
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# NÁVRH NA ZAVEDENÍ NUTNÝCH OBLASTÍ ISMS NA ZÁKLADNÍ ŠKOLE

THE PROPOSAL FOR IMPLEMENTATION OF ESSENTIAL ISMS SECTIONS AT THE PRIMARY SCHOOL

**DIPLOMOVÁ PRÁCE**
MASTER'S THESIS


**AUTOR PRÁCE** — **Bc. Tomáš Kryštof**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Petr Sedlák**
SUPERVISOR


**BRNO 2016**

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

# ZADÁNÍ DIPLOMOVÉ PRÁCE

**Kryštof Tomáš, 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 na zavedení nutných oblastí ISMS na základní škole**

v anglickém jazyce:

**The Proposal for Implementation of Essential ISMS Sections at the Primary School**

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Závěr
Seznam použité literatury

Seznam odborné literatury:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.
ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.
DOUCEK P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Vedoucí diplomové práce: Ing. Petr Sedlák

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

L.S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>Ředitel ústavu | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>Děkan fakulty |

V Brně, dne 29.2.2016

## Abstrakt

Tato diplomová práce se zabývá problematikou informační bezpečnosti na konkrétní základní škole. V první a druhé části práce je snahou autora poskytnout čtenáři základní teoretická východiska o problematice ISMS a získat přehled o stávajícím stavu informační bezpečnosti na vybrané základní škole. V praktické části pak budou navržena vhodná bezpečnostní opatření a doporučení pro řešení nejzávažnějších problémů z pohledu managementu bezpečnosti ICT.



## Abstract

This master thesis is concerned with the information security on a specific primary school. In the first and second part of this thesis there is an endeavor to provide basic theoretical starting points about ISMS issues, and to get an overview about the current state of the information security at the primary school. This is followed by the practical part where there is the proposal of suitable security steps and recommendation for solution of the most important tasks from the ICT management security perspective.



## Klíčová slova

Systém řízení informační bezpečnosti, ISMS, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, aktivum, řízení rizik

## Key words

Information Security Management System, ISMS, ISO/IEC 27001, ISO/IEC 27002, Asset, Risk Management

## Bibliografická citace práce

KRYŠTOF, T. *Návrh na zavedení nutných oblastí ISMS na základní škole.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 88 s. Vedoucí diplomové práce Ing. Petr Sedlák

## Čestné prohlášení

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

V Brně dne 26. května 2016 ……

Podpis

## Poděkování

Touto cestou bych rád poděkoval vedoucímu diplomové práce panu Ing. Petru Sedlákovi za poskytnutí cenných rad a připomínek. Dále bych chtěl poděkovat vedení základní školy, která mi poskytla důležité informace pro realizaci této diplomové práce.

# OBSAH

# ÚVOD

V době rychlého rozvoje informačních technologií začíná být počítačová bezpečnost jednou z priorit celého IT oboru. Význam informační techniky roste nezadržitelným tempem a s ním se zvyšuje také možnost využívání informačních a komunikačních technologií ve všech oblastech života dnešní společnosti. Těžko bychom hledali odvětví nebo společnost, do kterých informační technologie nepronikly. Informace, procesy nebo služby se pro každou firmu staly životně důležitým nástrojem. Správné informace vedou ke správnému rozhodování a tím i k úspěšnému splnění cílů. Lidé sbírají, spravují a vyhodnocují čím dál více dat, informací a zpráv než kdykoliv předtím a je více než jisté, že tento trend bude i nadále pokračovat.

Stejně jako téměř vše, má i tento pokrok v oblasti výpočetní techniky přinášející zvýšení pohodlí uživatelů i svou stinnou stránku, kterou je riziko napadení či zneužití dat. S tímto pokrokem tak přichází i nutnost ochrany dat a informací před poruchami, živelnými katastrofami, kriminalitou, vandalismem, neoprávněným přístupem a vůbec celkově zneužitím citlivých informací, kterých mají individuální uživatelé i firmy mnoho.

Je důležité si uvědomit, že každá organizace bez ohledu na typ či velikost vlastní mnoho citlivých dat, které si zaslouží přiměřenou ochranu. V posledních letech navíc výrazně stoupl počet kybernetických útoků. Čím dál častěji se objevují informace o napadených sítích či odcizených datech. Cílené útoky jsou prováděny profesionálně organizovanými skupinami, které již dnes mají své vlastní průmyslové odvětví.

Firemní data jsou to nejcennější, co organizace vlastní a jejich poškození, krádež nebo jakékoliv znehodnocení by mohlo mít zcela fatální vliv na budoucí existenci organizace. Většina z nás tráví na Internetu podstatnou část pracovní doby či svého volného času. Internet nám umožňuje přístup k velkému množství užitečných informací. Bohužel si velice málo lidí uvědomuje, jak nebezpečným prostředím Internet je. Stal se součástí našeho každodenního života, který už navíc navštěvujeme i z dalších zařízení, jako jsou chytré mobilní telefony, tablety apod. Málokdo si uvědomuje, kolik osobních dat a dalších stop po sobě zanecháváme. Protože valná většina populace má minimální znalosti o nebezpečí na síti, je Internet jedním z největších rizik dnešní doby.

Do problematiky bezpečnosti informací spadá i otázka fyzického zabezpečení. Stačí připomenout nešťastnou událost, která se stala v polovině roku 2014 ve Žďáru nad

Sázavou, kde byly během útoku mladé ženy pobodány dvě dívky a jeden chlapec usmrcen. Podobný útok v České republice nemá obdoby a dočasně vyvolal velkou diskuzi ohledně bezpečnosti ve školách. Dle mého však toto téma velmi rychle utichlo a většina škol nepřijala téměř žádná nebo minimum bezpečnostních opatření, směřujících především k zajištění fyzické bezpečnosti žáků, která by mohla podobnému útoku předejít nebo alespoň snížit jeho dopad. Přitom ochrana zdraví dětí, žáků a v neposlední řadě i aktiv, a tím pádem i citlivých dat a majetku, by měla být prioritou každého zřizovatele.

Cílem informační bezpečnosti je dosáhnout přijatelného řešení bezpečnosti informací. Způsobů, jak takového přijatelného řešení dosáhnout je několik, například stanovení organizačních, personálních, softwarových, hardwarových a dalších opatření, pravidel a postupů, které pomohou eliminovat případné ztráty. Samotné stanovení však samozřejmě nestačí. Nejdůležitější je zavedení tohoto řešení do praxe tak, že se jím budou bez výjimky řídit všichni zaměstnanci firmy. Právě systém managementu bezpečnosti informací neboli ISMS, kterým se zabývám v této diplomové práci, slouží k nalezení funkčního řešení splňujícího maximální možné bezpečí pro citlivá data.

# CÍLE PRÁCE

Cílem této diplomové práce je odhalit největší slabiny v oblasti bezpečnosti na dané základní škole a následně vybrat a navrhnout vhodná opatření, která by měla vést ke zvýšení bezpečnosti a bezpečnostního povědomí v oblasti ICT.

Nejprve bude posouzen současný stav informační bezpečnosti a poté provedena analýza rizik, která pomůže identifikovat kritické oblasti, jejichž ignorace by mohla mít velké negativní dopady na bezpečný chod školy. Pro analýzu rizik a návrhy bezpečnostních opatření poslouží jako vodítko normy ISO/IEC řady 27000.

V praktické části práce je pak mým cílem provést ekonomické zhodnocení nákladů na zavedení vybraných bezpečnostních opatření.

Důležitá data a informace pro práci mi byla poskytnuta přímo vedením školy a pověřeným pracovníkem, čerpal jsem také z jiných veřejně dostupných zdrojů.

# 1 TEORETICKÁ VÝCHODISKA PRÁCE

Tato kapitola zprostředkovává teoretická východiska, která budou následně využita v následujících částech této práce, a zároveň navozuje čtenáři jisté povědomí o problematice systému řízení informační bezpečnosti.

## 1.1 Důležité pojmy

Na úvod uvádím několik základních pojmů, které jsou důležité pro pochopení dané problematiky.

**Aktivum**

Vše, co má pro vlastníka aktiva nějakou hodnotu, která může být vlivem hrozby zničena či poškozena (1).

**Informace**

Informace představuje aktivum, které je podobně jako další důležitá aktiva organizace podstatné pro organizaci a vyžaduje odpovídající ochranu. Existuje mnoho způsobu uchování informací, a to **digitální** (například datové soubory uložené na elektronických nebo optických médiích), **materiální** (zapsané na papíře), nebo jako nevyjádřená informace v podobě **znalostí** pracovníků. Stejně tak existuje několik způsobů jejich přenášení jako například kurýrem, verbální nebo elektronickou komunikací. Ať už jsou jakékoliv informace přenášeny jakkoliv, **vyžadují vždy přiměřenou ochranu.** V informatice jsou informace tvořeny kódovanými daty, myšleno ve smyslu fyzikální interpretace v úložném zařízení nebo na přenosovém médiu (2).

**Data**

Data jsou **údaje**, mající nějakou **vypovídající hodnotu**, které jsou zachyceny optimálním způsobem a jsou srozumitelné pro příjemce, kým může být stroj nebo člověk. Jedná se o opakovaně interpretovatelnou a formalizovanou podobu informace, která je vhodná pro komunikaci, vyhodnocování nebo zpracování (3).

**Informační systém**

Vzhledem k rozmanitosti terminologie neexistuje přesná definice. Informačním systémem však můžeme rozumět **systém vzájemně propojených informací a procesů**, které s těmito informacemi pracují (3).

**Informační technologie**

Je množina **nástrojů, postupů a technologií**, které uživatelům umožňují nakládat s daty (3).

**Informační a komunikační technologie**

Ve chvíli, kdy zařízení začala **komunikovat** mezi sebou, byla zkratka IT rozšířena o písmeno C, znamenající „Communication“. Došlo tak k rozšíření původního konceptu informačních technologií o prvek komunikace a vznikla tak zkratka ICT, která zahrnuje veškeré HW i SW prostředky, které spolu s daty tvoří aktiva organizace (4).

**Dostupnost**

Je zajištěn přístup k informacím oprávněnému uživateli v požadovaný okamžik (3).

**Důvěrnost**

Je zajištěno, že k informacím mají přístup pouze oprávnění uživatelé (3).

**Integrita**

Je zajištěno, že informace nemohou být modifikovány nebo poškozeny neautorizovaným způsobem (3).

**Hrozba**

Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může zapříčinit škodu (5).

**Dopad hrozby**

Škoda, kterou způsobí hrozba při jednom působení na určité aktivum je nazývána dopad hrozby (5).

**Riziko**

Nebezpečí, že jedna či více hrozeb využije zranitelnost aktiva a zapříčiní jeho ztrátu či zničení. Dá se chápat jako možnost odlišného a především nežádoucího vývoje od předpokládaného (1).

**Zranitelnost**

Nedostatek nebo slabé místo aktiva, které může být využito hrozbou. Slabá místa mohou být zneužita k neautorizovanému přístupu k informačním zdrojům (3, 4).

**Opatření**

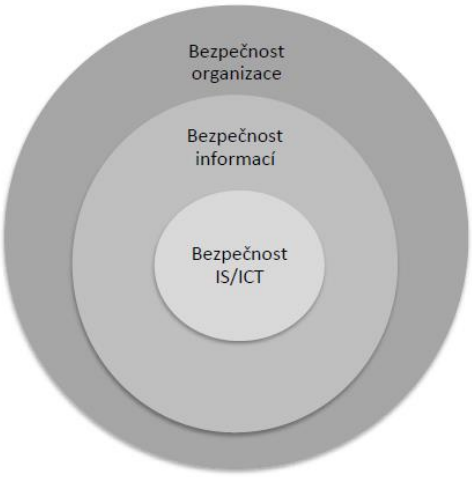
Postup, proces, procedura, technický prostředek nebo cokoliv, co lze využít pro z**mírnění** působení **hrozby**, snížení **zranitelnosti** nebo **dopadu hrozby** (5).

**Informační bezpečnost**

Lidstvo dnešní doby je na **informacích závislé** a většina informací je uchovávána v elektronické podobě. Nezadržitelný **vývoj** nových technologií a jejich neustále se rozšiřující využití v osobním i profesním životě přispívá k pohodlí a pokroku. Zároveň však přináší i **nová bezpečnostní rizika**, která ještě donedávna vůbec neexistovala nebo jím nebylo nutné věnovat **zvýšenou pozornost** (6).

Informační bezpečnost se zabývá ochranou informací a zahrnuje tři hlavní aspekty, kterými jsou **důvěrnost, dostupnost a integrita**. Jinými slovy má za úkol zajistit, aby správné a úplné informace měl včas k dispozici ten, kdo je opravdu potřebuje a pouze ten, kdo je k přístupu k nim oprávněn. Zahrnuje informace ve všech podobách, včetně té papírové i ústní. Stejně tak zahrnuje i nakládání s nimi, jejich zpracování, archivaci, rušení atd. (3).

Bezpečnost informací je ve vzájemném vztahu s pojmy bezpečnost organizace a bezpečnost IS/ICT. Bezpečnost organizace má za úkol **zajistit bezpečnost objektu** a tím pádem také **majetek** organizace. Je nadřazena bezpečnosti informací a bezpečnosti IS/ICT, které má na starost ochranu aktiv informačního systému podporovaná informačními a komunikačními technologiemi (3).




**Obrázek č. 1: Vztah úrovní bezpečnosti v organizaci**

Zdroj: (4, s. 56)

## 1.2 ISMS

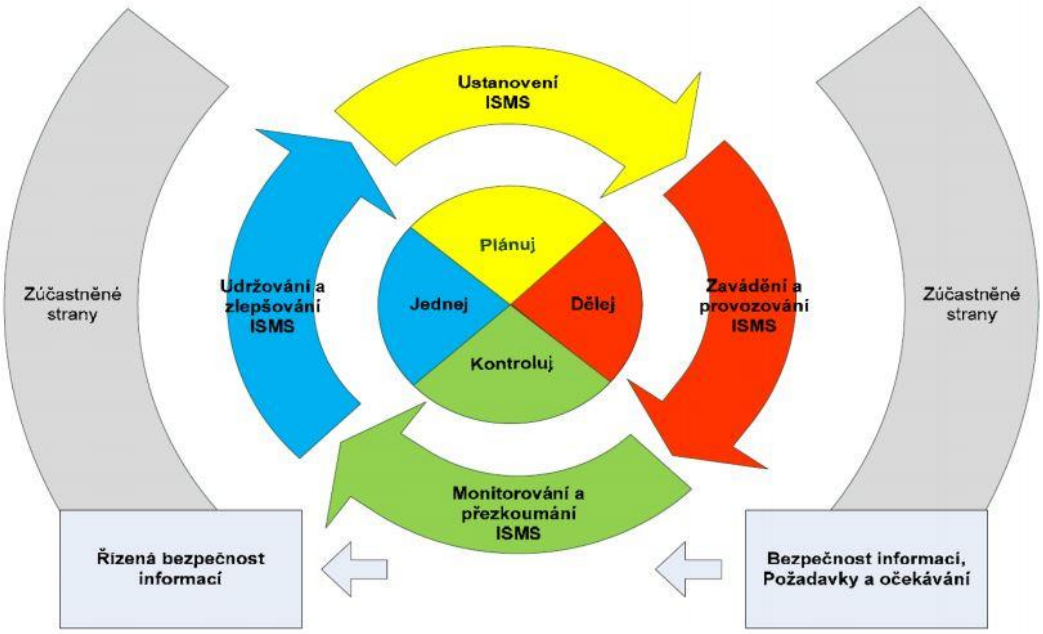
Pojmu ISMS neboli Systému řízení bezpečnosti informací se budu věnovat podrobněji. Jedná se o část celkového systému organizace, jehož cílem je eliminovat slabiny a možnou ztrátu nebo poškození aktiv. Nabízí systematický, profesní a efektivní přístup k řízení informační bezpečnosti. Celý systém je založen na využití modelu **PDCA.** Název modelu je tvořen počátečními písmeny slov Plan – Do – Check – Act (2).

### 1.2.1 Model PDCA

Autorem modelu PDCA je americký statistik W. Edwarwds Deming. Demingův cyklus, jak je někdy model nazýván, je metoda **postupného zlepšování** například kvality služeb, výrobků, procesů, aplikací a dat. Jde o cyklus změn, jehož 4 etapy jsou prováděny **neustále dokola** a dochází tak k neustálému zlepšování. Využití modelu pro ISMS a jednotlivé etapy celého životního cyklu ISMS jsou na obrázku č. 2.

- **Ustavení ISMS** má za cíl určit rozsah, hranice a odpovědnosti bezpečnostního řízení.
- **Zavedení a provoz ISMS** má za cíl prosadit vybraná bezpečnostní opatření do chodu organizace.
- **Monitorování a přezkoumání ISMS** má za cíl zajistit zpětnou vazbu a pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací.
- **Údržba a zlepšování ISMS** je realizace možností zlepšování systému řízení bezpečnosti informací. Jednak soustavné zlepšování systému, ale také odstraňování odhalených slabin a nedostatků (2).

Obsah jednotlivých etap ISMS vychází z norem ISO/IEC 27001 a ISO/IEC 27002 a bude podrobně rozebrán v kapitolách 1.5 – 1.8.

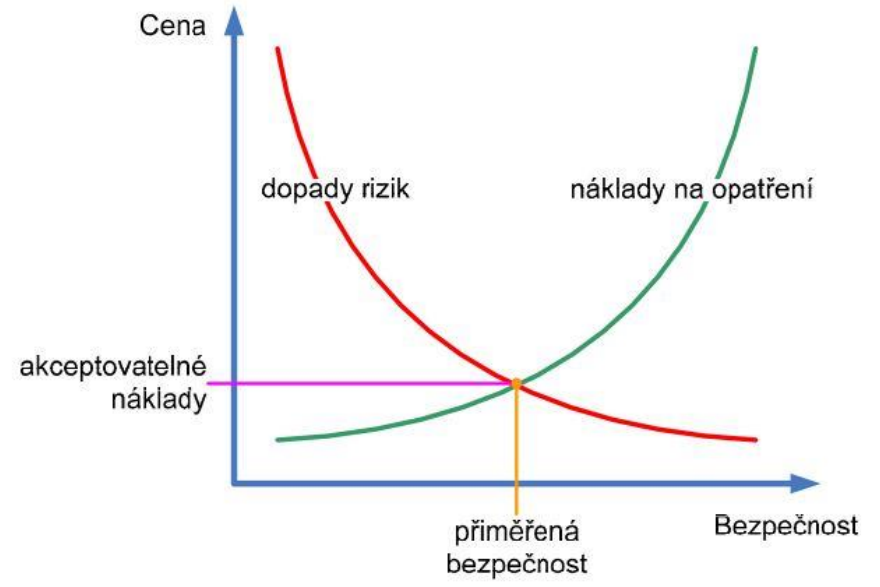



**Obrázek č. 2: Model PDCA v ISMS neboli životní cyklus ISMS**

Zdroj: (3, s. 25)

### Přiměřená bezpečnost

Protože finanční a lidské zdroje bývají často omezeny, je třeba, aby firma vynaložila takové úsilí a investice do bezpečnosti, které odpovídají hodnotě aktiv a míře možných rizik (3).




**Obrázek č. 3: Přiměřená bezpečnost za akceptovatelné náklady**

Zdroj: (3, s. 36)

## 1.3 Proč je dobré zavést ISMS?

Vůbec prvním a zároveň krokem **nutným a postačujícím** v zavádění a provozu ISMS je získání **souhlasu vedení společnosti** s nasazením systému. Tento souhlas je vyžadován normou a vedení se tímto dokumentem **zavazuje, že bude zavádění ISMS podporovat**. V této podkapitole bych proto rád uved několik přínosů a hlavních důvodů, proč by organizace měly o ISMS uvažovat bez ohledu na jejich velikost a typ, případně si systém řízení informací nechat certifikovat dle standardu ČSN/ISO 27001 (podmínkou používání certifikace není).

- Bezpečnost je sladěna se strategií a cíli organizace.
- Systémové řešení bezpečnosti.
- Stanovuje jasná bezpečnostní pravidla a postupy pro zaměstnance a dodavatele.
- Chrání aktiva.
- Řídí a eliminuje rizika.
- Zvyšuje důvěryhodnost a postavení v očích zákazníků.
- Úspora nákladů v souvislosti s řešením následků bezpečnostních incidentů (7).

## 1.4 Řada norem ISMS

Řada norem ISMS má pomoci organizacím bez ohledu na typ a velikost zavést a provozovat ISMS. Tato řada obsahuje několik mezinárodních norem, které mají společný název Informační technologie – Bezpečnostní techniky (2).

Předtím, než představím **nejdůležitější** normy zabývající se problematikou ISMS, bych rád uvedl několik **souvisejících důležitých pojmů**.

**Standard**

Standard je dokumentovaná úmluva, která obsahuje technické specifikace nebo jiná přesně stanovená kritéria důsledně používaná jako pravidla - směrnice. Může sloužit jako definice charakteristických vlastností zabezpečující, že výsledkem výroby, procesu, služby apod. je přesně to, co se očekávalo (3).

**Norma**

Naproti tomu norma je **doporučení** pro daný standard nebo řešení. V oblasti ICT mluvíme o normě jako o doporučení použitelných standardů k realizaci požadovaného kompatibilního řešení (3).

**ČSN**

ČSN neboli Česká státní norma vzniká dvěma způsoby. Prvním způsobem je přejímání evropských a mezinárodních norem do soustavy českých technických norem formou ČSN EN (ČSN ISO, ČSN IEC atd.). Druhým způsobem je pak tvorba původních ČSN, které vyplývají z národních potřeb a z hlediska zachování funkčnosti fondu ČSN (3).

**ISO**

Mezinárodní organizace pro standardizaci, jejímž posláním je podporování rozvoje standardizačních a s tím spojených aktivit ve světě se zaměřením na usnadnění mezinárodních směn zboží a služeb a na spolupráci ve sféře intelektuálních, vědeckých, technologických a ekonomických aktivit (3).

**IEC**

Mezinárodní elektrotechnická komise je celosvětovou organizací, která připravuje normy z oblasti elektrotechnické a oblastí elektronických norem včetně oblastí příbuzných (3).

**Přehled nejdůležitějších norem, které se zabývají problematikou ISMS:**

- **ISO/IEC 27 000** Systémy řízení bezpečnosti informací – Popisuje přehled a slovník systémů řízení bezpečnosti informací (2).
- **ISO/IEC 27001** Systémy řízení bezpečnosti informací – Požadavky – specifikuje požadavky na ustavení, provoz, údržbu a zlepšování systému managementu bezpečnosti informací. Obsahuje přílohu A, ve které jsou stanoveny jednotlivá opatření a jejich cíle (2).
- **ISO/IEC 27002** Soubor postupů pro opatření bezpečnosti informací – ve 14 kapitolách poskytuje specifická implementační doporučení a návod na použití doporučených postupů, podporujících opatření, která jsou uvedená v kapitolách A.5 až A.18 normy ISO/IEC 27001 (2).
- **ISO/IEC 27003** Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací – tato norma obsahuje návod pro návrh a implementaci ISMS systému řízení bezpečnosti informací v souladu s požadavky normy ISO/IEC 27001 (2).
- **ISO/IEC 27004** Bezpečnostní techniky – řízení bezpečnosti informací – Měření – Norma, poskytující doporučení pro vývoj a používání metrik a pro měření účinnosti zavedeného ISMS. Umožňuje tak posoudit efektivnost ISMS, cílů opatření a opatření

použitých k implementaci a řízení informační bezpečnosti na základě specifikace v normě ISO/IEC 27001 (2).

- **ISO/IEC 27005** Bezpečnostní techniky – Řízení rizik bezpečnosti informací – norma poskytující směrnice pro řízení rizik bezpečnosti informací. Popisuje přístup k řízení rizik v souladu s obecným pojetím specifikovaným v normě ISO/IE 270001 (2).
- **ISO/IEC 27006** Bezpečnostní techniky – Požadavky na orgány poskytující audit a certifikaci systému řízení bezpečnosti informací – Uvádí požadavky, na základě kterých jsou akreditovány certifikační organizace (2).
- **ISO/IEC 27007** – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací – poskytuje návod na provádění auditů ISMS (2).
- **ISO/IEC 27008** – Bezpečnostní techniky – Směrnice pro audit opatření ISMS – technická zpráva, poskytující návod na přezkoumávání opatření bezpečnosti informací (2).
- **ISO/IEC 27014** – Bezpečnostní techniky – Správa bezpečnosti informací – norma poskytující návod týkající se principů a procesů pro správu informační bezpečnosti, pomocí kterých může organizace hodnotit, usměrňovat a monitorovat řízení informační bezpečnosti (2).

## 1.5 Etapa č. 1 – Ustavení ISMS

Ustavení je první etapou budování ISMS, která upřesňuje správné formy řešení bezpečnosti informací. V této etapě je definován rozsah ISMS a především je nutné získat od vedení společnosti souhlas s nasazením systému. Etapa ustavení má zásadní dopad na fungování v průběhu celého životního cyklu (4).

Tuto etapu lze rozdělit na následující skupiny činností:

- Definice kontextu organizace.
- Demonstrování vůdčí role, stanovení odpovědností a politiky bezpečnosti informací.
- Stanovení přístupu organizace k hodnocení rizik.
    - Stanovení kontextu pro řízení rizik.
    - Posouzení rizik bezpečnosti informací.
    - Ošetření rizik bezpečnosti informací.
    - Akceptace rizik bezpečnosti informací.
    - Komunikace a konzultace rizik bezpečnosti informací.

    - Monitorování a přezkoumávání rizik bezpečnosti informací.
- Zajištění podpory organizace.
- Příprava Prohlášení o aplikovatelnosti (7).

### 1.5.1 Kontext organizace

Organizace musí určit **aspekty**, které ovlivňují dosažení výstupů ISMS, porozumět **potřebám** a očekáváním zainteresovaných stran, stanovit **rozsah** systému řízení bezpečnosti informací (7).

### 1.5.2 Vůdčí role

Vedení organizace musí s ohledem na ISMS demonstrovat **vůdčí roli**, vyjádřit **podporu a závazek ISMS**. Dále by mělo stanovit **politiku bezpečnosti informací** a cílů bezpečnosti informací v souladu se strategickým směřováním organizace. Stejně tak musí zajistit přidělení **odpovědnosti a pravomocí** pro role relevantní bezpečnosti informací (7).

### 1.5.3 Plánování – Proces řízení rizik

Tomuto procesu se budu podrobně věnovat v podkapitole 1.9 s názvem Proces řízení rizik.

### 1.5.4 Podpora

Organizace musí definovat a zajistit **zdroje** nutné pro ustavení, implementování, udržování a neustálé zlepšování ISMS. Dále musí zajistit, že odpovědné osoby jsou **kompetentní** a mají dostatečnou **kvalifikaci** pro vykonání dané práce. Všechny osoby pracující pro organizaci musí být **vědomy** politiky bezpečnosti informací, své role a případných důsledků nepřizpůsobení se požadavkům ISMS. Organizace musí zajistit **komunikaci**, která zahrnuje – o čem, kdy, s kým, kdo, procesy atd. Dle normy ISO/IEC 27001 je organizace povinna udržovat **dokumentované informace** dle definovaných pravidel, uvedených v normě (7).

### 1.5.5 Prohlášení o aplikovatelnosti

V praxi nejdůležitější dokument, ve kterém jsou popsány **cíle opatření a jednotlivá bezpečnostní opatření**, která byla vybrána na pokrytí bezpečnostních rizik (4).

## 1.6 Etapa č. 2 – Zavádění a provoz ISMS

V této, v pořadí druhé etapě ISMS, je cílem **prosadit všechna bezpečnostní opatření**, která byla navržena v první etapě při ustanovení ISMS. Je důležité připravit dílčí plány, ve kterých jsou definovány přesné termíny, odpovědné osoby apod. Všechna bezpečnostní opatření by měla být součástí dokumentu tzv. **Příručky bezpečnosti informací.** Během této etapy by také měly být vysvětleny bezpečnostní principy všem manažerům a uživatelům organizace.

Nezbytné činnosti etapy zavádění ISMS:

- Tvorba plánu zvládání rizik a začátek jeho zavádění.
- Zavedení plánovaných bezpečnostních opatření a tvorba příručky bezpečnosti informací, upřesňující pravidla a postupy zavedených opatření v oblastech bezpečnosti informací dle ISO/IEC 27002.
- Připravit a nastavit program budování bezpečnostního povědomí, zahrnující zaškolení všech zainteresovaných osob.
- Zvolit způsob měření účinnosti bezpečnostních opatření a následně dané ukazatele sledovat.
- Definovat postupy a další opatření pro případ potřeby rychlé reakce na bezpečnostní incidenty.
- Řízení zdrojů, dokumentů a záznamů ISMS (7).

### 1.6.1 Plán zvládání rizik

V dokumentu s názvem Plán zvládání rizik jsou popsány **všechny činnosti ISMS**, které jsou potřebné pro řízení bezpečnostních rizik, cíle a priority činností ISMS, omezující faktory a potřebné personální, finanční, technologické apod. zdroje. Obsahuje také jednoznačné **určení odpovědnosti** za provádění jednotlivých činností. Prvním zdrojem, ze kterého plán vychází, jsou **informace**, které jsou získány v první fázi ustavení ISMS, konkrétně ze zprávy o **hodnocení rizik a prohlášení o aplikovatelnosti**. Druhým zdrojem údajů, nezbytných pro vytvoření dokumentu, jsou podněty, které vznikají při pravidelném **přehodnocování ISMS**. Tím je plán zvládání rizik obohacen o zkušenosti s fungováním ISMS. Je také vhodné do plánu zahrnout činnosti pro snižování bezpečnostních rizik a činnosti, které požaduje norma ISO/IEC 27001, například naplánování interních auditů apod. (4).

### 1.6.2 Příručka bezpečnosti informací

Příručka bezpečnosti informací je dokument, který slouží k **podpoře prosazování ISMS**. Příručka definuje dílčí procesy a postupy, které zajišťují efektivní prosazení dílčích bezpečnostních opatření. Je v ní definováno kdo, co, kdy, kde a jak má učinit (4).

### 1.6.3 Prohlubování bezpečnostního povědomí

Jedná se jeden z nejdůležitějších prvků při prosazování ISMS. Samotné stanovení řešení ISMS nestačí. Nejdůležitější je **zavedení tohoto řešení do praxe** tak, že se všechna definovaná pravidla a postupy promítnou do skutečného chování všech zaměstnanců organizace, a to bez výjimky. Jedná se o zdánlivě jednoduchý cíl, který však vyžaduje vysoké a systematické úsilí. Proces prohlubování bezpečnostního povědomí je **nekonečný proces** rozhodující o skutečné efektivitě ISMS. Organizace by měla vytvořit dokument s názvem **Minimální bezpečnostní pravidla pro uživatele**, který by popisoval, jak se má uživatel chovat při práci s výpočetní technikou a při práci s IS. Celý proces obvykle probíhá formou školení, které by mělo vycházet právě z organizací definovaného návodu (7, 8).

Školení by mělo především zahrnovat:

- Seznámení s pojmem ISMS a jeho přínosu pro organizaci.
- Seznámení s dalšími spojenými pojmy, jako např. informační bezpečnosti, aktivum, analýza rizik.
- Aktuální stav bezpečnostní politiky v organizaci.
- Dokument Minimální bezpečnostní pravidla pro uživatele.
- Vyzdvižení změn a novinek oproti poslednímu školení.
- Závěrečné ověření znalostí uživatelů zvolenou formou, například testem (7).

Pro společnosti, ve které je ISMS certifikován, povinnost pravidelného školení vychází přímo z normy. Frekvenci a podrobnost školení je pak vhodné přizpůsobit různým typům uživatelů (7).

### 1.6.4 Měření účinnosti

Měření účinnosti aplikovaných bezpečnostních opatření je nutné pro efektivní řízení společnosti. Organizace by měla **pravidelně sledovat zvolené ukazatele,** vypovídající skutečnou **efektivitu systému řízení.** Na základě těchto informací pak lze provádět důležitá rozhodnutí. Tento proces je součástí **všech etap životního cyklu ISMS** a neměl

by být podceněn, protože případná chyba ve specifikaci ISMS a výše nákladů vynaložených na její odstranění od první etapy strmě stoupá (3, 4).

### 1.6.5 Řízení provozu, zdrojů, dokumentace a záznamu ISMS

Všechny činnosti by měly být prováděny řízeným způsobem. Samozřejmostí by mělo být dodržování stanovených pravidel a shromažďování podkladů pro další fáze. Jedním z provozních požadavků je také **definice postupů a opatření pro řízení incidentů**. Odpovědní pracovníci by měli být upozorněni na odhalené incidenty a bezpečnostní slabiny. Nabyté zkušenosti z řešení takových incidentů pak slouží pro optimalizaci pravidel ISMS (3, 4).

## 1.7 Etapa č. 3 – Monitorování a přezkoumání ISMS

Hlavním cílem třetí etapy je zajistit dostatek **podkladů o skutečném fungování** ISMS, na základě kterých bude moci vedení organizace posoudit, zda je realizace ISMS v souladu s obecnými potřebami organizace. Proto by mělo dojít k **prověření** všech zavedených bezpečnostních **opatření** a jejich **důsledků na ISMS**. Odpovědné osoby by měly být zkontrolovány svými nadřízenými či bezpečnostním manažerem. Dalším způsobem ověření fungování ISMS je forma **nezávislého interního auditu ISMS**. Výstupem této fáze je **zpráva o stavu ISMS**, na jehož základě může vedení systém přehodnotit (3, 4).

### 1.7.1 Monitorování, měření, analýza a hodnocení

Všechny osoby, které mají za fungování systému řízení bezpečnosti informací nějakou odpovědnost, jsou **povinni provádět kontroly**. Tyto osoby by měly svědomitě plnit svěřené úkoly a zároveň kontrolovat, že dochází k plnění všech bezpečnostních požadavků. Zároveň by mělo docházet ke kontrole, že zavedená bezpečnostní opatření **naplňují očekávání**, která se od nich očekávala. Provádění kontrol zahrnuje i včasná **detekce chyb, pokusů o narušení bezpečnosti, bezpečnostních incidentů**. Mezi kontrolní činnosti spadá i **vyhodnocení měření** účinnosti ISMS a aplikovaných bezpečnostních opatření, které bylo provedeno v předchozí etapě. Tyto výsledky jsou pak vstupem pro návaznou činnost, která spočívá v **přehodnocení výsledků** ohodnocení rizik na základě zkušeností z fungování ISMS. Všechny podněty z těchto aktivit by měly být zaznamenány do příslušných dokumentů a plánu ISMS (7).

### 1.7.2 Interní audit

Kritickým prvkem zpětné vazby jsou **interní audity ISMS**, které jsou na rozdíl od předchozích kontrol **nezávislé** a zajišťují tak nezávislý pohled na fungování systému. Audit má za úkol posoudit, do jaké míry jsou splněna předem stanovená kritéria, tedy **dodržování procesních pravidel** (především naplňování požadavků ISO/IEC 27001) a prověření **fungování jednotlivých bezpečnostních opatření** (7).

### 1.7.3 Přezkoumání vedením organizace

Vedení organizace je povinno v předem naplánovaných intervalech **přezkoumávat ISMS** v organizaci za účelem zajištění neustálé **vhodnosti, přiměřenosti a efektivnosti**. Vstupem jsou všechny související informace o fungování systému za uplynulé období, tedy především:

- Výsledky auditů ISMS.
- Zpětná vazba od zapojených uživatelů a třetích stran.
- Existující slabiny a hrozby, které mohly být při analýze rizik podceněny.
- Výsledky měření účinnosti ISMS.
- Změny v externím a interním aspektu, které ovlivňují ISMS.
- Příležitosti neustálého zlepšování (7).

Výstupy musí zahrnovat rozhodnutí, které se vztahují k příležitostem neustálého zlepšování a k libovolným potřebám změny v ISMS (7).

## 1.8 Etapa č. 4 – Údržba a zlepšování ISMS

Poslední, v pořadí čtvrtou etapou celého cyklu prosazování ISMS je **údržba a zlepšování** celého systému. Podstatou je sběr podnětů ke zlepšení ISMS a **náprava všech nedokonalostí** neboli neshod, které se v systému řízení informací objevují. Nezbytnou součástí této etapy jsou následující činnosti:

- Identifikace neshod a aplikace nápravných opatření
- Neustále zlepšování ISMS (7).

### 1.8.1 Neshody a nápravná opatření

Při výskytu **neshody musí** organizace **reagovat** na neshodu, pokud je to možné, tak přijmout a implementovat opatření **k řízení a nápravě neshody** a zabývat se jejími následky. Zároveň by měla **odhalit příčinu** této neshody a zajistit, aby se neshoda znovu

nevyskytla. U všech těchto přijatých nápravných opatření by se měla **přezkoumat efektivnost těchto opatření.** Veškeré informace o těchto neshodách a následně přijatých opatřeních by měly být dokumentovány (7).

### 1.8.2 Neustálé zlepšování

Organizace musí neustále zlepšovat vhodnost přiměřenost a efektivnost ISMS (7).

## 1.9 Proces řízení rizik

Dle normy ISO/IEC 27001 musí být opatření přijatá v rámci rozsahu, hranic a kontextu ISMS založená na riziku. A právě proces řízení rizik bezpečnosti umožňuje tento požadavek normy splnit (9).

**Řízení rizik** je pro systematické řízení bezpečnosti informací **klíčovým nástrojem**. Na základě přesné znalosti rizik se vybírají a prosazují vhodná bezpečnostní opatření ve snaze **snížit negativní dopady těchto rizik**. Řízení rizik podstatným způsobem ovlivňuje efektivitu fungování celého ISMS a je základem pro každý systém řízení bezpečnosti informací. Jedná se o **cyklický proces**, který probíhá v několika krocích. Nejprve je nutné stanovit kontext, pak se provádí posouzení rizik. V okamžiku, kdy máme dostatek informací pro efektivní určení akcí, které zajistí modifikaci rizik na přijatelnou úroveň, je na řadě **ošetření rizik**. Po dobu, kdy jsou informace nedostatečné, dochází k opakování posouzení rizik s revidovaným kontextem (9).

Součástí řízení rizik je i **zapojení zainteresovaných stran a jejich informování.** Během celého procesu řízení rizik bezpečnosti informací je důležité, aby byli informováni příslušní vedoucí pracovníci i řadoví zaměstnanci. Řízení rizik bezpečnosti informací by mělo také přispět k tomu, aby byla rizika a procesy ošetření rizik neustále sledovány a pravidelně přezkoumávány. Užitečné je také získávat informace ke zlepšení přístupu k řízení rizik a pravidelně školit vedoucí pracovníky i zaměstnance v oblasti rizik a přijímaných opatření (9).

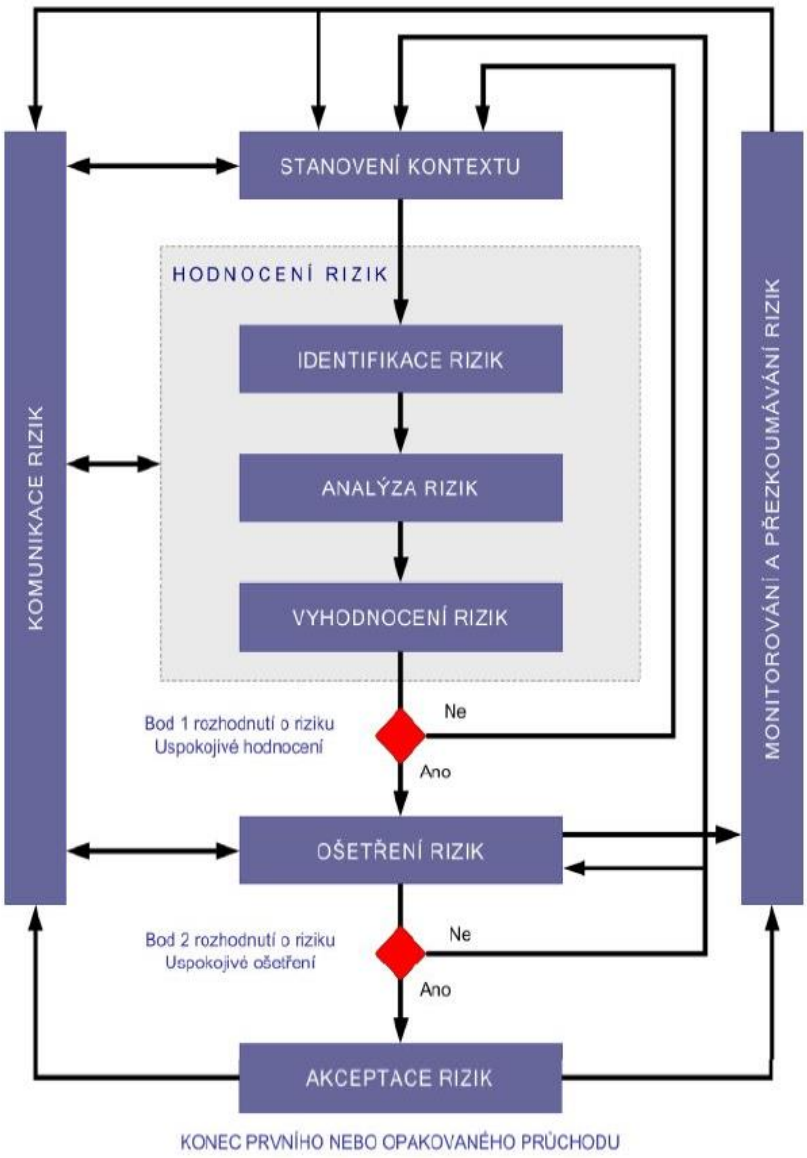
Propojení ISMS a procesu řízení rizik bezpečnosti informací neboli použití modelu PDCA při řízení rizik je znázorněno v tabulce č. 1.

**Tabulka č. 1: Propojení ISMS a procesu řízení rizik bezpečnosti informací**

| Proces ISMS | Proces řízení rizik bezpečnosti informací |
|---|---|
| Plánuj | Stanovení kontextu<br>Posouzení rizik<br>Příprava plánu ošetření rizik<br>Akceptace rizika |
| Dělej | Implementace plánu ošetření rizik |
| Kontroluj | Kontinuální monitorování a přezkoumávání rizik |
| Jednej | Udržování a zlepšování procesu řízení rizik bezpečnosti informací |

Zdroj: vlastní zpracování dle (9)

Pro přehlednost dodávám procesní pohled na řízení rizik bezpečnosti informací v grafické na obrázku č. 4.




**Obrázek č. 4: Proces řízení rizik bezpečnosti informací dle ČSN ISO/IEC 27005**

Zdroj: (9, s. 14)

Pro dosažení co nejvyšší efektivity řízení rizik je důležité, aby se do procesu zapojilo co nejvíce lidí a využit jejich různých názorů a pohledů. Celý proces by měl být **koordinován** a někdo by za něj měl nést odpovědnost. Součástí procesu musí být i dokumentace, která **eviduje provedená rozhodnutí** a napomáhá opakovat celý proces na základě poznatků z monitorování ISMS (9).

### 1.9.1 Stanovení kontextu

Organizace by si měla stanovit kontext pro řízení rizik bezpečnosti informací, který zahrnuje:

- Definování základních kritérií pro řízení rizik bezpečnosti informací
- Definování rozsahu a hranice
- Stanovení příslušné organizační struktury pro řízení rizik bezpečnosti informací (9).

Nejdůležitějším krokem je určit **účel řízení rizik** bezpečnosti informací, kterým může být právě podpora ISMS (9).

### 1.9.2 Posouzení rizik bezpečnosti informací

Po stanovení kontextu je nutné identifikovat rizika, následně je ohodnotit a určit priority v souladu s kritérii a cíli posouzení rizik vztaženým k organizaci. Posouzení rizik se skládá z těchto kroků:

1. Identifikace rizik
2. Analýza rizik
3. Hodnocení rizik

Nyní popíši jednotlivé kroky posouzení rizik bezpečnosti informací

**1) Identifikace rizik**

Smyslem identifikace rizik je definovat, **co** by se mohlo stát, aby byla způsobena **potencionální ztráta** a porozumět tomu jak, kde a proč ke ztrátě může dojít (9). V následujících krocích bude popsáno shromáždění vstupních dat pro posouzení rizik.

**a) Identifikace a ohodnocení aktiv**

Aktivum je cizí slovo, označující veškerý hmotný i nehmotný majetek, který má pro organizaci hodnotu a který tím pádem vyžaduje ochranu. Předtím, než můžeme aktivum ohodnotit, je nutné aktiva nejprve **identifikovat.** Identifikace aktiv by měla být realizována na určité úrovni podrobnosti tak, aby poskytovala pro posouzení rizik

dostatečné množství informací. Stupeň podrobnosti lze zpřesnit v dalším opakování posouzení rizik (3).

Seznam identifikovaných aktiv by měl obsahovat i **vlastníka aktiva**, tedy člověka, který na aktivum nemusí mít vlastnická práva, ale má přiměřenou odpovědnost za jeho produkci, vývoj, údržbu, používání a bezpečnost. Zároveň je vlastník aktiva vhodným člověkem pro **určení hodnoty** aktiva pro organizaci (3).

Po vytvoření seznamu aktiv je tak dalším krokem jejich ohodnocení. Pro to je třeba stanovit stupnici a hodnotící kritéria, která budou použita k přiřazování ohodnocení jednotlivých aktiv. Organizace může zvolit peněžní nebo kvalitativní stupnici. Příklad tabulky pro ohodnocení aktiv (při napadení aktiva) je zobrazen v tabulce níže:

**Tabulka č. 2: Tabulka pro hodnocení aktiv**

| Hodnota | Hodnocení dopadu |
|---|---|
| 1 | Žádný dopad na organizaci |
| 2 | Zanedbatelný dopad na organizaci |
| 3 | Malý dopad na organizaci |
| 4 | Vážné potíže organizace |
| 5 | Velmi vážné potíže organizace |

Zdroj: vlastní zpracování dle (3)

Je doporučeno používat barevné odlišení jednotlivých úrovní, které v případě rozsáhlých tabulek s hodnocením aktiv výrazně ulehčí orientaci. Výběr a rozsah termínů si organizace volí dle bezpečnostních potřeb, velikosti apod.

Hlavním principem pro ohodnocení aktiv jsou náklady vzniklé v důsledku **narušení** důvěrnosti, integrity a dostupnosti. Tato kritéria jsou hlavním podkladem pro ohodnocení jednotlivých aktiv (3).

Po určení váhy jednotlivých aktiv je dalším krokem **výpočet hodnoty aktiva**, ke kterému je možné dojít několika způsoby. Nejjednodušším a zároveň nejpoužívanějším je tzv. součtový algoritmus, jehož principem je vzorec:

**(Dostupnost + Integrita + Důvěrnost)/3**

Jedná se o nejrychlejší způsob získání hodnoty aktiva a zároveň odpovídá na otázku, jak velký dopad pro organizace bude mít zničení, případně poničení tohoto systému.

### b) Identifikace hrozeb

Hrozba je případná příčina nežádoucího incidentu, který může mít za následek poškození systému, organizace nebo jejích aktiv. Hrozby mohou mít buď **přírodního**

(povodně, požár) nebo **lidského původu** (odposlech, chyba uživatele, apod.) a mohou být **náhodné** (vymazání souboru) nebo **úmyslné** (zcizení, úmyslné poškození).
Z pohledu bezpečnosti je důležité identifikovat **všechny** náhodné i úmyslné **hrozby** a měla by být odhadnuta jejich úroveň a pravděpodobnost (3, 9).

**c) Posouzení hrozeb**

Posouzení hrozeb se provádí v závislosti na následujících otázkách:

- Ztráta důvěrnosti – může způsobit například ztrátu důvěry vůči zákazníkům, ohrozit osobní bezpečnost, finanční ztrátu nebo právní odpovědnost.
- Ztráta integrity – může způsobit akceptování nesprávného rozhodnutí, narušení funkčnosti organizace.
- Ztráta dostupnosti – může způsobit neschopnost vykonávání pro organizaci klíčových činností.
- Ztráta individuální odpovědnosti – může vést třeba k podvodu, špionáži, krádeži apod.
- Ztráta autentičnosti – může způsobit použití neplatných dat, které vedou k nesprávným výsledkům.
- Ztráta spolehlivosti – může vést například k nespolehlivým dodavatelům, demotivaci zaměstnanců (9).

Vždy je potřeba neopomenout tzv. **následný efekt hrozby**. Například hrozba – výpadek elektrické energie neznamená pouze nedostupnost dat, ale při dlouhodobém výpadku může vést k ohrožení činnosti organizace. Vždy je nutné se zamyslet nad možnými dopady hrozeb do nejmenších detailů.
Jako příklady nejčastějších hrozeb lze uvést například selhání dodávky elektrické energie, škodlivý software, selhání hardwaru nebo selhání komunikačních služeb (9).

**d) Identifikace stávajících opatření**

Před návrhem vhodných opatření je vhodné provést identifikaci stávajících opatření, aby se předešlo zbytečné práci nebo výdajům například při duplikaci opatření. Kromě identifikace stávajících opatření norma ISO/IEC 27005 doporučuje provést i kontrolu jejich funkčnosti a z této kontroly vyvodit patřičné závěry, například zavést dodatečné opatření, nahradit jiným či opatření úplně odstranit (9).

## 2) Analýza rizik

Analýzu rizik je možné provádět v různých stupních podrobnosti v závislosti na kritičnosti aktiv, rozsahu známé zranitelnosti a předcházejících incidentech zachycujících organizaci. Účelem analýzy rizik je **identifikovat zranitelná** místa informačního systému organizace, zachytit **seznam hrozeb** působících na IS a stanovit rizika příslušná každému zranitelnému místu a hrozbě. Cílem celé analýzy je pak **snížit velikost rizika** na přijatelnou úroveň, respektive přijmout **zbytková rizika** tam, kde je jejich minimalizace neefektivní (3, 9).

### a) Metodiky analýzy rizik

První metodou je k**valitativní analýza rizik**, která se používá k popisu velikosti potencionálních následků (například nízkých, středních a vysokých) a jejich pravděpodobnosti, škálu kvalifikačních atributů. Výhodou metody je, že je pro pracovníky snadno pochopitelná. Nevýhodou pak je závislost na subjektivním výběru škály. Je vhodné ji použít například v případě, že je nevhodné použít číselné údaje (9).

Druhou metodou je **kvantitativní analýza rizik**, která používá stupnici s číselnými hodnotami jak pro následky, tak pro pravděpodobnost. Její kvalita se odvíjí od přesnosti a úplnosti číselných hodnot a platnosti použitých modelů. Často používá historická data incidentů a její výhodou je, že může mít přímou souvislost s cíli bezpečnosti informací a zájmy organizace. Nevýhodou tohoto přístupu je, že mohou být k dispozici nepřesná data, což vytváří mylný dojem o významu a přesnosti posouzení rizik (9).

### b) Metody pro výpočet míry rizika

Míru rizika je možné stanovit pomocí dvou přístupů. Prvním z nich je analýza rizik pomocí **pravděpodobnosti incidentu a jeho dopadu**. Druhým přístupem je analýza rizik využívající **matice aktiv, hrozeb a zranitelností**.

**Analýza rizik, využívající matice aktiv, hrozeb a zranitelnosti** používá 3 parametry, a to (aktivum, hrozba, zranitelnost) a probíhá ve čtyřech krocích:

1. Spojením tabulky hodnocení aktiv a tabulky hrozeb a zranitelností vznikne matice zranitelnosti.
2. Doplnění jednotlivých aktiv do matice a posouzení jejich zranitelnosti
3. Výpočet míry rizika vztahem R = T*A*V, kde

R – míra rizika

T – pravděpodobnost vzniku hrozby

A – hodnota aktiva

V – zranitelnost aktiva

4. Stanovení hranic rizika (3).

**Analýza rizik pomocí pravděpodobností incidentu a jeho dopadu** využívá pouze 2 parametry, a to pravděpodobnost a dopad incidentu. Metoda probíhá v následujících 4 krocích:

1. K již vytvořené matici zranitelnosti se doplní identifikovaná existující opatření
2. Odhad pravděpodobnosti incidentu
3. Parametr dopad využívá shodnou tabulku, jako aktivum
4. Výpočet míry rizika vztahem R = PI*D, kde

   R – míra rizika

   PI – pravděpodobnost incidentu

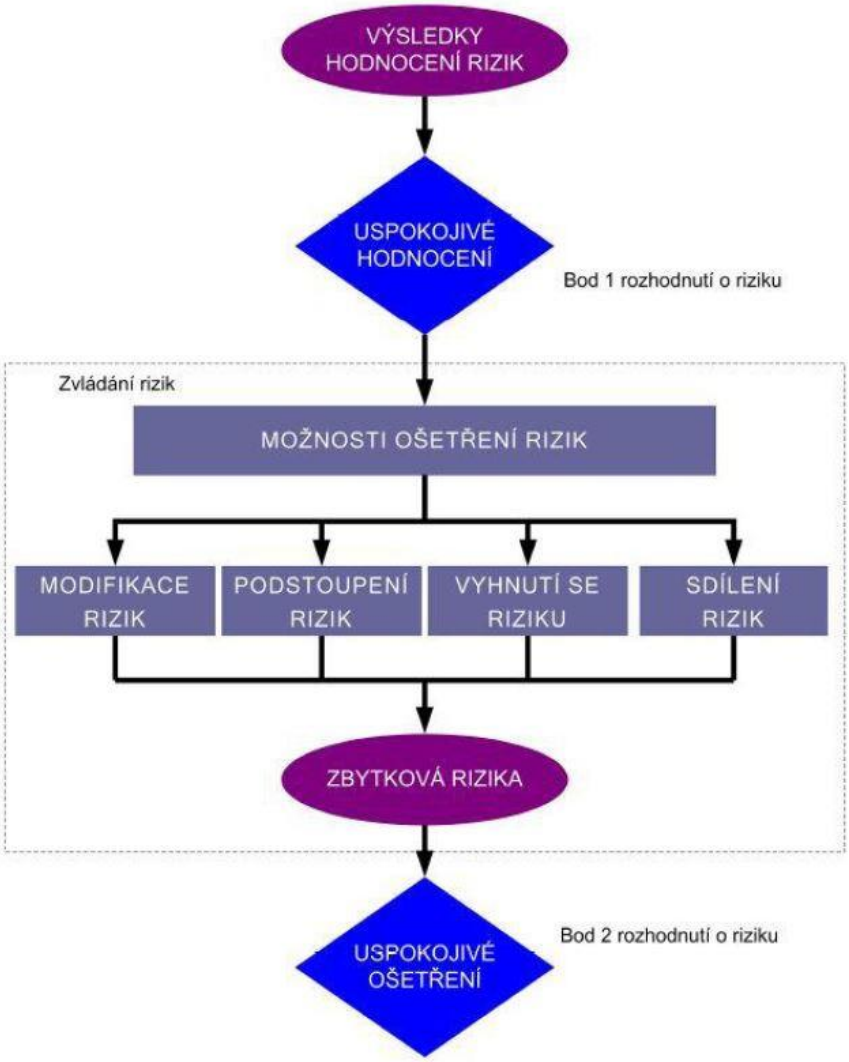
   D – dopad (3).

**3) Vyhodnocení rizik**

Výsledkem analýzy rizik je **seznam rizik a kritéria pro hodnocení rizik**, na jejichž základě je jim přidělena priorita, která zajistí jednotlivým opatřením odpovídající pozornost (9).

### 1.9.3 Ošetření rizik bezpečnosti informací

Pokud považujeme vyhodnocení rizik za uspokojivé, můžeme přistoupit k dalšímu kroku, a to je **ošetření rizik** bezpečnosti informací. Výběrem vhodných bezpečnostních opatření chceme docílit **minimalizace případných rizik**. Při výběru vhodných opatření musí být zohledněna kritéria pro akceptaci rizik, stejně tak jako legislativní a smluvní požadavky. Pro ošetření rizik jsou k dispozici čtyři volby: **modifikace** rizika, **podstoupení** rizika, **vyhnutí se** riziku a **sdílení** rizika. Obrázek č. 5 zobrazuje činnosti ošetření rizik v rámci procesu řízení rizik bezpečnosti informací, jak je uveden na obrázku č. 4 (9).




**Obrázek č. 5: Ošetření rizik**

Zdroj: (9, s. 25)

Způsoby ošetření rizik je vhodné volit na základě výstupu z posouzení rizik, očekávaných nákladů na implementaci a očekávaných přínosech plynoucích z těchto způsobů, přičemž jednotlivé způsoby se nevylučují a lze je kombinovat. Přednost by měly dostat možnosti, kterými lze dosáhnout **velké snížení rizika při poměrně nízkých nákladech**. Další možnosti mohou být neekonomické a je třeba posoudit, jestli jsou obhájitelné. Cílem je snížit nepříznivé následky rizik na nejnižší přiměřenou dosažitelnou míru bez ohledu na jakákoliv absolutní kritéria. Norma 27005 doporučuje definovat plán ošetření rizik, který jasně identifikuje pořadí priorit, ve kterém budou jednotlivé způsoby ošetření rizik aplikovány, včetně časového rámce (9).

**a) Modifikace rizika**

Úroveň rizika by měla být řízena implementací, odstraněním nebo změnou opatření tak, aby nové zbytkové riziko bylo vyhodnoceno jako **přijatelné**. Podrobné informace o jednotlivých opatřeních poskytuje norma ISO/IEC 27002 (9).

**b) Podstoupení rizika**

Pokud úroveň rizika splňuje kritéria **akceptace** rizik, není nutné zavádět další opatření a riziko lze **podstoupit** (9).

**c) Vyhnutí se riziku**

Pokud jsou identifikovaná rizika příliš **vysoká** nebo by náklady na uplatnění jiných způsobů **převyšovaly** přínosy, může organizace rozhodnout o celkovém **vyhnutí se** riziku tím, že se vyhne činnosti nebo podmínce, která dává riziku příležitost vzniknout. Ekonomicky nejvýhodnější může být například fyzicky **přestěhovat** zařízení na místo, kde riziko neexistuje nebo je pod kontrolou (9).

**d) Sdílení rizika**

Dalším způsobem ošetřením rizik je **sdílení** rizika s jinou externí stranou, která může toto konkrétní riziko podle hodnocení rizik nejúčinněji zvládnout. Sdílení rizik však může zapříčinit vznik **nových rizik** nebo **měnit existující**, identifikovaná rizika. V takovém případě je pak zapotřebí použít další způsoby ošetření rizik. Příkladem sdílení rizik je **pojištění**. Norma upozorňuje i na to, že je možné sdílet odpovědnost za sdílení rizika, ale obvykle není možné sdílet odpovědnost za dopad (9).

### 1.9.4 Akceptace rizik bezpečnosti informací

Po vypracování plánu ošetření rizik a posouzení zbytkových rizik v závislosti na rozhodnutí o akceptaci rizik, by měla být provedena a formálně zaznamenána rozhodnutí **akceptovat rizika** a o**dpovědnosti** za tato rozhodnutí (9).

### 1.9.5 Komunikace a konzultace rizik bezpečnosti informací

Po celou dobu procesu by si měli účastníci procesu vyměňovat a sdílet informace o jednotlivých rizicích. Efektivní obousměrná komunikace může mít podstatný vliv na nutná rozhodnutí (9).

### 1.9.6 Monitorování a přezkoumávání rizik bezpečnosti informací

Protože **rizika** a jejich faktory (např. hodnota aktiv, dopad, hrozby, zranitelnosti, pravděpodobnost výskytu) **nejsou stálá** a mohou se měnit bez předchozího náznaku, měly by být neustále **monitorovány a přezkoumávány**, aby bylo možné včas zareagovat na změny v kontextu organizace a udržovat přehled nad jednotlivými riziky.

Stejně tak by měl být monitorován, přezkoumáván a zdokonalován dle potřeb i proces řízení rizik bezpečnosti (9).

## 1.10 ITIL

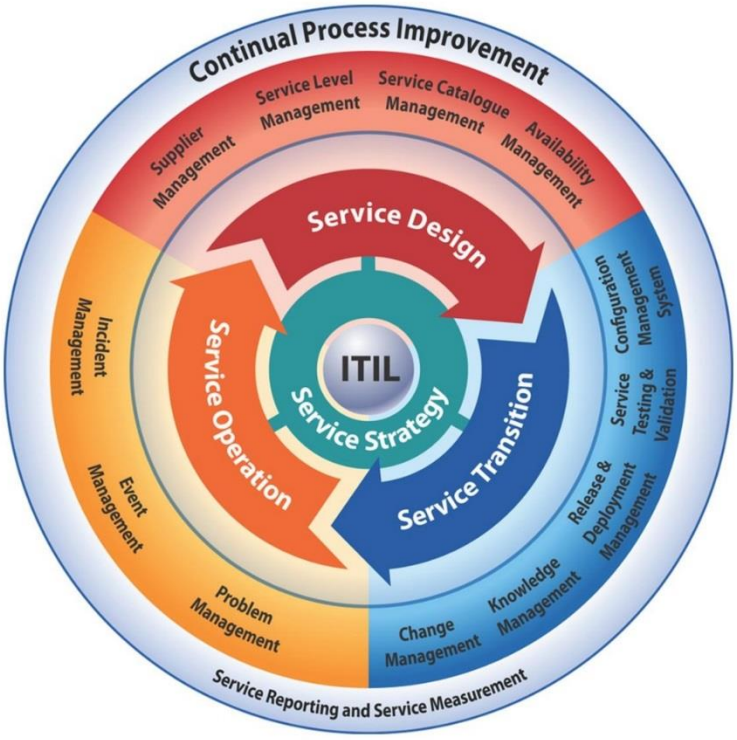
Zkratka ITIL vznikla jako zkratka z anglických slov Information Technology Infrastructure Library (ITIL). Je to **procesní rámec přístupů či standard** pro řízení a správu služeb IT (ITSM) za přiměřených nákladů, vycházející z nejlepších praktických zkušeností. Tyto „**best practices“** z oblasti řízení služeb ICT napomáhají, jsou-li implementovány, k dosažení kvality. ITIL definuje kdy a které činnosti a procesy vykonat a odpovědné role. Neříká ale, jak konkrétně tyto činnosti provádět, jakou mít organizační strukturu. Tato knihovna je spravována organizací Office of Government Commerce a je šíří se formou knih, CD, školení, konzultací a certifikací (3, 11).

Skládá se z několika částí, které jsou zaměřené na specifické oblasti řízení IT služeb, které odpovídají klíčovým procesům v IT. Sada knižních publikací se současně skládá z 5 ústředních **publikací**, které zahrnují celý **životní cyklus služby** od jejího vzniku až po provoz a zánik:

- ITIL Service Strategy – Strategie služeb.
- ITIL Service Design – Návrh služeb.
- ITIL Service Transition – Uvedení služby do provozu.
- ITIL Service Operation – Provoz služeb.
- ITIL Continual Service Improvement – Neustálé zlepšování služeb (11)

*„Protože je ITIL® nezávislý na platformě a protože je to „rámec“, jsou výstupy všech dodavatelů v celém odvětví kompatibilní a univerzálně použitelné (SW nástroje, školení, konzultační služby)“* (3, s. 28).

Vztah ústředních publikací a některých procesů je znázorněn na obrázku č. 6.



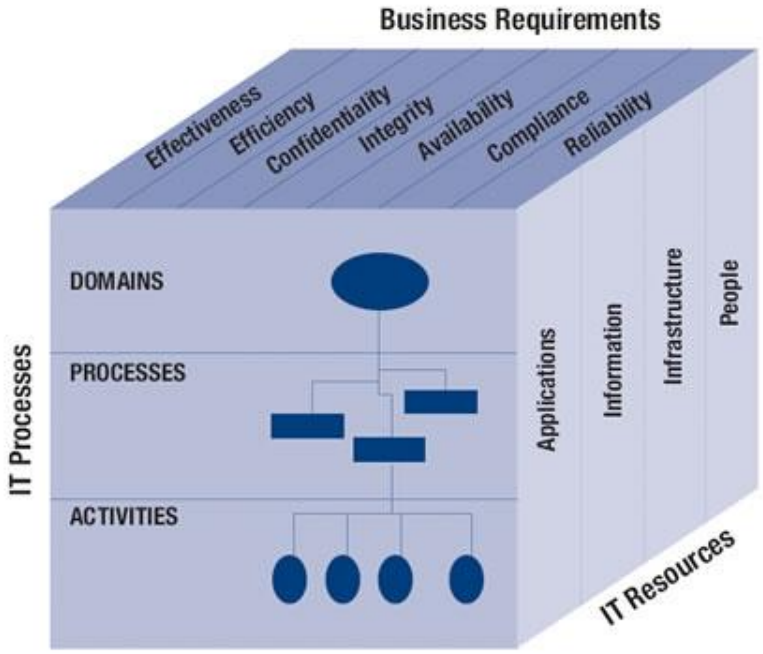

**Obrázek č. 6: ITIL**

Zdroj: (12)

## 1.11 COBIT

**C**ontrol **OB**jectives for **I**nformation and related **T**echnology je mezinárodně uznávaná **komplexní metodika**, která vychází ze souboru všeobecně uznávaných praktik řízení, kontroly a hodnocení IS/ICT a umožňuje propojit principy obecného řízení organizace s pravidly, kterými se řídí prostředí IT a nastavit tak lépe strategické řízení podnikové informatiky v souladu se strategickými cíli. Snahou metodiky je především strukturovat vysoce **složitý systém řízení ICT** tak, aby byl co nejvíce **srozumitelný** pro manažery a uživatele bez **detailních znalostí ICT** (3).

Významnou pomůckou pro vyjasnění vztahů mezi podnikovými **požadavky** (efektivita, účinnost, důvěryhodnost, integrita, dostupnost, soulad, spolehlivost), **IT zdroji** (aplikace, informace, infrastruktura, lidé) a **IT procesy** (domény, procesy, aktivity) je tzv. **Kostka COBIT** (viz. Obrázek č. 7).




**Obrázek č. 7: Kostka Cobit**

Zdroj: (13)

## 1.12 Minimální standard bezpečnosti

V roce 2015 bylo zpracováno **metodické doporučení** k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních, jako jedno z opatření ministerstva školství, mládeže a tělovýchovy, na základě úkolu ze schůze vlády České republiky, která se konala k tragické události ve Žďáru nad Sázavou (14).

Toto metodické doporučení by mělo posloužit školám a školským zařízením **při jednání se zřizovateli,** a to s ohledem na nutná opatření, které vyplývají z jejich potřeb, charakteru provozu a z místních podmínek.

Minimální standard bezpečnosti škol nebo školských zařízení obsahuje prostorová, organizačně-technická, personální opatření, včetně opatření v oblasti zpracované dokumentace. Opatření, uvedená v této metodice, jsou zaměřená především na zajištění **fyzické a psychické bezpečnosti** dětí, žáků a studentů.

Dle metodiky je třeba vnímat problematiku zajištění minimálního standardu bezpečnosti v těchto rovinách:

- **Prevencí** předcházet mimořádným událostem (aplikovat technická opatření, poučit o bezpečnosti žáky a zaměstnance, označení cizích osob v objektu, spolupráce se složkami integrovaného záchranného systému,…).

- Účinně a efektivně **reagovat na mimořádnou událost** a reagovat na ní ve snaze o omezení škod na životech a zdraví zaměstnanců i žáků.
- Vyhodnotit mimořádnou událost a **přijmout opatření**, aby nemohlo dojít ke stejné události znovu ze stejné příčiny (14).

V metodice jsou opatření rozdělena do tří skupin, a to:

**1. Prostorová a organizačně-technická opatření**

Obsahuje doporučení na využívání pouze jednoho zabezpečeného a monitorovaného vchodu, kontrolu vstupu cizích osob, úpravy zeleně pro zvýšení přehlednosti a funkční venkovní osvětlení (14).

**2. Personální opatření**

Škola by měla průběžně **dohlížet** na žáky po **celou dobu** od okamžiku, kdy vstoupí do prostor školy až po opuštění budovy či areálu. Dohled by měl být úměrný věku žáků, jejich vyspělosti, dopravním a jiným rizikům. Osoby odpovědné za dohled by měly být pověřeny ředitelem školy a rozvrh dohledu by měl být umístěn na všem známém místě. Dohled nad žáky by měl být i při vzdělávacích akcích mimo školu.

V metodice je zmíněno, že jednou z možností, jak získat finanční prostředky pro zajištění služby vrátného je vytvoření takzvaného **společensky účelného pracovního místa** na základě dohody s Úřadem práce ČR (14).

**3. Vnitřní předpisy, dokumentace školy**

Škola by měla provádět s odborně způsobilými osobami analýzu rizik a mít zpracované **dokumenty pro mimořádné události**, typu neoprávněný vstup do budovy, přítomnost neznámého či nezabezpečeného předmětu nebo látky ve škole, vandalismus, šikana, apod. Účinnost všech dokumentů by měla být pravidelně ověřována, včetně pravidelného zkoušení technických prostředků a zařízení.

Škola by měla mít ve své dokumentaci zmíněny povinnosti zaměstnanců, které jsou spojeny s mimořádnými událostmi, dodržování nastavených bezpečnostních opatření a předávat je dále na další zaměstnance a žáky (pravidelně minimálně na začátku školního roku, záznam o poučení).

Škola by měla mít definován **formální rámec bezpečnosti a ochrany zdraví** a měla by informovat zákonné zástupce o vydání a obsahu školního řádu.

Odchylky od tohoto minimálního standardu by měly být pouze v nezbytně nutných a odůvodněných případech. V případě jakýchkoli odchylek by měla být zavedena jiná bezpečnostní opatření tak, aby byla dodržena bezpečnost a ochrana zdraví žáků a zaměstnanců a zároveň nedocházelo k rozporu s výše uvedenými principy.

Výše zmíněné požadavky jsou pouze minimální a lze využít i jiné technické prostředky, např. vstupy opatřené čipem, kamerový systém, elektronický vrátný, apod., které však nemohou plně nahradit dohled fyzickou osobou. Navíc rozhodne-li se škola například pro kamerový systém, je povinna brát v úvahu i ochranu soukromí žáků i zaměstnanců školy. Ochranou soukromí při nasazování kamerových systémů se zabývá Zákon 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Přímo k možnosti instalovat kamerový systém v prostorách školy pak vydal Úřad pro ochranu osobních údajů vyjádření, které shrnuje několik zásad, které je nutno posoudit ještě předtím, než se učiní rozhodnutí o instalaci kamerového systému (14).

# 2 ANALÝZA PROBLÉMU A SOUČASNÁ SITUACE

Obsahem této kapitoly bude analýza současného stavu, na základě které budou v další kapitole navrženy odpovídající opatření pro zavedení nutných oblastí ISMS v konkrétní organizaci. V této části práce bude krátké představení organizace, kterou následně podrobím analýze bezpečnosti. V závěru kapitoly provedu krátké shrnutí zjištěných poznatků.

## 2.1 Základní charakteristika organizace

Základní škola, kterou se ve své práci zabývám, je jedna ze dvou základních škol v malém městě nedaleko krajského města Pardubice. Zřizovatelem školy je město a hlavní činností je poskytování základního vzdělání a výchova žáků. Škola provozuje také školní družinu, která slouží k výchově, vzdělání a rekreaci žáků před a po vyučování. Škola se skládá ze tří budov, přičemž dvě se nachází na jednom pozemku zároveň s budovou gymnázia, přes kterou jsou obě budovy propojeny. Součástí školního areálu je i školní jídelna, která zajišťuje společné stravování pro žáky a zaměstnance školy. Stravovací zařízení je však provozováno soukromým provozovatelem a nebude tak součástí této práce. Třetí budova je samostatná a nachází se nedaleko dvou výše zmíněných objektů.

V současné době školu navštěvuje něco přes 400 žáků v 19 třídách. V zařízení pracuje 38 zaměstnanců, z toho 31 kvalifikovaných pedagogů a 7 nepedagogických pracovníků (15).

## 2.2 Organizační struktura

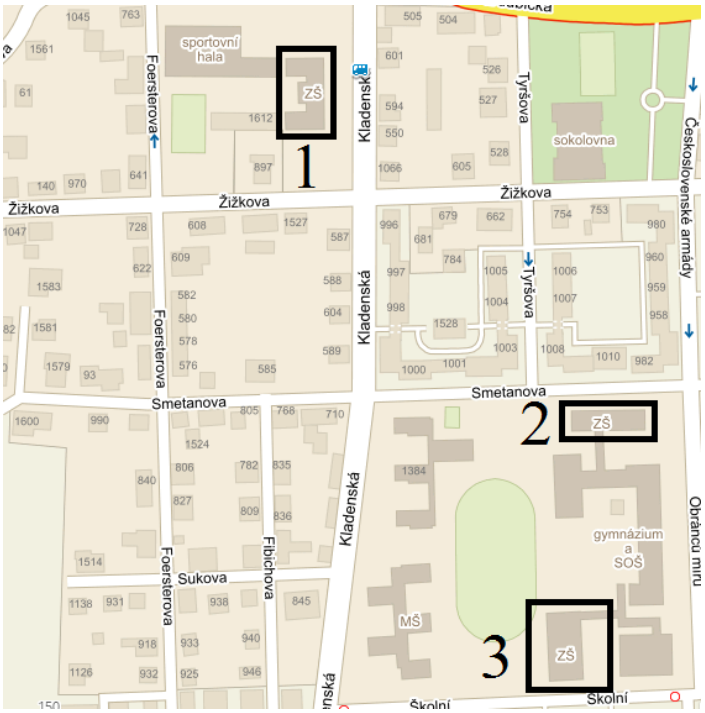
Ve vedení školy je ředitelka spolu se svojí zástupkyní a společně se podílí na řízení školy. Dále se škola dělí na I. stupeň, který pokrývá základní vzdělání od 1. do 5. třídy a II. stupeň od 6. do 9. třídy. Dalším oddělením je školní družina, kde působí čtyři vychovatelky. Ekonomický provoz školy má na starost hospodářský úsek, kde je vedoucí úseku a mzdová účetní. O technický provoz ve škole se stará školník, o pořádek pak 4 uklízečky (15).


**Obrázek č. 8: Organizační struktura základní školy**

Zdroj: (vlastní zpracování)

## 2.3 Poloha školy

Analýze podrobená základní škola se nachází v jižní části města a je součástí jediného městského sídliště, odkud do instituce dochází většina žáků. Jak již bylo zmíněno, jedná se o tři budovy, které jsou na obrázku č. 9. Pro snadnější orientaci ve zbytku práce, jsem si budovy pro přehlednost očísloval postupně čísly 1,2,3 (viz. Obrázek č. 9).




**Obrázek č. 9: Označení tří budov základní školy na mapě města**

Zdroj: (18)

## 2.4 Popis budovy č. 1

Budova číslo jedna, která je samostatná, slouží převážně pro I. stupeň (1. - 5. třída). Postavena byla na počátku 20. století a aktuálně ji navštěvuje denně přibližně 200 žáků. V této budově jsou kromě tříd I. stupně vyčleněny i 4 třídy, ve kterých je provozována školní družina. V budově se nachází jedna počítačová učebna s 20 stolními počítači. V posledních dvou letech navíc škola, částečně za pomoci peněz Evropské Unie, vybavila 10 tříd interaktivními tabulemi, které pomáhají zpestřit výuku. Učitelům slouží sborovna, ve které jsou umístěny dva stolní počítače a jedna síťová tiskárna. Všechny počítače jsou součástí jedné lokální sítě a se zbylými budovami prozatím nejsou propojeny. Internet zajišťuje firma Tlapnet s.r.o., poskytující připojení o rychlosti 1 Gbit/s.

**Obrázek č. 10: Interaktivní tabule v jazykové učebně**

Zdroj: (vlastní)

**Fyzická bezpečnost budovy č. 1**

Celý pozemek, na kterém se budova nachází, je oplocen a hlavní a jediný vstup na pozemek je branou z ulice Kladenská. Tato branka je přes den odemčena, odpoledne ji pak po skončení vyučování zamyká pověřený zaměstnanec. Vlastní budova má 2 vchody – jeden hlavní a jeden zadní, přičemž zadní vchod se nepoužívá a je trvale uzamčen. Hlavní vstup do budovy tvoří masivní dveře opatřené videotelefonem se čtyřmi zvonky do 4 tříd školní družiny. Pod videotelefonem jsou umístěny ještě obyčejné zvonky do jednotlivých tříd I. stupně a sborovny.

Vstup do budovy je zabezpečen elektronickým zabezpečovacím zařízením proti vloupání, které vždy aktivuje poslední odcházející zaměstnanec školy. Ráno je pak vypnuto prvním přicházejícím zaměstnancem. K aktivaci a deaktivaci systému dochází číselnou kombinací, kterou zná většina zaměstnanců a tento kód se mezi nimi šíří slovně.
V současné době v budově není nainstalované žádné nahrávací ani záznamové zařízení.

**Obrázek č. 11: Vstup a zvonky budovy č. 1**
Zdroj: (vlastní)

## 2.5 Popis budovy č. 2

V budově číslo dvě se kromě několika tříd druhého stupně nachází i kanceláře vedení školy. Objekt je spojen spojovací chodbou (dále jen spojovačka) s vedlejší budovou gymnázia (viz. Obrázek č. 9). V objektu se nachází třídy 5. ročníku a dále část tříd druhého stupně a několik odborných učeben. V sedmi třídách je interaktivní tabule a v blízké budoucnosti by tento počet měl dále narůstat.
Všechny počítače jsou součástí jedné lokální sítě, která je spojena bezdrátovým spojením s budovou číslo 3. V přízemí budovy jsou kanceláře ředitelky, její zástupkyně hospodářský úsek.

**Fyzická bezpečnost budovy č. 2**

Pozemek, na kterém se budova školy nachází, je oplocen a vstupní bránu zamyká každé odpoledne po skončení vyučování pověřený pracovník školy.

Celkově má budova 4 vstupy. Hlavní vchod, který využívají všichni žáci a většina pracovníků, je přístupný z pozemku školy. Tento vstup je kromě času příchodu a odchodu žáků uzamčen. V době, kdy jsou dveře uzamčeny, je pak možno použít videotelefon pro spojení s kanceláří školy, odkud jsou dveře dálkově ovládány elektrickým zámkem. Kancelář je však na druhé straně budovy a jediný vizuální kontakt s pouštěnou osobou je přes malou kamerku umístěnou na zvonku. V případě otevření dveří na dálku má osoba možnost volného pohybu po škole.

Další dva vchody jsou přístupné přímo z ulice a téměř se nevyužívají. Po celou dobu jsou zamčené a opět je možné použít zvonek pro spojení s kanceláří. Tento zvonek však není vybaven kamerou, jako je tomu v případě hlavních dveří.

Posledním způsobem, jak se dostat do budovy, je výše zmíněná spojovačka s budovou gymnázia, kterou se do budovy dá dostat odemčenými, zcela nezabezpečenými dveřmi.

V budově se nevyužívá elektronické zabezpečovací zařízení ani žádné záznamové zařízení.


**Obrázek č. 12: Hlavní vchod do budovy č. 2**

Zdroj: (vlastní)


**Obrázek č. 13: Zvonek s kamerou na budově č. 2**

Zdroj: (vlastní)

**Obrázek č. 14: Vstup ze spojovací chodby do budovy č. 2**

Zdroj: (vlastní)

## 2.6 Popis budovy č. 3

Budova číslo 3 se nachází asi 120 metrů od budovy číslo 2 a je z druhé strany spojena s budovou gymnázia stejným způsobem, tedy spojovací chodbou. Z budovy číslo 2 do budovy číslo 3 se tak dá dostat právě přes výše zmíněnou spojovací chodbou a budovu gymnázia a toto spojení se poměrně hojně využívá (viz. Obrázek č. 9) pro přesun mezi budovami. V budově je zbytek tříd II. stupně včetně několika odborných učeben. V přízemí se nachází učebna IVT, která byla vybudována v roce 2002 v rámci projektu Internet do škol, realizovaným Ministerstvem školství, mládeže a tělovýchovy České republiky. Učebna je současně vybavena 24 notebooky, které se škole podařilo získat

z peněz EU. V rohu učebny je i jediný server, který škola má a který prozatím slouží pro budovy 2 a 3. V učebně IVT je dále tiskárna, sloužící výhradně pro učebnu. Další tiskárna se nachází ve sborovně, která je připojená do lokální sítě a slouží pro potřeby pedagogů. Všechny počítače v budově, ať už stolní či přenosné, jsou svedeny do rozvaděče, který je umístěný ve výše zmíněné učebně IVT, kam také byla přivedena před 2 lety optická trasa poskytovatele Internetu Tlapnet s.r.o. a odkud je Internet bezdrátově přemostěn i na budovu č. 2.

**Technické parametry notebooků v učebně IVT**

Operační systém Microsoft Windows 7

Procesor: AMD Phenom™ II P650 Dual – Core Processor 2.60 GHz

Operační pamět: 3.00 GB

HDD: 250 GB

**Fyzická bezpečnost budovy č. 3**

Pro vstup do objektu slouží pouze jediný vchod z venku, který je mimo času příchodu a odchodu žáků uzavřen. U těchto dveří neexistuje možnost elektrického ovládání dveří a jedinou možností je tak ruční otevření dveří zevnitř. Druhou možností přístupu do budovy již zmíněnou spojovačkou, která je dostupná dveřmi, které jsou neustále odemčené a do budovy je tak touto cestou neomezený přístup.

**Obrázek č. 15: Hlavní vchod do budovy č. 3**

Zdroj: (vlastní)

**Obrázek č. 16: Vstup ze spojovací chodby do budovy č. 3**

Zdroj: (vlastní)

V budově se nevyužívá elektronické zabezpečovací zařízení ani žádné záznamové zařízení.

**Shrnutí fyzické bezpečnosti budov**

Fakt, že je škola rozprostřena do 3 budov přináší vedení školy několik komplikací. Jedním z nich je i fyzická bezpečnost budov, která je navíc oslabena o skutečnost, že dvě ze tří budov jsou spojeny s budovou gymnázia, do které je „volný“ přístup, byť pod kamerovým dohledem. V současné době jsou vstupy do budov po celý den uzamčeny s výjimkou časů, kdy děti přichází na vyučování. V době před vyučováním jsou vstupy odemčeny uklízečkami, které zároveň dohlíží na příchod žáků do budov. Především díky téměř volnému přístupu přes budovu gymnázia škola nemá pod kontrolou přístup a pohyb osob ve školních prostorách.

## 2.7 Kategorizace uživatelů

Ve škole jsou uživatelé kategorizování do 3 skupin, a to: žák, pedagog a administrátor. Pro každou z těchto kategorii byla správcem nastavena uživatelská práva omezující činnosti uživatelů. Po přihlášení uživatele se načte účet ze serveru a uživatel disponuje omezeným oprávněním, které je specifikováno na serveru.

**Žák**

Žáci, kteří jsou logicky nejpočetnější skupinou uživatelů na škole, se do sítě přihlašují pomocí Active Directory a jejich uživatelská práva jsou velmi omezená. Každý žák má na serveru vytvořený profil a přihlašuje se pomocí uživatelského jména ve tvaru příjmení a první písmeno z křestního jména (např. krystoft) a hesla. To je stejně jako uživatelské jméno pro každý účet vytvořeno podle jednotných pravidel. V učebnách mohou dále žáci využívat univerzální účet, jehož heslo je známo všem a jehož práva jsou také velmi omezena.

**Pedagog**

Všichni pedagogové vlastní účty a pro připojení do sítě využívají služby Active Directory, jejich uživatelská práva jsou taktéž velmi omezena. Pedagogové využívají počítače především k práci s e-maily, tvorbu dokumentů a v dohledné době je budou využívat i pro přístup do systému Bakaláři, který by se měl brzy postupně uvádět do provozu. Bohužel je však na většině PC v kabinetech a sborovnách možnost přihlásit se jako správce k lokálnímu účtu bez hesla, kde jsou práva neomezená. Soubory se navíc

neukládají na sdílené úložiště na serveru, ale pouze na lokální disk a nejsou tak žádným způsobem zabezpečena.

V případě problému obvykle kontaktují správce sítě. Zaměstnanci se nezúčastnili žádného školení o bezpečném používání počítačů a informačních technologií a nepodepsali žádnou písemnou formu takových pravidel.

**Administrátor**

Úkolem administrátorů, jakožto nejmenší uživatelskou skupinou s maximálními právy a administrátorským přístupem, je udržovat v chodu celou síťovou infrastrukturu a všechna zařízení, která do ní patří. Funkci správce vykonává jeden z pedagogů, který zároveň za tuto činnost odpovídá i na sousedním gymnáziu. Vzhledem k mnohaletým zkušenostem svou funkci zvládá bez problému sám. Pro své uživatelské činnosti využívá jiného účtu se standardním uživatelským nastavením.

## 2.8 Analýza komunikační infrastruktury

Datová síť je realizována pomocí UTP kabelů kategorie 5e, umožňující teoretickou přenosovou rychlost 1000 MBit/s. Trasy jsou vedeny v chráničkách ve zdech budov, případně v kabelových žlabech. Kabeláž neobsahuje žádnou ochranu, upozorňující na narušení kabelážního systému a neobsahuje žádné bezpečnostní prvky nultého ani druhého stupně.

Ve všech objektech jsou vytvořeny sítě LAN, do kterých jsou připojeny všechny PC, ať už stolní či přenosné s výjimkou stařičkého stolního počítače ve školní družině. Sítě v budovách 2 a 3 jsou bezdrátově, pomocí antén na střechách budov, spojeny do jedné školní sítě. Síť v budově 1 je prozatím samostatná, ale v létě 2016 je v plánu připojit i tuto budovu do jedné, velké školní sítě.

Z důvodu pohodlného připojení k síti se škola rozhodla vybudovat bezdrátovou síť s přístupem k interním datům, uloženým na serveru i Internetu, jejíž WIFI signál bude pokrývat všechny školní prostory. V současné chvíli probíhá realizace projektu, během které dojde k výměně starých switchů za nová zařízení značky ZyXEL, které umožní nasazení pokročilých technologií, včetně virtuálních sítí VLAN. Každá z budov bude osazena několika switchi, ke kterým budou připojeny jednotlivé přístupové body. Celkově bude takto po budovách rozmístěno 14 AP, které zajistí pokrytí WIFI signálu ve všech školních prostorách.

V budově č. 3, konkrétně v učebně IVT, je umístěn server, jenž je připojen k záložnímu zdroji elektrické energie UPS, který však momentálně není funkční z důvodu vadné baterie. Server je umístěn na koberci v rohu učebny, ta je uzamčena a žáci do ní mají přístup pouze s vyučujícím. Server je vybaven operačním systémem Microsoft Windows Server 2008 a je na něm aktivována služba Active Directory, zabezpečující přístupová práva jednotlivých uživatelů (viz. kapitola 2.7 - Kategorizace uživatelů). Dále na tomto serveru běží služba DNS, DHCP a server také slouží pro sdílení diskového prostoru. Data na serveru jsou zabezpečena metodou RAID.

**Technické parametry serveru:**

Operační systém: Windows Server 2008 Standard Edition

Procesor: Intel® Xeon® CPU X3220, 2.40GHz

Operační paměť: 4.00 GB RAM

HDD: 500 GB

**Obrázek č. 17: Server a tiskárna v učebně IVT**

Zdroj: (vlastní)


**Obrázek č. 18: Server umístěný na koberci v učebně IVT**

Zdroj: (vlastní)

## 2.9 Programové vybavení

Všechny počítače jsou vybaveny operačním systémem Microsoft Windows 7, dále kancelářským balíkem Microsoft Office a drobnými vzdělávacími programy, využívanými pro výuku, vše s legální licencí. Před nebezpečným softwarem jsou počítače chráněny zdarma dostupným antivirovým programem Avast. Aktualizace probíhá automaticky, přičemž je čas od času provedena kontrola aktualizací správcem sítě.

## 2.10 Informační systém

Škola využívá informační systém Bakaláři, lépe řečeno chystá se využívat. Citlivá data z aplikace Bakaláři, tedy data žáků a zaměstnanců, jsou uložena na pevném disku počítače ředitelky školy, která k nim má jako jediná přístup a která si je sama spravuje a dle svého uvážení si vytváří i kopie na externí disk. Škola se chystá postupně využívat funkcionalitu informačního systému Bakaláři od příštího školního roku, kdy budou data uložena na server, a po připojení budovy číslo 1 do školní sítě bude možné je spravovat z kteréhokoliv počítače v síti.

Hospodářský úsek využívá účetní systém Gordic, který obsahuje kompletní účetnictví. Účetní data, obsahující velmi citlivé informace, jsou uložena na počítači mzdové účetní

a ztráta těchto dat by měla na instituci vysoký vliv. Tvorba kopie těchto dat je v plné kompetenci zaměstnankyň hospodářského úseku.

## 2.11 Bezpečnost dat

Data uložená na serveru jsou zabezpečena proti jeho selhání metodou RAID. Disky na serveru jsou zapojeny do systému RAID1, takže jsou na dva disky současně ukládána stejná data a druhý disk je věrnou kopií prvního disku.

Zálohování dat není žádným způsobem řešeno. Nejcennější data (účetnictví, osobní údaje žáků a zaměstnanců) navíc leží na discích počítačů sekretářek a ředitelky. Tyto data nejsou uložena na serveru a kopii dat si provádí sama ředitelka respektive sama účetní a na externí disky. Učitelé mají možnost se přihlásit i k lokálním administrátorským účtům a tuto možnost často využívají. Veškerá data jsou pak uložena přímo na PC, nikoliv na serveru a jejich zabezpečení tak není žádným způsobem řízeno. Kopie svých dat si dle svého uvážení vytváří sami učitelé na flash disky, které mají od školy.

## 2.12 Analýza bezpečnosti dle oblastí v normě ISO/IEC 27001

Před závěrečným shrnutím analýzy současného stavu nyní doplním analýzu bezpečnosti podle oblastí definovaných v normě ISO/IEC 27001, čímž bude analýza informační bezpečnosti doplněna o údaje, které jsem neuvedl v předchozích podkapitolách.

### A.5 Politiky bezpečnosti informací

V organizaci není definována sada politik pro bezpečnost informací. Není určen směr ani podpora bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi, jak doporučuje norma ISO/IEC 27001.

### A.6 Organizace bezpečnosti informací

Nejsou definovány a přiděleny odpovědnosti za bezpečnost informací. Stejně tak chybí principy oddělení povinností jednotlivých zaměstnanců a definice pravidel pro použití mobilních zařízení a práce na dálku.

### A.7 Bezpečnost lidských zdrojů

Škola v současné době nedisponuje směrnicí, která by definovala pravidla bezpečnosti lidských zdrojů na úrovních před, během a po ukončení pracovního stavu.

### A.8 Řízení aktiv

S nárůstem počtu moderních zařízení, především těch hmotných, například interaktivních tabulí, notebooků apod., škola zavedla řízení aktiv. Každý pedagog má přidělen seznam aktiv, za která odpovídá. Typicky třídní učitel nese odpovědnost za vybavení své třídy (například PC, interaktivní tabule) a dále drobnější aktiva, jako třeba tablet, flash disk, případně externí disk.

Klasifikace informací a manipulace s médii není stanoveno.

### A.9 Řízení přístupu

Pravidla pro přístup k informacím a k vybavení pro zpracování informací není stanoven. Vytváření, rušení a nastavení uživatelských účtů je prováděno administrátorem sítě. Před začátkem školního roku je povinností správce sítě vytvořit uživatelské účty novým žákům, případně pedagogům. Stejně tak probíhá i rušení účtu žáků, kteří daný rok dokončili povinnou školní docházku. Rušení těchto účtů opět obstarává administrátor, a to obvykle na podzim následujícího školního roku.

### A.10 Kryptografie

Kryptografická opatření nejsou v organizaci využívána.

### A.11 Fyzická bezpečnost a bezpečnost prostředí

Problematika fyzické bezpečnosti a bezpečnosti prostředí byla podrobně řešena v rámci popisu jednotlivých budov v kapitolách 2.4 – 2.6.

### A.12 Bezpečnost provozu

Jak již bylo napsáno výše, před nebezpečným softwarem jsou počítače chráněny zdarma dostupným antivirovým programem Avast. Aktualizace probíhá automaticky, přičemž je „čas od času“ provedena kontrola aktualizací správcem sítě. Problematika zálohování a bezpečnosti dat byla popsána výše v podkapitole 2.11 – Zabezpečení dat.

Síťová komunikace není žádným způsobem logována ani monitorována. Právo na instalaci a aktualizaci softwaru na koncových stanicích má pouze administrátor sítě.

### A.13 Bezpečnost komunikací

Bezpečnost komunikací byla rozebrána v kapitole Analýza komunikační infrastruktury.

### A.14 Akvizice, vývoj a údržba systémů

Škola „využívá“ nebo lépe řečeno se chystá využívat informační systém Bakaláři. Tento informační systém je vyvíjen a udržován třetí stranou, proto pravidla bezpečnosti nejsou

ve škole definována. To samé platí i pro informační systém Gordic, který je taktéž vyvíjen i udržován třetí stranou.

### A.15 Dodavatelské vztahy

Škola nezaměstnává žádné externí pracovníky. Jediným dodavatelem, se kterým má škola smlouvu, je firma Tlapnet, s.r.o., která se smluvně zavazuje k poskytování Internetového připojení.

### A.16 Řízení incidentů bezpečnosti informací

Problematika řízení bezpečnostních incidentů není definována. Vznikne-li incident, řeší jej administrátor sítě, a jelikož se jedná o základní školu, tak výchovnou část incidentu přebírá výchovný poradce. Dokumentace zaznamenávající vzniklé incidenty a jejich řešení není vedena.

### A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

Organizace nedisponuje Disaster Recovery Planem.

### A.18 Soulad s požadavky

Škola, jakožto městem provozovaná instituce, splňuje požadavky stanovené státem.

## 2.13 Souhrn analýzy současného stavu

Po provedené analýze je nejbolestivější oblastí jednoznačně fyzická bezpečnost a bezpečnost prostředí, která by v případě základní školy, s ohledem na aktuální situaci, rozhodně neměla být podceňována.

Dalším slabým místem je, že si vedení školy patrně neuvědomuje, s jak citlivými daty disponuje. Jedná se především o osobní data žáků a účetní data. Tím mám na mysli jejich rodné číslo, datum narození, adresu trvalého bydliště, pohlaví, státní občanství. Nejedná se však pouze o data o jednotlivých žácích, ale i jejich rodičích, případně jiných příbuzných. Taková data mohou být zneužita, v lepším případě pro cílené firemní nabídky různého zboží.

S výše uvedeným souvisí i problematika zálohování, která není řešena. Data uložená na serveru jsou sice zabezpečena metodou RAID, která zabezpečuje data proti selhání pevného disku, ale nechrání data před omylným či úmyslným smazáním, například vlivem viru.

Dalším tématem je realizace nové bezdrátové sítě s přístupem k interním datům, uloženým na serveru i k Internetu, což přináší mnoho výhod. Zároveň však nelze opomenout stránku bezpečnosti, která je v případě bezdrátových sítí jednou z největších slabin. Není například žádoucí, aby byla školní síť využívána k činnostem nesouvisejícím se studiem, které nesou zvýšené riziko napadení systému. Proto by mělo být nalezeno řešení, které taková rizika eliminuje.

Závěrem provedené analýzy současného stavu tak je, že informační bezpečnost je na velmi nízké úrovni a je řešena pouze okrajově.

# 3 VLASTNÍ NÁVRH ŘEŠENÍ, PŘÍNOS PRÁCE

V této kapitole navrhnu bezpečnostní opatření, přičemž budu vycházet z přílohy A, normy ČSN ISO/IEC 27001. Návrh vybraných bezpečnostních opatření se bude týkat především těch oblastí, které budou identifikovány analýzou rizik jako nejohroženější, tzn. u těch, u kterých dochází k nejzásadnějšímu pochybení a u kterých je nutné co nejdříve sjednat nápravu. U některých oblastí pak podám konkrétní návrhy, jak změny realizovat, případně doplním o doporučení, vycházející z příslušných norem.

## 3.1 Identifikace rizik

Norma ISO/IEC 27001 specifikuje, že přijaté bezpečnostní opatření musí být založeno na riziku. Návrhu opatření tak předchází analýza rizik, která tento požadavek pomůže splnit. Účelem identifikace rizik je určit, co by mohlo způsobit potencionální ztrátu a také jak, kde a proč k takové ztrátě může dojít. V následujících krocích budou shromážděna vstupní data pro činnost posouzení rizik. Identifikace rizik by dále měla být prováděna v pravidelných intervalech (alespoň 1x ročně) určených bezpečnostním manažerem. Výstupem identifikace rizik je přehled, který k identifikovaným aktivům přiřazuje pro jednotlivé hrozby koeficienty rizik.

### 3.1.1 Identifikace aktiv

Prvním krokem je identifikace aktiv a následně jejich ohodnocení, tedy určení velikosti dopadů při ohrožení důvěrnosti, dostupnosti nebo integrity. Pro jejich ohodnocení navrhuji použít klasifikační schéma zobrazené v tabulce č. 3.

**Tabulka č. 3: Tabulka pro hodnocení aktiv**

| Hodnota | Hodnota aktiva slovy | Hodnocení dopadu |
|---|---|---|
| 1 | Žádná | Žádný dopad na organizaci |
| 2 | Zanedbatelná | Zanedbatelný dopad na organizaci |
| 3 | Malá | Malý dopad na organizaci |
| 4 | Významná | Vážné potíže organizace |
| 5 | Velmi velká | Velmi vážné potíže organizace |

Zdroj: vlastní zpracování dle (3)

V následující tabulce je již přehled jednotlivých aktiv a jejich hodnocení. Identifikace aktiv byla provedena ve spolupráci s vedením školy na vhodném stupni podrobnosti, který poskytne pro řízení rizik dostatečné množství informací. Pro výpočet hodnoty aktiva byl využit součtový algoritmus uvedený v teoretických východiscích práce.

**Tabulka č. 4: Identifikace aktiv**

| Aktivum | Dopad | | | Hodnota |
|---|---|---|---|---|
| | Dostupnost | Integrita | Důvěrnost | |
| notebook | 3 | 3 | 3 | 3 |
| pracovní stanice vedení školy | 5 | 4 | 5 | 5 |
| server | 4 | 3 | 4 | 4 |
| tištěné smlouvy | 3 | 4 | 5 | 4 |
| účetnictví | 5 | 4 | 4 | 4 |
| síťové prvky a kabeláž | 3 | 3 | 4 | 3 |
| osobní údaje žáků | 4 | 5 | 5 | 5 |
| osobní údaje pracovníků | 4 | 5 | 4 | 4 |
| kopie dat | 4 | 4 | 5 | 4 |

Zdroj: vlastní zpracování

### 3.1.2 Identifikace hrozeb

V okamžiku, kdy jsou definována aktiva důležitá pro chod organizace, je na řadě identifikace hrozeb. Nejprve opět uvedu klasifikační schéma pravděpodobnosti hrozeb (tabulka č. 5).

**Tabulka č. 5: Klasifikační schéma pravděpodobností hrozeb**

| Hodnota | Pravděpodobnost |
|---|---|
| 1 | Velmi malá až žádná |
| 2 | Nízká |
| 3 | Střední |
| 4 | Vysoká |
| 5 | Velmi vysoká |

Zdroj: vlastní zpracování

Dalším krokem je již konkrétní identifikace hrozeb, která vznikla po konzultaci s vedením školy a správcem sítě. V tabulce č. 6 jsou vyjmenovány hrozby, které mohou uvedená aktiva znehodnotit a subjektivní hodnocení jednotlivých hrozeb. V seznamu je pro každou hrozbu uveden i typ relevantního zdroje dle ISO/IEC 27005:

**A – accindental** – náhodný – použito pro lidské činnosti, které mohou následně poškodit informační aktiva

**D – deliberate** – úmyslný – použito pro úmyslné akce zaměřené na aktiva

**E – enviromental** – environmentální – použito pro všechny incidenty, které nejsou založeny na lidské činnosti.

**Tabulka č. 6: Tabulka hrozeb a jejich pravděpodobností**

| Typ | Hrozba | Zdroj | Pravděpodobnost |
|---|---|---|---|
| Fyzické poškození | Požár | A, D, E | 1 |
| Ztráta základních služeb | Přerušení dodávky elektřiny | A, D, E | 2 |
| Ohrožení informací | Krádež médií nebo dokumentů | D | 3 |
| | Krádež zařízení | D | 3 |
| Technická selhání | Chybné fungování zařízení (porucha SW) | A | 3 |
| | Selhání zařízení (porucha HW) | A | 3 |
| Neoprávněné činnosti | Neoprávněné použití zařízení | D | 4 |
| | Neoprávněný přístup do budovy školy | D | 4 |
| | Ztráta dat | D | 4 |

Zdroj: vlastní zpracování dle (9)

### 3.1.3 Matice zranitelnosti

Dalším krokem je vytvoření matice zranitelnosti, která udává zranitelnost aktiv vůči konkrétním hrozbám.

**Tabulka č. 7: Matice zranitelnosti**

| **Zranitelnost V** | **Popis aktiva** | Ntb | pracovní stanice vedení školy | server | tištěné smlouvy | Účetnictví | Síťové prvky a kabeláž | osobní údaje žáků | osobní údaje pracovníků | kopie dat |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Hodnota aktiva A** | 3 | 5 | 4 | 4 | 4 | 3 | 5 | 4 | 4 |
| **Hrozba** | **Pravděpodobnost T** | | | | | | | | | |
| Požár | 1 | 4 | 4 | 4 | 4 | 3 | 3 | 3 | 3 | 4 |
| Přerušení dodávky elektřiny | 2 | 1 | 4 | 4 | | 4 | 3 | 2 | 2 | 3 |
| Krádež médií nebo dokumentů | 3 | 0 | 0 | 0 | 5 | 5 | 0 | 3 | 3 | 0 |
| Krádež zařízení | 3 | 3 | 4 | 3 | 0 | 5 | 2 | 4 | 4 | 4 |
| Chybné fungování zařízení (porucha SW) | 3 | 3 | 4 | 3 | 0 | 4 | 0 | 0 | 0 | 0 |
| Selhání zařízení (porucha HW) | 3 | 3 | 3 | 3 | 0 | 4 | 3 | 3 | 3 | 4 |
| Neoprávněné použití zařízení | 4 | 3 | 5 | 4 | 0 | 0 | 3 | 4 | 4 | 4 |
| Neoprávněný přístup do budovy školy | 4 | 2 | 5 | 4 | 4 | 4 | 2 | 5 | 5 | 5 |
| Ztráta dat | 4 | 3 | 5 | 3 | 3 | 4 | 0 | 4 | 4 | 4 |

Zdroj: vlastní zpracování dle (3)

### 3.1.4 Matice rizik

Poslední tabulkou a výsledkem podkapitoly identifikace rizik je matice rizik, udávající míru rizik u jednotlivých aktiv.

Tabulka č. 8 udává slovní popis rizik na základě jejich vypočtené míry. Míra rizika byla vypočtena jako součin pravděpodobnosti T, hodnoty aktiva A a zranitelnosti V. Rizika byla klasifikována do tří skupin, na základě kterých bude k jednotlivým rizikům přistupováno.

**Tabulka č. 8: Klasifikace rizik**

| Hranice rizika | Míra rizika |
|---|---|
| <33 | Nízká |
| 34-66 | Střední |
| > 67 | Vysoká |

Zdroj: vlastní zpracování

**Tabulka č. 9: Matice rizik**

| **Riziko** | **Popis aktiva** | notebook | pracovní stanice vedení školy | server | tištěné smlouvy | Účetnictví | Síťové prvky a kabeláž | osobní údaje žáků | osobní údaje pracovníků | kopie dat |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Hodnota aktiva** | 3 | 5 | 4 | 4 | 4 | 3 | 5 | 4 | 4 |
| **Hrozba** | **Pravděpodobnost** | | | | | | | | | |
| Požár | 1 | 12 | 20 | 16 | 16 | 12 | 9 | 15 | 12 | 16 |
| Přerušení dodávky elektřiny | 2 | 6 | 40 | 32 | 0 | 32 | 18 | 20 | 16 | 24 |
| Krádež médií nebo dokumentů | 3 | 0 | 0 | 0 | 60 | 60 | 0 | 45 | 36 | 0 |
| Krádež zařízení | 3 | 27 | 60 | 36 | 0 | 60 | 18 | 60 | 48 | 48 |
| Chybné fungování zařízení (porucha SW) | 3 | 27 | 60 | 36 | 0 | 48 | 0 | 0 | 0 | 0 |
| Selhání zařízení (porucha HW) | 3 | 27 | 45 | 36 | 0 | 48 | 27 | 45 | 36 | 48 |
| Neoprávněné použití zařízení | 4 | 36 | 100 | 64 | 0 | 0 | 36 | 80 | 64 | 64 |
| Neoprávněný přístup do budovy školy | 4 | 24 | 100 | 64 | 64 | 64 | 24 | 100 | 80 | 80 |
| Ztráta dat | 4 | 36 | 100 | 48 | 48 | 64 | 0 | 80 | 64 | 64 |

Zdroj: vlastní zpracování dle (3)

### 3.1.5 Vyhodnocení identifikace rizik

Výše zpracovaná analýza rizik splnila svůj účel, tedy identifikovala největší rizika a velikost jejich dopadu v případě naplnění bezpečnostních hrozeb. Identifikovaná rizika byla rozdělena do tří kategorií (dle tabulky č. 8 – klasifikace rizik). Na základě výsledků analýzy rizik nyní navrhnu bezpečnostní opatření, která budou v souladu s normou ČSN ISO/IEC 27001. Největší rizika plynou ze ztráty dat, neoprávněného přístupu do budov školy a s tím souvisejícím neoprávněným použitím zařízení. Aplikace bezpečnostních opatření bude vycházet z doporučení normy ISO/IEC 27002.

## 3.2 Stanovení rozsahu ISMS

Vedení školy stanovilo rozsah ISMS na veškerý HW, SW, žáky, zaměstnance včetně dalších osob, které ve škole vykonávají libovolnou práci.

## 3.3 Vůdčí role

V souladu s požadavky ČSN ISO/IEC 27001 se vedení školy písemně zaváže k plné podpoře zavádění ISMS a přijetí závazku podporovat a prosazovat Politiku bezpečnosti informací.

## 3.4 Plánování

Proces řízení rizik bezpečnosti informací byl proveden v úvodu této kapitoly. Na základě vyhodnocení identifikace rizik budou nyní navržena bezpečnostní opatření, která sníží pravděpodobnost jejich vzniku nebo jejich dopad. Rizika byla v analýze rozdělená do tří skupin dle jejich hodnoty.

Navrhuji, aby rizika spadající do skupiny „Nízká hodnota rizika“ byla rovnou podstoupena a nebudu se jimi v této práci více zabývat. **Je nutné však tato podstoupená rizika sledovat pro případ zvýšení jejich míry a v případě potřeby s těmito riziky včas pracovat.**

Moje pozornost bude upřena především na rizika z kategorie „Vysoká hodnota rizika“ a „Střední hodnota rizika“, pro která navrhnu bezpečnostní opatření.

Protože se škola nebude ucházet o certifikaci ISMS, není třeba zavádět všechna bezpečnostní opatření. Z důvodu velkého množství opatření, které by bylo vhodné

implementovat, navrhuji, aby byla vybraná opatření a jejich implementace rozdělena do více etap.

**V první etapě implementace budou navržena pouze vybraná bezpečnostní opatření z oblastí, které z analýzy rizik vzešly jako kritické a nejohroženější a jejich další ignorace by mohla mít velké negativní následky na bezpečnost organizace.**

Na základě provedené analýzy byly do první fáze implementace vybrány následující oblasti dle ISO/IEC 27001:

- A.5 Politiky bezpečnosti informací
- A.6 Organizace bezpečnosti informací
- A.7 Bezpečnost lidských zdrojů
- A.8 Řízení aktiv
- A.9. Řízení přístupu
- A.11 Fyzická bezpečnost a bezpečnost prostředí
- A.12 Bezpečnost provozu
- A.13 Bezpečnost komunikací

## 3.5 Návrh na zavedení nejnutnějších oblastí ISMS

Nyní popíši vybraná bezpečnostní opatření z výše uvedených oblastí. Všechna navrhovaná opatření jsou v souladu s normou ISO/IEC 27002 a přizpůsobená potřebám školy.

### 3.5.1 Oblast A.5 - Politiky bezpečnosti informací

#### A.5.1 Směřování bezpečnosti informací vedením organizace

Cíl: „*Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi.“ (7, s. 14)*

#### A.5.1.1 Politiky pro bezpečnost informací

Opatření: Navrhuji definovat soubor politik pro bezpečnost informací ve formě dokumentu. Bezpečnostní politika organizace vyjadřuje postoj vedení školy k zajištění bezpečnosti informací. Předmětem bezpečnostní politiky je stanovení cílů a odpovědnosti pro zajištění ochrany informačních aktiv z hlediska důvěrnosti, integrity a dostupnosti. Organizace se dokumentem zaváže zajistit zpracování, řízení a uchování informací adekvátními bezpečnostními postupy. **Všichni** zaměstnanci a žáci budou s bezpečnostní

politikou seznámeni a budou odpovědni za její dodržování. Politika bude plně podporována a schválena ředitelkou školy.

Účelem bezpečnostní politiky je dosažení následujících cílů:

- Zachování důvěrnosti informací
- Zachování dostupnosti informací autorizovaným uživatelům v případě potřeby
- Zachování integrity informací
- Zajištění školení v oblasti bezpečnosti informací pro všechny zaměstnance a žáky, případně smluvní třetí strany

Formulace politik bezpečnosti informací: 8 hodin

#### A.5.1.2 Přezkoumávání politik pro bezpečnost informací

Opatření: Politiku bezpečnosti informací je třeba pravidelně revidovat. Tuto činnost bude mít na starost vedení instituce či jím pověřená osoba a bude ji provádět jednou ročně. V případě zjištění nedostatku je povinností bezpečnostního manažera vypracovat politiku novou, která bude muset být schválena vedením školy. Toto opatření zajistí neustálou vhodnost, přiměřenost a efektivnost bezpečnostní politiky.

Přezkoumávání politik bezpečnosti informací: 8 hodin/rok

### 3.5.2 Oblast A.6 - Organizace bezpečnosti informací

#### A.6.1 Interní organizace

Cíl: *„Ustavit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.“ (7, s. 14)*

#### A 6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Politika je tvořena a posuzována vedením organizace a za uplatnění této politiky odpovídá bezpečnostní manažer. Všichni zaměstnanci a žáci školy se řídí postupy v souladu s touto politikou. Stejně tak jsou obě skupiny odpovědny za okamžité hlášení bezpečnostních incidentů a jakýchkoliv zjištěných slabin. Úmyslné činy vedoucí k ohrožení bezpečnosti informací školy mohou být předmětem až soudního řízení.

Navrhuji, aby dále ředitelka školy definovala následující role, které ponesou následující odpovědnosti:

- **Bezpečnostní manažer**
    - Přímý podřízený ředitelky školy
    - Odpovědný za bezpečnost informací v organizaci
    - Prosazuje bezpečnostní politiku
    - Koordinuje zavádění bezpečnostních opatření
    - Koordinuje školení zaměstnanců i žáků v oblasti informační bezpečnosti
    - Vyhodnocuje dodržování bezpečnostních opatření ve všech oblastech informační bezpečnosti
    - Navrhuje změny bezpečnostní politiky, směrnic a dalších dokumentů
    - Slouží jako poradenská podpora zaměstnancům a žákům

- **Administrátor**
    - Přímý podřízený ředitelky školy
    - Realizuje opatření k zajištění bezpečnosti informací
    - Dohlíží na aplikaci bezpečnostních opatření z hlediska použitých technologií
    - Řešící bezpečnostní události
    - Zajišťující informační bezpečnost z technického hlediska
    - Slouží jako poradenská podpora zaměstnancům a žákům

Tyto dvě role musí být vykonávány **dvěma** osobami. Není-li to z důvodu nedostatku kvalifikovaných personálních zdrojů možné, existuje tu možnost **outsourcingu** této funkce, kterou v dnešní době nabízí několik firem.

#### A.6.1.2 Princip oddělení povinností

Opatření: Doporučuji oddělit neslučitelné povinnosti a odpovědnosti, což zabrání neoprávněné nebo neúmyslné modifikaci či zneužití aktiv.

Definice rolí a odpovědnosti, oddělení povinností: 10 hodin

### 3.5.3 Oblast A.7 – Bezpečnost lidských zdrojů

#### A.7.2 Během pracovního vztahu

Cíl: *„Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací.“ (7, s. 15)*

#### A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Opatření: Jedním z dílčích cílů této práce je nastartovat budování či zlepšení povědomí o ISMS u všech zaměstnanců i žáků základní školy. Tato problematika bude podrobně rozebrána v kapitole 3.7.

Vypracování školícího programu: 24 hodin + 8 hodin/rok obnova

Školení bezpečnostního manažera: 10 hodin ročně/ cca 25 000 Kč.

Školení zaměstnanců: 8 hodin/rok

Školení žáků: 16 hodin/rok

### 3.5.4 Oblast A.8 - Řízení aktiv

#### A.8.1 Odpovědnost za aktiva

Cíl: *„Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.“ (7, s. 15)*

#### A.8.1.1 Seznam aktiv

Opatření: Doporučuji stanovit pravidla pro evidenci aktiv. Rozšířit současný seznam o všechna aktiva, která jsou v rámci systému řízení bezpečnosti informací organizaci účelná a je vhodné je systematicky registrovat.

Tento seznam identifikovaných aktiv doporučuji evidovat v elektronické podobě. Registr aktiv by měl být průběžně (alespoň 1x ročně) aktualizován bezpečnostním manažerem a schválen ředitelkou školy. Seznam bude obsahovat název aktiva, míru důležitosti jeho ochrany z hlediska zachování dostupnosti, důvěrnosti a integrity a jeho vlastníka.

Aktualizace seznamu aktiv: 4 hodiny/rok

#### A.8.1.2 Vlastnictví aktiva

Opatření: Jak bylo uvedeno v předchozím bodě, každému aktivu bude přiřazen jeho vlastník. Vlastník, odpovědný za aktivum, si musí být vědom své odpovědnosti při nakládání s informacemi a za přidělená aktiva a měl by ji stvrdit svým podpisem. Informace a aktiva smějí zaměstnanci využívat výhradně k plnění pracovních úkolů a jakékoliv neoprávněné využití informací či aktiv bude považované za vážné porušení bezpečnostní politiky.

Přiřazení vlastníků aktiv: 4 hodiny + 1 hodina/rok

### A.8.2 Klasifikace informací

Cíl: „*Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.“ (7, s. 16)*

#### A.8.2.1 Klasifikace informací

Opatření: Účelem je stanovit pravidla pro klasifikaci informací a způsob, jak s klasifikovanými informacemi nakládat. Navrhuji použít třístupňovou klasifikaci informací, kde stupeň vyjadřuje míru důvěrnosti informace:

1. Stupeň – veřejné informace
2. Stupeň – interní informace
3. Stupeň – citlivé informace

**Veřejné informace**

Do 1. klasifikačního stupně patří široký okruh informací, které nemají z hlediska důvěrnosti omezení, např. informace poskytované na veřejných webových stránkách školy, propagační materiály určené veřejnosti atd.

**Interní informace**

Do 2. klasifikačního stupně patří informace, které jsou z hlediska důvěrnosti určeny zaměstnancům školy v souladu s jejich pracovní činností a zároveň nejsou určeny pro veřejnost, např. příkazy ředitelky školy.

**Citlivé informace**

Do 3. klasifikačního stupně patří informace, které jsou z hlediska důvěrnosti klasifikovány jako citlivé a jsou určeny pouze pověřeným zaměstnancům organizace, např. pracovní smlouvy, osobní údaje žáků, zaměstnanců atd.

Klasifikace aktiv: 6 hodin

#### A.8.2.2 Označování informací

Opatření: Doporučuji vypracovat postup pro označování informací do výše uvedených kategorií. Tento postup označování informací by měl být známý všem zaměstnancům. Povinné značení informací doporučuji minimálně stupeň č. 3 – Citlivé informace. Označování ostatních informací je na zvážení vedení školy, je možné ho vynechat z důvodu zjednodušení práce.

Formulace postupu pro označování informací: 4 hodiny

### A.8.3 Manipulace s médii

Cíl: *„Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích.“ (7, s. 16)*

#### A.8.3.2 Likvidace a vyřazení zařízení

Opatření: Administrátor bude odpovědný za to, že všechna paměťová média, která obsahují licencovaný software, neveřejné či interní informace, byla před vyřazením nebo likvidací nenávratně smazána či fyzicky zničena. Likvidace nebo vyřazení jednotlivých zařízení musí být schváleny ředitelkou školy. Postup pro bezpečnou likvidaci by měl být opět písemně definován a stvrzen podpisem osobou odpovědnou za tuto činnost.

Formulace postupu likvidace a vyřazení zařízení: 1 hodina

### 3.5.5 Oblast A.9 - Řízení přístupu

#### A.9.2 - Řízení přístupu uživatelů

Cíl: *„Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám.“ (7, s. 14)*

#### A.9.2.1 Registrace a zrušení registrace uživatele

Opatření: Současný stav registrace a rušení registrace uživatelů považuji za vyhovující. Doporučuji však nepoužívat univerzální účty a zamezit možnosti přihlášení se běžným uživatelům k lokálnímu administrátorskému účtu na všech PC.

#### A.9.4 Řízení přístupu k systémům a aplikacím

Cíl: *„Předcházet neautorizovanému přístupu k systémům a aplikacím.“ (7, s. 17)*

#### A.9.4.3 Systém správy hesel

Opatření: Řádná autentizace musí být zajištěna heslem. Za volbu a ochranu svého hesla odpovídají sami uživatelé. Hesla musí být uchována v tajnosti. V případě, že se uživatel vzdálí od svého PC, je povinen ho uzamknout (klávesová zkratka CTRL + ALT + DELETE a volba „uzamknout tento počítač). Pro vytváření hesla k uživatelským účtům navrhuji několik pravidel. Uživatelé z kategorie Pedagog jsou povinni používat silné heslo, tj. minimálně 8 pozic, které obsahují současně malá a velká písmena a číslice. Za zvážení stojí povinná pravidelná změna hesla, například 1x za rok.

Pro uživatele, spadající do kategorie žák, navrhuji požadovat alespoň slabé heslo, tj. heslo, které nesplňuje požadavky pro silné heslo (libovolný počet znaků, bez omezení

velkých/malých písmen, čísel atd.). Současný stav používání hesel vytvořených podle jednotných pravidel z uživatelského jména pro všechny žáky je nepřijatelný. Dětem je potřeba odmala připomínat důležitost používání hesel a dalších bezpečnostních návyků. Pro případ, že dítě zapomene heslo ke svému účtu, navrhuji vytvořit univerzální účet se stejnými právy (stejnými jako účty žáků), jehož heslo bude znát pouze pedagog, který žáka přihlásí. Vyučující poté informuje administrátora o nutnosti resetování hesla k účtu žáka. Uživatelé by si měli heslo pamatovat a nikde si ho nezapisovat!

Definice pravidel pro správu hesel: 2 hodiny

### 3.5.6 Oblast A.11 - Fyzická bezpečnost a bezpečnost prostředí

#### A.11.1 Bezpečné oblasti

Cíl: *„Předcházet neautorizovanému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.“ (7, s. 14)*

#### A.11.1.2 Fyzické kontroly vstupu

Škola by měla mít pod kontrolou vstup do objektu, tudíž každá osoba, vstupující do prostor školy, musí projít autorizací vstupu. Opatření řešící fyzickou kontrolu vstupu je podrobně řešeno v kapitole 3.6.

#### A.11.2 Zařízení

Cíl: *„Přecházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.“ (7, s. 18)*

#### A.11.2.1 Umístění zařízení a jeho ochrana

Opatření: Jedná se především o zařízení, které poskytují podpůrné služby koncovým zařízením, tedy server a další síťové aktivní prvky. Z důvodu charakteru místa, kde je mnoho mladých lidí s dostatkem energie a nápadů, mohou být aktivní prvky vystaveny úmyslným i neúmyslným škodám. Proto pro zamezení přístupu k nim by měly být nainstalovány tak vysoko, jak to jen bude možné a zároveň tak, aby bylo zabráněno nechtěné manipulaci či poškození.

Učebna IVT, ve které je umístěn server, je zajištěna dvěma zámky a žáci se do ní nedostanou bez přítomnosti vyučujícího. Okna učebny jsou navíc opatřeny mřížemi. Server tak může zůstat na stávajícím místě, tedy v rohu učebny, pouze by neměl být umístěn na koberci, ale doporučuji ho umístit minimálně 35 cm nad podlahu a to alespoň

na dřevěnou desku. Tuto úpravu doporučuji jednak z důvodu rizika zatopení učebny (nachází se pod úrovní zemského povrchu) a také z důvodu velkého množství prachu, který je serverem nasáván přímo z koberce.
Časová náročnost opatření: 4 hodiny

#### A.11.2.2 Podpůrné služby

Opatření: Doporučuji, aby minimálně server a počítače vedení školy byly vybaveny nepřerušitelným zdrojem napájení, včetně přepěťové ochrany. Tento zdroj by měl zajistit funkčnost všech zařízení minimálně na dobu 5 minut při výpadku dodávky elektrické energie. Tato doba by měla být dostatečná pro uložení a ukončení rozdělané práce a bezpečné vypnutí počítače. Pro server doporučuji UPS zdroj s výkonem 1500VA, jehož předpokládané finanční náklady na pořízení se pohybují v cenovém rozmezí 10 – 15 000 Kč. Cena záložního zdroje elektrické energie pro PC vedení školy se bude pohybovat v rozmezí v cenovém rozmezí od 2 do 3 000 Kč.

Instalace UPS zdrojů: 2 hodiny
Finanční náklady na pořízení UPS: 17 000 Kč.

### 3.5.7 Oblast A.12 - Bezpečnost provozu

#### A.12.3 Zálohování

Cíl: „*Chránit proti ztrátě dat.“ (7, s. 19)*

#### A.12.3.1 Zálohování informací

Opatření: V současné době data nejsou zálohována. Tvorba kopií dat na flash paměti, případně přenosné HDD je nebezpečné z důvodu přinášení nebezpečného obsahu do školní sítě. Takový obsah může porušit integritu dat a ohrozit fungování školy. Navíc by tento proces měl být zautomatizován.
Doporučuji proto sestavit směrnici pro zálohování dat, která bude definovat:

- Jaká data se budou zálohovat
- Kam se budou data zálohovat
- Jak často a jakým způsobem
- Kdo je za zálohování odpovědný
- Kdo bude mít k zálohám přístup
- Kolik záloh se bude uchovávat zpětně

Jedním z možných a v současné době moderních řešení je cloudové zařízení. Jedná se o dnes již cenově dostupné řešení. Doporučuji pořídit síťové úložiště NAS, které zabezpečí zálohování a zajistí eliminaci škod v případě HW poruchy serveru.
Síťové úložiště by mělo být uloženo na bezpečném místě tak, aby bylo zabráněno přístupu neoprávněným osobám. Zároveň by se mělo nacházet v jiné budově, než se nachází server. Nebudou-li dodrženy výše uvedené podmínky, postrádá celé řešení smysl.
Jako příklad uvádím Western Digital My Cloud EX4 se čtyřmi pozicemi a výslednou kapacitou až 12 TB. Předpokládané náklady na pořízení síťového úložiště jsou 20 000 Kč v závislosti na technických parametrech.
Druhou možností je pak využívat služby některé ze společností, které nabízí zálohování dat. Data jsou pak uložena obvykle ve dvou geograficky odlišných datových centrech. Cena služby je závislá na množství zálohovaných dat, pohybuje se kolem 20 Kč/GB měsíčně.
Návrh směrnice pro zálohování je uveden v příloze č. 1.

### 3.5.8 Oblast A.13 – Bezpečnost komunikací

#### A.13.1 Bezpečnost síťových služeb

Cíl: *„Zajistit ochranu informací v sítích a jejich podpůrných prostředích pro zpracování informací.“ (7, s. 20)*

#### A.13.1.3 Princip oddělení v sítích

Opatření: Vzhledem k nasazení pokročilých technologií v rámci vybudování bezdrátové sítě, doporučuji vytvořit dvě bezdrátové WIFI sítě, což zajistí oddělení bezdrátové sítě pro školní zařízení s přístupem k interním zdrojům od sítě pro žáky a návštěvníky školy, kteří budou mít přístup pouze do Internetu, a to navíc pouze omezenou rychlostí. Síť určenou pro školní zařízení doporučuji zabezpečit pomocí šifrování WPA2 a filtrováním na úrovni MAC adres, jakožto vstupní podmínkou do vnitřní školní sítě. Tabulka MAC adres, obsahující zařízení s povolením přístupu do školní sítě, by byla uložena na centrálním zařízení, odkud by byla dostupná pro další síťové prvky. Pro obě sítě navrhuji využít webové filtrování Content filtering, který poskytuje firma ZyXEL, díky němuž lze blokovat přístupy na všechny sociální sítě, pornografie a jiné potencionálně nebezpečné stránky.
Časová náročnost opatření: 6 hodin

## 3.6 Fyzické kontroly vstupu

Současný způsob řízení fyzického přístupu do budov není vhodný. Stačí připomenout hrůzný útok na žáky střední školy, který se odehrál v polovině října roku 2014 ve Žďáru nad Sázavou, který jsem připomněl hned v úvodu této diplomové práce. **Ochrana zdraví a životů žáků a zaměstnanců by měla být prioritou každého zřizovatele.**

Pro zvýšení fyzické kontroly vstupu se nabízí několik opatření. Jedním z nich, které zároveň doporučuji, je instalace přístupového systému, který pomůže omezit pohyb neoprávněných osob v prostorách školy. Zabezpečí se tím tak nejen školní majetek před loupeží či poškozením, ale především bezpečnost žáků. Přístupový systém je vhodné zároveň kombinovat se systémem docházkovým, který umožní sledovat a vyhodnocovat docházku žáků i zaměstnanců v reálném čase. V následující podkapitole se pokusím shrnout několik doporučení, které by škola neměla opomenout při tvorbě podkladů ke zpracování cenové nabídky do výběrového řízení na realizaci veřejné zakázky.

### 3.6.1 Přístupový systém

Škola by měla určit vždy jeden vchod v každé budově, který budou pro vstup do školy používat všichni žáci a zaměstnanci. Na tyto vchody doporučuji nechat nainstalovat snímací zařízení, které omezí vstup neoprávněných osob do prostor školy. Kromě všech hlavních vchodů doporučuji zabezpečit stejným mechanizmem i oba průchody do spojovacích chodeb.

**Obrázek č. 19: Snímací zařízení**
Zdroj: (19)

K identifikaci osob bude použito identifikátoru, kterým by mohl být například čip, který již většina žáků a zaměstnanců využívá ke stravování ve školní jídelně. Po přiložení identifikačního prvku k zařízení systém na základě nastavených přístupových práv umožní či zamezí otevření dveří. Systém tak umožní zaznamenat a regulovat vstup a pohyb osob do jednotlivých prostor školy.

I s takovýmto opatřením však zůstává riziko, že se vstupujícím žákem či jinou osobou, vejde do budovy i nežádoucí osoba. Z toho důvodu navrhuji, aby byly na školou určené hlavní vchody do zádveří nainstalovány turnikety, které umožní průchod pouze po řádné identifikaci, ke které dojde po přiložení stejného identifikačního prvku. Po přiložení identifikátoru k docházkovému terminálu umístěnému na turniketu, dojde k zaevidování průchodu dané osoby a k získání úplných docházkových záznamů.

Turnikety je vhodné doplnit o zábrany s výplní (aby ji nebylo možné prolézt) a minimální výškou 150 cm, které nebude možné jednoduše překonat. Doporučuji použít i elektronickou zábranu, která v případě překonání turniketu nepovoleným způsobem spustí zvukový poplach.

**Obrázek č. 20: Ukázka použití turniketů**

Zdroj: (19)

Jak bylo psáno v úvodu, tak celkově školu navštěvuje 426 žáků. Vzhledem k situaci, že žáci jsou téměř rovnoměrně rozděleni do 3 budov a turnikety jsou běžně schopny odbavit 30-40 osob za minutu, postačí pro každý hlavní vstup/budovu 1 turniket. Turnikety by měly být odolné vůči případnému nevhodnému chování.

Jedním z požadavků školy by měla být i možná integrace do informačního systému Bakaláři, díky které budou moci rodiče snadno přes webovou aplikaci sledovat, kdy jejich dítě přišlo a především kdy opustilo budovu školy. Systém tak pomůže zvýšit bezpečnost dětí a zároveň předejít i možnosti případného záškoláctví a jiných výchovných problémů. Systém by měl v budoucnosti umožňovat rozšíření počtů snímacích zařízení na další vstupy, například do tříd či kabinetů.

V podkladech ke zpracování cenové nabídky do výběrového řízení na realizaci veřejné zakázky se také může objevit informace o ceně, kterou by zakázka neměla překročit. Dle kvalifikovaného odhadu by měly být náklady na projekt v rozmezí 200 – 250 000 Kč v závislosti na zvoleném řešení a dodavateli.

O zavedení systému by měli být informováni všichni rodiče prostřednictvím webových stránek školy a dále by měly být aktualizovány vnitřní směrnice školy – provozní řád apod. Při příležitosti zavedení docházkově-přístupového systému doporučuji žáky vhodným způsobem seznámit s principy bezpečného prostředí školy, které bude zahrnovat poučení o průchodu turnikety a správném používání identifikátorů. Stejně tak je vhodné poučit žáky o nahlášení cizí osoby, která se pohybuje ve škole bez doprovodu zaměstnance.

Dále uvádím několik návrhů, pravidel užívání systému, které by se mohly objevit v provozním řádu školy.

V čase od 7:40 do 8:00, kdy do školy přichází velké množství dětí, budou hlavní dveře otevřeny a zajištěny proti zavření. Pro průchod přes turniket bude žák/zaměstnanec, povinen přiložit identifikátor. Po celou tuto dobu by u prostoru turniketu měl situaci sledovat pověřený zaměstnanec, který má možnost v případě nefunkčního či zapomenutého čipu uvolnit rameno turniketu do polohy, umožňující volný průchod. Mimo výše uvedený čas budou hlavní dveře uzavřeny a otevřít půjdou pouze po přiložení identifikačního prvku.

Doporučuji zpracovat tabulku přístupových práv, která by mohla vypadat přibližně takto:

**Tabulka č. 10: Tabulka přístupových práv**

| Skupina | Povolený vstup | Povolená doba přístupu |
|---|---|---|
| Žáci I. stupně nedocházející do družiny | Budova č. 1 | 7:40 – 14:00 |
| Žáci I. stupně docházející do družiny | Budova č. 1 | 6:00 – 16:30 |
| Žáci 4. a 5. tříd s třídou v budově č. 2 | Budova č. 2 | 7:40 – 15:00 |
| Žáci II. stupně s výukou pouze v budově 3 | Budova č. 3 | 7:40 – 15:00 |
| Žáci II. stupně s výukou v budovách č. 2 i 3 | Budova č. 2 | 7:40 – 16:00 |
| | Budova č. 3 | 7:40 – 16:00 |
| | Spojovací chodby | 7:40 – 16:00 |
| Zaměstnanci | Všechny budovy | 5:30– 19:00 |

Zdroj: vlastní zpracování

## 3.7 Budování či zvýšení bezpečnostního povědomí

Jak již bylo zmíněno výše, útok na zdraví či životy dětí a pracovníků v dnešní době nelze vyloučit a obecně jakákoliv hrozba krizové situace je pro účastníky velice stresová, zvláště pak v prostředí plném dětí. Správné rozhodování je v takových situacích zcela zásadní, proto je důležité průběžné posilování bezpečnostního povědomí. V této části práce se však budu zabývat bezpečnostním povědomím v oblasti informačních technologií. Učením dětí informační bezpečnosti již na základní škole, je velmi často podceňováno i přesto, že důležitost IT bezpečnosti v posledních letech roste.

Základní školu navštěvují děti, které denně používají e-mailové schránky, brouzdají po Internetu a především tráví čas na sociálních sítích, které jsou fenoménem dnešní doby. Proto je nesmírně důležité, aby v nich bylo budováno bezpečnostní povědomí již od raného věku a nebylo bráno na lehkou váhu.

Další skupinou jsou zaměstnanci školy – učitelé. Stejně jako pro žáky, tak i pro učitele je ICT součástí každodenního života. Navíc v době, kdy začínají být na základních školách čím dál více populární elektronické školní informační systémy, přes které mohou rodiče

sledovat výsledky žáků a mnoho dalších informací přes Internet. Budou to právě učitelé, kteří budou zadávat a mít přístup k velice citlivým datům. I to je důvod, proč by se zvyšování bezpečnostního povědomí mělo týkat všech bez výjimky.

Cílem je dosáhnout povědomí o bezpečnosti a vybudování či zvýšení úrovně povědomí na základní škole na úroveň, kdy se bezpečnost stane rutinou, která pro nikoho nebude nutným zlem. Všichni by si měli být vědomi důležitosti dodržování alespoň těch základních bezpečnostních zásad, což lze zajistit právě pravidelným školením.

Jak již bylo zmíněno, tak se ve škole vyskytují různí uživatelé s různými potřebami a znalostmi. Proto je důležité je rozdělit do skupin tak, aby nebyli zahlceni přemírou nepodstatných informací. Otázkou bezpečnostního povědomí se zabývá například americká norma **NIST SP 800 – 50 – Building an Information Technology Security Awareness and Training Program**, která radí, jak lze na škole vytvořit a zavést školící program.

## Návrh na zavedení bezpečnostního povědomí na základní škole:

Protože se na škole vyskytuje mnoho uživatelů s různými znalostmi a vztahem k ICT technologiím, navrhuji, aby budování bezpečnostního povědomí vycházelo z kategorizace uživatelů, která byla definována v druhé kapitole této práce. Každou skupinu uživatelů je nutné školit jiným způsobem a na jiné úrovni.

Vzdělávání by tak probíhalo na třech úrovních:

### Vzdělávání bezpečnostního manažera

Tato skupina by měla porozumět dané problematice a umět odpovědět na otázky co, jak, a proč. Mělo by jim být umožněno zúčastnit se vhodných seminářů a přednášek v oblasti informační bezpečnosti s možností závěrečné certifikace. Vzdělávání této skupiny by měl být dlouhodobý a nikdy nekončící proces. Příkladem může být 4 denní kurz „Manažer informační bezpečnosti podle ISO 27001“ za účastnický poplatek 25 000 Kč včetně zkoušky a certifikátu.

### Vzdělávání zaměstnanců

Zaměstnanci školy, tedy především učitelé, by měli dobře znát danou problematiku a jít příkladem žákům. Proto by měli pracovníci jednou ročně absolvovat školení na téma bezpečnost v informačních technologiích. Výsledkem školení by měl být dokument, obsahující jednotlivé body školení, podepsaný všemi zúčastněnými osobami, a především

proškolení zaměstnanci, uvědomující si důležitost této problematiky. Školení by se mělo týkat minimálně zaměstnanců přicházejících do styku s informačními technologiemi. Jejich vzdělávání by ideálně vždy před začátkem školního roku prováděl certifikovaný bezpečnostní manažer.

**Vzdělávání žáků**

Žáci, tedy papírově skupina s nejnižšími znalostmi, by měla mít minimálně povědomí o dané problematice. Vhodnou metodou, jak vybudovat, respektive zvýšit, bezpečnostní povědomí, jsou videokurzy, letáky nebo například praktická ukázka. Ověření účinnosti zvyšování může být například formou ano/ne testu nebo testu s výběrem z více možností.

Na závěr kapitoly zmíním několik základních rad pro uživatele, které by se mohly vyskytnout na letáku podporujícím bezpečnostní povědomí:

1. Používat silné heslo, které nemá žádný význam.
2. Použitá hesla si zapamatovat a v žádném případě nepsat na monitor, na spodek klávesnice apod.
3. Hesla pravidelně obměňovat.
4. Dodržovat pravidlo prázdného stolu a obrazovky při opuštění „pracoviště“.
5. Pravidelně zálohovat důležitá data.
6. Pravidla bezpečné e-mailové komunikace (neotevírat podezřelé e-maily/přílohy).
7. Nenavštěvovat podezřelé stránky na Internetu.
8. Nestahovat podezřelé soubory.
9. Používat jen legální software.
10. Používat antivirový program.
11. Hlásit bezpečnostní incidenty pověřené osobě.

Protože do školy dochází děti ve věku od 6 do 15 let, je důležité přizpůsobit obsah a formu vzdělávacího programu pro jednotlivé kategorie dětí tak, aby byl dostatečně efektivní.
Pravidla bezpečnosti ICT by měla být také zaznamenána v pravidelně aktualizovaném školním řádu jednotlivých učeben. Případné úpravy řádu provádí správce na požadavek některého z vyučujících, po schválení ředitelkou školy.

## 3.8 Zavedení bezpečnostních opatření a jejich náklady

V předchozích kapitolách byla navržena vybraná bezpečnostní opatření, která doporučuji zavést. Výše uvedená opatření jsou seřazena tak, jak jsou uvedena v normě ČSN ISO/IEC 27001. Toto pořadí však nijak nekoresponduje s jejich důležitostí a závažností rizik, které mají eliminovat. Mnou doporučené pořadí zavedení opatření ve fázi 1 je zobrazeno v tabulce č. 11, ve které jsou i náklady na jednotlivá opatření.

**Tabulka č. 11: Pořadí a náklady bezpečnostních opatření**

| Označení | Název opatření | Časová náročnost zavedení opatření | | Finanční náklady** |
|---|---|---|---|---|
| | | Jednorázově* | Ročně* | |
| A.5.1.1 | Politiky bezpečnosti opatření | 8 | 0 | 0 |
| A.6.1.1 a A.6.1.2 | Role odpovědnosti bezpečnosti informací + princip oddělení povinností | 10 | 0 | 0 |
| A.11.1.2 | Přístupový systém | 16 | 0 | 250 000 |
| A.11.2.2 | Podpůrné služby (UPS zdroje) | 2 | 0 | 17 000 |
| A.11.2.1 | Umístění zařízení a jeho ochrana | 4 | 0 | 0 |
| A.8.2.1 | Klasifikace informací | 6 | 0 | 0 |
| A.12.3.1 | Zálohování informací | 4 | 2 | 20 000 |
| A.8.2.2 | Označování informací | 4 | 0 | 0 |
| A.9.4.3 | Systém správy hesel | 2 | 0 | 0 |
| A.13.1.3 | Princip oddělení v sítích | 6 | 0 | 0 |
| A.8.1.1 | Seznam aktiv | 2 | 4 | 0 |
| A.8.1.2 | Vlastnictví aktiva | 4 | 1 | 0 |
| A.8.3.2 | Likvidace a vyřazení zařízení | 1 | 0 | 0 |
| A.7.2.2 | Povědomí, vzdělávání a školení bezpečnosti informací | 58 | 42 | 25 000 |
| A.5.1.2 | Přezkoumávání politik pro bezpečnost informací | 8 | 8 | 0 |
| **Celkem** | | **135** | **57** | **312 000** |

Zdroj: vlastní zpracování

*hodnoty uvedené v hodinách
**hodnoty uvedené v Kč bez DPH

Náklady na zavedení jednotlivých opatření jsou dvojího typu. Prvním typem je časová náročnost na zavedení opatření, která je udávána v hodinách. Druhým typem nákladů jsou

finanční náklady, které představují peněžní prostředky na zavedení opatření (pořízení zařízení) udávané v českých korunách.

## 3.9 Ekonomické zhodnocení

Důležitou částí této práce je i ekonomické zhodnocení zavedení ISMS. Celkové časové náklady na zavedení navržených opatření jsou odhadovány na 135 hodin. Jedná se pouze o odhad, který se v reálu může lišit s ohledem na znalosti osoby, která úkolem pověřena. Navrhuji, aby aplikace těchto opatření začala nejpozději na začátku letních prázdnin v červenci 2016 tak, aby se vše bezpečně stihlo do začátku nového školního roku, tedy do 5. září 2016. Vzhledem k předpokládané časové náročnosti na zavedení bezpečnostních opatření by měl být tento cíl splněn i v případě nečekaných drobných překážek při zavádění jednotlivých opatření.

Rozhodne-li se škola odměnit zaměstnance odpovědného za zavedení ISMS za každou hodinu práce 250 Kč, pak se náklady vyšplhají na 33 750 Kč.

Se zavedením některých opatření jsou spojeny i finanční náklady, které představují peněžní prostředky, například na pořízení zařízení. Odhad těchto nákladů se vyšplhal na 312 000 Kč, přičemž nejpodstatnější část finančních nákladů je tvořena cenou přístupového systému, který je nutno nainstalovat ve všech třech budovách. Pro součet nákladů jsem volil vždy částku horní hranice odhadu a skutečné náklady na opatření se mohou lišit. Náklady v dalších letech odhaduji na 57 hodin, do čehož nejsou zahrnuty náklady na opatření, jakožto reakce na vzniklé bezpečnostní incidenty a výsledný počet hodin se tak reálně může lišit. Roční náklady na udržování a zlepšování ISMS při hodinové dotaci 250 Kč vychází na 14 250 Kč. Každý rok by měl také proběhnout audit zavedených opatření, který byl kvalifikovanou osobou odhadnut na 20 000 Kč, a taktéž jsem ho zařadil do celkových nákladů v tabulce č. 12.

**Tabulka č. 12: Celkové náklady**

| | **Náklady** | |
|---|---|---|
| | **Jednorázové** | **Roční** |
| Zavedení vybraných opatření | 345 750 Kč | - |
| Údržba a zlepšování ISMS | - | 14 250 Kč |
| Audit zavedených opatření | - | 20 000 Kč |
| **Náklady celkem** | **345 750 Kč** | **34 250 Kč** |

Zdroj: vlastní zpracování

Vzhledem k charakteru organizace lze s jistotou říci, že ohrožení na zdraví či dokonce životech dětí, je škoda nevyčíslitelná. Náklady na navržená opatření sice nejsou nízké, ale vedení školy musí vzít na vědomí, že kromě ohrožení zdraví či životů žáků disponuje nemalým množstvím citlivých dat a v případě naplnění některé z hrozeb by mohla přijít nejen o dobrou pověst, na které si zakládá. **Náklady na navržená bezpečnostní opatření jsou ve srovnání s potencionální ztrátou minimální.**

## 3.10 Přínos práce

Práce by měla sloužit vedení školy, správci sítě, případně veřejnosti, jako podnět k zamyšlení nad otázkou bezpečnosti a především jako důvod k implementaci vybraných opatření. Rozhodne-li se škola mé návrhy realizovat, věřím ve zvýšení bezpečnosti informací ve škole a celkově lepší fungování celé organizace.

Jak již bylo zmíněno, řízení bezpečnosti informací je nekonečný proces, který nutné neustále udržovat a zlepšovat. Zavedením bezpečnostních opatření celý proces nekončí, je třeba pravidelně přezkoumávat zavedené postupy a politiky a zajistit tak neustálou vhodnost, přiměřenost a efektivnost celého systému.

Tato práce může posloužit jako základní metodika při zavedení ISMS. Pokud se vedení organizace rozhodne v budoucnu zavést celé ISMS, může navázat na tuto práci a pokračovat návrhem a následným zavedením další etapy.

Ekonomickým přínosem práce může být i ušetření nemalých finančních prostředků, které by škola musela vynaložit třetí straně za zpracování podobného projektu v rozsahu této práce. Dle kvalifikovaného odhadu by se tyto náklady vyšplhaly asi na 60 000 Kč, což dle mého soudu není zrovna malá částka.

Největším přínosem práce bude, pokud se navržená opatření zavedou do praxe a budou se jimi řídit bez výjimky všichni zaměstnanci a žáci.

Tato práce může být použita spolu s metodickým doporučením vydaným MŠMT, při jednání se školským zřizovatelem o zvýšení bezpečnosti základní školy.

# ZÁVĚR

Cílem této diplomové práce bylo odhalit největší bezpečnostní slabiny na dané základní škole a následně vybrat a navrhnout vhodná bezpečnostní opatření. Zavedení těchto opatření by mělo vést ke zvýšení bezpečnosti a bezpečnostního povědomí v oblasti ICT.

V první části práce jsem nejprve zprostředkoval teoretická východiska, která měla čtenáři navodit jisté povědomí o problematice ISMS. Hlavním zdrojem pro zpracování této kapitoly byly aktuální ISO normy řady 27000.

Ve druhé části jsem stručně představil vybranou základní školu a následně ji podrobil analýze současného stavu informační bezpečnosti, během které jsem rozebral jednotlivé oblasti ISMS dle aktuálních norem. Na závěr této kapitoly jsem provedl souhrn zjištěných poznatků a konstatoval, že bezpečnost ICT je na velmi nízké úrovni a je řešena pouze okrajově. Vzhledem k tomu, že škola neuvažuje o certifikaci ISMS, ani se na ni nevztahuje zákon o kybernetické bezpečnosti, jsem se rozhodl zaměřit pouze na vybraná opatření z nejvíce ohrožených oblastí.

V poslední části této práce jsem proto provedl analýzu rizik, pomocí které byla identifikována rizika a velikost jejich dopadu v případě naplnění bezpečnostních hrozeb. Rizika jsem následně rozdělil do tří kategorií dle jejich míry a odhalil tak nejkritičtější oblasti, pro které jsem následně vybral v souladu s přílohou A, normy ISO 27001, vhodná bezpečnostní opatření.

Na závěr práce jsem provedl ekonomické zhodnocení nákladů na zavedení bezpečnostních opatření. Odhadnuty byly jednak jednorázové náklady, ale i předpokládané roční náklady na pravidelné udržování a zlepšování celého systému.

Pevně věřím, že škola zváží mé návrhy na zavedení vybraných opatření a dojde ke zvýšení bezpečnosti informací na škole a ke zvýšení bezpečnostního povědomí v oblasti ICT. Ať už se škola k navrženým opatřením postaví jakkoliv, poslouží snad práce alespoň jako upozornění na stávající stav a v něm zjištěné bezpečnostní slabiny.

Cíle, které jsem si stanovil v úvodu této práce, tak byly splněny a nyní je již vše v rukou vedení školy.

# SEZNAM POUŽITÉ LITERATURY


(1) JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů II: kritické aplikace*. Vydání první. Brno: CERM, Akademické nakladatelství, 2015. ISBN 9788021452404.

(2) *ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(3) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 9788072048724.

(4) DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 9788074310508.

(5) RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2007, 152 s. ISBN 9788021435100.

(6) Informační bezpečnost. ČERMÁK, Miroslav. *Clever and Smart* [online]. 2009 [cit. 2016-04-19]. Dostupné z: http://www.cleverandsmart.cz/informacnibezpecnost

(7) *ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky – Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(8) *Building an Information Technology Security Awareness and Training Program: Computer security*. Gaithersburg, U.S.: National Institute of Standards and Technology, 2003.

(9) *ČSN ISO/IEC 27005. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014

(10) *ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(11) *Global Best Practice Solutions | AXELOS* [online]. London, 2014 [cit. 2016-04-19]. Dostupné z: https://www.axelos.com/

(12) ITIL - Wildcat! Technology. *Wildcat! Technology* [online]. Wildcat Information Technology, LLC, 2013 [cit. 2016-04-19]. Dostupné z: http://wildcatit.com/itil/

(13) COBIT | Office of Internal Audit. *Iowa State University* [online]. Iowa State University of Science and Technology, ©1995-2016 [cit. 2016-04-19]. Dostupné z: http://www.internalaudit.iastate.edu/internal-controls/cobit

(14) *Metodické doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních – Minimální standard bezpečnosti*. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2015.

(15) Základní informace. *ZŠ Smetanova Přelouč 1509* [online]. 2014 [cit. 2016-04-22]. Dostupné z: http://www.zssmprelouc.cz/index.php/info

(16) EU peníze školám. *ZŠ Smetanova Přelouč 1509* [online]. 2014 [cit. 2016-04-22]. Dostupné z: http://www.zssmprelouc.cz/index.php/eu

(17) MĚSTO PŘELOUČ. *Město - Oficiální stránky Města Přelouč* [online]. 2015 [cit. 2016-04-22]. Dostupné z:http://www.mestoprelouc.cz/

(18) *Mapy.cz* [online]. Seznam.cz, a.s, 2015 [cit. 2016-04-19]. Dostupné z: http://www.mapy.cz/

(19) *Z-WARE – identifikační systémy docházkové, stravovací, přístupové* [online]. Brno, 2008 [cit. 2016-05-19]. Dostupné z: http://www.z-ware.cz/

# SEZNAM ZKRATEK

| | |
|---|---|
| AD | *Active Directory* |
| ČSN | *Česká státní norma* |
| DNS | *Domain Name System* |
| DHCP | *Dynamic Host Configuration Protocol* |
| EU | *Evropská Unie* |
| HDD | *Hard Disc Drive* |
| HW | *Hardware* |
| ICT | *Informační a komunikační technologie* |
| IVT | *Informační a výpočetní technika* |
| IS | *Informační systém* |
| IT | *Informační technologie* |
| ISMS | *Information Security Management System* |
| ITIL | *Information Technology Infrastructure Library* |
| ITSM | *Information Technology Service Management* |
| IEC | *International Electrotechnical Commission* |
| ISO | *International Organization for Standardization* |
| IP | *Internet Protocol* |
| LAN | *Local Area Network* |
| MAC | *Media Access Control* |
| MŠMT | *Ministerstvo školství, mládeže a telovýchovy* |
| NAS | *Network Attached Storage* |
| OS | *Operační systém* |
| RAID | *Redundant Array of Independent Disks* |
| STP | *Shielded Twisted Pair* |
| SW | *Software* |
| TCP/IP | *Transmission Control Protocol/Internet Protocol* |
| UPS | *Universal Power Supply* |
| UTP | *Unshielded Twisted Pair* |
| ÚOOÚ | *Úřad pro ochranu osobních údajů* |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# SEZNAM PŘÍLOH

# Příloha č. 1: Směrnice pro zálohování dat

## Směrnice pro zálohování dat

**Odpovědná osoba:** Správce počítačové sítě

**Informovaná osoba:** Ředitelka školy

**Účel:** Tato směrnice definuje postup pro zálohování dat na základní škole

### Článek I.

Zálohování dat uložených na serveru bude probíhat dle časového plánu, který je v článku III této směrnice. Celý proces bude probíhat automaticky za využití softwarových nástrojů, případně manuálně odpovědnou osobou. Za celý proces je odpovědný správce počítačové sítě. Jeho povinností je pravidelně (1x měsíčně) kontrolovat funkčnost zálohování. Automatizovaná záloha bude prováděna na zabezpečené síťové úložiště NAS.

### Článek II.

Data ze serveru budou pravidelně zálohována, a to dle časového plánu vždy ve 22:00.

Pro plnou efektivitu zálohování jsou všichni uživatelé povinni dodržovat následující pravidla:

1. Soubory budou ukládat pouze do určených složek.
2. S ohledem na omezenou velikost diskového prostoru jsou uživatelé povinni mazat nepotřebné soubory.

Data, která nebudou uložena podle výše psaných pravidel, nebudou zálohována.

Za nastavení zálohování na síťové úložiště je odpovědný správce sítě.

### Článek III.

Na síťové úložiště dat budou ukládána data dle následujícího časového plánu:

**Tabulka č. 13: Časový plán zálohování**

| Data | Typ zálohy | Frekvence zálohy | Doba uchování zálohy | Přístup k zálohám |
|---|---|---|---|---|
| Uživatelské profily a Active Directory | Inkrementální | 1 měsíc | 6 měsíců | správce sítě |
| | Plná | 6 měsíců | 1 rok | |
| Účetní data, data z aplikace Bakaláři, školní dokumenty, instalační soubory | Inkrementální | 1 týden | 2 měsíce | správce sítě |
| | Plná | 1 měsíc | 6 měsíců | |
| Dokumenty zaměstnanců | Inkrementální | 1 týden | 2 měsíce | všichni zaměstnanci |
| | Plná | 1 měsíc | 6 měsíců | |

Zdroj: vlastní zpracování

## Článek IV.

Všechny zálohy dat musí být zabezpečeny a chráněny před zneužitím s ohledem na klasifikaci dat. Zařízení, na které je prováděno zálohování, musí být uloženo v geograficky odlišném místě a přenos dat musí být zajištěn v zašifrované podobě, aby bylo zabráněno odposlechu dat.

## Článek V.

Nastane-li HW, SW porucha nebo jiný důvod potřeby obnovení dat, je povinností poškozené osoby hlásit tuto skutečnost správci sítě, respektive bezpečnostnímu manažerovi, jehož povinností je zajistit obnovu dat z poslední dostupné zálohy.

## Článek VI.

Směrnice nabývá platnosti dne ____.____.20___.

Výjimky z výše uvedených pravidel je oprávněn udělit pouze správce sítě, respektive bezpečnostní manažer po zvážení nastalé situace. Výjimky musí být zdokumentovány a odůvodněny.

Udělené výjimky musí být v pravidelném intervalu 3 měsíců přezkoumány, zda nedošlo ke změně a výjimka je stále potřebná. Ke zrušení výjimky je oprávněn správce sítě na žádost původního žadatele nebo při pominutí důvodu udělení této výjimky.

V ……. dne ___.____._____ …….

Podpis ředitelky školy