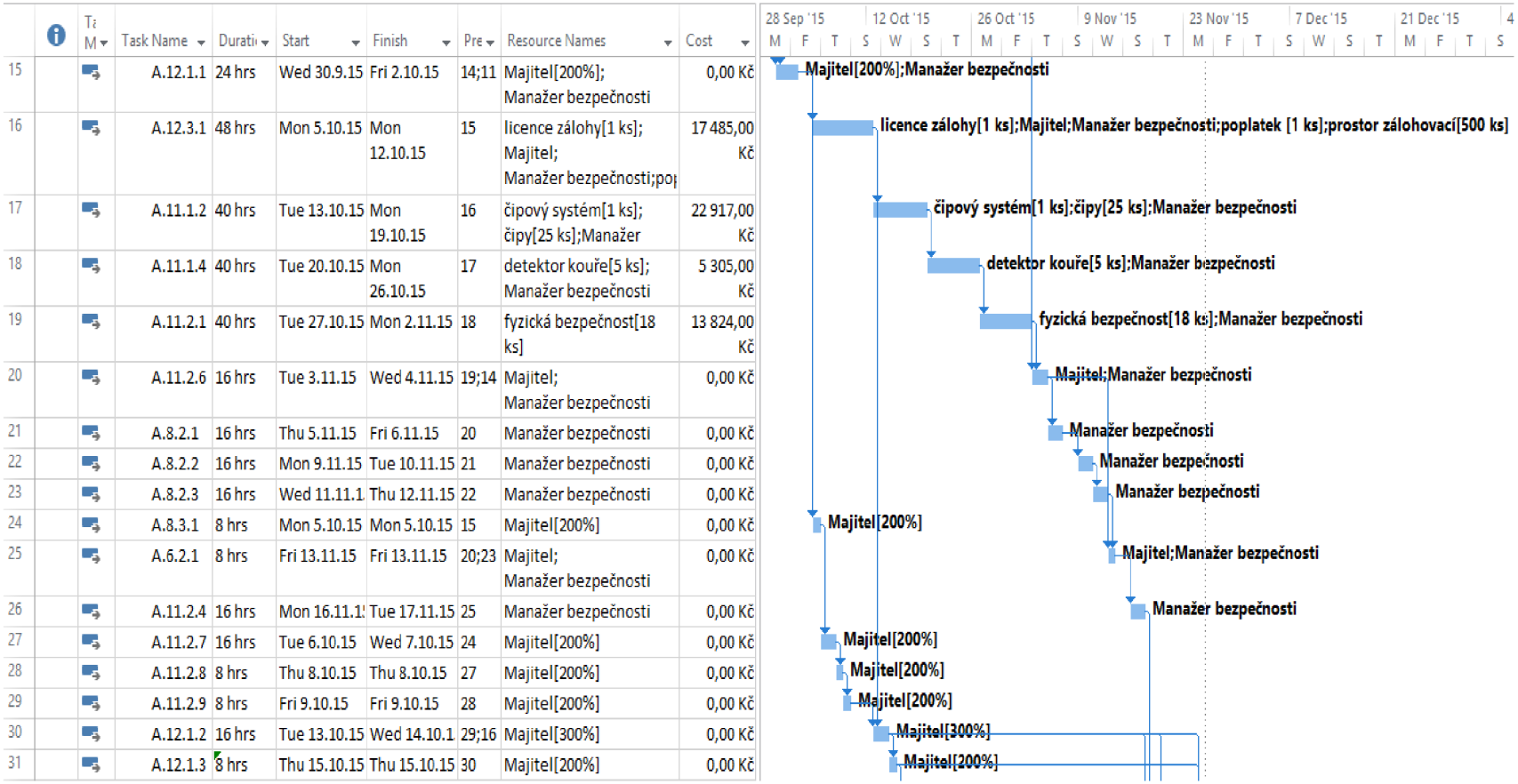
4.2.9 Časový harmonogram první etapy

Plán zavedení jednotlivých opatření je zobrazen na následujících Obrázcích 4.4, 4.5 a 4.6. Předpokládaný start zavádění je stanoveni na 1.9.2015, kdy všichni budou mít po dovolených a tudíž budou přítomni na firmě a mohou tedy být patřičně poučeni a tím se i podílet na bezpečnosti. Na obrázcích se nachází označení opatření a jak dlouho bude trvat. Opatření jsou seřazena podle důležitosti. Dále každé opatření je znázorněno v Gantově diagramu. První etapa zavádění by měla trvat 62 dní, kde je zahrnuta standardní pracovní doba i nepracující doba o víkendech. Hodiny stanovené na jednotlivé opatření by měly zohledňovat takový rozumný čas, aby se majitelé mohli zároveň věnovat i chodu firmy. Předpokládaný konec první etapy je stanoven na 25.11.2015 a v lednu potom by se mohlo začít s druhou etapou.

	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names	Cost
0		**První etapa**	**62 days**	**Tue 1.9.15**	**Wed 25.11.15**			**59 531,00 Kč**
1		**Začátek**	**0 days**	**Tue 1.9.15**	**Tue 1.9.15**			**0,00 Kč**
2		A.5.1.1	48 hrs	Tue 1.9.15	Tue 8.9.15	1	Majitel[300%]	0,00 Kč
3		A.5.1.2	8 hrs	Wed 9.9.15	Wed 9.9.15	2	Manažer bezpečnosti	0,00 Kč
4		A.6.1.1	24 hrs	Wed 9.9.15	Fri 11.9.15	2	Majitel[150%]	0,00 Kč
5		A.6.1.2	16 hrs	Wed 9.9.15	Thu 10.9.15	2	Majitel[150%]	0,00 Kč
6		A.7.1.1	16 hrs	Mon 14.9.15	Tue 15.9.15	4	Majitel[200%]	0,00 Kč
7		A.7.1.2	16 hrs	Wed 16.9.15	Thu 17.9.15	6	Majitel[200%]	0,00 Kč
8		A.7.2.1	16 hrs	Fri 18.9.15	Mon 21.9.15	7	Majitel[200%]	0,00 Kč
9		A.7.2.2	16 hrs	Tue 22.9.15	Wed 23.9.15	8	Majitel[200%]	0,00 Kč
10		A.7.2.3	24 hrs	Thu 24.9.15	Mon 28.9.15	9	Majitel[200%]	0,00 Kč
11		A.7.3.1	8 hrs	Tue 29.9.15	Tue 29.9.15	10	Majitel[200%]	0,00 Kč
12		A.8.1.1	0 hrs	Wed 9.9.15	Wed 9.9.15	3	Manažer bezpečnosti	0,00 Kč
13		A.8.1.2	4 hrs	Thu 10.9.15	Thu 10.9.15	12	Manažer bezpečnosti	0,00 Kč
14		A.8.1.3	16 hrs	Fri 11.9.15	Mon 14.9.15	13;5	Majitel; Manažer bezpečnosti	0,00 Kč
15		A.12.1.1	24 hrs	Wed 30.9.15	Fri 2.10.15	14;11	Majitel[200%]; Manažer bezpečnosti	0,00 Kč

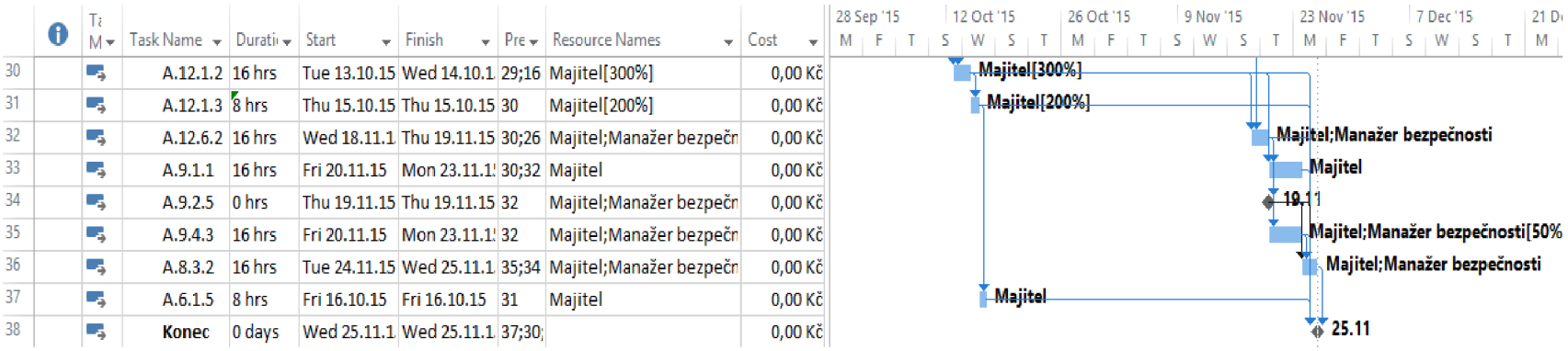


Obr. 4.4: Časový harmonogram část.1



	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names	Cost
15		A.12.1.1	24 hrs	Wed 30.9.15	Fri 2.10.15	14;11	Majitel[200%]; Manažer bezpečnosti	0,00 Kč
16		A.12.3.1	48 hrs	Mon 5.10.15	Mon 12.10.15	15	licence zálohy[1 ks]; Majitel; Manažer bezpečnosti;poj	17 485,00 Kč
17		A.11.1.2	40 hrs	Tue 13.10.15	Mon 19.10.15	16	čipový systém[1 ks]; čipy[25 ks];Manažer	22 917,00 Kč
18		A.11.1.4	40 hrs	Tue 20.10.15	Mon 26.10.15	17	detektor kouře[5 ks]; Manažer bezpečnosti	5 305,00 Kč
19		A.11.2.1	40 hrs	Tue 27.10.15	Mon 2.11.15	18	fyzická bezpečnost[18 ks]	13 824,00 Kč
20		A.11.2.6	16 hrs	Tue 3.11.15	Wed 4.11.15	19;14	Majitel; Manažer bezpečnosti	0,00 Kč
21		A.8.2.1	16 hrs	Thu 5.11.15	Fri 6.11.15	20	Manažer bezpečnosti	0,00 Kč
22		A.8.2.2	16 hrs	Mon 9.11.15	Tue 10.11.15	21	Manažer bezpečnosti	0,00 Kč
23		A.8.2.3	16 hrs	Wed 11.11.1	Thu 12.11.15	22	Manažer bezpečnosti	0,00 Kč
24		A.8.3.1	8 hrs	Mon 5.10.15	Mon 5.10.15	15	Majitel[200%]	0,00 Kč
25		A.6.2.1	8 hrs	Fri 13.11.15	Fri 13.11.15	20;23	Majitel; Manažer bezpečnosti	0,00 Kč
26		A.11.2.4	16 hrs	Mon 16.11.1	Tue 17.11.15	25	Manažer bezpečnosti	0,00 Kč
27		A.11.2.7	16 hrs	Tue 6.10.15	Wed 7.10.15	24	Majitel[200%]	0,00 Kč
28		A.11.2.8	8 hrs	Thu 8.10.15	Thu 8.10.15	27	Majitel[200%]	0,00 Kč
29		A.11.2.9	8 hrs	Fri 9.10.15	Fri 9.10.15	28	Majitel[200%]	0,00 Kč
30		A.12.1.2	16 hrs	Tue 13.10.15	Wed 14.10.1	29;16	Majitel[300%]	0,00 Kč
31		A.12.1.3	8 hrs	Thu 15.10.15	Thu 15.10.15	30	Majitel[200%]	0,00 Kč

Obr. 4.5: Časový harmonogram část.2



	Ta M	Task Name	Durati	Start	Finish	Pre	Resource Names	Cost
30		A.12.1.2	16 hrs	Tue 13.10.15	Wed 14.10.1	29;16	Majitel[300%]	0,00 Kč
31		A.12.1.3	8 hrs	Thu 15.10.15	Thu 15.10.15	30	Majitel[200%]	0,00 Kč
32		A.12.6.2	16 hrs	Wed 18.11.1	Thu 19.11.15	30;26	Majitel;Manažer bezpečn	0,00 Kč
33		A.9.1.1	16 hrs	Fri 20.11.15	Mon 23.11.1	30;32	Majitel	0,00 Kč
34		A.9.2.5	0 hrs	Thu 19.11.15	Thu 19.11.15	32	Majitel;Manažer bezpečn	0,00 Kč
35		A.9.4.3	16 hrs	Fri 20.11.15	Mon 23.11.1	32	Majitel;Manažer bezpečn	0,00 Kč
36		A.8.3.2	16 hrs	Tue 24.11.15	Wed 25.11.1	35;34	Majitel;Manažer bezpečn	0,00 Kč
37		A.6.1.5	8 hrs	Fri 16.10.15	Fri 16.10.15	31	Majitel	0,00 Kč
38		**Konec**	0 days	Wed 25.11.1	Wed 25.11.1	37;30		0,00 Kč

Obr. 4.6: Časový harmonogram část.3

4.3 Provoz, monitorování, přezkoumávání, údržba a zlepšování

Jak již bylo zmíněno v teoretické části práce zavedení systému bezpečnosti informací ve firmě je neustálý nekončící proces, který začíná vytvořením politiky bezpečnosti informací ve firmě a souhlasem vedení firmy. Systém bezpečnosti informací nemá stanovený konec díky cyklu PDCA, na který je navázán. Po dosažení požadovaných výsledků by mělo nadále docházet k neustálému zlepšování. S velkou rychlostí rozvoje informačních technologií přibývá i stále víc nových hrozeb, na které je zapotřebí reagovat. Je zapotřebí, aby vlastníci aktiv, se neustálé snažili vyhledávat nové hrozby, které by aktiva, za které jsou zodpovědní, mohly ohrozit a mohli je chránit před nimi. Důležité je dodržovat u všech zavedených opatření dle normy ISO/IEC 27001:2014 stanovené plány na kontroly opatření a monitorovat bezpečnostní incidenty. Vhodné je umožnit všem zaměstnancům možnost účastnit se různých bezpečnostních seminářů.

ZÁVĚR

Práce je rozdělena na dvě hlavní sekce a to na teoretickou a praktickou. Teoretickou částí se zabývá Kapitoly 2, kde se nachází hlavní pojmy a názvosloví informační bezpečnosti, související zákony, normy, ze kterých se v práci čerpalo, analýza rizik a popis bezpečnostních hrozeb. V druhé části teoretické sekce byla popsána problematika systému řízení bezpečnosti informací vycházející z ISO/IEC 27001.

Praktická sekce se skládá z několika částí. V Kapitole 3 byla provedena analýza aktuálního stavu firmu, kde došlo k analýze z pohledu situačního a informačního a následně byl zhodnocený stav společnosti. Tato analýza poukázala, na některé nedostatky, které by měly být eliminovány v druhé části byl sestaven seznam aktiv, která byla ohodnocena k vzhledem důležitosti pro firmu. Následně byl sestaven seznam hrozeb s pravděpodobností jejich výskytu a matice zranitelnosti. Z těchto tří hodnot byla sestavena matice rizik, která ukázala, která aktiva vůči kterým hrozbám jsou nejzranitelnější. Hlavní cíl práce je zpracován v Kapitole 4, kde došlo k návrhu opatření, které byly čerpány z normy ISO/IEC 27001:2014 příloha A a z normy ISO/IEC 27002/2014. Doporučená opatření pro firmu byla rozvržena do dvou etap. Opatření, která jsou navržena v první etapě, byly popsány detailněji předposlední sekci kapitoly. Většina opatření v první etapě byly administrativního charakteru, ale byly tam i takové, které vyžadovaly i finance. Finanční zhodnocení bylo zobrazeno ke konci této sekce. Závěr sekce je věnován podrobnému návrhu postupu první etapy při zavádění jednotlivých opatření. Cílem práce bylo navrhnout zavedení ISMS, čehož bylo i docíleno.

Přínos práce pro firmu je hlavně ve zlepšení bezpečnosti díky navrženým bezpečnostním opatřením, které by měly být zavedeny. Bylo zde i poukázáno na rizikovou situaci, která by s velkou pravděpodobnosti ukončila působení firmy na trhu, ale díky navrženým opatřením by mělo dojít k likvidaci těchto rizik. Postupy obsažené v navržených opatřeních ukazuji firmě, jak by měla bezpečnost vypadat a jak ji udržovat.

LITERATURA

[1] STAUDEK, Jan. Bezpečnost IT: Výkladový slovník pojmů. [online]. 2014. vyd. [cit. 2015-01-26]. Dostupné z: http://www.fi.muni.cz/usr/staudek/vyuka/security/PV017.xhtml

[2] DOUCEK, Petr et al. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 9788074310508.

[3] *ITIL - výkladový slovník a zkratky* [online]. 2012[cit. 2015-05-2]. Dostupné z: http://itsmf.cz/wp-content/uploads/2013/12/itil_2011_czech_glossary_v2.0.pdf

[4] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013, 377 s. ISBN 9788072048724.

[5] Seriál o ISMS. *Analýza rizik (1. část)* [online]. 2008, Díl 4 [cit. 2015-04-29]. Dostupné z: http://www.chrantesidata.cz/cs/art/1150-dil-4/

[6] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. ISBN 9788024746449.

[7] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

[8] KOCH, Miloš et al. *Management informačních systémů*. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. ISBN 9788021441576.

[9] MINISTR, Jan. *Informatika: Informační bezpečnost*. Karviná, 2011. Dostupné z: http://www.ivsosoom.cz/aktivity4.php

[10] ČERMÁK, Miroslav. Informační bezpečnost. *Clever and Smart* [online]. 2011 [cit. 2015-05-13]. Dostupné z: http://www.cleverandsmart.cz/informacni-bezpecnost/

[11] BRECHLEROVÁ, Dagmar. Řešení informační bezpečnosti (1. část). *SystemOnLine* [online]. 2005, č. 4 [cit. 2015-05-12]. Dostupné z: http://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm

[12] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, 2013.

[13] ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnostní informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, 2014.

[14] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, 2005.

[15] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, 2014.

[16] ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, 2014.

[17] Test autonomních detektorů kouře 2013. *DTest* [online]. 2013, č. 12 [cit. 2015-05-17]. Dostupné z: https://www.dtest.cz/clanek-3229/test-autonomnich-detektoru-koure-2013

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ISMS	systém řízení informační bezpečnosti
UPS	zdroj nepřerušovaného napájení
IS	informační systém
HDD	hard disk drive - pevný disk
SSD	solid state drive
CD	compact disk - kompaktní disk
DVD	digital versatile disc
HW	hardware
SW	software
OS	operační systém
DB	databáze
PC	personal computer - osobní počítač
NAS	network attached storage - datové úložiště na síti
LAN	local area network - lokální síť
WAN	wide area network - „široká“ síť
MAN	metropolitan area network - metropolitní síť
PDCA	plan-do-check-act - plánuj,udělej,zkontroluj,jednej

SEZNAM OBRÁZKŮ

2.1 Úrovně bezpečnosti ve firmě [2] 13
2.2 Základní struktura norem řady ISO 2700x 15
2.3 Proces řízení rizik dle ISO/IEC 27005 [12] 17
2.4 Model IT Governance dle [2] 19
2.5 Vztah ITG a ITSM dle [2] 20
2.6 Obecné schéma informačního systému [8] 24
2.7 Etapy procesu informační bezpečnosti [9] 25
2.8 PDCA model aplikovaný na procesy ISMS dle [15] 28
3.1 Zjednodušená topologie sítě firmy 37
4.1 KABA EVOLO LEGIC C-LEVER E300 64
4.2 Kensington zabezpečení 64
4.3 Detektor Jablotron JA–63S 65
4.4 Časový harmonogram část.1 67
4.5 Časový harmonogram část.2 68
4.6 Časový harmonogram část.3 69

SEZNAM TABULEK

2.1 Hlavní oblasti pro opatření dle normy ISO/IEC 27002 [16] 16
3.1 Ohodnocování aktiv 38
3.2 Ohodnocená identifikovaná aktiva 38
3.3 Ohodnocování hrozeb 39
3.4 Ohodnocené hrozby 40
3.5 Matice zranitelnosti 41
3.6 Ohodnocování rizik 42
3.7 Matice rizik 43
4.1 Soubor opatření 49
4.2 Aktiva a jejich vlastníci 56
4.3 Náklady celkem 66