Systém řízení bezpečnosti informací firmy XERXES a.s.

Information Security Management System of XERXES a.s.

Bc. Jan Sporek

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Bc. Jan SPOREK**
Osobní číslo:	**A08493**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Téma práce:	**Systém řízení informační bezpečnosti firmy XERXES a.s.**

Zásady pro vypracování:

1. **Proveďte literární rešerži na téma ISMS v podnikové sféře.**
2. **Teoreticky analyzujte možnosti ISMS pro bezpečnostní politiku zvolené organizace.**
3. **Dle pravidel ISMS proveďte analýzu aktiv firmy.**
4. **Vypracujte bezpečnostní politiku organizace a proveďte její diskusi.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DOUCEK, Petr, NOVÁK, Luděk, SVATÁ, Vlasta. Řízení bezpečnosti informací. [s.l.] : [s.n.], 2008. 240 s.**
2. **ISMS : Seriál o ISMS [online]. c2010 [cit. 2010-01-19]. Dostupný z WWW: http://www.chrantesidata.cz/cs/art/1146-isms/.**
3. **HANÁČEK, Petr, STAUDEK, Jan. Bezpečnost informačních systémů. [s.l.] : [s.n.], 2000. 127 s.**
4. **Data Security Management. 2006, č. 03-06.**
5. **PELTIER, Thomas R. Information Security Policies and Procedures : A practitioners Reference. [s.l.] : [s.n.], 2004. 373 s.**
6. **TIPTON, Harold F., KRAUSE, Micki. Information Security Handbook : Volume 2. [s.l.] : [s.n.], 2006. 415 s.**
7. **TIPTON, Harold F., KRAUSE, Micki. Information Security Handbook : Volume 3. [s.l.] : [s.n.], 2009. 401 s.**
8. **SMEJKAL, V., RAIS, K. Řízení rizik ve firmách a jiných organizacích. [s.l.] : [s.n.], 2009. 354 s.**

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

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Cílem práce je vytvořit systém řízení bezpečnosti informací, ISMS, dle norem řady ISO 27000. Hlavní náplní práce je zpracovat analýzu rizik a vytvořit bezpečnostní politiku na základě výsledků analýzy pro zadanou společnost.

Klíčová slova: systém řízení bezpečnosti informací, rizika, aktiva, analýza

ABSTRACT

Goal of this thesis is to create information security management system using standards of ISO 27000 range. Main goal is to create risk analysis and security policy based on results of analysis for selected company.

Keywords: information security management system, risk, actives, analysis

Děkuji vedoucímu práce doc. Mgr. Jaškovi, Ph.D. za poskytnuté rady a Mgr. Barbaře Talandové za praktické konzultace.

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

Cílem této práce je vytvořit hlavní část dokumentů ISMS dle norem řady ISO 27000. Hlavními prvky zavádění ISMS jsou ohodnocení aktiv a analýza rizik. Základním dokumentem, kterým se pak řídí bezpečnost v organizaci, je Bezpečnostní politika vytvořená na základě poznatků a závěrů z analýzy rizik. V teoretické části práce bude nejprve sepsáno, jak by se měl takový systém informační bezpečnosti vypracovávat dle nejlepších zkušeností firem podílejících se na dlouholetém vývoji norem této řady. V praktické části pak bude provedeno ohodnocení aktiv organizace, vytvoří se analýza rizik a dle ní bude vytvořena Bezpečnostní politika a doporučená bezpečnostní opatření pro ochranu identifikovaných aktiv.

I. TEORETICKÁ ČÁST

1 VZNIK ISMS

ISMS, anglická zkratka pro Information Security Management Systém, česky systém řízení bezpečnost informací. Pod pojmem bezpečnost informací, resp. Bezpečnost informačního systému rozumíme ochranu veškerých informací, které jsou přenášeny, zpracovávány a uchovávány v rámci IS (informační systém). Problém bezpečnosti celého IS rapidně nabývá na významu. Nedostupnost informačního systému je v dnešní době pro mnoho firem kritické selhání a je nutné jej rychle řešit, ale hlavně mu předcházet. Tyto problémy, jejich vznik a následky řeší ISMS. Bezpečnost IS lze rozdělit na bezpečnost hardwarovou, softwarovou a ochranu dat s využitím bezpečnostních standardů. Důvodem pro vznik těchto standardů byla zejména potřeba sestavení praxí ověřených pravidel a doporučení v oboru managementu bezpečnosti informací. Těch na konci 20. století vznikla celá řada. Nejprve jako britský standard 7799, dále pak jako standard ISO 17799. V roce 2005 byl pak uveden v platnost nový komplexnější standard než jeho předchůdci pro ISMS s označením 27000. Spolu s řadou 27000 se ještě v souvislosti s ISMS využívá řada ISO/IEC standardů 20000. Ta se zaměřuje na management služeb v IT (informační technologie), zlepšování kvality, zvyšování efektivity a snižování nákladů u procesů IT. Tato řada se svými ustanoveními řídí IT Infrastructure Library (dále i jako „ITIL"). ITIL je rámec přístupů k zajištění dodávky kvalitních služeb. Knihovna ITIL je spravována organizací Office Of Government Commerce a je šířena formou školení, konzultací atp. (http://www.ogc.gov.uk/). Zavádění bezpečnosti informací je také popsáno v českých normách řady ČSN/ISO TR 13335. V případě této české normy je řada rozdělena do pěti částí, a každá se zabývá jednou z částí zavádění ISMS. Například první část se zabývá pojetím a modely bezpečnosti IT, zatímco část třetí se soustředí na techniky bezpečnosti IT.[6][7]

2 ZÁKLADY ISMS

Hlavní myšlenou ISMS je, že celá bezpečnost musí být řízena bez ohledu na velikost firmy. Celá koncepce se bude v různě velkých firmách lišit, ne však v jejich základech a principech. Systém řízení informací je jeden, rozdílné však mohou být jeho výklady doporučení a postupů jak jednotlivé cíle dosáhnout. Principem celého ISMS je takzvaný model PDCA (Plan-Do-Check-Act) Edwarda Deminga. Deming se proslavil zavedením tohoto modelu po 2. světové válce v Japonsku a díky jeho obrovským úspěchům se začal hojně používat. Tento model zavádí kontinuální systém řízení bezpečnosti informací v organizaci – tedy nejen jeho zavedení, ale i zdokonalování. Využívá tedy zpětné vazby získané ze zavedeného procesu řízení a její analýzou pak upravuje prvky procesu pro jeho zlepšování. Tím se celý proces ISMS nestává pouze jednorázovou záležitostí, nýbrž cyklickým procesem řízení bezpečnosti. Norma jasně popisuje, kterých náležitostí je nutno dosáhnout. To je popsáno v normě 27002 – Information Security Management systém příloha A. Ta je základem celého zavádění ISMS. [6][7]

V první fázi cyklu, tedy Plan, je nutné získat souhlas vedení společnosti se zavedením ISMS. Nutné je aby se v úvodním dokumentu vedení zavázalo k podpoře ISMS, což v praxi znamená vyčlenit jak personální, tak zejména finanční zdroje k jeho implementaci. Pokud společnost plánuje i certifikaci celého systému, je vhodné mít tento dokument dobře připraven – to však neznamená, že by měl být úvodní dokument rozsáhlý, musí však jasně prohlašovat ochotu vedení se zaváděním systému řízení bezpečnosti uvnitř organizace.

V druhém kroku, za předpokladu souhlasu vedení a na jeho základě, je vytvořen tým pro zavedení ISMS, je třeba provést identifikaci aktiv, jejich ocenění a zejména analýzu rizik. Aktivem se rozumí jakákoliv hmotná, či nehmotná (know-how, školení zaměstnanci) věc, která má pro společnost hodnotný význam. Identifikací a oceněním aktiv se přiřadí určitá hodnota v závislosti na jeho integritě, hodnotě a dostupnosti. Ta je pak použita v analýze rizik jako váha dopadu rizika na chod společnosti. Hodnota aktiva tedy není jen jeho pořizovací cena, ale je to průnik hodnot charakterizující celé aktivum. Analýza rizik je nejdůležitější dokument ISMS a je potřeba jej důkladně zpracovat. [6][7]

Následujícím krokem je vypracování dokumentu nazývaného „Návrh protiopatření“. V něm je popsáno, jak na nalezená kritická místa bude společnost reagovat. Jasně a stručně popisuje, jak by měl vypadat cílový stav, v jakém termínu a jaké finanční nároky vynaloží společnost v reakci na riziko. Tento dokument je velmi důležitý pro certifikaci ISMS

a v případě zájmu o certifikaci je tedy nutné jej zpracovat důkladně. Ne na všechna rizika je výhradně nutné hledat řešení. Například pokud by bylo odstranění rizika například extrémně drahé a jeho případný dopad na chod společnosti minimální. To se nazývá akceptace rizika. Doporučuje se však tohoto využívat v minimální míře. Na závěr tohoto kroku se vypracovává takzvané prohlášení o aplikovatelnosti. Jak již bylo zmíněno, v části 27002 jsou všechny náležitosti, které musí být zpracovány pro správné zavedení ISMS. V prohlášení o aplikovatelnosti je nutné krok za krokem vypsat, které části a jak jsou zavedené.

Poslední, čtvrtý, krok je nepovinný. Jedná se o certifikaci systému, ta však není podmínkou pro jeho zavedení. Pokud by se ale společnost rozhodla pro certifikaci, na úvod se certifikuje dokumentace ISMS, poté postupy při zavádění systému. [6][7]

Na závěr seznam dokumentů vypracovaných v průběhu zavádění ISMS:

- rozsah a hranice ISMS
- politika ISMS
- definice a popis k přístupu hodnocení rizik
- identifikace rizik
- analýza a vyhodnocení rizik
- identifikace a varianty zvládání rizik
- cíle opatření a bezpečnostní opatření pro zvládání rizik
- akceptace rizik
- získání povolení k provozování ISMS v rámci organizace
- prohlášení o aplikovatelnosti

Některé dokumenty je možné slučovat. Typicky se tak v rámci PCDA cyklu reviduje 5 dokumentů.

3 FÁZE ISMS

Jak již bylo řečeno dříve, ISMS se řídí Demingovým PCDA cyklem, což rozděluje proces zavádění a spravování ISMS do čtyř logických celků. Obsah jednotlivých etap je detailně popsán v normách ISO/IEC 27001 a ISO/IEC 27002.

3.1 Ustanovení ISMS

Cílem etapy ustanovení ISMS je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká. Dále stanovuje manažerské povinnosti vůči ISMS a na základě ohodnocení rizik je také nutné vybrat bezpečnostní opatření.

Ustanovení ISMS je možné dělit do následujících činností:

- určit rozsah a hranice ISMS na základě specifických rysů společnosti
- definovat politiku ISMS
- stanovit přístup organizace k hodnocení rizik
  - určit metodiku hodnocení rizik
  - vytvořit kritéria pro akceptaci rizik
- identifikovat rizika
- analyzovat a vyhodnotit rizika
  - dopady rizik, úrovně rizika, akceptovatelnost rizik
- zpracovat varianty zvládání rizik
- vybrat cíle opatření a jednotlivá bezpečnostní opatření
- získat souhlas vedení organizace se zbytkovými riziky a se zavedením ISMS [5]

3.1.1 Určení rozsahu a hranic ISMS

V této části je vhodné si shrnout cíle činnosti a organizace, organizační strukturu uvnitř firmy, umístění nemovitostí či využívané technologie pro přenos a zpracování informací. Na těchto základech lze pak stanovit rozsah a hranice ISMS, neznamená to však, že ISMS musí pokrývat celou organizaci. V takovém případě lze pak rozsah stanovovat dvěma způsoby, buď je rozsah ISMS shodný s rozsahem organizace, což vyžaduje značné finanční zdroje, nebo se ISMS aplikuje pouze na omezenou část organizace – například na

jednu pobočku, nejčastěji však na ucelený informační systém. Nemusí si však nutně jednat o nejdůležitější část organizace. Soustředění ISMS na dílčí části má dvě velké výhody. První je snadnější prosazení a obhájení účelnosti systematického řízení bezpečnosti. Druhá je omezené množství dat o ISMS, tedy i snadnější zvládnutí všech požadavků ISMS při jejich praktickém prosazování. Jinými slovy se tak zmenší množina možných problémů, které mohou nastat. [5]

3.1.2 Definice politiky ISMS

Politika ISMS vzniká na základě specifických potřeb organizace. Z praktického hlediska by však politika ISMS měla:

- specifikovat cíle ISMS a definovat základní směr a rámec pro řízení bezpečnosti informací
- zohledňovat cíle a zákonné požadavky
- vytvořila potřebné prostředky pro budování a údržbu ISMS
- stanovila kritéria pro hodnocení rizik
- být schválena vedením společnosti

Správně definovaná politika může velmi usnadnit budoucí prosazování pravidel na bezpečnost informací v rámci organizace. [5]

3.1.3 Přístup k hodnocení rizik

Na úvod slovník pojmů:

analýza rizik – systematické používání informací k odhadu rizika a k identifikaci jeho zdrojů [ISO/IEC Guide 73:2002];

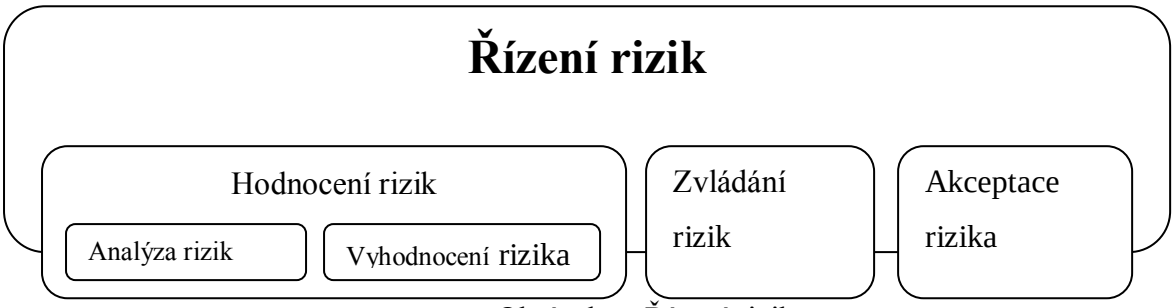
hodnocení rizik – celkový proces analýzy a vyhodnocení rizik [ISO/IEC Guide 73:2002];

vyhodnocení rizik – proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu [ISO/IEC Guide 73:2002];

management rizik – koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika [ISO/IEC Guide 73:2002];

zvládání rizik – proces výběru a přijímání opatření ke změně rizika [ISO/IEC Guide 73:2002];

Řízení rizik je klíčovým nástrojem pro systémové řízení bezpečnosti a tak přesná znalost rizik rozhoduje o výběru a prosazení bezpečnostních opatření pro snížení dopadů těchto rizik. Dalo by se říci, že řízení rizik je základem pro každý systém ISMS a ten navíc výrazně ovlivňuje efektivitu celého ISMS systému.



Obrázek 1: Řízení rizik

3.1.3.1 Teorie analýzy a řízení rizik

Analýza a řízení rizik slouží jako nástroj pro ochranu investic vynaložených do informačních systémů. Lze rozlišovat analýzu rizik dle její hloubky a podrobnosti:

Základní přístup

Postupy jsou rámcově zdokumentovány a organizace má celkovou koncepci a vizi řešení bezpečnosti informací.

Mezi výhody tohoto přístupu patří - pro podrobnou analýzu nejsou potřeba žádné zdroje, stejně tak jsou minimalizovány zdroje pro identifikaci základních ochranných opatření. Pro mnoho systémů mohou být bez velkých modifikací použita totožná nebo obdobná základní ochranná opatření.

Nevýhodami tohoto přístupu jsou – pokud je základní úroveň nastavena příliš vysoko může být pro některé systémy příliš nákladná, naopak pokud je úroveň nastavena nízko může být pro některé systémy bezpečnost nedostačující. Při aktualizaci systému pak již nemusí být dostačující základní ochranná opatření.[2]

Neformální přístup

Analýza se provádí náhodně bez dokumentace postupů.

Výhodou této metody je její jednoduchost, tedy není potřeba se učit nové postupy a dovednosti. Je to postup vhodný pro malé organizace.

Nevýhodami jsou – bez strukturovaného postupu je možnost opomenutí některých rizik nebo oblastí. Neformálnost postupu může způsobit neobjektivnost celého procesu subjektivními názory a zaujatostí pracovníka. Existuje velmi málo ospravedlnění zvolených opatření, je tedy obtížné zdůvodnit výdaje na ně potřebné. [2]

Podrobná analýza rizik

Všechna rizika jsou analyzována podrobně podle předem definované metodiky.

Výhodami tohoto přístupu jsou – je identifikovaná bezpečnostní úroveň vhodná pro potřeby systému. Řízení změn týkajících se bezpečnosti bude mít přínos z dodatečných informací získaných z analýzy rizik.

Hlavní nevýhodou se pak stává fakt, že k získání použitelných výsledků je potřeba značného úsilí, zdrojů a zkušeností. [2]

Kombinovaný přístup

Některá rizika jsou analyzována detailně, některá jsou případně záměrně opomenuta.

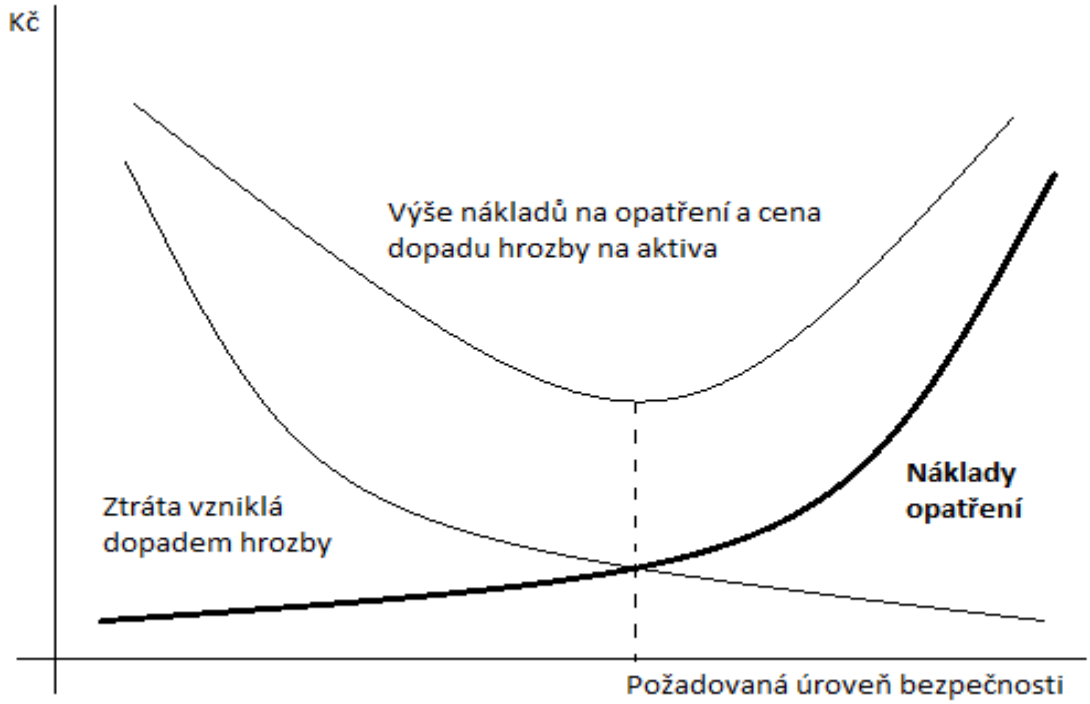
Mezi výhody této metody patří – použitím jednoduchého přístupu ke shromáždění potřebných informací může zvýšit pravděpodobnost přijetí programu managementu rizik. Umožňuje vybudovat okamžitý obraz organizačního programu bezpečnosti. Zdroje mohou být použity tam, kde to bude nejvýhodnější a u systémů, kde je vysoká pravděpodobnost rizika mohou být včas řešeny.

Nevýhodou této metody je, že pokud vede analýza rizik hrubé úrovně k nepřesným výsledkům, neměly by takto být řešeny systémy, u nichž je potřebná detailní analýza rizik.

Je možné v určitém časovém úseku také žádné bezpečnostní opatření nepřijímat. Někdy může být tento způsob nejvýhodnější.

Na základě analýzy rizik je pak možné určit jednotlivá bezpečnostní opatření vzhledem k identifikovaným hrozbám. Výběr opatření se stává součástí bezpečnostní politiky společnostmi. Důležitý faktor při výběru vhodných opatření hraje také ekonomická stránka. Ekonomický prvek je v praxi realizován ohodnocením aktiv adekvátní hodnotou (ve skutečnosti se jedná o vyčíslování ztrát v případě, že riziko nastane). Ohodnocování aktiv není jednoduchou záležitostí, protože se musí zvážit i případná škoda na know-how, dobré pověsti společnosti atd. Vhodné je aby se hodnocení aktiv účastnilo více manažerů společnosti, nejlépe z jiných oddělení – aktivum může mít jinou hodnotu pro vedení společnosti a jinou pro vedení některé z organizační jednotky. Vztah mezi ztrátou vzniklou

v případě zničení nebo poškození aktiva a náklady na realizaci aktiva jsou znázorněny na následujícím grafu. [2]



Obrázek 2: Závislost nákladů na úrovni bezpečnosti

Přestože jsou metody pro ocenění dopadu hrozby prověřenými způsoby, finální ocenění zůstává na vedení společnosti. [5]

3.1.3.2 Základní principy řízení rizik

Řízení rizik je složitou částí řízení bezpečnosti informací, který se snaží o identifikaci existujících rizik, vyjádření úrovně působnosti a určení nejvhodnějších opatření ke snížení vlivu těchto rizik na co možná nejlepší úroveň. V praxi je možné využít těchto metod:

- multidisciplinární přístup - vychází z pohledu mnoha uživatelů na rizika, jejich identifikaci, zvládání a akceptaci
- systematické a centralizované řízení – využívá standardizace postupů, jednotné koncepce, úplných postupů, plánování a využití zkušeností

- integrovaný proces – integrují se procesy pro řízení informatiky, řízení bezpečnosti informací, řízení kontinuity organizace atd.
- odpovědnost za činnost – zavádí se odpovědnost jednotek a jejich manažerů za řízení a zavedení v celé organizaci
- dokumentace – musí být kompletní a musí obsahovat postupy, které umožní zjistit odpovědnosti za provedená rozhodnutí
- zlepšování znalostí – vzhledem k cyklické povaze ISMS je nutné znalosti ukládat pro následný rozvoj systému řízení rizik a schopnost včas reagovat na případné změny
- pravidelná aktualizace – nutnost provádět pravidelné aktualizace systému na základě informací z externích zdrojů nebo monitorování celého systému nejméně jedenkrát ročně. [5]

Efektivita řízení rizik má významný vliv na fungování ISMS. Je vhodné poznamenat, že řízení rizik pracuje s odhady možných dopadů, které nemusí být vždy naprosto přesné. Proto vyšší úroveň nepřesnosti informací o rizicích a vyšší úroveň dynamiky zlepšuje postavení řízení rizik oproti jejich analýze.

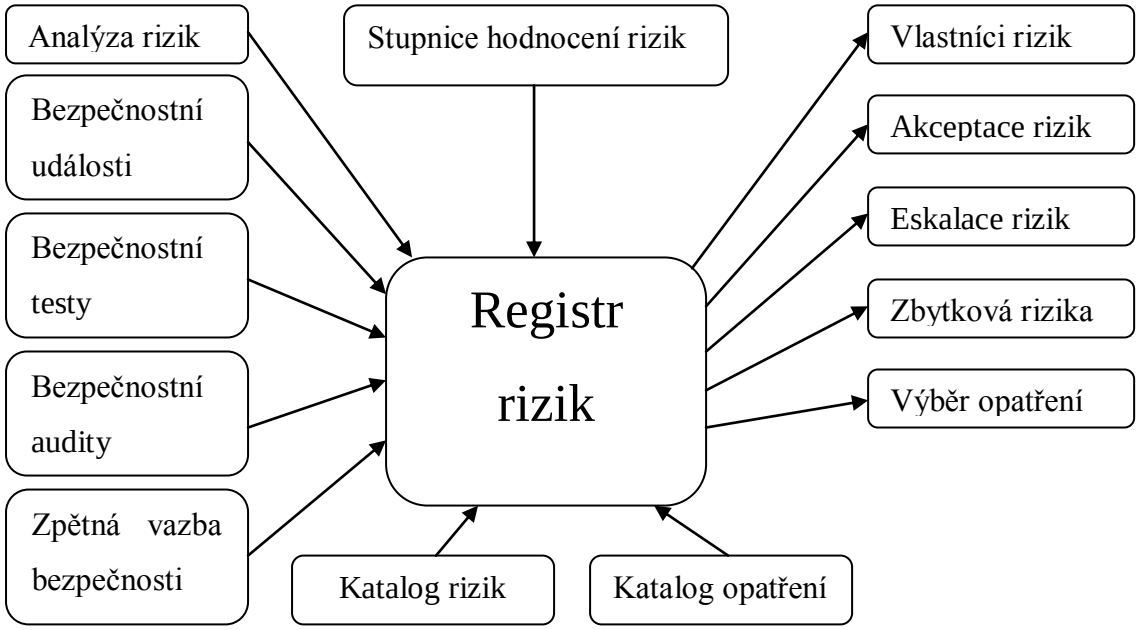
V praxi se dnes aplikují převážně klasické metody, což znamená provést relativně složité analytické operace, na jejichž výstupu jsou pak více či méně přesné znázornění existujících bezpečnostních rizik. To však má několik nedostatků. V prvé řadě začínají být pro klasické metody problémem složité interní vazby organizace, které se promítnou při výpočtech dopadu rizika a podobně. To pak značně omezuje flexibilitu celé analýzy. Dále i značné časové nároky na jednotlivé analýzy omezují flexibilitu systému. Je to dáno zejména tím, že klasické metody jsou navrženy jako jednorázové. Metody jsou soustředěny na analýzu rizik, zatímco zvládání rizik je bráno jako jednorázová činnosti. [5]

3.1.3.3 Moderní metody řízení rizik

Moderní metody nechápou řízení rizik jako jednorázovou analýzu a následný výběr protiopatření, ale jako každodenní činnost. Tím se přesouvá pozornost od analýzy k samotnému řízení rizik.

Základem moderních metod je takzvaný registr rizik, do kterého se ukládají informace o všech bezpečnostních rizicích. Cílem je pak všechna rizika evidovat, ohodnotit jejich

priority a určit osobu za rizika odpovědnou. Toto dovoluje rychle reagovat na nová rizika, revidovat priority již zavedených rizik a kontrolovat odpovědné osoby.



Obrázek 3: Registr rizik

Hlavní výhodou moderních metod je výrazné posílení schopnosti zvládání rizik. Metody dovolují sledovat životní cyklus rizika, dále zavádí nová vstupní kritéria pro hodnocení rizik. Těmi nejsou jen výstupy z analýzy ale také sebehodnocení, výsledky auditů, bezpečnostní testy a podobně. [5]

Pro samotnou analýzu je pak vhodné používat metody vhodné pro dané prostředí. Využívá se například metody FRAP (Facilitated Risk Analysis Process), která využívá zejména pracovních setkání mezi odborníky využívající IS a mezi IT pracovníky odpovědnými za vývoj a provoz systému. [5]

3.1.4 Hodnocení rizik

V případě hodnocení rizik je nejen nutné aby se celý proces opíral o jasně stanovená pravidla pro hodnocení a akceptaci rizik, je také ale nutné, aby vedení definovalo stupnice pro vyjádření veličin potřebných pro řízení rizik. Zejména je důležité definovat stupnice pro:

- míru důvěrnosti aktiv
- míru integrity aktiv
- míru dostupnosti aktiv
- míru dopadů a škod
- pravděpodobnosti uplatněné hrozby
- pravděpodobnosti zranitelnosti (selhání využívaných bezpečnostních opatření)
- vyjádření rizik a hladiny přijatelnosti rizika

Všechny tyto parametry pak ulehčují rozhodovací procesy při řízení rizik. Zvolená metoda by měla usnadňovat rozhodování při analýze, hodnocení a zvládání rizik. [5]

3.1.5 Význam aktiv ISMS

Jedním z prvních kroků celého řízení rizik je identifikace a ohodnocení aktiv, tedy hmotných i nehmotných prvků nějaké ceny pro organizaci. Aktiva lze dělit do 2 základních skupin:

- primární aktiva

  1. obchodní procesy – procesy, jejichž ztráta znemožňuje plnit poslání organizace, procesy nutné pro plnění právních náležitostí atd.

  2. Informace – informace důležité pro plnění poslání organizace, osobní informace, strategické informace, velmi nákladné informace

- sekundární aktiva – zejména aktiva hmotná, tedy software, hardware, komunikační sítě, pracovníci zajišťující chod organizace, prostory v nichž organizace funguje

Důležité je každému aktivu přiřadit tři hodnoty – míru důvěrnosti, integrity a dostupnosti. Pro řízení rizik jsou zejména důležitá primární aktiva, která odrážejí potřeby organizace s ohledem na ochranu informací. Identifikace a ohodnocení sekundárních aktiv má

zejména význam pro další rozhodování při zvládání rizik, protože jsou schopna upřesnit bezpečnostní potřeby. Je vhodné aktiva seskupovat podle jejich ohodnocení. To v dalších fázích značně ulehčuje práci. [5][2]

3.1.6 Analýza rizik ISMS

Tady je nutné identifikovat hrozby, které mohou ohrozit určitou skupinu aktiv. V ISO/IEC 27005 je katalog častých hrozeb. U hrozeb se v katalogu rozlišují tři původy zavinění – A (accidental – náhodný), D (deliberate – úmyslný), E (environmental – environmentální). Tady jsou příklady: [2]

Typ	Hrozby	Zdroj
Fyzické poškození	Požár	A, D, E
	Znečištění	A, D, E
	Závažná nehoda	A, D, E
Technická selhání	Selhání zařízení	A
	Přetížení inf. systému	A, D
	Chyba údržby	A, D
Neoprávněné činnosti	Neoprávněné použití zařízení	D
	Poškození dat	D
	Nezákonné zpracování dat	D
Poruchy způsobené zářením	Elektromagnetické záření	A, D, E
	Termální záření	A, D, E
	Elektromagnetické impulzy	A, D, E
Ohrožení funkčnosti	Chyba v používání	A
	Zneužití oprávnění	A, D
	Nedostatek personálu	A, D, E

Tabulka 1: Katalog hrozeb

Následující tabulka ukazuje příklady zranitelností pro různé sekce bezpečnosti včetně příkladů hrozeb, které mohou zranitelnosti využít. Nemusí ale nutně platit, že je zranitelnost využita pouze přiřazenou hrozbou.

Skupiny	Příklady zranitelností	Příklady hrozen
Hardware	Nedodržení pravidelné výměny	Zničení zařízení nebo médií
	Nechráněné uskladnění	Krádež médií nebo dokumentů
Software	Známé chyby v programech	Zneužití oprávnění
	Nechráněné tabulky s hesly	Falšování zpráv
	Široce rozšířené programy	Poškození dat
Sítě	Nechráněné komunikační linky	Odposlech
	Přenos odkrytých hesel	Vzdálená špionáž
	Bod totálního selhání	Selhání telekomunikačního zařízení
Zaměstnanci	Nedostatečné bezpečnostní školení	Chyba použití
	Nedostatek kontrolních mechanizmů	Nezákonné zpracování dat
	Nedostatek povědomí o bezpečnosti	Chyba použití
Lokality	Poloha v zátopové oblasti	Povodeň
	Nestabilní elektrická síť	Přerušení dodávky elektřiny
	Nedostatečná ochrana budov, dveří a oken	Krádež zařízení

Tabulka 2: Katalog zranitelností

Seznamy nejsou vyčerpávající ani v normách, hrozby a zranitelnosti jsou specifické pro každý obor a pole působnosti společnosti. [2]

3.1.7 Zvládání rizik

V konečném kroku zvládání rizik je nutné vybrat vhodná bezpečnostní opatření ke zjištěným rizikům, která jsou schopna je efektivně eliminovat. K tomu je možné využít katalog takových opatření v normě ISO/IEC 27002. V případě potřeby je možné opatření doplňovat nad rámec uvedený v normě. Celý postup by měl být také zdokumentován.

3.1.8 Akceptace rizik a souhlas se zavedením ISMS

Na základě výsledků řízení rizik by měla společnost odsouhlasit navrhovaná bezpečnostní opatření a odsouhlasit zbytková rizika, zda jsou přijatelná či ne. Pokud vedení zjistí, že požadovaná úroveň bezpečnosti nebyla dosažena, je možnost ještě včas upravit návrh bezpečnostních opatření. [5]

3.1.9 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti je povinný dokument, pokud společnost usiluje o certifikovaný systém. Prohlášení o aplikovatelnosti je dokumentované prohlášení, popisující cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná na ISMS organizace. [1]

V praxi se tento dokument stává jedním z nejdůležitějších díky systémovým vazbám, které postihuje. Doporučené formáty nejčastěji uvádějí matici vztahů mezi zjištěnými riziky a bezpečnostními opatřeními. Z té matice pak vyplývají důvody pro nasazení konkrétních bezpečnostních opatření a samotná realizace pak může na tyto důvody vhodně reagovat. V prohlášení jsou také jednoduše viditelná všechna pokrytá rizika, a je zároveň vhodné v tomto smyslu zapsat i nepokrývá rizika. V prohlášení také uvádíme, proč některá opatření nebyla přijata. Například odůvodnit neaplikování opatření A.11.7.2 pro práci na dálku využitím mobilních technologií může být velice jednoduché, pokud žádnou práci na dálku činnost organizace nevyužívá a nevyžaduje. V příloze A normy ISO/IEC 27001 je relativně rozsáhlý seznam bezpečnostních opatření. Na ty by se mělo v prohlášení o aplikovatelnosti odpovědět, a pokud nějaké opatření chybí a obtížně se zdůvodňuje jeho absence, je naopak většinou vhodné i tato opatření zavést. Seznam však není vyčerpávající a každá organizace může seznam rozšířit dle vlastních potřeb. Prohlášení o aplikovatelnosti má velký význam pro audit ISMS, kde již letmý pohled naznačuje kvalitu ISMS. Další význam spočívá v tom, že pokud je prohlášení uděláno pečlivě, je při ztrátě dokumentů bezpečnostní politiky snazší ji opět vypracovat za jeho pomoci. Dále je dobré

do prohlášení o aplikovatelnosti zavést i odkazy na umístění popisů daných bezpečnostních řešení. [5][1]

Tato etapa je velmi důležitou činností při zavádění ISMS protože její nedokonalosti se pak projeví v dalších procesech zavádění ISMS.

3.2 Provoz ISMS

V této etapě se usiluje o prosazení všech opatření, tak jak byla navržena a schválena v předchozí etapě. Zejména je důležité připravit plány a odpovědné osoby za prosazování. Opatření by pak měla být zdokumentována v Příručce bezpečnosti informací a mělo by dojít k jejich vysvětlení jednotlivým odpovědným osobám. V této etapě musí organizace:

- formulovat plán zvládání rizik, který vymezí činnosti a zdroje pro ISMS
- zavést plán zvládání rizik tak, aby dosáhl identifikovaných cílu opatření
- zavést bezpečnostní opatření
- určit metodu, jakou bude měřit účinnost těchto opatření a stanovit, jakým způsobem budou opatření
- zavést programy školení
- řídit provoz a zdroje ISMS
- zavést postupy a opatření pro rychlou detekci a reakci na bezpečnostní incidenty [5]

3.2.1 Plán zvládání rizik

Tento dokument popisuje všechny činnosti potřebné pro řízení rizik, stanovené cíle a priority těchto činností ISMS, omezující faktory a potřebné zdroje. Zde se také definuje osobní odpovědnost za provádění dílčích činností. Plán se sestavuje jednak z výstupu fáze ustanovení ISMS – zejména výsledky řízení rizik a pak také z pravidelného přehodnocování ISMS které by měly být zapsány ve zprávě o stavu ISMS. Dále je v hodné do dokumentu zapracovat činnosti vedoucí k snižování bezpečnostních rizik a také rutinní činnosti jako je audit, přezkoumání ISMS atd. [5][3]

3.2.2 Příručka bezpečnosti informací

Při prosazování bezpečnostních opatření je potřeba definovat stanovená bezpečnostní pravidla a odpovědnosti. Toho je dosaženo dokumenty jako bezpečnostní politika či směrnice bezpečnosti. Soubor těchto dokumentů se nazývá příručka bezpečnosti informací. Při tvorbě dokumentace je vhodné rozlišovat úrovně připravovaných dokumentů. Obvykle

na nejvyšší úrovni stojí dokumenty povinné pro zavedení ISMS (rozsah, politika, hodnocení rizik atd.). Na nižší úrovni je pak dokumentace sloužící k prosazování ISMS a ta by vždy měla být přizpůsobena konkrétnímu systému. Zde také patří ona příručka bezpečnosti informací. V té je důležité definovat dílčí procesy – tedy kdy, kdo, jak a co bude provádět. Na nejnižší úrovni se pak nachází pracovní postupy, které vysvětlují úkony pro naplnění dílčích procesů. Tato úroveň není ale vždy nutná a je možné se odkázat na příslušné dokumentace technických systémů.

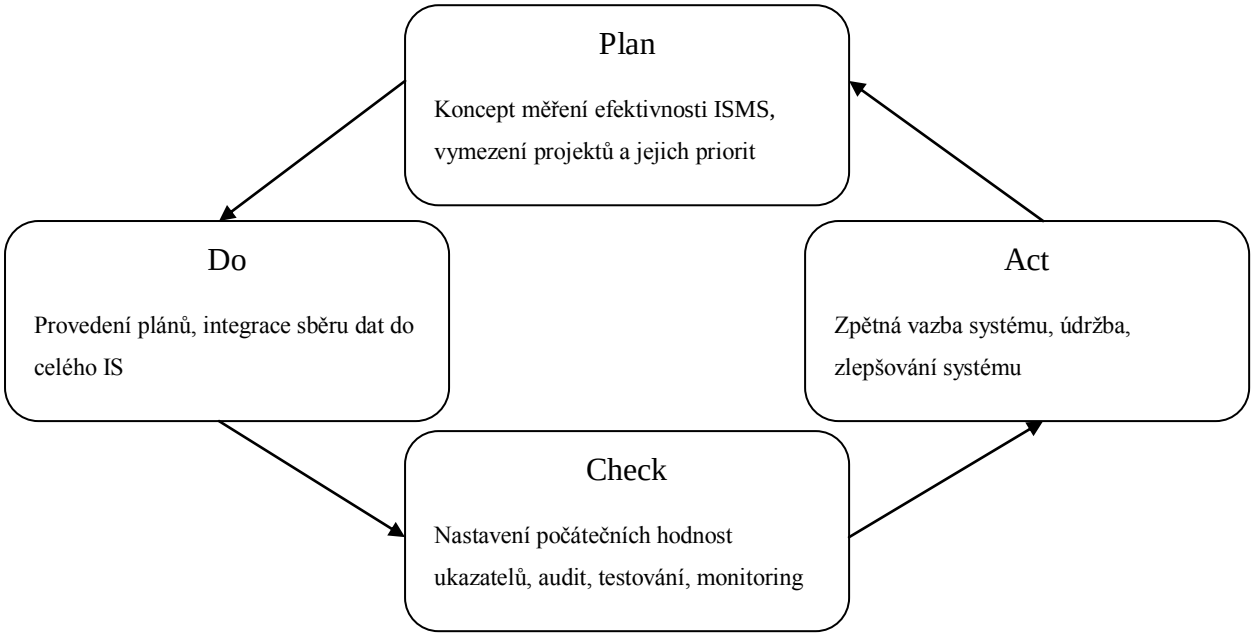
Hlavním cílem tvorby dokumentace je předání informací určité skupině pracovníků a tak by se měl této skupině podřídit i způsob popisu problematiky. Mění se tedy podrobnost popisovaných procesů, zaměření atd. Nejlepší dokumentace tedy není ta, co má nejvíce stránek, ale ta která je srozumitelná pro její cílovou skupinu. [5][3]

3.2.3 Školení o bezpečnosti

I když se tento bod může jevit jako podřadný, opak je pravdou. Pokud mají zaměstnanci dobré povědomí o bezpečnosti, dopouští se méně bezpečnostních chyb. Tento proces je velmi náročný, zejména také proto, že se stále opakuje jak v souvislosti se změnami celého systému, tak s obměnou zaměstnanců. Lidský faktor hraje významnou roli v mnoha rizicích a je tedy nutné pracovníky obeznámit se všemi jejich povinnostmi, případnými následky jejich počínání, bezpečnostními riziky a jak na případná rizika reagovat. [5]

3.2.4 Měření účinnosti ISMS

V této fázi je nutné sledovat účinnost nasazených opatření. Je nutné definovat a pravidelně sledovat objektivní data o skutečném fungování systému řízení bezpečnosti. Na jejich základech je pak vhodné dělat důležitá rozhodnutí.



Obrázek 4: PCDA pro měření účinnosti ISMS

Je nutné mít na paměti systém řízení účinnosti bezpečnosti již v začátcích navrhování ISMS, protože velmi podstatné kroky pro měření je potřeba provést již v první fázi cyklu. Jaké následky má případná chyba ve specifikaci ISMS a jaká je výše relativních nákladů na její odstranění, je uvedeno v následující tabulce. [5]

Etapa PDCA modelu	**Výše relativních nákladů v %**
Plánuj	1,00 %
Dělej	6,50 %
Kontroluj	15,00 %
Jednej	100,00 %

Tabulka 3: Náklady při chybě v postupech

V každé etapě je tedy nutné věnovat určitý čas přípravě účelnosti a účinnosti. V etapě „Plánuj“ jsou to tyto činnosti:

- zajistit soulad systému měření účinnosti se systémem řízení v organizaci
- navrhnout koncept měření účinnosti
- navrhnout metody měření účinnosti ISMS
- navrhnout ukazatele, podle nichž se bude měřit účinnost systému
- určit způsob sběru dat pro měření účinnosti
- určit způsoby vyhodnocování

V etapě „Dělej“ se musí úspěšně implementovat monitorování a vyhodnocování do systému ISMS již při jeho zavádění.

V etapě „Kontroluj“ je nutné, aby se:

- nastavily počáteční hodnoty ukazatelů
- otestoval systém měření
- provedl směr dat a monitoring za chodu ISMS

V poslední etapě „Jednej“ je zajištěn rozvoj, tedy jakási zpětná vazba systému. [5]

Je zejména nutné sestavení konkrétního systému ukazatelů včetně nastavení jejich výchozích hodnot a zajištění sběru dat pro pravidelné zkoumání. Existuje celá řada doporučení a zkušeností, jak využívat různé druhy ukazatelů pro různé informační systémy. Použití ale závisí na konkrétních podmínkách organizace, na možnostech sběru dat a vyhodnocování. Seznam některých ukazatelů je uveden například v normách ISO/IEC 27004, NIST SP800-55 a ISO/IEC 18028 1-5. Ukazatele pro měření bezpečnosti informací lze rozdělit podle předmětu měření na: [5]

- finanční
- personální
- technické – provoz IS

V následující tabulce jsou uvedeny návrhy některých ukazatelů pro měření účinnosti ISMS:

Název ukazatele	Hodnotí	Jednotka
Finanční náklady na bezpečnost informací/Finanční náklady na bezpečnost IS/ITS*100	Měří procento rozpočtu IS/ICT	Sleduje se v procentech finančního ukazatele
Pracovníci pracující v bezpečnosti informací /pracovníci v IS/ICT* 100	Měří procento času vynaloženého na IT	Sleduje se v procentech člověkohodin práce
Počet pracovních stanic s ochranou firewallem/ Počet všech pracovních stanic * 100	Měří rozsah implementace firewallu v organizaci	Sleduje se v procentech ochráněných stanic
Počet pracovních stanic s ochranou proti spamu /Počet všech pracovních stanic * 100	Měří rozsah ochrany proti spamu v organizaci	Sleduje se v procentech ochráněných stanic
Počet serverů s ochranou proti spywaru /Počet všech serverů * 100	Měří rozsah ochrany proti spywaru v organizaci	Sleduje se v procentech chráněných serverů

Tabulka 4: Příklady ukazatelů

V praxi převažují ukazatelé technické – tedy provozní – které byly navrženy na provoz IS/ITC. Rizikem využití finančních ukazatelů je fakt, že je velmi složité odlišit prostředky využité na řízení bezpečnosti a na samotný provoz společnosti. Proto je i vypovídající hodnota finančních ukazatelů velmi omezená a závisí na odpovědnosti pracovníků, kteří je vyhodnocují. Podobný problém nastává při vyčíslování ztrát při bezpečnostním incidentu. Obvykle se totiž vyčíslují pouze ztráty přímé, je nutné však zahrnout i práci bezpečnostních techniků atd. Kritické ukazatele by měly být nastaveny tak, aby čas pro jejich výpočet nebyl dlouhý, a vedení mohlo dostávat informace o důležitých sekcích ISMS v krátkých časových intervalech. Schéma a koncept ukazatelů pro měření bezpečnosti informací spolu s jejich významem a doporučenou frekvencí zjišťování jsou uvedeny v následující tabulce: [5][2]

Krizové řízení • indikátory hrozeb • detekce průniků do systému	**Strategické plánování** • řízení pomocí rozpočtu • alokace zdrojů • soulad s požadavky • řízení aktiv	**Vysoký**
Operativní řízení • ochrana proti škodlivým programům • řízení sítí • řízení bezpečnosti • údržba/správa	**Taktické plánování** • řízení zdrojů • ukazatele pro řízení životního cyklu vývoje aplikací • analýza auditních a logovacích záznamů	**Nízký**

Význam

Vysoká **Nízká**

Frekvence měření

Obrázek 5: Schéma ukazatelů

Řízení účinnosti je nedílnou součástí cyklu ISMS. Celková podoba a doporučení však vychází z návrhu celého systému. Měření celkové účinnosti organizace vychází z měření hlavních procesů, následně procesů vedlejších a podpůrných. [5][2]

3.2.5 Řízení provozu, zdrojů, dokumentace a záznamů

Při zavádění ISMS je nutné všechny činnosti řídit. To neznamená pouze postupovat dle dohodnutých stanov, ale je nutné i shromažďovat informace pro další fázi monitorování. Je podstatné vytvořit pravidla pro tvorbu, distribuci, schvalování a aktualizaci dokumentace řízení bezpečnosti. Současně je dobré vytvářet záznamy o jednotlivých provedených činnostech ISMS, ve kterých se objeví základní informace o provedené činnosti (kdo, kdy, výsledky činnosti apod.). Záznamy musí být prováděny tak, aby umožňovaly snadné vyhledávání určité skupiny aktivit. [5]

3.3 Monitoring ISMS

Cílem této etapy je zajistit vhodné zpětné vazby. V této souvislosti by mělo dojít k prověření všech bezpečnostních pravidel a jejich dopadů na ISMS. To zahrnuje jak prověření odpovědných osob, tak poznatků z interních auditů ISMS. Během fáze monitorování je tedy nutné provést následující kroky:

- monitorovat a ověřit účinnost bezpečnostních opatření
- provést interní audit pokrývající celý rozsah ISMS
- připravit zprávu o ISMS a na jejím základě přehodnotit ISMS [5]

3.3.1 Kontroly ISMS

Kontrola se prování zpravidla u osob odpovědných za chod ISMS. Tyto osoby dohlíží na dodržování bezpečnostních pravidel. Zároveň by měly dohlížet na to, zda zavedená bezpečnostní pravidla naplňují očekávání do nich vložená. Součástí monitoringu musí být i schopnost rychlé detekce chyb, úspěšných i neúspěšných pokusů o narušení bezpečnosti. Sem také patří i měření účinnosti ISMS a aplikování bezpečnostních opatření. [5]

3.3.2 Interní audity ISMS

Ten poskytuje nezávislý pohled na fungování a stav ISMS.

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 [ČSN EN ISO 9001:2000]

Audit by měl být rovnoměrně rozložen na celý rozsah ISMS při zvážení cílů a priorit ISMS. Audit by měl zejména prověřovat dva aspekty ISMS – prvním je dodržování procesních pravidel podle normy ISO/IEC 27001. Druhým aspektem je prověření fungování zavedených bezpečnostních pravidel dle normy ISO/IEC 27002 – auditoři prověřují způsob, vhodnost a míru prosazení aplikovaných opatření. [5]

3.3.3 Přehodnocování ISMS vedením společnosti

Přezkoumávání na základě zpráv získaných monitoringem by mělo být prováděno alespoň jednou ročně. Je vhodné při nově zavedených ISMS provádět přezkoumávání častěji než pouze jednou za rok.

Přezkoumání – činnost prováděná k určení vhodnosti, přiměřenosti a efektivnosti předmětu přezkoumání k dosažení stanovených cílů [ČSN EN ISO 9001:2000]

Jako vstupy slouží zejména následující skutečnosti:

- výsledky interních auditů
- zpětná vazba uživatelů a zainteresovaných třetích stran
- existující slabiny a hrozby
- výsledkům měření účinnosti ISMS
- změnám ovlivňující ISMS
- získaným doporučením pro zlepšení ISMS [5]

Na základě těchto vstupů dochází k vyhodnocení silných a slabých stránek ISMS. Toto se nazývá SWOT analýza. SWOT je anglickou zkratkou slov Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti) a Threats (hrozby). Následující obrázek znázorňuje schéma SWOT analýzy.

SWOT	**S – Strengths**	**W - Weaknesses**
O - Opportunities	Strategie SO	Strategie WO
T - Threats	Strategie ST	Strategie WT

Tabulka 5: SWOT analýza

Strategie SO – využití silné stránky pro získání výhody

Strategie WO – překonat slabiny využitím příležitosti

Strategie SW – využít silné stránky proti hrozbám

Strategie WT – minimalizovat náklady a čelit hrozbám

Výsledkem přehodnocení ISMS je obvykle zpráva, která shrnuje, co funguje dobře a zda je možné se o tyto vlastnosti opřít. Tato zpráva by měla být především orientovaná na budoucnost, ve které by se například mohla uzavřít dohoda s vedením o prohlubování bezpečnosti. Zpráva také definuje cíle pro další období a tak je možné vyčlenit i příslušné zdroje. [9]

3.4 Údržba a zlepšování ISMS

V této fázi by mělo docházet ke zlepšování všech nedostatků, takzvaných neshod systému. Je tedy vhodné zavést vylepšení chodu ISMS a provést odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků. Níže jsou vysvětleny použité termíny.

Neshoda (nonconformity) – nesplnění požadavků [ČSN EN ISO 9001:2000]

Náprava (correction) – opatření pro odstranění zjištěné neshody [ČSN EN ISO 9001:2000]

Opatření k nápravě (corrective action) – opatření k odstranění příčiny zjištěné neshody nebo jiné nežádoucí situace [ČSN EN ISO 9001:2000]

Preventivní opatření (preventive action) – opatření k odstranění příčiny potenciální neshody nebo jiné nežádoucí potenciální situace [ČSN EN ISO 9001:2000]

3.4.1 Zlepšování a odstraňování nedostatků ISMS

Základem zlepšování ISMS je využití pozitivní zpětné vazby. Je vhodné, aby se zlepšování z velké části zakládalo na podnětech aktivních uživatelů. Takové praktické nápady jsou nenahraditelné a jejich zpracování by měla být věnována velká pozornost. Neznamená to ale, že se každý nápad musí automaticky zavést. Je nutné zvážit všechny dopady možného zlepšení, rizika z jeho zavedení plynoucí apod.

Pro odstraňování nedostatků existují dvě formy opatření:

- preventivní opatření
- opatření k nápravě

Preventivní opatření je proaktivní formou řešení nedostatků ISMS. Řeší možný výskyt nedostatku a jeho případné řešení, neznamená to ještě ale, že nedostatek se nějak projevil. Předpokládá se však, že je nutné je co nejdříve vyřešit.

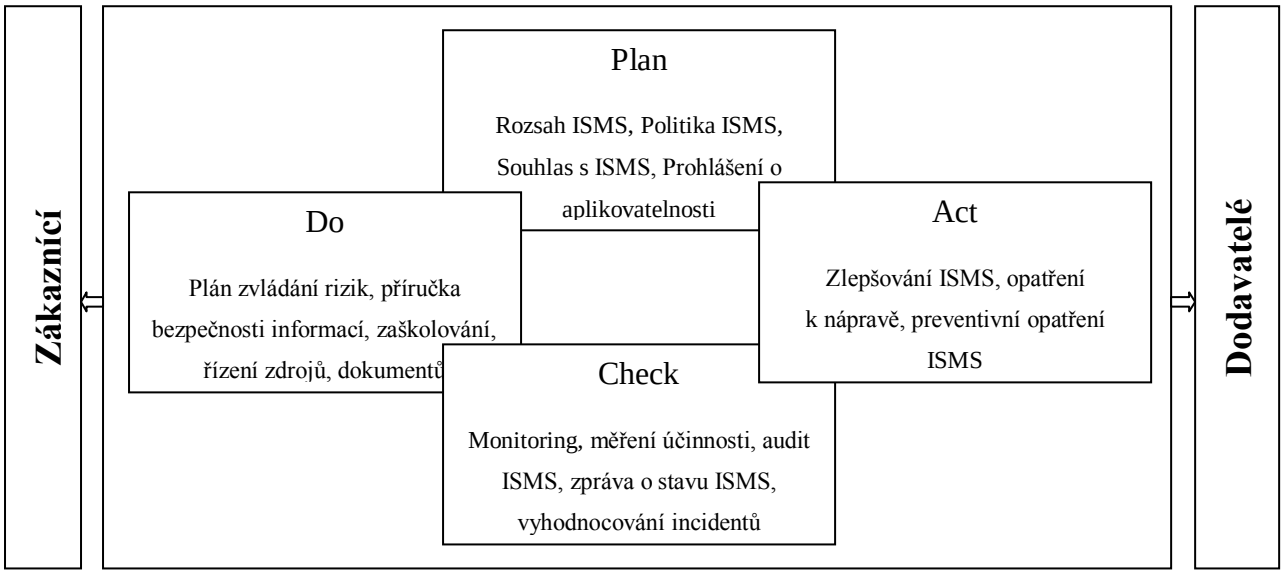
Opatření k nápravě je reaktivní formou řešení nedostatku. Nedostatek se již nějak projevil a je nutné jej adekvátním způsobem řešit.

Při řešení nedostatku je vhodné se zaměřit i na souvislosti s daným nedostatkem, neřešit pouze nedostatek samotný. Tím dosáhneme vyšší šance vyhnout se opakování výskytu nedostatku. Postupy pro řešení opatření k nápravě a prevenci musí být zdokumentovány. Je dobré následně přezkoumat, zda zavedené opatření dosáhlo kýženého efektu. Nejčastější

příčinou objevování nedostatků se v praxi ukazuje být neznalost všech souvislostí v systému. [5]

3.5 Shrnutí cyklu ISMS

Základem celého systému řízení bezpečnosti jsou doporučení normy ISO/IEC 27001, která využívá model PCDA.



Obrázek 6: Cyklus PDCA

V posledních letech se poslední úpravy normy ISO/IEC 27001 zaměřují zejména na:

- aplikaci vhodných forem měření účinnosti ISMS – upřesnění vhodných ukazatelů pro zjišťování účinnosti ISMS
- rozšíření obsahu prohlášení o aplikovatelnosti
- pravidelnou aktualizaci ohodnocení rizik

Pro úspěšné zavedení ISMS jsou nezbytné především následující činnosti:

- vymezení rozsahu ISMS
- definice politiky ISMS
- analýza a zvládání rizik
- prohlášení o aplikovatelnosti
- plán zvládání rizik
- záznamy
- přehodnocení

Tyto prvky ISMS by neměly být v žádném případě opomenuty, pokud chceme dosáhnout solidně fungujícího bezpečnostního systému. [5]

4 BEZPEČNOSTNÍ OPATŘENÍ

Druhým základním dokumentem je norma ISO/IEC 27002 (dříve ISO/IEC 17799). Ta obsahuje takzvané nejlepší zkušenosti při řízení bezpečnosti. V ní je 133 bezpečnostních opatření rozdělených do 11 oblastí. Jejich rozdělení lze vidět na následujícím obrázku: [5]

Obrázek 7: Oblasti bezpečnosti informací

4.1 Bezpečnostní politika

Bezpečnostní politika (Security Policy) – pravidla, směrnice a zvyklosti určující způsoby, pomocí kterých jsou v dané organizaci a jejích systémech řízena, chráněna a distribuována aktiva, včetně citlivých informací [ČSN ISO/IEC 21827:2003]

Norma obsahuje dvě doporučení. Prvním je potřeba naformulovat dokument bezpečnostní politiky, kde vedení organizace:

- vyjádří cíle a význam bezpečnosti
- stručně upřesní výklad základních bezpečnostních pravidel a zásad
- vyjádří svůj zájem o rozvoj bezpečnosti v rámci organizace

Druhým doporučením je zajištění pravidelných revizí dokumentu bezpečnostní politiky, kterými by měla být pověřena odpovědná osoba. Při přezkoumávání by měla být hodnocena zejména vhodnost, přiměřenost a efektivnost stanovených opatření. [1][5]

4.2 Organizace bezpečnosti informací

Tato část normy pak klade požadavky na organizaci bezpečnosti informací. Organizace se dělí na dvě části – interní organizace a externí organizace. Norma předkládá osm opatření. Prvním opatřením s názvem „Závazek vedení směrem k bezpečnosti informací“ se požaduje po vedení, aby podporovalo a hlavně se také řídilo všemi bezpečnostními pravidly, které se v rámci ISMS zavedou. Tím také vedení dává najevo, že zavedená pravidla považuje za správná a účelná.

Další opatření je zaměřeno zejména na větší organizace a popisuje způsob koordinace při řízení bezpečnosti. Jde tedy o to, aby byl zajištěn jednotný výklad všech pravidel.

Smyslem dalších dvou opatření je upřesnění rolí, pravomocí a odpovědností při řízení bezpečnosti informací. V prvním opatření se zejména klade důraz na upřesnění úrovně oprávnění zmocněných osob. V druhém opatření se pak norma soustředí na upřesnění pravomocí.

V pořadí páté opatření ustavuje požadavek na uzavírání dohod o ochraně informací se všemi, kteří pracují s jakýmikoliv důvěrnými informacemi. V tomto opatření je také popsán věcný obsah takovýchto dohod mezi subjekty.

Šesté a sedmé opatření je směřováno na udržování kontaktů na orgány veřejné moci a zájmové skupiny. To umožňuje rychlejší nápravu škod a podobně.

Poslední, osmé, opatření zavádí do organizace nezávislý prvek, který by měl na základě žádosti vedení provést nestranné přezkoumání bezpečnosti, které zhodnotí, zda je prosazování bezpečnosti dostatečně účinné. Opatření zdůrazňuje nezávislost tohoto přezkoumání, což se může jevit problematické u malých firem.

Druhým blokem bezpečnostních opatření této sekce jsou pravidla pro zajištění bezpečnosti u externích subjektů. Je tedy nutné identifikovat aktiva, která jsou spojena s daným subjektem a uzavřít dohody jak o přístupu klientů, tak třeba třetích stran. [1][5]

4.3 Řízení aktiv

Cílem této oblasti je nalezení a udržování adekvátní ochrany pro všechna identifikovaná aktiva v rámci ISMS. Pro tyto potřeby jsou definované dvě skupiny bezpečnostních opatření. První skupina se zaměřuje na určení odpovědnosti za aktiva. Toto je popsáno ve třech bezpečnostních opatřeních. První doporučuje pečlivou evidenci aktiv, která umožní určit, která z aktiv jsou pro organizaci důležitá. Další opatření popisuje nutnost určení vlastníka aktiva, čímž také určí odpovědnost za aktivum. Poslední opatření stanovuje přípustné použití aktiv. To v praxi znamená, že jsou pro aktiva, nejčastěji však skupiny aktiv, určena pravidla jejich používání.

Druhá skupina opatření určuje způsob klasifikace informací, jejímž základem je zákon č. 412/2005 Sb., ochraně utajovaných informací, ve znění pozdějších předpisů. Organizace by si tak měla vytvořit vlastní schéma klasifikace informací pro její potřeby. Většina malých organizací ani nepřijde do styku s klasifikovanými informacemi, tak jak je popisuje zákon. I tak je vhodné, aby si organizace provedla vlastní klasifikaci informací podle jejich významu a důležitosti. Jedno z opatření této skupiny také definuje nutnost upřesnění pravidel a postupů nutné pro ochranu informací. [1][5]

4.4 Bezpečnosti lidských zdrojů

Důležitou oblastí bezpečnosti je bezpečnost z hlediska lidských zdrojů. Opatření jsou v normě rozdělena podle toho, kdy jsou použita – před vznikem pracovního vztahu, během pracovního vztahu a při ukončení nebo změně pracovního vztahu.

Opatření uplatňující se před vznikem pracovního vztahu se zabývají ustanovením a dokumentací bezpečnostních rolí a odpovědností pracovníka. Zavádí prověrky pracovníků – prověrky totožnosti, dosaženého vzdělání, absolvovaná školení, certifikáty apod. V případě nutnosti i například výpis z trestního rejstříku či reference. Je důležité ale dbát na to, aby činnosti byly prováděny v souladu s platnými zákony. Poslední doporučení se zabývá dohodnutím přesných podmínek o výkonu práce.

Pro rozvoj bezpečnosti informací v průběhu pracovního vztahu jsou důležitá tři opatření. První definuje odpovědnost vedoucích pracovníků, jejich povinnost seznamovat podřízené s bezpečnostními pravidly atd. Další opatření popisuje nutnost prohlubovat bezpečnostní povědomí zaměstnanců formou školení a seminářů. Smyslem je promítnou všechna

bezpečnostní pravidla do činností pracovníků. Poslední opatření definuje disciplinární řízení pro řešení porušení bezpečnostních pravidel. Sankce mohou být napomenutí při mírnějším prohřešku, až po finanční či změnu pozice pracovníka při prohřešku vážnějším.

Poslední skupina opatření se zaměřuje na období ukončení pracovního vztahu. Podobným způsobem jako tyto opatření by měly být navrženy i opatření spojené se změnou pozice pracovníka. Hlavní opatření stanovuje jasné odpovědnosti spojené s ukončením pracovního procesu. Je nutné zdůraznit, že závazky o mlčenlivosti platí pro zaměstnance i po skončení pracovního poměru. Dalším opatřením je vrácení všech zapůjčených věcí. V těchto případech může být navrácení dat například ze soukromého notebooku velmi obtížné, proto použití soukromých prostředků nebývá u určitých typů společností provoleno vůbec. Posledním opatřením je uzamčení či zrušení všech účtů pro přístup jak do počítačových stanic, tak do budov. [1][5]

4.5 Bezpečnost prostředí a fyzická bezpečnost

Tato opatření tvoří dvě skupiny – zabezpečené oblasti a bezpečnost zařízení. Opatření skupiny zabezpečené oblasti má za úkol chránit prostředí organizace jako celek. Naproti tomu fungují opatření ze skupiny bezpečnost zařízení jako ochrana dílčích součástí ICT.

Skupina opatření zabezpečené oblasti je tvořena šesti opatřeními. Základem je vytvoření fyzického bezpečnostního perimetru ploty, zdmi, signalizací vniku do prostoru atd. Další opatření se soustředí na kontrolu fyzického vstupu. Součástí je například označení osob, identifikace, doprovázení návštěv apod. Další opatření se aplikuje, pokud zjištěná rizika v rámci ISMS vyžadují dodatečnou ochranu místností a prostředků ve kterých se nachází zvláště citlivé informace nebo jsou obzvláště důležité pro chod organizace – datová centra apod. Tato místa pak pokrývá ještě další opatření ochranou z vnějšku. Tedy proti požáru, prachu, vodě atp. Následující opatření zavádí pravidla pro osoby pracující v takových prostorech. Poslední opatření této skupiny se zaměřuje na ochranu veřejně přístupných prostor a prostor pro manipulaci se zbožím. Toho lze dosáhnout například recepcí pro evidenci externích příchozích, nebo označením zboží čipy.

Balík opatření zaměřující se na bezpečnost zařízení obsahuje sedm částí. První doporučení se týká umístění zařízení a to tak, aby byla zajištěna jejich fyzická ochrana. Snahou je minimalizovat přístup k nim, omezit možnosti neoprávněného sledování a podobně. Další opatření doporučuje využití UPS zdrojů, tedy záložních zdrojů pro nepřerušený chod

zařízení. Další opatření sleduje zabezpečení kabelových rozvodů v organizaci. Tedy zajištění dostatečné fyzické ochrany a vedení kabelů místy s minimálním rušením. Pro vyšší životnost je vhodné zařízení adekvátně udržovat, což pokrývá další opatření. Další dvě opatření pokrývají ochranu zařízení i mimo prostory společnosti či při jejich přesunu. Poslední opatření se zabývá důslednou likvidací datových médií a to z důvodu aby na nich nezůstávala žádná data i po jejich vyřazení. Toho lze dosáhnout jak softwarově, tak silným elektromagnetickým polem, které zničí data na magnetických médiích. V poslední řadě pak fyzické zničení médií. [1][5]

4.6 Řízení provozu a komunikací

Tato oblast normy popisuje v deseti skupinách opatření. V prvním opatření zavádí stanovení provozních procesů, postupů a pravomocí. Opatření se soustřeďuje na dokumentaci důležitých provozních procesů (start, stop, přerušení či obnova systému, zálohování atd.). V této skupině jsou ještě uvedena opatření popisující neslučitelnost určitých rolí v systému (auditor nemůže být zároveň manažerem systému). Podobně další opatření odděluje prostředky určené pro vývoj a testování.

Druhá skupina opatření usnadňuje řízení outsourcingu (dodávky služeb třetími stranami). Soustředí se na to, aby specifikace dodávek obsahovaly parametry bezpečnosti a dostupnosti. Tyto závazky by pak měly být monitorovány, aby nedocházelo k odchylkám v průběhu platnosti smlouvy.

Skupina opatření s názvem „plánování a přejímání informačních systémů“ postihuje zejména dvě oblasti. První je zejména sledování míry využití stávajících možností informačního systému a cílem odhalovat kapacitní nedostatky a případně na ně včasně reagovat. Druhou oblastí jsou opatření související s předáním nově vyvinutých IS či jejich částí do ostrého provozu. Zde je vhodné kromě ověření všech funkcí také zajistit předání veškeré potřebné dokumentace a know-how na jeho obsluhu.

Další skupina se nazývá „ochrana proti škodlivým programům a mobilním kódům“ a řeší antivirovou problematiku, která je rozšířena o ochranu proti spyware a malware. Doporučení je pak možno shrnou do tří nejdůležitějších závěrů:

- použití antivirového programu
- pravidelná aktualizace definic AV – antivirový program
- prohlubování znalostí o bezpečnosti manažerů a uživatelů systému

V pořadí pátá skupina se zaměřuje na zálohování dat a programového vybavení pro možnost případné obnovy. Opatření by se opět dala shrnout do několika nejdůležitějších bodů:

- vytvořit plán zálohování
- dodržovat tento plán
- testovat čitelnost zálohovaných dat
- vhodně a bezpečně uložit tyto zálohy

Skupina šestá má za úkol zajistit správu bezpečnosti komunikační sítě. Snaha je o definování pravidel a koordinaci bezpečnostních činností. Důležité je prosazovat bezpečnost jako součást komunikačních služeb a využívat moderní bezpečnostní technologie (bezpečnostní brány, virtuální sítě).

Další skupina opatření se zaměřuje na bezpečnost při zacházení s médii. Základem je údržba a správa vyměnitelných médií – HDD disků, flash disků, disket apod. Ta by měla zajistit evidenci a sledování jejich předpokládané životnosti. Jedno z opatření také popisuje spolehlivou likvidaci starých či vadných nosičů.

Jeden z balíků opatření se zaměřuje na elektronickou výměnu informací mezi danou organizací a jejími partnery. První část se věnuje formální stránce komunikace a vyžaduje definici smluvního základu, kterým se bude výměna řídit, a stanovení základních pravidel která jsou s výměnou dat spojena (ochrana médií během přepravy). Druhá část se zaměřuje na výměnu dat elektronickou poštou nebo s využitím informačních systémů. U informačních systémů, které jsou určeny k výměně informací, je vhodné sledovat jeho zranitelnosti a co nejrychleji pak na případnou zranitelnost reagovat (patch IS).

Předposlední skupinou opatření jsou služby elektronického obchodu, která se zabývá různými formami moderních nástrojů pro jak statickou webovou stránku tak e-shop.

Poslední, desátou, skupinou opatření je monitorování provozu informačních systémů včetně zaznamenávání činností uživatelů a správců. Ta obsahuje několik opatření pro sběr a vyhodnocení informací o fungování systému a uživatelů. Cílem je schopnost včas odhalit možná ohrožení ze strany správců či uživatelů a také zajistit důkazy pro řešení incidentů či pro audit. [1][5]

4.7 Řízení přístupu

Základem řízení přístupu je sledování jeho požadavků a stanovení politiky jeho řízení, která by se měla promítat do všech IS a aplikací. Důležité je vázat přístupová práva na skupiny, ne na jednotlivce.

Druhá skupina opatření řeší přístup uživatelů IS k aktivům organizace. Ta doporučuje, aby každý uživatel měl jedinečnou identitu, aby nedošlo k omylu.

Skupina s názvem „odpovědnosti uživatelů“ zahrnuje povinnosti uživatelů jak chránit uživatelská hesla, povinnost odhlašovat se ze systému při nepřítomnosti (lunch-break), nenechávat rozdělanou práci na stole při nepřítomnosti atd.

Další tři skupiny se zaměřují na přístup k síti, řízení přístupu k operačním systémům a řízení přístupu k datům a aplikacím. Poslední skupinou jsou opatření postihující mobilní zařízení a práci na dálku.

Celá problematika řízení přístupu se opírá o tři pojmy, resp. činnosti:

Identifikace – proces, který umožní rozpoznání entity, obvykle za použití unikátních prostředků výpočetní techniky zpracovatelných jmen. Jména bývají jedinečná v rámci určité skupiny, jejíž rozsah je dán systémovou politikou. [9]

Autentizace – je proces ověřování proklamované identity subjektu. Autentizace znamená ověřování pravosti, autentický znamená původní, pravý, hodnověrný. Autentizace patří k bezpečnostním opatřením a zjišťuje ochranu před falšováním identity, kde se subjekt vydává za někoho, kým není. Rozlišujeme autentizaci entity a autentizaci zprávy. [9]

Autorizace – znamená oprávněnost, autorizovat znamená povolit, schválit, zmocnit. O autorizaci hovoříme, pokud určitá entita chce přistupovat k určitým zdrojům. Aby mohla entita ke zdrojům přistoupit, musí být k tomu autorizována – oprávněna. Předpokladem autorizace je úspěšná autentizace. [9]

V praxi jsou tedy tyto činnosti využity následovně: Uživatel se snaží přistoupit k nějakému systému, kde se musí nejdříve identifikovat – to je zadáním login jména. Tato informace se následně ověří autentizací, nejčastěji zadáním příslušného hesla. Lze také využít různé nástroje biometriky pro autentizaci. Na základě prokázané identity se pak prověřuje, zda má konkrétní entita usilující o přístup požadovaná oprávnění – autorizace. [1][5]

4.8 Vývoj a údržba IS

Tato oblast obsahuje zejména opatření související s rozvojem informačních systémů. To jsou například různorodá opatření, nejčastěji v souvislosti se softwarovými aplikacemi, jejich rozvojem a údržbou.

Nejdůležitější skupinou jsou opatření definující bezpečnostní požadavky systémů. Tedy jejich analýza a specifikace, která by měla být zahájena už při výběru nových IS.

Druhá skupina opatření se zaměřuje na správné zpracování dat v aplikacích. Cílem je zavést kontrolní mechanismy, které ověří smysluplnost vstupních i výstupních dat a zajistí ochranu dat při předávání mezi aplikacemi. K tomu je možné využít technik, jako jsou kontrolní součty, bilanční kontroly atd.

Třetí skupina se zabývá kryptografií (kryptografie je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí) a její aplikací na data. Základem je definice pravidel kryptografie, zvolení metod, algoritmů a odpovědností. Samostatně se opatření věnují i správě klíčů – ta zahrnuje jejich generování, rušení, distribuci, uložení aktualizaci atd.

Další skupina opatření se věnuje bezpečnosti systémových souborů. Snahou je kontrolovat jaké aplikace jsou na systémy instalovány a zda jsou řádně prověřeny (neobsahují viry apod.).

Skupina opatření s názvem „bezpečnost procesů vývoje a podpory“ se zaměřuje na prosazení pravidel při vývoji aplikací. Opatření jsou určena pro řízení změn či ověření aplikací po úpravách operačního systému.

Poslední skupina, řízení technických zranitelností, doporučuje včasnou instalaci všech dostupných záplat, ale až po ověření jejich schopnosti fungovat v daném prostředí. [1][5]

4.9 Zvládání bezpečnostních incidentů

Tato skupina opatření je dělena na dvě části - první nabádá uživatele k hlášení všech bezpečnostních incidentů, slabin či podezřelých situací. Druhá je pak určena pro IT specialisty a upřesňuje kroky pro zvládání incidentů a jejich nápravě. Zde je v první řadě nutné definovat postupy a odpovědnosti, které zajistí rychlou reakci případně nápravu na možné incidenty. Další opatření se věnují rozboru vzniklých incidentů s cílem zamezit jejich opakovaný výskyt a celkové zlepšení systému bezpečnosti.

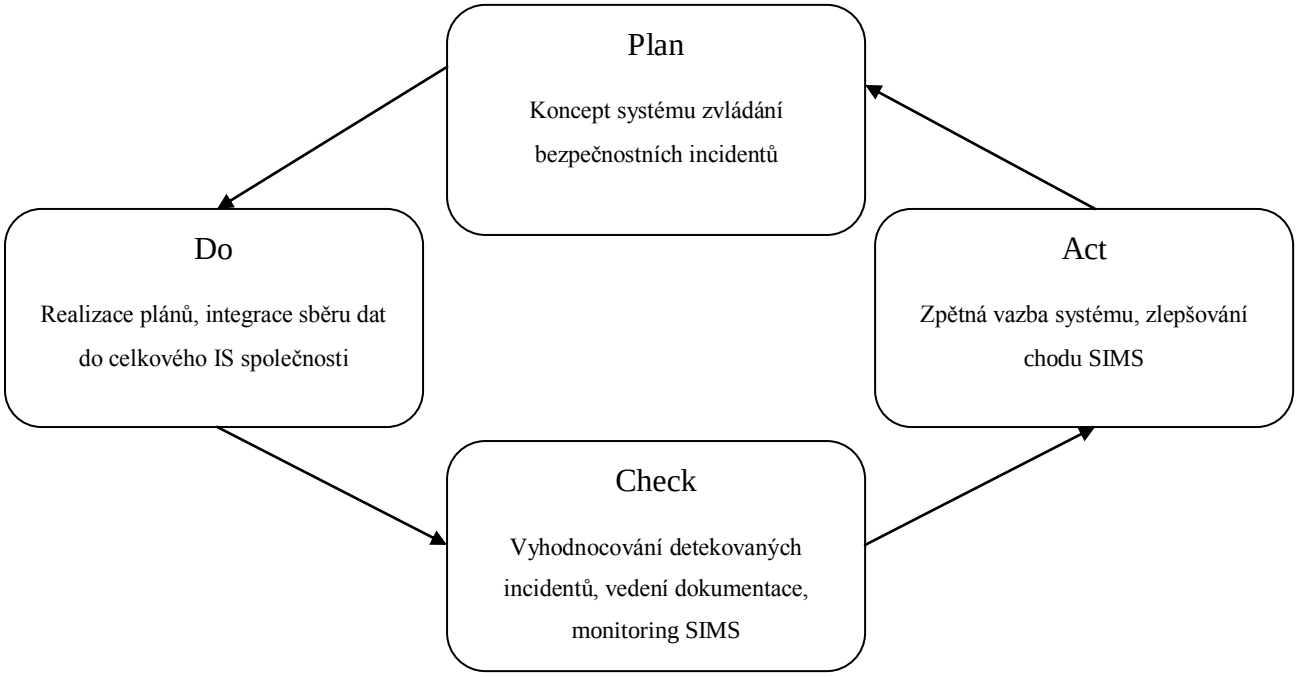
V souvislosti s touto problematikou je vhodné definovat dva základní pojmy:

Bezpečnostní událost – lze označit za identifikovaný stav informačního systému, služby nebo počítačové sítě, jež může narušit pravidla bezpečnostní politiky nebo selhání opatření nebo dříve neznámá nebo nepředpokládaná situace, jež může ovlivnit bezpečnost. [ISO/IEC TR 18044]

Samotný vznik události ještě není incidentem. Tím se stane až po jejím vyhodnocení.

Bezpečnostní incident – je jedna nebo více nechtěných nebo neočekávaných indikovaných bezpečnostních událostí, jimiž může být s vysokou pravděpodobností narušena podpora hlavních procesů organizace nebo díky nimž může dojít k narušení bezpečnosti informačního systému. [ISO/IEC TR 18044]

Pro řešení bezpečnostních incidentů se využívá aplikace modifikovaného Demingova modelu PDCA: [1][5]



Obrázek 8: Model SIMS

II. PRAKTICKÁ ČÁST

5 ANALÝZA INFORMAČNÍHO SYSTÉMU SPOLEČNOSTI

Firma se zabývá tvorbou projektů pozemních staveb. Ve firmě se nachází 38 počítačů, 30 z nich je využíváno pro samotnou projekci, 3 počítače mají manažeři jednotlivých úseků, 1 majitel firmy, 1 sekretářka majitele, 1 účetní a 2 servery. Servery jsou obyčejné PC s mírně poupravenou stavbou hardwaru. Každé PC má 2 síťové karty. Jednou jsou pomocí switchů napojeni do serveru A, na kterém běží Novell systém, pomocí něhož se uživatelé přihlašují do sítě a systému. IP adresy jsou přiřazeny staticky. Ten také sdílí disky a spravuje uživatelské účty. Pomocí druhé síťové karty jsou počítače připojeny do routeru a z něj do druhého serveru, který sdílí internet. Vnitřní síť je zvenčí neviditelná, viditelná je pouze serverová stanice. IP adresy jsou tady přiřazeny DHCP.

Všechny počítače jsou tedy v jedné lokální síti. Lokální síť je topologie hvězdicové. Technologie ethernet, kabely UTP s koncovkami RJ-45. Disky na lokálních stanicích jsou nevyjímatelné. Disky jsou rozděleny na dva oddíly. Na Novell serveru je diskové pole pro síťové využití. Každé oddělení (12, 10, 8 počítačů) je ve vlastní lokální síti. Sítě se navzájem „nevidí“, pro sdílení dat jsou určeny právě síťové disky na Novell serveru. Na stanicích běží operační systém Windows XP SP3.

Pro práci jsou využívány zejména programy AutoCAD pro projekční činnost a pro účetnictví program Pohoda a jako kancelářský program využívá společnost MS Office 2003.

Nedostatky systému:

Prvním nedostatkem je pouze jedna chráněná oblast pokrývající celou budovu společnosti. Chybí tak hlavně místa pro přístup s vyšším oprávněním do serverovny a do kanceláří manažerů. Bylo by tedy vhodné zavést čipové čtečky u vstupů do těchto prostor. Do serverovny, kde jsou umístěny oba servery a switch, by měl mít přístup pouze správce systému – bezpečnostní manažer.

Dalším nedostatkem je vysílání SSID místní bezdrátové sítě. Vzhledem k tomu, že jsou do sítě připojeny pouze počítače firmy nacházející se v budově, není nutné SSID vysílat a tak dávat možnost pro útok z vnějšku. Stanice jsou připojeny do těchto routerů pomocí kabelů. Pro zvýšení bezpečnosti by bylo vhodné přiřazovat IP adresy staticky – ke každé MAC adrese vždy stejná IP adresa stanice. Napomáhá to lehčí identifikaci v síti a snazšímu záznamu aktivit na síti.

Jako nedostatečná se také projevila ochrana hesel. Vzhledem ke způsobu ukládání hesel ve Windows XP a délce hesla menšího než 14 znaků je vhodné nastavit minimální délku hesla na 14 znaků, kde alespoň dva znaky musí být číslice.

Dále jeden ze serverů, server pro přístup na internet postrádá záložní zdroj. Dalším nedostatkem je funkčnost USB slotů na účastnických stanicích. Vhodné by bylo používání zakázat, aby nebylo možné vynášet tímto způsobem informace bez povolení.

Na celou počítačovou síť připadá pouze jeden zkušený správce. V ideálním případě najmout dalšího zaměstnance na jednu z technických pozic popsanou v příloze, případně pověřit jinou, školenou osobu bezpečnostními povinnostmi.

5.1 Rozsah ISMS

Vytvořený systém bezpečnosti bude pokrývat celou podnikovou počítačovou síť a všechny periferie do ní připojené. Dále bude zahrnovat všechny dokumenty (elektronické i papírové), které jsou výstupem práce v informačním systému (lokální síti).

5.2 Analýza rizik

Seznam aktiv společnosti:

- vypracované projekty uložené na disku serveru
- rozpracované projekty na discích lokálních stanic
- účetní informace za období činnosti společnosti
- archivované smlouvy
- pracovní smlouvy
- dokumentace k projektům
- licenční smlouvy softwaru – AutoCAD, Stormware Pohoda, Windows XP, Microsoft Office
- 12 pracovních stanic s označením Office
- 10 pracovních stanic s označením Office Professional
- 8 pracovních stanic s označením GraphicsPro
- 3 switche D-link DGS
- 1 router Cisco systems
- 1 plotter HP
- 4 multifunkční tiskárny HP CMP
- 4 obyčejné přenosné telefony
- 1 digitální fotoaparát Nikon
- 1 projektor BenQ
- vybudovaná podniková síť (kabeláž, struktura)
- budova ve vlastnictví společnosti
- webové stránky společnosti

5.2.1 Hodnocení aktiv

Ohodnocení aktiv:

Každý z hodnocených aspektů – důvěrnosti, integrity a dostupnosti bude hodnocen 5 stupni míry ohrožení.

Nízká:

- žádný dopad pro organizaci
- nepatrný dopad pro organizaci

Střední:

- potíže či finanční ztráty společnosti, řešitelné

Vysoká:

- vážné potíže či finanční ztráty společnosti
- může znamenat existenční potíže pro společnost

Průměrem těchto hodnot jsem získal následující ohodnocení aktiv společnosti:

Aktivum	**Zdroj**	**Dostupnost**	**Integrita**	**Důvěrnost**	**Váha aktiva**
doposud vypracované projekty v elektronické podobě	disky serveru	2	2	2	2
rozpracované projekty na discích stanic	disky stanic	4	4	4	4
účetní informace za období činnosti organizace	disk stanice účetní	4	5	4	4
	disky záloh	3	5	4	4
smlouvy se zákazníky	papírové zálohy	3	5	5	4
pracovní smlouvy	papírové zálohy	4	5	5	5
dokumentace k projektům	papírové zálohy	4	4	2	3
softwarové vybavení	AutoCad	5	5	5	5
	Stormware Pohoda	3	5	5	4
	Windows XP	5	5	5	5
	Microsoft Office	3	5	5	4
pracovní stanice Office	Kancelář 1	5	3	4	4
pracovní stanice Office Pro	Kancelář 2	5	3	4	4
pracovní stanice Graphics Pro	Kancelář 3	5	3	4	4
switche D-Link DGS	Kanceláře	4	2	1	2
PC majitele	Kancelář majitele	4	4	5	4
PC sekretářky	Kancelář majitele	4	4	5	4
PC manažerů	Kanceláře 1,2,3	3	4	4	4
router cisco systems	Serverovna	3	2	1	2
plotter HP	Kancelář 1	2	1	1	1
tiskárny HP CMP	Kancelář 1,2,3	2	1	1	1
přenosné telefony	Kancelář 1,2,3, majitele	1	1	1	1
fotoaparát Nikon	XXX	1	1	1	1
projektor BenQ	XXX	1	1	1	1
vybudovaná podniková síť	celá budova	5	4	5	5
budova sídla společnosti	XXX	5	2	5	4
webové stránky firmy	externí poskytovatel webhostingu	3	4	1	3

Tabulka 6: Ohodnocení aktiv

V první tabulce se nalézají 4 kritická aktiva – softwarové vybavení pro každodenní činnost organizace nutné pro náplň její práce, kde jejich ztráta znamená nemalé finanční škody a pak také účetní informace a pracovní smlouvy se zaměstnanci.

V druhé části je pak kritické aktivum pouze podniková síť. Při jejím výpadku je ohrožena efektivní spolupráce zaměstnanců a výrazně zpomalen provoz společnosti.

V následující tabulce je seznam identifikovaných hrozeb pro zpracovávaný systém a jejich možné zranitelnosti.

HROZBY	**P(hrozby)**	**Příklad zranitelnosti**
zničení zařízení nebo médií	3	Nedodržení pravidelné výměny
Prach, koroze, zamrznutí	4	Citlivost na prach
Požár	1	Požár
přerušení dodávky elektřiny	2	Citlivost na změnu napětí, nestabilní elektrická síť
selhání telekomunikačního zařízení	3	Nekvalitní kabelové spojení, bod totálního selhání
elektromagnetické záření	1	Citlivost na elektromagnetickou radiaci
krádež médií nebo dokumentů	4	Nedostatečná kontrola externích zaměstnanců nebo zaměstnanců zajišťujících úklid, nechráněné uskladnění
krádež zařízení	4	Nedostatečné kontroly zařízení mimo lokalitu
chybné fungování zařízení	3	nedostatečná údržba zařízení
chybné fungování aplikačního programového vybavení	2	neodladěný nebo nový program
chyba údržby	4	nedostatečná údržba, chybná instalace záznamových médií
neoprávněné použití zařízení	4	chyba v produkci reportů pro management, nechráněné připojení do veřejné síťe
podvodné kopírování aplikačního programového vybavení	5	neprovádění logování událostí
poškození dat	5	nedostatky v postupech pro řízení dokumentace ISMS
chyba v používání	5	složité uživatelské rozhraní
zneužití oprávnění	3	chybné přiřazení přístupových práv

Tabulka 7: Hrozby a zranitelnosti

Po identifikaci a ohodnocení aktiv je vhodné udělat matici zranitelností. V nich – tabulka 1 a 2 - lze pak vidět závislosti hrozeb a zranitelností na daném aktivu. Veličina T je pravděpodobnost výskytu hrozby, A je hodnota aktiva získaná z předešlého kroku hodnocení aktiv. Zranitelnosti jsou opět hodnoceny stupnicí 1 až 5, kde 5 představuje nejvyšší pravděpodobnost výskytu zranitelnosti.

V maticích zranitelností je tak vidět důležitost některých aktiv a jejich náchylnost na využití zranitelnosti. Matice rizik pak využívá jednoduchého vzorce A*T*V pro vyjádření závažnosti zranitelností na jejich pravděpodobnosti a hodnotě aktiva. Z matice rizik pak součtem můžeme dostat teoretickou hodnotu aktiva pro společnost, resp. jeho důležitost při přijímání opatření – neznačí jeho peněžní hodnotu. Je vhodné pro přesnost dát hodnoty na stejný základ – v mém případě například aritmetickým průměrem sjednotit hodnoty

5.2.2 Matice analýzy rizik

Matice zranitelností část 1.	XXX	**Aktivum**	vypracované projekty	rozpracované projekty	účetní informace	smlouvy se zákazníky	pracovní smlouvy	dokumentace k projektům	programové vybavení	pracovní stanice	PC manažerů	router Cisco	switch D-Link
XXX		**A**	3	4	5	4	4	3	4	4	4	3	3
Hrozba	**T**												
zničení zařízení nebo médií	3								2	2	2	1	1
Prach	4									1	1	1	1
přerušení dodávky elektřiny	2									2	2	2	2
selhání telekomunikačního zařízení	3											4	4
elektromagnetické záření	1												2
krádež médií nebo dokumentů	4		2		3	3	3	2	4				
krádež zařízení	4									2	2	2	2
chybné fungování zařízení	3									3	2	1	1
chybné fungování aplikačního programového vybavení	2								3				
chyba údržby	4									2	2	3	3
neoprávněné použití zařízení	4									1	3	3	3
podvodné kopírování aplikačního programového vybavení	5								4				
poškození dat	5			4	4								
chyba v používání	5								3	2	2		
zneužití oprávnění	3												

Tabulka 8: Matice zranitelností část 1.

V tabulce je sestavena takzvaná matice zranitelností, kde jsou proti sobě postaveny hrozby, jejich závažnost a aktiva a jejich hodnoty. Pro každé aktivum a hrozbu se pak dle zkušenosti doplní číselná hodnota vyjadřující pravděpodobnost výskytu hrozby pro dané aktivum.

Matice zranitelností, část 2.	XXX	**Aktivum**	Plotter HP	Tiskárny HP	přenosné telefony	fotoaparát	projektor	podniková síť	budova společnosti	webové stránky	WEB server	LAN Server
XXX		**A**	1	1	1	1	1	5	4	3	5	5
Hrozba	**T**											
zničení zařízení nebo médií	3		1	1	1	1	1				2	3
Prach	4											
přerušení dodávky elektřiny	2		1	1	1	1	1	4	4		2	3
selhání telekomunikačního zařízení	3							5				
elektromagnetické záření	1		2					3				
krádež médií nebo dokumentů	4											
krádež zařízení	4				1	1	1				3	3
chybné fungování zařízení	3		1	1	1	1	1				1	2
chybné fungování aplikačního programového vybavení	2										1	2
chyba údržby	4		1	1							2	2
neoprávněné použití zařízení	4		1	1	1	1	1				3	3
podvodné kopírování aplikačního programového vybavení	5											
poškození dat	5											
chyba v používání	5		1	1			1				1	1
zneužití oprávnění	3										3	3

Tabulka 9: Matice zranitelností část 2.

Matice rizik, část 1.	XXX	**Aktivum**	vypracované projekty	rozpracované projekty	účetní informace	smlouvy se zákazníky	pracovní smlouvy	dokumentace k projektům	programové vybavení	pracovní stanice	PC manažerů	router Cisco	switch D-Link
XXX		**A**	3	4	5	4	4	3	4	4	4	3	3
Hrozba	**T**												
zničení zařízení nebo médií	3								24	24	24	9	9
Prach	4									16	16	12	12
přerušení dodávky elektřiny	2									16	16	12	12
selhání telekomunikačního zařízení	3											36	36
elektromagnetické záření	1											6	6
krádež médií nebo dokumentů	4		24		60	60	48	24	64				
krádež zařízení	4									32	32	24	24
chybné fungování zařízení	3									36	24	9	9
chybné fungování aplikačního programového vybavení	2								24				
chyba údržby	4									32	32	36	36
neoprávněné použití zařízení	4									16	48	36	36
podvodné kopírování aplikačního programového vybavení	5								80				
poškození dat	5			80	80								
chyba v používání	5								60	40	40		
zneužití oprávnění	3												

Tabulka 10: Matice zranitelností část 1.

Tabulky maticí rizik pak představují konečnou úroveň, nebo hodnotu závislou na náchylnost k výskytu hrozby.

Matice rizik, část 2.	XXX	**Aktivum**	Plotter HP	Tiskárny HP	přenosné telefony	fotoaparát	projektor	podniková síť	budova společnosti	webové stránky	WEB server	LAN Server
XXX		**A**	1	1	1	1	1	5	4	3	5	5
Hrozba	**T**											
zničení zařízení nebo médií	3		3	3	3	3	3				20	45
Prach	4											
přerušení dodávky elektřiny	2		2	2	2	2	2	40	40		20	30
selhání telekomunikačního zařízení	3							75				
elektromagnetické záření	1							15				
krádež médií nebo dokumentů	4											
krádež zařízení	4				4	4	4				20	40
chybné fungování zařízení	3		3	3	3	3	3				30	30
chybné fungování aplikačního programového vybavení	2										10	20
chyba údržby	4		4	4							40	40
neoprávněné použití zařízení	4		4	4	4	4	4				60	60
podvodné kopírování aplikačního programového vybavení	5											
poškození dat	5											
chyba v používání	5		5	5							25	25
zneužití oprávnění	3										45	45

Tabulka 11: Matice zranitelností část 2.

Sjednocení hodnot 1.část	**Aktivum**	vypracované projekty	rozpracované projekty	účetní informace	smlouvy se zákazníky	pracovní smlouvy	dokum. k projektům	programové vybavení	pracovní stanice	PC manažerů	router Cisco	switch D-Link
Aritmetický průměr		**24**	**80**	**70**	**60**	**48**	**24**	**50**	**27**	**29**	**18**	**18**

Tabulka 12: Sjednocení hodnot 1. část

Sjednocení hodnot 2.část	**Aktivum**	Plotter HP	Tiskárny HP	přenosné telefony	fotoaparát	projektor	podniková síť	budova společnosti	webové stránky	WEB server	LAN Server
Aritmetický průměr		**4**	**4**	**3**	**3**	**3**	**43**	**40**	**XX**	**28**	**37**

Tabulka 13: Sjednocení hodnot 2. část

Aktiva s velmi malým významem jsou hlavně elektronické vybavení používané pro kancelářské práce. A i když mohou být relativně nákladné na pořízení (plotter), jejich náhrada může být okamžitá, a tak ztráty při jeho výpadku budou minimální. Do této skupiny pak patří tato aktiva:

- plotter
- tiskárny
- projektor
- telefony
- fotoaparát

Navrhovaná opatření pro ochranu aktiv: pravidelná údržba zařízení, evidence používání zařízení (přenosné telefony, fotoaparát). U malých zařízení jako telefony je relativně velké riziko krádeže zařízení. Toto riziko sníží také celkové zabezpečení a kontrola přístupu do budovy.

Další skupinou aktiv, u nichž využitím zranitelnosti může mít společnost střední dopady – finanční, provozní jsou tato:

- vypracované projekty
- dokumentace k projektům
- pracovní stanice
- PC manažerů
- router
- switch
- WEB server

První dvě aktiva mají částečně jak elektronickou, tak papírovou podobu.

Navrhovaná opatření pro jejich ochranu: záloha na externí disky, pravidelná kontrola záloh, častá údržba, uschování projektů na místo s omezeným přístupem (archív), evidence používání papírových dokumentů.

Další dvě aktiva jsou stanice užívané běžnými zaměstnanci a manažery oddělení. Každý uživatel má vlastní pracovní stanici. Přihlášení se prování pomocí Novell serveru. Uživatel je povinen se odhlašovat při odchodu od pracovní stanice. Manažer taktéž.

Navrhovaná opatření: fyzicky uzamknout počítačové skříně, zakázat používání USB slotů. Logování činností na stanicích. Antivirový nástroj na každé stanici.

Další aktiva této úrovně jsou aktivní síťové prvky zajišťující fungování lokální sítě a trvalé připojení k internetu na lokálních stanicích.

Navrhovaná opatření: umístění prvků v serverovně. Pravidelná údržba prvků. Přidělování adres staticky, pro každou MAC adresu. Zaheslování přístupu do prvků silným heslem. Pouze správce a jeho zástupce znají heslo. Vypnout wi-fi u routeru, využívat pouze metalického spojení.

Poslední aktivum je web server. I když samotný není až tak důležitý pro chod firmy, vzhledem k tomu, že skrze něj je možné dostat se k lokálním stanicím, je důležité jej dobře zabezpečit.

Navrhovaná opatření: umístění v serverovně s omezeným přístupem, použití silného hesla pro přístup k serveru. Instalace kvalitního antivirového softwaru a firewallu. Zakázání využívání peer-to-peer sítí. Logování využívání sítě uživatelskými stanicemi. Zakázání

zranitelných portů. Výsledkem penetračních testů provedených na webovém serveru je seznam takovýchto portů.

Poslední třídou jsou aktiva s nejvyšší hodnotou pro chod firmy. Mezi ně patří:

- rozpracované projekty
- účetnictví firmy
- smlouvy
- programové vybavení
- podniková síť
- budova společnosti
- LAN server

Opatření na ochranu rozpracovaných projektů: Nastavení v programech automatického ukládání. Pravidelné vytváření záložních kopií pracovních souborů. Archivace na síťové disky.

Opatření pro ochranu účetních informací: Ty jsou v elektronické podobě uložené jako databáze programu Pohoda. Je tedy vhodné pravidelně zálohovat měněné databáze jak na síťové disky, tak jednou za delší časové období na přenosná média.

Opatření pro ochranu smluv: Smlouvy jsou v papírové podobě i elektronické podobě. Vhodné by bylo uložit smlouvy do archivu a omezit přístup pouze na vedení firmy a smlouvy elektronické zálohovat na datová média a rovněž uložit do archivu.

Opatření pro ochranu programového vybavení: Uschování originálních médií na vyhrazené místo s omezeným přístupem. Znemožnění uživatelům využívání přenosných médií pro možné podvodné kopírování softwaru. Zálohování médií a uložení na separátní místo pro případ zničení médií (požár, pád).

Opatření pro ochranu podnikové sítě: Uložení aktivních prvků a serverů v serverovně s omezeným přístupem. Vedení metalické kabeláže mimo běžný provoz (stropy, podlahy). Využití stíněných metalických vedení pro ochranu proti rušení. Vypnutí wi-fi na routeru. Zavedení unikátních uživatelských účtů s pouze nutnými právy pro vykonávání práce.

Opatření pro ochranu budovy: Zavedení kontrolovaného přístupu do archívů a do serverovny pomocí čipových karet (přístup do budovy takto kontrolován je).

Opatření pro ochranu LAN serveru: Umístění v serverovně. Instalace silného firewall nástroje. Zavedení silného hesla pro přístup do systému serveru.

5.3 Bezpečnostní cíl

Bezpečnostní cílem spojeným s využíváním informačního systému je zajištění důvěrnosti a integrity utajované informace všude, kde se vyskytuje, dostupnosti informace a služeb informačního systému a odpovědnosti uživatele informačního systému za jeho činnost v něm.
Zavedením ISMS do chodu společnosti bude mít přínos zejména v lepším, kontrolovaném řízení procesů, ve zlepšení úrovní oprávnění uživatelů a tím také pro vyřešení odpovědností zaměstnanců v rámci organizace. Z analýzy rizik pak přínosem pro společnost bude vyšší bezpečnosti celého informačního systému díky navrhovaným opatřením pro ochranu aktiv. Vzhledem k tomu že vytvářené ISMS není v plném rozsahu a v žádném případě by nebylo možné nechat ho v tomto stavu certifikovat, i tak poskytuje společnosti dobrý přehled aktiv, a způsob jejich ochrany.

5.4 Bezpečnostní politika

Bezpečnostní cílem spojeným s využíváním informačního systému je zajištění důvěrnosti a integrity utajované informace všude, kde se vyskytuje, dostupnosti informace a služeb informačního systému a odpovědnosti uživatele informačního systému za jeho činnost v něm.

Odpovědnosti:

Za provoz je odpovědný správce systému, který je zároveň bezpečnostním správcem systému. V případě nepřítomnosti správce je odpovědný jeho zástupce.

Za zálohy a postup při zálohování je zodpovědný pověřený manažer úseku. Manažeři jsou v tomto ohledu proškoleni. Kontroly záloh provádí manažeři jednotlivých úseků. Zálohy účetních informací provádí správce IS.

Přístup:

Přístup do budovy je evidován pomocí unikátních čipových karet každého zaměstnance, evidující příchod a odchod. Ředitel společnosti a jmenovaný správce systému a jeho zástupce mají přístup do serverovny a archívu, kde je potřeba zvláštního oprávnění pro vstup.

Přístup do systému je založen na unikátních uživatelských účtech každého pracovníka. Minimální délka hesla 14 znaků, změna hesla povinná každých 6 měsíců. Uzamčení pracovní stanice po 20 minutách nečinnosti. Povoleny maximálně tři neplatné pokusy o přihlášení za jednu hodinu. Při prvním přihlášení povinnost změnit heslo přidělené

administrátorem. Heslo nesmí být odvozeninou jména uživatele či posloupností znaků na klávesnici (qwert) a to v jakémkoliv směru. Heslo nelze používat opakovaně.

Vytváření záznamů o přístupu do systému, přístupu k uzamčeným souborům. Tyto záznamy se vytvářejí na serverech a tam jsou také ukládány. Záznamy jsou spravovány správcem systému a jen on (případně zástupce) k nim má přistup. Záznamy jsou uloženy v elektronické podobě po dobu tří měsíců. Pak se záznamy archivují na CD, ty se pak uchovávají nejméně tři roky. Přístup k těmto záznamům má pouze správce systému, případně jeho zástupce.

Komunikační linky musejí být vedeny stropy, podlahami, zdmi – bez přímého přístupu ke kabeláži mimo jejich zakončení. Počítačové skříně jsou uzamčeny, přístup k nim má pouze správce systému a zástupce.

Switche i router musejí být umístěny v serverovně, chránící zařízení proti neoprávněnému užití.

Ochrana stanic:

Každá počítačová skříň je uzamčena, přístup k ní má pouze správce a jeho zástupce. Jsou zakázány USB sloty pro připojení externích datových médií. Každá stanice musí mít nainstalován antivirový program. Při odchodu se musí pracovník odhlásit. Uživatelské účty nemají přístup do ovládacího panelu systému Windows a je znemožněno používání pravého tlačítka myši ve Windows. V prostředí, kde je umístěna pracovní stanice, je zakázáno kouřit, jíst a pít.

Ochrana serverů:

Servery jsou uzavřeny v místnosti s omezeným přístupem. Každý z nich má unikátní heslo. Hesla znají pouze správce systému a jeho zástupce. Heslo musí být délky minimálně 14 znaků, kombinace velkých a malých písmen a musí obsahovat minimálně 2 číslice. Hesla jsou také uloženy v zalepené obálce, která je uložena v bezpečnostní schránce. Hesla se musí měnit každého půl roku.

V prostředí, kde je umístěna pracovní stanice, je zakázáno kouřit a jíst.

Oba servery musejí mít nainstalován antivirový software. Server pro přístup na internet musí mít nainstalován firewall. Na serveru pro přístup na internet musí být nainstalován software monitorující pohyb uživatelů na internetu. Skříně serverů budou zapečetěny pro ochranu hardwarové konfigurace.

Evidence uživatelů:

Správce systému je povinen vést a udržovat seznam všech uživatelů systému, včetně jejich práv. Při odchodu zaměstnance je správce povinen v co nejkratší době uživatele ze seznamu odstranit a zrušit jeho uživatelský účet a přístupová práva.

Povinnosti uživatelů jsou deklarovány v příručce užívání IS. Uživatel podpisem potvrdí srozumění s tímto dokumentem a případě revize i s touto revizí.

Audit záznamů:

Využitím auditních možností v systému Windows XP je nutné zaznamenávat přístup k souborům, přihlášení do systému, selhání auditech záznamů, jejich vymazání.

ZÁVĚR

Zadáním práce bylo seznámit se s problematikou managementu bezpečnosti informací podle standardů ISO řady 27000. V teoretické části jsem shrnul celé pozadí a teoretické znalosti této oblasti. První část se věnuje historii a důvodu vzniku tohoto odvětví managementu. Následuje popis částí PCDA cyklu, jímž se celý systém řídí. Jsou vypsány všechny náležitosti a dokumenty, které musí správné ISMS obsahovat, pokud se uchází o certifikaci. Většina teoretické části se věnuje nejdůležitější části procesu zavádění ISMS – ohodnocení aktiv a analýza rizik. Poslední část teorie rozebírá důležitá doporučení popsaná v normě ISO 27002.

V praktické části jsem pak dle zadání vypracoval analýzu rizik a bezpečnostní politiku systému. Analýze rizik předchází identifikace informačního systému firmy, jeho struktura a nedostatky. V dalším kroku jsem vypracoval identifikaci aktiv a určil jejich hodnotu dle definované stupnice hodnocení. Dle doporučení norem řady 27000 jsem sestavil matice zranitelností a rizik pro určení hodnot aktiv vzhledem ke zranitelnostem a rizikům na ně působící. Součástí analýzy rizik jsem pak vypracoval opatření vhodná k přijetí pro ochranu identifikovaných aktiv. Na tyto kroky pak přímo navazuje bezpečnostní politika udávající pravomoci, pravidla a bezpečnostní prvky pro ochranu aktiv při práci s nimi v každodenní činnosti.

Společnost vznesla požadavek pro vytvoření čtyř úrovní přístupu do informačního systému. Tyto úrovně jsou zpracovány a uloženy v příloze této práce.

Díky této práci jsem nahlédl do správy IS a informací a pochopil základy vyšší administrace informačního systému a celkového managementu bezpečnosti informací v podnikové sféře.

ZÁVĚR V ANGLIČTINĚ

Aim of this work was to get acquainted with the problems of information security management according to ISO number 27000. In the theoretical part, I summarized the entire background and theoretical knowledge of the area. The first part deals with the history and purpose of this type of management. Followed by a description of the parts of the PCDA cycle whereby the entire system follows. Work contains a list of all documents ISMS should contain in order to pass a certification. A large part of the theoretical chapter is focused on the most important process of implementing ISMS - asset valuation and risk analysis. The last section discusses important recommendations described in ISO 27002.

The practical part of my diploma is divided into two main chapters – risk analysis and security policy. Before that I analyzed current IS, its structure and shortcomings. The next step, I made the identification of assets and determined their value as defined by scale of assessments. Recommended by the standards ISO 27000, I have compiled a matrix of vulnerabilities and risks to determine asset values, given the vulnerabilities and risks involved in them. As a part of risk analysis I created list of recommendations to protect identified assets. These steps are followed by security policy giving rights to employees, forming rules and security features to protect assets in everyday environment. The company made a request to create four levels of access to the information system. These levels are made and placed in the annex to this work.

By writing this work I looked into the higher administration of an information system and the overall information security management in enterprise environments.

SEZNAM POUŽITÉ LITERATURY

[1] ČSN ISO/IEC 27001. *IT - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. [s.l.] : Český normalizační institut, 2006. 35 s. ISSN 8590963765334

[2] ČSN ISO/IEC 27005. *IT - Bezpečnostní techniky - Řízení bezpečnosti informací*. [s.l.] : Český normalizační institut, 2009. 52 s. ISSN 8590963831930.

[3] ČSN ISO/IEC 27006. *IT - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*. [s.l.] : Český normalizační institut, 2008. 40 s. ISSN 8590963805276.

[4] ČSN ISO/IEC TR 13335. *IT - Směrnice pro řízení bezpečnosti IT : části 1 a 2*. [s.l.] : Český normalizační institut, 1999. 48 s.

[5] DOUCEK, Petr, NOVÁK, Luděk, SVATÁ, Vlasta. Řízení bezpečnosti informací. [s.l.] : [s.n.], 2008. 240 s.

[6] ISMS : Seriál o ISMS [online]. c2010 [cit. 2010-01-19]. Dostupný z WWW: http://www.chrantesidata.cz/cs/art/1146-isms/.

[7] Data Security Management. 2006, č. 03-06.

[8] HANÁČEK, Petr, STAUDEK, Jan. Bezpečnost informačních systémů. [s.l.] : [s.n.], 2000. 127 s.

[9] HÖNIGOVÁ, A.; MATYÁŠ, V. *Anglicko-česká terminologie bezpečnosti informačních technologií*. [s.l.] : Computer Press, 1996. 95 s. ISBN 80-85896-44-3.

[9] MILÁČEK, Marek SWOT analýza. In *SWOT analýza*. [s.l.] : [s.n.], 2002 [cit. 2010-04-06]. Dostupné z WWW: <http://www.stavebnitechnologie.cz/view.php?cisloclanku=2002041701>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISMS	Information Security Management System
PDCA	Plan Do Check Act
IS	Informační systém
IT	Informační technologie
ISO	International Organization of Standardization
FRAP	Facilitated Risk Analysis Process
AV	Antivirový program
UTP	Unshielded Twisted Pair
DHCP	Dynamic Host Configuration Protocol
USB	Universal Serial Bus
HDD	Hard Disc Drive
ICT	Information and Communication Technologies

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I.: ÚROVNĚ OPRÁVNĚNÍ

4. úroveň – Správce IS

- správce zná administrátorské heslo pro přístup ke všem stanicím, serverům a aktivním síťovým prvkům

- správce je oprávněn měnit nastavení aktivních síťových prvků dle potřeb společnosti a dle nejlepších znalostí

- uvolňovat místo na discích serveru a stanic likvidací nepotřebných souborů

- zakládat a rušit uživatelská jména v systému

- přidělovat práva v rámci informačního systému

- zastavit práce v daném informačním systému v případě havárie, kritické situace vyžadující neodkladné řešení

- koordinovat práce v IS

- správce má přístup do všech počítačů IS a ke všem aktivním síťovým prvkům IS

Práva v systému Windows – plná administrace systému, přístup do všech součástí jak na serverech, tak na účastnických stanicích

3. úroveň – Správce počítačů

- je oprávněn určit uživatele pro práci na jemu svěřených stanicích

- požadovat archivaci dat od Technika

- školit zaměstnance pro práci na pracovních stanicích

- požadovat aktualizaci softwaru od Technika

- správce počítačů má přístup do svého počítače a do pracovních stanic svého úseku

Práva v systému Windows – plná administrace systému, přístup do všech součástí počítače manažera úseku a všech účastnických stanic příslušného úseku

2. úroveň – Technik IS

- smazat dočasné a nevýznamné soubory

- kontrolovat bezpečnost počítačové sítě, její vytížení, případně narušení

- zastavit práci uživatelů v případech havárie, poruchy, rozšíření viru, upřednostnění některých prací, které nelze vykonat za chodu počítačové sítě

- technik má přístup do počítačů manažerů úseku a do pracovních stanic zaměstnanců

Práva v systému Windows – plná administrace systému, přístup do všech součástí počítačů manažerů a účastnických stanic

1. úroveň – uživatel IS

- přistupovat k přidělené uživatelské stanici pomocí svého uživatelského hesla

- ukládat data na síťové disky a na disk pracovní stanice

- užívat všech dostupných funkcí systému potřebných pro vykonávání práce

Práva v systému Windows – omezená práva, znemožnění přístupu do nastavení systému, zakázání funkce pravého tlačítka myši, znemožnění používání USB disků