VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZAVEDENÍ ISMS V MALÉM PODNIKU

THE IMPLEMENTATION OF ISMS IN SMALL COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. VÍT PALARCZYK
AUTHOR

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

BRNO 2015

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2014/2015
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Palarczyk Vít, Bc.

Informační management (6209T015)

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

Zavedení ISMS v malém podniku

v anglickém jazyce:

The Implementation of ISMS in Small 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. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 1.12.2014

Abstrakt

Tato diplomová práce je zaměřena na návrh implementace systému řízení bezpečnosti informací (ISMS) do konkrétní společnosti. V teoretické části jsou uvedeny základní pojmy a také podrobný popis ISMS. Dále je zde popsána analýza současného stavu bezpečnosti informací v dané společnosti. V praktické částí práce je provedena analýza rizik a výběr opatření pro minimalizaci nalezených rizik. Na závěr je navržen postup a časový plán zavedení vybraných opatření.

Abstract

This master's thesis is focused on the design of the implementation of information security management system (ISMS) into a specific business. In the theoretical part, it provides basic concepts and detailed description of ISMS. There is also described the analysis of a current information security state of the company. In the practical part, it provides a risk analysis and selection of measures to minimize found risks. In the final part is designed a process and a schedule of an implementation of the selected measures.

Klíčová slova

ISMS, systém řízení bezpečnosti informací, analýza rizik, PDCA model, normy řady ISO/IEC 27000

Key words

ISMS, information security management system, risk analysis, PDCA model, standards of ISO/IEC 27000

Bibliografická citace

PALARCZYK, V. Zavedení ISMS v malém podniku. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. 81 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

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

V Brně dne 21.ledna 2015 ....….....

Vít Palarczyk

Poděkování

Chtěl bych poděkovat vedoucímu práce panu Ing. Viktoru Ondrákovi, Ph.D. za vstřícný přístup a odbornou pomoc a také panu Ing. Petru Sedlákovi za cenné rady, které mi pomohly při psaní této práce.

Obsah

Úvod....10
1 Cíle práce, metody a postupy zpracování....11
2 Teoretická východiska práce....12
2.1 Základní pojmy....12
2.2 Systém řízení bezpečnosti informací....16
2.2.1 Model PDCA....17
2.2.2 Ustanovení ISMS....18
2.2.3 Zavádění a provoz ISMS....23
2.2.4 Monitorování a přezkoumání ISMS....26
2.2.5 Údržba a zlepšování....27
2.3 ITIL a metodiky COBIT....28
2.3.1 ITIL....28
2.3.2 COBIT....28
2.4 Normy řady ISO/IEC 27000....29
2.5 Právní rámec bezpečnosti informací v ČR....32
2.5.1 Zákon o svobodném přístupu k informacím....33
2.5.2 Zákon o elektronickém podpisu....33
2.5.3 Zákon o archivnictví a spisové službě....33
2.5.4 Zákon o ochraně osobních údajů....33
2.5.5 Zákon o ochraně utajovaných informací....34
2.5.6 Zákon o kybernetické bezpečnosti....34
2.6 Instituce zabývající se bezpečnosti informací....37
2.6.1 Národní instituce....37
2.6.2 Mezinárodní instituce....38
3 Analýza současného stavu....40
3.1 Informace o společnosti....40
3.2 Současný stav bezpečnosti....41
3.2.1 Fyzická bezpečnost....41
3.2.2 Bezpečnost provozu a komunikací....41
3.2.3 Bezpečnost lidských zdrojů....42
3.2.4 Řízení přístupu a ochrana osobních údajů....42
4 Vlastní návrhy řešení....43
4.1 Analýza rizik....43
4.2 Bezpečnostní opatření....49

4.2.1 Politiky bezpečnosti informací (A.5)....54
4.2.2 Organizace bezpečnosti informací (A.6)....54
4.2.3 Bezpečnost lidských zdrojů (A.7)....56
4.2.4 Řízení aktiv (A.8)....58
4.2.5 Řízení přístupu (A.9)....61
4.2.6 Kryptografie (A.10)....62
4.2.7 Fyzická bezpečnost a bezpečnost prostředí (A.11)....63
4.2.8 Bezpečnost provozu (A.12)....65
4.2.9 Bezpečnost komunikací (A.13)....67
4.2.10 Řízení incidentů bezpečnosti informací (A.16)....68
4.2.11 Soulad s požadavky (A.18)....70
4.3 Postup zavedení bezpečnostních opatření....72
4.4 Ekonomické zhodnocení a časový plán....74
5 Závěr....77
Seznam použité literatury....79
Seznam tabulek....80
Seznam obrázků....81

Úvod

V dnešní době mají informace velkou, někdy až nevyčíslitelnou hodnotu. Pro každou organizaci je důležité chránit důvěrné informace před zneužitím a veškerá data i zařízení chránit před poškozením či ztrátou. Ani při použití těch nejmodernějších technologií není možné zajistit stoprocentní bezpečnost. Snahou každé organizace je však předejít těm největším hrozbám a minimalizovat škody způsobené působením těchto hrozeb. Čím je však požadována vyšší bezpečnost, tím se zvyšují také náklady na zavedení patřičných opatření. Každá organizace se tak musí rozhodnout, jaké finanční prostředky je ochotna do zabezpečení investovat a také, zda další vynaložené finanční náklady opravdu přinesou odpovídající navýšení bezpečnosti. Mnoho společností zapomíná při zavádění bezpečnostních opatření na nejrizikovější faktor a tím jsou sami lidé, neboli zaměstnanci, dodavatelé, zákazníci a jiné externí strany. Největší přístup k důležitým a důvěrným informacím mají zaměstnanci dané společnosti. Je tedy vhodné oddělit pravomoci a umožnit zaměstnancům přístup pouze k informacím, které opravdu potřebují k výkonu práce. Vždy zde však musí být někdo, kdo zná bezpečnostní kódy, nebo má přístup k tajným informacím apod. I tito lidé mohou svého postavení zneužít, či kvůli své neopatrnosti a nedbalosti ztratit nebo zničit důležitá data a způsobit tak organizaci značné škody. Proto je vždy důležité dbát na důkladné školení zaměstnanců v oblasti bezpečnosti informací, seznámení zaměstnanců s jejich odpovědnostmi a stanovení disciplinárního řízení pro případné narušení bezpečnosti. Samotné donucování dodržování pravidel, hrozby postihu při porušení bezpečnosti a jiné externí faktory motivace jsou však často nedostačující. Mnohem efektivnější je přesvědčit zaměstnance o důležitosti dodržování bezpečnostních pravidel tak, aby sami chtěli a cítili potřebu tato pravidla dodržovat.

1 Cíle práce, metody a postupy zpracování

Cílem této práce je navrhnout zavedení systému řízení bezpečnosti informací (ISMS) ve společnosti, která působí jako účetní a daňová kancelář. Hlavním podnětem pro zavedení ISMS je požadavek vedení společnosti na zvýšení bezpečnosti informací. Vedení společnosti tak zavedení ISMS plně podporuje. Postup analýzy rizik a návrh bezpečnostních opatření se bude opírat o normu ČSN ISO/IEC 27001. Společnost neplánuje certifikaci ISMS, proto není cílem zavést všechna bezpečnostní opatření této normy, ale vybrat pouze ta, která jsou důležitá pro minimalizaci velkých bezpečnostních rizik ve společnosti. Sběr informací pro analýzu rizik probíhal přímo v dané společnosti a to převážně komunikací s vedením i se zaměstnanci společnosti. Cílem této práce je také zhodnocení finanční a časové náročnosti projektu a návrh časového plánu pro zavedení vybraných bezpečnostních opatření.

V první části této práce jsou zpracována teoretická východiska, tedy základní pojmy a podrobnosti týkající se systému řízení bezpečnosti informací (ISMS). Také je zde shrnuta metodika COBIT, knihovna ITIL, normy řady ISO/IEC 2700, zákony ČR týkající se bezpečnosti informací, především zákon o kybernetické bezpečnosti a dále jsou zde uvedeny národní i mezinárodní instituce zabývající se bezpečnosti informací. V další části jsou uvedeny základní informace o dané společnosti a je provedena analýza současného stavu bezpečnosti informací v této společnosti. Poslední část této práce obsahuje analýzu rizik a návrh bezpečnostních opatření i s postupem zavedení daných opatření pro minimalizaci zjištěných rizik. Na závěr je provedeno ekonomické zhodnocení zavedení ISMS a shrnutí celé práce.

2 Teoretická východiska práce

V každé organizaci je důležité chránit informace jak proti náhodnému poškození, tak proti úmyslnému zneužití. S nástupem internetu jsou digitální data stále ve větším nebezpečí. Je však potřeba chránit veškeré informace, tedy i v papírové či ústní podobě. Největší hrozbu vždy tvoří sami lidé, a to především vlastní zaměstnanci organizace, kteří mají k informacím vždy snazší přístup. Je proto důležité informace zabezpečit nejen proti útokům z vnějšku, ale také vůči nedbalosti a neznalosti či dokonce krádeži a zneužití ze strany vlastních lidí. Zároveň je důležité brát v potaz finanční náklady potřebné pro zabezpečení. Ani vynaložení veškerých nákladů nám nikdy nezaručí naprosto dokonalou bezpečnost, je proto nutné stanovit takové náklady, které budou odpovídat přiměřené bezpečnosti.

V této kapitole budou popsány základní pojmy informační bezpečnosti a také vysvětlena problematika systému řízení bezpečnosti informací (ISMS).

2.1 Základní pojmy

Data

Přestože jsou data a informace někdy chápány jako jeden a tentýž pojem, je potřeba je rozlišovat. Data získáváme měřením, pozorováním, výpočtem atd. Jsou to holá fakta v podobě čísel nebo textu, která sama o sobě nemají význam. Teprve přiřazením významu získáme informace [1].

Informace

Základem informace jsou samotná data. Jako informaci pak chápeme poznatek, který má v daném kontextu určitý význam a odstraňuje neznalost či neurčitost nějakého jevu nebo události. Je tedy upravena do podoby, která je pro daného příjemce čitelná a užitečná [1] [2].

Informační systém (IS – Information system)

Pro pojem informační systém existuje spousta definic. Systém je obecně soubor prvků, které mezi sebou mají určité vazby. Informační systém lze tedy chápat jako soubor

informací, které jsou vzájemně propojeny, a procesů, které dané informace využívají a pracují s nimi [1] [2].

Informační technologie (IT – Information Technology)
Pojem informační technologie zahrnuje množinu nástrojů, procesů a dalších prostředků, které slouží k získávání, uchovávání a zpracovávání dat a také k jejich manipulaci, přenosu a prezentaci [3].

Informační a komunikační technologie (ICT – Information and Communication Technology)
Zkratka ICT v sobě zahrnuje nejen informační, ale také komunikační technologie, což představuje množinu technických prostředků, kterých se využívá pro sdělování a přijímání informací, tedy pro komunikaci [3].

Bezpečnost (Security)
Bezpečnost určuje míru ochrany určitého objektu proti hrozbám a škodám, které mohou nastat [1].

Dostupnost (Availability)
Zajištění, že daná informace je oprávněnému uživateli přístupná v požadovaný okamžik [2].

Důvěrnost (Confidentiality)
Zajištění, že daná informace je přístupná pouze oprávněným uživatelům [2].

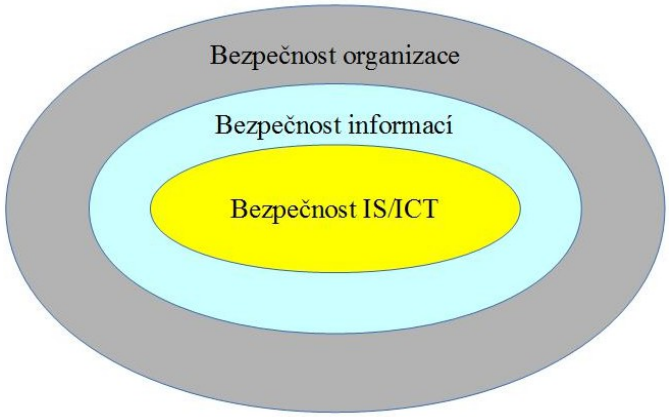
Integrita (Integrity)
Zajištění, že daná informace je správná a úplná [2].

Bezpečnost informací (Information Security)
Bezpečnost informací (informační bezpečnost) řeší ochranu informací a zaměřuje se na zachování integrity, dostupnosti a důvěrnosti informací. Má tedy za úkol, aby informace byly správné, kompletní, neporušené a dostupné v případě potřeby, ale zpřístupněny

pouze po úspěšné autorizaci a chráněny tak proti zneužití. Nejedná se však pouze o informace digitální, ale o informace všeho druhu a všech typů. Tedy jak o materiály v papírové podobě, tak o veškeré informace podané ústní formou, např. při sdělování informací novinářům apod. Informační bezpečnost zahrnuje způsoby nakládání s těmito informacemi, jejich zpracování, archivování, skartaci apod. [1] [2].

Podmnožinu bezpečnosti informací tvoří bezpečnost IS/ICT, která chrání pouze aktiva, která jsou přímo součástí informačního systému podporovaného informačními a komunikačními technologiemi [1].

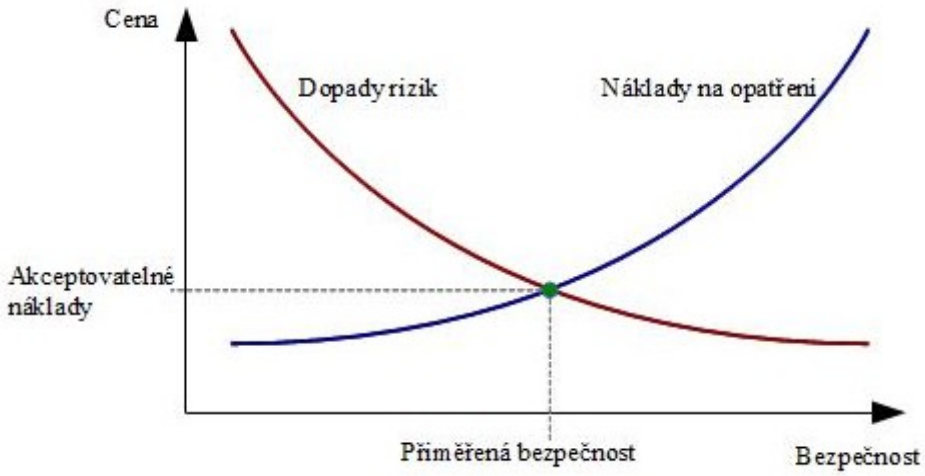
Bezpečnost informací i bezpečnost IS/ICT jsou společně součástí bezpečnosti organizace, která jim je nadřazena. Celé schéma je zobrazeno na obrázku 1. Bezpečnost organizace zajišťuje bezpečnost fyzických objektů a také majetku organizace [1].



Obrázek 1: Bezpečnost organizace (upraveno dle [1])

Přiměřená bezpečnost

Jako přiměřenou bezpečnost chápeme, když velikost vynaloženého úsilí a investic do bezpečnosti IS odpovídá hodnotě aktiv organizace a míře bezpečnostních rizik. Přiměřenou bezpečnost stanovuje především politika organizace. Na obrázku 2 je znázorněn graf přiměřené bezpečnosti za akceptovatelné náklady [2].



Obrázek 2: Přiměřená bezpečnost za akceptovatelné náklady (upraveno dle [2])

Aktivum (Asset)

Mezi aktiva patří vše co má pro vlastníka určitou hodnotu. Jedná se tedy o veškerý hmotný i nehmotný majetek. Za nejcennější aktiva se považují právě informace, jejichž ztráta či vyzrazení a zneužití může mít pro organizaci někdy až fatální následky [1].

Hrozba (Threat)

Hrozba je jakákoli událost, která určitým způsobem ohrožuje bezpečnost, působí na zranitelné místo aktiva a může mít za následek způsobení škody na tomto aktivu. Hrozby můžeme rozdělit podle jejich původu na objektivní a subjektivní. Objektivní jsou přírodního původu jako např. požár, povodeň, blesk, zemětřesení apod. A subjektivní jsou hrozby, které plynou z lidského faktoru. Dále je můžeme dělit na úmyslné (krádež, útok hackera apod.) a neúmyslné, které jsou způsobené nedbalostí či neznalostí [1].

Zranitelnost (Vulnerability)

Zranitelnost je slabina systému, která může být zneužita k poškození či zničení aktiv. Hodnota každého aktiva je ohrožena různými vlivy, proto jsou určitou mírou zranitelná všechna aktiva [1].

Riziko (Risk)

Riziko určuje stupeň či míru do jaké je dané aktivum ohroženo neboli s jakou pravděpodobností dojde k poškození nebo zničení hodnoty aktiva působením konkrétní hrozby [1].

Dopad (Impact)

Dopad je škoda, která vznikla působením hrozby na určité aktivum [2].

Opatření (Countermeasure)

Jako opatření chápeme jakoukoli aktivitu, která nám umožní snížit působící hrozbu [2].

Bezpečnostní incident (Security Incident)

Bezpečnostní incident je jakýkoli útok neboli využití zranitelného místa s cílem krádeže nebo poškození určitého aktiva. Dále se jedná i o neúmyslnou akci, která způsobí škodu na aktivech [1].

Správa informační bezpečnosti (Security Management)

Tato správa je v každé organizaci důležitým článkem pro řešení bezpečnostních incidentů a také pro havarijní plánování. Jejím úkolem je tedy řízení problematiky ochrany veškerého majetku a také řízení bezchybného provozu a rozvoje dané organizace [1].

2.2 Systém řízení bezpečnosti informací

Tato kapitola je v souladu s normou ČSN ISO/IEC 27001 z roku 2006 a následně doplněna podle nové verze této normy z roku 2014, která sice byla přepracována do více kapitol, avšak principiálně se význam normy nezměnil. I proto je pro tuto kapitolu ponechána původní kostra dle starší verze normy.

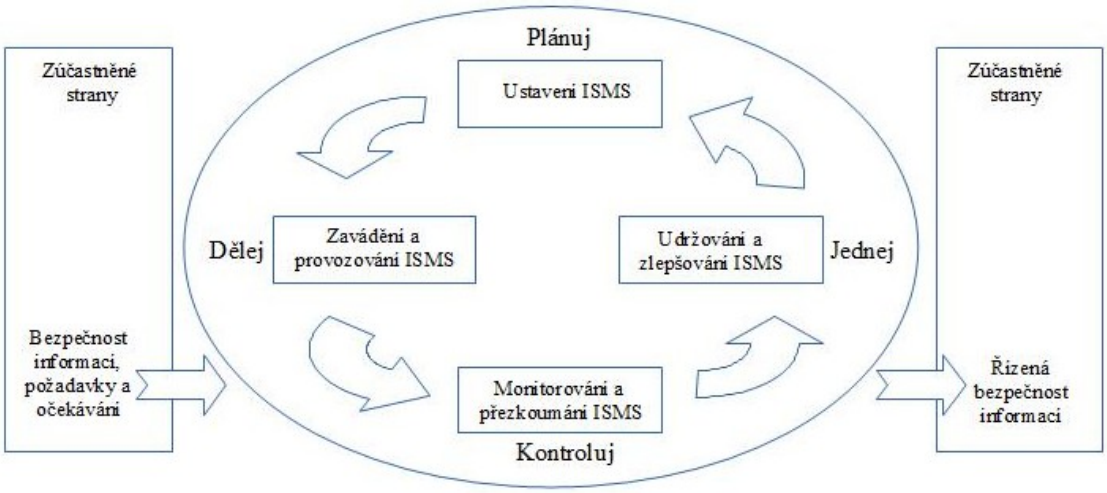
ISMS (Information Security Management System) je základem pro účelné a účinné řízení bezpečnosti informací. Představuje část celkového systému řízení organizace, založenou na přístupu organizace k rizikům činností, která je zaměřena na ustanovení,

zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací [4].

2.2.1 Model PDCA

Tvůrcem modelu PDCA „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act) je W. E. Deming, který tento model (někdy také Demingův model) použil ve svých pracích jako první. Deming v tomto modelu formuloval zásady vymezení určitého systému řízení, také jeho realizaci a cyklickou snahu o neustálé zlepšování daného systému. Koncept PDCA modelu se dříve používal v průmyslu pro inovaci a nasazování systému řízení. Dnes je tento přístup základem nejen pro oblast řízení informační bezpečnosti, ale také pro mezinárodní standardy v oblasti integrovaných systémů řízení [4].

Na obrázku 3 je znázorněn PDCA model aplikovaný na procesy ISMS. Je zde vidět, že ISMS očekává na vstupu požadavky bezpečnosti informací a také očekávání zainteresovaných stran, které dané požadavky a očekávání splňují. Také je zde vidět vzájemné propojení jednotlivých ISMS procesů, které jsou aplikovány na dané činnosti PDCA modelu [5].



Obrázek 3: PDCA model aplikovaný na procesy ISMS (upraveno dle [5])

Jedná se tedy o snahu postupného zlepšování způsobem neustálého opakování těchto čtyř činností [5]:

- Ustavení ISMS (Plánuj) – v první etapě je úkolem stanovit politiku ISMS a také cíle, procesy a postupy, které souvisejí s řízením rizik a zlepšováním bezpečnosti informací organizace, a to takovým způsobem, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
- Zavádění a provozování ISMS (Dělej) – zde již zavedeme stanovenou politiku ISMS a také všechna opatření, procesy i postupy.
- Monitorování a přezkoumání ISMS (Kontroluj) – dále provádíme posouzení, případně i měření výkonu procesu vůči stanovené politice ISMS, cílům a praktickým zkušenostem. Získané výsledky předáme vedení organizace ke kontrole.
- Udržování a zlepšování ISMS (Jednej) – z výsledků interního auditu ISMS přijmeme preventivní opatření i patřičná opatření k nápravě. Pro dosažení neustálého zlepšování ISMS je potřeba přezkoumání systému řízení vedením organizace.

2.2.2 Ustanovení ISMS

Tato etapa má za úkol stanovit rozsah a hranice, ve kterých je ISMS uplatňováno. V podstatě definuje základy celého systému řízení bezpečnosti informací (ISMS) a její výsledky se dále využívají v dalších etapách PDCA cyklu, kde mají dlouhodobější vliv. Proto je velice důležité promyslet veškeré souvislosti již v této první etapě. Pozdější úpravy jsou velmi náročné a vyžadují vysoké finanční náklady. Je tedy nutné stanovit jasné manažerské zadání a po definici rozsahu a hranic ISMS se musí vedení podniku zavázat k podpoře informační bezpečnosti tím, že odsouhlasí tzv. Prohlášení o politice ISMS. Důležitým krokem je i provést analýzu rizik a po ohodnocení rizik vybrat vhodná bezpečnostní opatření. Pro větší přehlednost je vhodné vytvořit skupiny aktiv, které mají podobné bezpečnostní parametry. V posledních krocích etapy plánování je potřeba formální souhlas vedení organizace s výběrem daných opatření a se zbytkovými riziky a také příprava Prohlášení o aplikovatelnosti, které se dále použije v druhé etapě PDCA cyklu [4].

Kontext organizace

Pro organizaci je důležité porozumět jejímu kontextu, tedy určit významná interní i externí hlediska, dle kterých bude dosahovat daných cílů ISMS. Dále je také nutné určit zainteresované strany, které mají k ISMS organizace určitý vztah, včetně jejich potřeb a očekávání, které se vztahují k bezpečnosti informací [6].

Stanovení rozsahu a hranic ISMS

Výchozí rozsah a hranice ISMS nemusí vždy pokrývat celou organizaci. Je zde hlavně potřeba shrnout činnosti a cíle organizace, dále organizační strukturu, umístění lokalit a technologie, které organizace využívá pro zpracování a přenos informací. Pokud jako rozsah ISMS stanovíme celou organizaci, máme sice výhodu v tom, že je bezpečnost informací již od počátku řešena pro celou organizaci, ale potřebné zdroje a finanční prostředky jsou často velice vysoké a celý projekt tak může být pro organizaci přítěží a způsobit více škody než užitku. Je proto často vhodné zvolit jiný přístup a ze začátku omezit rozsah ISMS pouze na určitou část organizace. Nejlépe tu, kde je jednoduché zavádět změny a vylepšení, ať už se jedná o konkrétní organizační celek, vybranou pobočku nebo informační systém společnosti. Dává nám to pak i tu výhodu, že na vybranou oblast můžeme soustředit více úsilí, zvládnout veškeré požadavky ISMS a obhájit tak výhody i potřebu samotného zavádění ISMS. Už při stanovení rozsahu můžeme počítat s tím, že v prvním roce budeme chtít zavést ISMS rychleji, abychom získali co nejvíce zkušeností. Zkrátíme tedy cyklus PDCA tak, abychom ho za rok mohli dvakrát či třikrát zopakovat a postupně tak použili zkušenosti získané z předchozích cyklů [4].

Prohlášení o politice ISMS

Politika ISMS je důležitý dokument, který usnadňuje prosazování pravidel a požadavků na bezpečnost informací v dané organizaci. Jejím úkolem je upřesnit cíle, kterých má být v rámci ISMS dosaženo a zohlednit přitom cíle a požadavky organizace spolu se zákonnými a regulativními požadavky. Dále musí být určen směr pro řízení bezpečnosti informací a vytvořeny vazby potřebné nejen pro vybudování, ale i pro údržbu ISMS. Nakonec je zapotřebí určit kritéria pro popis a hodnocení rizik. Celá politika ISMS musí být schválena vedením organizace [4].

Vůdčí role

Pro role, které jsou relevantní bezpečnosti informací, musí být přiřazeny dané odpovědnosti a pravomoci. Za samotné přiřazení zodpovídá vrcholové vedení organizace. Určené odpovědné osoby musí zajistit, že ISMS organizace bude v souladu s normou a že budou podávány zprávy o výkonnosti ISMS vedení organizace [6].

Řízení rizik

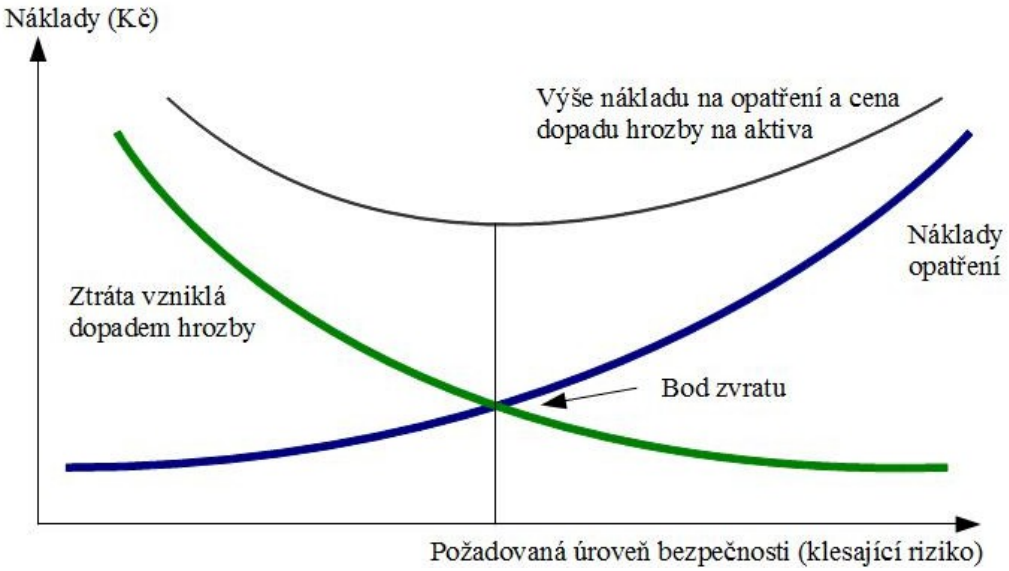
Řízení rizik je základem pro každý systém řízení bezpečnosti informací a také ovlivňuje celkovou efektivitu fungování ISMS. Pokud dobře známe daná rizika, můžeme vybrat vhodná bezpečnostní opatření a snížit tak dopady rizik. Rizika nám v podstatě určují do jaké míry můžeme vyhovět potřebám ISMS. Celý postup řízení rizik by měl být zdokumentován [4].

Řízení rizik se skládá z jejich hodnocení, zvládání a akceptace. Hodnocení rizik se dále skládá z analýzy a vyhodnocení rizika, což představuje odhad míry rizika, určení jeho zdrojů a také určení významu odhadnutého rizika jeho porovnáním vůči daným kritériím. Zvládání rizik je proces, který se snaží změnit riziko pomocí výběru a přijímání opatření. Samotné rozhodnutí přijmout riziko se pak označuje jako Akceptace rizika [4].

Podle podrobnosti analýzy můžeme proces analýzy rizik rozlišit následovně [4]:

- nedělat nic – akceptace všech rizik
- neformální přístup – přesné postupy analýzy nejsou dokumentovány
- základní přístup – postupy analýzy jsou dokumentovány pouze rámcově, ale je k dispozici vize řešení bezpečnosti informací
- detailní přístup – analýza je velice podrobná pro všechna rizika, dodržuje se předem stanovená metodika
- přístup kombinovaný – podrobná analýza je pouze u některých rizik a některá rizika mohou být i záměrně opominuta

Abychom stanovili maximální náklady pro opatření na ochranu aktiv, je zapotřebí aktiva ocenit. Na obrázku 4 jsou znázorněny vztahy mezi hodnotou aktiva, resp. vzniklou ztrátou (při poškození nebo zničení), a náklady potřebných pro realizaci ochrany aktiva formou opatření [4].



Obrázek 4: Nákladový model pro realizaci bezpečnostních opatření (upraveno dle [4])

Pro efektivní řízení rizik je důležité, aby se na něm podílelo více lidí s různými pohledy a názory. Dále aby za koordinaci i integraci postupů organizace byl vždy někdo odpovědný a procesy pro řízení informatiky, řízení bezpečnosti informací apod. byly navzájem provázány. Neméně důležitá je jak dokumentace, díky které musí být možnost zjistit odpovědnost za provedená rozhodnutí, tak pravidelná aktualizace (alespoň jednou ročně) na základě nových poznatků z monitorování ISMS. Posledním důležitým faktorem pro efektivní řízení rizik je zlepšení znalostí, tedy systematické ukládání a správa znalostí tak, aby posloužili dalšímu rozvoji systému řízení rizik [4].

V moderních metodách řízení rizik je snaha vybudovat a udržovat přehled o aktuálních, známých bezpečnostních rizicích, tyto rizika ohodnotit podle jejich významnosti, určit odpovědnou osobu a sledovat postup zvládání rizika v čase. Toto se zajišťuje vybudováním tzv. registru rizik, kde jsou ukládány informace o všech bezpečnostních rizicích. Všechny tyto informace lze pak použít pro rychlé a správné rozhodování, což vede k efektivnějšímu řízení bezpečnosti informací [4].

Popis rizik se často využívá při přijímání důležitých rozhodnutí a to nejen v rámci ISMS, proto je důležité, aby řízení rizik splňovalo tyto zásady [4]:

- První zásadou je, aby byly rizikové scénáře pro danou organizaci jedinečné a vyjadřovaly konkrétní situaci. Není tedy dobré omezit se pouze na obecně definované hrozby jako je např. požár.
- Další zásadu tvoří přiměřený počet rizikových scénářů. Rozsah by měl být 20 až 50 rizik. Po překročení tohoto rozsahu může být složité až nemožné učinit správná rozhodnutí, lze však rizika vhodně uspořádat do skupin a limity dodržet.
- Poslední zásadou je, aby hodnoty stanovené při hodnocení rizik byly okomentovány. Díky tomu jsme schopni ohodnocení rozvíjet a upravovat podle aktuálních změn a nemusíme vždy začínat od začátku.

Pro řízení rizik je důležité především identifikovat všechna aktiva a určit jaký mají význam vzhledem k organizaci. Aktiva se dělí na primární (nehmotná) a sekundární (hmotná). Mezi nehmotná patří informace, procesy i aktivity organizace, ale také znalosti a know-how. Mezi hmotná aktiva samozřejmě patří prostory organizace, technické a programové vybavení a komunikační infrastruktura. Pro každé aktivum je potřeba vyjádřit míru jeho důvěrnosti, integrity a dostupnosti. Také je vhodné daná aktiva uspořádat do skupin dle jejich ohodnocení, protože každá taková skupina bude následně obsahovat aktiva s podobnými riziky. Díky tomu se zjednodušuje následné hodnocení a zvládání rizik [4].

Po identifikaci aktiv následuje identifikace hrozeb, které mohou působit na konkrétní skupinu aktiv a negativně tak ovlivnit jejich hodnotu. S ohledem na tuto hodnotu a také na význam aktiv dané skupiny se určí výše dopadu na aktivum a výše škody, kterou by hrozba mohla způsobit. Dále se určí pravděpodobnost s jakou může hrozba nastat a míra zranitelnosti. Jakmile určíme nejrizikovější scénáře, tedy situace, kde jsou odhadovány největší škody, s vysokou pravděpodobností i mírou zranitelnosti, vybereme vhodná bezpečnostní opatření. Pro zvládání rizik existují čtyři možné formy [4]:

1. Vyhýbání riziku – riziku se můžeme vyhnout, když se sníží pravděpodobnost, s jakou hrozba nastane, nebo se sníží dopad dané hrozby.
2. Přenesení rizika – určitá rizika můžeme přenést na jiný subjekt, např. na pojišťovnu. Tento subjekt je potom potřeba doplnit do rozsahu ISMS.

3. Aplikace vhodného bezpečnostního opatření – tato forma zvládání rizika je nejčastější. Díky zavedení bezpečnostního opatření snižujeme zranitelnost u daného rizika.
4. Akceptace rizika – přijmutí rizika je v podstatě konečný výsledek zvládání rizik. Je zde vždy potřeba zaznamenat zbytková rizika.

Souhlas se zavedením ISMS

Další krok v etapě Ustanovení ISMS je získání souhlasu vedení se zavedením ISMS. Vedení by mělo odsouhlasit návrh bezpečnostních opatření, nutných pro snížení rizik, a také přijmout nebo vyjádřit nesouhlas se zbytkovými riziky. Při nesouhlasu je ještě možné daná bezpečnostní opatření upravit [4].

Prohlášení o aplikovatelnosti

Posledním krokem v této etapě je příprava dokumentu Prohlášení o aplikovatelnosti, který je povinný pro ty organizace, které usilují o shodu svého ISMS s normou ISO/IEC 27001. Tento dokument obsahuje cíle opatření a také vybraná bezpečnostní opatření pokrývající bezpečnostní rizika [4].

Podpora

Organizace musí zajistit potřebné zdroje pro všechny etapy ISMS a také zaručit, že odpovědné osoby jsou kompetentní a kvalifikovány pro výkon dané práce. Pracovníci musí být seznámeni s politikou bezpečnosti informací a také s důsledky při nedodržování pravidel a požadavků ISMS [6].

2.2.3 Zavádění a provoz ISMS

V druhé etapě PDCA cyklu je hlavním cílem prosadit daná bezpečnostní opatření, která byla ustanovena v první etapě. Tato opatření by měla být součástí dokumentu Příručka bezpečnosti informací. Také je nutné všem uživatelům i manažerům vysvětlit dané bezpečnostní principy. Vše je potřeba podrobně naplánovat spolu s termíny, odpovědnými osobami apod. Pro tuto etapu jsou důležité následující činnosti [4]:

- Vytvořit Plán zvládání rizik a postupně tento dokument aplikovat do praxe.
- Zavést bezpečnostní opatření, která byla stanovena v předchozí etapě.

- Ujasnit si podrobnosti pravidel a postupů daných opatření v definovaných oblastech bezpečnosti informací a zapsat je do příručky bezpečnosti informací.
- Zajistit, aby se v organizaci správně rozšiřovalo povědomí o bezpečnosti.
- Zaškolit uživatele, manažery a především pracovníky z oblasti řízení bezpečnosti.
- Stanovit jakým způsobem se bude měřit účinnost zavedených opatření a následně dané ukazatele sledovat.
- Dále je potřeba mít ujasněny postupy při bezpečnostních incidentech. Tedy nejen pro rychlou reakci na ně, ale i pro jejich detekci.
- Všechny zdroje, dokumenty a záznamy ISMS musí podléhat procesu řízení.

Plán zvládání rizik

Tento dokument v sobě zahrnuje [4]:

- všechny činnosti potřebné pro řízení bezpečnostních rizik,
- popis, stanovené cíle a priority těchto činností,
- určení osobní odpovědnosti za provádění těchto činností,
- omezující faktory,
- potřebné zdroje (finanční, personální apod.),
- činnosti pro snižování bezpečnostních rizik,
- činnosti, které jsou dány požadavky ISO/IEC 27001.

Příručka bezpečnosti informací

Příručka bezpečnosti informací je souhrn dokumentů, které udávají bezpečnostní pravidla, principy, zásady a odpovědnosti. Důležité u těchto dokumentů je, aby nebyl jeden dokument pro všechny, ale aby každá cílová skupina měla přiřazen dokument určený přímo pro ni s konkrétní mírou podrobnosti. Cílovými skupinami tedy myslíme např. skupinu manažerů, uživatelů, správců apod. Tyto dokumenty navíc rozdělujeme do tří úrovní podle důležitosti [4]:

- Nejvyšší úroveň tvoří ty nejdůležitější dokumenty. Tedy ty, které jsou povinné a potřebné pro systém řízení. Patří mezi ně rozsah i politika ISMS, zpráva o hodnocení rizik, prohlášení o aplikovatelnosti, plán zvládání rizik apod.

- Střední úroveň obsahuje dokumenty, které definují dílčí procesy a postupy takovým způsobem, aby bylo vždy jasné kdo, co, kdy, kde a jak má vykonat. Tedy tak, aby bylo zajištěno efektivní prosazení dílčích bezpečnostních opatření daného konkrétního ISMS.
- Na nejnižší úrovni jsou pak pracovní postupy, tedy dokumenty, které obsahují podrobný popis úkonů jednotlivých dílčích procesů. Tato úroveň dokumentů není vždy nutná, je možné se pouze odkázat na příslušnou dokumentaci použitích technických systémů.

Povědomí o bezpečnosti v organizaci

Je důležité, aby se bezpečnostní povědomí neustále prohlubovalo. Je to především kvůli změnám při rozvoji ISMS a náboru nových pracovníků. Jde tedy o nikdy nekončící proces promítnutí definovaných pravidel a postupů do reálného chování všech uživatelů i odpovědných pracovníků. Jelikož je lidský faktor v oblasti bezpečnosti vždy ten nejslabší článek, je potřeba zajistit neustálou komunikaci s pracovníky a projednávat s nimi bezpečnostní incidenty včetně jejich příčin a možných následků. A zajistit tak, aby byly všichni seznámeni s bezpečnostními riziky, a byli tak schopni zvládat i situace, které nejsou v dokumentaci popsány [4].

Měření účinnosti ISMS

Pro efektivní řízení bezpečnosti je důležité měřit účinnost zavedených bezpečnostních opatření. Jedná se tedy o pravidelné sledování stanovených ukazatelů, které by nám měli poskytovat informace o tom, jak doopravdy systém řízení bezpečnosti funguje. Získané výsledky jsou pak následně podkladem pro všechna důležitá rozhodnutí. Stanovení těch správných ukazatelů je velmi důležité. Z počátku je lepší stanovit spíše méně ukazatelů, ale takovým způsobem, abychom pokryli oblasti řízení, které mají nejvyšší prioritu. Jakmile získáme základní zkušenosti z chování systému řízení, můžeme počet ukazatelů navýšit. Dále není příliš vhodné snažit se o získávání absolutních ukazatelů. Příliš vysoká přesnost ukazatelů je spojena s vysokými náklady a většinou nám pro rozhodování stačí pouze relativní představa. Tento proces měření účinnosti není jednoduchý a je potřeba s ním počítat už od první etapy PDCA cyklu, tedy v době návrhu celého ISMS [4].

Proces řízení

Je důležité, aby veškeré činnosti byly prováděny řízeným způsobem. Jedná se tedy hlavně o řízení provozu, zdrojů, dokumentace i záznamů ISMS. Kromě dodržování dohodnutých pravidel, je také nutné zaznamenávat všechny informace týkající se ISMS, tedy jak dosažené výsledky, tak všechny provedené činnosti, odpovědné osoby, termíny apod. Dané podklady nám pak poslouží ve fázi monitorování [4].

Dále je nutné definovat postupy a opatření pro řízení incidentů. Jsou tedy zapotřebí nástroje, které dokáží včas odhalit bezpečnostní slabiny a incidenty a upozornit na ně odpovědné pracovníky. Zkušenosti získané z řešení těchto incidentů jsou pak využity pro optimalizace pravidel ISMS [4].

2.2.4 Monitorování a přezkoumání ISMS

V této třetí etapě PDCA cyklu je nutné prověřit všechny zavedené bezpečnostní opatření a také jejich důsledky na ISMS tak, abychom zajistili účinnou zpětnou vazbu. Cílem této zpětné vazby je mít představu o skutečném fungování ISMS. Vedení organizace následně přezkoumá, zda je realizace ISMS v souladu s obecnými potřebami organizace. Důležité je především prověřit účinnost prosazení zavedených opatření. Dále je potřeba ověřit jak odpovědné osoby ze strany jejich nadřízených, tak fungování ISMS pomocí interních auditů. Posledním krokem této fáze je pak příprava zprávy o stavu ISMS a následné přehodnocení ISMS vedením organizace [4].

Kontroly ISMS

Všechny osoby na všech manažerských úrovních, které mají odpovědnost za fungování ISMS, musejí provádět kontroly a dohlížet na to, aby byly splněny všechny bezpečnostní požadavky. Navíc by měly kontrolovat, zda daná bezpečnostní opatření splňují předpokládaná očekávání. Mezi kontrolní činnosti patří následující [4]:

- detekce chyb,
- detekce bezpečnostních incidentů,
- detekce úspěšných i neúspěšných pokusů o narušení bezpečnosti,
- sledování bezpečnostních událostí,
- vyhodnocení měření účinnosti ISMS a zavedených bezpečnostních opatření.

Interní audity

Cílem auditu je stanovit rozsah, v jakém jsou splněna předem stanovená kritéria. Interní audit na rozdíl od kontroly zajišťuje nezávislý pohled na fungování ISMS a měl by rozložit své zaměření rovnoměrně na celý rozsah ISMS. Audit by měl vždy prověřit jak dodržování procesních pravidel, tak fungování jednotlivých bezpečnostních opatření [4].

Přezkoumání ISMS

Na základě podnětů a připomínek by mělo pravidelně (min. jednou za rok) docházet k přezkoumání ISMS ze strany vedení organizace. Při přezkoumání je důležité zaměřit se především na [4]:

- výsledky provedených auditů,
- zpětnou vazbu od zainteresovaných uživatelů a třetích stran,
- změny, které ovlivňují ISMS,
- výsledky měření účinnosti ISMS,
- slabiny a hrozby, které jsme mohli podcenit,
- získaná doporučení pro další zlepšování ISMS.

Po přezkoumání je vhodné sestavit zprávu o stavu ISMS, ve které budou uvedeny jak vlastnosti, které již fungují správně, tak vlastnosti, které je potřeba zlepšit. Na základě této zprávy pak můžeme definovat cíle pro další období a připravit potřebné zdroje pro naplnění uvedených cílů [4].

2.2.5 Údržba a zlepšování

V poslední etapě by mělo docházet ke sběru podnětů k možným zlepšením ISMS a tato zlepšení zavádět a také by měla být provedena odpovídající opatření k nápravě i preventivní opatření k odstranění všech nedostatků. Je proto nutné zavést zpětnou vazbu, která bude získávat podněty pro efektivnější fungování a zároveň odhalovat nedostatky. Ke zlepšování ISMS mohou značnou měrou přispět i zkušenosti a podněty od řadových pracovníků. Je však vždy nutné u těchto požadavků zvážit dopady a důsledky pro organizaci i spolu s možnými riziky. Při odstraňování nedostatků, ať už opatřením k nápravě nebo preventivním opatřením, je důležité objasnit příčiny

nedostatku a snažit se předejít jeho opakování. Častou příčinou je přitom nedostatečná znalost požadavků, které ISMS vyžaduje [4].

2.3 ITIL a metodiky COBIT

V této kapitole budou zmíněny celosvětově rozšířená metodika COBIT a knihovna ITIL, které se také využívají v oblasti řízení bezpečnosti.

2.3.1 ITIL

Information Technology Infrastructure Library (ITIL) je v podstatě mezinárodní standard pro oblast řízení IT služeb. Je to knihovna praktických zkušeností, které řeší jak dodávat kvalitní IT služby za přiměřené náklady. Není to tedy norma ani metodika, její obsah tvoří doporučení a osvědčené postupy. ITIL obsahuje soubor knih, ve kterých jsou popsány způsoby procesního řízení služeb a také infrastruktury IT, jejímž prostřednictvím jsou služby poskytovány. Výstupy všech dodavatelů služeb v daném odvětví jsou kompatibilní a univerzálně použitelné. Knihovnu ITIL spravuje organizace Office of Government Commerce (OGC) a v roce 2007 vydala již třetí verzi této knihovny [2] [4].

ITIL je rámec pro návrh procesů IT Service Managementu (ITSM - Řízení služeb informačních technologií). ITIL obsahuje za prvé definování procesů potřebných pro zajištění ITSM a za druhé zásady pro implementaci procesů ITSM. Knihovna ITIL tedy neřeší [2]:

- jak bude konkrétně vypadat organizační struktura,
- konkrétní pracovní pozice pro dané role,
- projektovou metodiku implementace ITSM,
- ani jak budou vypadat pracovní postupy a co bude jejich obsahem.

2.3.2 COBIT

Protože je systém řízení IT většinou velice složitý, je potřeba jej strukturovat takovým způsobem, aby mu rozuměli řídící pracovníci i uživatelé bez hlubších znalostí IT. A právě o to se snaží metodika COBIT (Control Objectives for Information and related

Technology), která umožňuje pracovníkům definovat vhodná objektivní kritéria pro posouzení úspěšnosti daných oblastí řízení IT. Cílem této metodiky je využít informace a nasadit informační a komunikační technologie (ICT) tak, aby podporovaly dlouhodobý rozvoj organizace a snižovaly rizika, která přímo souvisí s používáním ICT. Metodika vychází z nejlepších zkušeností a ze všeobecně uznávaných praktik řízení ICT [2].

Koncepci metodiky nejlépe reprezentuje tzv. COBIT kostka, která na svých třech osách znázorňuje prolínání strategických požadavků (cílů organizace), zdrojů informačních technologií a IT procesů. Zdroje IT jsou řízeny procesy způsobem, kterým organizace nejlépe dosáhne daných cílů (strategických požadavků). Mezi tyto cíle (požadavky) patří účelnost, účinnosti, důvěryhodnost, integrita, dostupnost a spolehlivost. Mezi zdroje IT řadíme aplikace, informace, infrastrukturu a lidi. A samotné IT procesy rozlišujeme na úrovni domény, procesů a cílů kontrol/aktivit [4].

2.4 Normy řady ISO/IEC 27000

V této kapitole budou popsány některé normy řady ISO/IEC 27000, které obsahují doporučení pro zavedení systému řízení bezpečnosti informací. Řada norem ISMS má souhrnný název *Informační technologie - Bezpečnostní techniky* a jejím úkolem je pomoct organizacím všech typů a velikostí zavést a provozovat ISMS. Obsahuje především následující normy:

ČSN ISO/IEC 27000 Systémy řízení bezpečnosti informací - Přehled a slovník

V této normě je uveden přehled systémů řízení bezpečnosti informací a také související termíny a definice. Nejedná se však o všechny termíny a definice, ale pouze o ty, které jsou obecně použity v rodině norem ISMS. Norma vysvětluje co je to ISMS, k čemu se využívá a proč je důležitý. V současnosti je platná verze této české normy z roku 2014, která byla přeložena z mezinárodní normy vydané téhož roku [2].

ČSN ISO/IEC 27001 Systémy řízení bezpečnosti informací - Požadavky

Tato norma specifikuje požadavky na ustavení, implementování, udržování, neustálé zlepšování a případnou certifikaci zdokumentovaného ISMS v rámci kontextu

organizace. Jsou zde zahrnuty požadavky na posuzování a ošetření rizik, tedy na výběr a zavedení bezpečnostních opatření. Pro dosáhnutí shody s touto normou, musí být splněny všechny požadavky. V příloze jsou stanoveny cíle opatření a jednotlivá opatření, které jsou odvozeny a propojeny s těmi, které jsou v normě ISO/IEC 27002. Nejnovější vydání normy 27001 je z roku 2014, resp. její mezinárodní předlohy z roku 2013, která nahradila mezinárodní normu ISO/IEC 27001:2005, jenž byla přejata z britské normy BS 7799-2 v říjnu 2005 [2] [6].

ČSN ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací

Norma se dočkala nového vydání v roce 2013, resp. jejího českého překladu v roce 2014. Norma nyní obsahuje 114 strukturovaných oblastí doporučení rozdělených do 14 kapitol tykajících se opatření bezpečnosti, které obsahují 35 hlavních kategorií bezpečnosti. Dohromady je zde obsaženo několik tisíc přímých i odvozených bezpečnostních opatření, které slouží k dosažení daných podnikatelských cílů. Lze tak rychle vymezit oblasti, které jsou nedostatečně zabezpečeny, zjistit celkový stav bezpečnosti v organizaci a následně navrhnout odpovídající opatření na zlepšení stavu bezpečnosti [2].

ČSN ISO/IEC 27003 Směrnice pro implementaci systému řízení bezpečnosti informací

Tato mezinárodní norma byla vydána roku 2010 a do češtiny přeložena v roce 2011. Jejím obsahem jsou doporučení pro úspěšný návrh a implementaci ISMS v souladu s požadavky normy ISO/IEC 27001. Norma popisuje proces plánování implementace ISMS, na jehož konci je jako výsledek finální plán, který slouží pro realizování projektu implementace ISMS. Celý proces plánování implementace ISMS je rozdělen na pět etap [2]:

- získání souhlasu vedení organizace se zahájením projektu ISMS,
- definování rozsahu, hranic a politiky ISMS,
- provedení analýzy požadavků bezpečnosti informací,
- provedení hodnocení rizik a plánování zvládání rizik,
- návrh ISMS.

Na konci poslední etapy je výstupem právě konkrétní finální plán pro implementaci projektu ISMS, který obsahuje návrh bezpečnostních opatření, které jsou v souladu s normou ISO/IEC 27001 [2].

ČSN ISO/IEC 27004 Řízení bezpečnosti informací - Měření

Pro měření účinnosti zavedeného ISMS a účinnosti zavedených bezpečnostních opatření je potřeba zavést určité metriky. Právě tato norma obsahuje doporučení pro vývoj a používání těchto metrik. Program měření bezpečnosti informací, jehož úkolem je právě implementace těchto doporučení, obsahuje procesy pro rozvoj metrik a měření, analýzu dat a hlášení výsledků měření. České vydání této normy z roku 2011 je překladem mezinárodní normy z roku 2009 [2].

ČSN ISO/IEC 27005 Řízení rizik bezpečnosti informací

Norma je určená převážně pro manažery a pracovníky, kteří jsou v organizaci odpovědní za řízení rizik bezpečnosti informací. V normě jsou doporučení právě pro řízení těchto rizik. Norma je v souladu s konceptem normy ISO/IEC 27001 a je strukturovaná pro podporu implementace informační bezpečnosti založené na přístupu řízení rizik. Záleží na každé organizaci, jaký zvolí přístup k řízení rizik bezpečnosti informací, tato norma neposkytuje konkrétní metodiky. Poslední platná verze normy je z roku 2011 a její český překlad z roku 2013 [2].

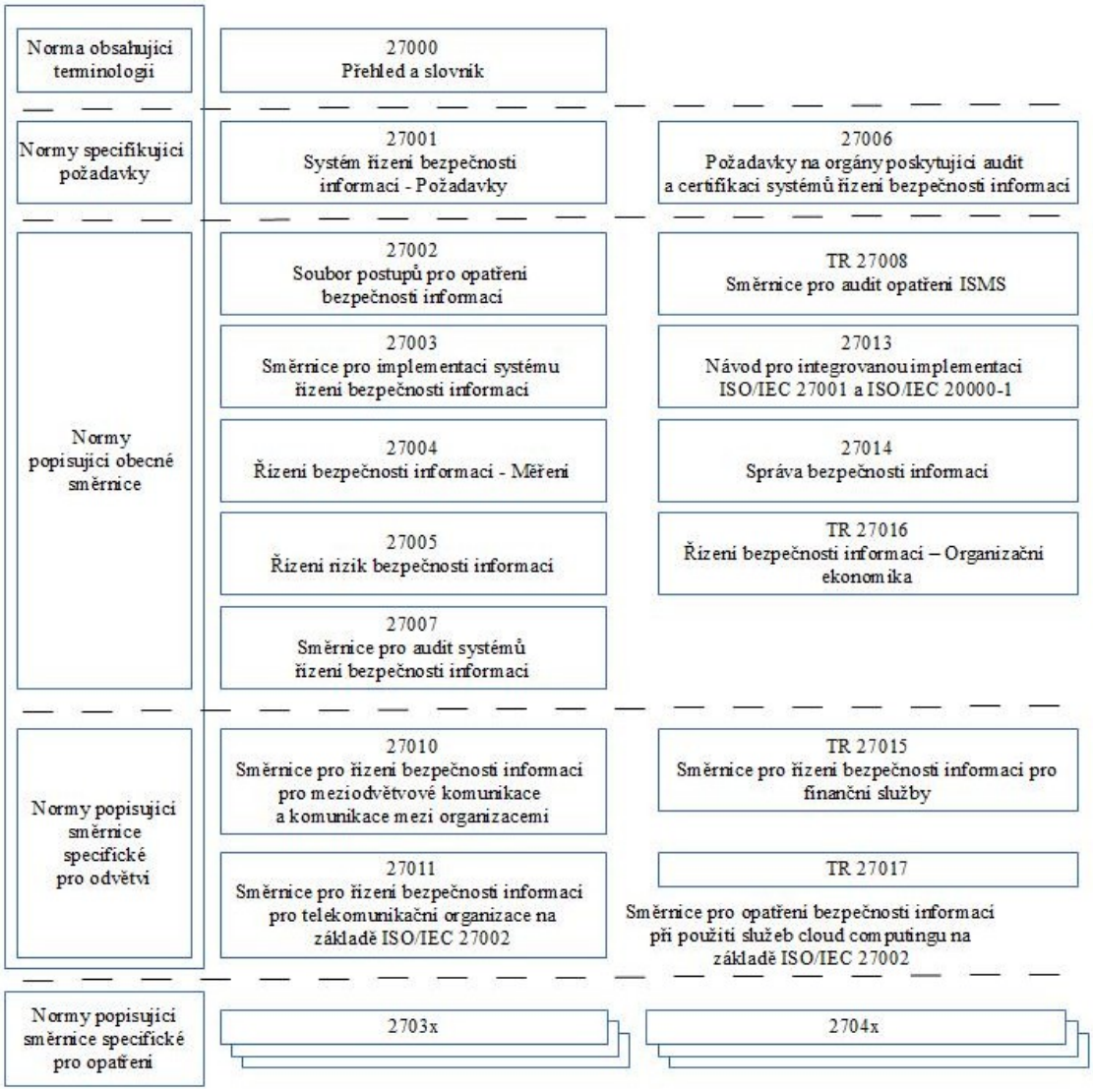
ČSN ISO/IEC 27006 Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Norma podporuje proces akreditace pro orgány, které poskytují audit a certifikaci ISMS. Obsahuje především požadavky a poskytuje doporučení pro tyto orgány. Platná verze mezinárodní normy je z roku 2011 a českého překladu z roku 2013 [2].

ČSN ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací

Tato norma čerpá z normy ČSN EN ISO/IEC 19011 Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu. Obsahuje doporučení pro řízení programu auditů ISMS podle ISO/IEC 27001, pro provádění

auditů a pro odbornou způsobilost auditorů ISMS. Platná verze mezinárodní normy je z roku 2011 a českého překladu z roku 2013 [2].



Obrázek 5: Vztahy mezi normami řady ISO/IEC 27000 (upraveno dle [6])

2.5 Právní rámec bezpečnosti informací v ČR

V této kapitole budou zmíněny některé důležité zákony České republiky, které se týkají bezpečnosti informací a je potřeba je brát v úvahu při zavádění systému řízení bezpečnosti informací (ISMS). Převážně zde bude zmíněn nový zákon o kybernetické bezpečnosti, který vchází v účinnost od začátku roku 2015.

2.5.1 Zákon o svobodném přístupu k informacím

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím ukládá organizacím i orgánům povinnost poskytnout a zpřístupnit informace o veškeré své činnosti. Tento zákon určuje způsob poskytování informací, vyřizování žádostí, podávání žádostí a také stanovuje potřebné lhůty. Tento zákon neupravuje nakládání s informacemi, které jsou předmětem jiných zákonů, jako např. zákon upravující ochranu známek, nebo zákon o vynálezech apod [4].

2.5.2 Zákon o elektronickém podpisu

Zákon č. 227/2000 Sb., o elektronickém podpisu, který byl upraven zákonem č. 101/2010 Sb. a později zákonem č. 167/2012 Sb., upravuje používání elektronického podpisu, elektronické značky, ale také např. poskytování certifikačních služeb. Zákon dále stanovuje sankce při porušení tohoto zákona. Od roku 2010 je také povinnost vést a zveřejňovat i dálkovým přístupem seznam důvěryhodných certifikačních služeb [4].

2.5.3 Zákon o archivnictví a spisové službě

Zákon č. 499/2004 Sb., o archivnictví a spisové službě upravuje především výběr, evidenci, kategorizaci a ochranu archiválií, dále práva a povinnosti vlastníků, držitelů a správců archiválií, a také zpracování osobních údajů pro účely archivnictví. Vyhláškou č. 645/2004 Sb. byly vymezeny pojmy dokument a archiválie. Dokument je jakýkoli písemný, obrazový, zvukový, elektronický nebo jiný záznam (digitální či analogový), který vznikl z činnosti původce. A jako archiválie se chápe záznam, který byl vybrán k trvalému uchování. Může to být však i pečetidlo, razítko apod. [4].

2.5.4 Zákon o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů v souladu s naplněním práva na ochranu před neoprávněným zasahováním do soukromí a zneužíváním osobních údajů upravuje práva i povinnosti při zpracování osobních údajů. Zákon také stanovuje podmínky, za kterých je možno předat osobní údaje jiným státům [4].

2.5.5 Zákon o ochraně utajovaných informací

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti stanovuje zásady pro určení zda se jedná o utajované informace. Dále definuje podmínky pro přístup k utajovaným informacím a požadavky na jejich ochranu. Zákon také upravuje zásady pro stanovení citlivých činností a vymezuje činnost Národního bezpečnostního úřadu (NBÚ) [4].

2.5.6 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti s účinností od 1.1.2015 vznikl mimo jiné také jako reakce na směrnici Evropské unie, podle které by členské státy EU měly zvyšovat svou schopnost odolávat případným útokům na kybernetické úrovni. Díky novému zákonu by tak Česká republika měla být odolnější vůči případným útokům na důležité počítačové systémy, na kterých jsou závislé obory podstatné pro bezpečný a bezchybný chod státu. Tím je myšlena např. doprava, energetika nebo ekonomika jako celek. Útoků hackerů stále přibývá nejen v ČR, ale po celém světě, kde se každoročně odhadují škody v řádech stovek milionů dolarů. Dle zákona by mělo dojít ke sjednocení elektronické komunikace a to jak ve státní, tak částečně i v soukromé sféře. Také u osobních dat občanů uchovaných na úřadech nebo v bankách by mělo dojít ke zvýšení bezpečnosti. Zákon by měl také podporovat české dodavatele ICT technologií, zatraktivnit tuzemské prostředí pro zahraniční investice a tím tak pomoci samotné české ekonomice [7].

V českých firmách chybí v přístupu k bezpečnosti náležitá systematičnost a organizovanost. To ohrožuje bezpečnost občanů i jejich dat a jelikož v bezpečnosti jde převážně o pokrytí rizik, klade nový zákon důraz právě na systém řízení rizik. Zákon se hodně podobá standardu pro systém řízení bezpečnosti informací ISO/IEC 27001. Společnosti, které úspěšně projdou certifikací aktuálně platné verze ISO/IEC 27002, budou ke splnění zákona velice blízko [8].

Se samotným zákonem souvisí ještě prováděcí předpisy, které definují kritéria pro určení, zda daný systém patří do tzv. kritické informační infrastruktury. Celkem se jedná o tyto tři prováděcí předpisy [9]:

- vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti),
- vyhláška o významných informačních systémech - vyhláška, kterou se stanoví významné informační systémy a jejich určující kritéria,
- novela nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické informační infrastruktury.

První vyhláška udává, jak by přesně měly dané subjekty postupovat, avšak už zde nejsou uvedeny kritéria pro určení těchto subjektů. To je stručně popsáno v zákonu, ale konkrétní kritéria a definice jsou zmíněna právě v druhém a třetím prováděcím předpisu, zmíněných výše. Dle zákona se tedy jedná o [9]:

- správce významných informačních systémů,
- správce informačních systémů kritické informační infrastruktury,
- správce komunikačních systémů kritické informační infrastruktury.

Kromě kritérií pro stanovení významného informačního systému, jsou ve vyhlášce stanoveny i některé významné IS přímo. V každém případě se však jedná jen o systémy z veřejné správy, tedy systémy jejichž správcem je orgán veřejné moci a narušením bezpečnosti informací by mohl být omezen či ohrožen výkon působnosti tohoto orgánu [9].

Prvky kritické informační infrastruktury, tedy informační systémy i komunikační systémy, mohou být systémy z veřejné správy, ale i z privátního sektoru. Nařízení vlády však neobsahuje seznam konkrétních systémů, které patří do kritické infrastruktury. Jsou zde uvedeny pouze kritéria pro určení takovýchto prvků. Pro informační systémy je kritérium pro zařazení do kritické informační infrastruktury, aby počet uživatelů, o kterých jsou uchovávány osobní údaje, byl vyšší než 300 000. U komunikačních systémů se jedná zase o připojení s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s. A např. u zdravotnických zařízení je kritériem pro zařazení do kritické informační infrastruktury, aby počet akutních lůžek byl vyšší než 2 500 lůžek [9].

Pro zajištění kybernetické bezpečnosti jsou v zákoně rozděleny požadavky na technická a organizační opatření. A právě na organizační opatření, která jsou ve společnostech často opomíjena, se budou muset dané společnosti zaměřit. Hlavním organizačním opatřením je zavedení systému řízení bezpečnosti informací, u kterého je důležitá převážně podpora ze strany vedení organizace [8].

Důležitým opatřením je i bezpečnost lidských zdrojů, která v sobě zahrnuje školení zaměstnanců. Jednorázové krátké proškolení již však nestačí, neustále přibývají nové hrozby a je nutné zavést systematické a neustálé vzdělávání. Pro efektivní snížení nákladů na pokrytí rizik, je potřeba předávat znalosti z oblasti bezpečnosti takovým způsobem, aby byly srozumitelné a zaměstnanci chápali jejich důležitost [8].

Jak již bylo zmíněno, bezpečnostní opatření se dělí na organizační a technická [10]:

- Mezi organizační opatření patří převážně:
  - systém řízení bezpečnosti informací,
  - řízení rizik,
  - bezpečnostní politika,
  - organizační bezpečnost,
  - stanovení bezpečnostních požadavků pro dodavatele,
  - řízení aktiv,
  - bezpečnost lidských zdrojů.
- Mezi technická opatření, patří převážně:
  - fyzická bezpečnost,
  - nástroje pro:
    - ochranu integrity komunikačních sítí,
    - ověřování identity uživatelů,
    - řízení přístupových oprávnění,
    - ochranu před škodlivým kódem.

Nový zákon se vztahuje na osoby a orgány veřejné moci v oblasti kybernetické bezpečnosti. Nevztahuje se však na informační či komunikační systémy, které spravují utajované informace. Orgány a osoby, které spadají do oblasti kybernetické bezpečnosti, jsou povinny zavést a provádět bezpečnostní opatření pro daný systém kritické informační infrastruktury a vést o něm bezpečnostní dokumentaci. Stejně tak jsou povinni zohlednit bezpečnostní požadavky při výběru dodavatelů takovýchto systémů.

A také hlásit kybernetické bezpečnostní incidenty národnímu bezpečnostnímu úřadu. Bezpečnostní incident je zde myšleno narušení bezpečnosti informací v IS nebo bezpečnosti služeb [10].

Ačkoli se nyní zákon vtahuje převážně na velké společnosti a orgány veřejné moci, dřív nebo později budou o splnění zákona usilovat i menší soukromé společnosti, a to převážně ty, které se společnostmi spadajícími do oblasti kybernetické bezpečnosti, pracují v úzkém vztahu a vyměňují si navzájem informace. Společnosti, které nebudou zákon splňovat, budou mít nevýhodu při výběrových řízeních poskytovaných právě organizacemi, které zákon splňovat musejí.

2.6 Instituce zabývající se bezpečnosti informací

V České republice i v zahraničí působí několik úřadů a institucí, které řeší otázky ohledně bezpečnosti informačních systémů a ICT technologií. Tyto instituce vznikají právě na základě zákonů o bezpečnosti informací a mají za úkol stanovit bezpečnostní požadavky. Vydávají proto vyhlášky, směrnice, normy, standardy a další dokumenty pro vybrané oblasti bezpečnosti informací [4].

2.6.1 Národní instituce

Úřad pro ochranu osobních údajů (ÚOOÚ)

Úřad pro ochranu osobních údajů je nezávislý orgán, který se stará o dodržování povinností stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů. Hlavním úkolem je ochrana soukromí občanů proti zneužívání jejich dat, které zpracovávají soukromé či státní organizace. Daný orgán musí tedy řešit jakékoliv stížnosti občanů ohledně porušení tohoto zákona a vést veřejný registr povolených zpracování osobních údajů. Dále také kontroluje shromažďování osobních údajů a nabízí konzultace týkající se ochrany osobních údajů [4].

Národní bezpečnostní úřad (NBÚ)

Národní bezpečnostní úřad má za úkol vykonávat státní správu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti dle zákona č. 412/2005 Sb. Na

základě členství ČR v Evropské Unii, Organizaci Severoatlantické smlouvy a z dalších mezinárodních smluv vyplývají závazky i v oblasti ochrany utajovaných informací. A právě NBÚ má povinnost plnit úkoly v této oblasti. Má také za úkol rozhodovat o poskytování utajovaných informací v mezinárodním styku. Tento úřad dále vyvíjí a schvaluje národní algoritmy pro šifrování a zajišťuje výzkum a vývoj prostředků pro kryptografii [4].

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ)
Tento úřad se stará o zabezpečení úkolů, které vyplývají ze zákonů ČR upravující technickou normalizaci, metrologii a státní zkušebnictví. Stejně tak zabezpečuje úkoly v oblasti technických norem a předpisů, které ČR uplatňuje na základě členství v EU. Dále tento úřad zajišťuje tvorbu, vydávání, zveřejňování a šíření českých technických norem [4].

2.6.2 Mezinárodní instituce

Evropská komise pro normalizaci (CEN)
CEN je nezisková technická organizace založena roku 1961. Pomáhá k dosažení cílů EU při budování evropského ekonomického prostoru, přičemž se řídí belgickými zákony. Hlavním cílem této organizace je tvorba technických norem v oblasti bezpečnosti pracovníků a zákazníků, ochrany životního prostředí, nebo i vědy a výzkumu [4].

Institute of Electrical and Electronics Engineers (IEEE)
Tato celosvětová nezisková organizace byla původně institucí inženýrů elektroniky a elektrotechniky. Dnes je její rozsah působnosti v mnohem větším množství oblastí rozvoje technologií. Co se týče norem, zaměřuje se především na normy v oblasti definice síťových protokolů, označovaných identifikátorem 802 [4].

International Electrotechnical Commission (IEC)
IEC byla založena v roce 1906 se sídlem v Ženevě. Zabývá se vydáváním mezinárodních norem v oblasti elektrotechniky a podobných oblastí včetně IS/ICT [4].

Mezinárodní organizace pro normalizaci (ISO)

I tato mezinárodní organizaci má sídlo v Ženevě a byla založena roku 1947. Jejím úkolem je tvorba a aktualizace mezinárodních norem ISO a dalších dokumentů, jako jsou technické zprávy, technické specifikace apod. Je to světová federace národních organizací pro normalizaci, která má již více než sto členů. Všichni členové musí patřičně informovat zainteresované strany ve své zemi o všech nových normalizačních aktivitách. Jejich povinností je také finančně podporovat činnost ISO [4].

3 Analýza současného stavu

Tato kapitola obsahuje základní informace o společnosti, jejích zaměstnancích, vlastněném HW a SW a také je zde shrnut současný stav bezpečnosti informací organizace. Dané informace byly získány komunikací s majiteli společnosti i se zaměstnanci.

3.1 Informace o společnosti

Analyzovaná společnost působí jako účetní a daňová kancelář. Byla založena v roce 1992. Dnes nabízí své služby pro ziskové i neziskové organizace. Poskytuje nejen daňové a účetní poradenství, ale také zpracování daňových přiznání, kontroly účetnictví, vedení podvojného účetnictví a daňové evidence, nebo i vypracování ekonomických výhledů potřebných pro žádost o úvěr či dotaci.

Společnost sídlí v prostorách rodinného domu, kde má v přízemí vyhrazeny dvě místnosti jako kancelářské prostory a v prvním patře jednu místnost jako archiv dokumentů. Lokalita rodinného domu byla těsně před začátkem stavby změněna z důvodu záplav v původně vybrané oblasti. Dům je tedy postaven na vyvýšeném místě, kde k záplavám nedochází. Majitelé při nedávné přestavbě nechali vybudovat do domu druhé vchodové dveře, které vedou přímo do kancelářských prostor. Klienti tedy již neprocházejí skrz soukromou obytnou část domu, ale vstupují rovnou do prostor firmy.

Firma zaměstnává osm pracovníků a má k dispozici čtyři osobní počítače a čtyři notebooky, které zaměstnanci denně používají. V první místnosti jsou umístěny osobní počítače a router, ke kterému jsou připojeny standardním UTP kabelem. Notebooky jsou k routeru připojeny pomocí Wi-Fi sítě. Společně tak vytváří vnitřní firemní síť. Všechny počítače i notebooky mají nainstalovaný operační systém Windows 7 a jsou zabezpečeny heslem. Na většině počítačů jsou nainstalovány účetní programy, kancelářské balíky Microsoft Office a samozřejmě je na každém počítači antivirus.

Připojení k internetu je zpřístupněno přes ADSL linku a majitelé mají k dispozici navíc ještě osobní připojení k internetu od Wi-Fi poskytovatele, které je možné použít při výpadku primárního připojení. Společnost nevlastní žádný server ani informační systém v podobě softwarové aplikace. Webové stránky společnosti jsou umístěny na serveru od externího poskytovatele webhostingu i samotné domény.

3.2 Současný stav bezpečnosti

3.2.1 Fyzická bezpečnost

Fyzický přístup do prostor firmy je v prvé řadě zabezpečen oplocením kolem pozemku. Brána k plotu je vždy odemčena kvůli snazšímu přístupu klientů. Majitelé však vlastní psa, který přispívá k vyšší bezpečnosti už jen tím, že upozorní na jakoukoli cizí osobu v prostorách kolem domu. Přístup do domu, resp. do kanceláří firmy je možný pouze přes vchodové dveře, které nelze z vnější strany otevřít jinak než klíčem. Do kanceláří tedy není umožněn volný přístup pro klienty ani pro samotné zaměstnance, kterým ráno umožňují vstup do domu sami majitelé. Vzhledem k malým prostorám firmy tak mají majitelé neustálý přehled o přítomnosti všech osob v objektu. Dokumenty i média obsahující důležité a důvěrné informace jsou umístěny v prvním patře domu, kam mají přístup pouze sami majitelé.

Zařízení jako jsou stolní počítače a notebooky jsou bezpečně umístěny tak, aby se minimalizovalo riziko fyzického poškození (např. vodou apod.) i riziko neoprávněného sledování při práci osobami, které ve firmě nepracují (klienti apod.). Stejně tak je zajištěno bezpečné vedení kabeláže, aby nedošlo k poškození. Komunikační a napájecí kabely jsou od sebe odděleny tak, aby nedocházelo k rušení. V případě požáru jsou k dispozici hasící přístroje jak v prostorách kanceláří, tak v prvním patře, kde je archiv dokumentů a jiných médií.

3.2.2 Bezpečnost provozu a komunikací

Informace, které společnost zpracovává, jsou chráněny před malwerem a to dostatečně bezpečným antivirovým softwarem AVG Internet Security, který blokuje viry, spyware a jiný malware, obsahuje navíc i firewall a kontroluje jak data v počítači, tak příchozí soubory z e-mailu či z webu. Pro vyšší bezpečnost je zavedena politika, která zakazuje instalovat neautorizovaný software a přistupovat na neznámé a nebezpečné webové stránky.

Pro ochranu informací v sítích je fyzické připojení do vnitřní sítě chráněno umístěním routeru na bezpečném místě, kam nemá veřejnost přístup. Bezdrátové Wi-Fi připojení do sítě je chráněno zabezpečením WPA2 a je nastaveno silné heslo, které

brání připojení neoprávněných osob k dané síti. Samozřejmě k bezpečnosti komunikací přispívá i zabezpečení každého připojeného počítače pomocí antiviru a firewallu.

3.2.3 Bezpečnost lidských zdrojů

Společnost má definovaná pravidla pro sepisování pracovních smluv s novými zaměstnanci. Tedy postupy podle, kterých mají být zaměstnanci seznámeni s podmínkami pracovního vztahu, se svými právy a povinnostmi, které zahrnují mimo jiné i dohodu o mlčenlivosti, která řeší únik informací mimo organizaci. Při nástupu do pracovního poměru tedy podepisují všichni zaměstnanci dohodu o zachování mlčenlivosti, což je velice důležité, protože mohou při práci přijít do styku s citlivými a důvěrnými informacemi, které se týkají společnosti, nebo i samotných klientů.

Stejně tak má společnost definovaná pravidla pro ukončení pracovního vztahu, která v sobě zahrnují povinnost navrátit všechny prostředky, odebrání přístupových práv apod. Samozřejmostí je i to, že dohodou o mlčenlivost jsou zaměstnanci vázáni i po skončení pracovního poměru. Stejně tak jsou stále platné i některé další odpovědnosti a povinnosti již bývalých zaměstnanců.

3.2.4 Řízení přístupu a ochrana osobních údajů

Pro zabránění neoprávněného přístupu k informacím jsou všechny počítače chráněny heslem. Každý zaměstnanec tak má přístup pouze ke svému účtu. Také jsou zavedeny postupy pro vytvoření nového uživatelského účtu pro nového zaměstnance a odstranění uživatelského účtu při zrušení pracovního poměru. Společnost nepoužívá žádné další sdílené aplikace ani informační systém v podobě softwaru, ke kterým by bylo potřeba spravovat uživatelský přístup. Nemá tedy zavedeny žádné další postupy ani procesy správy privilegovaných přístupových práv, či skupinových autentizačních informací apod.

Osobní údaje všech zaměstnanců společnost bezpečně uchovává a zajišťuje tak jejich ochranu v souladu se zákonem o ochraně osobních údajů. Má také vypracovanou politiku pro ochranu osobních údajů, se kterou je každý zaměstnanec seznámen při nástupu do zaměstnání a má tedy povinnost dodržovat organizační opatření definovaná touto politikou.

4 Vlastní návrhy řešení

Úkolem této kapitoly je navrhnout bezpečnostní opatření pro minimalizaci největších rizik. Nejprve je tedy nutné provést analýzu rizik. Je potřeba identifikovat aktiva společnosti a tato aktiva ohodnotit. Dalším krokem je identifikace hrozeb a stanovení pravděpodobností jejich výskytu. Následně se ohodnotí zranitelnost aktiv vůči hrozbám a vypočte míra rizika. Podle určených bezpečnostních rizik budou vybrána vhodná bezpečnostní opatření pro zajištění přiměřené bezpečnosti.

4.1 Analýza rizik

Prvním krokem analýzy je tedy identifikace aktiv. Tento seznam byl sestaven na základě komunikace s vedením společnosti. Další krok je ohodnocení aktiv podle dopadu na organizaci v důsledku porušení důvěrnosti, integrity a dostupnosti daného aktiva. Je použita stupnice hodnot od 1 do 5. Výsledná hodnota aktiva je pak vypočtena součtovým algoritmem:

Hodnota aktiva = (Dostupnost + Důvěrnost + Integrita) / 3

Popis dopadu	Hodnota aktiva
žádný dopad na organizaci	1
minimální dopad na organizaci	2
střední potíže i finanční ztráty	3
velké potíže i finanční ztráty	4
existenční potíže	5

Tabulka 1: Stupnice pro hodnocení aktiv

Skupina	Aktivum (A)
Data	Osobní údaje zaměstnanců
	Výkazy práce
	Zálohy dat
	Osobní údaje klientů
	Účetní doklady klientů – papírově
	Účetní doklady klientů – elektronicky
	Autentizační údaje
Hardware	Počítače
	Router
	Tiskárny
	Kabeláž
	Síťová infrastruktura
	Přenosná média
Software	Operační systém
	Účetní programy
Služby	Elektronická pošta
	Webové stránky
	Připojení k internetu
	Pevná linka

Tabulka 2: Identifikace aktiv

Skupina	Aktivum (A)	Důvěrnost	Integrita	Dostupnost	Hodnota aktiva
Data	Osobní údaje zaměstnanců	5	3	3	4
	Výkazy práce	3	3	2	3
	Zálohy dat	5	5	5	5
	Osobní údaje klientů	5	3	3	4
	Účetní doklady klientů – papírově	5	3	2	3
	Účetní doklady klientů – elektronicky	5	5	4	5
	Autentizační údaje	5	4	4	4
Hardware	Počítače	5	4	4	4
	Router	4	3	3	3
	Tiskárny	1	1	1	1
	Kabeláž	3	4	3	3
	Síťová infrastruktura	4	4	3	4
	Přenosná média	5	4	3	4
Software	Operační systém	4	4	4	4
	Účetní programy	5	3	3	4
Služby	Elektronická pošta	3	3	2	3
	Webové stránky	4	1	1	2
	Připojení k internetu	3	3	3	3
	Pevná linka	2	2	2	2

Tabulka 3: Ohodnocení aktiv

Další krok v analýze je identifikace hrozeb a stanovení pravděpodobnosti, s jakou mohou nastat. Stupnice má opět hodnoty od 1 do 5.

Popis	Hodnota
velmi malá pravděpodobnost	1
malá pravděpodobnost	2
střední pravděpodobnost	3
vysoká pravděpodobnost	4
velmi vysoká pravděpodobnost	5

Tabulka 4: Stupnice pravděpodobností hrozeb

Hrozba	Pravděpodobnost
Útok z vnějšku	2
Neoprávněný přístup do prostor firmy	1
Požár	1
Poškození vodou	1
Krádež zařízení	3
Krádež dokumentů	2
Porucha hardwaru	5
Počítačový virus	2
Výpadek internetu	4
Výpadek pevné linky	4
Výpadek elektrického proudu	4
Prozrazení autentizačních údajů	1
Chybné zaslání citlivých dat	3
Porušení mlčenlivosti zaměstnance	2
Nedostupnost webových stránek	3
Poškození zálohovacího média	4

Tabulka 5: Identifikace a ohodnocení hrozeb

Identifikované aktiva i hrozby jsou v dalším kroku promítnuty do matice zranitelnosti, která udává zranitelnost aktiva vůči dané hrozbě. Stejným způsobem je následně sestavena matice rizik, která obsahuje míry rizika pro kombinace aktiv a hrozeb. Pro výpočet míry rizika je použit následující vzorec: R = T * A * V, kde T je pravděpodobnost, A je aktivum a V je zranitelnost. Výsledné hodnoty jsou pak rozděleny do tří kategorií rizik, které jsou barevně rozlišeny:

Rozmezí	Popis
1 – 40	Nízká míra rizika
41 – 80	Střední míra rizika
81 – 125	Vysoká míra rizika

Tabulka 6: Ohodnocení míry rizika

Zranitelnost (V)	**Popis aktiva**	Osobní údaje zaměstnanců	Výkazy práce	Zálohy dat	Osobní údaje klientů	Účetní doklady klientů – papírově	Účetní doklady klientů – elektronicky	Autentizační údaje	Počítače	Router	Tiskárny	Kabeláž	Síťová infrastruktura	Přenosná média	Operační systém	Účetní programy	Elektronická pošta	Webové stránky	Připojení k internetu	Pevná linka
	Hodnota Aktiva (A)	4	3	5	4	3	5	4	4	3	1	3	4	4	4	4	3	2	3	2
Popis hrozby	**Pravděpodobnost (T)**																			
Útok z vnějšku	2	3	2	3	3	3	3													
Neoprávněný přístup do prostor firmy	1	2	2	5	3	5	4	3	4	2	1	2	3	3	2	3	3		4	2
Požár	1	3	2	5	3	5	4		5	3	1	2	3	2	2	3			4	4
Poškození vodou	1	2	1	4	3	5	4		5	2	1	2	3	2	2	2			3	3
Krádež zařízení	3	4	1	4	3		4		4	2	1	1	2	3	2	3	3		4	3
Krádež dokumentů	2	3			3	5														
Porucha hardwaru	5	3	2	4	4		4		4	3	1	2	3	3	2	2			3	3
Počítačový virus	2	4	2	3	3		3		3	2			3		3	3	3		4	
Výpadek internetu	4																		2	
Výpadek pevné linky	4																			3
Výpadek elektrického proudu	4	2	1	3	3		4		4	4	1	2	3		2	3	3		5	
Prozrazení autentizačních údajů	1	3	2	4	4		5	4	3						2	3	4			
Chybné zaslání citlivých dat	3	3			4		5													
Porušení mlčenlivosti zaměstnance	2	3			4	5	4													
Nedostupnost webových stránek	3																	4		
Poškození zálohovacího média	4	2		5	4		5							3						

Tabulka 7: Matice zranitelnosti

Riziko (R)	Popis aktiva	Osobní údaje zaměstnanců	Výkazy práce	Zálohy dat	Osobní údaje klientů	Účetní doklady klientů – papírově	Účetní doklady klientů – elektronicky	Autentizační údaje	Počítače	Router	Tiskárny	Kabeláž	Síťová infrastruktura	Přenosná média	Operační systém	Účetní programy	Elektronická pošta	Webové stránky	Připojení k internetu	Pevná linka
	Hodnota Aktiva (A)	4	3	5	4	3	5	4	4	3	1	3	4	4	4	4	3	2	3	2
Popis hrozby	**Pravděpodobnost (T)**																			
Útok z vnějšku	2	24	12	30	24	18	30	0	0	0	0	0	0	0	0	0	0	0	0	0
Neoprávněný přístup do prostor firmy	1	8	6	25	12	15	20	12	16	6	1	6	12	12	8	12	9	0	12	4
Požár	1	12	6	25	12	15	20	0	20	9	1	6	12	8	8	12	0	0	12	8
Poškození vodou	1	8	3	20	12	15	20	0	20	6	1	6	12	8	8	8	0	0	9	6
Krádež zařízení	3	48	9	60	36	0	60	0	48	18	3	9	24	36	24	36	27	0	36	18
Krádež dokumentů	2	24	0	0	24	30	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Porucha hardwaru	5	60	30	100	80	0	100	0	80	45	5	30	60	60	40	40	0	0	45	30
Počítačový virus	2	32	12	30	24	0	30	0	24	12	0	0	24	0	24	24	18	0	24	0
Výpadek internetu	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	0
Výpadek pevné linky	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24
Výpadek elektrického proudu	4	32	12	60	48	0	80	0	64	48	4	24	48	0	32	48	36	0	60	0
Prozrazení autentizačních údajů	1	12	6	20	16	0	25	16	12	0	0	0	0	0	8	12	12	0	0	0
Chybné zaslání citlivých dat	3	36	0	0	48	0	75	0	0	0	0	0	0	0	0	0	0	0	0	0
Porušení mlčenlivosti zaměstnance	2	24	0	0	32	30	40	0	0	0	0	0	0	0	0	0	0	0	0	0
Nedostupnost webových stránek	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	0	0
Poškození zálohovacího média	4	32	0	100	64	0	100	0	0	0	0	0	0	48	0	0	0	0	0	0

Tabulka 8: Matice rizik

4.2 Bezpečnostní opatření

Podle výsledků analýzy rizik jsou následně navržena bezpečnostní opatření, která jsou v souladu s přílohou A normy ČSN ISO/IEC 27001. Všechna doporučení jsou převzata ze souboru postupů pro opatření bezpečnosti informací normy ČSN ISO/IEC 27002 a z další literatury [4].

Byla vybrána ta opatření, která ještě nejsou zavedena a která minimalizují vysoká a střední bezpečnostní rizika. Tato opatření jsou v tabulce 9 označena jako „**zavést**“. Společnost prozatím neuvažuje o certifikaci ISMS, není tedy důležité zavádět všechna opatření. Pro dosažení přiměřené bezpečnosti, tak byla vybrána pouze podstatná opatření. U opatření, která jsou již ve společnosti zavedena, je uveden stav „zavedeno“. Tam, kde by byly náklady nepřiměřeně vysoké, nebo by přírůstek bezpečnosti nebyl významný, jsou tato opatření označena jako „*ignorovat*“. Stejně tak je tento stav uveden i u opatření, která nejsou pro danou společnost relevantní. Jedná se např. o opatření, která mají za úkol zajistit bezpečnost informací při vývoji informačních systémů. Společnost se však vývojem softwaru nezabývá.

A.5 Politiky bezpečnosti informací		
A.5.1 Směřování bezpečnosti informací vedením organizace		
A.5.1.1	Politiky pro bezpečnost informací	**zavést**
A.5.1.2	Přezkoumání politik pro bezpečnost informací	**zavést**
A.6 Organizace bezpečnosti informací		
A.6.1 Interní organizace		
A.6.1.1	Role a odpovědnosti bezpečnosti informací	**zavést**
A.6.1.2	Princip oddělení povinností	**zavést**
A.6.1.3	Kontakt s příslušnými orgány a autoritami	**zavést**
A.6.1.4	Kontakt se zájmovými skupinami	*ignorovat*
A.6.1.5	Bezpečnost informací v řízení projektů	*ignorovat*
A.6.2 Mobilní zařízení a práce na dálku		
A.6.2.1	Politika mobilních zařízení	**zavést**
A.6.2.2	Práce na dálku	*ignorovat*
A.7 Bezpečnost lidských zdrojů		
A.7.1 Před vznikem pracovního vztahu		
A.7.1.1	Prověřování	**zavést**
A.7.1.2	Podmínky pracovního vztahu	zavedeno
A.7.2 Během pracovního vztahu		
A.7.2.1	Odpovědnosti vedení organizace	**zavést**
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	**zavést**
A.7.2.3	Disciplinární řízení	**zavést**
A.7.3 Ukončení a změna pracovního vztahu		
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	zavedeno
A.8 Řízení aktiv		
A.8.1 Odpovědnost za aktiva		
A.8.1.1	Seznam aktiv	**zavést**
A.8.1.2	Vlastnictví aktiv	**zavést**
A.8.1.3	Přípustné použití aktiv	**zavést**
A.8.1.4	Navrácení aktiv	**zavést**
A.8.2 Klasifikace informací		
A.8.2.1	Klasifikace informací	**zavést**
A.8.2.2	Označování informací	**zavést**
A.8.2 3	Manipulace s aktivy	**zavést**
A.8.3 Manipulace s médii		
A.8.3.1	Správa výměnných médií	**zavést**
A.8.3.2	Likvidace médií	**zavést**
A.8.3.3	Přeprava fyzických médií	**zavést**
A.9 Řízení přístupu		
A.9.1 Požadavky organizace na řízení přístupu		
A.9.1.1	Politika řízení přístupu	**zavést**
A.9.1.2	Přístup k sítím a síťovým službám	*ignorovat*
A.9.2 Řízení přístupu uživatelů		

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	*ignorovat*
A.9.2.4	Správa tajných autentizačních informací uživatelů	*ignorovat*
A.9.2.5	Přezkoumání přístupových práv uživatelů	*ignorovat*
A.9.2.6	Odebrání nebo úprava přístupových práv	**zavést**
A.9.3 Odpovědnosti uživatelů		
A.9.3.1	Používání tajných autentizačních informací	**zavést**
A.9.4 Řízení přístupu k systémům a aplikacím		
A.9.4.1	Omezení přístupu k informacím	*ignorovat*
A.9.4.2	Bezpečné postupy přihlášení	*ignorovat*
A.9.4.3	Systém správy hesel	*ignorovat*
A.9.4.4	Použití privilegovaných programových nástrojů	*ignorovat*
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	*ignorovat*
A.10 Kryptografie		
A.10.1 Kryptografická opatření		
A.10.1.1	Politika pro použití kryptografických opatření	**zavést**
A.10.1.2	Správa klíčů	**zavést**
A.11 Fyzická bezpečnost a bezpečnost prostředí		
A.11.1 Bezpečné oblasti		
A.11.1.1	Fyzický bezpečnostní perimetr	zavedeno
A.11.1.2	Fyzické kontroly vstupu	zavedeno
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	zavedeno
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	zavedeno
A.11.1.5	Práce v bezpečných oblastech	*ignorovat*
A.11.1.8	Oblasti pro nakládku a vykládku	*ignorovat*
A.11.2 Zařízeni		
A.11.2.1	Umístění zařízení a jeho ochrana	zavedeno
A.11.2.2	Podpůrné služby	**zavést**
A.11.2.3	Bezpečnost kabelových rozvodů	zavedeno
A.11.2.4	Údržba zařízení	**zavést**
A.11.2.5	Přemístění aktiv	**zavést**
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	**zavést**
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 Provozní postupy a odpovědnosti		
A.12.1.1	Dokumentované provozní postupy	**zavést**
A.12.1.2	Řízení změn	**zavést**
A.12.1.3	Řízení kapacit	**zavést**
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	*ignorovat*
A.12.2 Ochrana proti malwaru		

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

A.15 Dodavatelské vztahy		
A.15.1 Bezpečnost informací v dodavatelských vztazích		
A.15.1.1	Politika bezpečnosti informaci pro dodavatelské vztahy	*ignorovat*
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	*ignorovat*
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	*ignorovat*
A.15.2 Řízení dodávek služeb dodavatelů		
A,15.2.1	Monitorování a přezkoumávání služeb dodavatelů	*ignorovat*
A.15.2.2	Řízení změn ve službách dodavatelů	*ignorovat*
A.16 Řízení incidentů bezpečnosti informací		
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování		
A.16.1.1	Odpovědnosti a postupy	**zavést**
A.16.1.2	Hlášení událostí bezpečnosti informací	**zavést**
A.16.1.3	Hlášení slabých míst bezpečnosti informací	**zavést**
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	**zavést**
A.16.1.5	Reakce na incidenty bezpečnosti informací	**zavést**
A.16.1.6	Ponaučeni z incidentů bezpečnosti informací	**zavést**
A.16.1.7	Shromažďování důkazů	**zavést**
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací		
A.17.1 Kontinuita bezpečnosti informací		
A.17.1.1	Plánování kontinuity bezpečnosti informací	*ignorovat*
A.17.1.2	Implementace kontinuity bezpečnost informací	*ignorovat*
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	*ignorovat*
A.17.2 Redundance		
A.17.2.1	Dostupnost vybavení pro zpracování informací	*ignorovat*
A.18 Soulad s požadavky		
A.18.1 Soulad s právními a smluvními požadavky		
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	**zavést**
A.18.1.2	Ochrana duševního vlastnictví	**zavést**
A.18.1.3	Ochrana záznamů	**zavést**
A.18.1.4	Soukromí a ochrana osobních údajů	zavedeno
A.18.1.5	Regulace kryptografických opatření	**zavést**
A.18.2 Přezkoumání bezpečnosti informací		
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	*ignorovat*
A.18.2.2	Shoda s bezpečnostními politikami a normami	*ignorovat*
A.18.2.3	Přezkoumání technické shody	*ignorovat*

Tabulka 9: Vybraná bezpečnostní opatření

4.2.1 Politiky bezpečnosti informací (A.5)

Úkolem těchto opatření je nejen zavést politiky pro bezpečnost informací, ale také jejich pravidelné přezkoumávání.

Politiky pro bezpečnost informací (A.5.1.1)

Úkolem je vypracovat sadu politik pro bezpečnost informací v souladu s danými zákony, předpisy a hlavně požadavky organizace. Je důležité, aby sadu politik schválil management organizace a aby s ní byli seznámeni všichni zaměstnanci. Pokyny pro vypracování těchto politik jsou rozebrány v následujících opatřeních. Na nejvyšší úrovni by však měla být definována „politika bezpečnosti informací". Tato politika musí definovat přístup organizace k řízení svých cílů v oblasti bezpečnosti informací. Vedení organizace by měla prostřednictvím tohoto dokumentu:

- definovat stanovené cíle a zdůraznit význam bezpečnosti informací,
- specifikovat a stručně vysvětlit bezpečnostní zásady, principy, omezení, požadavky, pravidla a postupy,
- přiřadit odpovědnosti a pravomoci pro řízení bezpečnosti informací,
- ubezpečit o svém zájmu neustále bezpečnost informací prohlubovat.

Vypracování politiky bezpečnosti informací: 8 hodin.

Přezkoumání politik pro bezpečnost informací (A.5.1.2)

Pro zajištění nepřetržité vhodnosti, přiměřenosti i efektivnosti stanovených politik je důležité v pravidelných intervalech tyto politiky přezkoumávat. Navrhuji alespoň jednou ročně. Každá politika musí mít vlastníka, který bude mít za přezkoumání odpovědnost. Každá revidovaná politika musí být opět schválena managementem.

Doba potřebná pro přezkoumání politik: 12 hodin.

4.2.2 Organizace bezpečnosti informací (A.6)

Pro bezpečnost informací v organizaci je důležité zavést rámec řízení její implementace a provozování. Následující opatření se zabývají odpovědnostmi a povinnostmi v oblasti bezpečnosti informací a také politikou používání mobilních zařízení.

Role a odpovědnosti bezpečnosti informací (A.6.1.1)

Za bezpečnost informací by měly být definovány a přiděleny odpovědnosti daným osobám. Odpovědnosti je důležité přidělit za ochranu aktiv, za provádění bezpečnostních postupů, za činnosti v oblasti řízení rizik a také za přijetí zbytkových rizik. Úkoly v oblasti bezpečnosti informací mohou být i delegovány na ostatní, odpovědný však zůstává ten, kdo úkol delegoval.

Princip oddělení povinností (A.6.1.2)

Povinnosti zaměstnanců a oblasti jejich působností je vhodné oddělit. Zabrání se tak neoprávněným či neúmyslným změnám nebo zneužití aktiv organizace.

Přidělení rolí a odpovědností a oddělení povinností: 8 hodin.

Kontakt s příslušnými orgány a autoritami (A.6.1.3)

Je důležité zavést postupy, které stanoví kdo a kdy by měl kontaktovat autority (jako např. orgány vymáhající právo apod.) a jak včas hlásit incidenty bezpečnosti informací. Je také vhodné udržovat kontakty s dalšími autoritami jako např. s dodavateli elektřiny, poskytovateli telekomunikačních služeb apod.

Vypracování postupů pro kontaktování autorit: 2 hodiny.

Politika mobilních zařízení (A.6.2.1)

Při používání mobilních zařízení musí být zajištěno, že nedojde k odcizení, zničení či ztrátě informací související s činností organizace. Převážně je třeba dávat pozor při používání těchto zařízení na veřejnosti. Mobilní zařízení by měla být fyzicky chráněna a měla by být omezena instalace softwaru. Data by měla být zálohována a také je vhodné mít možnost vzdáleně data vymazat nebo zařízení zablokovat. Zařízení, které obsahují citlivé informace, by neměly být nikdy ponechány bez dozoru (v hotelových pokojích apod.), měly by být bezpečně uzamčeny. Dále je nutné dodržovat bezpečnostní postupy při připojování k bezdrátovým sítím. Některé veřejné sítě mohou být špatně zabezpečeny a mohlo by dojít k odcizení či ztrátě informací při přenosu dat.

Vypracování politiky mobilních zařízení: 4 hodiny.

4.2.3 Bezpečnost lidských zdrojů (A.7)

Tato bezpečnostní opatření jsou důležitá pro řízení bezpečnosti z hlediska lidských zdrojů. Jde především o opatření, která je potřeba provést před vznikem i během pracovního vztahu a také při ukončení či změně pracovního vztahu.

Prověřování (A.7.1.1)

Prověřování nových zaměstnanců před vznikem pracovního vztahu je důležité pro zajištění přiměřené úrovně bezpečnosti. Pro prověřování těchto pracovníků je tedy nutné zavést postupy, které budou jak v souladu s příslušnými zákony, jako je např. ochrana osobních údajů, tak v souladu s etikou. Tyto postupy by měly zahrnovat především:

- ověření totožnosti podle dokladů,
- ověření dokladů (diplomů apod.) o dosaženém vzdělání,
- ověření bezúhonnosti podle výpisu z rejstříku trestů,
- získání uspokojivých osobních i profesních posudků.

Zavedení postupů pro prověřování nových zaměstnanců: 2 hodiny.

Odpovědnosti vedení organizace (A.7.2.1)

Během pracovního vztahu musí management zajistit, aby byli zaměstnanci i smluvní strany seznámeni s bezpečnostními pravidly, která jsou v souladu se zavedenými politikami a postupy organizace, a aby všichni tato pravidla dodržovali. Management musí politiku bezpečnosti informací podporovat a jít všem příkladem.

Ti, kteří si nejsou vědomi svých povinností a odpovědností v oblasti bezpečnosti informací, mohou organizaci způsobit velké škody. Stejně tak ti, kteří nejsou motivováni k dodržování těchto povinností, se stávají velice nespolehliví a způsobují spoustu bezpečnostních incidentů. Špatný management může způsobit opomíjení bezpečnosti, nebo i zneužití aktiv organizace.

Je tedy důležité, aby byli všichni informováni o svých rolích a odpovědnostech ještě před tím, než je jim vůbec povolen přístup k důvěrným informacím. K tomu, aby zaměstnanci odpovědně plnili politiku bezpečnosti informací, musí management tyto zaměstnance motivovat a musí zajistit dostatečnou úroveň povědomí o bezpečnosti informací tak, aby se zaměstnanci vhodně přizpůsobili podmínkám plynoucích z této

politiky. Podstatnou částí je i vytvoření anonymního kanálu, který mohou zaměstnanci využít pro ohlašování porušení bezpečnostních pravidel a postupů. Stejně tak může sloužit pro upozornění na protiprávní jednání.

Vypracování postupů pro seznámení zaměstnanců s bezpečnostními pravidly: 4 hodiny.

Povědomí, vzdělávání a školení bezpečnosti informací (A.7.2.2)

Ke zvyšování povědomí v oblasti bezpečnosti informací je potřeba pravidelně provádět vzdělávání a školení pracovníků. Mělo by být realizováno formou různých školení, seminářů, tréninků a jiných vzdělávacích aktivit. Počáteční školení a vzdělávání je důležité pro nové pracovníky, ale také pro ty, kteří např. přestupují na novou pozici.

Samotný program zvyšování povědomí bezpečnosti informaci by měl být v souladu s politikami a postupy organizace v oblasti bezpečnosti informací. Důležité je, aby se programu účastnili všichni zaměstnanci a to v pravidelných intervalech, a aby tak měli představu o cíli bezpečnosti informací a možných dopadech na organizaci. Program zvyšování povědomí musí brát ohled na jednotlivé role zaměstnanců a být v souladu s politikami organizace.

Vypracování programu zvyšování povědomí bezpečnosti informací: 12 hodin.

Pravidelné školení a zvyšování povědomí bezpečnosti informací: 10 hodin / ročně.

Disciplinární řízení (A.7.2.3)

Je důležité, aby existoval disciplinární proces pro podniknutí kroků v případě narušení bezpečnosti informací. Cílem je zjednat nápravu a vhodným způsobem upozornit na zjištěné prohřešky. Před samotným procesem je potřeba ověřit, že opravdu došlo k narušení bezpečnosti informací. Podniknuté kroky v disciplinárním procesu by měly brát v úvahu povahu a závažnost narušení bezpečnosti, zda jde o první přestupek nebo opakovaný a také to, jestli byl daný zaměstnanec řádně vyškolen. Jako řešení lze využít slovní napomenutí nebo výtku a u závažných problémů finanční sankce, ukončení pracovního poměru nebo i soudní spor. Disciplinární proces by měl také sloužit jako odstrašující prostředek odrazující od narušení bezpečnosti informací.

Vypracování postupů disciplinárního procesu: 6 hodin.

4.2.4 Řízení aktiv (A.8)

Cílem těchto bezpečnostních opatření je nalezení a udržování přiměřené bezpečnosti všech aktiv, které jsou součástí ISMS. Jsou zde tři skupiny opatření, první vymezuje odpovědnost za aktiva, další určuje pravidla pro klasifikaci informací a poslední pravidla pro manipulaci s médii.

Seznam aktiv (A.8.1.1)

Toto opatření představuje sestavení důsledného seznamu aktiv, díky kterému má organizace přehled o aktivech a může tak určit, která aktiva jsou kritická a která ne. Tento seznam by měl být přesný, konzistentní, uspořádaný a hlavně aktuální. Je potřeba jej tedy neustále udržovat a aktualizovat. Seznam aktiv je již v rámci této práci sestaven, je tedy nutné ho pouze obnovit a minimálně jednou ročně znovu prověřit.

Prověření seznamu aktiv: 6 hodiny.

Vlastnictví aktiv (A.8.1.2)

Aktiva, která jsou v seznamu, by měla mít přiděleného vlastníka, tedy osobu, která je zodpovědná za správu a řízení daného aktiva. Vlastnictví by mělo být přiděleno hned při vytvoření aktiva. Vlastník musí zajistit inventarizaci aktiv, jejich klasifikaci a také ochranu. Stejně tak je zodpovědný za správné vymazání či zničení.

Přiřazení vlastníků: 3 hodiny.

Přípustné použití aktiv (A.8.1.3)

Je nutné sestavit pravidla pro bezpečné používání informací, aktiv a vybavení spojených s informacemi. Např. obchodní tajemství a jiné utajené informace by neměli být přenášeny po síti bez zašifrování ani kopírovány na mobilní média. Zaměstnanci, kteří mají přístup k aktivům, musí být obeznámeni s požadavky bezpečnosti informací.

Sestavení pravidel pro přípustné používání aktiv: 4 hodiny.

Navrácení aktiv (A.8.1.4)

Po ukončení zaměstnání musí každý zaměstnanec navrátit všechna aktiva organizace, která měl u sebe a používal. Pokud má zaměstnanec vlastní zařízení, je potřeba stanovit postupy, podle kterých budou bezpečně vymazány veškeré informace, které z bezpečnostních důvodů nemůže daná osoba nadále používat a vlastnit. Pokud má zaměstnanec znalosti, které jsou pro organizaci důležité a nezbytné pro probíhající operace, je potřeba tyto informace zdokumentovat. Během výpovědní lhůty je důležité zamezit neoprávněnému kopírování důležitých informací a vynášení mimo organizaci.

Sestavení postupů pro navrácení aktiv: 3 hodiny.

Klasifikace informací (A.8.2.1)

Klasifikace je důležitá pro indikaci toho, jak s informacemi zacházet a jak je chránit. Pro usnadnění je vhodné vytvořit skupiny informací s podobnými potřebami ochrany a určit postupy pro každou takovouto skupinu. Díky tomu není potřeba posuzovat rizika případ od případu. Při klasifikaci je nutné vzít v úvahu, že informace mohou být časem zveřejněny a tím přestanou být citlivé nebo kritické. Přehnaná klasifikace může vést ke zbytečným nákladům, nedostatečná klasifikace zase naopak k ohrožení bezpečnosti. Proto je vhodné jednou ročně znovu klasifikaci prověřit. Při klasifikaci by měl být brán ohled především na úroveň škod, které může způsobit prozrazení informací. Hlavní tři úrovně klasifikace by měly být rozděleny na veřejné, citlivé a utajované informace.

Doba potřebná pro klasifikaci informací: 8 hodin.

Označování informací (A.8.2.2)

Podle vytvořeného schématu pro klasifikaci informací je potřeba vypracovat postupy pro označování těchto informací. Je důležité, aby dané označení bylo jednoduše rozpoznatelné, a aby byli všichni zaměstnanci seznámeni s postupem označování informací. U informací, které nejsou citlivé ani utajované je možné označení vynechat a ulehčit tak zaměstnancům práci.

Vypracování postupů pro označování klasifikovaných informací: 4 hodiny.

Manipulace s aktivy (A.8.2.3)

V souladu s klasifikací je dále nutné zavést postupy pro zacházení, zpracování, ukládání a předávání informací. Pro každou úroveň klasifikace umožnit přístup jen oprávněným osobám, o kterých by měl být udržován záznam. A veškeré kopie informací musí být chráněny stejně jako originál a každá kopie musí být přehledně označena.

Vypracování postupů pro manipulaci s aktivy: 4 hodiny.

Správa výměnných médii (A.8.3.1)

Podle stanovené klasifikace informací, je potřeba zavést postupy pro správu výměnných médií, které tyto informace obsahují. Jedná se o výměnné disky, Flash média, diskety apod. Jde tedy o to, aby tyto informace nebyly prozrazeny, modifikovány, odstraněny ani zničeny. Média musí být uložena v bezpečném prostředí. Pro důvěrné informace je vhodné při uložení dat na médium použít kryptografické techniky. Dále je potřeba přenášet data na nová média, pokud se stávající média blíží ke konci životnosti a je zde riziko ztráty dat. Při likvidaci médií je nutné zajistit, aby nebylo možné data znovu obnovit a zneužít, stejně tak je potřeba uchovávat záznam o takto odstraněných médiích. U velice cenných a důležitých dat je vhodné mít více kopií uložených na oddělených médiích. Používání médií a přenos informací by měl být monitorován a všechny stanovené postupy a úrovně oprávnění musí být dokumentovány.

Vypracování postupů pro správu výměnných médií: 2 hodiny.

Likvidace médií (A.8.3.2)

I pro likvidaci médií je nutné mít postupy, které budou určovat bezpečnou likvidaci. Musí zajistit, že neuniknou žádné důvěrné informace mimo organizaci. O každé likvidaci je nutné vést záznam. Likvidace by měla probíhat spalováním, skartováním nebo kompletním a neobnovitelným vymazáním. Při likvidaci je možné soustředit se pouze na média obsahující důvěrné informace, pro větší bezpečnost je však vhodné likvidovat hromadně všechna, která jsou určena k likvidaci, bez ohledu na důležitost obsahu. Likvidace může být někdy potřebná i v případě, že se médium poškodí a jeho zaslání k opravě by bylo příliš rizikové, protože obsahuje citlivá data.

Vypracování postupů pro likvidaci médií: 1 hodina.

Přeprava fyzických médií (A.8.3.3)

Pokud je nutné média s důvěrnými informacemi přepravit, je potřeba zajistit ochranu před neoprávněným přístupem, zneužitím nebo poškozením. Přeprava tedy musí být spolehlivá a pokud jsou využívány kurýrní služby, musí být řádně ověřeny a schváleny managementem. Média musí být fyzicky chráněna proti poškození, vystavení teplu, vlhkosti apod. Je potřeba zaznamenat všechna média, která se přepravují, použitou ochranu, čas předání a přijetí na místo určení.

Vypracování postupů pro přepravu fyzických médií: 2 hodiny.

4.2.5 Řízení přístupu (A.9)

Tato opatření se snaží omezit přístup k informacím a k vybavení pro zpracování informací tak, aby je mohli využívat pouze osoby, které jsou k tomu oprávněny a které tyto informace či vybavení opravdu nezbytně potřebují.

Politika řízení přístupu (A.9.1.1)

Je důležité vytvořit dokumentovanou politiku, která bude upravovat pravidla pro řízení přístupu k informacím. Tato pravidla by měla být postavena na principu, který zakazuje vše co není výslovně povoleno. Přístupová práva by měla být stanovena obecně pro role a tyto role by pak měly být přiřazeny jednotlivým pracovníkům. Přístup k daným informacím by měl pracovník mít pouze v případě, že tyto informace nezbytně potřebuje k vykonání úkolu. Stejně tak přístup k vybavení je poskytnut pouze pro vykonání daného úkolu.

Vypracování politiky řízení přístupu: 4 hodiny.

Odebrání nebo úprava přístupových práv (A.9.2.6)

Zde je důležité, aby byla pracovníkovi odebrána přístupová práva k informacím hned po ukončení zaměstnání. Je vhodné změnit přístupové heslo, popřípadě zrušit starý uživatelský účet a vytvořit nový pro nového zaměstnance. Důležité je především informovat ostatní zaměstnance, aby nadále nesdíleli důležité firemní informace s osobou, která odešla. Tento postup by měl být součástí politiky řízení přístup.

Používání tajných autentizačních informací (A.9.3.1)

Uživatele musí být odpovědní za ochranu autentizačních informací, tedy v tomto případě přihlašovacího hesla k danému uživatelskému účtu. Je především důležité, aby tato hesla nesdělovali nikomu vně ani uvnitř organizace, aby byla hesla snadno zapamatovatelná a přitom dostatečně silná na to, aby je nebylo možné snadno uhodnout.

Sepsání pravidel pro používání autentizačních informací: 2 hodiny.

4.2.6 Kryptografie (A.10)

Pro ochranu důvěrnosti, autenticity a integrity informací lze využít i kryptografických technik. Je nutné zvážit, kdy je potřeba tyto techniky využít a kdy by jejich zavedení bylo zbytečně příliš nákladné.

Politika pro použití kryptografických opatření (A.10.1.1)

Pro patřičnou ochranu informací je nutné vypracovat politiku, která stanoví použití kryptografických opatření. Každá informace vyžaduje jinou úroveň zabezpečení a to i s ohledem na to, zda jsou permanentně uloženy v prostorách firmy, nebo je nutné je přenášet mimo organizaci. Právě mobilní zařízení, která obsahují citlivé informace, by měly mít kryptografickou ochranu, protože jinak by při jejich ztrátě či odcizení měl útočník neomezený přístup k těmto informacím.

Vypracování politiky pro použití kryptografických opatření: 4 hodiny.

Správa klíčů (A.10.1.2)

Při použití kryptografických technik je také nutné zavést postupy pro správu a ochranu kryptografických klíčů. Postupy by měly zahrnovat generování, ukládání a archivaci klíčů. Je také důležité, aby byly klíče chráněny před modifikací a ztrátou. Avšak v případě ztráty, odcizení nebo poškození klíčů, musí existovat možnost obnovit zašifrované informace.

Vypracování postupů pro správu klíčů: 4 hodiny.

4.2.7 Fyzická bezpečnost a bezpečnost prostředí (A.11)

Tato opatření mají zabránit především fyzickému přístupu do prostor společnosti a úmyslnému poškození informací a jiných aktiv. Tato opatření jsou již ve firmě z části zavedená a dobře zvládnutá. Druhou část tvoří opatření, která mají za úkol chránit samotná zařízení proti ztrátě, poškození či krádeži.

Podpůrné služby (A.11.2.2)

Zde jde především o ochranu zařízení před výpadkem napájení. Navrhuji zakoupit čtyři UPS záložní zdroje ke všem stolním počítačům, díky kterým bude možné, při výpadku elektřiny, uložit stávající práci a počítače bezpečně vypnout. Samozřejmostí těchto záložních zdrojů je i přepěťová ochrana.

Zakoupení čtyř UPS zdrojů EATON UPS 5E 650i: 4 * 1 000 Kč = 4 000 Kč
Instalace UPS zdrojů: 1 hodina.

Údržba zařízení (A.11.2.4)

Je důležité, aby byla zařízení udržována a zachována tak jejich dostupnost i integrita. Každé zařízení má jiný interval, v jakém je potřeba provádět servis. Pokud jsou opravy prováděny mimo organizaci, je nutné zvážit zda zařízení obsahuje důvěrné informace, které by měly být před servisem ze zařízení odstraněny. Nejrizikovější jsou pevné HDD disky, které obsahují samotná data. Při poškození disku tak může dojít ke ztrátě důležitých dat. Toto z velké části řeší opatření A.12.3.1 pro zálohování informací. Abychom však předešli poškození disků, lze využít i diagnostické a monitorovací nástroje, které zjistí v jakém stavu disk je a zda je potřeba disk opravit nebo rovnou zakoupit nový. Tuto kontrolu je vhodné provádět alespoň jednou za šest měsíců.

Vypracování zásad pro údržbu zařízení: 3 hodiny.
Kontrola životnosti zařízení: 2 hodiny / každých 6 měsíců.

Přemístění aktiv (A.11.2.5)

Toto opatření má zajistit, aby žádná zařízení, informace či software nebyli vynášeny mimo organizace bez předchozího povolení. Je potřeba určit, kteří zaměstnanci jsou

oprávnění přemisťovat taková aktiva, a také v jaké časové lhůtě musí tato aktiva navrátit.

Vypracování zásad pro přemístění aktiv: 1 hodina.

Bezpečnost zařízení a aktiv mimo prostory organizace (A.11.2.6)

Používání zařízení pro uchovávání informaci mimo prostory organizace by mělo být schváleno managementem. Veškerá taková zařízení nesmí být ponechána na veřejném místě bez dozoru. Je také důležité dodržovat pokyny výrobců a nevystavovat zařízení přímému slunečnímu záření apod. Také je vhodné vést o těchto zařízeních záznamy.

Vypracování zásad pro používání aktiv mimo organizaci: 1 hodina.

Bezpečná likvidace nebo opakované použití zařízení (A.11.2.7)

Likvidace jakéhokoli zařízení, které obsahuje citlivé a důvěrné informace, je potřeba provést bezpečným způsobem. Tedy tak, aby nebylo možné tato data znovu obnovit. Při vyřazení počítače je nutné permanentně vymazat obsah disků, nebo tyto disky fyzicky zničit.

Vypracování zásad pro bezpečnou likvidaci zařízení: 1 hodina.

Uživatelská zařízení bez obsluhy (A.11.2.8)

Zařízení, u kterých zaměstnanci ukončí svou práci, je potřeba zabezpečit proti neoprávněnému přístupu. Tedy u počítače je potřeba se odhlásit apod.

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

Zaměstnanci by měli dodržovat tuto zásadu a nenechávat citlivé informace, ať už v papírové podobě nebo na paměťovém médiu, ležet volně na stole. Stejně tak by počítače měli být automaticky zamknuty pokud na nich nikdo nepracuje.

Vypracování zásad pro zařízení bez obsluhy a zásad prázdného stolu: 1 hodina.

4.2.8 Bezpečnost provozu (A.12)

Opatření, která zajišťují bezpečnost provozu, se týkají především údržby zařízení, řízení změn v organizaci, zálohování informací a také postupů instalaci softwaru.

Dokumentované provozní postupy (A.12.1.1)

Provozní činnosti, které souvisí s vybavením a zařízeními pro zpracování informací, by měly mít stanovené a dokumentované postupy. Jedná se o postupy pro údržbu zařízení, zálohování, zacházení s médii, bezpečnost práce, ale i zacházení s poštou nebo zapnutí a vypnutí počítače. Jednotlivé postupy a jejich časová náročnost jsou rozepsány v následujících opatřeních.

Řízení změn (A.12.1.2)

Změny ve společnosti, které se týkají podnikových procesů, vybavení pro zpracování informací a systémů ovlivňující bezpečnost informací, by měly být řádně řízeny a také kontrolovány. Všechny změny by měly být plánovány dopředu a také je potřeba zvážit dopady na bezpečnost informací. Před nasazením změn je důležité otestování a o všech významných změnách vést záznamy. S provedenými změnami musí být seznámeni všichni, kterých se dané změny dotýkají.

Řízení kapacit (A.12.1.3)

Toto opatření má za úkol především předejít vyčerpání kapacit lidských zdrojů, vybavení kanceláří, ale i kapacity diskového prostoru. Jako řešení může být buď navýšení kapacity a nebo snížení nároků. U diskového prostoru lze vymazat zastaralá data, u vybavení kanceláří je stejně tak možné skartovat nepotřebné dokumenty apod.

Vypracování zásad pro řízení změn a řízení kapacit: 1 hodina.

Zálohování informací (A.12.3.1)

Zálohovány by měly být všechny informace, software, ale i bitové kopie operačního systému. Všechny zálohy je nutné pravidelně kontrolovat a testovat, zda nejsou poškozeny. Média se zálohami musí být uchovány na bezpečném místě a minimálně

v jiné místnosti, než jsou originální data. Pro vytváření a správu záloh je potřeba sestavit dokumentovanou politiku.

Navrhuji, aby byly prováděny zálohy dat jednou týdně na USB Flash disk. Data, která je potřeba zálohovat, jsou v řádech desítek MB. Stačí tedy i Flash disk s nízkou kapacitou, např. 16 GB. Na konci měsíce by se měly všechny zálohy z Flash disku vypálit na nepřepisovatelné DVD, které bude uskladněno v jiné místnosti. Tím se předejde problémům při nechtěném smazání záloh a na Flash disku mohou zálohy zůstat a sloužit pro rychlé vyhledání konkrétní zálohy. Stejně tak dvojí zálohování zvyšuje bezpečnost a snižuje dopady vzniklé při ztrátě nebo zničení Flash disku.

Důležité je také data na záložních médiích zašifrovat. Je tedy vhodné zakoupit média, která již mají zabudované hardwarové šifrování. USB Flash disk Verbatim Secure'n' Go podporuje hardwarové 256 bitové šifrování Premium AES (Advanced Encryption Standard). Stejné šifrování podporují i SecureSave DVD disky od společnosti Verbatim. Software na šifrování je integrován přímo do DVD disku, není tedy potřeba nic instalovat.

Kromě samotných dat je také vhodné vytvářet bitové kopie operačního systému alespoň jednou za šest měsíců. Diskový oddíl, na kterém je nainstalován operační systém, neobsahuje žádná citlivá ani důvěrná data. Ta jsou vždy uložena na vedlejším diskovém oddílu, což zvyšuje bezpečnost a umožňuje přeinstalovat celý operační systém bez nutnosti zálohovat jakákoli data. Díky tomu také není nutné zálohovat bitové kopie na šifrované DVD disky a lze zakoupit pouze obyčejné DVD.

Vytvoření politiky pro zálohování informací: 4 hodiny.
Zakoupení USB Flash disk Verbatim Secure'n' Go 16GB: 700 Kč.
Zakoupení Verbatim DVD-R SecureSave 12ks: 1500 Kč / ročně.
Zakoupení Verbatim DVD-R 50ks: 300 Kč / ročně.
Zálohování dat na Flash disk a následně na DVD: 1 hodina / každý měsíc.
Vytvoření bitových kopií a vypálení na DVD: 4 hodiny / každých 6 měsíců.
Kontrola zálohovaných dat a médií: 4 hodiny / každých 6 měsíců.

Instalace softwaru na provozní systémy (A.12.5.1)

Pro instalaci softwaru by měly být sestaveny postupy. Software by měl být aktualizován pouze školenými zaměstnanci a až po schválení managementem. Před nasazením nové verze by měl být softwaru otestován a předchozí verze i s daty bezpečně zálohovány.

Vytvoření postupů pro instalaci softwaru: 1 hodina.

4.2.9 Bezpečnost komunikací (A.13)

Cílem těchto opatření je zajistit bezpečnost komunikací, tedy převážně ochranu informací, které jsou při komunikaci sdělovány či posílány. Opatření v rámci sítě má organizace již z části zvládnuté. Následující opatření se týkají především samotného přenosu informací v rámci organizace i s jakýmkoli externím subjektem.

Politiky a postupy při přenosu informací (A.13.2.1)

Při přenosu informací v rámci organizace i s externím subjektem je potřeba dodržovat bezpečnostní postupy. Je nutné zavést politiku pro ochranu přenosu informací prostřednictvím jakýchkoli komunikačních zařízení. Postupy by měly chránit přenášené informace před odposloucháváním, kopírováním, úpravami či zničením. Zaměstnanci musí být poučeni o odpovědnosti za prozrazení důvěrných informací, pomlouvání či jiné kompromitace organizace. Stejně tak by měli být zaměstnanci poučeni, že nesmí vést důvěrné rozhovory na veřejnosti nebo skrze nezabezpečené komunikační kanály. Důvěrné informace by také neměli být zanechány na záznamníku, aby nebyly zneužity neoprávněnými osobami.

Vypracování politiky pro bezpečný přenos informací: 4 hodiny.

Dohody o přenosu informací (A.13.2.2)

Pro přenos informací mezi organizací a externími stranami, by měly být zavedeny dohody, které daný přenos zabezpečí. Obě strany by měly přijmout dostatečná bezpečnostní opatření, aby nedošlo ke ztrátě či odcizení informací. Za řízení přenosu, odesílání a přijímání dokumentů a jiných informací by měl být vždy odpovědný

management organizace. Je také potřeba stanovit odpovědnosti a povinnosti v případě ztráty informací.

Vypracování dohod o přenosu informací: 2 hodiny.

Elektronické předávání zpráv (A.13.2.3)

Při elektronickém zasílání zpráv je důležité, aby byly zprávy přiměřeně chráněny a nedostaly se do neoprávněných rukou. Je potřeba zavést zásady pro správné adresování i přepravu zpráv. Také je vhodné zakázat nezabezpečené komunikační kanály a také ty, které mohou omylem vystavit informace veřejně, jako jsou sociální sítě apod. Předejde se tak chybnému zaslání citlivých dat na nesprávnou adresu, nebo jejich zveřejnění.

Vypracování zásad pro elektronické předávání zpráv: 1 hodina.

4.2.10 Řízení incidentů bezpečnosti informací (A.16)

Úkolem těchto opatření je, aby incidenty bezpečnosti informací byly řízeny důsledně a efektivně. Důležité je také zajištění komunikace ohledně bezpečnostních událostí a slabých míst organizace.

Odpovědnosti a postupy (A.16.1.1)

Je potřeba stanovit postupy, které zajistí, že incidenty bezpečnosti informací budou řádně hlášeny, neboli že budou mít efektivní odezvu. Měly by být zavedeny postupy pro plánování a přípravu odezvy na incidenty. Bezpečnostní incidenty je potřeba monitorovat, detekovat, analyzovat a podávat o nich zprávy. Při řízení incidentů by měli být všechny incidenty zaznamenávány. Je především důležité, aby personál zvládal problémy, které souvisí s bezpečnostními incidenty. Také je vhodné vytvořit kontaktní místo, kde mohou zaměstnanci podávat zprávy o incidentech. Při výskytu incidentu by měly být zaznamenány všechny podrobnosti, jako je typ závady, zprávy zobrazené na obrazovce apod. Po zaznamenání všech detailů by měla být okamžitě předána zpráva kontaktnímu místu. Při vyřešení incidentu by měly příslušné osoby dostat zpětnou

vazbu. Podrobnější rozbor a odhad časové náročnosti je uveden v následujících opatřeních.

Hlášení událostí bezpečnosti informací (A.16.1.2)

Jakékoli závady nebo nezvyklé chování systému může ukazovat na bezpečnostní útok. Pro zabránění prolomení bezpečnosti je proto důležité hlásit všechny události bezpečnosti informací. Všichni zaměstnanci musí být obeznámeni s povinností hlásit bezpečnostní události v co nejkratším čase. Také musí znát kontaktní místo a postup podávání zpráv o takovýchto událostech. Mezi události bezpečnosti informací můžeme zařadit neefektivní bezpečnostní opatření, lidské chyby, prolomení opatření fyzické bezpečnosti, špatnou funkci softwaru nebo hardwaru, nebo také narušení očekávané integrity, důvěrnosti či dostupnosti informací.

Vypracování postupů pro hlášení událostí: 1 hodina.

Hlášení slabých míst bezpečnosti informací (A.16.1.3)

Všichni zaměstnanci by měly být povinni hlásit jakákoli slabá místa bezpečnosti informací, která považují za opodstatněná. Při zjištění takovýchto slabých míst je potřeba oznámit tuto skutečnost co nejdříve. Proto by mělo být podávání zpráv snadné, přístupné a hlavně dostupné. Je také důležité, aby se zaměstnanci nesnažili sami ověřit, zda se opravdu jedná o slabé místo. Pokusy o narušení bezpečnosti mohou být chápány jako cílené zneužití systému.

Vypracování postupů pro hlášení slabých míst: 1 hodina.

Posouzení a rozhodnutí o událostech bezpečnosti informací (A.16.1.4)

Při výskytu bezpečnostní události je potřeba danou událost posoudit a rozhodnout, zda ji klasifikovat jako incident bezpečnosti informací. Pro tato rozhodnutí je potřeba stanovit klasifikační stupnici, podle které lze následně stanovit i prioritu incidentu a definovat tak jeho rozsah a dopad na organizaci. Každé rozhodnutí je potřeba zaznamenat, aby bylo možné v budoucnu ověřit správnost rozhodnutí.

Vypracování postupů pro posouzení a rozhodnutí o událostech: 3 hodiny.

Reakce na incidenty bezpečnosti informací (A.16.1.5)

Po výskytu a nahlášení incidentu by mělo kontaktní místo adekvátně reagovat. Za prvé by měly být shromážděny všechny důkazy ihned po výskytu incidentu, také je důležité oznámit výskyt incidentu všem patřičným osobám. Se slabým místem bezpečnosti informací je potřeba se vypořádat a incident vyřešit. Nakonec vše formálně uzavřít a incident zaznamenat.

Vypracování postupů pro reakci na incidenty: 1 hodina.

Ponaučeni z incidentů bezpečnosti informací (A.16.1.6)

Pro snížení pravděpodobnosti opakování incidentů nebo i pro snížení dopadu incidentů, je vhodné využít znalosti získané z řešení předchozích incidentů. Lze je využít např. při pravidelných školeních zaměstnanců.

Shromažďování důkazů (A.16.1.7)

Pro identifikaci, shromažďování, získávání, uchovávání důkazů a zacházení s důkazy je potřeba zavést vhodné postupy. Je důležité vzít v úvahu jak bezpečnost důkazů, tak bezpečnost personálu, dále úlohy a povinnosti zapojených zaměstnanců, nebo také dokumentaci a kompetence personálu.

Vypracování postupů pro shromažďování důkazů: 2 hodiny.

4.2.11 Soulad s požadavky (A.18)

Tato opatření se snaží zabránit porušení právních a smluvních povinností, které souvisí s bezpečností informací. Jsou zde převážně opatření zajišťující splnění požadavků bezpečnosti. Druhou část pak tvoří opatření pro přezkoumání bezpečnosti souvisejících s certifikací ISMS, kterou však organizace prozatím neplánuje.

Identifikace odpovídající legislativy a smluvních požadavků (A.18.1.1)

Je důležité identifikovat, dokumentovat a udržovat v aktuální stavu všechny zákonné a smluvní požadavky dané legislativy i přístupy ke splnění těchto požadavků. Měla by

být také stanovena opatření ke splnění těchto požadavků, která jsou dále popsána v následujících opatřeních.

Ochrana duševního vlastnictví (A.18.1.2)

Práva duševního vlastnictví, která zahrnují práva k softwaru nebo i k dokumentům, by měla být dodržována a pomocí vhodných opatření by měl být zajištěn soulad s legislativními a smluvními požadavky, které se těchto práv týkají. Je tedy potřeba zavést politiku, která zajistí ochranu subjektů, které představují duševní vlastnictví. Software by měl být získáván pouze ze známých a důvěryhodných zdrojů, aby nedošlo k porušení autorských práv. Je také důležité udržovat povědomí o politice na ochranu práv duševního vlastnictví a při jejím porušení zahájit disciplinární řízení. Doklady o vlastněných licencích by měly být bezpečně uchovány pro případné prokazování. Je potřeba zajistit, že nebude překročen maximální počet uživatelů na licenci a že budou dodrženy všechny licenční podmínky.

Vypracování politiky pro ochranu duševního vlastnictví: 3 hodiny.

Ochrana záznamů (A.18.1.3)

Veškeré důležité záznamy by měly být chráněny proti ztrátě, poškození, falšování a neoprávněnému přístupu. Pro rozhodování o ochraně daných záznamů by měla být rozhodující klasifikace informací. U každého typu záznamu je nutné stanovit dobu uchování a typ paměťového média, u kterého je důležité vzít v úvahu jeho životnost a předejít tak ztrátě dat. Samotné skladování médií tak musí být v souladu s doporučeními výrobce. U médií, která jsou uskladněna delší dobu, je nutné zajistit nejen jejich čitelnost, ale také samotný formát obsažených dat. V průběh času totiž může změnami technologií dojít ke ztrátě dat ve smyslu nemožnosti jejich přečtení novými nekompatibilními technologiemi.

Vypracování postupů pro ochranu záznamů: 5 hodin.

Regulace kryptografických opatření (A.18.1.5)

Použitá kryptografická opatření by měla být v souladu s danými předpisy i legislativou. Při provádění či doplňování kryptografických funkcí, je nutné vždy zvážit vývoz

hardwaru či softwaru mimo organizaci, aby nedošlo k narušení bezpečnosti. Samotné šifrování dat by mělo také být omezeno dle potřeby. Aby byl zajištěn soulad s příslušnou legislativou je vhodné vyhledat právní pomoc.

Vypracování postupů pro regulaci kryptografických opatření: 3 hodiny.

Přezkoumání bezpečnosti informací (A.18.2)

Poslední tři opatření slouží pro přezkoumání bezpečnosti informací a shody s bezpečnostními politikami a normami. Jsou tedy podstatnou částí pro certifikaci ISMS. Tato společnost prozatím o certifikaci neuvažuje, bylo by to pro ni zbytečně příliš nákladné. Avšak myslím, že je vhodné pravidelně provádět alespoň ověření, že jsou daná opatření implementována a provozována v souladu se zavedenými postupy a politikami.

4.3 Postup zavedení bezpečnostních opatření

V předchozí kapitole 4.2 byla popsána opatření, která je potřeba zavést. Tato opatření jsou seřazena podle jejich číselného označení v příloze A normy ČSN ISO/IEC 27001. Při jejich zavádění je však nutné zvolit pořadí dle jejich důležitosti a dle závažnosti rizik, které tato opatření minimalizují.

Na základě analýzy rizik a výsledné Matice rizik v tabulce 8 je vidět, že vysoké míry rizik představují hrozby jako jsou porucha hardwaru a poškození zálohovacího média. Tyto hrozby mají největší vliv právě na zálohy dat, na účetní doklady, osobní údaje a další data uložené na daných médiích. Je proto důležité nejprve zavést efektivní a bezpečné zálohování dat, které bude obsahovat i kryptografická opatření. Tato opatření jsou součástí skupin **A.12** a **A.10** v tabulce 9.

Střední míry rizik dále představují hrozby jako jsou výpadek elektrického proudu, krádež zařízení a chybné zaslání dat. I tyto hrozby mají velký vliv na integritu a důvěrnost informací. Proto je potřeba zavést opatření pro ochranu při výpadku elektrického proudu a také opatření pro údržbu zařízení, které částečně sníží vysoké riziko poruchy hardwaru, které již bylo zmíněno v předchozím odstavci. V tabulce 9 najdeme tato opatření pod označením **A.11**. Tato opatření také obsahují zásady pro používání aktiv mimo organizaci, pro bezpečnou likvidaci zařízení, pro zařízení bez

obsluhy a zásadu prázdného stolu. I tato opatření zvyšují bezpečnost informací. Další opatření, která přispívají ke snížení středních rizik, jsou v tabulce 9 pod označením **A.6**, **A.8** a **A.13**. Tato opatření zavádějí postupy a politiky, které chrání proti ztrátě a zneužití informací. Také jsou zde postupy pro manipulaci s aktivy, pro správu výměnných médií a jejich bezpečnou likvidaci. V neposlední řadě jsou zde také opatření, které mají za úkol poučit zaměstnance o odpovědnosti při prozrazení důvěrných informací a předejít tak i např. chybnému zaslání dat na špatnou adresu.

Po zavedení výše zmíněných opatření je možné pokračovat dále opatřeními, které přispívají ke zvýšení bezpečnosti informací. Tato opatření jsou v tabulce 9 pod označením **A.9**, **A.16** a **A.18**. Jedná se o politiku řízení přístupu k informacím a o opatření, která chrání autentizační informace. Dále jsou zde postupy pro hlášení bezpečnostních událostí a slabých míst a také postupy pro řešení incidentů. Poslední skupina opatření jsou důležitá pro zvyšování povědomí o politice pro ochranu duševního vlastnictví, aby nedocházelo k porušení autorských práv.

Se všemi vypracovanými politikami a postupy je potřeba zaměstnance seznámit. K tomu slouží opatření s označením **A.7**, která slouží právě pro vypracování programu pro seznámení zaměstnanců s bezpečnostními pravidly a pro zvyšování povědomí o bezpečnosti informací. Součástí těchto opatření je i vypracování postupů pro prověřování nových zaměstnanců a pro disciplinární řízení. Před samotným školením zaměstnanců, je také důležité provést přezkoumání všech vypracovaných politik, což je součástí opatření s označením **A.5.1.2**. Na začátku školení je vhodné seznámit zaměstnance s tzv. politikou bezpečnosti informací, která má určit směr a vyjádřit podporu bezpečnosti informací ze strany managementu. Tato politika, která je součástí opatření s označením **A.5.1.1**, by měla být vypracována jako první ještě před zaváděním jakýchkoli opatření, protože bez podpory managementu není možné daná opatření zavádět. V tabulce 10 je shrnut postup zavádění daných opatření, počet hodin, které je potřeba pro jejich zavedení a následně počet hodin pro každoroční kontrolu.

Označení	Název opatření	Počet hodin potřebných pro zavedení opatření	
		jednorázově	každoročně
A.5.1.1	Vypracování politiky bezpečnosti informací	8	0
A.12	Bezpečnost provozu	15	28
A.10	Kryptografie	8	0
A.11	Fyzická bezpečnost a bezpečnost prostředí	10	4
A.6	Organizace bezpečnosti informací	14	0
A.8	Řízení aktiv	37	21
A.13	Bezpečnost komunikací	7	0
A.9	Řízení přístupu	6	0
A.16	Řízení incidentů bezpečnosti informací	8	0
A.18	Soulad s požadavky	11	0
A.7	Bezpečnost lidských zdrojů	24	0
A.5.1.2	Přezkoumání vypracovaných politik	12	12
A.7.2.2	Seznámení zaměstnanců s bezpečnostními pravidly	10	10
	Celkem hodin:	**170**	**75**

Tabulka 10: Pořadí zavedení bezpečnostních opatření

4.4 Ekonomické zhodnocení a časový plán

Důležitou součástí při zavádění ISMS je určit časovou a finanční náročnost projektu. V tabulce 10 je vidět, že celkový předpokládaný počet hodin pro zavedení bezpečnostních opatření vychází na 170 hodin. Vedení se dohodlo, že odpovědná osoba, která bude daná opatření zavádět, se bude tomuto projektu věnovat 20 až 30 hodin týdně. Předpokládaná doba zavedení všech opatření je naplánována na 9 týdnů, což představuje v průměru 19 hodin týdně. Je zde tedy dostatečná časová rezerva, která počítá s možnými problémy a překážkami při zavádění daných opatření. Počátek projektu je plánován na 2.3.2015 a konec tedy na 4.5.2015, kdy už by měly být všichni zaměstnanci seznámeni s danými opatřeními a politikami. Detailní časový plán zavedení opatření je zobrazen v tabulce 12 na straně 76.

ISMS je však nikdy nekončící proces, který vyžaduje neustálé udržování a zlepšování, nelze jej tedy pouze zavést a dále nic nedělat. Zavedené postupy a politiky je potřeba pravidelně kontrolovat a aktualizovat, zaměstnance je potřeba vždy seznámit

s danými změnami a samozřejmě je důležité pravidelně provádět zálohování, údržbu zařízení a další činnosti, které neustále přispívají ke zvýšení bezpečnosti informací. V tabulce 10 je vypočítána pravidelná roční náročnost těchto opatření na 75 hodin ročně. Samozřejmě, že některá opatření je potřeba dodržovat v měsíčních intervalech, jiná v půlročních atd. Počet hodin je tedy přepočítán na roční náročnost, abychom mohli vyjádřit pravidelné roční náklady.

Vedení společnosti se dohodlo na hodinové mzdě 300 Kč/hod. Při předpokládaných 170 hodinách jsou tedy přibližné náklady 51 000 Kč. K tomu je zapotřebí přičíst náklady na zakoupení UPS zdrojů a zálohovacích médií s kryptografickým zabezpečením, která postačí na následujících 12 měsíců. Tyto náklady jsou ve výši 6 500 Kč. Dohromady jsou tedy jednorázové náklady na zavedení ISMS ve výši 57 500 Kč. To představuje přibližně 3,57% obratu společnosti. Každý následující rok pak bude potřeba investovat do udržování a zlepšování ISMS. Při předpokládaných celkových 75 hodinách, hodinové mzdě 300 Kč/hod a ceně zálohovacích médií 2 500 Kč by měly být celkové roční náklady ve výši 25 000 Kč. To představuje přibližně 1,55% obratu společnosti. Shrnutí všech nákladů je zobrazeno v tabulce 11.

	Jednorázové náklady	**Každoroční náklady**
Zavedení/udržování opatření	51 000 Kč	22 500 Kč
Zakoupení UPS zdrojů	4 000 Kč	0 Kč
Zakoupení zálohovacích médií	2 500 Kč	2 500 Kč
Celkové náklady:	**57 500 Kč**	**25 000 Kč**
Poměr nákladů k ročnímu obratu:	3,57%	1,55%

Tabulka 11: Náklady na zavedení, udržování a zlepšování ISMS

Označení	Název opatření	Od 2.3.2015 do 4.5.2015								
		2.března	9.března	16.března	23.března	30.března	6.dubna	13.dubna	20.dubna	27.dubna
A.5.1.1	Vypracování politiky bezpečnosti informací									
A.12	Bezpečnost provozu									
A.10	Kryptografie									
A.11	Fyzická bezpečnost a bezpečnost prostředí									
A.6	Organizace bezpečnosti informací									
A.8	Řízení aktiv									
A.13	Bezpečnost komunikací									
A.9	Řízení přístupu									
A.16	Řízení incidentů bezpečnosti informací									
A.18	Soulad s požadavky									
A.7	Bezpečnost lidských zdrojů									
A.5.1.2	Přezkoumání vypracovaných politik									
A.7.2.2	Seznámení zaměstnanců s politikami									

Tabulka 12: Časový plán zavedení opatření

5 Závěr

Úkolem této práce bylo navrhnout v daném podniku zavedení systému řízení bezpečnosti informací (ISMS). Společnost prozatím neuvažuje o certifikaci ISMS, ani se na ni nevztahuje nový zákon o kybernetické bezpečnosti, proto tedy neplánuje zavádět všechna opatření, která stanovuje norma ČSN ISO/IEC 27001. Avšak opatření, která byla vybrána, odpovídají opatřením v příloze A této normy. Při analýze rizik, byla zjištěna vysoká a střední rizika, která je potřeba minimalizovat. Mezi největší zjištěné hrozby tak patří porucha hardwaru a poškození zálohovacího média. Při naplnění těchto hrozeb by byly největší škody způsobeny ztrátou důležitých dat. Samotné zálohy byly do dnes prováděny na jediné médium a pouze občas bez jakýchkoli zásad a pravidelnosti. Proto jako prioritní opatření, které minimalizují dopady těchto hrozeb, bylo navrženo týdenní zálohování na USB Flash disk a následné měsíční vytváření permanentních kopií těchto záloh na nepřepisovatelný DVD disk. Oba typy médií byly zvoleny s již integrovaným hardwarovým šifrováním, které chrání uložená data proti zneužití. Pro samotné snížení pravděpodobnosti těchto hrozeb byla také navržena pravidelné kontrola životnosti zařízení i zálohovacích médií a pravidelná kontrola integrity a dostupnosti dat uložených na médiích. Další zjištěná rizika, která mají střední míru, jsou výpadek elektrického proudu, krádež zařízení a chybné zaslání citlivých údajů. Tyto hrozby mohou mít také negativní vliv na integritu, dostupnost a hlavně důvěrnost informací. Pro snížení dopadů těchto hrozeb byla navržena opatření, která zahrnují zakoupení UPS zdrojů, které při výpadku elektřiny umožní práci uložit a počítač bezpečně vypnout. Stejně tak tyto zařízení slouží pro ochranu počítačů proti přepětí. Pro snížení pravděpodobnosti dalších hrozeb byla navržena opatření, která zavádějí postupy a politiky pro bezpečné zacházení s informacemi i s mobilními zařízeními.

Zavedení ISMS je naplánováno celkově na devět týdnů. Celkový počet hodin je vypočítán na 170 hodin práce, je zde tedy dostatečná časová rezerva v případě chybného časového odhadu či pro případné řešení neočekávaných problémů. Předpokládané náklady jsou stanoveny na 57 500 Kč, což tvoří 3,57% ročního obratu společnosti. Tyto náklady zahrnují vypracování všech postupů i politik a také zakoupení potřebných zařízení i médií pro zálohování. Kromě těchto jednorázových nákladů jsou zde ještě náklady na pravidelné udržování a zlepšování ISMS, které činí 25 000 Kč ročně, což

představuje 1,55% ročního obratu. Tyto náklady zahrnují i přepočítané měsíční výdaje na zálohovací média. Samozřejmě tyto pravidelné roční náklady jsou již započítány do jednorázových nákladů na zavedení ISMS, takže s jejich vynaložením se počítá až za dalších dvanáct měsíců.

I přesto, že organizace neuvažuje o certifikaci ISMS, která by zvýšila její důvěryhodnost v očích klientů, má zavedení ISMS velký přínos ve zvýšení bezpečnosti informací v organizaci. I samotná analýza současného stavu bezpečnosti informací je pro organizaci přínosem, protože bylo poukázáno na značné bezpečnostní mezery. Po úspěšném zavedení navržených bezpečnostních opatření tak dojde k výraznému snížení velkých i středních rizik a organizace tak dosáhne přiměřené bezpečnosti za akceptovatelné náklady, které oproti ročnímu obratu společnosti nejsou nijak výrazné. Důsledné poučení zaměstnanců a jejich motivace k dodržování daných bezpečnostních pravidel však přispívá k samotné bezpečnosti nejvíce. Školení zaměstnanců tak musí probíhat pravidelně, stejně jako kontrola, udržování a zlepšování samotného systému řízení bezpečnosti informací.

Seznam použité literatury

[1] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[2] ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

[3] BÉBR, R. a P. DOUCEK. *Informační systémy pro podporu manažerské práce*. 1. vyd. Praha: Professional Publishing, 2005. ISBN 80-86419-79-7.

[4] DOUCEK, P. et al. *Řízení bezpečnosti informací*. 2. Rozšířené vydání o BCM. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[5] ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*. Praha: Český normalizační institut, 2006

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

[7] Bureau Veritas Czech Republic, spol. s r.o.: Zákon o kybernetické bezpečnosti podepsán prezidentem, účinnost od 1. ledna 2015 [online]. 2014 [cit. 2014-10-22]. Dostupné z: http://www.bureauveritas.cz/wps/wcm/connect/bv_cz/local/home/news/press-releases/zakon-o-kyberneticke-bezpecnosti

[8] Krátký, P.: Zákon o kybernetické bezpečnosti v praxi. Časopis IT Systems 9/2014 [online]. 2014 [cit. 2014-10-22]. Dostupné z: http://www.systemonline.cz/it-security/zakon-o-kyberneticke-bezpecnosti-v-praxi.htm

[9] Peterka, J.: Kdo (a co) bude spadat pod nový zákon o kybernetické bezpečnosti? [online]. 2014 [cit. 2014-10-22]. Dostupné z: http://www.lupa.cz/clanky/kdo-a-co-bude-spadat-pod-novy-zakon-o-kyberneticke-bezpecnosti/

[10] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. 29.8.2014. ISSN 1211-1244.

Seznam tabulek

Tabulka 1: Stupnice pro hodnocení aktiv....43
Tabulka 2: Identifikace aktiv....44
Tabulka 3: Ohodnocení aktiv....45
Tabulka 4: Stupnice pravděpodobností hrozeb....45
Tabulka 5: Identifikace a ohodnocení hrozeb....46
Tabulka 6: Ohodnocení míry rizika....46
Tabulka 7: Matice zranitelnosti....47
Tabulka 8: Matice rizik....48
Tabulka 9: Vybraná bezpečnostní opatření....53
Tabulka 10: Pořadí zavedení bezpečnostních opatření....74
Tabulka 11: Náklady na zavedení, udržování a zlepšování ISMS....75
Tabulka 12: Časový plán zavedení opatření....76

Seznam obrázků

Obrázek 1: Bezpečnost organizace (upraveno dle [1])....14
Obrázek 2: Přiměřená bezpečnost za akceptovatelné náklady (upraveno dle [2])....15
Obrázek 3: PDCA model aplikovaný na procesy ISMS (upraveno dle [5])....17
Obrázek 4: Nákladový model pro realizaci bezpečnostních opatření (upraveno dle [4])....21
Obrázek 5: Vztahy mezi normami řady ISO/IEC 27000 (upraveno dle [6])....32