Model PDCA v řízení informační bezpečnosti

PDCA Model in Information Security Management

Bc. Filip Hujer

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Filip HUJER**
Osobní číslo:	**A10853**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Model PDCA v řízení informační bezpečnosti**

Zásady pro vypracování:

1. **Proveďte literární rešerši problematiky ISMS v rámci legislativy EU.**
2. **Vyhodnoťte požadavky na informační bezpečnost dle modelu PDCA ve firmě Brabec s.r.o..**
3. **Navrhněte formou projektu implemetaci PDCA do specifického firemního prostředí.**
4. **Realizujte implementaci ISMS.**
5. **Vyhodnoťte přínosy pro firmu včetně ekonomických a proveďte diskusi.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **UČEŇ, Pavel a kolektiv: Metriky v informatice. Grada Publishing, 2001, 140 stran, 159 Kč, ISBN 80?247?0080?8.**
2. **DOUCEK, Petr; NEDOMOVÁ, Lea; NOVÁK, Luděk; SVATÁ, Vlasta. Řízení bezpečnosti informací. Druhé přepracované vydání, Praha : Professional Publishing, 2011, ISBN 978-80-7431-050-8.**
3. **MLÝNEK, Jaroslav. Zabezpečení obchodních informací. 1. BIZBOOK, 2007-02-05. ISBN 9788025115114.**
4. **POŽÁR, Josef. Systém řízení informační bezpečnosti. In Kný, Milan; Požár, Josef. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. Brno : Tribun EU,2010, s. 93 ? 110. ISBN 978-807399-067-1.**
5. **Risk Analysis Consultants: Překlad a interpretace normy BS ISO/IEC 27001:2005 pro české prostředí 2005.**
6. **Risk Analysis Consultants: Překlad a interpretace normy BS ISO/IEC 17799:2005 pro české prostředí 2005.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tématem diplomové práce je implementace modulu PDCA (Plan, do, check, act) systematického řízení bezpečnosti informací do organizace Brabec s.r.o.. Přínosem této práce je praktická implementace systému bezpečnosti informací do dané organizace a popis implementačního procesu bezpečnosti informaci. V první kapitole se budu věnovat popisu modelu PDCA, který bude nástrojem určující tvar celého systému řízení bezpečnosti informací. Druhá kapitola bude zaměřena na literární rešerši systémového řízení bezpečnosti informaci. V této kapitole se budu věnovat ustanovení ISMS, zavádění a provozu ISMS, monitorování a přezkoumaní ISMS, údržbě a zlepšování ISMS a shrnuti celého cyklu ISMS. Ve třetí kapitole se budu věnovat popisu organizace Brabec s.r.o. do které budu implementovat systém řízení bezpečnosti informací. Ve čtvrté kapitole se budu věnovat popisu jednotlivých kroku při implementaci modulu PDCA v rámci systémového řízení bezpečnosti informací. V pátá kapitola budu provádět již praktickou implementaci ISMS do organizace. V této kapitole budu vycházet z postupu stanoveným v předchozí kapitole a budu vybírat reálné bezpečnostní opatření proti identifikovaným hrozbám. Poslední kapitolu budu věnovat popisem přínosů implementace modulu PDCA do ISMS a to jak z praktického hlediska, tak i z ekonomického úhlu pohledu.

Klíčová slova: plan, do, check, act, systémové řízení bezpečnosti informací, PDCA, ISMS

ABSTRACT

The theme of the thesis is the implementation module PDCA (Plan, Do, Check, Act) systematic management of information security in organizations Ltd. Brabec. The benefit of this work is the practical implementation of information security within the organization and description of the implementation process safety information. In the first chapter, I will give the description of the PDCA model, which will be instrumental in determining the shape of the entire information security management system. The second chapter will focus on literature search of information security management system. In this chapter I will examine the provisions of the IMS, IMS implementation and operation, monitoring and reviewing the IMS, maintenance and improvement of the IMS and IMS summarized the entire cycle. In the third chapter I will describe the organization pay Brabec Ltd. to which I will implement information security management system. In the fourth chapter, I will give a description of each step in the implementation of the module within the PDCA information security management system. In the fifth chapter I will no longer carry out the practical implementation of the IMS in the organization. This chapter will be based on the procedure set out in the previous chapter, and I choose a real safeguard against identified threats. The last chapter will give a description of the benefits of the implementation of the IMS PDCA module, both from a practical standpoint and from an economic point of view.

Keywords: plan, do, check, act, information management system, PDCA, IMS

PODĚKOVÁNÍ

Chtěl bych s úctou poděkovat svému vedoucímu práce, panu ***doc. Mgr. Romanu Jaškovi Ph.D.,*** za jeho cenné rady a připomínky, bez kterých by tato diplomová práce nevznikla v podobě, jaké je.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Ve své diplomové práci nazvané „Model PDCA v řízení informační bezpečnosti“ se budu věnovat popisu a implementaci modelu PDCA v systému řízení bezpečnosti informací do vybrané organizace Brabec s.r.o..

V první kapitole teoretické části se budu věnovat popisu modelu PDCA, který později použiji při tvorbě systémového řízení bezpečnosti informaci pro organizaci Brabec s.r.o.. Také zde uvedu provázanost modulu PDCA se systémem řízení bezpečnosti informací.

Druhá kapitola teoretické části se budu věnovat literární rešerši o systému řízení bezpečnosti informací podle modulu PDCA. Tato kapitola obsahuje popis možností. Které lze využit při tvorbě systémového řízení bezpečnosti informací.

Třetí kapitola teoretické části se bude věnovat popisu požadavku a organizace samotné Brabec s.r.o.. Tato organizace v následných kapitolách podstoupí implementační proces systémového řízení bezpečnosti informací pomocí modulu PDCA dle normy ISO ČSN 27001:2006.

První kapitola praktické části bude věnována popisu postupu implementace a nástrojů systémového řízení bezpečnosti řízení informací. Kapitola bude rozdělena na čtyři části. V první části se bude popisovat metodika ustanovení systémového řízení bezpečnosti informaci. Druhá část bude mít za úkol popsat metodiku zavádění systémového řízení bezpečnosti informací. Třetí část této kapitoly se bude věnovat metodice monitorování a přezkoumávání daného systému řízení bezpečnosti informací. Poslední část této kapitoly bude zaměřena na poslední krok cyklu, který bude popisovat metodiku udržování a zlepšování daného systému.

Druhá kapitola praktické části se bude věnovat praktické implementaci modulu PDCA systémového řízení bezpečnosti informací do vybrané organizace Brabec s.r.o.. Tato kapitola se rozděluje na čtyři podkapitoly (dle plánu PDCA). V první části se budu věnovat ustanovení systémového řízení bezpečnosti informací, které bude obsahovat rozsah a hranice, bezpečnostní politiku, identifikaci rizik a jejich analýzu s vyhodnocením, prohlášení o aplikovatelnosti apod. Druhá část se bude věnovat zavádění a provozování dané systému ve firmě Brabec s.r.o.. V této části se budou definovat bezpečnostní opatření, odpovědné osoby za tyto opatřeni a stanoví se cíle, kterých mají dosáhnout. Monitorování a přezkoumávání je název další podkapitoly. Zde se budou realizovat metodiky měření a přezkoumávání z předešlé kapitoly a budou se zde identifikovat osoby odpovědné za tyto činnosti. Poslední kapitola se bude věnovat přezkoumávání nedostatečný opatření a nenaplněných cílů. Dále se nadefinuje údržba daného systému pro chod a určí se osoby odpovědné za tyto i předešlé činnosti.

Poslední část se bude věnovat posouzení přínosů pro vybranou firmu Brabec s.r.o.. Na tyto přínosy se bude nahlížet dvojím způsobem a to uhlem pohledu praktických přínosů a pohledu ekonomických přínosů.

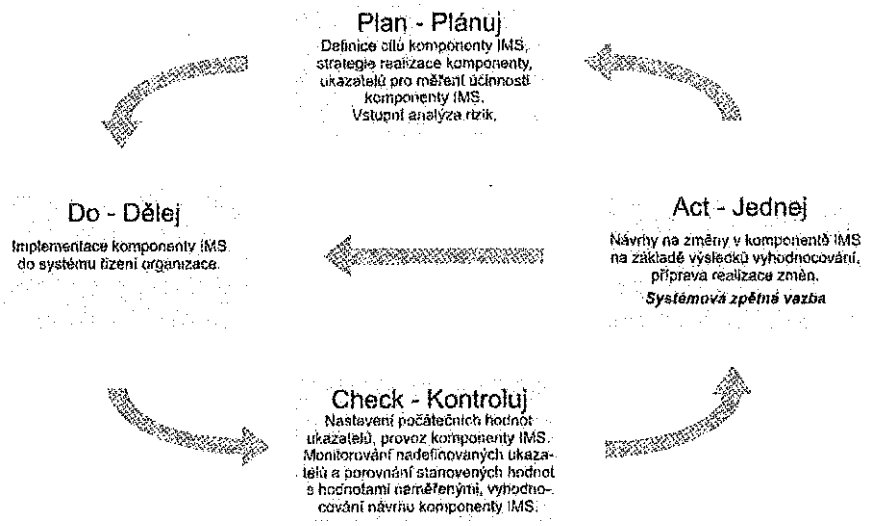
I. TEORETICKÁ ČÁST

1 MODEL PDCA

Model řízení PDCA ukazuje schématické vzor, který je vyjadřuje životní cyklus integrovaného systému řízení a jeho dostupných komponent. Tento cyklus je konečné fázi zajištěn zpětnou kontrolní vazbou. Životní cyklus PDCA je znázorněn na obrázku.

Tento model podává možnost využívat podobné metody, metodiky a postupy pro řízení každého prvku integrovaného systému řízení a ISMS jako celku. Kromě řízení prvků integrovaného systému řízení je podstatné dokázat pozorovat a vyhodnocovat i jejich efektivitu a vhodnost. Vhodnost prvků se měří obvykle srovnáváním s některým mezinárodním standardem (normou). Dané normy jsou systematickým návodem jak dané činnosti provádět s nejvyšší efektivitou nebo-li dle nejvýhodnějších empirií, které se vyvinuly v odlišných dílech světa a které se prosadily v praxi. I když se jedná o nejlepší empirie, není možné je přebírat mechanicky a bez kreativního postoje. Kterákoliv organizace má svoje vlastní specifika, která si vynucují kompetentní strůjce integrovaného systému řízení modifikovat návrhy mezinárodních norem. Normy sice vlastní celosvětovou působnost, ale zvláštnosti individuálních organizací, podniků, zemí a kultur musí vyjádřit místní specialisté.

Účinnost pak prezentuje metody jak vykonávat věci správným způsobem. Je měřena zevnitř životního cyklu buď prvky ISMS, nebo ISMS jako celku a to obvykle soustavou indikátorů.



Obrázek 1 Princip Demingova PDCA modelu

1.1 Modul Plan, Do ,Check a Act

1.1.1 1. etapě životního cyklu - PLAN

Obsahem této části je:

- Vymezení cílů prvků ISMS a určení metod, způsobů a pracovní postupů a jejich měření
- Vymezení indikátorů pro měření dosažení met
- Stanovení indikátorů pro měření činnosti komponentů
- Stanovení podoby sbírání dat pro vyhodnocování činnosti prvků a pro vyhodnocování dosažení jejích záměrů
- Stanovení náležitých organizačních struktur, zodpovědných osob za sbírání dat a za vyhodnocování účinnosti komponentů ISMS
- Koncept oprávnění a vymezení reportovacích závazků těmto organizačním strukturám.

1.1.2 2. etapě životního cyklu - DO

- Uskutečnění navržených organizačních struktur v soustavě řízení organizace počítaje v to prosazení jejich kompetencí, ručení a reportovacích povinností
- Implementace požadovaných kvantit a indikátorů do systému řízení organizace
- Nastavení postupu jejich pozorování a zabezpečení transferu příslušných dat příslušným organizačním strukturám.

1.1.3 3. etapě životního cyklu - CHECK

- Určení počátečních prvotních hodnot sledovaných indikátorů, které vymezují startovací nastavení systému měření účinnosti prvků
- Podpora činnosti náležejících organizačních struktur zodpovědných za vyhodnocování efektivity prvků ISMS.
  [1]

1.1.4 4. etapě životního cyklu - ACT

- Uskutečnění nápravných opatření a preventivních činností, etablovaných na bázi vyhodnocení provedených vedením organizace
- Stálé zlepšování ISMS.

Složkou modelu PDCA je i dokumentace kterékoliv jeho fáze. Dokumentace je mnohdy chápána jako nejobtížnější a nejnepříjemnější prvek implementace integrovaného systému řízení. V okruhu zachování nestrannosti hlediska na model PDCA a integrovaný systém řízení je nezbytné podtrhnout, že dokumentace je jednou ze zásadních dílů celého modelu PDCA. Aby bylo uskutečnitelné realizovat jakýkoli reengineering libovolných procesů, je nevyhnutelné dodržet zásady procesního řízení. To v praxi znamená:

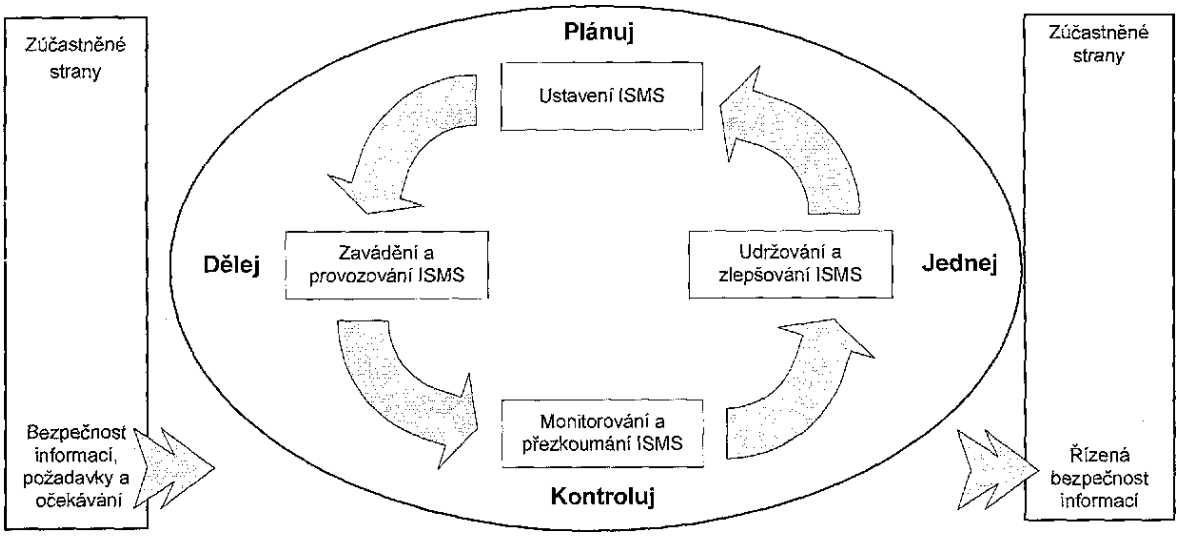
- Identifikovat procesy [4]
- Procesy popsat a zdokumentovat [4]
- Na základě dokumentace procesy řídit [4]
- Následná optimalizace průběhu [2]

1.2 Model PDCA v ISMS

Vztah a provázanosti modelu PLAN, DO, CHECK, ACT s systémem řízení bezpečnosti informací je velmi blízký a provázaný. Dle plánu PDCA je systémové řízení bezpečnosti informací také rozloženo (viz následující obrázek a tabulka).

Tabulka 1 Vztah PDCA a ISMS

PDCA	ISMS	Popis pro ISMS
PLAN	Ustavení ISMS	Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
DO	Zavádění a provozování ISMS	Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
CHECK	Monitorování a přezkoumání ISMS	Posouzení, kde je to možné i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
ACT	Udržování a zlepšování ISMS	Přijetí opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.



Obrázek 2 Provázanost modelu PDCA s ISMS [8]

2 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

V dnešní době se žádná organizace nemůže obejít bez řízení bezpečnosti informací. Bezpečnost je stala nedílnou součástí každodenního řízení a vnitřní kultury organizace. Abychom byli schopni řízení bezpečnosti cíleně a efektivně rozvíjet, je potřebné na tento prvek řízení pohlížet jako na systém řízení bezpečnosti informací.

„Systém řízení bezpečnosti informací ISMS je část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informaci.“ [8]

Model PDCA je elementárním prvkem, na kterém je založen nejen systém řízení bezpečnosti informací. Pomocí tohoto modelu je tento systém vnímán jako čtyři etapy systému řízení:

1. **Ustanovení ISMS:** první etapa má za cíl zpřesnění hranic a rozsahu řízení bezpečnosti. Tato etapa na základě ohodnocení rizik stanovuje jasné manažerské zadání a podává podklad jak vybrat nezbytná bezpečnostních opatření.
2. **Zavádění a provoz ISMS:** ve druhé etapě se udává systematické a efektivní implementace vybraných bezpečnostních opatření.
3. **Monitorování a přezkoumání ISMS:** během této etapy se pozoruje zejména zpětná vazba a zajišťuje se pravidelné sledování a ohodnocování dostatečných i neuspokojivých prvků řízení bezpečnosti informací.
4. **Údržba a zlepšování ISMS:** V poslední etapě bylo za cíl určeno vyhodnocení a následná realizace všech možností zlepšování systému nebo nalezení a napravení zjištěných chyb a nespojujících prvků.

Pro popis všech části ISMS je obsažen normami ISO ČSN 27001.

ISO ČSN 27001 je norma, která má podobu hlavních nároků a požadavků. Závaznost daného požadavku umístěného v normě upřesněno výrazem „**musí**“. Tím je zajištěna zřetelná závaznost dané podmínky. Podmínky této normy tvoří postup, kterým se vytváří model PDCA. Tyto podmínky dohromady tvoří propracovaný systém. Shoda s normou ISO IEC 27001 je podmíněna splněním všech daných závazků a podmínek. [2]

2.1 Ustanoveni ISMS

Ustanoveni ISMS je první etapou pro její tvoření. V této etapě se upřesňují formy řešení bezpečností informací, které jsou adekvátní k danému problematice. Jejím obsahem je nejen rozsahová definice ISMS ale také schválení Prohlášení o politice ISMS, což je závazek pro udržování a dotování informační bezpečnosti v adekvátním stavu. Dále sem náleží provedení analýzy rizik a výběr vhodných bezpečnostních opatření, kterými se snižují vlivy reálných rizik, což jsou kritické činnosti. Zavedením ISMS, které bylo schváleno vedením podle požadavků (zjištěných při analýze zvládaní rizik) na bezpečnost organizace, se zakončuje tato etapa.

Ustanovení ISMS se rozděluje na následující skupiny činností:

- definice vazeb, rozsahu a hranic ISMS
- definice a odsouhlasení Prohlášení o politice ISMS,
- zvládání rizik a analýzy:
    - definice přístupu organizace k hodnocení rizik,
    - identifikace rizika včetně určení aktiv a jejich vlastníků,
    - analýza a vyhodnocení rizik
    - identifikace a ohodnocení variant pro zvládání rizik
    - výběr cílů opatření a jednotlivých opatření pro zvládání rizik
- souhlas vedení organizace s navrhovanými zbytkovými riziky a se zavedením ISMS, příprava Prohlášení o aplikovatelnosti.

Tato etapa zanechává významné důsledky na další tvoření a fungování ISMS během následného životního cyklu až po jeho ukončení.

[1]

2.1.1 Definice rozsahu a hranic ISMS

Mezi prvními úkoly při řízení bezpečnosti patří popsání a zpřesnění hranic a rozsahu ISMS. Používaná organizační struktura, charakteristické činnosti a cíle organizace, umístění důležitých lokalit a technologie pro přenos a zpracování informací jsou v rámci této části ISMS důležité prvky. Z výše zmíněných základních informací je už možno lépe stanovit výchozí rozsah a hranice ISMS. Tento rozsah nemusí vždy obsahovat celou organizaci.

V úhlu pohledu posazování ISMS po praktické stránce je možné se k identifikování rozsahu přiblížit dvěma rozdílnými způsoby. První rozsáhlejší způsob rozsahu ISMS musí být už začátkové fázi stejně velký, jako je rozložení celé organizace. Že řízení už od začátku řeší bezpečnost informací v rámci celé organizace je zde evidentní výhodou. Stinnou stránkou tohoto způsobu je výrazné zvýšení nákladů a investic z úhlu pohledu spotřeby financí a zdrojů. Další nevýhodou může být, že ne všechny očekávané a plánované přínosy řízení bezpečnosti jsou na konec realizovány. Pro evoluci bezpečnosti tento způsob bývá v mnoha případech spíše na škodu. Další způsob určení rozsahu a hranic ISMS je omezit ho na počátku a při aplikaci pohlížet pouze určitou před-definovanou část vedené organizace. Nejčastějším případem bývá ucelený informační systém. Je lepší spíše vybrat takovou část organizace, ve které se často zavádějí novinky nebo se vkládají jiné operace s informacemi.

Zaměření na organizaci jako na dílčí celky muže být významnou výhodou, a to díky možnosti se zaměřit větší měrou na zvolené oblasti. To znamená, že v omezeném rozsahu se mohou být lépe zvládnutelné dva nelehké úkoly. Prvním úkolem je obhájit potřebu a účel systematického řízení bezpečnosti. To se nesmí brát jako samozřejmost. Výhodou je představeni pozitivních znaků na základě praktické zkušenosti.

Důsledné zvládnutí všech požadavků ISMS při praktické implementaci je cílem druhého úkolu. Důležité je vymezení, jak reálně funguje organizace a jaká její kultura. Zde se klade důraz na volbě účinných a správných způsobů pro prosazování ISMS. Tento úkol bývá komplikovaný i pro osoby bohatými a letitými zkušenostmi. Proto je dobré ověřovat a kontrolovat, jak probíhá aplikace teoretických pravidel v reálných situacích. Mezi největší rozdíly, mezi teoriemi a realitou, patří reálné odchylky, rozličnost osobních a skupinových zájmů, koncepční nedostatky, drobné chyby a jiné nepředvídatelné negativní události. Při zmenšeném rozsahu definice ISMS, tak se minimalizují výše zmíněné negativní dopady, entropie a nepochopení zadavatele ISMS.

Důležitou informací je, že implementace ISMS je o důvěře a schopnosti sdílet znalosti a zkušenosti, než schopnosti jednotlivců. Na základě sdílení zkušenosti a poznatků se potom může lépe rozvíjet řízení bezpečnostní činnosti.

Důležitou skutečností stanovení rozsahu je výhoda zkrácení cyklu PDCA počátečních fázích. Zkrácením této periody tak, že cyklus se opakuje rychleji, ve výsledku přinese více informaci a poznatků. Tím to způsobem se lze během realizace koncentrovat na menší bezpečnostní okruhy.

[1]

2.1.2 Prohlášeni o politice ISMS

Dalším krokem je definovaní Prohlášení o politice ISMS. Specifické potřeby organizace definují Prohlášení o politice. Důležité praktické vlastnosti této politiky:

- Upřesnění jakých cílů má ISMS dosáhnou, definice rámce řízení bezpečnosti informaci a jejich základní směr
- Srovnání požadavků a cílů organizace se všemi spojenými zákonnými, smluvními a regulativními podmínkami
- Zavedeni vazeb, které jsou důležité pro vytvoření a udržování ISMS pro danou organizaci
- Definice kritérii pro popis a ohodnocení rizik
- Schválení vedením organizace

Prohlášení o politice ISMS je nedlouhý dokument, který je velmi významný. Tento dokument předkládá zájem vedení organizace o řízení bezpečnosti informací a udává hlavní podmínky pro

hodnocení rizik. Při prosazování pravidel a požadavků na bezpečnost informací v organizaci může napomoci dobře definované Prohlášení o politice.

[1]

2.1.3 Pravidla a postupy řízení rizik

Mezi klíčové nástroje pro systematické řízení bezpečnosti informací řadíme řízení rizik. O výběru a prosazení optimálních bezpečnostních opatření rozhoduje přesná znalost skutečných rizik. Tyto opatření pak umožnují snížit negativní účinky těchto rizik. Efektivitu pak zaručuje přesné a adekvátní znalosti bezpečnostních rizik. Díky kterým se pak účinně využije úsilí při prosazování bezpečnostních opatření. Základem pro každý systém řízení bezpečnosti informací a důležitým faktorem, který ovlivňuje efektivitu funkčnosti daného ISMS, je řízení rizik. S danou problematikou je pro vázána níže zmíněná terminologie.

[1]

Řízení rizik (Risk Management) — koordinované činnosti sloužící k řízeni a kontrole organizace s ohledem na rizika [5]

Hodnoceni rizik (Risk Assessment) — celkový proces analýzy a vyhodnoceni rizik [5].

Analýza rizik (Risk Analysis) — systematické používání informaci k odhadu miry rizika a k určení jeho zdrojů [5]

Vyhodnocení rizik (Risk Evaluation) — proces porovnáváni odhadnutého rizika vůči daným kritériím pro určeni jeho významu [5]

Zvládáni rizik (Risk Treatment) proces výběru a přijímání opatření pro změnu rizika [5]

Akceptace rizika (Risk Acceptance) rozhodnutí přijmout riziko [5]

2.1.3.1 Teorie analýzy a řízení rizik

Řízení a analýza bezpečnostních rizik, je pro vrcholové vedení organizace základním nástrojem. Tento nástroj se využívá k ochraně investic, které jsou vložené do informačních systémů a také se vkládají na podpoření základních procesů organizace. Provedení procesů se samo o sobě rozlišuje podle hloubky a podrobnosti možných řešeni. Možná řešení jsou:

- **Nereagovat.**
- **Neformální přistup:** Analýza se provádí bez předem připravených postupů.
- **Základní přístup:** Používají se rámcově zpracované dokumenty a využívá se celková koncepce bezpečnosti informací.
- **Detailní přistup:** Podrobně se provádí analýza všech rizik a to podle dopředu plně nadefinované soustavy metodických postupů.
- **Přistup kombinovaný:** Část rizik se analyzuje do podrobného detailu a druhá část se záměrně pomíjí.

Varianta nereagovat na daný problém, tedy přijmout riziko o neznámém možném dopadu na organizace v moderním pojetí řízení bezpečnosti informací by mohlo mít nedozírné následky. [1]

2.1.3.2 Určení metody pro hodnocení rizik

Hlavním účelem tohoto kroku je jednoznačné stanovení kritérii pro hodnocení a akceptaci rizik. O tyto kritéria se značně opírá systém hodnocení a řízení rizik organizace. V tom to bodě je důležité rozhodnutí organizace o přesném znění metody pro výpočet rizika a výběr vhodného nástroje. Ve stejném momentu je důležité nadefinovat stupnice pro ohodnocení veličin, které budou určující pro řízení rizik. U takovéto stupnice je potřeba nadefinovat pro:

- Míry důvěrnosti aktiv.
- Míry integrity aktiv.
- Míry dostupnosti aktiv.
- Míry dopadů a škod.
- Pravděpodobnosti uplatnění hrozby.
- Pravděpodobnosti selhání využívaných bezpečnostních opatření
- Stupnice pro vyjádření rizik a hladiny přijatelnosti rizika.

Tyto veličiny, pravděpodobnosti a stupnice prezentují reálné hodnoty ke všem jednotlivým parametrům rizik. Rozhodovací procesy tak mají k dispozici podklady související se řízením rizik. [1]

2.1.3.3 Identifikace a ohodnocení aktiv ISMS

Identifikace všech aktiv a určení jejich významu pro běh organizace, je jedním z důležitých kroků pro řízení rizik. Aktiva ISMS se rozdělují na dvě výchozí skupiny:

- **Primární aktiva**: Jsou z většiny tvořena nehmotnými aktivy. Patří sem pro organizaci důležité informace, aktivity a funkční procesy organizace, u kterých je požadavek na zajištění jejich zabezpečení.
- **Sekundární aktiva:** Z většiny tvořena hmotnými aktivy. Do této skupiny započítáváme komunikační infrastrukturu, technické a programové vybavení, organizační struktury. Zahrnují se zde i pracovníci, jejichž činnost se projevuje na životaschopnost organizace.

Pro popis každého identifikovaného aktiva je nutnost vyjádřit míru jeho integrity, dostupnosti a důvěry. Primární aktiva, která jsou důležitá pro řízení rizik, odrážejí nutnost organizace hlídat zajišťování a ochranu informací. Sekundární aktiva a jejich identifikace a ohodnocení tvoří významnou část pro zvládání rizik a rozhodovacích procesů při hodnocení rizik. A to hlavně z důvodu možnosti lépe zajistit informace pro optimální vyjádření bezpečnostního požadavku.

Pro zjednodušení a lepší orientaci je pro další fázi lepší vhodně seskupit do skupin identifikovaná aktiva. A to v rámci hodnocení.

[]1

2.1.3.4 Zvládání rizik ISMS

Problematika vhodné zvolené formy návrhu patří do závěrečné části. Zde se vybírají vhodná bezpečností opatření a to na základě zjištěných bezpečnostních priorit a potřeb. Tyto opatření pak následně umožňují eliminaci zjištěných rizik. V pokud to bude situace vyžadovat, existuje možnost doplnit bezpečnostní opatření i mimo rámcový koncept obecných doporučení. [3]

2.1.4 Prohlášení o aplikovatelnosti

Dokument, který vyjadřuje dokumentované prohlášení podávající popis cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace. Dokument „Prohlášení o aplikovatelnosti" musí obsahovat následující:

- Cíle opatření a jednotlivá bezpečnostní opatření vybrané a důvody pro jejich výběr;
- Cíle opatření a jednotlivá bezpečnostní opatření, která jsou již v organizaci implementována;
- Vyřazené cíle opatření a jednotlivá vyřazená bezpečnostní opatření uvedená v příloze A, včetně zdůvodnění pro jejich vyřazení.

Prohlášení o aplikovatelnosti skýtá shrnutí rozhodnutí, kterým postupem bude naloženo s identifikovanými riziky. Odůvodnění pro vyřazení cílů a individuálních opatření umožňuje regresívní dozor, zda nebyly odstraněny chybnou úvahou.

[1]

2.1.5 Shrnutí etapy ustanovení ISMS

Etapa ustanovení ISMS je významnou etapou při vytváření ISMS. Tato etapa definuje základní vztahy celého systému řízení bezpečnosti informací. Zásadní nevýhodou je fakt, že výstupní informace z této části se přenáší do následných etap ISMS. Následky této etapy mají dlouhodobý vliv a v mnoha případech se pak později mohou objevit v dříve nepředpokládaných souvislostech. Provádění zpětných změn je podstatně náročnější a většinou i vyžaduje vyšší investiční a finanční náklady.

Rizika ISMS podávají míru, která popisuje do jakého stupně je možnost uspokojit požadavky ISMS. Zde se nachází více úhlů pohledu na danou problematiku. V prvním úhlu pohledu je možné riziko obejít, pak se změní potřeby ISMS. Tyto potřeby se změní tak že sníží dopad míněné hrozby nebo se upraví pravděpodobnost výskytu hrozby. Další možností zvládání rizik je přenesení rizika. Při tomto přenesení se změní rozsah a to z důvodu doplnění subjektu, na který je dané riziko přeneseno. Nejčastější se volí taková forma zvládání rizik, která je vhodně aplikovatelná jako bezpečnostní opatření. A to má vliv na snižování zranitelnosti daného rizika. Další možností, jak zvládat rizika, je akceptace rizika. To je poslední krok a poslední možný konečný stav, který zvládaní rizik nabízí. V této formě se mohou nacházet zbytková rizika a tyto rizika by se neměla opomíjet.

V poslední fázi plánování je potřeba se zaměřit na získání souhlasu vedoucí osob organizace s danými opatřeními a zbytkovými riziky.

[1]

2.2 Zavádění a provoz ISMS

Další etapa životního cyklu ISMS je zaměřena na uskutečnění veškerých bezpečnostních opatření. A to tak jak tato opatření byla navržena v předchozí etapě. Významná část pak připadá na přípravu dílčích plánů, které obsahují seznamy odpovědných osob a přesné termíny. Vytvoří se dokument Příručka bezpečnostních informací, ve které bude zdokumentována bezpečností opatření a vysvětlené bezpečnostní principy pro uživatele a manažery. V této etapě zavádění ISMS se klade důraz na činnosti:

- Formulace dokumentu plánu na zvládání rizik a postupné jeho zavádění.
- Definice programu pro vytváření bezpečnosti a zavádění se školením všech uživatelů, kteří se mohou dostat do styku s programem.
- Upřesnění způsobu měření efektivity bezpečnostních opatření a sledování stanovených ukazatelů
- Zavadění postupů a jiných opatření alarmující a reagující na bezpečnostní incidenty.
- Řízení zdrojů, záznamů a dokumentů ISMS.

[1]

2.2.1 Plán zvládaní rizik

Důležitý dokument, který popisuje veškeré činnosti ISMS, se nazývá plán zvládání rizik. Popisované činnosti jsou nutné pro stanovení cílů, řízení bezpečnostních rizik a nastavení priorit těchto činností ISMS. Jedním z hlavních a velmi důležitých prvků, je ustanovení osobní zodpovědnosti za kontrolu a uvádění daných plánovaných činností. Osobní odpovědnost musí být jednoznačně určena.

Základním výchozím bodem pro sestavení plánů zvládaní rizik, jsou dva základní zdroje informací o ISMS. V počátku fáze se tím to míní podkladovou část, která vychází ze ustanovení ISMS. Jmenovitě se jedná o výsledky řízení rizik, které jsou popsány ve zprávě hodnocení rizik. Tento dokument určuje míru realizace bezpečnostních potřeb. Potřebné zlepšení činnosti ISMS se definuje na základě rozdílu mezi potřebami a skutečným stavem bezpečnostních opatření.

Následujícím neméně významným zdrojem dat, která jsou důležité pro tvorbu plánů zvládání rizik, jsou údaje získávané pří periodických kontrolách ISMS vedením

organizace. Tyto údaje se shromažďuji do zprávy o stavu ISMS. Dané informace umožňují do plánu zvládaní rizik skloubit získané postřehy s fungováním ISMS.

V praktickém úhlu pohledu je doporučováno do plánu zvládání rizik implementovat činnosti, vedoucí k minimalizaci bezpečnostních rizik. Při této implementaci, bude očekávaná nevýhoda, kterou je seznam dílčích aktivit nebo sumou činností. Tyto činnosti ale se snižování rizik souvisí. Také je doporučené do tohoto plánu implementovat pro ISMS rutinní činnosti ale které jsou dány normou ISO ČSN 27001. Při realizaci plánů o zvládání rizik se nesmí opomíjet reálný fakt, že o všech podkladech by měli být zanechávány záznamy.

[1]

2.2.2 Příručka bezpečnosti informací

Během procesu prosazení zvolených bezpečnostních opatření je nutné nadefinovat a ustanovit bezpečnostní pravidla a kompetence, které jsou s tím provázené. Definice a ustanovování bývají prováděny za prostřednictvím dokumentů, jako jsou bezpečnostní politiky či bezpečnostní směrnice, které vymezují dlouhodobě závazné bezpečnostní zásady, předpisy, podstaty a zodpovědnosti, které jsou souhrnně pojmenovávány jako Příručka bezpečnosti informací.

Během vytváření této bezpečnostní dokumentace se vyskytne nutnost pro diferenciaci úrovně důležitosti dokumentů. Nejvyšší úroveň zaujímají dokumenty, vyžadující systém řízení a bez kterých by nemohla být naplněna implementace ISMS. Jsou to například rozsah ISMS, bezpečnostní politika ISMS, prohlášení o aplikovatelnosti a plán na zvládání rizik. Dané dokumenty mají své zvláštní postavení v systému a tomuto postavení se musí podřizovat i forma jejich zpracování.

V další úrovni se nachází dokumentace, která poskytuje podporu při prosazování ISMS a podmínkou její adaptování odpovídajícímu ISMS. Dokumenty na této úrovní bývají obsahem příručky bezpečnostních informací. Významným prvkem při vytváření této dokumentace je definování dílčích procesů a metod, které obstarávají úspěšnou aplikaci jednotlivých bezpečnostních opatření. Zde je hlavní nutnost nadefinovat kompetentní osobu, zabezpečený systém, servisní a kontrolní intervaly, místo určení a následná reakce na incident.

Poslední a nejnižší úroveň bezpečnostní dokumentace je velké části tvořena pracovními postupy. Nezbytné úkony pro naplnění jednotlivých procesů by měly být podrobně popsány a vysvětleny tomto dokumentu. Tato úroveň není nezbytně nutná. Ve většině případů bývá řešena odkazem na jinou dokumentaci pro použití technických systémů.

[1]

2.2.3 Prohlubování bezpečnostního povědomí

Prvkem, který bývá označován při implementaci ISMS jako jeden z nejdůležitějších, udržování kontaktu s bezpečnostní realitou. U tohoto prvku je možné upravit či obejít všechny dřívější definovaná pravidla a metody a to s cílem reakce na reálné chování všech kompetentních osob. Jedná se o lehce pojmenovatelný cíl ale s velmi těžkým provedením úkolu, který požaduje značné a systematické snahu. Rozvoj ISMS vyžaduje nutnost pravidelných obměn kompetentních osob organizace. To je trvalý a nikdy nekončící proces, který bývá označován za jeden z rozhodujícího faktoru efektivity ISMS.

Aby nedocházelo ke ztrátě či zveřejnění přístupových hesel běžných uživatelů, je nutné všem těmto uživatelům srozumitelně definovat bezpečnostní principy a metody, obeznámit je bezpečnostními riziky tak, aby vhodně a včasně byli schopni reagovat na vzniklé stavy, které nejsou zahrnuty v dokumentaci a prodiskutovávat s nimi bezpečnostní incidenty a vysvětlovat jim jejich původ s reálnými a potenciálními důsledky. Tomuto se dá předejít systematickou komunikací po případě školením. Tím je možné zvýšit bezpečnostní odolnost nejslabších článků, kterým budou vždy lidští aktéři se svými nepředvídatelnými projevy.

[1]

2.2.4 Měření účinnosti ISMS

Měření účinnosti aplikovaných bezpečnostních opatření je dalším důležitým tématem. Toto téma se spojuje s prosazováním bezpečnostních opatření. Pokud jsou definovány a pravidelně sledovány objektivní údaje o reálné funkčnosti systému řízení bezpečnosti, vytváří se pevný výchozí bod pro provádění všech důležitých rozhodnutí. [4]

Již etapa plánování rozhoduje, jak v reálu bude účinnost účelná. Kvalita navrženého ISMS je bezprostředně definována kvalitou vstupní analýzy rizik, která probíhá v etapě plánování. Vrcholové vedení organizace svým přístupem a kompetencemi významně ovlivňuje účinnost celého navrhovaného ISMS. Důležité je neopomenout žádné další zákonné nebo případně normované úpravy, které je organizace vázaná se řídit a které upravují strategická rozhodnutí této organizace. V určitých případech se může jednat o speciální požadavky a volby vlastníků dané organizace.

Důsledky a případné dopady chyb, ve specifikaci ISMS plánu PDCA , s vyjádřenou úrovní relativních výloh, které jsou svázané i s jejich odstraňováním, jsou uvedeny v přiložené tabulce.

[1]

Tabulka 2 Rozložení zdrojů v rámci modulu PDCA[1]

Etapa PDCA modelu	Úroveň relativních výloh v %
Plánuj	1
Dělej	6,5
Kontroluj	15
Jednej	100

Do první etapy, nazvanou **PLAN**, je uskutečnitelné shrnout hlavní aktivity do následujících bodů:

- Zajištění shody stému měření účinnosti s celkovým systémem řízení organizace.
- Návrh celistvého konceptu měření účinnosti ISMS v organizaci.
- Navržení rázu a techniky vlastního měření účinnost ISMS
- Určení projektů vycházejících z analýzy rizik, které ve výsledku slouží k uskutečnění bezpečnostní politiky a určení jejich priorit pro uskutečnění.
- Návrh indikátorů pro měření účinnosti ISMS a definice způsobu a periodicity jejich kalkulace.
- Stanovení cesty pro sběr dat k individuálním indikátorům, vyhodnocování, reportování a určení osob, které budou s nimi pracovat.
- Specifikace eventuálních vazeb se systém měření a vyhodnocování informatiky v organizaci.

Ve Druhá etapě, nazvané **DO**, se provádí uskutečňování projektů. V této části se zapojují projektoví manažeři, kteří zodpovídají za chod systému řízení účinnosti. Nejvýznamnějším úkolem je zajištění integraci systému pro monitoring dat pro vyhodnocování efektivnosti do celého monitorovacího systému organizace.

Ve třetí etapě, nazvané **CHECK**, se doporučuje týmu, který připravuje řízení účinností ISMS, držet se následujících bodů:

- Definice výchozích kvality indikátorů měření účinnosti ISMS.
- Testování systému měření.
- Uskutečňování vlastního sběru dat a monitoring ISMS v chodu svého cyklu.
- Sběr podkladů pro průběžný audit ISMS.

V konečné etapě, nazvanou **ACT**, se zajišťuje trvalý vývoj ISMS a varianty pravidelných upgradů, které jsou založeny na bázi zjišťování výsledků z předchozí etapy. Praktická realizace systémové zpětné vazby je hlavním cílem této etapy.

Dalším úkolem této etapy je vyhodnocovat jednotlivé složky ISMS a nálezní způsobu, jak tyto složky ohodnocovat indikátory. Principiálně se vyskytuje možnost užití dvou základních indikátorů:

- Indikátory vyjádřené číslem.
- Indikátory popisující průběh procesu.

Snižování investic, navyšování zisku, nárůst produktivity, zkracování doby životního cyklu nebo snižování rizika jsou procesy, které jsou popisovány indikátory vyjádřené numerickou hodnotou. Pro způsob popisu dat, popis implementace a integrace do řídicích procesů slouží procesní indikátory. Z důvodu občasné podobnosti a často úzké sprovázanosti indikátorů obou typů, vzniká poslední době mezi manažery trend časté kontroly těchto indikátorů s vytyčenou metou eliminace aktivit a procesů nepřinášející svým trváním žádnou přidanou hodnotu.

[2]

Ukázky indikátorů:

- **Účinnost bezpečnosti informací** (Information Security Effectiveness) - rozsah, ve kterém působení bezpečnosti informací naplňuje cíle organizace. [7]
- **Míra** (Measure) - jeden nebo více ukazatelů a souvisejících výkladů, které určují informační potřebu. [7]
- **Měření** (Measurement) - proces získávání informací o účinnosti ISMS a bezpečnostních opatření, dosažení cílů bezpečnostních opatření a výkonnosti procesů ISMS, který využívá metody měření, funkce měření, analytický model a kritéria do rozhodování. [9]

Sled události vychází z bodu řízení rizik jakožto stavebním kamenem nejen pro řízení bezpečnosti, ale ukazatel priority měření. Posléze se nalézá podmínka nastavení vhodných metod měření. Tyto metody měření pomocí indikátorů napomáhají rozhodovacím procesům v systému řízení bezpečnosti. Vše ovšem vychází ze strategických potřeb organizace.

Měřící indikátory bezpečnosti informací je možné rozdělit, dle svého oboru, do následujících výchozích skupin

• Finanční indikátory

• Personální indikátory

•Technické indikátory, popisující provoz informačních systémů.

[1]

Tabulka 3 Ukázka technických indikátory IS [1]

Indikátor	Co měří	Výstupní jednotka
Čas nedostupnosti služby/ celkový čas provozu systému	Měří nedostupnost služeb IS	Procento času nedostupnosti služby
Počet bezpečnostních incidentů způsobených nedostatečným školením/ Po-čet všech bezpečnostních incidentů * 100	Měří efektivnost školení bezpečnosti informací.	Sleduje se v procentech zjištěných incidentů.
Počet subsystémů chráněných před škodlivým kódem/počet všech ohrožených subsystémů * 100	Měří ochranu před škodlivým kódem.	Sleduje se v procentech ochrá-něných subsystémů.
Počet pracovních stanic s ochranou firewallem/ Počet všech pracovních stanic * 100	Měří rozsah implementace firewallu v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou firewallem/ Počet všech serverů * 100	Měří rozsah imple-mentace firewallu v organizaci	Sleduje se v procentech ochráněných serverů
Počet pracovních stanic s ochranou proti spamu/ Počet všech pracovních stanic * 100	Měří rozsah ochrany proti spamu v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou proti spamu/ Počet všech serverů * 100	Měří rozsah ochrany proti spamu v organizaci.	Sleduje se v procentech ochráněných serverů.
Počet pracovních stanic s ochranou proti spywaru/ Počet všech pracovních stanic * 100	Měří rozsah ochrany proti spywaru v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou proti spywaru/ Počet všech serverů * 100	Měří rozsah ochrany proti spywaru v organizaci.	Sleduje se v procentech ochráněných serverů.
Počet pracovních stanic s ochranou proti nežádoucí útokům/ Počet všech pracovních stanic * 100	Měří rozsah ochrany proti nežádoucím útokům v organizaci.	Sleduje se v procentech ochráněných pracovních stanic.
Počet serverů s ochranou proti nežádoucím útokům / Počet všech serverů * 100	Měří rozsah ochrany proti nežádoucím útokům v organizaci.	Sleduje se v procentech ochráněných serverů.
Počet bezpečnostních incidentů v určité oblasti.	Měří počet incidentů v určité oblasti IS	Číslo, udávající počet bezpečnostních incidentů.
Počet bezpečnostních incidentů/Počet uživatelů v oblasti	Měří počet bezpečnostních incidentů na jednoho uživatele IS.	Číslo, udávající počet bezpečnostních incidentů.
Počet subsystémů s plány na obnovu a se scénáři nouzového provozu/Počet všech subsystémů * 100	Měří zajištění organizace pro případ nenadálého výpadku systému.	Sleduje v procentech části systému, které mají scénáře pro nouzový provoz a svoji obnovu.
Počet subsystémů podléhajících archivaci /Počet všech subsystémů * 100	Měří zajištění organizace pro případ zničení dat a programového vybavení.	Sleduje v procentech části systému, které jsou v organizaci archivovány.

2.2.5 Řízení provozu, zdrojů, dokumentace a záznamů ISMS

Závěrečným bodem etapy zavádění ISMS je provedení všech činností a to řízeným způsobem. V této části není dostatečné jen dodržovat postup dle nadefinovaných pravidel, ale v tomto bodě je nutné hromadit informace pro nadcházející fázi nazvanou monitorování, a proto tato část nepatří jednoduchým. Zde je velmi nutné dobře vytvořit nadefinovat pravidla pro tvoření, distribuci, aktualizování a akceptaci dokumentů řízení bezpečnosti a to pro umožnění kontroly relevantního fungování ISMS.

Záznam - dokument, ve kterém jsou uvedeny dosažené výsledky nebo ve kterém se poskytují důkazy o provedených činnostech, resp. jiné informace záznamového charakteru související se systémem řízení kvality [6]

Ve stejné době je potřeba produkovat záznamy o individuálně provedených operacích ISMS, kde se vyskytují základní údaje o provedené aktivitě. Na záznamu musí být identifikace osoby provádějící danou činnost, určení místa a času uskutečňování operace a výstup o provedené činnosti. Při tvoření výše míněných záznamů je potřeba dbát na fakt, aby existovala co nejméně komplikovaná možnost dohledání těchto záznamů.

Při řízeni zdrojů, je nezbytně nutné pozorovat, jak potřeby ISMS jsou pokryty adekvátním množstvím expertních zdrojů a jak účinně se řídí užívání zdrojů pro účinnost běhu ISMS. Tyto zdroje mohou být lidské, finanční, technické nebo znalostní.

Dalším nezbytně nutným požadavkem provozu je definování metod a nařízení pro řízení nahodilých příhod. Na dané události by měly být alarmováni příslušní pracovníci organizace. Tito pracovníci by měli používat zvláštní nástroje, které umožňují detekovat včas bezpečnostní incidenty a slabiny. Pak na základě prošetření dle definovaných nařízení a postupů, a to se samozřejmým zaznamenáváním postupu výsledku řešení. Tyto výsledky z výstupu bezpečnostních incidentů, by se měly uplatňovat pro zpřesňování hodnocení rizik a pro optimalizací definic.

[1]

2.3 Monitorování a přezkoumání ISMS

Zajišťování učiněné zpětné vazby je hlavním úkolem této etapy ISMS. V rámci zajištění této zpětné vazby se klade požadavek pro přezkoumání všech aplikovaných bezpečnostních opatření a následků ISMS. Skutečné ověřování počíná u přímé kontroly odpovědného personálu ze strany jejich vedoucích nebo bezpečnostního manažera. Důležitým prvkem je nezávislé posouzení funkčnosti a účinnosti ISMS prostřednictvím interních auditů ISMS. Všeobecným předpokladem všech používaných zpětných vazeb je příprava dostatečného množství podkladů o reálném fungovaní ISMS. Tyto vazby se posléze předkládají vedení za účelem přezkoumání, je-li zrealizování ISMS v souladu všeobecnými potřebami organizace. Průběhu této části implementace ISMS je nutnost provádět činnosti monitorování a ověřování účinnosti prosazení bezpečnostních opatření, provedení interního auditu ISMS. Náplně těchto činnosti pokrývají celý rozsah ISMS, připravují stavové zprávy ISMS a na základech těchto činností se přehodnocuje ISMS. [1]

2.3.1 Provádění kontrol ISMS

Výchozí zpětná vazba nezbytná pro funkčnost ISMS, je realizace kontrol ze strany všech prvků (osob) odpovědných a to na všech manažerských úrovních. Důležité je aktivně se podílet na dozoru kontroly splňování všech bezpečnostních podmínek. Posléze je důležité ujišťování se, jestli opravdu dochází ke splňování všech bezpečnostních opatření, náležící do jejich pravomoci, a jestli uspokojuje očekávání předem do nich vložená.

Včasná detekce chyb a zdařilých i nezdařilých pokusů o narušení bezpečnosti nebo včasná reakce na tyto podněty musí být součást kontroly ISMS. Pro tyto účely byl vytvořen termín zvládání bezpečnostních incidentů.

Do kontrolních aktivit patří také výsledné ohodnocení měření účinnosti ISMS a bezpečnostní opatření, které již byla aplikovány. Přehodnocování výstupu ohodnocení rizik na základě dřívějších poznatků z praktického běhu ISMS, vychází z podmětu, který podávají výstupy o měření účinnosti. Příslušné dokumenty a plány ISMS, musí být sjednoceny s aktualizovanými podněty daných aktivit.

[1]

2.3.1.1 Interní audity ISMS

Jedním z kritických prvků zpětné vazby je realizace interních auditů ISMS. Rozdíl mezi interním auditem a kontrolou je, že interní audity zabezpečují nezbytný nezávislí úhel pohledu na běh funkčnosti ISMS.

Audit (Audit) - systematický, nezávislý a dokumentovaný proces pro získání důkazu a pro jeho objektivní hodnocení s cílem stanovit rozsah, v němž jsou splněna předem stanovená kritéria [6]

Auditor (Auditor) - osoba s odbornou způsobilostí k provádění auditu [6]

Při přípravě auditů se nesmí opomenout skutečnost, že by interní audity měly být rovnoměrně rozloženy na celý rozsah ISMS a také při uvážení priorit, cílů rizikových částí ISMS. Oba tyto aspekty ISMS by měly být prověřovány audity ISMS. Prvním aspektem je nutnost dodržení procesních nařízení, kde nejdůležitějším kritériem auditu uskutečňování požadavku ISO ČSN 27001. Aspekt číslo dvě auditu ISMS je ověřování funkčního běhu jednotlivých opatření zavedených pro potřeby ISMS. U druhého aspektu je za hlavní kritérium určená uplatňující norma ISO ČSN 27002. Zde auditoři ověřují metodu, přiměřenost a míru realizace bezpečnostních operací aplikovaných v ISMS.

2.3.1.2 Přezkoumání ISMS vedením organizace

Impulzy a poznámky k ISMS obstarané během provádění monitoringu jsou významnými zdroji informací. Tyto zdroje pracují pro objektivní a efektivní přezkoumávání ISMS vedením organizace. Takovéto přezkoumávání pro dostatečnou efektivitu by mělo být prováděno v pravidelných dobách a největší hodnota intervalu by měla být jeden rok. U nově instalovaných ISMS, kde je optimální častější přehodnocování, tato doby bývá poloviční.

Přezkoumání (Review) - činnost prováděná k určení vhodnosti, přiměřenosti a efektivnosti předmětu přezkoumání k dosažení stanovených cílů [6]

Do vstupních informací pro přezkoumávání ISMS náleží všechny zásadní informace o běhu ISMS za celou hodnocenou periodu. Důležité je se zaměřit zvláště na tyto skutečnosti:

- Zpětné vazbě od zainteresovaných uživatelů a třetích stran.
- K existujícím slabinám a výstrahám, které mohly být při analýze rizik přehlédnuty.
- Důsledkům měření efektivity ISMS.
- Přeměnám, ovlivňující ISMS.
- Získaní doporučení pro další zlepšování ISMS.

Na bázi těchto podnětů dospívá k posouzení silných a slabých stránek nebo-li k SWOT analýze. Mezi výstupy SWOT analýzy náleží:

- Vylepšení efektivity ISMS (zvyšování míry bezpečnosti při snižování i ročnosti realizace bezpečnostních opatření).
- Aktualizování zhodnocení rizik a souvisejících plánů pro zvládání rizik.
- Nevyhnutelné úpravy procesů, zásad a metod ISMS.
- Plánovaná náročnost ISMS na zdroje (finanční, lidské, technologie apod.) v následujícím údobí.

Mezi nejčastější vyjádření přehodnocení ISMS je zpracování zprávy o stavu ISMS, kde musí být zahrnuty přínosy ISMS a zároveň analýzy části které optimálně nefungují a je třeba je zlepšit. Zpráva o stavu ISMS, která je nasměrovanou na budoucno, je výchozí bod pro uzavření kontraktu o prohlubování bezpečnosti. Definovat nové cíle pro další období a žádat vedení organizace o přidělení nových zdrojů jsou akty, které mohou být dosaženy pomocí této zprávy.

[1]

.

2.4 Údržba a zlepšování ISMS

Etapa nazvaná údržba a zlepšování ISMS je v životním cyklu implementace ISMS tou poslední etapou. Hlavním cílem je udržování a zlepšování chodu ISMS. V této fázi by mělo docházet ke sbírání pohnutek k vylepšení ISMS a k reformě všech nedokonalostí nebo rozporů, které se v ISMS vyskytli.

Průběhem tohoto úseku zavádění je nevyhnutelné realizovat následující aktivity:

- Zavádění identifikované potenciálnosti zdokonalení ISMS.
- Provedení příslušných opatření k opravě a preventivní opatření pro odstranění nedokonalostí.

Neshoda (Nonconformity) - nesplnění požadavku [5]

Náprava (Correction) - opatření pro odstranění zjištěné neshody [6]

Opatření k nápravě (Corrective action) - opatření k odstranění příčiny zjiště né neshody nebo jiné nežádoucí situace [7]

Preventivní opatření (Preventive action) - opatření k odstranění příčiny potenciální neshody nebo jiné nežádoucí potenciální situace [8]

2.4.1 Soustavné zlepšování ISMS

Navržení dokonalého systému řízení je při aplikaci v praxi velmi náročným úkolem. Dokonalý systém můžeme považovat za ideální plyn definovaný ve fyzice. Jeho vlastnosti jsou dobře definované, ale vytvoření podobného stavu je prakticky nemožné. Podobné je to s dokonalým systémem řízení. Do všech systémů by měla být zapracována efektivní zpětná vazba. Ta by měla umět získávat impulzy, které by jí pomáhaly se přiblížit dokonalému stavu. Taková to vazba musí mít schopnost odhalovat chyby s jejich důsledky a adekvátním způsoben na tyto důsledky odpovídat.

Jedním z podstatných prvků zlepšování je obzvláště užívání kladné zpětné vazby. Je potřebné, aby zlepšování ISMS mělo oporu o praxi činných aktérů. Tito aktéři by měli kompetentní osoby za ISMS instruovat o svých pohnutkách, které mohou fungování ISMS vylepšit. Myšlenky přicházející z reálné praxe jsou vždy nenahraditelné a jejich pečlivému zpracování by měla být poskytována velká ostražitost.

[1]

Osoby zodpovědné za ISMS by si stimulů, přicházejících od běžných pracovníků, měli vážit. Tím ale není myšleno, jen jejich nepromyšlená instalace. U všech stimulů je potřebné promyslet jejich přímé i nepřímé odezvy a následky pro organizaci a s tím spojená rizika. Řádné promyšlení následků někdy může znamenat zamítnutí či modifikovaní požadavku, což by mělo být příhodným postupem prodiskutováno s prvotním navrhovatelem.

Pro rozvoj ISMS je závažné i zvyšovat motivaci zaměstnanců na zúčastnění při všech aktivitách sjednocených s ISMS v tom, aby se dělit o své zkušenosti a aby neskrytě nabízeli, co je příhodné a žádané na chodu ISMS vylepšit.

[1]

2.4.2 Odstraňování nedostatků ISMS

Pro odstraňování nedokonalostí se vyskytují dvě formy opatření:

- Opatření k nápravě.
- Preventivní opatření.

Opatření k nápravě je reaktivní formou vyřešení nedokonalostí. V tomto případě se již nedokonalost nějakou cestou projevila a je nutnost na něj adekvátním postupem reagovat.

Vstříc tomu **preventivní opatření** je proaktivní formou řešení nedokonalostí ISMS. V daném řešení je východisko to, že se zjištěná nedokonalost se dosud neprojevila, ale další odročení jeho vyřešení by mohlo směřovat k tomu, že se v budoucnu nějaký incident objeví a vyvolá nebezpečnější problémy.

Významnou a nenahraditelnou složkou odstraňování nedokonalostí oběma postupy je explikace důvodů, které daným nedokonalostem podněcovaly. V daném smyslu je nedostatečné pouze zajistit opravu u určité neshody. Je významné se podílet na spojitosti a opatření uskutečňovat omezení eventuality opětování této nedokonalosti. Před prosazením obou typů opatření je též nevyhnutelné uvážit, zda vybrané opatření dostatečně zabrání repetici nedokonalosti a případně rozkryje jeho pohnutky.

[1]

Metody pro východisko opatření k nápravě a preventivních opatření musí být zdokumentovány a kterýkoliv aktivity s nimi sloučené musí být zaregistrovány a obsáhnuty v dokumentaci. Po instalaci opatření je též podstatné zkontrolovat, zda vybraná opatření opravdu zabezpečila očekávanou transformaci účinnosti ISMS. To se mnohokrát realizuje naprostou kontrolou či v případě kritičtějších nedostatků zvláštním auditem ISMS.

Faktické zkušenosti poukazují, že často nedoceňovanou příčinou nedostatků je neuspokojivá vědomost předpokladů, které ISMS požaduje. Obvyklým vyjádřením této příčiny jsou nezřetelnosti či nevědomosti spojitostí a vazeb mezi jednotlivými předpoklady. ISMS se stává komplexem jednotlivých operací, nikoli však systémem řízení. Je neobvyklé, že neuspokojivá zběhlost v ISMS je jako původ představován pouze výjimečně.

[1]

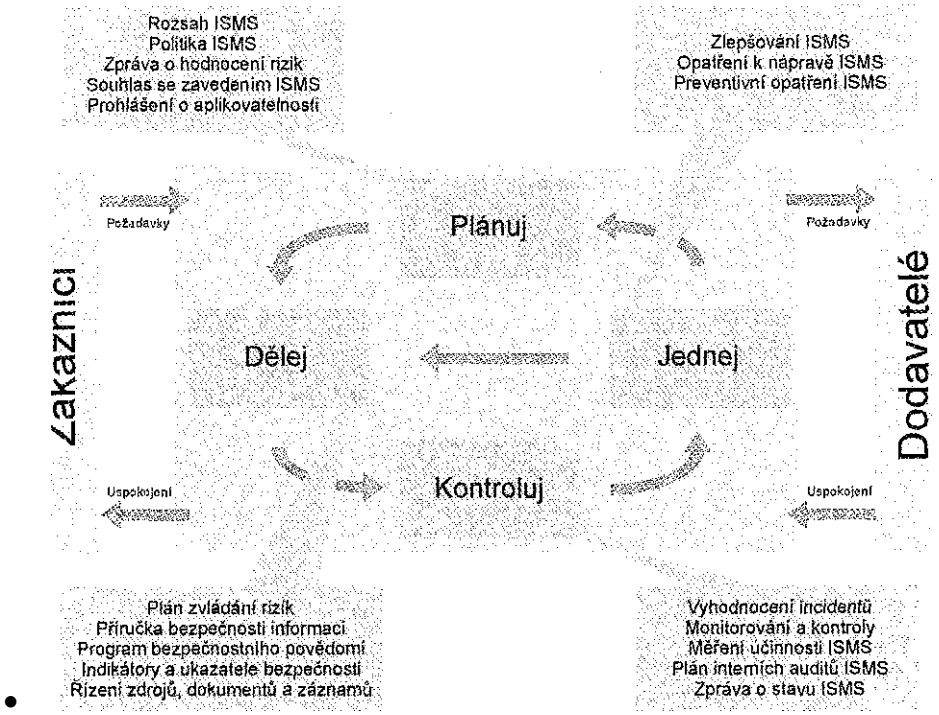
2.5 Shrnutí celého cyklu ISMS

Vyjma využití nového katalogu bezpečnostních opatření se konečné modifikace normy ISO ČSN 27001 koncentrovaly na následující oblasti:

Uplatnění přiměřených forem měření účinnosti ISMS - rozměr žádaných aktivit ve fázi implementace a chodu a při monitorování a ohodnocování ISMS je rozšířen o aktivity sloučené se zpřesněním příhodných indikátorů pro zjišťování efektivity implementace ISMS a o periodickém vyhodnocování získávaných dat.

- Posílení formálních spojitostí při vytváření ISMS - v některých případech došlo v novém textu normy k modifikaci nároků na postižení formálních vazeb při vytváření ISMS.
- Zvětšení obsahu prohlášení o aplikovatelnosti jako náplň tohoto zásadního dokumentu ISMS byl zvětšen o nezbytnost detekovat realitu, zda je dané bezpečnostní opatření již reálně implementováno. Tato realita je velmi prospěšná pro skutečné řízení bezpečnosti.
- Pravidelné aktualizování hodnocení rizik - jako složka ohodnocení ISMS správou organizace, které postupuje v cyklech s největší periodou 1 rok.

  [1]



Obrázek 3 Model PDCA pro řízení bezpečnosti informací [1]

Ze stanoviska faktických postojů k řízení a implementaci bezpečnosti jsou veškeré dané přeměny žádané a reflektují skutečné nezbytnosti. V počátečním případě je podstatné, že je nárok srovnávat a potvrzovat rozměr implementaci bezpečnosti, a to i se zřetelem na ekonomickou smysluplnost nasazení bezpečnostních opatření. V následujícím případě je pak snaha redukovat méně ztuhlé vstupy k východisku a více se zaměřovat na způsobilost ISMS ukazovat příčiny volby opatření. Úsilím je vložit do ISMS interní vazby, které vulgarizují pozdější modifikace systému. Třetí transformace pak do prohlášení o aplikovatelnosti vkládá i sdělení o stavu uskutečnění bezpečnostních opatření, což je pro vhodné rozhodování bezpečnostního manažera více než nutností. Konečná změna zdůrazňuje nezbytnost periodického překontrolování bezpečnostních rizik jako nutného prvku přehodnocení ISMS správou organizace. [1]

3 VYHODNOŤTE POŽADAVKY NA INFORMAČNÍ BEZPEČNOST DLE MODELU PDCA VE FIRMĚ BRABEC S.R.O..

3.1 Popis Brabec s.r.o

Firma Brabec s.r.o byla založena roku 1998, panem Alexandrem Brabcem jako společnost s ručením omezeným. Firma působí v oboru výroby plastových dveří, oken a jiných plastových doplňků pro dům z plastových profilů Shucco. Pro organizaci pracuje 10 zaměstnanců.

Obchodní firma (název), místo a PSČ, tel./ fax /e-mail, IČ:

- Brabec s.r.o.
- http://www.brabecplastsro.cz
- Kontaktní údaje:
- Adresa: J. Wericha 837, 675 71
- Telefon:+420 515 533 837
- Mobil:+420 774 710 731
- E-mail:abrabec@brabecsro.com
- IČ: 26274604

Zaměstnanci:

- Jednatel:
    - Ing. Alexander Brabec
- IT oddělení
    - Ing. Jiří Zátopek
    - Bc. Petr Štípek
- Obchodní oddělení:
    - Jan Vald
    - Petr Horňák
    - Daniel Kováč
    - Milan Lakomí
    - Tomáš Ondič
- Administrativní oddělení:
    - Ludmila Ročáková
    - Andrea Šímová

3.2 Požadavky firmy Brabec s.r.o.

Jednatel organizace pan Brabec vyložil požadavek:

- Zavést systém řízení bezpečnosti informací
- Identifikovat rizika pro firmu
- Zajistit bezpečnostní opatření rizika
- Bezpečnostní opatření musí mít minimální účinnost 90%
- Zavést bezpečnostní opatření proti:
  - Narušení škodlivým kódem
  - Narušení jádra operačního sytému
  - Vnější infiltrace
  - Výpadek proudu
  - Nekontrolovanému pohybu v síti
  - Neautentizovanému přístupu uživatelů ke koncovým stanicím
  - Ztrátě dat

II. PRAKTICKÁ ČÁST

4 NAVRHNĚTE FORMOU PROJEKTU IMPLEMETACI PDCA DO SPECIFICKÉHO FIREMNÍHO PROSTŘEDÍ.

4.1 Ustanovení ISMS

Tato podkapitola je chápána jako první krok modulu PDCA, která je pojmenovaná PLAN, nebo-li plánuj. Zde se budou vytvářet definice požadavků organizace, dle kterých se pak bude vycházet při dalších krocích modulu PDCA.

4.1.1 Rozsah a hranice

Cílem dané části bude popis činnosti organizace, její funkční struktury a lokality. Dále se budou vytvářet soupis aktiv.

4.1.2 Bezpečnostní politika

Bezpečnostní politika bude obsahovat rámec své politiky, které budou obsahovat bezpečnostní požadavky zadavatele. Bezpečnostní politika bude také obsahovat vyjádření ke všem externím požadavkům jak zákonnými tak normativními úpravami, kterými je organizace zavázána při své činnosti. Dále bude bezpečnostní politika obsahovat definici a vztah kritérii pro ohodnocení rizik. V poslední části bezpečnostní politiky musí být politika stvrzena a schválena vedením organizace.

4.1.3 Identifikace rizik

Při identifikaci rizik se nejdříve zpracuje identifikace aktiv. Aktiva se rozdělí na primární a sekundární. Obě tyto skupiny aktiv budou dále ohodnocovány dle své důležitosti pro danou firmu. Důležitost bude tvořit výstup kvantifikátoru následků, který bude získán vztahem:

$$N = \frac{T + G + V}{3}$$

N kvantifikátor následků

T míra dostupnosti

G míra integrity

V míra důvěrnosti

Dalším krokem pro identifikací rizik bude určení hrozeb pro aktiva. Tato část bude vykazovat soupis všech aktiv a ke každému aktivu budou přiřazeny adekvátní hrozby. Třetí část bude reprezentovat zranitelnost aktiv skrze určené hrozby. V poslední části se bude provádět identifikace možných dopadů, které mohou výše zmíněné hrozby vytvořit.

4.1.4 Analýza a vyhodnocení rizik

V části analýza a vyhodnocování rizik se nejdříve bude posuzovat dopad při selhání implicitního bezpečnostního opatření. V praxi to bude prezentováno jako popis implicitního bezpečnostního opatření s identifikovaným dopadem pro organizaci. V Další části se bude identifikovat reálné pravděpodobnosti selhání jednotlivých výchozích bezpečnostních opatření. Další část se bude věnovat definic úrovně rizik a škály, kterou budou rizika definována. V poslední části bude definováno, jak se bude určovat, která rizika mohou být akceptována a která naopak musí být nutně zvládnuta.

4.1.5 Vyhodnocování variant pro zvládání rizik

Vyhodnocování variant pro zvládání rizik bude mít dvě části. Úkolem první části bude identifikovat varianty pro zvládání rizik. Druhá část bude věnovaná realizaci daných variant. V praxi to bude prezentováno jako nalezení aplikace či postupu na zvládnutí daného rizika.

4.1.6 Vybrat cíle opatření pro zvládání rizik

Úkolem této části bude vypracovat cíle, kterých by měla daná bezpečnostní opatření dosáhnout.

Opatření na ochranu proti škodlivým programům

- „Na ochranu proti škodlivým programům a nepovoleným mobilním kódům musí být implementována opatření na jejich detekci, prevenci a obnovu a zvyšováno odpovídající bezpečnostní povědomí uživatelů.“ [8]

Udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.

- „Záložní kopie informací a programového vybavení organizace musí být pořizovány a testovány v pravidelných intervalech.“ [8]

Zajistit ochranu informací v počítačových sítích

- „Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících sítí a pro zajištění bezpečností informací při přenosu musí být počítačové sítě vhodným způsobem spravovány a kontrolovány.“ [8]

Řízení přístupu uživatelů

- „Musí existovat postup pro formální registraci uživatele včetně jejího zrušení, který zajistí autorizovaný přístup ke všem víceuživatelským informačním systémům a službám.“
- „Přidělování a používání privilegií musí být omezeno a řízeno.“
- „Přidělování hesel musí být řízeno formálním procesem.“
- „Vedení organizace musí v pravidelných intervalech provádět přezkoumání přístupových práv uživatelů.“ [8]

Odpovědnosti uživatelů

- „Při výběru a používání hesel musí být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy“
- „Musí být přijata zásada prázdného stolu ve vztahu k dokumentům a výměnným médiím a zásada prázdné obrazovky monitoru u prostředků pro zpracování informací.“ [8]

Řízení přístupu k operačnímu systému

- „Přístup k operačnímu systému musí být řízen postupy bezpečného přihlášení.“ [8]
- „Všichni uživatelé musí mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), musí být také zvolen vhodný způsob autentizace k ověření jejich identity.“ [8]
- „Systém správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.“ [8]
- „Použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly musí být omezeno a přísně kontrolováno.“
- „Neaktivní relace se musí po stanovené době nečinnosti ukončit.“ [8]

4.1.7 Získání souhlasu vedení organizace

V této části musí být potvrzeno podpisem vedením organizace, že daná organizace souhlasí akceptací rizik zmíněných v přiloženém dokumentu a že souhlasí se zavedením systémového řízení bezpečnosti informací.

4.1.8 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti bude obsahovat tři hlavní části. Patří sem:

a) Cíle opatření a jednotlivá bezpečnostní opatření

Tato část bude obsahovat název bezpečnostních cílů a výčet jejich zabezpečujících opatření.

I. Ochrana proti škodlivým programům

- Opatření na ochranu proti škodlivým programům

II. Zálohování

- Zálohování informací

III. Správa bezpečnosti sítě

- Síťová opatření

IV. Řízení přístupu uživatelů

- Registrace uživatele
- Řízení privilegovaného přístupu
- Správa uživatelských hesel
- Přezkoumání přístupových práv uživatelů

V. Odpovědnosti uživatelů

- Používání hesel
- Zásada prázdného stolu a prázdné obrazovky monitoru

VI. Řízení přístupu k operačnímu systému

- Bezpečné postupy přihlášení
- Identifikace a autentizace uživatelů
- Systém správy hesel
- Použití systémových nástrojů
- Časové omezení relace

b) Již implementované cíle opatření

V tomto bodě se bude nacházet seznam všech bezpečnostních opatření, které již byly a jsou používány před začátkem tvorby systémového zabezpečení bezpečnosti informací.

c) Vyloučené cíle opatření (včetně zdůvodnění)

Tento bod bude obsahovat všechny cíle opatření, které nebudou implementovány. Kromě seznamu samotného zde bude uvedeno i zdůvodnění proč daný cíl opatření bude vyloučen z dalších kroků ISMS.

4.2 Zavádění a provozování ISMS

Tato část je věnování popisu jak bude implementace probíhat a následná realizace bude popsána v kapitole realizace ISMS.

4.2.1 Formulovat plán zvládání rizik

Stěžejní činnost v této části bude formulace plánu na zvládání rizik, která byla odhalena v předchozí kapitole nazvanou Ustanovení ISMS. Zde se musí vymezit rizika a cíle opatření. Dále se zde musí nadefinovat, jaké finanční zdroje jsou k dispozici a odpovědnou osobu, která bude tito opatření zavádět a udržovat.

Tabulka 4 Formulace plánu na zvládání rizik

Riziko	Priorita	Cíle opatření	Finanční zdroje	Odpovědná osoba
Narušení škodlivým kódem	3	Minimalizovat riziko	25 000 Kč	Vedoucí pracovník IT oddělení
Nechtěné narušení jádra OS	2	Zabránit narušení	0 Kč	Vedoucí pracovník IT oddělení
Narušení hackrem.	3	Minimalizovat riziko	0 Kč	Vedoucí pracovník IT oddělení
Narušení škodlivým Makro kódem.	1	Minimalizovat riziko	0 Kč	Vedoucí pracovník IT oddělení
Výpadek proudu	2	Chod HW	28 000 Kč	Vedoucí pracovník IT oddělení

4.2.2 Zavést plán zvládání rizik

V této části se bude provádět realizace implementace zvládání rizik. Tato sekce bude detailněji rozepsána v kapitole popisující realizaci implementace ISMS tak, aby dosáhla identifikaci typu cílových opatření.

4.2.3 Zavést bezpečnostní opatření

Úkolem této části bude nalézt u identifikovaných typů řešení cílových opatření reálné řešení. V praxi to bude vypadat, že se riziko narušení z vnější sítě má jako typové bezpečnostní opatření určeno firewall, bude k němu vybrán specifický typ firewallu.

4.2.4 Měření účinnosti opatření

Měření účinnosti opatření bude probíhat pomocí měřících indikátorů. Všechny indikátory budou měřeny v procentech.

Indikátor účinnosti opatření proti narušení škodlivým kódem bude získáván následovně. Získávání bude prováděno pomocí sady vybraného škodlivého kódu a budou se zaznamenávat logy tohoto opatření. Nejlépe to popíše vztah:

$$\mathrm{I}_1 = \frac{Z_{\,1}}{C_1} * 100$$

I_1 indikátor narušení škodlivým kódem (v procentech)

Z_1 počet zadržených škodlivých kódů

C_1 Celkový počet testovacích kódů

Měření indikátoru nechtěné narušení jádra operačního systému běžným uživatelem, se bude provádět pomoci pokusného útoků do systému z vnitra. Bude se provádět 50 útoku. Pro daný identifikátor platí vztah.

$$I_2 = \frac{Z_2}{C_2} * 100$$

I_2 indikátor narušení OS

Z_2 počet neúspěšných útoků

C_2 celkový počet útoků

Indikátor narušení koncové stanice z vnější sítě bude měřen pomocí penetračních testů. Výstup indikátoru bude popisovat podíl úspěšných útoků na počet celkových útoků. Definice vztahem:

$$I_3 = \frac{Z_3}{C_3} * 100$$

I_3 indikátor narušení hackrem

Z_3 počet neúspěšných útoků

C_3 celkový počet útoků

Indikátor narušení škodlivým makro kódem bude probíhat podobně jako při získávání indikátoru obecného škodlivého kódu s výjimkou, že testovaná sada bude specificky zaměřena na makroviry. Daný indikátor popisuje vztah:

$$I_4 = \frac{Z_4}{C_4} * 100$$

I_4 indikátor infikace makrovirem

Z_4 počet neúspěšných infiltrací

C_4 celkový počet útoků

Indikátor účinnosti výpadek proudu, bude měřen pomocí sérii výpadku proudu a budou se zaznamenávat stavy, kdy opatření zabránilo nevítaného vypnutí hardwaru. Nejlepší definici se prokáže vzorcem:

$$I_5 = \frac{Z_5}{C_5} * 100$$

I_5 indikátor výpadku proudu

Z_5 počet úspěšnosti opatření

C_5 celkový počet útoků

Indikátor integrity a dostupnosti programových prostředků a dat bude popisovat test záložních kopii programu a kopie jiných dat na jejich funkčnost a zpětnou implementaci. Metodika bude popisovat počet úspěšné inkrementaci zálohy ku celkovému počtu pokusných inkrementací.

$$I_6 = \frac{Z_6}{C_6} * 100$$

I_6 indikátor narušení integrity

Z_6 počet úspěšných obnov záloh

C_6 celkový počet obnov záloh

Řízení přístupu uživatelů bude měřeno jiným způsobem. V daném případě budou stanoveny podmínky, které musí být splněny. Indikátor bude popisovat počet splněných podmínek ku celkovému počtu podmínek.

Podobně tomu tak bude i při měření odpovědnosti uživatelů. Indikátor dané problematiky bude také měřit počet splněných podmínek ku počtu všech požadavků.

Pro oba indikátory bude platit vztah:

$$I_u = \frac{D}{S} * 100$$

I_u indikátor uživatelů

D počet splněných podmínek

S celkový počet podmínek

4.2.5 Školení

Tato část bude popisovat, jaké školení budou muset absolvovat běžní uživatele pro správu opatření, se kterými budou přicházet do styku.

4.2.6 Řídit provoz ISMS

Tato část se bude věnovat popisem požadavků k udržování a provozu jednotlivých bezpečnostních opatření, kterými může být například aktualizace softwaru.

4.2.7 Řídit zdroje ISMS

Řízení zdrojů bude popisovat odpovědného činitele pro rozpočet ISMS a případné řízení financí pro danou problematiku.

4.2.8 Detekce a reakce incidentů

Opatření na ochranu proti škodlivým programům

Bezpečnostní opatření na ochranu proti škodlivým programům bude mít za hlavní úkol detekci a odstranění škodlivého kódu, který se bude pokoušet napadnout danou koncovou stanici. Detekce bude prováděna pomocí antivirové ochrany. V tomto případě bude uživatel jednat dle postupu, převzatého ze svého absolvovaného školení. V případě že škodlivý kód nebude odhalen ihned, bude každý týden prováděna heuristická analýza vedoucím pracovníkem IT oddělení popřípadě osobou, k danému úkonu zmocněnou touto osobou. Při odhalení napadení škodlivým kódem bude první akcí vyléčení daného souboru. Pokud vyléčení nebude možné, chybný soubor bude vymazán a znovu obnoven z připravených záloh. Tato akce bude vykonána vedoucím IT oddělení nebo personálem určeným danou osobou.

Udržovaní integrity a dostupnosti záloh

Na zodpovědnost vedoucího pracovníka IT oddělení budou čerstvě vytvořené zálohy testovány ve virtuálním prostředí, jestli během vytvoření záloh nedošlo k žádným chybám. Každá záloha musí být nejdříve otestována, než bude zpětně inkrementována do systému.

Zajistit ochranu informací v počítačových sítích

Detekce incidentu při ochraně pohybu dat v sítích bude použit speciální nástroj na kontrolu pohybu dat v síti organizace. Pomocí tohoto nástroje bude osoba určená k tomu to výkonu monitorovat datový chod po sítích. Reakce na možné hrozby nelze jednoduše popsat, kvůli šíři možných stavů. Proto daná osoba musí projít školením, které na dané situace připraví.

Řízení přístupu uživatelů a odpovědnosti uživatelů

Detekci této části bude náležet personálu organizace. Každá ztráta přístupového hesla se musí ihned ohlásit pracovníku, který bude mít na starost správu hesel a řídit jak jejích archivaci tak i platnost. Při přidělování privilegii přístupu bude správce hesel vycházet z dokumentu o prioritě přístupů, který bude vytvořen vedoucím organizace.

4.3 Monitorování a přezkoumání ISMS

Účelem této části je popis metodiky monitorování chodu ISMS a jeho přezkoumávání pro výchozí data zlepšení systému.

4.3.1 Monitorovat, přezkoumávat a zavést další opatření:

Tato část se bude věnovat monitorování zavedených bezpečnostních opatření. Na tuto činnost se budou používat indikátory, které se definovaly v předešlé podkapitole. Poté bude následovat přezkoumání těchto opatření, jestli jsou dostatečně účinná a pokud to bude vyžadovat situace v tomto bodě je možnost zavést opatření další.

4.3.2 Pravidelně přezkoumávání účinnosti ISMS

Následující část bude věnována přezkoumání splnění politiky ISMS, cílů a bezpečnostních opatření a to s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření, návrhů a podnětů všech zainteresovaných stran.

4.3.3 Měření účinnost opatření pro ověření požadavků na bezpečnost

V této části se bude vycházet z indikátorů, se kterými se pracovalo v předchozí podkapitole. Stanoví se definice určení hranice uspokojení požadavků na bezpečnost.

4.3.4 Plánování přezkoumání rizik s ohledem na změny

V plánovaných intervalech provádět přezkoumání hodnocení rizik a přezkoumávat zbytková rizika a úroveň akceptovatelného rizika s ohledem na změny:

a) organizace
b) cílů činností organizace a procesů
c) identifikovaných hrozeb
d) účinnosti zavedených opatření

4.3.5 Provádět interní audity ISMS v plánovaných intervalech

Interní audity budou prováděny ve spolupráci s externími auditory, aby byla zajištěna relevance výsledků. Jejich by dalších v cyklech mohlo být například prověření systému managementu před samotným certifikačním auditem.

4.3.6 Aktualizace bezpečnostních plánů

Tato část podkapitoly o monitorování ISMS, bude vycházet ze závěru monitoringu a přezkoumávaní ISMS. Z daných závěru se budou aktualizovat bezpečnostní plány.

4.3.7 Zaznamenávat všechny činnosti a události

V této části bude vytvořen systém práce se záznamy, popisující požadované úkony pro jejich tvoření.

4.4 Udržování a zlepšování ISMS

Účelem této části je reakce na nově získané poznatky, bezpečnostní hrozby a rizika. Dané informace budou mít výchozí bod definovaný pomocí předchozí podkapitoly.

4.4.1 Identifikování nepostačujících opatření

V této části se budou označovat bezpečnostní opatření, která dle měření byla vyhodnocena jako nedostačující.

4.4.2 Provedení nápravných opatření

V části provedení nápravných opatření se k identifikovaným neuspokojivým bezpečnostním opatřením bude přiřazovat nápravná opatření.

4.4.3 Návrh na nové preventivní činnosti

Pokud se dospěje k názoru, že bezpečnostní opatření by mohli být posíleny o nove preventivní akce či postupy, bude to definováno v této kapitole.

5 REALIZUJTE IMPLEMENTACI ISMS.

5.1 Ustanovení ISMS

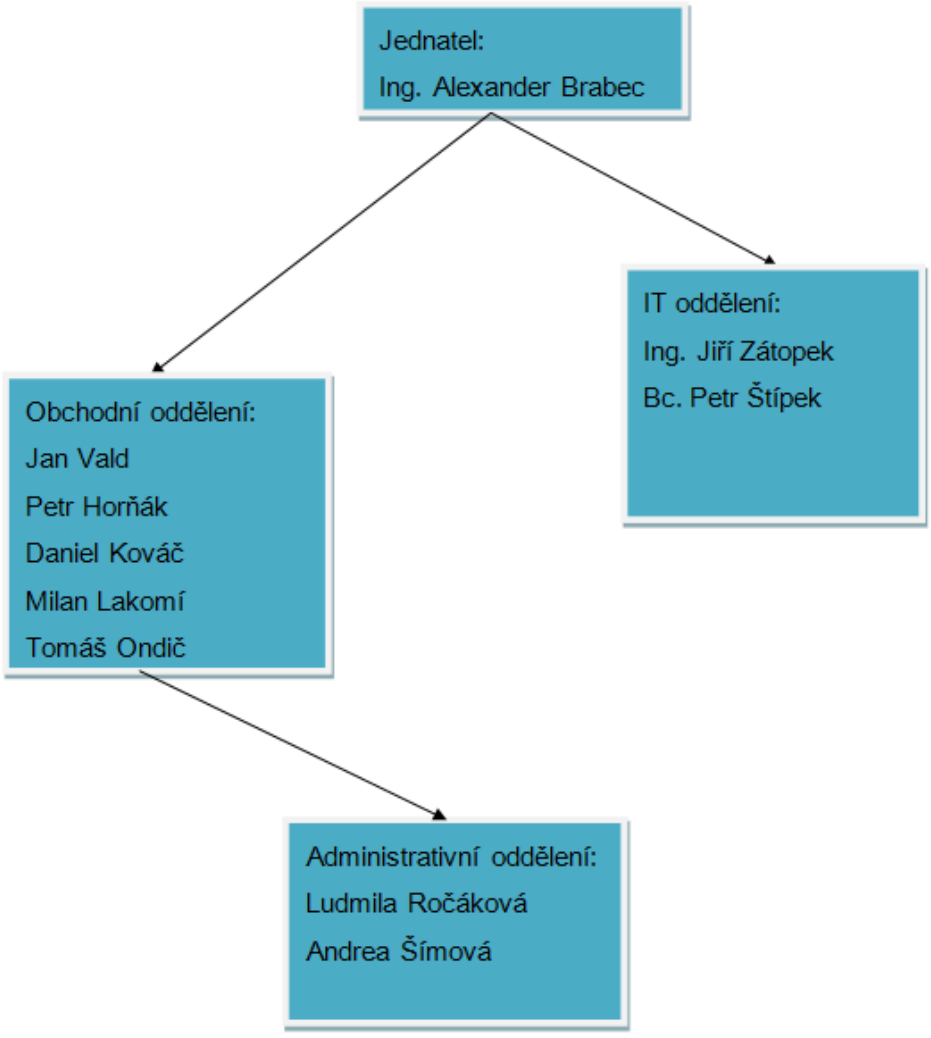
5.1.1 Rozsah a hranice

a) Činnost firmy

Firma Brabec s.r.o se zabývá prodejem plastových dveří, oken a jiných plastových výrobků. Tyto výrobky odebírá od výrobny plastových dveří a oken Sedma plus systém, která má sídlo v Kuřimi.

b) Struktura organizace

Firma Brabec s.r.o. je firma s ručením omezeným. Organizační struktura z pohledu subordinace:



Obrázek 4 Organizační struktura Brabec s.r.o.

c) Lokalita

Firma Brabec s.r.o. sídlí v ulici Zborovská v obci Náměšť nad Oslavou.

d) Aktiva

1) Hardware (PC, tiskárna, notebook)

Počet	Typ	Název	Cena za kus	Celková Hodnota
10	Stolní počítač	HAL3000 Platinum	12 321 Kč	123 210 Kč
13	LCD	Asus VE228T	3 111 Kč	40 443 Kč
4	Tiskárna	HP LaserJet M1132	2 799 Kč	11 196 Kč
10	Klávesnice	Genius Slimstar 110	256 Kč	2 560 Kč
10	Myš	Genius DX-ECO	513 Kč	5 130 Kč
1	Router	D-link 2690	11 267 Kč	11 267 Kč

2) Software (aplikace apod.)

Počet	Typ	Název	Cena za kus	Celková Hodnota
10	Operační systém	Windows 7 Profesional 64bit CZ	6 695 Kč	66 950 Kč
10	Aplikace	Microsoft Office 2010 Professional CZ	13 747 Kč	137 470 Kč
6	Aplikace	Klaes project 3.0	16 890 Kč	101 340 Kč

5.1.2 Bezpečnostní politika

a) Určení rámce bezpečnostní politiky

Bezpečnostní politika bude obsahovat požadavky na obory, které si zadavatel chce zabezpečit. Mezi tyto požadavky patří obory:

1) Ochrana proti škodlivým programům
2) Zálohování
3) Řízení přístupu uživatelů
4) Odpovědnosti uživatelů
5) Řízení přístupu k operačnímu systému

b) Externí požadavky

Externí požadavky a ani jiné zákonné normy nejsou v tomto případě relevantní.

c) Kritéria pro hodnocení rizik

Rizika budou ohodnocována dle vzorce:

$$R = (P + N)/k$$

R míra rizika

P pravděpodobnost realizace rizika

N kvantifikátor následků

k je šíře škály popisující aktiva

Dále se dle velikosti míry rizika bude rozhodovat o akceptovatelnosti rizika to dle tabulky. Akceptovatelná rizika budou, během prvního cyklu, považovány za irrelevantní.

d) Schválení vedením

Bezpečnostní politika byla bez výhrad schválena vedením organizace.

5.1.3 Hodnocení rizik

Hodnocení rizik bude vycházet z modelu popsaného v bezpečnostní politice.

5.1.4 Identifikace rizik

a) Identifikace aktiv

Primární aktiva:

- software (aplikace apod.)

Tabulka 5 Primární aktiva

Typ	Zkrácený název	Dostupnost	Integrita	Důvěrnost	Kvant. Následků
OS	MS Windows 7	3	3	3	3
Aplikace	MS Office 07	2	2	2	2
Aplikace	Klaes	2	3	3	2,7

Sekundární aktiva:

- hardware (PC, tiskárna, notebook)

Tabulka 6 Sekundární aktiva

Typ	Zkrácený název	Dostupnost	Integrita	Důvěrnost	Kvant. Následků
Stolní počítač	Hal 3000	2	2	3	2,3
LCD	Asus 228	1	1	1	1,0
tiskárna	HP Laserjet	1	1	1	1,0
Kláv.+ myš	Genius	1	1	1	1,0
Router	D-Link	3	4	4	3,7

b) Identifikace hrozeb pro aktiva

Primární aktiva:

- **Microsoft Windows 7**
  - Narušení škodlivým kódem.
  - Nechtěné narušení jádra operačního systému běžným uživatelem.
  - Narušení hackrem.
- **Microsoft Office 2010**
  - Narušení škodlivým Makro kódem.
- **Klaes project 3.0**
  - Narušení chodu programu škodlivým kódem
  - Infiltrace aplikace uživatelem

Sekundární aktiva:

- **Hal 3000**
  - Výpadek elektrického proudu
- **LCD Asus 228**
  - Bez hrozby.
- **Klávesnice a myš**
  - Bez hrozby.
- **Router D-Link**
  - Výpadek elektrického proudu

c) Identifikace zranitelnosti využitelnou hrozbami

Tabulka 7 Identifikované zranitelnosti

Hrozba	Zranitelnost	Windows 7	Office 2010	Klaes	Hal 3000	Router
Infiltrace škodlivým kódem	Neschopnost se ubránit	ANO	ANO	ANO	Ne	Ne
Nechtěné narušení jádra OS běžným uživatelem.	Neomezený přístup k jádru OS	ANO	Ne	Ne	Ne	Ne
Narušení hackrem.	Nekontrolovaný přístup ze sítě	ANO	Ne	Ne	Ne	Ne
Narušení škodlivým Makro kódem	Neschopnost odhaleni makroviru	Ne	ANO	Ne	Ne	Ne
Infiltrace aplikace uživatelem	Malá délka přístupového hesla	Ne	Ne	ANO	Ne	Ne
Výpadek Proudu	Zastavení dodávky elektrického proudu	Ne	Ne	Ne	ANO	ANO

d) Identifikace dopadů na aktiva

Tabulka 8 Dopady na aktiva

Hrozba	Dopad	Postižená aktiva
Narušení škodlivým kódem	Ztráta správné funkčnosti SW až nevratné změny v jeho chodu	MS Windows 7 MS Office 2010 Klaes project 3.0
Narušení jádra OS	Ztráta správné funkčnosti SW až nevratné změny v jeho chodu	MS Windows 7
Výpadek proudu	Samovolné vypnutí, a fyzické poškození HW	Hal 3000 Router D-Link
Infiltrace	Znehodnocení nebo zcizení dat	MS Windows 7 MS Office 2010 Klaes project 3.0

5.1.5 Analýza a vyhodnocení rizik

a) Posouzení dopadu při selhání bezpečnostních opatření

V této části je potřeba zmínit že zde nebylo nalezeno vysoký počet bezpečnostních opatření.

Tabulka 9 Dopad selhání

Aktivum	Výchozí bezpečnostní opatření	Dopad selhání
MS Windows 7	Windows Defender	Možnost vnějšího narušení OS
MS Office 2010	žádné není	žádné není
Klaes project 3.0	Přístup heslem	Přistup nepovolaným osobám
Hal 3000	žádné není	žádné není
Router D-Link	žádné není	žádné není

b) Reálná pravděpodobnost selhání bezpečnostních opatření

Tabulka 10 Selhání opatření

Bezpečnostní opatření	Pravděpodobnost selhání
Windows Defender	40%
Klaes-Heslo	3%

V této části je potřeba zmínit, že bezpečností opatření popsanou jako nutnost hesla k přístupu má pohyblivou pravděpodobnost selhání. Pohyblivá pravděpodobnost selhání vychází z délky hesla potřebného k přihlášení. V tomto případě byla stanovena délka hesla na 10 numerických a alfa-numerických znaků.

c) Definování úrovně rizik

Rizika budou definována pomoci stupnice, která bude hodnotit rizika v intervalu od 1 do 4. Stupeň jedna označuje riziko, které se při svém realizování nesetká s žádnými nežádoucími účinky pro danou organizaci. Stupeň číslo dvě označuje stav, kdy zrealizované riziko se stává určitou finanční ztrátou pro organizaci. Pro závažnější potíže a finanční ztrátu vyšší než 40% jmění organizace byl vytvořen stupeň tři. Stupeň číslo čtyři je ukazatelem takového rizika, které by při své realizaci mohlo vést k ukončení existence organizace jak z funkčního hlediska, tak i z finančního.

Tabulka 11 Stupnice definice rizik

Stupeň	Efekt
1	Žádný Dopad
2	Potíže či ztráta
3	Vážné potíže
4	Existencionální potíže

d) Určení zvládaní nebo akceptace rizik

Tabulka 12 Míra rizika

Riziko	Bezpečnostní opatření	Kvantifikátor následků	Pravděpodobnost realizace	Míra rizika
Narušení škodlivým kódem	Není	3,00	72%	93%
Nechtěné narušení jádra OS	Není	3,00	48%	87%
Narušení hackrem.	Windows Defender	1,80	72%	63%
Narušení škodlivým Makro kódem.	Není	2,00	85%	71%
Infiltrace aplikace cizím uživatelem	Šifrovaný přístup	0,08	45%	13%
Výpadek proudu	není	1,80	51%	58%

Ve výše zmíněné tabulce je potřeba upřesnit některé veličiny.

Kvantifikátor následků je bezrozměrná veličina obsahující hodnoty v intervalu nula až čtyři. Používá se zde míra rizika, která je vybraná od aktiv, se kterými riziko souvisí. Kvantifikátor následku je popsán vztahem:

$$N = A - ((1 - B) * A)$$

N kvantifikátor následků

A průměrná míra rizika

B pravděpodobnost bezpečnostního selhání opatření

Míra rizika je veličina definovaná v procentech a popsána vztahem:

$$R = (P + N)/k$$

R míra rizika

P pravděpodobnost realizace rizika

N kvantifikátor následků

k je šíře škály popisující aktiva(v tomto případě je to číslo 4)

Rizika se rozdělují na nutně zvládnutelné a akceptovatelné. Mez akceptovatelnosti bude stanovena do výše 55% míry rizika.

Tabulka 13 Akceptace rizik

Riziko	Míra rizika	Nutnost zvládání
Narušení škodlivým kódem	93%	Nutné zvládání
Nechtěné narušení jádra OS	87%	Nutné zvládání
Narušení hackrem.	63%	Nutné zvládání
Narušení škodlivým Makro kódem.	71%	Nutné zvládání
Infiltrace aplikace cizím uživatelem	13%	Akceptovatelné
Výpadek proudu	58%	Nutné zvládání

5.1.6 Vyhodnocování variant pro zvládání rizik

a) Identifikace variant pro zvládání rizik

V této části budou vyhledány různé varianty jak se chránit a jak zvládat výše zmíněná rizika. Pro zvládání byla určena pouze rizika, která mají míru rizika ohodnocenou více než 55% a byly označeny pro nutné zvládání. Těmito riziky jsou:

I. **Narušení škodlivým kódem**
   Zavedení antivirové ochrany

II. **Nechtěné narušení jádra operačního systému uživatelem**
   Vytvoření uživatelských účtů. Administrátorský přístup bude mít pouze pracovník z oddělení IT a tento účet musí byt chráněn heslem. Běžný uživatelský účet, bude mít blokován přístup k jádru operačního systému a bude též chráněn heslem.

III. **Narušení vnějším útokem hackera**
   Zavedení firewallová ochrany a zavedení prostředků na monitoring sítové komunikace.

IV. **Narušení škodlivým makro kódem**
   Zavedení antivirové ochrany a kontrolu všech nových souborů Word, Excell a podobných programů z balíku Office.

V. **Výpadek proudu**
   Zavedení záložní jednotky, která bude zabraňovat poškození hardwaru při výpadku proudu.

b) Aplikace variant zvládání rizik

I. Narušení škodlivým kódem

Proti riziku napadení škodlivým kódem bude vybráno jako bezpečnostní opatření antivirový program Symantec Endpoint Protection Small Business Edition. Antivrus bude nainstalován na všech deset koncových stanic nacházejících se ve firmě. Daný software se zaměřuje jako ochrana proti:

- virům
- trojským koňům
- spywaru
- rootkitům
- infiltraci cizím uživatelů z externí sítě
- makrovirům

II. Nechtěné narušení jádra operačního systému uživatelem

Opatření proti nechtěnému narušení jádra operačního systému běžným uživatelem nebude řešeno pomocí externího softwaru. Řešení opatření proti danému riziku bude nastavení práv přístupu do systému. V praxi musí nastavit pracovník IT oddělení dva typy účtů. První typ bude administrátorský, ke kterému bude umožněn přístup, pouze pracovníkovi IT oddělení. Ten to účet bude používán pouze ke správním a údržbovým činnostem na dané koncové stanici. Druhý typ účtu bude obsahovat znepřístupnění části harddisku, na které se bude nacházet samotný operační systém.

III. Narušení vnějším útokem hackera

Bezpečnostní opatření proti vnějšímu narušení uživatelem z vnější sítě bude považován výše zmíněný antivirový program od společnosti Symantec. Tento program obsahuje firewallovou ochranu pomocí, které se bude řídit komunikace se síťovým okolím koncové stanice. Ihned po instalaci musí určeny pracovník IT nastavit řídící pravidla firewallu.

IV. Narušení škodlivým makro kódem

Dané riziko bude taktéž zabezpečeno pomocí antiviru od společnosti Symantec. Zde bude stanovena podmínka, že všechny soubory vytvořené programovým vybavením Office 2010, které budou doručeny na email, musí být zkontrolovány pomoci daného programu od Symantecu.

V. Výpadek proudu

Bezpečnostní opatření proti výpadku proudu bude tvořit jednotka APC Back-UPS BX650CI. Tato jednotka bude schopná zabránit okamžitému vypnutí LCD, stolního počítače HAL 3000 a routru D-link. Dané zařízení obsahuje baterie o kapacitě 7,2 ampérhodiny při napětí 12 voltů.

5.1.7 Vybrat cíle opatření pro zvládání rizik

Tabulka 14 Cíle opatření pro zvládání rizik

Riziko	Stanovený cíl opatření	Bezpečnostní opatřeni
Narušení škodlivým kódem	Zabránit narušení škodlivým kódem	Symantec Endpoint Protection Small Business Edition
Narušení jádra OS běžným uživatelem	Zabránit narušeni jádra OS	Nastavení uživatelských účtů
Narušení vnějším útokem hackrem	Zabránit vnější infiltraci	Symantec Endpoint Protection Small Business Edition
Narušení škodlivým makro kódem	Zabránit narušení makroviry	Symantec Endpoint Protection Small Business Edition
Výpadek proudu	Zabránit poškození při výpadku proudu	APC Back-UPS BX650CI

5.1.8 Získání souhlasu vedení organizace

a) Souhlas s navrhovanými akceptovatelnými riziky

Jako jediné akceptovatelné riziko byla určena infiltrace aplikace Klaes project 3.0 přes přístupové heslo. Po předložení dat vedoucím k tomuto výsledku, vedení organizace souhlasilo, že toto riziko může být zanedbáno. Tedy nebude se vyhledávat žádné další opatření.

b) Souhlas se zavedením provozu ISMS

Vedení souhlasilo se stanovenými cíli ISMS a také vyjádřilo souhlas se zavedením toho to systému v plném znění kapitoly ustanovení ISMS.

5.1.9 Prohlášení o aplikovatelnosti

a) Cíle opatření a jednotlivá bezpečnostní opatření

Výčet cílů opatření a k nim přiřazené vybrané opatření jsou popsány v následující tabulce. V tabulce se objevují nové cíle, které nebyly stanoveny pomocí identifikací zvládání hrozeb, ale musí být implementovány jako požadavky, který byly vydány zadavatelem.

.

Tabulka 15 Stanovení cílů opatření

Stanovený cíl opatření	Navrhované Bezpečnostní opatřeni	Funkce pro cíl
Ochrana proti škodlivým programům	Symantec Endpoint Protection Small Business Edition	Antivirová ochrana
Řízení přístupu uživatelů	Stanovení přístupových definic	Zábrany přístupu nepovolaným osobám
Správa bezpečnosti sítě	Symantec Endpoint Protection Small Business Edition	Firewallová ochrana
Zabránit narušení makroviry	Symantec Endpoint Protection Small Business Edition	Kontrola nových souborů
Zabránit poškození při výpadku proudu	APC Back-UPS BX650CI	Umožňuje předejít poškozeni HW a ztrátě dat při výpadku
Zálohování	Shadow Protect	Vytvoří zálohy dat
Odpovědnosti uživatelů	Pokyny pro chování uživatelů	Zvýšení bezpečnostního povědomí
Řízení přístupu k operačnímu systému	Nastavení uživatelských účtů	Omezeni přístupu k jádru

b) Již implementované cíle opatření

Tato část bude více využita až při dalších cyklech implementace modulu PDCA v rámci systémového řízení bezpečnosti informací. V prvním cyklu byly zjištěny pouze tyto bezpečnostní opatření:

- Windows Defender

  Windows Defender je implicitní firewall Windows 7, který byl vytvořen firmou Microsoft. Toto bezpečnostní opatření bylo v ustanovením ISMS odhaleno jako nedostačující.

- Přistup k Klaes project 3.0

  Přistup k programu Klaes project 3.0 je chráněn vstupním heslem. Délka tohoto hesla je uspokojivá. Dané bezpečnostní opatření tedy bylo vyhodnoceno jako uspokojivé a nebude se vyhledávat další náhrada.

c) Vyloučené cíle opatření (včetně zdůvodnění)

Žádná vyloučena opatření nejsou.

5.2 Zavádění a provozování ISMS

5.2.1 Formulovat plán zvládání rizik

a) Narušení škodlivým kódem

Dané riziko se bude zvládat pomoci antivirového programu značky Symantec. Daný program je vybaven schopností detekovat, léčit, pokud to nebude možné, odstranit škodlivý kód. Tak to budou zabezpečeny všechny koncové stanice. Přidělenou osobou je Pan Zátopek. K danému bodu jsou přiděleny finance na výlohy 20 000 Kč na pořízení.

b) Narušení jádra operačního sytému

Riziko narušení jádra operačního systému minimalizování přístupových práv běžných uživatelů. Běžný uživatel nesmí mít přístup do adresáře Windows, k systémovým nástrojům. Tak to budou zabezpečeny všechny koncové stanice. Zajišťuje pan Štípek, bez přidělení financí na tuto činnost.

c) Vnější infiltrace

Riziko vnější infiltrace bude chráněno firewallovým opatřením. Dané opatření musí mít náležitě nastavena pravidla datového toku. Firewall je obsažen v produktu Symantec. Tím to způsobem budou zabezpečeny všechny koncové stanice. Odpovědnou osobou je pan Zátopek, bez přidělených financí na tento úkol.

d) Narušení Marko virem

Tento problém bude zvládat stejným způsobem jako narušení škodlivým kódem.

e) Výpadek proudu

Ochranné opatření proti výpadku proudu bude tvořeno záložní zdrojem APC Black UPS. Při výpadku proudu dojde ke zvukovému oznámení, při kterém uživatel určeným způsobem ukončí svou činnost a bezpečně vypne daný hardware. K danému bodu jsou přiděleny finance na výlohy 27 000 Kč na pořízení.

5.2.2 Zavést plán zvládání rizik

Narušení škodlivým kódem

Stanovený postup bude dodržen u všech koncových stanic. Na začátku proběhne instalace daného ochranného softwaru od Symantecu. Po dokončení instalace proběhne aktualizace daného programu. Po provedení aktualizace se vytvoří záloha. Popsané činnosti budou v kompetenci pana Zátopka. Na pořízení softwaru mi bylo přiděleno 20000 Kč.

Narušení jádra operačního sytému

Na počátku se vytvoří administrátorský účet, který nebude omezen. Tento účet bude chráněn heslem o minimální délce 13-ti znaků. Heslo se zapíše do souboru pro správu hesel. Kompetentní osobě, která bude na dané koncové stanici vykonávat svou činnost, bude vytvořen vlastní účet. Tento účet bude mít zakázaný přístup do kořenového adresáře Windows, systémovým nástrojům a softwaru Symantec. Daný účet bude chráněn přiděleným heslem o minimální délce 13-ti znaků. Odpovědnost za daný postup má pan Štípek. Finance nejsou nutné.

Vnější infiltrace

Vnější infiltraci bude zabraňovat program Symantec, tedy jeho firewallová část. Hned v počátku se musí nadefinovat pravidla komunikace s vnější sítí. Určí se také, jaké programy budou moci komunikovat s externím prostředím. Mezi tyto programy patří Outlook z programového vybavení a antivirový program Symantec. Odpovědnost za danou činnost náleží panu Zátopkovi.

Narušení Marko virem

Tento problém bude zvládat stejným způsobem jako narušení škodlivým kódem.

Výpadek proudu

Každá koncová stanice a router bude mít k dispozici vlastní záložní zdroj APC Black UPS. Každý měsíc se provede kontrola baterii, že je daný hardware k dispozici. Odpovědnost za tyto činnosti náleží panu Štípkovi. K této činnosti bude dodáno 27000 Kč na pořízení nástroje.

5.2.3 Zavést bezpečnostní opatření

Bezpečnostní opatření, které byly uvedeny v plánu zavádění rizik, budou zaváděny dle naformulovaného plánu uvedeného předchozí části. Jsou to opatření:

- Opatření na ochranu proti škodlivým programům
  - Program Symantec
- Síťová opatření
  - Firewall obsažen v programu Symantec
- Registrace uživatele
- Řízení privilegovaného přístupu
- Používání hesel
- Použití systémových nástrojů

Další opatření již nejsou formulovány v plánu zvládání rizik:

I. Správa uživatelských hesel

Všechny hesla, která jsou použita v dané firmě, budou spravována panem Štípkem**.** Tyto hesla budou uloženy jak v digitální zašifrované podobě, tak ve dvou fyzických dokumentech. První dokument bude mít uschován pan Zátopek a druhý pan Brabec. Oba je budou mít za svou odpovědnost. Digitální správa hesla musí výt aktualizována ihned po změně a fyzické dokumenty odevzdá pan Štípek nejdříve do 24 hodin. Všechny správy hesel budou obsahovat historii změn.

II. Přezkoumání přístupových práv uživatelů

Každý kdo bych chtěl změnit svá přístupová práva, musí si podat formální žádost o jejich změnu s přiloženým odůvodněním. Tuto žádost pak odevzdá panu Štípkovi k přezkoumání. Pokud se změna uskuteční, bude o této změně informován pan Brabec. Hlavní odpovědnou osobou je pan Štípek.

III. Zásada prázdného stolu a prázdné obrazovky monitoru

Každý uživatel, který se vzdálí od své koncové stanice, musí aktivovat šetřič obrazovky. Daný šetřič obrazovky bude obsahovat řízené vypnutí pouze po zadání uživatelského hesla. Odpovědnost spadá na uživatele, kterému byla daná stanice přidělená.

IV. Časové omezení relace

Pokud dojde k neaktivitě na pracovní ploše koncové stanice delší než 9 minut, tato stanice automaticky přejde do režimu šetřiče obrazovky, který je chráněn heslem. Odpovědnost spadá na uživatele, kterému byla daná stanice přidělená.

V. Použití systémových nástrojů

Používání systémových nástrojů bude omezeno na administrátorské účty. Za tyto účty zodpovídají pan Štípek a pan Zátopek.

VI. Identifikace a autentizace uživatelů

Uživatelé se budou identifikovat pomocí přihlašovacího jména a k němu přiděleného hesla. Autentizaci uživatelů odpovídá pan Štípek.

5.2.4 Měření účinnosti opatření

Měření účinnosti opatření probíhalo dle definic a vztahů uvedených v předchozí kapitole. Požadavek vedení organizace je aby opatření měly účinnost minimálně 90%.

Tabulka 16 Výpočty indikátorů účinnosti

Bezpečnostní opatření	Z_k nebo D	C_k nebo S	Indikátor účinnosti	Požadavek	Splnění
Symantec- Antivirová ochrana	48	50	96%	90%	Ano
Přístup k jádru OS	59	60	98%	90%	Ano
Symantec- Firewall	109	113	96%	90%	Ano
Symantec- ochrana před makroviry	60	60	100%	90%	Ano
APC UPS	38	40	95%	90%	Ano
Shadow Protect	25	25	100%	90%	Ano
Řízení přístupů	6	6	100%	90%	Ano

5.2.5 Školení

Odpovědná osoba za přípravu školení je určen pan Zátopek. Běžní uživatelé koncových stanic absolvují tato školení:

- Základní operace se škodlivým kódem pomocí programu Symantec
- Bezpečnost hesla a práce s ním

5.2.6 Řídit provoz ISMS.

Osobami odpovědnými za provoz ISMS jsou pan Zátopek a pan Štípek. Mezi jejich hlavní činnosti patří:

Aktualizace softwaru ve firmě minimálně jednou týdně

Zkontrolovat aktualizace před implementaci do systému

Vytvářet zálohy programů každý týden a uchovávat je minimálně po dva měsíce

Pravidelná kontrola záložních zdrojů

Správa hesel a činnosti s tím spojené

5.2.7 Řídit zdroje ISMS

Řízení finančních zdrojů bude mít jako odpovědná osoba ve své kompetenci pan Brabec. Návrhy na změny finančních zdrojů podávají ve formální žádosti pan Štipek a pan Zátopek.

5.3 Monitorování a přezkoumání ISMS

5.3.1 Monitorovat, přezkoumávat a zavést další opatření:

Monitorování bude prováděno pomocí měřená bezpečnostních indikátorů nadefinovaných v předešlé kapitole. Pokud indikátor daného bezpečnostního opatření nebude splňovat určený limit účinnosti 90% (v dalších cyklech se dle požadavků tato hodnota může změnit), přijde na řadu přezkoumání daného opatření a ihned bude vyhledána náprava. Monitorování opatření se budou opakovat každý měsíc. Výstupem každého monitorování bude bezpečnostní zpráva o stavu ISMS. Tato správa bude podána a vysvětlena panu Brabcovi. Monitoring spolu s vytvořením zprávy bude provádět na svou odpovědnost pan Zátopek.

5.3.2 Pravidelně přezkoumávat účinnost ISMS

Pravidelné přezkoumání bude provádět pan Brabec z výstupu monitorovací zprávy, která bude zpracována panem Zátopkem. Dále se budou přezkoumávat splnění cílů bezpečnostní politiky s ohledem na udané incidenty. Dané přezkoumání bude prováděno jednou do měsíce.

5.3.3 Měření účinnost opatření pro ověření požadavků na bezpečnost

Daný úkon již byl proveden v předchozí podkapitole (5.2.4).

5.3.4 Plánování přezkoumání rizik s ohledem na změny

Žádné změny nenastaly. Každé přezkoumání bude opakováno v novém cyklu ISMS.

5.3.5 Provádět interní audity ISMS v plánovaných intervalech.

Interní audity budou prováděny každé dva měsíce, pro ověření relevantnosti výsledků externími auditory, kteří jsou autorizováni ke kontrole ISMS.

5.3.6 Aktualizace bezpečnostních plánů

V tom to bodě se aktualizační plány s ohledem na závěry monitorování a přezkoumání provádět nebudou, z důvodu uspokojení všech požadavků. Pokud by k uspokojení požadavků na bezpečnostní opatření nedošlo, pan Zátopek na příkaz pana Brabce provede aktualizaci.

5.3.7 Zaznamenávat všechny činnosti a události

Všechny změny, incidenty a události, které se dotýkají tématu systémového řízení bezpečnosti informací v dané firmě, se budou zapisovat a vytvářet jejich záznamy. Tyto záznamy se budou uchovávat. Odpovědná osoba za tuto činnost je pan Štípek.

5.4 Udržování a zlepšování ISMS

V posledním kroku modulu PDCA nazvaném ACT, se bude soustředit pozornost na zjištěné poznatky, z předchozí kapitoly. Tedy se zde jedná hlavně o údržbu zlepšení daného ISMS zkušenostmi z části monitorování a měření.

V daném případě zlepšování není potřeba, jelikož při měření bylo dosaženo stanovených cílů a požadavků. Tento měření výsledek bude relevantní jen po určitou dobu, a to z důvodu velmi rychlé evoluce informačních hrozeb v reálném světě. Proto je důležité provádět měření v určených intervalech, jak jsou nadefinovány předchozí kapitole. Pokud nedojde k naplnění cílů či k nevítaným incidentům je důležité zpracovat zlepšování ISMS.

5.4.1 Identifikování nepostačujících opatření a provedení nápravných opatření

Pokud budou identifikovány některá bezpečnostní opatření jako nedostačující ke stanoveným cílům, nutně musí proběhnout činnost, při které se musí nalézt zlepšení bezpečnostního opatření, které musí splňovat bezpečnostní požadavky. Pro danou činnost byl pan Zátopek určen jako odpovědná osoba.

6 VYHODNOŤ TE PŘÍNOSY PRO FIRMU VČETNĚ EKONOMICKÝCH A PROVEĎTE DISKUSI.

6.1 Výhody

Mezi hlavní výhody, které byly získány implementací systému řízení bezpečnosti informací pomocí modulu PDCA, je zajištění bezpečí informací. V této době je velmi populární zneužívat informační technologie k získání lepší pozice na trhu. V praxi dané organizace bývají cílovou informací ceníky. A to buď ceníky subdodavatelské anebo koncepty zakázek (s cenovým ohodnocením) pří výběrových řízení. Konkurenční zpravodajství skýtá vysoký počet techniky umožňující zcizení či zkopírování informace.

Za další výhodu můžeme považovat samotný modul PDCA. Hlavním důvodem je rychlost zpětné vazby na daný incident popřípadě předělání všech cílů a bezpečnostních opatření při stejně stanovených způsobech měření.

Třetím přínosem je samostatnost daného systému, který je svým nastavením schopný se z incidentu ponaučit a vytvořit nápravu daného systému. Velký díl tohoto systému tvoří systém odpovědných osob a znalostní kompetence těchto osob.

6.2 Ekonomická stránka

Vztah bezpečnostní a ekonomické stránky organizace je úzce provázán. Bezpečnost musí chránit ekonomickou stránku firmy a bezpečnost bez dostatečných finančních zdrojů nemusí být účinná. Obě tyto stránky jsou na sobě závislé. U menších organizací bývá bezpečnost informací většinou podceňována a to z důvodů, že finanční náklady na bezpečnost menší firma pocítí mnohem intenzivněji než velká korporátní společnost. V dnešní době kyberterorismu a „zlaté horečky“ konkurenčního zpravodajství je tato daň byť drahá ale opodstatněná.

ZÁVĚR

Ve své diplomové práci psané na téma „Model PDCA v řízení informační bezpečnosti“ sem se věnoval popisu a implementaci modelu PDCA v systému řízení bezpečnosti informací do vybrané organizace Brabec s.r.o..

V první kapitole teoretické části jsem se věnoval popisu modelu PDCA a jeho provázanosti s použitým systémem řízení bezpečnosti informací. V modulu se nachází části Plan (Ustanovení ISMS), Do (Zavádění ISMS), Check (Monitorování ISMS) a Act (Údržba a zlepšování ISMS).

Druhá kapitola teoretické části byla zaměřena na literární rešerši problematiky systematického řízení bezpečnosti informací. Popisoval jsem zde součásti hlavních podkapitol, které jsem pak aplikoval v první kapitole praktické části.

Ve třetí kapitole teoretické části jsem se zaměřil na popis firmy Brabec s.r.o. Popis obsahoval identifikační údaje firmy, popis její činnosti a seznam všech zaměstnanců přiřazených do svých oddělení. Těmito oddělení byly administrativní, IT, obchodní a oddělení jednatele firmy. Dále jsem vytvořil soupis požadavků, které mi přednesl pan Brabec.

V první kapitole praktické části jsem se věnoval popisu implementace a nástrojů systémového řízení bezpečnosti informací. Systém jsem vytvořil spojením poznatků druhé kapitoly teoretické části s normou ISO ČSN 27001:2006. První podkapitola nazvaná „Ustanoveni ISMS“ obsahuje metodiku pro určení rozsahu a rámce, bezpečnostní politiky, identifikace rizik s jejich ohodnocením a analýzou, vyhodnocení variant pro zvládání rizik, vybrání opatření pro jejich zvládání a prohlášení o aplikovatelnosti. Druhá podkapitola Nazvaná „Zavádění a provozování ISMS“ obsahuje metodiku pro formulaci plánu zvládání rizik, zavádění plánu na jejich zvládání a bezpečnostní opatření, metodiku měření účinnosti opatření, řízení provozu a zdrojů ISMS. Třetí podkapitola se věnuje metodice monitorování opatření, přezkoumávání účinnosti, provádění auditů aktualizaci plánů a zaznamenávaní činností. V poslední podkapitole se definovala metodika pro udržování systému řízení bezpečnosti informací.

Ve druhé kapitole praktické části jsem aplikoval metodiku, kterou jsem popsal předchozí kapitolu. V první části jsem vytvořil Ustanovení ISMS spolu s prohlášením o aplikovatelnosti. V druhé části jsem zavedl a zprovoznil ISMS. Jednalo se zavedení bezpečnostních opatření, určení finančních zdrojů, provedení měření účinnosti pomocí mým způsobem nadefinovanými identifikátory a určení odpovědných osob za provoz ISMS tak za finanční zdroje ISMS. Předposlední podkapitole jsem se zaměřil provedení měření účinnosti a kontroly zda tyto činnosti splňují nastavené limity. Také zde jsem nadefinoval odpovědné osoby, které tuto činnost budou provádět i při dalších cyklech. Poslední podkapitola byla věnována udržování a zlepšování ISMS. Jelikož se hned při prvním cyklu podařilo splnit všechny požadavky, stanovené analýzou i panem Brabcem, nebylo nutné pokračovat ve zlepšování. Tento výsledek je pouze prozatímní a proto se celý cyklus musí opatrovat jednou ročně z důvodu nezastavitelné evoluce hrozeb. Pro udržování a sledovaní ISMS byly určeny odpovědné osoby, které vykonávají jednotlivé kontrolní a údržbové činnosti ISMS.

V poslední kapitole jsem se věnoval hlavním přínosům implementaci modelu PDCA do systému řízení bezpečnosti informací. Mezi významné výhody patří rychlá zpětná vazba, ochrana před konkurenčním zpravodajstvím, dobře definovaný systém náprav, oprav a kompetencí osob a mnoho dalších výhod.

Problematika implementace systémů řízení bezpečnosti informací se nemůže považovat za jednoduchou činnost. Složitost daného systému roste s vyšším počtem požadavků a složitosti organizační struktury podniku. Důležité je neopomenout že modul PDCA se musí periodicky opakovat z toho důvodu, aby daný systém vydržel být konkurence schopný vůči novým hrozba, které vždy budou vyvíjet. Běžný interval mezi dvěma cykly bývá jeden rok, pokud se neobjeví nový incident či mimořádná událost. Model PDCA je v tom to případě soustavná činnost se snahou co nejvíce se přiblížit ke stoprocentnímu zabezpečení organizace.

Moje diplomová práce má za úkol seznámit čtenáře s danou problematikou a ukázat aplikaci normy ISO ČSN 27001:2006 v praxi. V blízké době je v očekávání vydání nové úpravy s označenou ISO ČSN 27001:2012. Mělo by se v ní objevit soupisy dalších bezpečnostních opatření

ZÁVĚR V ANGLIČTINĚ

In his thesis written on the topic "ModelPDCA in information security management" here I devoted myself to the description and implementation of the PDCA model in information security management system to the selected organizations Ltd. Brabec.

In the first chapter of the theoretical part is devoted to the description of the PDCA model and used his links with the safety management system information. The module is part of the Plan (Provisions ISMS),Do (Implementation ISMS), Check(Monitoring ISMS) and Act (Maintenance and improvement of the ISMS).

The second theoretical chapter focused on the issue of systematic literature search of information security management. I have described the main components of subchapters, which I then applied in the first chapter the practical part.

In the third chapter of the theoretical part, I focused on the description of the company Brabec Ltd. Description of the company include personally identifiable information, a description of its activities and a list of all employees assigned to their department.These departments are administrative, IT,business
and executive departments of the company. Next, I created a list of requirements that I gave Mr. Brabec.

In the first chapter of the practical part I devoted to the description of implementation tools and information security management system. I created a system combining theoretical knowledge of the second chapter of the ISO standard ISO 27001:2006. The first sub-chapter entitled "The provisions of the ISMS" a methodology for determining the scope and framework of security policy, risk identification with their ranking and analysis, evaluation of options for risk management, selecting measures for their management and the statement of applicability. The second sub-chapter entitled "The implementation and operation of the ISMS" a methodology for formulating the risk management plan, implementation plan for the management and security measures, a methodology for measuring the effectiveness of measures, traffic management and resources ISMS. The third subsection is devoted to the methodology of monitoring measures, review the effectiveness, audit plans, updating and recording activities. In the last subchapter is defined methodology for maintaining information security management system.

In the second chapter, the practical part, I applied the methodology I have described the previous chapter. In the first part I created provisions ISMS with a statement of applicability. In the second part, I introduced and put in ISMS. It was the introduction of security measures, identification of financial resources, performance measurement using force my way has calendar identifiers and identifying those responsible for the operation of the ISMS and ISMS for financial resources. Penultimate subchapter I focused the measurement of efficiency and control that these activities meet the set limits. Here, too, I defined the responsible persons who will carry out this work and in other cycles. The last section will be devoted to maintaining and improving the ISMS. As at the first cycle have met all the requirement said down by Mr. Brabec and analysis, it was necessary to continue to improve. This result is only provisional and therefore must take care of the whole cycle once a year because of the unstoppable evolution of threats. For maintaining and monitoring the ISMS identified responsible persons performing each inspection and maintenance activities of ISMS.

The last chapter is devoted to the main benefits of implementing the PDCA model to Information Security Management System. The major advantages include rapid feedback, protection against competitive news, well-defined system of axles, repair and competencies of people and many other benefits

The issue of implementation of information security management systems cannot be considered as a simple activity. The complexity of the system increases with increasing number of requirements and complexity of organizational structure. It is important to note that the module PDCA must be repeated periodically in order that the system held out to be a competitive threat to the new that will always evolve. The current interval between two cycles is one year, unless there is a new incident or incident. PDCA model is that it is the case of continuous operation as much effort to get closer to one hundred percent security of organization.

My thesis aims to acquaint readers with the issues and show the application of ISO27001:2006 BS in practice. In the near future is expected to issue new regulations to a designated ISO 27001:2012 ISO. It should appear in the lists of additional security measures

SEZNAM POUŽITÉ LITERATURY

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

[2] DOUCEK, Petr. Řízení projektů informačních systémů. 2., rozš. vyd. Praha: Professional Publishing, 2006, 180 s. ISBN 80-86946-17-7.

[3] PIRONTI, John. Developing Metrics for Effective Information Security Governance, IS Control: Journal volume 2. DOI: ISACA 2007.

[4] ŘEPA, Václav. *Podnikové procesy*: *procesní řízení a modelování*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-2252-8.

[5] ISO IEC Guide 73. Risk management - Vocabulary - Guidelines for use in standards. 2002. vyd.

[6] ISO ČSN EN 9001. Systémy managementu jakosti: Požadavky. 2000.

[7] ISO IEC 15939. Software engineering: Software. 2007. Vyd

[8] ISO ČSN 27001. Information technology - Security techniques. 2006. vyd.

[9] ISO 27004. Information technology: Information Security Management - Measurements.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISMS	Systémové řízení bezpečnosti informací
PDCA	plan do check act
IT	information technology
HW	hardware
SW	software
ISO	označení mezinárodní normy
ČSN	označení české normy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK