VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH METODIKY PRO ZAVEDENÍ ISMS
DESIGN OF METHODOLOGY FOR IMPLEMENTATION OF ISMS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Ondřej Dokoupil**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Dokoupil Ondřej, Bc.

Informační management (6209T015)

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

Návrh metodiky pro zavedení ISMS

v anglickém jazyce:

Design of Methodology for Implementation of ISMS

Pokyny pro vypracování:

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

Seznam odborné literatury:

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

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

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

L.S.

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

V Brně, dne 29.2.2016

Abstrakt

Tato diplomová práce se zabývá návrhem metodiky pro zavedení ISMS, tedy systému řízení bezpečnosti informací (Information Security Management System). V teoretické části jsou popsány základní principy a postupy při zpracování této oblasti, včetně normativních a právních – legislativních aspektů. V další části je provedena analýza současného stavu v organizaci, na jejímž základě je v praktické části vypracován samotný návrh včetně ekonomického zhodnocení projektu a přínosů případné implementace.

Abstract

This master's thesis deals with the design of methodology for implementation of ISMS (Information Security Management System). The theoretical part describes the basic principles and procedures for processing of this domain, including normative and legal - legislative aspects. The next section is an analysis of the current state of the organization. On its basis the practical part is drafted, including an economic evaluation of the project and possible benefits of implementation.

Klíčová slova

ISMS, systém řízení bezpečnosti informací, analýza, riziko, PDCA, norma, ISO/IEC 27000

Keywords

ISMS, information security management system, analysis, risk, PDCA, standard, ISO/IEC 27000

Bibliografická citace

DOKOUPIL, O. *Návrh metodiky pro implementaci ISMS.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 90 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

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

V Brně dne 27. května 2016 …….....

Poděkování

Touto cestou bych rád poděkoval vedoucímu bakalářské práce Ing. Viktoru Ondrákovi, Ph.D. za cenné informace, dále zaměstnancům Muzea Prostějovska v Prostějově za poskytnutou spolupráci a také rodině, přátelům a přítelkyni za podporu.

OBSAH

ÚVOD

V posledních letech je velmi dobře patrný přechod k tzv. informační společnosti. To znamená, že pro různé subjekty na trhu se data, informace a potažmo znalosti získávané ať už svou vlastní činností, či z jiných externích zdrojů stávají čím dál důležitějším, ne-li klíčovým faktorem rozvoje, úspěchu a konkurenční výhody. Přitom množství takto shromažďovaných dat a informací stále roste, stejně, jako roste jejich význam.

Mezi tyto informace se řadí nejen běžné provozní informace komunikované v interním prostředí, ale vše, od obchodních a výrobních tajemství, přes informace o vývoji, budoucích patentech, informace o účetních záležitostech, personální informace až po informace sdílené a komunikované s různými externími subjekty.

Ovšem zde je třeba si uvědomit, že velká část, ne-li většina těchto informací je pro daný subjekt velmi citlivá a je potřeba tyto informace co nejlépe chránit. Žádná společnost nechce, aby její citlivá data a informace byla snadno dostupná neoprávněným uživatelům, konkurenci nebo veřejnosti. Nechce ani, aby tato data byla nějak poškozena, změněna, či dokonce zcela zničena nebo nějak zneužita.

Jelikož systémy pro zpracování a uchovávání informací, jakož to i procesy při jejich komunikaci bývají většinou velice složité, je potřeba k tomuto problému přistupovat velice pečlivě a komplexně. Někdy je dokonce potřeba v organizaci zavést systémový přístup k tomuto řešení, včetně zavedení procesního řízení a dalších pokročilých praktik.

Důležité je také identifikovat všechny možné hrozby a zranitelnosti, které mohou mít na informace, jinak také aktiva informační bezpečnosti, vliv. Faktorů je zde mnoho. Hrozby mohou být interního charakteru – chybné jednání zaměstnanců, jejich „pokusy“ ve firemním prostředí, nebo dokonce jejich snaha získané informace nějak zneužít nebo zničit, ať už pro vlastní prospěch (obohacení), nebo jen v případě msty za ukončení pracovního poměru. Druhou skupinou jsou útoky zvenčí, ty mívají podobný charakter. Útočník chce získané informace buď zpeněžit, nebo je využít pro konkurenční výhodu, popř. je „jen“ zničit u vlastníka a tím mu uškodit.

V neposlední řadě jsou to živelné pohromy a selhání hardwaru, popř. špatně navržený zpracovávající software, které mohou uložené nebo přenášené informace poškodit, zničit, nebo v lepším případě jen znemožnit jejich přístupnost a tím omezit běžný provoz organizace, která je na těchto informacích a přístupu k nim někdy i existenčně závislá.

Ve všech těchto věcech je ale třeba dbát i požadavků a omezení, která vyvstávají z právních a legislativních opatření. Pokud chce organizace splnit všechny požadavky na bezpečnost informací a dokázat i navenek, že má tuto problematiku velmi dobře zvládnutou, přidává se ke všemu ještě nutnost dodržet předepsané normy a splňovat určité certifikace.

Je tedy vidět, že problematika bezpečnosti informací je velmi rozsáhlá, multioborová a mezioborová záležitost. Pokud se organizaci podaří zavést všechna plánovaná opatření, může tím výrazně omezit dopady případných problémů a snížit náklady na jejich nápravu.

1 CÍLE PRÁCE

Cílem této práce je navrhnout metodiku pro zavedení systému řízení bezpečnosti informací (ISMS). Půjde o jakýsi manuál (příručku), v kterém budou navržena veškerá pravidla a směrnice pro zavedení ISMS. Bude obsahovat doporučení jak zavádět jednotlivá opatření tak, aby byly splněny požadavky vyplývající z analýz (současného stavu, rizik, interního a externího prostředí). Tato opatření budou dále splňovat požadavky a podmínky dané vedením organizace, ale také právní a legislativní omezení. Kromě toho budou opatření podložena doporučeními, která můžeme najít v normách souvisejících s daným tématem.

Tento manuál bude pouze doporučením pro budoucí zavádění ISMS. Nezahrnuje volbu konkrétních technických řešení, ani výběr produktů, ale jen obecnější, avšak dostatečně přesné vymezení rozsahu zavádění. Upozorňuje na možná úskalí různých řešení a poskytuje určitá variantní řešení. Podle tohoto manuálu by mělo být bez problému možné systém postupně zavést v organizaci.

V teoretické části jsou vysvětleny nezbytné okruhy témat související se zadáním a cílem práce. Jsou zmíněny zavedené praktiky běžně používané pro řešení konkrétní problematiky. Dále je potřeba zmínit normy, které budou podkladem pro výběr konkrétních postupů a řešení, a které budou zároveň tyto volby opodstatňovat. Na posledním místě, avšak neméně důležité je potřeba uvést aktuálně platné legislativní požadavky a omezení platné pro takový projekt.

V druhé části práce jde zejména o identifikaci aktiv společnosti a analýzu zranitelností, hrozeb a rizik. Analýzu interního prostředí – zaměstnanců, hardwaru, softwaru a dalšího technického zázemí informační bezpečnosti, jako např. síťové infrastruktury. A to včetně aktuálního stavu informační bezpečnosti, současných směrnic a pravidel již zavedených.

V praktické části je již zpracován konkrétní návrh metodiky, který obsahuje např. požadavky na změny nebo zavedení určitých praktik nebo technologií, opatření, pravidel a směrnic. V závěru kapitoly je proveden rozbor ekonomického dopadu a časové náročnosti takového řešení a jeho přínosů pro organizaci.

2 TEORETICKÁ VÝCHODISKA

V této kapitole je zachycena problematika teoretických východisek, která jsou zapotřebí pro analýzu problému a návrh řešení. Důležitá je znalost základních pojmů a principů, ale také normy, které návrh omezují, doporučují postupy a měly by zajistit bezproblémovou implementaci.

2.1 Důležité základní pojmy

Pro jasné porozumění a orientaci tématu jsou v této podkapitole popsány nejzákladnější relevantní pojmy. (1)

IT - Informační technologie

Pojem informační technologie zahrnuje širokou škálu technologií, které slouží k získávání, zpracovávání, uchovávání, přenosu a prezentaci dat. (1)

ICT - Informační a komunikační technologie

(Z anglického Information and Communication Technology). Jelikož dochází ke konvergenci informačních technologií (myšleno ve smyslu počítačového zpracování a přenosu dat) a hlasových i video služeb, vznikl tento pojem, který souhrnně označuje tyto zmíněné technologie. (1)

Konvergence

Jde o slučování různých používaných technologií, např. přenosových médií nebo protokolů z různých oblastí. Např. přenos hlasu po počítačové síti za pomoci IP protokolu. V tomto případě je to nástroj pro přechod od IT k ICT. (1)

Data

Data jsou vlastně základem pro získávání informací. Dají se chápat jako posloupnost symbolů/znaků, které jsou po získání nějakým určitým způsobem uloženy tak, aby při jejich interpretaci vyjadřovaly zjištěnou skutečnost. Taková data se pak dají dále zpracovávat a přenášet. (1)

Informace

Informace jsou získávány z dat. Jedná se o určitý poznatek, který nám data po pochopení a využití v relevantní situaci přináší. Získáváním informací z dat se dosahuje snížením neznalosti nebe neurčitosti. (1)

IS - Informační systém

Jako informační systém se dá označit soubor vzájemně provázaných informací a procesů, které s těmito informacemi pracují. Mezi základní funkce informačního systému patří ukládání, převody, přenos a prezentace dat. V širším pohledu zahrnuje informační systém také využívaný hardware, software a také lidi, kteří IS využívají a kteří se starají o jeho chod. V praxi se informační systémy používají nejčastěji k řízení, rozhodování a plánování. (1)

Síťová infrastruktura

Síťová infrastruktura souhrnně označuje veškeré síťové prvky a zařízení, které jsou součástí realizace ICT prostředí, které v tomto kontextu slouží k vytváření a podpoře informačního systému, kde také působí jako aktivum organizace. (1)

2.2 Základní pojmy v oblasti bezpečnosti ICT

Dále budou popsány již o něco specifičtější pojmy, týkající se konkrétně oblasti bezpečnosti v IT. (1)

Bezpečnost organizace

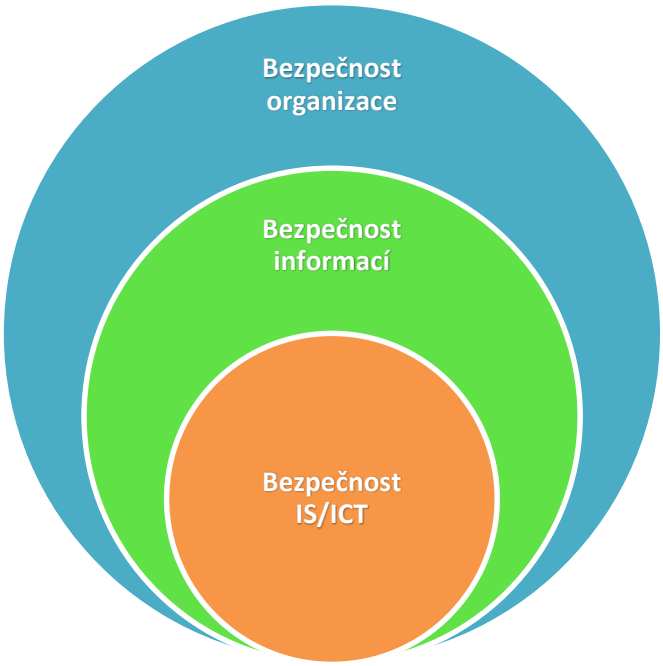
Bezpečnost organizace je pojem, kterým se označuje bezpečnost objektu, to znamená, fyzická bezpečnost majetku organizace. Zároveň zahrnuje i následující dva stupně bezpečnosti. (1)

Bezpečnost IS/ICT

Bezpečnost IS/ICT se zabývá pouze ochranou samotných aktiv informačního systému podporovaných informačními a komunikačními technologiemi. Je jakousi podmnožinou bezpečnosti organizace, bez které by ve skutečnosti nebylo možné ji realizovat. (1)

Informační bezpečnost

Tento pojem chápeme jako ochranu a dostupnost samotných informací, jinak také bezpečnost informací. Samotná bezpečnosti informací by se neobešla bez předchozích dvou stupňů bezpečnosti, jelikož stojí pomyslně mezi nimi. V prvním případě je potřeba zajistit fyzickou ochranu organizace jako celku, zatímco v druhém případě je v dnešní době nutné postarat se o bezpečnost přenosového prostředí informací, kam patří právě i informační systémy a informační a komunikační technologie. Pro lepší pochopení jsou na následujícím obrázku vyobrazeny všechny tři stupně. (1)



Obrázek 1: Bezpečnost organizace, informací a IS/ICT (Vlastní zpracování dle (2))

Je také potřeba si uvědomit, že se nejedná jen o bezpečnost digitálních informací, ale také například o bezpečnost papírových dokumentů, mluveného slova a podobně. (1)

Důvěrnost

Vlastnost, jež zajišťuje, že určitá informace je dostupná pouze oprávněné osobě. (1)

Integrita

Integrita zajišťuje, že konkrétní informace je správná a úplná. (1)

Nepopiratelnost

Nelze popřít, že určitá informace pochází z určitého zdroje / od určitého původce. (1)

Dostupnost

Dostupnost znamená, že daná informace je dostupná oprávněnému uživateli v okamžiku potřeby. (1)

Aktivum

Za aktiva se označuje veškerý hmotný i nehmotný majetek, který má pro vlastníka (organizaci) nějakou hodnotu. V tomto případě to může být hardware, software, ale hlavně informace, které svou hodnotou často převyšují i mnohá hmotná aktiva. Proto je jejich ochraně věnována taková pozornost. (1)

Zranitelnost

Je to vlastnost aktiva, která popisuje jeho slabé místo. Toto slabé místo může být v případě hroby důvodem poškození, zničení nebo zcizení aktiva. (1)

Hrozba

Jako hrozba je chápána jakákoliv aktivit, činnost nebo síla, která může ohrozit bezpečnost aktiva. A to buď využitím jeho zranitelnosti, nebo jiným způsobem. To může mít za následek vznik škody na tomto aktivu. (1)

Hrozby nejsou původem jen ze strany člověka (subjektivní), ale patří sem i ohrožení přírodními vlivy jako záplavy, požáry, úder blesku apod. Subjektivní hrozby se dají dále dělit podle toho, zda jsou úmyslné (odcizení, útok na dostupnost, zničení), nebo neúmyslné (omyl, nedbalost). (1)

Riziko

Riziko udává míru, s jakou může mít hrozba dopad na aktivum. Obecně se vyjadřuje jako pravděpodobnost realizace hrozby a vzniku škody na aktivu. Riziko může být vyjádřeno buď ve vztahu k aktivům, nebo také k jednotlivým hrozbám. (1)

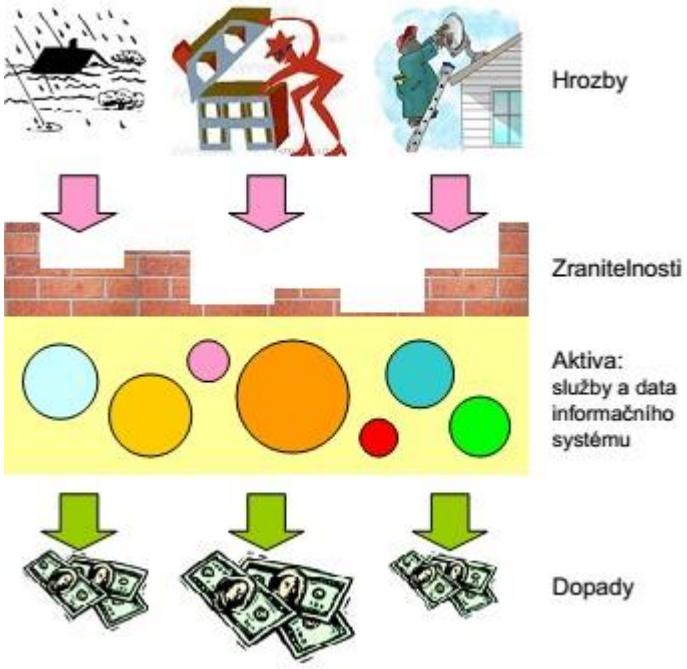
Dopad

Dopad se dá nejjednodušeji charakterizovat jako škoda, která vznikne na aktivu v případě působení hrozby. (1)

Opatření

Za opatření můžeme označit aktivitu, technologii či postup, které sníží dopad na aktivum. A to buď snížením rizika, omezením působení hrozby nebo její eliminaci. Popř.

snížením zranitelnosti aktiva. Souvislosti mezi jednotlivými pojmy jsou názorně a přehledně vyobrazeny na následující ilustraci. (1)



Obrázek 2: Aktiva informační bezpečnosti (2)

Bezpečnostní mechanizmus

Pro implementaci bezpečnosti se využívají různé techniky, těm se říká bezpečnostní mechanismy. Jsou to obecné principy používané pro zajištění bezpečnosti informací. Patří sem: (1)

- **Logické bezpečnostní mechanismy (softwarové)** – řízení přístupu v OS (operačním systému), kryptografie, údržba systému – aktualizace, antiviry, hesla, autentizace
- **Technické (hardwarové)** – autentizační karty, HW šifrování
- **Organizační** – důvěryhodné osoby, hesla, autentizace, autorizace

Zde je vidět, že některé mechanismy svým způsobem můžou patřit do více skupin.

Bezpečnostní funkce

Bezpečnostní funkce je pak samotná funkce produktu (systému, aplikace, hardwaru), která dovoluje zavést některý bezpečnostní mechanismus. (1)

Bezpečnostní událost

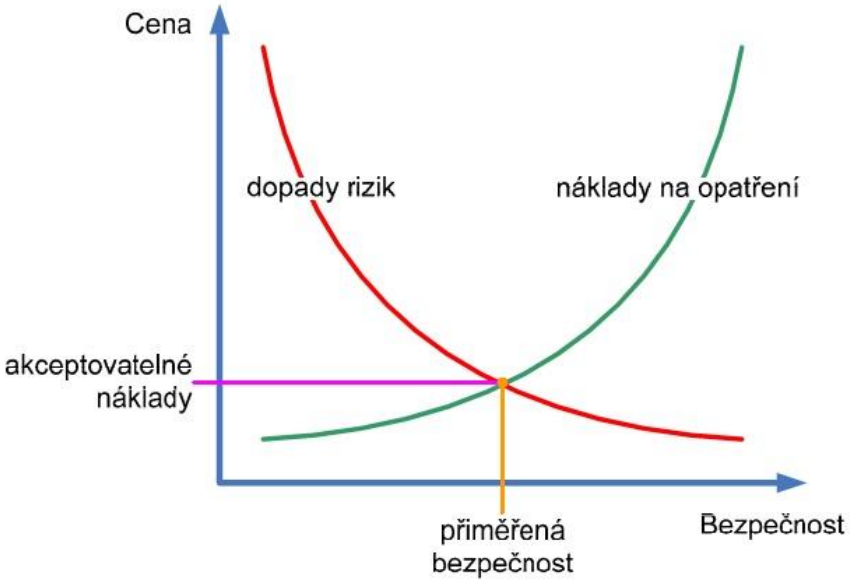
Jde o děj týkající se informačního systému, služby nebo počítačové sítě, který může narušit bezpečnostní politiky organizace, čímž může dojít k narušení aktiva. Může jít také o selhání již zavedeného opatření nebo i neznámou situaci, která může ovlivnit bezpečnost. (1)

Bezpečnostní incident

Prakticky jde o nastalou bezpečnostní událost, která může s vysokou pravděpodobností narušit hlavní procesy organizace nebo bezpečnost informačního systému. Jedná se vlastně o stav (případ) selhání bezpečnosti. (1)

Přiměřená bezpečnost

Je potřeba si uvědomit, že pokud nějaká organizace požaduje určitou míru bezpečnosti, měla by také zvážit ekonomickou stránku navrhovaného řešení. Jde o to, že pokud se bude snažit za každou cenu prosadit co nejvyšší bezpečnostní standardy, pak se může stát, že náklady na takové řešení přesáhnou jeho ekonomický přínos pro tuto organizaci. Proto je třeba dbát na vzájemný vztah mezi mírou bezpečnosti a náklady na její dosažení. Nejlepší je dosáhnout takového případu, kdy **bezpečnost je přiměřená** požadavkům, a to při **akceptovatelných nákladech**. Tuto situaci zachycuje následující obrázek. (1)



Obrázek 3: Přiměřená bezpečnost (2)

2.3 ISMS – Definice

ISMS – Information Security Management System, neboli Sytém řízení bezpečnosti informací (někdy také Systém řízení informační bezpečnosti) je systémovým řešením ochrany informací v organizaci. Jde o sytém popisující neustále opakující se proces postupného zlepšování stavu ochrany informací (informační bezpečnosti) v organizaci. Takový systém se řídí tzv. PDCA cyklem (Demingův model). Řízení informační bezpečnosti zasahuje do mnohých aspektů managementu celé organizace. Proto je důležité, aby takový systém byl v souladu s těmito aspekty a zároveň podporoval dosahování cílů organizace a to v rovině normativní, strategické i provozní. (3, s. 14)

2.3.1 PDCA cyklus (Demingův model)

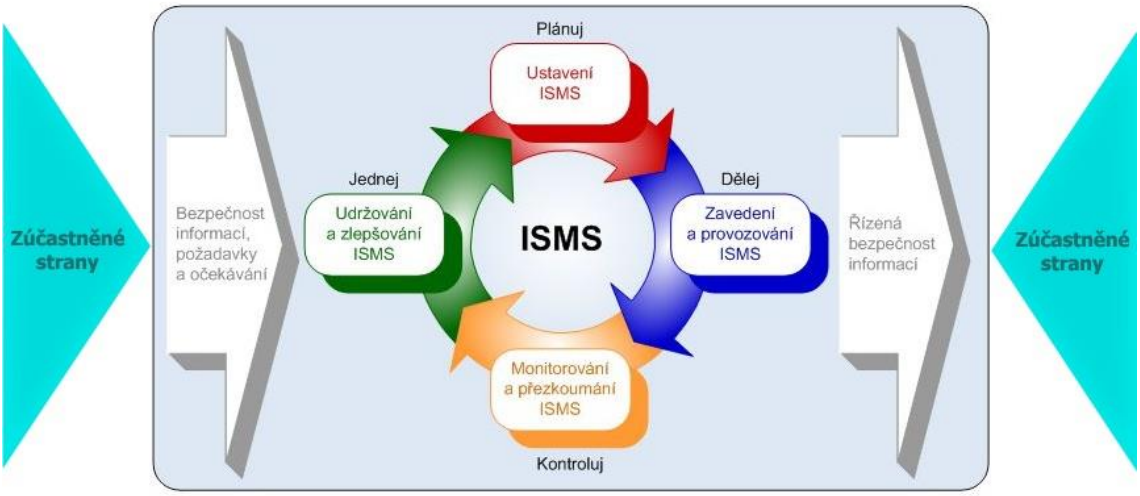
Jedná se o metodu, díky které je možné postupně zlepšovat kvalitu např. výrobků, služeb, procesů, aplikací a dat. Toho má být dosaženo za pomoci čtyř stále se opakujících se činností. Ty jsou následující: (4)

- **Plan (plánuj)** – naplánování zamýšleného záměru (zlepšení)
- **Do (dělej)** – realizace plánu
- **Check (kontroluj)** – ověření výsledku realizace oproti původnímu plánu
- **Act (jednej)** – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe

Tato metoda je obecně používána v procesu řízení organizace. V oblasti ISMS každá činnost cyklu odpovídá určité etapě provozu ISMS. (4)

2.3.2 Model PDCA v ISMS

Jak již bylo zmíněno výše, princip ISMS je založen na metodě PDCA. Na následujícím schématu jsou názorně vyobrazeny vztahy při provozu ISMS na základě PDCA cyklu.



Obrázek 4: Model PDCA v ISMS (Životní cyklus ISMS) (Upraveno dle (5) a (2))

2.4 ISMS - Systém řízení bezpečnosti informací

V této podkapitole již budou popsány základní etapy provozu ISMS zmíněné výše. U každé etapy je detailněji uvedena jejich náplň, kroky při realizaci a podmínky potřebné k úspěšnému naplnění požadavků každé fáze. Popis obsahuje také další používané postupy a metody, ale např. i informace o požadované dokumentaci každé fáze provozu ISMS.

Většina požadavků na realizaci systému řízení bezpečnosti informací má charakter závazných podmínek daných normou ISO/IEC 27001, pouze splnění všech těchto podmínek současně může zajistit shodu s touto normou. Oproti tomu norma ISO/IEC 27002 je souborem doporučení, jejichž splnění není závazné, ale může výrazně usnadnit a zlepšit zavádění ISMS. (6)

2.4.1 Obsah ISMS

Hlavním obsahem systému řízení bezpečnosti informací je zavedení a provoz systému, který zahrnuje tři základní činnosti. První z nich je určení důležitých informačních aktiv, která mají být chráněna. Dále je potřeba určit a řídit možná rizika týkající se těchto aktiv a v důsledku toho i celé bezpečnosti informací. Neméně důležitou částí ISMS je pak volba a zavedení opatření a jejich kontrola. Tyto kroky by měly eliminovat, nebo alespoň snížit pravděpodobnost poškození nebo ztráty těchto aktiv. (6)

2.4.2 Etapy zavádění ISMS

Ustanovení

Jedná se o zásadní etapu budování ISMS v organizaci. V této fázi jsou konkretizovány správné formy řešení a je upřesněn rozsah a hranice, ve kterých se budou další etapy realizovat. (7, s. 86)

Obsahuje následující skupiny činností: (7)

- Definice rozsahu, hranic a vazeb ISMS
- Definice a odsouhlasení „**Prohlášení o aplikovatelnosti**“
- Analýza a zvládání rizik
- Souhlas vedení organizace se zavedením ISMS a zbytkovými riziky
- Příprava „**Prohlášení o aplikovatelnosti**“

Zavádění a provoz

V této etapě dochází k implementaci bezpečnostních opatření navržených v předchozí etapě ustanovení ISMS. (7, s. 104)

Zde je nezbytné provést následující kroky: (7, s. 104)

- Formulace dokumentu „**Plán zvládání rizik**“ a jeho zavedení
- Zavedení plánovaných opatření a formulace “**Příručky bezpečnosti informací**“
- Definice programu budování bezpečnostního povědomí a provést zaškolení zaměstnanců a dalších uživatelů
- Definice způsobů měření účinnosti opatření a sledování ukazatelů
- Zavedení postupů pro detekci a reakci na bezpečnostní incidenty
- Řízení zdrojů, dokumentů a záznamů ISMS

Monitorování a přezkoumávání

Nejdůležitější funkcí této etapy je získání zpětné vazby týkající se zavádění a dalšího provozu ISMS, zejména pak dopady zavedených opatření a jejich účinnost. Cílem je poskytnout vedení informace o tom, zda jsou opatření v souladu s obecnými potřebami organizace. (7, s. 117)

Pro dosažení výše zmíněných cílů je potřeba realizovat následující činnosti: (7, s. 117)

- Monitoring a ověření účinnosti aplikovaných opatření
- Provedení interních auditů, které pokryjí celý rozsah ISMS
- Příprava zprávy o stavu ISMS pro vedení organizace

Údržba a zlepšování

Prakticky každá implementace nějakého systému není na první pokus stoprocentní, to platí i v případě ISMS. Proto je potřeba shromažďovat podněty ke zlepšení ISMS a na jejich základě napravovat zjištěné nedostatky (neshody). (7, s. 119)

V této fázi se provádí zejména: (7, s. 119)

- Zavádění zlepšení na základě neshod identifikovaných vedením
- Provádění opatření k nápravě neshod a preventivních opatření

2.4.3 Povinná dokumentace

Jelikož zavádění a provoz ISMS se řídí mnohými normami a často si organizace chtějí systém řízení informační bezpečnosti certifikovat, jsou vyžadovány některé povinné dokumenty, jejich přehled je uveden v následujícím textu. (8)

Rozsah a hranice ISMS – Definuje dotčené oblasti ISMS na základě atributů konkrétní organizace. Těmi může být např. její uspořádání, organizační struktura, obor činnosti, nebo struktura aktiv. Také zdůvodňuje případné vynechání některých oblastí ISMS. (8)

Politika ISMS – Tímto dokumentem vedení organizace vyjadřuje, že chápe podstatu zavedení ISMS, deklaruje odpovědnost k prosazování cílů při zavádění ISMS a dává najevo, že je připraveno podpořit zavádění a provoz ISMS uvolněním potřebných personálních a finančních zdrojů. (8)

Definice a přístup k hodnocení rizik – Dokument určuje metodiku hodnocení rizik. Ta by měla vyhovovat konkrétní organizaci a zároveň by měla respektovat legislativní a normativní omezení. Podle tohoto dokumentu se později provádí analýza rizik a určují se pravidla pro akceptaci rizik. (8)

Identifikace a ohodnocení aktiv – Dokument obsahující seznam aktiv společnosti, včetně jejich majitelů a popisu. Z těchto aktiv jsou vybrána a ohodnocena ta, která jsou

důležitá z hlediska informační bezpečnosti. Takto zpracované údaje jsou přehledně zaznamenána v tabulce. Dokument obsahuje i popis způsobu hodnocení aktiv. (8)

Identifikace rizik – Samostatně se zpracovává jen ve větších organizacích. Běžně bývá součástí předchozího zmíněného dokumentu. Obsahuje informaci o zvolené metodice hodnocení rizik a tabulku možných hrozeb s mírou rizika. (8)

Analýza rizik – Dokument obsahující popis zvolené metodiky pro analýzu rizik, přehled aktiv, rizik a výsledky samotné analýzy rizik. (8)

Návrh opatření – Obsahuje popis opatření zvolených ke snížení (minimalizaci/eliminaci) zjištěných rizik, ale také seznam akceptovaných rizik. V případě opatření se může jednat buď o volbu konkrétního řešení, nebo návrh obecnějšího řešení. (8)

Cíle opatření a bezpečnostní opatření pro zvládání rizik – Tento dokument obsahuje seznam cílů jednotlivých opatření, které byly zvoleny na základě předchozích analýz. Tyto cíle jsou vybírány z přílohy A normy (ČSN) ISO/IEC 27001. Cíle uvedené v této příloze jsou obecně použitelné pro všechny typy organizací, a měly by napomoct k tomu, aby nebyla opomenuta důležitá opatření. Avšak v konkrétní organizaci musí zohledňovat kritéria pro akceptaci rizik a dále pak legislativní a smluvní požadavky. (8)

Akceptace rizik – Vychází z dokumentu „Návrh opatření“. Obsahuje přehled rizik k akceptaci, které jsou zde popsány a následně schváleny nebo naopak zamítnuty. (8)

Získání povolení k provozování ISMS v rámci organizace – V tomto dokumentu se vedení organizace zavazuje k ustavení, zavedení, provozu, monitorování přezkoumávání, udržování a zlepšování ISMS. Povinně obsahuje následující kapitoly: (8)

- Zajištění stanovení cílů ISMS a plánu jejich dosažení
- Stanovení role, povinnosti a odpovědnosti v oblasti bezpečnosti informací
- Propagace (v rámci organizace) významu plnění cílů bezpečnosti informací, jejich souladu s politikou bezpečnosti informací, plnění povinností vyplývajících ze zákona a potřebu soustavného zlepšování
- Zajištění dostatečných zdrojů pro ustavení, zavedení, provoz, monitorování, přezkoumání, údržbu a zlepšování ISMS

- Stanovení akceptovatelné úrovně rizika
- Zajištění provádění interních auditů ISMS
- Provádění přezkoumání ISMS

Prohlášení o aplikovatelnosti – Obsahuje prohlášení, které popisuje relevantní opatření bezpečnosti informací a jejich cíle. Dále zdůvodňuje rozhodnutí o jednotlivých rizicích, o vyřazení určitých opatřeních a jejich cílech, to umožňuje kontrolu, zda nebyly vyřazeny nesprávně. Opět má povinné následující kapitoly: (8)

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

2.4.4 Měření účinnosti

Po zavedení opatření informační bezpečnosti je třeba nějakým způsobem zkoumat jejich účinnost. K tomuto účelu se zavádějí **metriky**, kterými se na základě **měření** zjišťuje dosažen **míra** bezpečnosti. Na jejím základě se vyhodnocuje naplnění cílů. (3, s. 71)

2.5 Rámce a metodiky pro management informační bezpečnosti

Obsahem této podkapitoly jsou definice rámců a metod používaných v problematice managementu informační bezpečnosti. Většinou se jedná o určitá doporučení, kdy a co dělat, ovšem už neurčují, jak to dělat. To platí např. u rámcové knihovny ITIL. Díky této skutečnosti a také kvůli tomu, že takové rámce jsou nezávislé na platformě, jsou velmi univerzální. Podobně je na tom metodika COBIT. V obou případech se vlastně také jedná o soubor nejlepších praktik v oboru. Patří sem např. i metodika CRAMM. Všechny budou blíže popsány dále.

Metodika

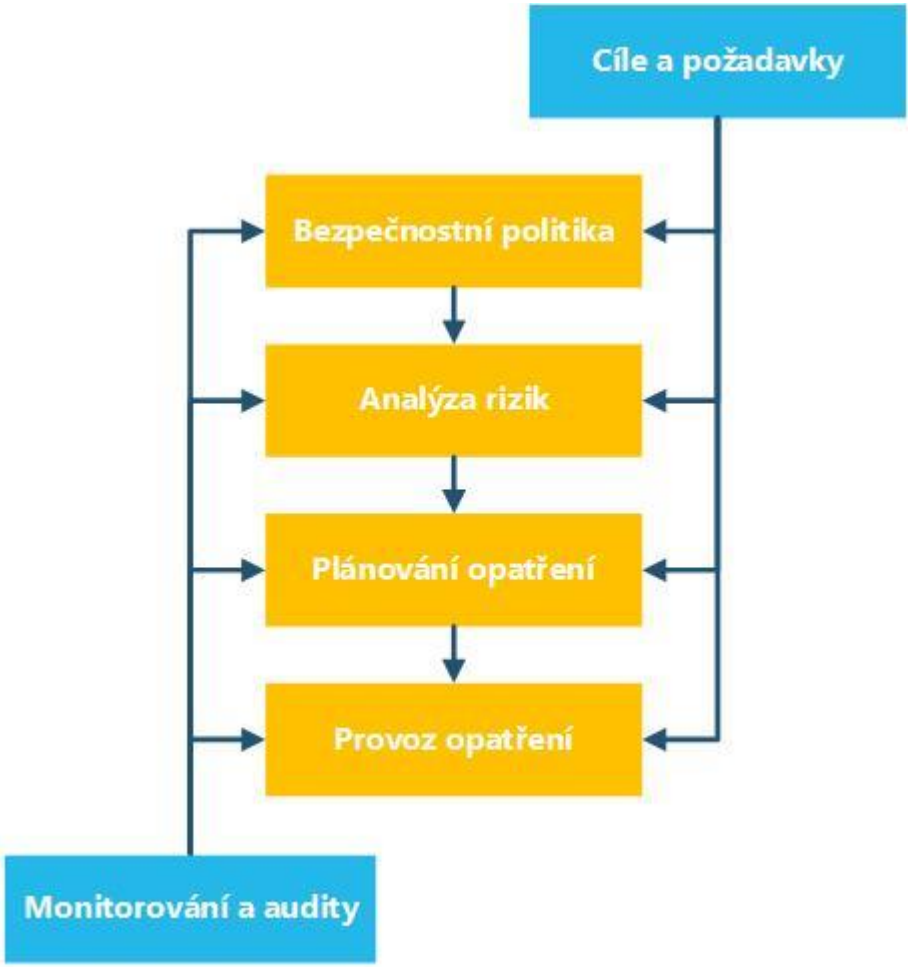
Metodika je podrobný popis celkové činnosti. (3, s. 349)

2.5.1 ITIL

ITIL je vlastně knihovna nejlepších oborových praktik. Zkratka pochází z anglického **IT Infrastructure Library**. Jedná se o soubor doporučení co a kdy dělat při provozování a managementu IT služeb. Nejedná se o metodiku ani normu. Je to rámec nezávislý na platformě a proto neříká, jak postupovat v konkrétních případech. (9)

Důležitým znakem ITIL je proaktivní přístup. To znamená, že oproti reaktivnímu přístupu, kdy se pouze reaguje na nastalé události, se ITIL zabývá aktivním řešením případných problémů, které by mohly v budoucnu vyústit v problémové incidenty. (9)

Hlavním obsahem ITIL je definování procesů pro ITSM a zásady pro jejich zavedení. Naopak se nezabývá např. konkrétní podobou organizační struktury nebo obsazení rolí konkrétními pracovními pozicemi. (9)



Obrázek 5: Procesy řízení bezpečnosti informací dle ITIL (Vlastní zpracování dle (2))

2.5.2 COBIT

Jedná se metodiku pro řízení informatiky v organizaci. Zkratka označuje anglické spojení **Control Objectives for Information and related Technology**. Jejím cílem je propojení principů obecného řízení organizace a pravidel uplatňovaných v IT. Její využívání by mělo napomoct k dlouhodobému rozvoji organizace, naplňování jejích strategických cílů a snižování rizika souvisejícího s používáním ICT v organizaci a to právě díky využití informací a ICT. Úkolem metodiky COBIT je strukturovat složitý systém řízení IT do podoby, která by byla srozumitelná pro management podniku bez hlubších znalostí oblasti IT. Díky tomu by pro ně mělo být snazší definovat vhodná kritéria pro posouzení stavu řízení IT v organizaci. (10)

Informační kritéria

Cíle organizace (strategické požadavky) jsou v metodice COBIT zastoupena Informačními kritérii (požadavky na informace) a mají následující strukturu: (10)

- **Efektivita (účelnost)** – včasné doručování relevantních informací ve správném konzistentním a použitelném tvaru
- **Účinnost** – optimální využívání IT zdrojů pro zpracování informací
- **Důvěryhodnost** – ochrana důležitých informací proti neautorizovanému použití
- **Integrita** – přesné a kompletní informace ve vztahu k požadavkům podnikání
- **Dostupnost** – dostupnost informací pro podnikání nyní i v budoucnosti a jejich ochrana (zdrojů)
- **Soulad** – se zákony, regulacemi, směrnicemi, kontrakčními podmínkami
- **Spolehlivost** – přínos informace pro rozhodování

IT zdroje

Mezi IT zdroje v organizaci podle metodiky COBIT patří: **Aplikace**, **Informace**, **Infrastruktura** a **Lidé**. (10)

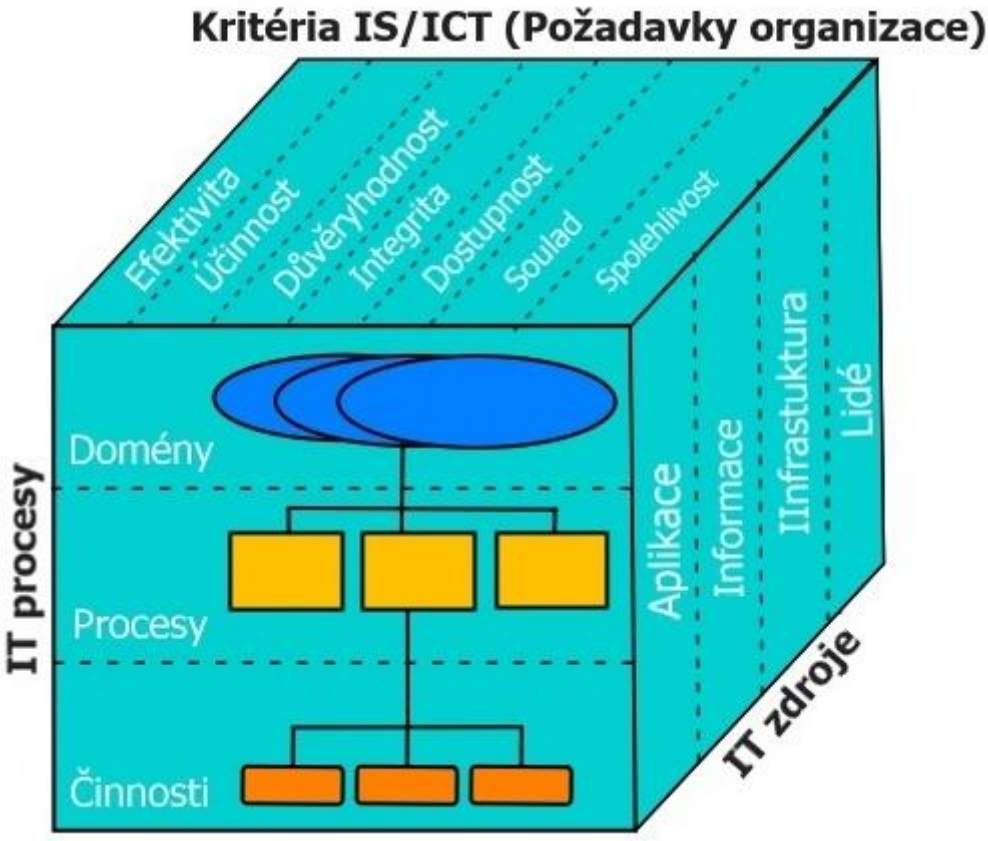
IT procesy

Procesy IT v metodice COBIT jsou hierarchicky uspořádány podle podrobnosti do třech úrovní. (10)

Tu nejvyšší (ve verzi 4.1 z roku 2007) tvoří čtyři následující **domény**: **Plánování a organizace**, **Akvizice a implementace**, **Dodávka a podpora**, **Sledování a hodnocení**. (10)

Na nižších úrovních jsou to pak **Procesy**, kterých je 34, označované jako High Level Control Objectives a **Detailní kontrolní cíle**, těch je 214. (10)

Pro lepší orientaci, přehlednost a pochopení souvislostí se uvedené členění znázorňuje jako tzv. COBIT kostka, viz. obrázek níže.



Obrázek 6: COBIT kostka (Upraveno dle (2))

2.5.3 CRAMM

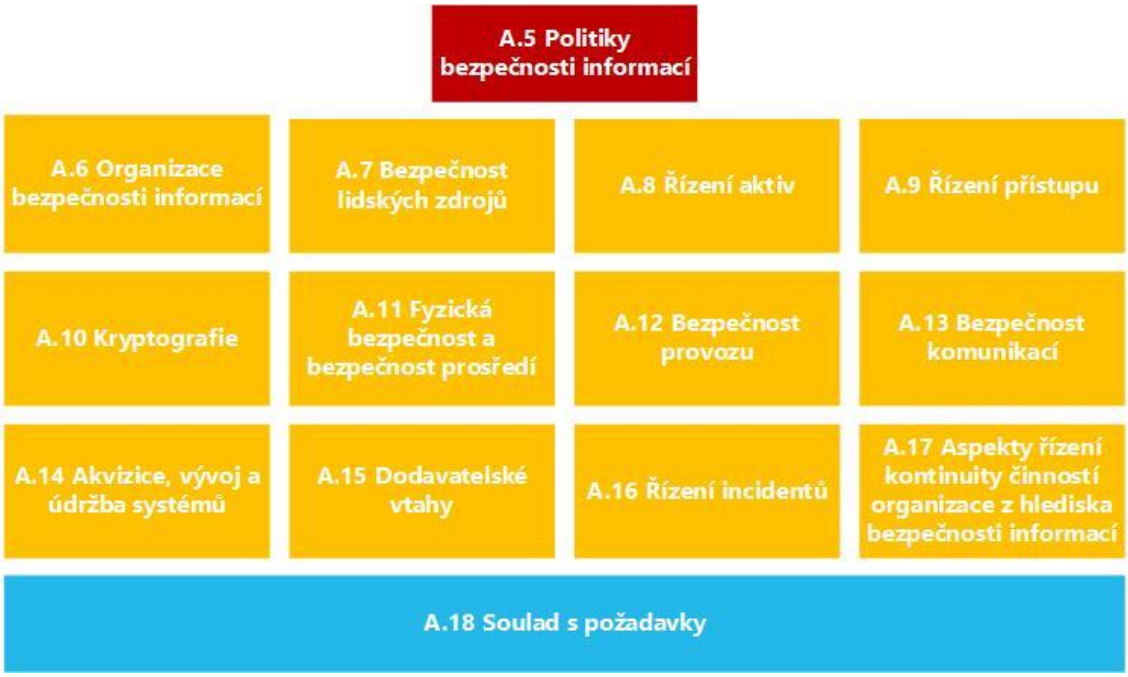
Zkratka znamená **CCTA Risk Analysis and Management Method**, což je metodika pro identifikaci a ohodnocení aktiv, analýzy rizik IS a sítí, návrh opatření a řešení havarijních situací. Pro tuto metodiku existuje také sada softwarových nástrojů. CRAMM plně podporuje zavádění ISMS v souladu s normou ISO/IEC 27001 a vytváří potřebnou dokumentaci systému pro certifikaci dle této normy. (11)

CRAMM analýzu je možné provést ve dvou variantách: (11)

- **CRAMM Express** – jednodenní analýza rizik – využívá pouze některá možná opatření
- **CRAMM Expert** – detailní analýza využívající plnohodnotnou knihovnu opatření

2.6 Opatření

Po provedení potřebných analýz a zjištění požadavků přichází na řadu výběr opatření pro minimalizaci identifikovaných rizik. Jednou z praktických možností je využití souboru postupů uvedených v příloze A normy (ČSN) ISO/IEC 27001. Ta obsahuje 113 bezpečnostních opatření rozdělených do 14 oblastí. Tato příloha obsahuje jejich obecný popis a cíle. Podrobnější popis pak obsahuje norma (ČSN) ISO/IEC 27002. Kompletní seznam opatření je použit v kapitole zabývající se výběrem opatření v praktické části. (12)



Obrázek 7: Oblasti ISMS dle přílohy A normy ISO/IEC 27001 (Upraveno dle (2) a (13))

2.7 Síťová bezpečnost

V problematice bezpečnosti sítí se uvádějí dva podobné, avšak významově odlišné pojmy, jedná se o následující: (3, s. 162)

Síťová bezpečnost – vztahuje se k bezpečnosti sítí, tím je myšlena vnitřní ochrana a ochrana perimetru – místa připojení vnitřní sítě s cizími sítěmi

Bezpečnost síťové architektury – tento pojem definuje stupeň zabezpečení digitálního přenosového prostředí

Základním způsobem nahlížení na bezpečnost sítí je z hlediska referenčního modelu ISO/OSI, tedy na základě rozdělení komunikace v síti na sedm vrstev. (3, s. 162)

1. Management bezpečnosti pasivní vrstvy

Jinak také management bezpečnosti fyzické vrstvy (L1 - první vrstva ISO/OSI). Tato vrstva je tvořena kabelážním systémem (kabely, kabelové trasy, konektory, zásuvky, patch panely). Opatření fyzické bezpečnosti se dělí do tří skupin: (3, s. 166)

0. Stupeň = identifikace – barevné odlišení pomocí kabelů nebo kroužků, nezajišťuje bezpečnosti, ale pouze usnadňuje správu
1. Stupeň = blokace – ochrana portu proti připojení nebo odpojení, ochrana datového boxu a kabelových tras proti přístupu
2. Stupeň = klíčování – znemožňuje připojení kabelů do nepovolených portů, implementace pomocí různých tvarů konektorů a portů

2. Bezpečnost vrstvy datového spoje

Jedná se o druhou vrstvu (L2 - linková) modelu ISO/OSI, na které se realizuje přepínání ethernetových rámců pomocí přepínačů (switch). Zde jsou aplikována například tato opatření: (3, s. 166-167)

- Bezpečná komunikace díky certifikátům
- Digitální podpisy
- AAA (authentication, authorization, accounting) mechanismus – ověření identity, přidělení oprávnění a tvorba záznamů o uživateli
- Bezpečnostní protokoly

3: Bezpečnosti síťové vrstvy

Třetí vrstva (L3) ISO/OSI modelu. Pomocí směrovačů (router) se na ní realizuje směrování IP paketů. Zahrnuje například: (3, s. 167)

- IPSec – autentizace a šifrování IP datagramů
- VPN – virtuální privátní sítě
- Bezpečnost síťových služeb
- IDS a IPS systémy – detekce a prevence průniků
- Firewally – nastavení pravidel síťového provozu

2.8 Specifická řešení

2.8.1 NAC

Toto označení zkracuje anglická slova Network Access Control, což v překladu znamená řízení přístupu k síti. Jedná se o systém, který umožňuje vynucení bezpečnostní politiky pro koncové pracovní stanice. Většinou se skládá z hardwaru a softwaru a dovoluje ověřit koncové zařízení ještě před připojením do sítě. Systém funguje na principu ověření (bezpečnostních) požadavků a teprve po jejich splnění umožní zařízení připojit se do sítě. Využívané možnosti takového systému jsou následující: (3, s. 230)

- Možnost odmítnout nebo přesunout do karantény uživatele nesplňující požadavky
- Řízení přístupu do sítě na základě identity
- Sledování a hodnocení (bezpečnostního) stavu během celého připojení

To například umožňuje přinutit uživatele k tomu, aby měli aktuální operační systém a antivir, v opačném případě jim bude zamítnut přístup k síti. Výhody systému jsou tedy následující: (3, s. 230)

- Lepší bezpečnostní stav zařízení
- Méně incidentů
- Jednotné řízení přístupu k sítí a do systémů
- Bezpečnější vzdálený přístup a přístup třetích stran

BOYD (Bring Your Own Device) – Současný trend, kdy zaměstnanci mohou pracovat na vlastních zařízeních, to je možné zejména právě díky systému NAC. (3, s. 230)

2.9 Normalizační instituce

Jakožto i v dalších oblastech lidské činnosti, tak i v oboru informačních a komunikačních technologií a jejich bezpečnosti existuje celá řada norem vytvořených institucemi různého rozsahu působení. V následující části je uveden základní přehled institucí, od kterých pochází normy, mající nějakou souvislost s ICT a informační bezpečností.

Standard

„*Je dokumentovaná úmluva obsahující technické specifikace nebo jiná podobná přesně stanovená kritéria důsledně používaná jako pravidla, směrnice, resp. jako definice charakteristických vlastností zabezpečující, že materiály, výrobky, procesy, služby apod. jsou takové, jaké se zamýšlelo.*“ (3, s. 40)

Norma

„*Jedná se o doporučení použitelných standardů k realizaci požadovaného kompatibilního řešení.*“ (3, s. 40)

2.9.1 Nadnárodní

Normy nadnárodních institucí mívají často celosvětové užití a působnost. Jejich úpravy bývají také přejímány jako normy národní. (3, s. 41)

ISO – International Organisation for Standardisation

Tato instituce vydává normy, které by měly napomoct standardizaci ve světě, zejména pak usnadnit mezinárodní směnu zboží a služeb a spolupráci při intelektuálních, vědeckých, technologických a ekonomických aktivitách. (3, s. 41)

IEC – International Electrotechnical Comission

Organizace vydávající normy z oblasti elektroniky, elektrotechniky a jim příbuzných oblastí (mimo jiné také telekomunikace a bezpečnost). (3, s. 41)

ITU – International Telecommunications Union

Tato organizace spadá pod OSN. V současnosti se zabývá zejména globální informační infrastrukturou a konvergovanými multimediálními systémy. Hraje klíčovou roli ve správě spekter radiových frekvencí, čímž zabezpečuje jejich bezproblémový provoz. (3, s. 41)

Všechny tři výše zmíněné instituce při vydávání norem úzce spolupracují. Díky tomu vydávají například základní normy s celosvětovou působností. (3, s. 41)

2.9.2 Evropské

CEN – Comité Européen Normalisation

Hlavní náplní činnosti CEN je harmonizace norem napříč Evropou. To by mělo zmenšovat obchodní překážky, podporovat bezpečnost a zlepšovat vzájemnou funkčnost systémů, výrobků a služeb. (3, s. 42)

CEN/ISSS – Information Society Standardizatio System – Hraje klíčovou roli v oblasti standardů ICT a bezpečnosti ICT. Spadá sem např. oblast bankovních karet, čárových kódů apod. (3, s. 42)

CENELEC – Comité Européen de Normalisation Eléctrotechnique

Má vlastní sektor ICT, spolupracuje s CEN a ETSI. (3, s. 43)

ETSI – European Telecomunications Standards Institute

Nezisková organizace zabývající se normalizací v telekomunikačních službách v evropském regionu. (3, s. 43)

Spoluprací zmíněných organizací vznikly například normy týkající se elektronického podpisu, certifikátů veřejných klíčů nebo protokol pro práci s časovými razítky. (3, s. 43)

2.9.3 Národní

Národní organizace obvykle vyvíjejí normy dle potřeb konkrétního státu (legislativních a místních technických a dalších požadavků), popř. pro něj přebírají adekvátní normy nadnárodních institucí, jichž bývají členy. (3, s. 43)

ANSI – American National Standards Institute (USA)

Přímo nevyvíjí normy, ale umožňuje to díky kongresu kvalifikovaných skupin. (3, s. 43)

BSI – British Standard Institute (UK)

Normy zde vyvíjí kvalifikovaní lidé. Normy jsou nejdříve vydány jako návrhy, které je možno komentovat, po uplynutí určité doby je návrh publikován jako norma. (3, s. 43)

DIN – Deutsches Institut für Normung (Německo)

DIN umožňuje díky veřejné diskuzi zainteresovaných odborných účastníků (stát, vědci, podniky, spotřebitelské organizace apod.) tvořit oficiální normy. Tyto normy často podporují např. míru jakosti a bezpečnosti nebo zlepšení komunikaci mezi zainteresovanými stranami. (3, s. 43-44)

ČSNI – Český normalizační institut

Jedná se o příspěvkovou organizaci podřízenou Ministerstvu průmyslu a obchodu. Zastupuje národní zájmy v nadnárodních organizacích. Je členem ISO, IEC, CEN, CENELEC a ETSI s kterými spolupracuje. Jejím úkolem je tvorba českých technických norem, jejich vydávání, distribuci a poskytování informací. (3, s. 44)

ČSN – Česká technická norma

ČSN vznikají buď přejímáním nadnárodních norem, nebo tvorbou vlastních norem na základě národních potřeb. (3, s. 44)

2.9.4 Další

IEEE – Institute od Electrical and Electronics Engineers (USA)

Jedná se o americkou normalizační instituci, avšak její normy jsou ve většině případů mezinárodního významu. Mimo jiné zahrnuje oblasti PC inženýrství, telekomunikace, elektroniky, bezpečnosti lokálních sítí aj. (3, s. 45)

NIST – National Institute for Standards and Technology

Americká laboratoř měřících standardů, jejímž cílem je podpora inovací zlepšováním vědeckých měření a měřících technik a technologií pro zvýšení produktivity, usnadnění obchodu a zlepšení života. (3, s. 45)

2.10 Normy

Jelikož bylo zmíněno, že bezpečnost informací a její řízení je v dnešní době velmi důležitou činností pro velké množství (ne-li většinu) organizací, není divu, že pro tuto oblast vznikla samostatná skupina norem. Pro oblast řízení bezpečnosti informací je to konkrétně řada norem ISO/IEC 27000 (někdy také označovaná jako ISO27k). Některé jsou již přebrány v podobě ČSN ISO/IEC 2700x. V této podkapitole je uveden přehled některých norem této řady se základním popisem jejich obsahu.

Na konci výčtu jsou zmíněny i další normy, které nejsou součástí ISO27k, ale úzce souvisí s problematikou bezpečnosti informací a bývají využívány pro podporu snazšího a lepšího zavádění norem řady ISO/IEC 27000 a podporují realizaci některých jejich částí.

2.10.1 Normy řady ISO/IEC 27000

ČSN ISO/IEC 27000 – Přehled a slovník – Obsahuje základní přehled systémů řízení bezpečnosti informací, dále základní termíny a definice, ovšem pouze ty, jež jsou používány v rodině norem ISO27k. (6, s. 48)

ČSN ISO/IEC 27001 – Požadavky – Obsahuje požadavky na jednotlivé etapy zavádění ISMS. V přílohách obsahuje, mimo jiné, také souhrn doporučených opatření, které je možné využít v etapě zavádění ISMS. Doporučuje využití procesního přístupu a vyzdvihuje vhodnost modelu PDCA při řešení ISMS. Je úzce propojena s normami **ISO/IEC 17799 (Soubor postupů pro ISMS)**, **ISO/IEC 9001 (Systém managementu kvality)** a **ISO/IEC 14001 (Systém environmentálního managementu)**. (6, s. 48-49)

ČSN ISO/IEC 27002 – Soubor postupů – Obsahuje velké množství (více než 5000) doporučených opatření pro řešení bezpečnosti informací. Umožňuje rychle zjistit současný stav bezpečnosti informací a pro nedostatečně zajištěné oblasti navrhnout patřičná opatření. Jedná se o náhradu normy **CŠN ISO/IEC 17799 (Soubor postupů pro ISMS)**. (6, s. 49)

ČSN ISO/IEC 27003 – Směrnice pro implementaci systému řízení bezpečnosti informací – Obsahuje doporučení pro ustanovení a implementaci ISMS v souladu s požadavky normy ISO/IEC 27001. Je použitelná pro všechny typy organizací a řeší proces návrhu a implementace ISMS jehož výsledkem je finální plán implementace projektu ISMS. Ten obsahuje např. návrh organizace bezpečnosti informací, bezpečnosti ICT, fyzické bezpečnosti a dalších opatření dle specifických požadavků ISO/IEC 27001 (přezkoumání ISMS vedením, program zvyšování povědomí bezpečnosti informací - školení apod.). Přílohou normy jsou kontrolní seznamy činností pro ustanovení a implementaci ISMS, dále popis rolí a odpovědností bezpečnosti informací, informace o interních auditech, monitorování a měření bezpečnosti informací a struktury politik. (6, s. 50)

ČSN ISO/IEC 27004 – Měření – Obsahuje doporučení pro zavedení programu měření bezpečnosti informací. Ten zahrnuje procesy vývoje a rozvoje metrik a měření účinnosti zavedeného ISMS a opatření zvolených dle ISO/IEC 27001, provádění měření, analýzu naměřených dat, hlášený výsledků a následné vyhodnocení a zlepšování samotného programu. Příloha obsahuje příklady konceptů měření pro konkrétní opatření a procesy ISMS. (6, s. 51)

ČSN ISO/EIC 27005 – Řízení rizik bezpečnosti informací – Obsahuje doporučení pro řízení rizik bezpečnosti informací organizace. Norma není závislá na přístupu organizace k řízení rizik, který se může lišit např. podle rozsahu ISMS, kontextu řízení rizik a odvětví. Díky tomu se dá aplikovat na všechny typy organizací, kde jsou rizika řízena kvůli možnosti narušení bezpečnosti informací. Z toho důvodu norma nenabízí konkrétní metodiku pro řízení rizik bezpečnosti informací, avšak dává možnost výběru z řady existujících metodik v souladu s přístupem k řízení rizik v každé organizaci. Nahrazuje sadu technických zpráv **ČSN ISO/IEC TR 13335 (Směrnice pro řízení bezpečnosti IT)**. (6, s. 51)

ISO/IEC 27033 – Network security – Jedná se o soustavu norem, které obsahují doporučení pro implementaci opatření týkajících se bezpečnosti sítí. Normy vycházejí ze soustavy norem **ISO/IEC 18028 (IT network security)**, kterou mají revidovat, aktualizovat a doplnit. V současné době je vydáno pět částí. Po vydání šesté části, která

je ve fázi finálního návrhu, soustava ISO/IEC 27033 nahradí soustavu ISO/IEC 18028, která má pět částí. (3, s. 57)

ISO/IEC 27035 – Information security incident management – Obsahuje doporučení pro řízení incidentů bezpečnosti informací. Pokrývá procesy pro řízení událostí bezpečnosti informací, incidentů a zranitelností. Tzn. zejména postupy pro včasnou detekci incidentů, jejich hlášení, vyhodnocení a následnou reakci. V případě zranitelností řeší jejich identifikaci, posouzení a přijetí preventivních nebo nápravných opatření. Nahrazuje normu ISO/IEC TR 18044, je rozdělena do tří částí. (3, s. 53)

ISO/IEC 27039 – Selection, deployment and operations of intrusion detection systems (IDPS) – Obsahuje doporučení pro výběr, zavedení a provoz systémů pro detekci a prevenci průniků. Mimo jiné poskytuje informace, jaký je původ potřeby takových systémů. (3, s. 55)

ISO/IEC 27040 – Storage security – Obsahuje doporučení pro pořizovatele a uživatele technologií pro ukládání dat a pomáhá jim identifikovat a snižovat související rizika. Tato oblast zahrnuje nejen samotná zařízení a média pro ukládání dat, ale také koncové uživatele, management ukládání dat a jejich přenos při ukládání. (3, s. 55)

Další normy řady ISO27k

Celkem řada ISO27k obsahuje skoro 50 různých norem. Kromě základních a obecnějších zmíněných se jedná např. o normy obsahující doporučení pro organizace provádějící audit a certifikaci ISMS, požadavky na osoby provádějící audit, požadavky pro používání ISO/IEC 27001 ve specifických odvětvích, pro bezpečnou komunikaci mezi jednotlivými organizacemi, sektory nebo celými státy, pro využívání ISMS v telekomunikačních společnostech, zdravotnickém prostředí nebo ve finančních službách. (3, s. 48-57)

Další normy řeší např. nejlepší praktiky řízení bezpečnosti informací v cloudových službách a ochranu osobních údajů v nich, ISMS v energetickém průmyslu, souběžnou implementaci norem ISO/IEC 20000 a ISO/IEC 27001, použití ISMS s ohledem na zajištění kontinuity činností organizace, bezpečnost na internetu, aplikační

bezpečnost, bezpečnost informací při outsourcingu ICT nebo pravidla pro publikování digitálních dokumentů. (3, s. 48-57)

V poslední době jsou ve velké míře vyvíjeny normy týkající se zjišťování, sběru, získávání a uchovávání digitálních důkazů a to pro jejich analýzu, vyhodnocování, vyšetřování a zkoumání. (3, s. 48-57)

Další podrobné informace je možné nalézt na webových stránkách www.iso.org v sekci technické podkomise JTC 1/SC 27 – Information technology – Security techniques, která normy řady ISO27k vydává.

2.10.2 Další normy z oblasti ICT a bezpečnosti informací

ISO/IEC 28028 – IT network security – Norma zaměřená na bezpečnost sítí. Zejména na jejich řízení, provoz, správu, používaní a propojování, sestává se z pěti částí. V současnosti nahrazována normou **ISO/IEC 27033**. (3, s. 57-59)

ČSN ISO/IEC 20000 – Management služeb – Skládá se z pěti částí. Jedná se o normu standardizující řízení a správu procesů v organizaci. Úzce souvisí s již zmíněným rámcem ITIL, který zastupuje jakousi knihovnu nejlepších praktik – „jak to udělat“. Samotná norma pak určuje „co je nutné udělat“ v případě požadavku na certifikaci. Často se zavádí s normou ISO/IEC 27001, k souběžné implementaci těchto dvou norem dává doporučení norma **ISO/IEC 27013 (Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1)**. (3, s. 61-62)

ČSN ISO/IEC 15408 – Kritéria pro hodnocení bezpečnosti – Sada tří norem zabývajících hodnocením bezpečnosti IT produktů nebo systémů. Pro tento účel zavádí hodnotící kritéria - požadavky na bezpečnostní funkce a na opatření týkající se záruk. Dále bezpečnostní funkční komponenty, které vyjadřují požadavky na bezpečnost. Ty by měly zvládnout čelit určitým hrozbám v konkrétním prostředí při dodržení bezpečnostních politik a předpokladů. Třetí část popisuje komponenty bezpečnostních záruk. (3, s. 62-63)

2.11 Právní prostředí

Jelikož data a informace, získávané, uchovávané, zpracovávané a šířené různými subjekty často obsahují i citlivé osobní údaje, je tato problematika ošetřena různými právními předpisy daných zemí. V České republice se jedná zejména o následující zákony: (3, s. 264)

- Zákon č. **106/1999 Sb.** – o svobodném přístupu k informacím
- Zákon č. **101/2000 Sb.** – o ochraně osobních údajů
- Zákon č. **412/2005 Sb.** – o ochraně utajovaných informací a o bezpečnostní způsobilosti
- Zákon č. **480/2004 Sb.** – o některých službách informační společnosti
- Zákon č. **227/2000 Sb.** – o elektronickém podpisu
- Zákon č. **499/2004 Sb.** – o archivnictví a spisové službě

Dále sem patří jejich novely a poslední znění. Toto je jen základní přehled nejdůležitějších.

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Základní údaje

3.1.1 Název, sídlo a právní forma společnosti

Název: Muzeum Prostějovska v Prostějově, příspěvková organizace

Sídlo: Nám. T. G. Masaryka 2, 796 01 Prostějov

Právní forma: Příspěvková organizace

IČO: 00091405

Zřizovatel: Olomoucký kraj, IČO 60609460

3.1.2 Předmět činnosti

- Správa sbírek z oblasti archeologie, botaniky, geologie, historie, literárních památek, národopisu, numismatiky, umění a užitého umění
- Provoz stálých expozic Jiřího Wolkera, hodin, geologie, národopisu a pravěku v hlavní budově muzea, dále pak expozic „Edmund Husserl“ a „Z prostějovského ghetta“ v budově špalíčku
- Pořádání dalších dočasných výstav v obou zmíněných budovách
- Samostatná odborná činnost zaměstnanců na vlastních projektech a jejich následné zapracování do sbírek
- Vydávání periodik a publikací

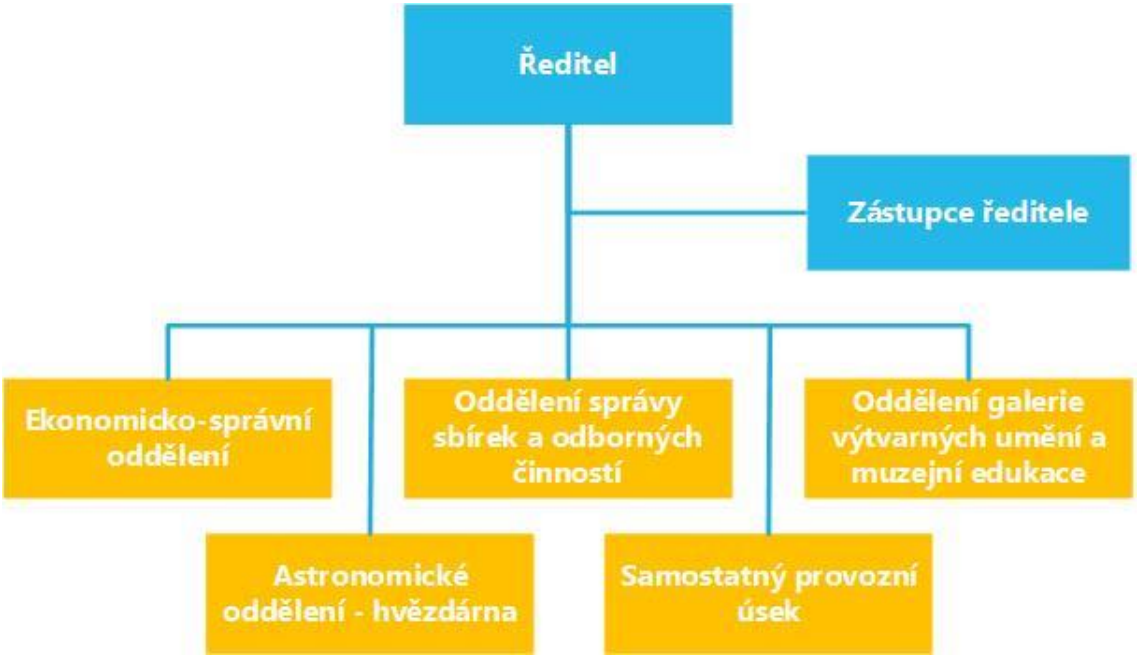
3.1.3 Sortiment služeb

- Nabídka výstav v hlavní budově muzea a také v galerii ve špalíčku
- Komentované prohlídky muzea pro školy a skupiny veřejnosti
- Komentované provádění městem pro školy a skupiny
- Poskytování historických dat, např. pro potřeby tvorby rodokmenů apod.

Muzeum Prostějovska poskytuje jako vedlejší činnost ohodnocování a určování stáří a původu různých předmětů. Např. uměleckých děl, potřeb běžné potřeby dříve používaných v domácnostech a dalších.

3.2 Organizační struktura

Ředitelem organizace je Mgr. Daniel Zádrapa., historik, kurátor výstav. Zástupcem ředitele je Kamila Husaříková, kurátor výstav, propagace. Další členění je znázorněno na následujícím schématu.



Obrázek 8: Organizační schéma

Nadřízeným orgánem a zřizovatelem je Olomoucký kraj, dalším kontrolním orgánem je Ministerstvo kultury ČR.

3.3 Informační technologie a informační systém firmy

3.3.1 Hardware

IT správce má v muzeu na starosti cca 30 počítačů, které využívají zaměstnanci. Většinou jde o starší modely, avšak dostačující na běžnou práci většiny zaměstnanců. Výkonnější PC mají např. grafik, fotograf a člověk, který má na starost zpracování videí z různých akcí pořádaných muzeem. V budově je také přítomen jeden počítač jako router a další jako poštovní server. Další slabší počítače slouží jako pokladny ve výstavních prostorách muzea. Muzeum také vlastní jeden služební notebook, který je možné použít na služebních cestách třeba pro potřeby prezentace. Někteří zaměstnanci mají k dispozici služební telefony.

3.3.2 Software

Jelikož hlavní činností je správa sbírek, nejdůležitější a nejpoužívanější software je právě pro tuto činnost. Jedná se o program CESik od společnosti BACH. Ten je založený na databázi MS Access a v dnešní době se stává zastaralým a nedostačujícím právě kvůli této technologii. Proto se v současnosti řeší přechod na nějaký software založený na platformě SQL. Tento problém byl zadán například i na Fakultu informačních technologií VUT v Brně a dále jsou k dispozici nabídky od komerčních subjektů, což by bylo dražší řešení. Dalším problémem starého systému je decentralizovanost a složité shromažďování databází. Toto vše by měl nový produkt řešit.

Na velkém počtu počítačů je nainstalován operační systém Microsoft Windows XP, některé běží na OS Windows 7. Router a poštovní server běží na Linuxu.

Zaměstnanci dále také běžně používají kancelářský balík MS Office 2003 a poštovní klienty.

Grafik má k dispozici kompletní balík Adobe Creative Suite. Na tvorbu reklamních letáků používá program CorelDRAW.

Na většině počítačů je nainstalovaný antivirový program Eset NOD32. Bohužel, nedá se říct, že by to bylo ideální řešení, jelikož se ve všech případech nejedná o stejné a aktuální verze a občas se vyskytují problémy s aktualizací virové databáze a licencováním. O centralizované správě zde nemůže být řeč, to zásadně znesnadňuje práci administrátorovi IT v organizaci.

3.3.3 Počítačová síť

Všechny počítače v budově jsou spojeny do sítě pomocí 32 portového switche umístěného na chodbě v kancelářském traktu budovy. Zde je umístěn také router a poštovní server. Organizace využívá připojení do internetu od společnosti GTS.

3.3.4 Záloha a archivace

V muzeu se zálohují a archivují hlavně databáze sbírek a vlastní práce zaměstnanců. V současnosti je tato činnost jednou z nejslabších stránek organizace, jelikož každý zaměstnanec se o toto zálohování stará sám za sebe a to převážně prostřednictvím externích médií, CD, DVD a flash disků, v horších případech pouze vytvářením lokálních kopií ve stejném stroji.

V nejbližší době je v plánu tento problém řešit, a plánuje se pořízení síťového úložiště, kde by se shromažďovaly databáze sbírek, které by se pak mohly efektivněji a snáze zálohovat a také by byly lépe přístupné pro ostatní zaměstnance. Nyní si každý spravuje sbírky podle oblasti svého zájmu a v případě potřeby je nutné tyto databáze přesouvat složitými způsoby.

3.3.5 Informační systém

Muzeum žádný vlastní informační systém nemá, ale spolu se zprovozněním síťového úložiště bude v řešení zavedení nějakého jednoduchého informačního systému na bázi jednoduché agendy, sdílení informací, dokumentů a aktualit.

Navíc je v jednání možnost automatického sledování podmínek v depozitářích muzea. Tato možnost by měla lépe ochránit cenné sbírky, včetně informací v analogové podobě.

3.3.6 Správa ICT

Správou ICT je pověřen jeden zaměstnanec, který se stará o veškeré činnosti od pořizování nového hardwaru a softwaru, přes konfiguraci a provoz systémů, až po řešení incidentů. Tento člověk úzce spolupracuje s odporníky a dodavateli používaných technologií.

3.4 Současný stav bezpečnosti informací

3.4.1 Fyzická bezpečnost

Budova

Veškeré kancelářské prostory muzea umístěny v prvním a druhém nadzemním podlaží budovy, jsou přístupné dvěma způsoby. Prvním z nich je služební vchod pro zaměstnance. Ten je opatřen klasickými dveřmi s bezpečnostním kováním. Za nimi následuje chodba a schodiště, které je zakončeno masivními kovovými mřížemi. Za nimi se již nacházejí kancelářské prostory. Jednotlivé kanceláře jsou opatřeny zámky, od nichž mají klíče vždy jen konkrétní zaměstnanci. Někteří výše postavení zaměstnanci mají k dispozici univerzální klíče. Z chodby jsou ještě dostupné prostory dílen a depozitářů. Druhá možnost přístupu do kancelářských prostor je z výstavních sálů. Přístup je realizován dvěma dveřmi v úrovni mezi 1. a 2. nadzemním podlažím, mezi kterými se nachází venkovní ochoz.

Celá budova muzea je opatřena elektronickým zabezpečovacím systémem napojeným přímo na bezpečnostní agenturu a policii ČR. Ten má tři nezávislé okruhy pro kancelářské prostory, depozitáře a výstavní prostory. Všechna okna v 1. přízemním a 1. nadzemním podlaží jsou opatřena masivními kovovými mřížemi. Budova dále obsahuje požární hlásiče napojené na systém hasičského záchranného sboru a automatické hasicí zařízení.

Řízení fyzického přístupu

Každý zaměstnanec má k dispozici klíče od služebního vchodu, kovových mříží a své vlastní kanceláři, jak již bylo zmíněno, někteří zaměstnanci mají pro přístup do některých dalších prostorů univerzální klíče. Zaměstnanci nemají žádné elektronické identifikační prvky, po příchodu a při odchodu se pouze zapisují do deníku umístěného za mříží. Někteří zaměstnanci mají také pravomoci pro aktivaci a deaktivaci zabezpečovacího zařízení budovy – mají k dispozici zabezpečovací kódy.

Pokud se chce do kancelářských prostor dostat návštěvník mimo řady zaměstnanců, musí použít interkom u služebního vchodu, následně je vpuštěn na schodiště a mříží je propuštěn osobně zaměstnancem. Bohužel se často stává, že mříž nebo dveře do technického zázemí nejsou zavřeny.

3.4.2 Prvky ICT

Samotné uživatelské stanice jsou v kancelářích většinou umístěny dle vlastního zvážení uživatelů. Některé jsou tak volně na stolech, jiné ve skříních nebo pod stoly. Pro jejich používání a ochranu nejsou zavedena žádná pravidla nebo směrnice. To může znamenat riziko v podobě snadnějšího přístupu k zařízením, jejich poničení, např. politím.

Stanice s routerem, poštovní server a další síťová zařízení včetně switche jsou umístěny v prostorách chodby mezi 1. a 2. nadzemním podlažím v uzamykatelné rackové skříni s průhledným čelem. I přes poměrně vysokou teplotu ve skříni není instalován žádný systém chlazení.

Kabeláž počítačové sítě je vedena v lištách. Ovšem problémem může být nezavedený systém značení kabeláže a datových zásuvek. Taktéž zásuvky ani koncovky kabelů nejsou zajištěny proti neoprávněnému vytažení nebo zasunutí. Vzhledem k občasným problémům (nechtěné vytažení/vytrhnutí kabelu, špatné zasunutí, „pokusy“ zaměstnanců) je tato stránka bezpečnosti nedostatečná.

3.4.3 Bezpečnost lidských zdrojů

Jelikož v organizaci nedochází k příliš častým změnám v oblasti personální, není zde zaveden žádný pokročilejší systém pravidel v oblasti bezpečnosti při navazování nebo ukončování pracovního poměru. Jsou zde v platnosti pouze základní pravidla, mezi která patří např. ověření beztrestnosti uchazeče o zaměstnání, seznámení s pravidly fyzického přístupu, požadavek na mlčenlivost v případě udělení pravomocí k manipulaci s bezpečnostním systémem nebo povinnost odevzdat veškeré klíče, které měl zaměstnanec k dispozici. V průběhu pracovního vztahu nejsou zaměstnanci nijak školeni ani jinak vzdělávání v oblasti bezpečnosti informací.

3.4.4 Bezpečnost provozu a přístupu k ICT

Slabou stránkou bezpečnosti informací jsou pravidla a směrnice týkající se samotného ICT. Zaměstnanci nemají povinnost mít nastavená hesla k uživatelským účtům, nemusí dodržovat pravidla prázdného stolu a monitoru. Není definována podoba hesel ani požadavky na jeho změnu. Nejsou definována pravidla pro přístup k síťovým službám a zdrojům.

Uživatelé mají naprostou volnost při nastavování svých pracovních stanic, instalaci softwaru a konfiguraci hardwaru. Nejsou nijak sledovány jejich aktivity, ani zavedeny uživatelské skupiny a oprávnění. Taktéž nejsou zavedeny plány pro aktualizaci OS a antivirového softwaru. Tyto činnosti není možné spravovat hromadně nebo vzdáleně. Většina uživatelů nepoužívá personální firewall. Jak již bylo uvedeno, na uživatelských stanicích jsou většinou pouze antivirové programy v nevyhovujícím stavu.

V případě sítě jako celku jsou pro větší bezpečnost nastaveny pouze proxy server, firewall a poštovní server.

3.4.5 Zálohování

V organizaci není stanoven plán ani pravidla pro zálohování důležitých dat a jejich obnovu. Jak již bylo uvedeno v kapitole 3.3.4, o zálohování se starají zaměstnanci sami za sebe. Často tak dochází k nekonzistenci dat při jejich obnově nebo přenosu do jiných lokací, nebo dokonce k nenávratné ztrátě dat. Opatření jsou v tomto případě naprosto nedostatečná.

3.4.6 Řízení incidentů

Stejně tak nejsou v organizaci jasně dané žádné postupy, jak řešit incidenty tak, aby byl zajištěn další bezproblémový chod procesů. Není určeno, jak se mají zaměstnanci chovat v určitých problémových situacích a jak mají postupovat při hlášení problému. Nejsou jasně určené odpovědnosti za řešení těchto problémů ani reakční doba na incidenty. Zaměstnanci se tak často snaží incidenty řešit svépomocí nebo s kolegy, kteří k tomu nemají potřebnou kvalifikaci a zkušenosti. Druhou variantou je pak čekání na to, až se o problému dozví někdo, kdo je schopen jej vyřešit nebo alespoň zajistit řešení pomocí další osoby.

4 NÁVRH ŘEŠENÍ

V této části práce bude zpracována samotná metodika pro zavedení ISMS v organizaci. Bude proveden výběr vhodných metod, postupů a opatření na základě zjištěných skutečností o aktuálním stavu. U každého takového prvku bude uveden příklad, který pomůže pověřeným zaměstnancům s implementací.

4.1 Rozsah a hranice ISMS

Prvním formálním krokem pro zavedení je zpracování dokumentu „Rozsah a hranice ISMS“. Tento dokument bude obsahovat popis dotčených oblastí systému ISMS v konkrétním případě. Jeho přesná podoba bude stanovena vedením organizace ve spolupráci s kompetentními zaměstnanci. Avšak obecně lze určit, že rozsah bude zahrnovat všechny zaměstnance organizace a všechna hmotná a nehmotná aktiva ve vlastnictví organizace v místě sídla organizace. Za hranice se zde budou považovat aktiva, která jsou spravována dodavateli a jež bude možné nějakým způsobem ovlivnit. Z těchto aktiv budou vyjmuta ta, u kterých nebude shledán oprávněný důvod na zavedení opatření dle provedené analýzy rizik (z důvodu velmi nízkého rizika těchto aktiv)

4.2 Politika ISMS

Dalším důležitým dokumentem je „Politika ISMS“. Zde by mělo vedení organizace potvrdit svoji vůli k zavedení ISMS a vyjádřit, že chápe podstatu zavedení opatření a dalšího řízení ISMS. Zde je také potřeba přislíbit uvolnění personálních zdrojů a také obstarání finančních prostředků.

V tomto konkrétním případě se bude pravděpodobně jednat o jednoho zaměstnance, který již v současnosti spravuje ICT v organizaci. Zde by bylo ještě vhodné určit zastupující osobu pro tuto pozici, která by byla zároveň asistentem ve fázi zavádění opatření. Po finanční stránce by se dalo uvažovat o čerpání dotací od zřizovatele, popř. nějakém grantu.

V první řadě je nezbytné vypracovat metodiku pro analýzu rizik, a to tak, aby vyhovovala rozsahu pro konkrétní rozsah řízení bezpečnosti informací v organizaci. Na základě zjištěných skutečností bude určen další postup pro zavádění opatření.

4.3 Definice přístupu k hodnocení rizik

Vedení organizace by mělo sestavit dokument definující systematický přístup k hodnocení rizik. Ten by měl zahrnovat popis metodiky hodnocení rizik. Na jeho základě se bude provádět analýza rizik a budou se určovat kritéria pro jejich akceptaci a jejich akceptační úroveň. Obsah tohoto dokumentu bude čerpat z následujících kapitol.

4.4 Analýza rizik

Abychom mohli zkoumat míru rizik, musíme mít k dispozici informace o objektech, kterých se tato rizika týkají. Za tímto účelem se nejdříve provádí identifikace a ohodnocení aktiv. Dále je potřeba identifikovat hrozby a určit pravděpodobnost jejich výskytu. Následně posoudíme zranitelnost jednotlivých aktiv a v posledním kroku vypočteme míru rizik.

4.4.1 Identifikace a hodnocení aktiv

Identifikace aktiv proběhla s odpovědným zaměstnancem organizace. Ohodnocení aktiv bude realizováno číselnou škálou od 1 do 5, kde 1 bude znamenat nejméně důležitá aktiva a 5 nejdůležitější. V následujících tabulkách je uveden přehled aktiv informační bezpečnosti, která jsou důležitá pro činnost organizace a barevné znázornění důležitosti aktiv pro organizaci. Pro lepší orientaci a přehlednost je vhodné aktiva rozdělit do skupin a uvést jejich zdroj.

Tabulka 1: Stupnice hodnocení aktiv

Míra dopadu	Číselné hodnocení aktiva
Žádný dopad	**1**
Minimální dopad	**2**
Střední potíže nebo finanční ztráty	**3**
Velké potíže nebo finanční ztráty	**4**
Existenční potíže	**5**

Tabulka 2: Aktiva a jejich ohodnocení

Aktivum	Zdroj	Hodnota
Data		
Databáze sbírek	PC uživatelé	5
Dokumenty samostatné činnosti zaměstnanců	PC uživatelé	4
Osobní údaje zaměstnanců	PC ekonomické oddělení	4
Účetnictví - data	PC ekonomické oddělení	4
Účetnictví – doklady, výkazy	Kancelář ekonomické oddělení	4
Zálohy	PC uživatel	5
Software		
Operační systém	PC všechny	4
Účetní software	PC ekonomické oddělení	3
Software pro správu sbírek	PC uživatelé	3
Grafický software	PC grafik	2
MS Office	PC všechny	4
Antivirový software	PC některé	3
Hardware		
Uživatelské stanice	PC všechny	4
Síťová infrastruktura	Síťová kabeláž	4
Kancelářské vybavení	Tiskárny, skenery, kopírka	2
Síťové vybavení	Proxy server, firewall, poštovní server	4
Úložná zařízení	Přenosná média CD, DVD, USB	3
Služby		
Internetové připojení	Proxy server	3
Elektronická pošta	Poštovní server	3
Služby sdílení v síti	Switch, síťová infrastruktura	2

4.4.2 Identifikace hrozeb a zranitelnosti

Dalším krokem při zpracování analýzy rizik je identifikace hrozeb, které mohou aktiva ovlivnit a určení pravděpodobnosti jejich výskytu. Opět byla zvolena pětistupňová škála pro pravděpodobnost výskytu hrozby, která bude označena podle následujícího schématu. Z hrozeb byla vytvořena tabulka níže.

Tabulka 3: Stupnice pravděpodobnosti hrozeb

Míra pravděpodobnosti	Číselná hodnota
Velmi nízká pravděpodobnost	**1**
Nízká pravděpodobnost	**2**
Střední pravděpodobnost	**3**
Vysoká pravděpodobnost	**4**
Velmi vysoká pravděpodobnost	**5**

Tabulka 4: Identifikované hrozby

Hrozba	Pravděpodobnost
Ztráta či poškození úložných zařízení	4
Porucha HW	3
Chybné zadání dat	4
Únik bezpečnostních kódů	2
Výpadek napájení	3
Živelná pohroma	1
Narušení síťové infrastruktury	3
Útok na síť z vnějšku	2
Malware	4
Výpadek připojení do internetu	2
Požár	2
Vniknutí vody do zařízení	3
Krádež zařízení	2
Fyzické vniknutí neoprávněné osoby	3
Kompromitace hesel	3
Chybné řešení incidentu	5

Nyní je potřeba posoudit zranitelnost jednotlivých aktiv. K tomu slouží matice zranitelnosti, do které zaneseme údaje o hodnotě aktiv a pravděpodobnosti hrozeb, následně doplníme zranitelnost. I zde je zranitelnost určena škálou od 1 do 5 dle tabulky níže.

Tabulka 5: Stupnice zranitelnosti aktiv

Zranitelnost	Číselná hodnota
Zanedbatelná zranitelnost	1
Nízká zranitelnost	2
Střední zranitelnost	3
Vysoká zranitelnost	4
Kritická zranitelnost	5

Tabulka 6: Matice zranitelnosti - část 1/2

Zranitelnost (1/2)	Popis aktiva	Databáze sbírek	Dokumenty samostatné činnosti zaměstnanců	Osobní údaje zaměstnanců	Účetnictví - data	Účetnictví – doklad, výkazy	Zálohy	Operační systém	Účetní software	Software pro správu sbírek	Grafický software
	Hodnota aktiva	5	4	4	4	4	5	4	3	3	2
Popis hrozby	Pravděpodobnost										
Ztráta či poškození úložných zařízení	4	3	3	2	2		4				
Porucha HW	3	3	3	2	2		2				
Chybné zadání dat	4	3		3	3	2	3	2	3	2	
Únik bezpečnostních kódů	2			1	1	2	1				
Výpadek napájení	3	2						1			
Živelná pohroma	1	2	2			3	2				
Narušení síťové infrastruktury	3										
Útok na síť z vnějšku	2	1	1	2	2			2			
Malware	4	2	2	4	3			3			
Výpadek připojení k internetu	2										
Požár	2	2	2	2	2	3	3				
Vniknutí vody do zařízení	3	1	1	1	1		1				
Krádež zařízení	2	1	1	3	3		2				
Fyzické vniknutí neoprávněné osoby	3	1	1	3	3	3	2				
Kompromitace hesel	3	3	3	3	3			3	3		
Chybné řešení incidentu	5	3	3	3	3	3	3	3	3		

Tabulka 7: Matice zranitelnosti - část 2/2

Zranitelnost (2/2)	Popis aktiva	MS Office	Antivirový software	Uživatelské stanice	Síťová infrastruktura	Kancelářské vybavení	Síťové vybavení	Úložná zařízení	Internetové připojení	Elektronická pošta	Služby sdílení v síti
	Hodnota aktiva	4	3	4	4	2	4	3	3	3	2
Popis hrozby	Pravděpodobnost										
Ztráta či poškození úložných zařízení	4							3			
Porucha HW	3			3	2	3	3	2	2	2	2
Chybné zadání dat	4		1				1				
Únik bezpečnostních kódů	2			3		2	2	2	1	1	1
Výpadek napájení	3			2		2	2		2	2	2
Živelná pohroma	1			3	2	3	3	2	3	2	2
Narušení síťové infrastruktury	3		1		4		3		3	3	3
Útok na síť z vnějšku	2		1	2			3		2	2	2
Malware	4	2	2	2			2		1	3	1
Výpadek připojení k internetu	2								3	2	
Požár	2			3	3	3	3	3	2	2	2
Vniknutí vody do zařízení	3			4		2	2		1	1	1
Krádež zařízení	2			3		2	2	3			
Fyzické vniknutí neoprávněné osoby	3			2	2	2	2	2	1	1	1
Kompromitace hesel	3		2							3	
Chybné řešení incidentu	5		3	3	3	3	3	3	1	3	2

Posledním krokem je výpočet míry rizika a její vynesení do matice rizik. Míra rizika se vypočte dle vzorce **R = T*A*V**,

Přičemž **R** = míra rizika

T = pravděpodobnost vzniku hrozby

A = hodnota aktiva

V = zranitelnost aktiva

Nakonec je ještě vhodné stanovit hranice rizika podle toho, jak jsou pro organizaci významná. Zvolené hranice jsou uvedeny v tabulce níže a jejich barevné znázornění je použito v matici rizik.

Tabulka 8: Hranice míry rizika

Míra rizika	Číselná hodnota
Bezvýznamné riziko	**0 - 10**
Akceptovatelné riziko	**10 – 20**
Mírné riziko	**20 – 30**
Nežádoucí riziko	**30 – 60**
Nepřijatelné riziko	**60 -**

Tabulka 9: Matice rizik - část 1/2

Riziko (1/2)	Popis aktiva	Databáze sbírek	Dokumenty samostatné činnosti zaměstnanců	Osobní údaje zaměstnanců	Účetnictví - data	Účetnictví – doklad, výkazy	Zálohy	Operační systém	Účetní software	Software pro správu sbírek	Grafický software
	Hodnota aktiva	5	4	4	4	4	5	4	3	3	2
Popis hrozby	Pravděpodobnost										
Ztráta či poškození úložných zařízení	4	60	48	32	32		80				
Porucha HW	3	45	36	24	24		30				
Chybné zadání dat	4	60		48	48	32	60	32	36	24	
Únik bezpečnostních kódů	2			8	8	16	10				
Výpadek napájení	3	30						12			
Živelná pohroma	1	10	8			12	10				
Narušení síťové infrastruktury	3										
Útok na síť z vnějšku	2	10	8	16	16			16			
Malware	4	40	32	64	48			48			
Výpadek připojení k internetu	2										
Požár	2	20	16	16	16	24	30				
Vniknutí vody do zařízení	3	15	12	12	12		15				
Krádež zařízení	2	10	8	24	24		20				
Fyzické vniknutí neoprávněné osoby	3	15	12	36	36	36	30				
Kompromitace hesel	3	45	36	36	36			36	27		
Chybné řešení incidentu	5	75	60	60	60	60	75	60	45		

Tabulka 10: Matice rizik - část 2/2

Riziko (2/2)	Popis aktiva	MS Office	Antivirový software	Uživatelské stanice	Síťová infrastruktura	Kancelářské vybavení	Síťové vybavení	Úložná zařízení	Internetové připojení	Elektronická pošta	Služby sdílení v síti
	Hodnota aktiva	4	3	4	4	2	4	3	3	3	2
Popis hrozby	Pravděpodobnost										
Ztráta či poškození úložných zařízení	4							36			
Porucha HW	3			36	24	18	36	18	18	18	12
Chybné zadání dat	4		12				16				
Únik bezpečnostních kódů	2			24		8	16	12	6	6	4
Výpadek napájení	3			24		12	24		18	18	12
Živelná pohroma	1			12	8	6	12	6	9	6	4
Narušení síťové infrastruktury	3		9		48		36		27	27	18
Útok na síť z vnějšku	2		6	16			24		12	12	8
Malware	4	32	24	32			32		12	36	8
Výpadek připojení k internetu	2								18	12	
Požár	2			24	24	12	24	18	12	12	8
Vniknutí vody do zařízení	3			48		12	24		9	9	6
Krádež zařízení	2			24		8	16	18			
Fyzické vniknutí neoprávněné osoby	3			24	24	12	24	18	9	9	6
Kompromitace hesel	3		18							27	
Chybné řešení incidentu	5		45	60	60	30	60	45	15	45	20

4.4.3 Vyhodnocení analýzy rizik

Po provedení analýzy rizik bylo zjištěno, v kterých aspektech bezpečnosti informací má organizace největší nedostatky. Při konzultaci s kompetentními osobami v organizaci bylo rozhodnuto, že by měla být zavedena opatření týkající se aktiv a hrozeb s nejvyšším stupněm rizika a také některých s nežádoucím a mírným stupněm rizika.

Pro další postup byla tedy vybrána následující témata:

- Bylo zjištěno, že největší podíl na případných bezpečnostních událostech a incidentech mají zaměstnanci
- A to hlavně v souvislosti s jejich neznalostí problematiky informační bezpečnosti a povědomím o tom, jak incidenty řešit
- Tyto skutečnosti mohou ovlivnit velkou část aktiv organizace, jak hmotných, tak i nehmotných
- Mezi nezanedbatelné problémy patří také hrozba malwaru (nedostatečná ochrana), což může ovlivnit zejména nehmotná aktiva organizace
- Zásadním problémem je také politika hesel v organizaci
- Určité rezervy jsou i v možnostech zadávání chybných dat do databází sbírek
- Nemalý problém se týká také metodiky zálohování a nakládání se zálohami
- Je třeba vyřešit určité nedostatky týkající se síťové infrastruktury
- V neposlední řadě je nutné lépe kontrolovat fyzických přístup cizích osob do prostor organizace

Zbylá rizika s nižší hodnotou (do 20), budou pravděpodobně akceptována, ovšem měla by zůstat v přehledu rizik a být sledována kvůli jejich dalšímu vývoji. Rozhodnutí o jejich akceptaci a stanovení akceptační úrovně bude definováno v kapitole „Akceptace rizik“.

4.5 Návrh opatření

V tomto bodě budou popsány doporučené kroky k minimalizaci zjištěných rizik. Jelikož se jedná o návrh metodiky a doporučení pro zavádění pro organizaci, budou opatření navržena s takovou mírou konkrétnosti, aby bylo zaměstnancům jasné, co daná opatření znamenají a zahrnují, ale zároveň dávala prostor pro návrh vlastního konkrétního řešení. Tedy bude doporučeno co je potřeba udělat, ale nebude přesně specifikováno, jak to udělat. Obsah této kapitoly je zároveň nutné zformovat do podoby dokumentu, který je součástí povinné dokumentace ISMS.

Na konci kapitoly budou uvedena rizika, která budou doporučena k akceptaci. V následující kapitole budou také uvedena vybraná opatření tak, jak jsou obsažena v příloze A normy ČSN ISO/IEC 27001:2014, to pomůže lépe zohlednit cíle opatření a také umožní kontrolu, zda nebyla některá důležitá opatření opomenuta. Dále bude uveden odkaz na odpovídající kapitoly normy ČSN ISO/IEC 27002:2014, kde jsou jednotlivá opatření detailněji popsána.

4.5.1 Zvyšování povědomí zaměstnanců v oblasti informační bezpečnosti

Jak vyplynulo z analýzy rizik, a pokud zároveň budeme na rizika nahlížet ze strany hrozeb, je zřejmé, že jedním z nejslabších článků informační bezpečnosti v organizaci je povědomí zaměstnanců o informační bezpečnosti vůbec. Do tohoto problému je možné zahrnout jejich nezájem současný stav vůbec nějak měnit nebo řešit, ale také neznalost toho, jak se v případě bezpečnostních událostí nebo incidentů zachovat.

Z tohoto důvodu bude nezbytné zavést systém školení, která by zaměstnancům pomohla pochopit důležitost informační bezpečnosti, a zároveň jim dala jasné pokyny pro řešení problémů. Aby se takový systém podařilo prosadit, bude vhodné jej zavést do interních směrnic. Zaměstnanci tak budou povinni absolvovat tato školení v předem určených intervalech a v předem určeném rozsahu. Následně bude nutné prokázat nabyté znalosti pomocí testů. Zaměstnancům, kterým se nepodaří prokázat znalosti na určené úrovni, budou doporučena dodatečná školení.

Doporučený obsah a podoba vzdělávacího systému zaměstnanců

- Zaměstnanci budou seznámeni s pojmem informační bezpečnosti a jeho významem, se směrnicemi bezpečnosti informací, pravidly a plány zálohování, politikou hesel, pravidly pro umístění a zacházení s HW a pravidly pro řešení událostí a incidentů bezpečnosti informací
- Nejdříve bude vhodné ověřit znalosti problematiky obecnějším testem a dle jeho výsledků upravit obsah jednotlivých školení
- V prvotní fázi proběhne několik školení s odstupem jednoho měsíce, rozdělených dle témat uvedených výše, po uskutečnění školení bude s odstupem jednoho měsíce provedeno ověření získaných znalostí a hodnocení aktuálního stavu
- Po dokončení prvotní fáze bude zaveden systém pravidelného ověřování znalostí každých 6 měsíců
- V případě nesplnění daných podmínek v kterékoliv fázi bude konkrétním jedincům doporučeno dodatečné školení s navazujícím opětovným testováním

4.5.2 Metodika zálohování, plány, pravidla

Pro organizaci jsou velmi cenná data o sbírkových předmětech a dokumenty prací vlastní tvorby zaměstnanců. I přesto je současný stav zálohováni v organizaci žalostný. Bude tedy vhodné vytvořit metodiku pro zálohování, určit pravidla a stanovit plány.

Doporučená podoba metodiky zálohování

- Je třeba změnit návyky zaměstnanců, k tomu slouží školení a testy
- Pravidla pro zálohování by měla být závazná a měla by být zanesena do interních směrnic, nedodržováním pravidel by se zaměstnanec dopouštěl porušení směrnic a mohly proti němu být vyvozeny patřičné důsledky
- V podmínkách organizace připadají v úvahu méně nákladné metody zálohování dat
- Za nedostatečnou zálohu by se mělo považovat vytvoření kopie dokumentu nebo dat na stejném fyzickém médiu, minimální dostatečnou zálohou se rozumí vytvoření kopie dat nebo dokumentu na jiném fyzickém médiu i ve stejné stanici, doporučeným způsobem je záloha na externí médium, v úvahu připadá i síťové úložiště s diskovým polem minimálně úrovně RAID 1

- Měl by být doporučen nebo závazně stanoven interval pro zálohu důležitých dat, aktuálně zpracovávaná data by měla být zálohována nejlépe každý den, dokončené práce a historická data alespoň na konci pracovního týdne
- Je vhodné zohlednit typ zálohovacího média, v případě CD/DVD disků je třeba kontrolovat integritu dat nebo používat média určená k zálohování a archivaci, popř. se jim úplně vyhnout, v současnosti lze doporučit média s pamětí typu flash, tedy USB disky a paměťové karty
- Dále je důležité dodržovat zásady správného zacházení s takovými médii, u optických disků zajistit ochranu povrchu a uložení v odpovídajících podmínkách teploty, vlhkosti a světla, u pamětí typu flash se vyvarovat silným elektrostatickým výbojům
- Zaměstnanci by měli udržovat pořádek v zálohách a měli by kontrolovat jejich konzistenci

4.5.3 Uživatelské účty, kontrola, skupiny

I přes zavedení školení nebude úplně snadné se vyhnout incidentům, které uživatelé způsobí ať už neúmyslným jednáním, nebo snahou uskutečnit svoje „pokusy“. To je jen jeden z důvodů, proč by se vyplatilo přemýšlet o zavedení nějakého systému na protokolu LDAP, např. MS Active Directory. To by umožnilo nejenom mít o uživatelích lepší přehled, ale také by bylo snazší řídit jejich účty po různých stránkách. Zejména by se snáze prosazovala politika hesel, bylo by možné na dálku a centralizovaně omezit práva uživatelů na různé zásahy do systému, bylo by možné vytvořit uživatelské skupiny a na jejich základě udělovat autorizace pro různé činnosti v síti (přístup do sdíleného úložiště apod.), v neposlední řade by byl zajištěn větší přehled nad autentizacemi uživatelů a sledování jejich aktivit.

Doporučení pro uživatelské účty

- V nejzákladnějším scénáři provést kontrolu uživatelských účtů na pracovních stanicích, odebrat administrátorská práva, sjednotit pravidla pro nastavení operačních systémů, prosadit politiku hesel

- V ideálním případě pořídit server a odpovídající OS pro zavedení MS Active Directory, zřídit uživatelské účty pro AD, vytvořit domény, skupiny, rozdělit do nich uživatele, přiřadit jednotlivým skupinám oprávnění, omezit možnosti nastavení a modifikace OS, prosadit politiku hesel, v případě nutnosti dovybavit stanice odpovídajícím OS.
- V případě nutnosti a po dohodě se správcem ICT přiřadit konkrétním zaměstnancům dodatečná oprávnění
- V případě zprovoznění bezdrátové sítě bude možné pomocí AD autentizovat, autorizovat a kontrolovat klienty díky protokolu 802.1x a bude možné provozovat NAC (Network Access Control – řízení přístupu k síti)
- Měla by být ustanovena povinnost dodržování pravidla čistého stolu a monitoru

4.5.4 Politika hesel

S předchozím bodem částečně souvisí problematika hesel, pro kterou nejsou v organizaci prakticky žádná pravidla. Proto bude vhodné tato pravidla stanovit a také je zanést do interních směrnic a školení. Dodržování těchto pravidel bude povinné.

Doporučení pro politiku hesel

- Za povinné bude považováno používání hesel k uživatelským účtům zaměstnanců na pracovních stanicích
- **Heslo musí splňovat požadavky na minimální délku 8 znaků a musí obsahovat minimálně jedno velké písmeno, jedno malé písmeno, jednu číslici a jeden speciální znak**
- Zaměstnanec nesmí mít své heslo nikde poznamenané a nesmí jej vyzradit další osobě
- Zaměstnanec je povinen své heslo změnit jednou za 12 měsíců, přičemž nesmí použít již v minulosti nastavené heslo

4.5.5 Ochrana proti malwaru

Jelikož v organizaci není úplně ideální stav ochrany proti malwaru, bude vhodné dovybavit nedostatečně chráněné uživatelské stanice odpovídajícím softwarovým vybavením a zajistit správu této ochrany. Na základě toho, že organizace využívá výhodného licencování konkrétní společnosti, bude vhodné doplnit další licence od stejné společnosti a zkontrolovat stav stávajících licencí a instalací antivirového softwaru.

Doporučení pro ochranu proti malwaru

- Zkontrolovat stav aktuálních licencí antivirového softwaru, stav instalací, nastavení a aktuálnost virových databází
- V nevyhovujících případech pořídit nové licence, aktualizovat software a databáze na nejnovější verze, upravit potřebná nastavení
- Sjednotit podobu ochrany a nastavení na všech uživatelských stanicích
- Provádět ve spolupráci se zaměstnanci kontrolu aktuálnosti virových databází, zaměstnanci budou mít povinnost alespoň jednou týdně zkontrolovat stav antivirového softwaru a případné nedostatky hlásit správci ICT
- Vhodné by bylo také vyjednat výhodnější podmínky licencování z důvodu právní formy příspěvkové organizace
- Vyškolit zaměstnance v problematice přenosu malwaru pomocí internetu, elektronické pošty a přenosných úložných zařízení a zavést povinnost jejich kontroly při připojování do pracovních stanic v organizaci

4.5.6 Bezpečnost zařízení

Vzhledem k nevyhovujícím podmínkám umístění některého zařízení a neexistenci pravidel pro jejich umístění a manipulaci bude vhodné učinit změny v umístění zejména některých pracovních stanic a dalšího hardwaru a také určit pravidla pro zacházení s ním.

Doporučení pro ochranu zařízení

- Je třeba zkontrolovat, zda se některé uživatelské stanice a další hardware nenachází v přílišné blízkosti zdrojů tepla nebo tekutin, a zda je k nim zajištěn dostatečný přístup vzduchu z důvodu chlazení, případné nedostatky odstranit
- Stanovit pravidla pro manipulaci zejména s tekutinami v blízkosti technického vybavení
- Zakázat konfiguraci hardwaru nepovolaným osobám, určit zaměstnance, kteří k tomu budou mít kompetence
- Zavést výše zmíněná pravidla do interních směrnic a kontrolovat jejich dodržování
- Prověřit lepší možnosti chlazení rackové skříně se síťovým vybavením umístěné na chodbě

4.5.7 Ochrana a správa síťové infrastruktury

Kvůli nevyhovujícímu systému značení síťové kabeláže a dalších prvků sítě a jejich ochrany bude vhodné zavést systém značení dle běžných zvyklostí a také zajistit ochranu zejména datových zásuvek v kancelářích a ochranu jejich zapojení.

Doporučení pro správu síťové infrastruktury

- Zavést systém značení síťových prvků
- Nejdříve by měl být zaveden systém značení jednotlivých místností, ten by měl obsahovat i vysvětlující popis a seznam prvků v jednotlivých místnostech
- Dále by měly být označeny všechny datové zásuvky, a to tak, aby jejich označení korespondovalo s místem výskytu, a také jejich jednotlivé porty
- Do nevyužitých portů datových zásuvek by měly být umístěny blokátory, zapojené kabely by měly být uzamčeny proti neoprávněné manipulaci
- Mělo by být doplněno i značení prvků v rackové skříni, tzn. porty patch panelu, jednotlivá zařízeni, porty switche, kabely na obou koncích
- Do systému by měly být zahrnuty i koncové stanice, které by měly mít také vlastní označení v systému
- Měly by být pověřeny osoby pro manipulaci se síťovými prvky a stanovena pravidla pro jejich konfiguraci a manipulaci

4.5.8 Incident management

Pokud dojde v organizaci k bezpečnostnímu incidentu, zaměstnanci většinou netuší, jak nastalý incident řešit. Tato situace si žádá zavedení jednoznačných pravidel, která pomohou zaměstnancům správně odhadnout situaci a incident buď samostatně vyřešit, nebo jeho popis předat správným způsobem předat odpovědné osobě.

Doporučení pro zavedení incident managementu

- Zaměstnanci musí být v rámci školení poučeni o možnostech samostatného řešení nastalých incidentů, dále o nutnosti hlášení incidentů odpovědné osobě a o eskalaci incidentů mimo jejich schopnosti a znalosti
- Měla by být určena závazná forma a způsoby hlášení a eskalace incidentů, měly by být pověřeny odpovědné osoby

- Schéma postupu při výskytu incidentu: incident > zvládnu jej vyřešit sám? > pokud ano, vyřeším jej dle daných postupů a poté ohlásím / pokud ne, nebudu se snažit o jeho vyřešení a ohlásím jej odpovědné osobě
- Způsoby hlášení dle možností seřazené dle preferované podoby: osobně, telefonicky, emailem, v papírové formě, ke každému incidentu je nutné vyplnit elektronický nebo tištěný formulář s povinnými údaji
- Povinné údaje při hlášení incidentu: datum a čas incidentu, místo incidentu, čeho se incident týká, popis incidentu, údaje o osobě hlásící incident
- Z nahlášených incidentů bude vhodné tvořit statistiky, které poslouží v dalších analýzách rizik a které pomohou při návrhu dalších opatření k zabránění nejzávažnějších incidentů

4.5.9 Fyzický přístup

V problematice fyzického přístupu na tom není organizace úplně špatně, ale i zde je určitý prostor pro zlepšení. Zásadním nedostatkem je kontrola přístupu cizích osob do kancelářských prostor budovy. Částečným řešením tohoto problému by byla instalace kamerového systému v místech vstupu do těchto prostor, tedy např. v prostorách schodiště nebo mříží služebního vchodu a v prostorách ochozu spojujícího výstavní a kancelářskou část budovy. Druhou část doporučení by měla tvořit povinnost zavírat a zamykat veškeré přístupové dveře a mříže do kancelářských a technických prostor, což se ne vždy dodržuje. Proti nedodržování těchto pravidel by měly být zavedena kárná opatření.

Doporučení pro fyzický přístup

- Instalace kamerového systému ve vstupních prostorách do kancelářského traktu
- Zavedení povinnosti zavírat a zamykat přístupové dveře a mříž
- Zavedení kárných opatření při nedodržování pravidel
- Prosadit povinnost vyprovodit návštěvy až ke vstupním dveřím

4.5.10 Konfigurace softwaru

Tato oblast se v konkrétním případě týká dvou hlavních oblastí. Jedno z nich je aktuálnost operačního systému na uživatelských stanicích. Druhou pak vhodnost a schopnosti softwaru pro správu sbírek, který se v současnosti v organizaci používá.

Doporučení týkající se softwarového vybavení

- Součástí politiky uživatelských účtů a jejich konfigurace by měla být správa aktualizací operačního systému na uživatelských stanicích zaměstnanců, je třeba zajistit včasnou instalaci důležitých aktualizací OS bez zbytečného odkladu
- Je žádoucí, aby byl dokončen projekt nahrazení stávajícího softwaru pro správu sbírek, to bude mít za výsledek vyřešení problémů s integritou dat v databázích sbírek a přispění k informační bezpečnosti pro organizaci stěžejní oblasti
- Předchozí krok také usnadní přenos dat mezi jednotlivými uživateli a umožní jejich centralizované uložení, správu a přístup, potažmo zálohování
- Další výhodou bude omezení vstupu pouze na platné hodnoty včetně jejich automatické kontroly

4.5.11 Interní směrnice bezpečnosti informací

Aby měla všechna předešlá opatření nějaký smysl a váhu, je nutné jejich zavedení podpořit tím, že budou součástí interních směrnic informační bezpečnosti v organizaci. Proto je důležité takový dokument vypracovat a jasně v něm definovat, co je povinnostmi zaměstnanců v zájmu prosazení jednotlivých opatření a dosažení jejich cílů.

Interní směrnice by měly mít formu závazných pravidel, při jejichž nedodržení budou vyvozeny důsledky ve smyslu kárného opatření. Dokument by měl obsahovat odkazy na jednotlivá opatření a stanovy, jež byly vybrány v rámci zavádění systému řízení informační bezpečnosti. Měl by jasně definovat dotčené osoby, jejich funkce v systému, kompetence, povinnosti a pravomoci. Dále časový rozsah platnosti a podmínky pro změny směrnic. Dokument by měl být součástí pracovněprávního vztahu mezi zaměstnavatelem a zaměstnancem. Zaměstnanec by měl být seznámen s každou jeho změnou.

4.6 Cíle opatření a bezpečnostní opatření pro zvládání rizik

Tato část dokumentu by měla výrazně usnadnit zaměstnancům organizace implementaci vybraných opatření a pochopit jejich podstatu a cíle. Bude se jednat o výčet konkrétních opatření nebo jejich skupin, tak jak jsou uvedena v příloze A normy ČSN ISO/IEC 27001:2014 a jejich detailní popis je obsažen v normě ČSN ISO/IEC 27002:2014.

Kromě zmíněné výhody bude dalším přínosem i to, že při výběru opatření z těchto norem dochází i kontrole toho, zda nebyly opomenuty některé důležité oblasti a některá důležitá opatření. Při zavádění opatření dle zmíněných norem není potřeba zavést všechna, pokud organizace neuvažuje o certifikaci. Výhodou je i samotný fakt, že opatření jsou součástí normy a jsou tedy zpracována oborníky v daném oboru.

4.6.1 Přehled opatření vybraných z přílohy A normy ČSN ISO/IEC 27001:2014

Tabulka 11: Přehled opatření dle přílohy A normy ČSN ISO/IEC 27001:2014 (Převzato z (13))

A.5 Politiky bezpečnosti informací		
A.5.1 Směřování bezpečnosti informací vedením organizace Cíl: Poskytovat pokyny v oblasti řízení a podporu pro informační bezpečnost v souladu s obchodními požadavky a příslušnými zákony a předpisy.		
A.5.1.1	Politiky pro bezpečnost informací	**Zavést**
A.5.1.2	Přezkoumání politik pro bezpečnost informací	**Zavést**
A.6 Organizace bezpečnosti informací		
A.6.1 Interní organizace Cíl: Vytvořit rámec řízení pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace.		
A.6.1.1	Role a odpovědnosti bezpečnosti informací	**Zavést**
A.6.1.2	Princip oddělení povinností	**Zavést**
A.6.1.3	Kontakt s příslušnými orgány a autoritami	**Doplnit**
A.6.1.4	Kontakt se zájmovými skupinami	Ignorovat
A.6.1.5	Bezpečnost informací v řízení projektu	Ignorovat
A.6.2 Mobilní zařízení a práce na dálku Cíl: Zajistit bezpečnost práce na dálku a používání mobilních zařízení.		
A.6.2.1	Politika mobilních zařízení	**Doplnit**

A.6.2.2	Práce na dálku	Ignorovat
A.7 Bezpečnost lidských zdrojů		
A.7.1 Před vznikem pracovního poměru Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.		
A.7.1.1	Prověřování	**Doplnit**
A.7.1.2	Podmínky pracovního vztahu	**Doplnit**
A.7.2 Během pracovního vztahu Cíl: Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spojených, svých odpovědností a povinností a aby byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.		
A.7.2.1	Odpovědnosti vedení organizace	**Doplnit**
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	**Zavést**
A.7.2.3	Disciplinární řízení	**Zavést**
A.7.3 Ukončení a změna pracovního vztahu Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.		
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	**Doplnit**
A.8. Řízení aktiv		
A.8.1 Odpovědnost za aktiva Cíl: Identifikovat aktiva organizace a definovat odpovídající odpovědnost za jejich ochranu.		
A.8.1.1	Seznam aktiv	**Zavést**
A.8.1.2	Vlastnictví aktiv	**Zavést**
A.8.1.3	Přípustné použití aktiv	**Zavést**
A.8.1.4	Navrácení aktiv	**Doplnit**
A.8.2 Klasifikace informací Cíl: Zajistit, že informace budou chráněny na odpovídající úrovni v souladu s jejich důležitostí pro organizaci.		
A.8.2.1	Klasifikace informací	**Zavést**
A.8.2.2	Označování informací	**Zavést**
A.8.2.3	Manipulace s aktivy	**Zavést**

A.8.3 Manipulace s médii Cíl: Zabránit neoprávněnému zpřístupnění, úpravě, odstranění nebo zničení informací na médiích.		
A.8.3.1	Správa výměnných médií	**Zavést**
A.8.3.2	Likvidace médií	**Doplnit**
A.8.3.3	Přeprava fyzických médií	**Zavést**
A.9 Řízení přístupu		
A.9.1 Požadavky organizace na řízení přístupu Cíl: Omezit přístup k informacím a zařízením pro zpracování informací.		
A.9.1.1	Politika řízení přístupu	**Zavést**
A.9.1.2	Přístup k síti a síťovým službám	**Zavést**
A.9.2 Řízení přístupu uživatelů Cíl: Zajistit autorizovaný přístup uživatelů a zabránit neautorizovanému přístupu k systémům a službám.		
A.9.2.1	Registrace a zrušení uživatele	**Zavést**
A.9.2.2	Správa uživatelských přístupů	**Zavést**
A.9.2.3	Správa privilegovaných přístupových práv	**Zavést**
A.9.2.4	Správa tajných autentizačních informací uživatelů	**Zavést**
A.9.2.5	Přezkoumání přístupových práv uživatelů	**Zavést**
A.9.2.6	Odebrání nebo úprava přístupových práv	**Zavést**
A.9.3 Odpovědnosti uživatelů Cíl: Učinit uživatele odpovědné za ochranu svých autentizačních informací.		
A.9.3.1	Používání tajných autentizačních informací	**Zavést**
A.9.4 Řízení přístupu k systémům a aplikacím Cíl: Zabránit neautorizovanému přístupu k systémům a aplikacím.		
A.9.4.1	Omezení přístupu k informacím	**Zavést**
A.9.4.2	Bezpečné postupy přihlášení	**Zavést**
A.9.4.3	Systém správy hesel	**Zavést**
A.9.4.4	Použití privilegovaných programových nástrojů	Ignorovat
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	Ignorovat
A.10 Kryptografie		
A.10.1 Kryptografická opatření		

Cíl: Zajistit správné a efektivní využívání kryptografie pro ochranu důvěrnosti, autenticity a/nebo integrity informací.		
A.10.1.1	Politika pro použití kryptografických opatření	Ignorovat
A.10.1.2	Správa klíčů	Ignorovat
A.11 Fyzická bezpečnost a bezpečnost prostředí		
A.11.1 Bezpečné oblasti Cíl: Zabránit neoprávněnému fyzickému přístupu, poškození a zásahu do informací a zařízení pro zpracování informací organizace.		
A.11.1.1	Fyzický bezpečnostní perimetr	**Doplnit**
A.11.1.2	Fyzické kontroly vstupu	**Doplnit**
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	**Doplnit**
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	**Doplnit**
A.11.1.5	Práce v bezpečných oblastech	Ignorovat
A.11.1.6	Oblasti pro nakládku a vykládku	Ignorovat
A.11.2 Zařízeni Cíl: Zabránit ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace.		
A.11.2.1	Umístění zařízení a jeho ochrana	**Doplnit**
A.11.2.2	Podpůrné služby	**Doplnit**
A.11.2.3	Bezpečnost kabelových rozvodů	**Doplnit**
A.11.2.4	Údržba zařízení	**Doplnit**
A.11.2.5	Přemístění aktiv	**Zavést**
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	**Doplnit**
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	**Zavést**
A.11.2.8	Uživatelská zařízení bez obsluhy	**Doplnit**
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	**Zavést**
A.12 Bezpečnost provozu		
A.12.1 Provozní postupy a odpovědnosti Cíl: Zajistit správnou a bezpečnou činnost zařízení pro zpracování informací		
A.12.1.1	Dokumentované provozní postupy	**Zavést**
A.12.1.2	Řízení změn	**Zavést**
A.12.1.3	Řízení kapacit	Ignorovat

A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	Ignorovat
A.12.2 Ochrana proti malwaru Cíl: Zajistit ochranu informací a zařízení pro zpracování informací proti malwaru.		
A.12.2.1	Opatření proti malwaru	**Doplnit**
A.12.3 Zálohování Cíl: Zabránit ztrátě dat.		
A.12.3.1	Zálohování informací	**Doplnit**
A.12.4 Zaznamenávání formou logů a monitorování Cíl: Zaznamenávat události a vytvářet důkazy.		
A.12.4.1	Zaznamenávání událostí formou logů	**Doplnit**
A.12.4.2	Ochrana logů	Ignorovat
A.12.4.3	Logy o činnosti administrátorů a operátorů	Ignorovat
A.12.4.4	Synchronizace hodin	Ignorovat
A.12.5 Správa provozního softwaru Cíl: Zajistit integritu provozních systémů.		
A.12.5.1	Instalace softwaru na provozní systémy	**Zavést**
A.12.6 Řízení technických zranitelností Cíl: Zabránit zneužití technických zranitelností		
A.12.6.1	Řízení technických zranitelností	**Zavést**
A.12.6.2	Omezení instalace softwaru	**Zavést**
A.12.7 Hlediska auditu informačních systémů Cíl: Minimalizovat dopad aktivit auditu na provozní systémy.		
A.12.7.1	Opatřeni k auditu informačních systémů	Ignorovat
A.13 Bezpečnost komunikací		
A.13.1 Správa bezpečnosti sítě Cíl: Zajistit ochranu informací v sítích a jejich podpůrných zařízeních pro zpracování informací.		
A.13.1.1	Opatření v sítích	**Zavést**
A.13.1.2	Bezpečnost síťových služeb	**Zavést**
A.13.1.3	Princip oddělení v sítích	**Zavést**
A.13.2 Přenos informací		

Cíl: Zachovat bezpečnost informací přenášených v rámci organizace a s externími subjekty.		
A.13.2.1	Politiky a postupy při přenosu informací	**Zavést**
A.13.2.2	Dohody o přenosu informací	**Zavést**
A.13.2.3	Elektronické předávání zpráv	**Zavést**
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	**Zavést**
A.14 Akvizice, vývoj a údržba systémů		
A.14.1 Bezpečnostní požadavky informačních systémů Cíl: Zajistit, že informační bezpečnost je nedílnou součástí informačních systémů v průběhu celého životního cyklu. To zahrnuje také požadavky na informační systémy, které poskytují služby prostřednictvím veřejných sítí.		
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	Ignorovat
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	Ignorovat
A.14.1.3	Ochrana transakci aplikačních služeb	Ignorovat
A.14.2 Bezpečnost v procesech vývoje a podpory Cíl: Zajistit, že informační bezpečnost je navržena a realizována v rámci životního cyklu vývoje informačních systémů.		
A.14.2.1	Politika bezpečného vývoje	Ignorovat
A.14.2.2	Postupy řízení změn systému	Ignorovat
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	Ignorovat
A.14.2.4	Omezení změn softwarových balíků	Ignorovat
A.14.2.5	Principy budování bezpečných systémů	Ignorovat
A.14.2.6	Prostředí bezpečného vývoje	Ignorovat
A.14.2.7	Outsourcovaný vývoj	Ignorovat
A.14.2.8	Testování bezpečnosti systémů	Ignorovat
A.14.2.9	Testování akceptace systémů	Ignorovat
A.14.3 Data pro testování Cíl: Zajistit ochranu dat používaných pro testování.		
A.14.3.1	Ochrana dat pro testování	Ignorovat
A.15 Dodavatelské vztahy		
A.15.1 Bezpečnost informací v dodavatelských vztazích Cíl: Zajistit ochranu aktiv organizace, která jsou přístupná dodavatelům.		

A.15.1.1	Politika bezpečnosti informaci pro dodavatelské vztahy	Ignorovat
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	Ignorovat
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	Ignorovat
A.15.2 Řízení dodávek služeb dodavatelů Cíl: Zachovat dohodnutou úroveň informační bezpečnosti a poskytování služeb v souladu s dodavatelskými smlouvami.		
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	Ignorovat
A.15.2.2	Řízení změn ve službách dodavatelů	Ignorovat
A.16 Řízení incidentů bezpečnosti informací		
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování Cíl: Zajistit konzistentní a efektivní přístup k řízení incidentů informační bezpečnosti, včetně hlášení bezpečnostních událostí a zranitelností.		
A.16.1.1	Odpovědnosti a postupy	**Zavést**
A.16.1.2	Hlášení událostí bezpečnosti informací	**Zavést**
A.16.1.3	Hlášení slabých míst bezpečnosti informací	**Zavést**
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	**Zavést**
A.16.1.5	Reakce na incidenty bezpečnosti informací	**Zavést**
A.16.1.6	Ponaučeni z incidentů bezpečnosti informací	**Zavést**
A.16.1.7	Shromažďování důkazů	**Zavést**
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací		
A.17.1 Kontinuita bezpečnosti informací Cíl: Kontinuita informační bezpečnosti by měla být součástí systémů řízení kontinuity činnosti organizace.		
A.17.1.1	Plánování kontinuity bezpečnosti informací	Ignorovat
A.17.1.2	Implementace kontinuity bezpečnost informací	Ignorovat
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	Ignorovat
A.17.2 Redundance Cíl: Zajistit dostupnost zařízení pro zpracování dat.		
A.17.2.1	Dostupnost vybavení pro zpracování informací	Ignorovat

A.18 Soulad s požadavky		
A.18.1 Soulad s právními a smluvními požadavky Cíl: Zabránit porušení právních, zákonných, normativních nebo smluvních závazků souvisejících s informační bezpečností a veškerými bezpečnostními požadavky.		
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	**Zavést**
A.18.1.2	Ochrana duševního vlastnictví	**Zavést**
A.18.1.3	Ochrana záznamů	**Zavést**
A.18.1.4	Soukromí a ochrana osobních údajů	**Doplnit**
A.18.1.5	Regulace kryptografických opatření	Ignorovat
A.18.2 Přezkoumání bezpečnosti informací Cíl: Zajistit, že informační bezpečnost je zavedena a provozována v souladu s organizačními zásadami a postupy.		
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	**Zavést**
A.18.2.2	Shoda s bezpečnostními politikami a normami	**Zavést**
A.18.2.3	Přezkoumání technické shody	**Zavést**

Přehled opatření byl převzat z přílohy A normy ČSN ISO/IEC 27001:2014. U jednotlivých opatření je uveden jejich současný stav. Jednotlivé varianty mají následující význam:

- **Zavést** – tato opatření nejsou zavedena v žádné formě a je žádoucí je implementovat v plném rozsahu
- **Doplnit** – tato opatření jsou v organizaci zavedena částečně nebo formou plně neodpovídající normě, je potřeba jim věnovat pozornost, provést změny, nebo doplnit
- **Ignorovat** – tato opatření není potřeba zavádět, jelikož nemají souvislost s činností organizace nebo pro ně neexistuje dostatečné odůvodnění (i z hlediska nákladů)

U opatření označených „**Zavést**“ nebo „**Doplnit**“ jsou odpovědné osoby odkázány na odpovídající části zmíněné normy. Pro upřesnění jednotlivých opatření budou dále odkázáni na odpovídající kapitoly normy ČSN ISO/IEC 27002:2014, kapitoly jsou v této normě uvedeny pod odpovídajícím číslem. Toto číslo se shoduje s číselným označením opatření v prvním sloupci přehledu.

Volba konkrétních opatření odpovídá obecnějšímu výběru z předchozí kapitoly a také přesněji pokrývá rizika identifikovaná v průběhu analýzy rizik. Mapování konkrétních opatření do skupin opatření je zřejmé z jejich názvu, popisu a cíle, tak jak jsou v normě.

4.7 Akceptace rizik

Mezi povinné patří dokument s názvem „Akceptace rizik“. Vedení organizace musí na základě návrhů odpovědných osob rozhodnout o schválení nebo zamítnutí akceptovaných rizik. Na základě analýzy rizik se v tomto konkrétním případě bude jednat pravděpodobně o rizika spojená s:

- únikem kódů zabezpečovacího zařízení budovy
- živelnými pohromami
- útoky na interní počítačovou síť zvenčí
- požárem

Jelikož se jedná o rizika, která mají velmi malou hodnotu, která leží pod akceptační úrovní (hodnota rizika do 20), měla by být akceptována a zařazena do skupiny sledovaných rizik, aby nedošlo k jejich podcenění v budoucnosti. Navíc se jedná o rizika, proti kterým má organizace zavedena opatření a není schopna je výrazně více ovlivnit.

4.8 Získání povolení k provozování ISMS v rámci organizace

Jedním z posledních dokumentů, které by měla organizace mít vypracovaný ještě před zahájením implementace ISMS se nazývá „Získání povolení k provozování ISMS v rámci organizace“. Zde by mělo vedení organizace deklarovat svoji vůli k podpoře všech činností ISMS. Tím je myšleno jeho ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování. Jelikož ISMS není jen jednorázovou záležitostí, ale ve skutečnosti donekonečna opakující se sled činností, je důležité, aby vedení tuto skutečnost bralo na zřetel a poskytovalo pro jeho fungování dostatečnou podporu. Dokument musí povinně obsahovat následující kapitoly:

- Zajištění stanovení cílů ISMS a plánu jejich dosažení
- Stanovení role, povinnosti a odpovědnosti v oblasti bezpečnosti informací
- Propagace významu plnění cílů bezpečnosti informací, jejich souladu s politikou bezpečnosti informací, plnění povinností vyplývajících ze zákona a potřebu soustavného zlepšování
- Zajištění dostatečných zdrojů pro ustavení, zavedení, provoz, monitorování, přezkoumání, údržbu a zlepšování ISMS
- Stanovení akceptovatelné úrovně rizika
- Zajištění provádění interních auditů ISMS
- Provádění přezkoumání ISMS

Jelikož vedení organizace si je vědomo aktuální situace a má vůli ji řešit, a také díky podpoře zaměstnanců, kteří mají na starost správu ICT, nepředpokládá se, že by se získáním povolení byly nějaké problémy.

4.9 Prohlášení o aplikovatelosti

Závěrečný dokument, který bude obsahovat prohlášení s popisem jednotlivých opatření a jejich cílů. Tato opatření musí být relevantní a aplikovatelná v rámci ISMS organizace. Povinně obsahuje:

- Jednotlivá bezpečnostní opatření vybraná k implementaci, jejich cíle a důvod jejich výběru
- Jednotlivá bezpečnostní opatření, která jsou již v organizaci zavedena
- Vyřazené cíle opatření a jednotlivá bezpečnostní opatření k jejich naplnění, která jsou uvedena v příloze A normy ČSN ISO/IEC 27001:2014, včetně důvodu jejich vyřazení

Takový dokument poskytuje ucelený pohled na přístup organizace k problematice ISMS. Ilustruje způsob, jakým organizace nakládá se zjištěnými riziky. Navíc podává vysvětlení ohledně vyřazení některých cílů a opatření, a zároveň poskytuje kontrolu, zda nebyly vyřazeny omylem.

4.10 Časová náročnost a plán

Při zavádění a provozu ISMS bude žádoucí mít přehled o časové náročnosti a průběhu jednotlivých etap a činností. Je také potřeba určit pořadí zavádění jednotlivých opatření nebo jejich skupin tak, aby jednotlivé etapy na sebe logicky navazovaly a byly splněny podmínky pro implementaci opatření následujících. Proto byl sestaven přibližný plán, který bude postup prací orientačně ilustrovat a zároveň sloužit jako podklad a podpora v průběhu zavádění a provozu.

4.10.1 Časová náročnost opatření a skupin opatření

Tabulka 12: Časová náročnost činností

Opatření/skupina opatření	Při zavádění	Opakovaně Frekvence
A.5.1 Směřování bezpečnosti informací vedením organizace	12	8 6 měsíců
A.6.1 Interní organizace	8	0
A.6.2 Mobilní zařízení a práce na dálku	1	0
A.7.1 Před vznikem pracovního poměru	1	0
A.7.2 Během pracovního vztahu	50	4 6 měsíců
A.7.3 Ukončení a změna pracovního poměru	1	0
A.8.1 Odpovědnost za aktiva	6	0
A.8.2 Klasifikace informací	6	0
A.8.3 Manipulace s médii	3	0
A.9.1 Požadavky organizace na řízení přístupu	6	0
A.9.2 Řízení přístupu uživatelů	8	2 měsíc
A.9.3 Odpovědnosti uživatelů	3	0
A.9.4 Řízení přístupu k systémům a aplikacím	16	0
A.11.1 Bezpečné oblasti	12	0
A.11.2 Zařízení	20	0
A.12.1 Provozní postupy a odpovědnosti	12	0
A.12.2. Ochrana proti malwaru	12	1 týden

A.12.3 Zálohování	6	1 týden
A.12.4 Zaznamenávání formou logů a monitorování	6	0
A.12.5 Správa provozního softwaru	8	0
A.12.6 Řízení technických zranitelností	6	0
A.13.1 Správa bezpečnosti sítě	6	0
A.13.2 Přenos informací	6	0
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování	30	2 měsíc
A.18.1 Soulad s právními a smluvními požadavky	12	0
A.18.2 Přezkoumání bezpečnosti informací	12	8 6 měsíců
Celkem / Ročně [h]	**269**	**192**

Odhady jsou uvedeny v hodinách

Celkový odhadnutý čas tedy vychází na 269 hodin pro implementační fázi. Při pracovní době jednoho zaměstnance 8 hodin denně resp. 40 hodin týdně vychází etapa zavádění na cca 34 dní resp. 7 pracovních týdnů pro jednoho zaměstnance. Předpokládá se však, že na projektu se bude podílet více osob, na druhou stranu bude projekt realizován po částech a postupně. Ve výsledku je dokončení zaváděcí fáze naplánováno v rámci cca 6 měsíců.

Roční časové nároky na provoz jsou předpokládány na 192 hodin/rok (16 hodin/měsíc, 4 hodiny/týden). Tato časová náročnost se jeví jako přijatelná pro nahrazení části běžné pracovní doby dotčených zaměstnanců. Za účasti na projektu budou zaměstnanci pravděpodobně dodatečně ohodnoceni v rozsahu 200-300 Kč/hod proti běžné mzdě.

4.10.2 Plán zavádění

Jelikož ještě není jasné přesné datum začátku zavádění ISMS a přesné podmínky v době zavádění v organizaci, bude detailní plán teprve zpracován v rámci projektu. Dále je uvedeno pouze pořadí a návaznost jednotlivých úkonů tak, aby bylo možné opatření správně zavést.

Jako první je potřeba provést zpracování povinné dokumentace, ta zahrnuje dokumenty Rozsah a hranice ISMS, Politika ISMS (A.5.1.1), Definice přístupu k hodnocení rizik, Identifikace a ohodnocení aktiv (A.8.1.1, A.8.1.2), Identifikace rizik, Analýza Rizik, Návrh opatření, Cíle opatření a bezpečnostní opatření pro zvládání rizik, Akceptace rizik, Získání povolení k provozování ISMS v rámci organizace a Prohlášení o aplikovatelnosti (A.18.1). Poté je možné zahájit samotnou implementaci zvolených opatření.

Obecná pravidla a směrnice

Implementace by měla probíhat v takovém pořadí, kdy budou zaváděna nejdříve ta opatření, která budou snadno a rychle implementovatelná a taková, která podpoří a usnadní zavádění opatření dalších a složitějších.

V počátku zavádění připadá v úvahu skupina opatření A.6.1 Interní organizace, která by měla ujasnit role a odpovědnosti bezpečnosti informací. Dalšími skupinami a opatřeními, která objasní obecná pravidla ISMS v organizaci, a bude výhodné je zavést v počáteční fázi jsou A.12.1 Provozní postupy a odpovědnosti, A.9.3 Odpovědnosti uživatelů, A.8.1.3 Přístupné používání aktiv a A.8.2 Klasifikace informací. Tato opatření by měla být zpracována hromadně a poté postupně zavedena.

Správa hardwaru a sítě

Aby byly jasně dány podmínky pro aplikaci dalších opatření týkajících se zejména softwaru a řízení přístupu uživatelů ke službám a síti, další fáze by měla být zaměřena na oblast ochrany a správy hardwaru a sítě. Díky tomu nebude nutné některé aspekty zasahující jak do oblasti HW tak i SW řešit dodatečně. Do této skupiny opatření patří zejména A.11.1 Bezpečné oblasti, A.11.2 Zařízení a A.13.1 Správa bezpečnosti sítě.

Správa softwaru, uživatelů a přístupu

Pokud budou správně zavedena opatření z předchozí skupiny, může to výrazně usnadnit implementaci následujících opatření zaměřených na správu a konfiguraci softwaru, správu a řízení přístupu uživatelů a provoz systémů. Patří sem zejména A.12.5 Správa provozního softwaru, A.9.1 Požadavky organizace na řízení přístupu, A.9.2 Řízení přístupu uživatelů, A.9.4 Řízení přístupu k systémům a aplikacím.

Ochrana proti malwaru a zálohování

Díky aplikaci předchozích opatření bude opět snazší implementace následujících opatření spadajících do společné skupiny. Obsahem jsou zejména opatření A.12.2 Ochrana proti malwaru, A.12.3 Zálohování a A.8.3 Manipulace s médii.

Školení a řízení incidentů

Do poslední skupiny opatření, která je žádoucí zavést v počáteční fázi a lze je označit za velmi důležitá, patří ještě ta, která se týkají zvyšování povědomí bezpečnosti informací a řízení incidentů.

Jelikož tyto dvě skupiny budou pravděpodobně časově nejnáročnější, bude vhodné je řešit hned zpočátku a také dlouhodobě. Avšak ve větším měřítku nejlépe až po zavedení opatření předchozích. Zde jsou zahrnuty skupiny A.7.2 Během pracovního vztahu, A.16.1 Řízení incidentů bezpečnosti informací a zlepšování a A.12.6 Řízení technických zranitelností.

Další pravidla

Další opatření, která nejsou pro organizaci stěžejní a nejsou pro ni nikterak kritická, mohou být zaváděna až v pozdějších fázích implementace. Většinou se jedná o doplnění pravidel a směrnic z různých oblastí bezpečnosti informací o normované praktiky. Spadají sem opatření a skupiny A.6.2.1 Politika mobilních zařízení, A.7.1 Před vznikem pracovního poměru, A.7.3 Ukončení a změna pracovního vztahu, A.8.1.4 Navrácení aktiv, A.12.4 Zaznamenávání formou logů a monitorování a A.13.2 Přenos informací.

Periodická opatření (přezkoumávání)

V neposlední řadě jsou zde opatření, která nejsou provozována ve fázi implementace, ale je potřeba na ně myslet v budoucnu. Jedná se o přezkoumávání stavu systému a jeho nastavení, patří sem A.5.1.2 Přezkoumání politik pro bezpečnost informací a A.18.2 Přezkoumání bezpečnosti informací. Tato opatření jsou důležitá pro udržení systému v odpovídajícím a funkčním stavu.

4.11 Finanční zhodnocení

V případě systému řízení informační bezpečnosti se z hlediska nákladů nejedná pouze o finance potřebné k implementaci projektu, ale je třeba počítat s pravidelným vynakládáním prostředků v průběhu provozu a udržování systému. V přehledu budou uvedeny náklady jak na zpracování samotného projektu, tak na pořízení dodatečného vybavení a materiálu, a také na personální zabezpečení projektu.

Jelikož nejsou jasně stanoveny všechny parametry projektu (počet podílejících se zaměstnanců a míra jejich zapojení, přesný počet a specifikace zálohovacích médií, přesná konfigurace serveru apod.) budou uvedeny orientační náklady při předpokládaných parametrech. U prvků které to vyžadují, budou uvedeny i roční náklady.

Konkrétněji se počítá s nákupem serveru a OS pro provoz MS Active Directory, prvků pro správu a ochranu pasivní vrstvy sítě (blokátory, značení), materiálu a zařízení pro zálohování (DVD, HDD, flash), cenou za projekt a personálními náklady na zabezpečení implementace a provozu.

Tabulka 13: Náklady na zavedení a provoz ISMS

	Jednorázové náklady	Roční náklady
Server pro MS Active Directory	25 000,00	-
Licence MS Windows Server 2012 R2 Standard	18 700,00	-
Prvky značení a ochrany síťové infrastruktury	1 000,00	-
Flash disky pro zálohy (30 ks, 16 GB)	6 000,00	-
Externí pevný disk (2 ks, 1 TB)	3 400,00	-
Zálohovací média DVD (300 ks/rok)	-	1 500,00
Projekt	30 000,00	-
Materiál cekem bez DPH	**57 100,00**	**1 500,00**
DPH 21%	**11 991,00**	**315,00**
Materiál celkem s DPH	**69 091,00**	**1 815,00**
Personální náklady	**30 000,00**	**60 000,00**
Celkem	**99 091,00**	**61 815,00**

Uvedené ceny jsou bez DPH

U zálohovacích médií se počítá s přibližnou potřebou 300 ks za rok, personální náklady jsou stanoveny orientačně v rozmezí 200-300 Kč/hod. V úvahu připadá také varianta se síťovým úložištěm NAS (2x 1TB HDD) v ceně 10 000-15 000 Kč namísto externích HDD.

4.12 Přínosy zavedení ISMS pro organizaci

Zavedením vybraných opatření získá organizace lepší přehled nad svými aktivy informační bezpečnosti. Bude moci lépe řídit uživatele a jejich chování, které ovlivňuje důležité a citlivé informace. Další výhodou jsou jasná pravidla pro zacházení s informačními aktivy, kontrola jejich dodržování a případná možnost postihu v opačném případě. Asi nejdůležitějším aspektem je však samotný fakt, že bude zlepšen stav informační bezpečnosti v organizaci a povědomí zaměstnanců o ní. To může napomoct lepšímu rozvoji některých aktivit organizace, stejně jako lepším vztahům s ostatními organizacemi a novým možnostem v této oblasti. Díky předpokládanému snížení incidentů informační bezpečnosti a nutnosti je řešit, se předpokládá i snížení některých nákladů s tím spojených.

ZÁVĚR

Tato práce měla za cíl navrhnout vhodnou metodiku pro implementaci systému řízení bezpečnosti informací v konkrétní organizaci. Na základě analýzy prostřední a současného stavu informační bezpečnosti byly zjištěny nedostatky, na které byla zaměřena pozornost při dalším zkoumání problému. Praktická část již pomohla identifikovat aktiva informační bezpečnosti, která mají pro organizaci největší cenu. Dále byla provedena analýza hrozeb, zranitelností aktiv a konečně vypočteny míry rizik informační bezpečnosti.

Jako nejdůležitější a nejcennější aktiva informační bezpečnosti byly označeny databáze sbírek, osobní dokumenty a údaje zaměstnanců, účetní data a jejich zálohy. To ostatně není překvapením, jelikož zpracování sbírkových dat a vlastních prací zaměstnanců je hlavní a stěžejní aktivitou v organizaci. Ztráta či porušení integrity nebo dostupnosti sbírkových databází by znamenala nemožnost orientace ve sbírkových předmětech, kterých se v depozitářích muzea vyskytují tisíce. Tuto skutečnost by bylo možné dočasně řešit použitím původních inventárních karet, ovšem bylo by to značně neefektivní a složité z důvodu jejich rozmístění a stavu uspořádání. Pokud se jedná o práce zaměstnanců v digitální podobě, zde by při ztrátě nebo porušení integrity mohl nastat problém s průkazností jejich pracovní aktivity. Žádný zaměstnanec si nepřeje být nařknut z neaktivity v pracovní době v případě, že o svá data přijde. V případě účetních dat by mohl nastat problém, pokud by některé údaje chyběly, nebo nebyly kompletní. Tato problematika je o to zásadnější, protože se jedná o příspěvkovou organizaci, která podléhá častějším kontrolám hospodaření.

V případě hrozeb bylo zjištěno, že největším problémem je lidský faktor. Zaměstnanci nemají příliš povědomí o pojmu informační bezpečnosti a v organizaci nejsou využívány nástroje k tomu, aby se tento stav zlepšil. S tím souvisí i nevědomost zaměstnanců jak řešit incidenty informační bezpečnosti. V důsledku toho dochází k častým problémům s integritou dat, funkcí zařízení a řešením dalších následných chyb. Částečně s lidským faktorem i daty souvisí problematika zálohování. Bylo zjištěno, že tato oblast, ač je velmi důležitá, nemá v organizaci stanovená žádná závazná pravidla. Mezery byly nalezeny také v ochraně proti malwaru, tedy škodlivým kódům, které již nesčetněkrát vedly k nedostupnosti důležitých informací a nemožnosti pokračovat

v důležitých činnostech. Mezi hrozby s nižší pravděpodobností a dopadem pak patří neexistence politiky hesel, nedostatky v ochraně fyzického přístupu a neexistence pravidel týkajících se manipulaci s hardwarem, prvky síťové infrastruktury, pravidel pro ochranu zařízení před vlivy okolí a také omezení konfigurace softwaru včetně operačních systémů na uživatelských stanicích.

K odstranění největších nedostatků byla navržena odpovídající opatření. Ta byla navíc doplněna o odkazy do norem, což ještě zvyšuje jejich váhu a šanci na úspěšnou a efektivní implementaci. Byla vznesena doporučení na vytvoření povinné dokumentace ISMS, která dá vedení organizace i zaměstnancům lepší představu a přehled o důležitých dotčených oblastech. Navíc díky ní bude pro vedení organizace snazší prosazování zvolených politik, pravidel a směrnic. Opatření byla zvolena tak, aby pokryla největší rizika informační bezpečnosti v organizaci a rozdělena do skupin, aby jejich zavádění bylo logicky provázáno a bylo snazší. První skupinou opatření je návrh interních směrnic a stanovení pravidel, která umožní lépe definovat další cíle informační bezpečnosti. Zaměstnanci budou nyní povinni dodržovat zásady informační bezpečnosti a za jejich nedodržování budou moct být káráni. Byla navrhnuta doporučení na zavedení vzdělávacího systému zaměstnanců, včetně ověřování jejich vědomostí. Dále byla zpracována metodika a plán zálohování, doporučení pro řízení přístupu uživatelů, politika hesel, pravidla pro bezpečnost zařízení a sítě, doporučení pro fyzický přístup, ochranu proti malwaru a správu konfigurace softwaru. V neposlední řadě bylo důležité podat doporučení ohledně zavedení incident managementu.

Důležité je, že vedení organizace projevilo svou vůli a deklarovalo podporu pro zavedení ISMS. Bylo seznámeno s hlavními úskalími i důležitostí neustálého rozvíjení a zlepšování systému řízení bezpečnosti informací. Rovněž náklady, které v orientačním návrhu dosahují hodnoty 99 091 Kč na zavedení ISMS a roční náklady 61 815 Kč shledalo vedení jako opodstatněné a přijatelné. Časová náročnost pro vedení nehraje příliš velkou roli, ovšem orientační časové nároky na zavedení v hodnotě 269 hodin rozprostřených do 6 měsíců a roční zatížení 192 hodin se jeví rovněž jako přijatelné

V každém případě by zavedení opatření a provoz ISMS měl organizaci přinést zvýšení bezpečnosti důležitých informací a eliminaci případných nákladů na řešení bezpečnostních incidentů.

SEZNAM POUŽITÉ LITERATURY

1) POŽÁR, J. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.
2) SEDLÁK, P. *Management informační bezpečnosti.* Přednáška. Brno: VUT, Fakutla podnikatelská, akdemický rok 2014/2015.
3) ONDRÁK V., SEDLÁK P., MAZÁKEK V. *Problematika ISMS v manažerské informatice.* Brno: CERM, 2014. ISBN 978-80-7204-784-0.
4) Demingův cyklus PDCA. *SystemOnLine* [Online]. ©2001-2016 [cit. 2016-04-18]. Dostupné z: http://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm
5) SEKERKA,V. *Vaše jistota na trhu IT www.i.cz ISMS VE STÁTNÍ SPRÁVĚ A SAMOSPRÁVĚ.* Přednáška. Hradec Králové, 2008.
6) DRASTICH, M. *Systém managementu bezpečnosti informací.* Praha: Grada Publishing, 2011. ISBN 978-80-247-4251-9.
7) DOUCEK P., NOVÁK L., NEDOMOVÁ L., SVATÁ V. *Řízení bezpečnosti informací: 2. rozšířené vydání.* Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
8) Díl 7 - www.chrantesidata.cz. *GiTy - bezpečnost v kostce* [Online]. ©2015 [cit. 2016-04-20]. Dostupné z: http://www.chrantesidata.cz/cs/art/1154-dil-7/
9) Co je to ITIL®? | bestpractice.cz. *BESTPRACTICE:CZ* [Online]. ©2008-2016 [cit. 2016-04-23]. Dostupné z: https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/Co-je-to-ITIL-.alej
10) 1COBIT tajemství zbavený - CleverAndSmart. *Clever And Smart* [Online]. ©2008-2016 [cit. 2016-04-24]. Dostupné z: http://www.cleverandsmart.cz/cobit-tajemstvi-zbaveny/
11) Metodika CRAMM (CCTA Risk Analysis and Management Method) - ManagementMania.com. *MANAGEMENT MANIA* [Online]. ©2011-2013 [cit. 2016-04-18]. Dostupné z: https://managementmania.com/cs/metodika-cramm-ccta-risk-analysis-and-management-method.
12) Změny a dopady nové normy ISO/IEC 27001:2013. *SystemOnLine* [Online]. ©2001-2016 [cit. 2016-04-26]. Dostupné z: http://www.systemonline.cz/it-security/zmeny-a-dopady-nove-normy-iso-iec-27001-2013.htm

13) ČESKÝ NORMALIZAČNÍ INSTITUT ČSN ISO 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Český normalizační institut, 2014. 28 s. Třídící znak: 369797
14) POŽÁR, J. *Základy teorie informační bezpečnosti.* Praha: Vydavetelství PA ČR, 2007. ISBN 978-80-7251-250-8.
15) DOBDA, L. *Ochrana dat v informačních systémech.* Praha: Grada Publishing, 1998. ISBN 80-716-9479-7.
16) ČESKÝ NORMALIZAČNÍ INSTITUT ČSN ISO 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Český normalizační institut, 2014. 76 s. Třídící znak: 369798.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

AAA	**Authentication Authorization Accounting** – Protokol pro autentizaci, autorizaci a účtování uživatelů
AD	**Active Directory** – Adresářová služba
BOYD	**Bring Your Own Device** – Používání osobního zařízení zaměstnanců ve firmách
CD	**Compact Disc** – Kompaktní disk pro ukládání dat
CRAMM	**CCTA Risk Analysis and Management Method** – Metodika pro analýzu rizik IS
COBIT	**Control Objectives for Information and related Technology** – Rámec pro správu a řízení informatiky
ČSN	**Česká technická norma**
DVD	**Digital Versatile Disc** – Digitální disk pro ukládání dat
HDD	**Hard Drive Disc** – Pevný disk pro ukládání dat
HW	**Hardware** – Technické vybavení počítače
ICT	**Information and Communication Technologies** – Informační a komunikační technologie
IDS	**Intrusion Detection Systém** – Systém detekce průniků
IEC	**International Electrotechnical Commission** – Mezinárodní elektrotechnická komise
IPS	**Intrusion Prevention Systém** – Systém prevence průniků
IS	**Information System** – Informační systém
ISMS	**Information Security Management Systém** – Systém řízení bezpečnosti informací
ISO	**International Organisation for Standardization** – Mezinárodní organizace pro normalizaci
IT	**Information Technology** – Informační technologie
ITIL	**Information Technology Infrastructure Library** – Knihovna nejlepších oborových praktik
NAC	**Network Access Control** – Řízení přístupu k síti
OS	**Operating Systém** – Operační systém
PDCA	**Plan Do Check Act** – Plánuj, dělej, ověř, jednej
SW	**Software** – Programové vybavení počítače
VPN	**Virtual Private Network** – Virtuální privátní síť

SEZNAM PŘÍLOH

Práce neobsahuje žádné přílohy.