VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ ISMS VE VEŘEJNÉ SPRÁVĚ
THE PROPOSAL OF ISMS IMPLEMENTATION IN THE PUBLIC ADMINISTRATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Kamil Štukhejl**
AUTHOR

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

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Kamil Štukhejl**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh zavedení ISMS ve veřejné správě

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem této práce je na základě analýzy rizik vybrané organizace odhalit riziková místa v oblasti bezpečnosti informací a s pomocí řady norem řady ISO/IEC 27000 navrhnout vhodná opatření, která povedou ke zvýšení informační bezpečnosti.

Základní literární prameny:

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 a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

ABSTRAKT

Tato diplomová práce se zaměřuje na zavádění systému řízení bezpečnosti informací ve veřejné správě pomocí řady norem ISO/IEC 27000. Práce obsahuje teoretická východiska, představení organizace, dále analýzu rizik a návrh vhodných opatření pro minimalizaci těchto nalezených rizik. V závěru je navržen plán pro implementaci včetně ekonomického zhodnocení.

ABSTRACT

This diploma thesis focuses on the implementation of information security management system in the public administration based on ISO/IEC 27000 series of standards. The thesis contains theoretical background, introduction of the organization, risk analysis and a proposal of appropriate measures for minimization of these identified risks. In the end, an implementation plan is proposed including an economic evaluation.

KLÍČOVÁ SLOVA

Systém řízení bezpečnosti informací, ISMS, analýza rizik, PDCA model, normy řady ISO/IEC 27000, aktivum, hrozba, zranitelnost, opatření

KEYWORDS

Information security management system, ISMS, risk analysis, PDCA model, standards of ISO/IEC 27000, asset, threat, vulnerability, measure

BIBLIOGRAFICKÁ CITACE

ŠTUKHEJL, Kamil. *Návrh zavedení ISMS ve veřejné správě* [online]. Brno, 2019 [cit. 2019-05-12]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/112157. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce 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 10. května 2019 ……....……

Podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval svému vedoucímu práce Ing. Petru Sedlákovi za odborné vedení, užitečné rady a vstřícný přístup při tvorbě této diplomové práce. Dále bych rád poděkoval své rodině, která mě podporovala po celou dobu mého studia.

OBSAH

ÚVOD 10
1 VYMEZENÍ ROZSAHU A CÍLE PRÁCE 11
2 TEORETICKÁ VÝCHODISKA 12
2.1 Základní pojmy 12
2.2 PDCA cyklus 15
2.3 ISMS 15
2.3.1 Ustanovení ISMS 17
2.3.2 Zavádění a provoz ISMS 21
2.3.3 Monitorování a přezkoumání ISMS 24
2.3.4 Údržba a zlepšování ISMS 25
2.4 Normy řady 27000 25
2.5 Kyberkriminalita 28
2.6 ISMS ve státní správě 32
2.7 Informační systémy veřejné správy 32
2.8 Ganttův diagram 33
3 ANALÝZA SOUČASNÉHO STAVU 35
3.1 Představení organizace 35
3.1.1 Organizační struktura obce 35
3.2 Analýza ICT 36
3.2.1 Hardware 36
3.2.2 Software 37
3.3 Analýza zabezpečení objektu 37
3.4 Analýza rizik 37
3.4.1 Identifikace a hodnocení aktiv 38
3.4.2 Identifikace zranitelností a hrozeb 39
3.4.3 Matice zranitelnosti 40
3.4.4 Matice rizik 40
3.4.5 Vyhodnocení analýzy rizik 43
4 VLASTNÍ NÁVRH ŘEŠENÍ 44
4.1 A.7 Bezpečnost lidských zdrojů 46

4.2 A.11 Fyzická bezpečnost a bezpečnost prostředí 49
4.3 A.12 Bezpečnost provozu 55
4.4 Shrnutí opatření 62
4.5 Metriky 64
4.6 Ekonomické zhodnocení 68
4.7 Časový harmonogram 70
4.8 Rizika projektu 75
4.9 Přínos práce 75
ZÁVĚR 77
POUŽITÁ LITERATURA 78
SEZNAM OBRÁZKŮ 80
SEZNAM TABULEK 81
SEZNAM PŘÍLOH 82

ÚVOD

Dnešní doba je známá pro raketový nárůst digitalizace ve všech oborech. Čím dál více činností a procesů je závislých na fungování nějakého informačního nebo komunikačního systému, to sebou nese potřebu věnovat čím dál tím větší pozornost bezpečnosti těchto systémů. A právě informační bezpečnosti je u mnoha organizací velmi podceňovaná a opomíjená. Proto je vhodné, aby se informační bezpečnosti dostalo větší pozornosti. Jedním z nástrojů, který řeší komplexní přístup k informační bezpečnosti je ISMS neboli systém pro řízení bezpečnosti informací. Úkolem systému řízení informační bezpečnosti je pomoct organizacím najít vhodná opatření, která sníží celkovou hodnotu všech rizik na co nejnižší úroveň za přiměřené náklady.

1 VYMEZENÍ ROZSAHU A CÍLE PRÁCE

Hlavním cílem této práce je snížení celkového rizika obecního úřadu z pohledu informační bezpečnosti s využitím norem systému řízení informační bezpečnosti ISO/IEC 27000. Pro dosažení tohoto hlavního cíle je nezbytné splnění dílčích cílů jako je vypracování analýzy prostředí zvolené organizace, analýzy a vyhodnocení rizik a návrhu vhodných a přiměřených opatření včetně ekonomického a časové zhodnocení návrhu. Pro tento návrh nejsou požadovány veškeré náležitosti dané normou ISO/IEC 27001, které jsou nutné pro certifikaci, avšak v tomto případě má tato norma sloužit jako doporučení pro zavádění ISMS.

2 TEORETICKÁ VÝCHODISKA

Tato kapitola popisuje teoretické základy, ze kterých bude vycházeno v dalších kapitolách této práce. Seznámíme se základními pojmy, jako jsou data, informace, znalosti, informační bezpečnost, dále bude popsán systém řízení informační bezpečnosti a hrozby plynoucí z kyberkriminality.

2.1 Základní pojmy

Data, informace a práce s nimi jsou stejně staré jako lidstvo samo. Práce s informacemi, byť nezáměrná a neuvědomělá, je stará dokonce jako život sám. Bouřlivý rozvoj informačních systémů a komunikačních technologií vedl až ke zrodu současné informační společnosti a vnesl informační systémy a komunikační technologie do každodenního života. Práce s daty má rozhodující význam pro chod lidské společnosti. Nové technologie sebou přináší značné výhody, ale i rizika. V případě selhání systému by byly následky pro vyspělá společenství značné (5).

Termínem **data** rozumíme údaje, fakta čísla, události, grafy, mapy, transakce atd., které byly zaznamenány vhodným způsobem a jsou srozumitelná pro příjemce. Jestliže člověk momentálně data používá k rozhodování, stávají se pro něj informacemi, neboť přiřazuje datům nějaký význam. Z toho vyplývá, že data jsou potencionálními informacemi (1,2).

Samotný termín **informace** by se dal definovat takto: *„Informacemi rozumíme data, kterým jejich uživatel přisuzuje určitý význam a které uspokojují konkrétní objektivní informační potřebu svého příjemce“* (3, s.62). Jedná se tedy o funkčně a cílově interpretovaná data (5).

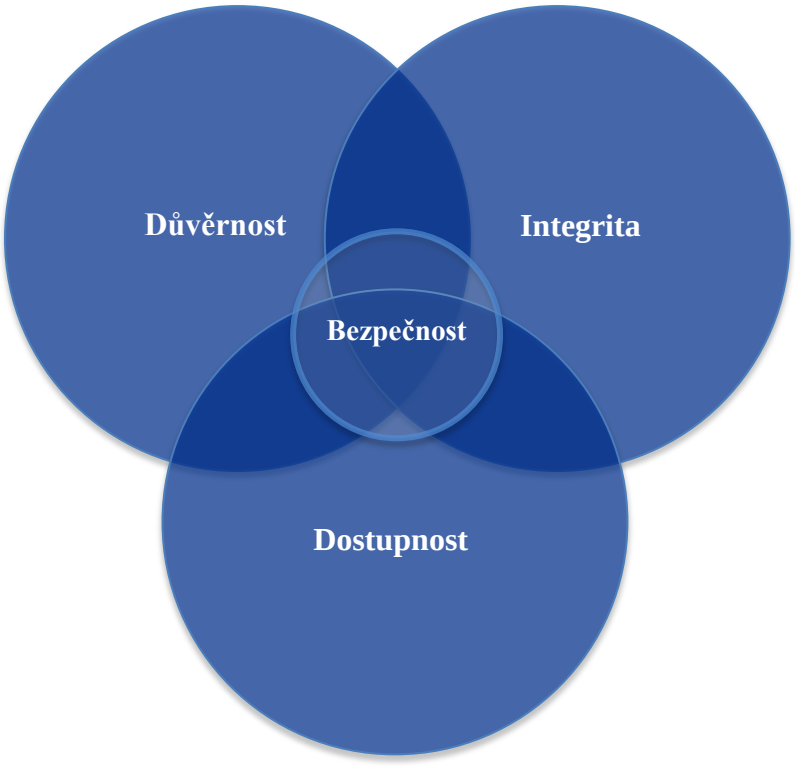
Informace vzniká v primárním zdroji, který převádí obraz daného subjektu do nějakého jazyka (jazykem rozumíme jakýkoliv smluvený způsob zápisu údajů o subjektu). Vzniklá data se pak přenášejí, zpracují a převádějí dále. Tomuto sledu se říká „**informační řetězec**“. Výstup toho řetězce je buď sdělen koncovému uživateli, nebo je zdrojem dalšího informačního řetězce. Prvky informačního řetězce mohou být lidé i stroje (5).

Komunikace obecně je sdělování a přijímání informací, může probíhat mezi lidmi, mezi stroji nebo i mezi strojem a člověkem. Informace jsou přenášeny pomocí signálů (obecně je signál fyzikální veličina, nesoucí informace) informačním kanálem (5).

Na to můžeme navázat pojmem **informační systém**. Definic je mnoho. Obecně můžeme říci, že se jedná o systém vzájemně propojených informací a procesů, který s těmito informacemi pracují. Zjednodušeně můžeme říci, že procesy jsou funkce zabezpečující sběr, přenos, uložení, zpracování a distribuci informací (2).

Jiný přístup vymezuje informační systém jako soubor lidí, technických prostředků a metod zabezpečujících sběr, přenos, uchování a zpracování dat za účelem tvorby a prezentace informací pro potřebu uživatelů (2).

S tím je spojena **bezpečnost informací**, která by měla být nedílnou součástí takového systému. V zájmu bezpečnosti informací (informační bezpečnosti) je především ochrana důvěrnosti, integrity a dostupnosti informací. **Důvěrnost** (Confidentiality) je vlastnost definovaná jako zajištění, že informace není dostupná nebo není odhalena neautorizovaným jedincům, entitám nebo procesům. **Integritu** (Integrity) chápeme jako zajištění správnosti a úplnosti informací. **Dostupnost** (Availability) je vlastnost přístupnosti a použitelnosti na žádost autorizované entity (6).

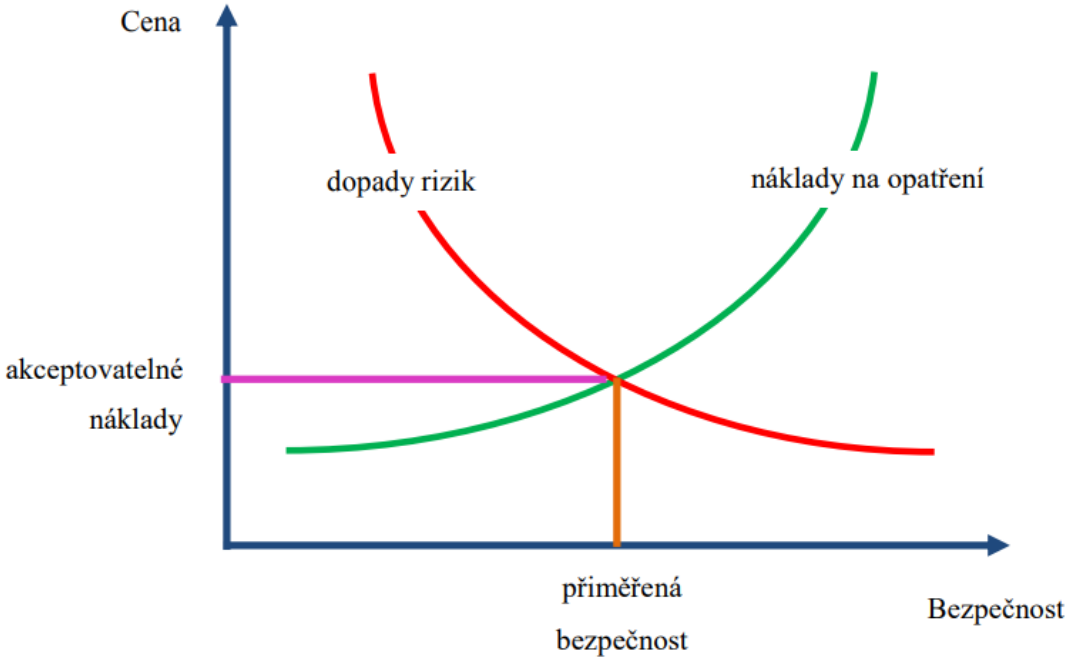


Obrázek 1: Bezpečnost informací (Zdroj:4)

Informační bezpečnost je ve vzájemném vztahu s pojmy bezpečnost organizace a bezpečnost IS/ICT. Jak je znázorněno na obrázku číslo 2, nejvýše je postavena **bezpečnost organizace** s úkolem zajištění bezpečnosti objektu a tím také majetku organizace. Zahrnuje automaticky také zajištění bezpečnosti IS/ICT a bezpečnosti informací. Bezpečnost informací zahrnuje kromě bezpečnosti IS/ICT práci s informacemi v nedigitální podobě. **Bezpečnost IS/ICT** chrání pouze aktiva informačního systému podporovaná informačními a komunikačními technologiemi (4).

Obrázek 2: Vzájemné vztahy bezpečností v organizaci (Zdroj: 4)

Přiměřená bezpečnost je stav bezpečnosti, kdy velikost úsilí a investic do bezpečnosti informačního systému odpovídá hodnotě aktiv a míře možných rizik. Tyto aspekty by měly být zohledněny v bezpečnostních politikách organizace. Pro lepší pochopení této úměrnosti se můžeme podívat na obrázek číslo 3 (4).



Obrázek 3: Přiměřená bezpečnost za akceptovatelné náklady (Zdroj: 4)

2.2 PDCA cyklus

Za zkratkou PDCA stojí čtyři anglická slova: plan, do, check, act, v překladu plánuj, dělej, kontroluj a jednej. Tyto čtyři slova velmi výstižně definují tuto metodu. Jde o metodu postupného zlepšování například kvality výrobků nebo služeb. Skládá se z těchto kroků (obrázek číslo 4) (4):

- plan (plánuj) – naplánování zamýšleného zlepšení (záměru),
- do (dělej) – realizace plánu,
- check (kontroluj) ověření výsledků realizace oproti původnímu záměru,
- act (jednej) – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe.

2.3 ISMS

Information security managment system (zkráceně ISMS) je tedy, jak ze samotného překladu vyplývá, systém řízení informační bezpečnosti, řídí bezpečnost informací se všemi atributy, které to obnáší. ISMS je část celkového systému řízení organizace. ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že (4):

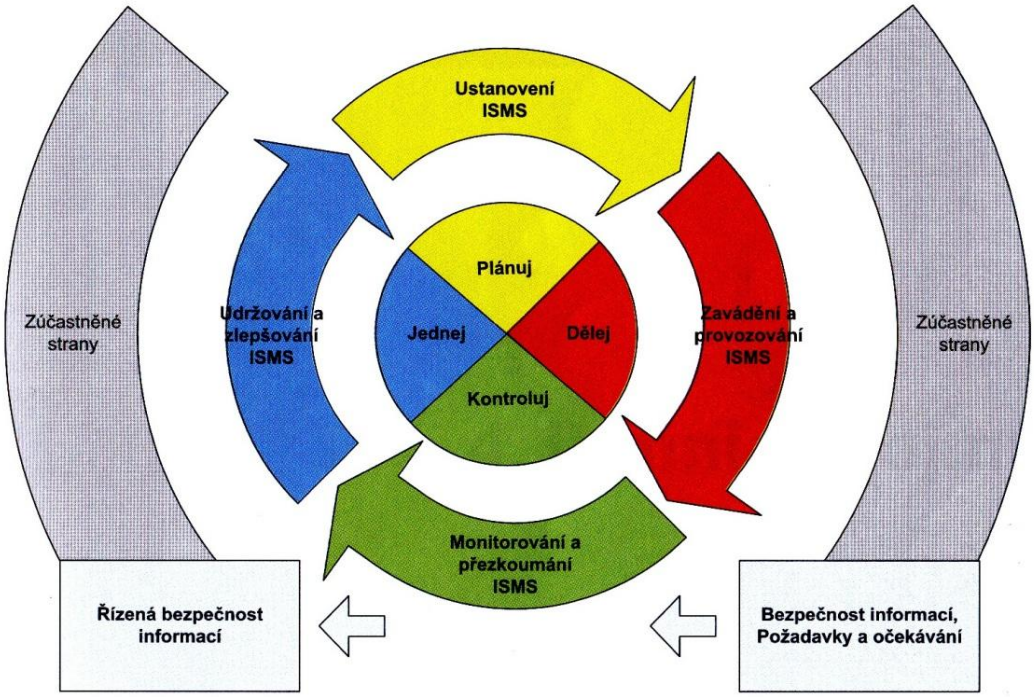
- jsou určena aktiva, která se mají chránit,
- jsou zvolena a řízena možná rizika a bezpečnosti informací,
- jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolovaná.

ISMS může být zaveden pro organizační složku společnosti, informační systém nebo jeho část, případně může zahrnovat celou organizaci. Zavedení systému řízení bezpečnosti informací je strategickým rozhodnutím vedení společnosti, tento systém se dotýká všech následujících okruhů (4):

- IT bezpečnost,
- komunikační bezpečnost
- personální bezpečnost,
- administrativní bezpečnost,
- fyzická bezpečnost,
- dokumentace,
- bezpečnostní funkce a mechanizmy.

ISMS se je založen na principu modelu PDCA (předešlá kapitola) a má tedy 4 základní etapy (6):

- **Ustanovení ISMS** – hlavním cílem této etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření.
- **Zavádění a provoz ISMS** – tato etapa se zaměřuje na účelné a systematické prosazení vybraného bezpečnostního opatření do chodu organizace.
- **Monitorování a přezkoumání ISMS** – cílem této etapy je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení informační bezpečnosti.
- **Údržba a zlepšování ISMS** – v poslední etapě jsou realizována možná zlepšení systému řízení bezpečnosti informací ať už soustavným zlepšováním systému nebo odstraňování zjištěných slabin a nedostatků.



Obrázek 4:Model PDCA v ISMS (životní cyklus ISMS) (Zdroj: 4)

Jednotlivé etapy si nyní detailně rozebereme. Popis částí ISMS jsou obsahem norem ISO/IEC 27001 a ISO/IEC 27002, přičemž norma ISO/IEC 27001 má podobu množiny požadavků, které jsou závazné, ve spojení s požadavky této normy tedy používáme výraz „musí“. Zajištění shody s normou ISO/IEC 27001 je podmíněno splněním všech těchto závazných požadavků (7).

Naproti tomu norma ISO/IEC 27002, které je souborem postupů, je navržena jako soubor doporučení a jednotlivé požadavky závazné nejsou. To se odráží i v používání obratu „měl by“ (7).

2.3.1 Ustanovení ISMS

První etapu cyklu ISMS je jeho ustanovení. Kromě definice rozsahu ISMS a odsouhlasení „Prohlášení o politice ISMS“ (závazek vedení podniku podporovat informační bezpečnost) patří mezi kritické činnosti provedení analýzy rizik a výběr vhodných bezpečnostních opatření pro snížení vlivu existujících rizik. Tato etapa by měla být zakončena souhlasem vedení se zavedením ISMS podle potřeb organizace, zjištěných při analýze a zvládání rizik ISMS. Tuto etapu můžeme rozdělit na několik dílčích činností (7):

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

Tato etapa budování má zásadní dopady na fungování ISMS během jeho celého životního cyklu!

Definice rozsahu a hranic ISMS, ve kterých je ISMS uplatňováno, je prvním úkolem řízení bezpečnosti. Jedná se o dokument popisující dotčené části systému ISMS určené k implementaci. Definuje rozsah a hranice ISMS na základě posouzení specifických rysů činností organizace, jejího uspořádání, organizační struktury, lokace a topologie, aktiv a technologií. Popisuje důvody vyjmutí některých oblastí z rozsahu ISMS (je-li tomu tak) (4,7).

Druhým krokem je **prohlášení o politice ISMS** (zkráceně politika ISMS). V tomto dokumentu je definován cíl, směr a rámec pro řízení bezpečnosti informací. Dalším a hlavním bodem je deklarace vedení organizace, že je společnost plně připravená a odpovědná k prosazení cílů při zavádění systému řízení bezpečnosti informací. Tento dokument reprezentuje zájem vedení organizace o řízení bezpečnosti informací a definuje klíčové podmínky pro ohodnocení rizik, což je základem pro celý ISMS. Tento dokument znamená, že managment společnosti chápe, co znamená zavádění tohoto systému a je připraven uvolnit potřebné zdroje (personální i ekonomické) (4,7).

Pravidla a postupy řízení rizik definují systematický přístup k řízení rizik. Řízení rizik je klíčovým nástrojem pro systematické řízení bezpečnosti informací. Přesná znalost skutečných rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření schopných snížit negativní dopad těchto rizik. Definice přístupu k řízení rizik určuje

metodiku hodnocení rizik, která vyhovuje ISMS a stanovené bezpečnosti informací. Na základě tohoto dokumentu se provádí analýza rizik včetně určení kritérií pro akceptaci rizik (4, 7).

Obrázek 5: Uspořádání terminologie řízení rizik (Zdroj: 7)

Analýza rizik je prováděna za účelem identifikace zranitelných míst a informačního systému organizace. Zachycuje seznam hrozeb působících na informační systém a stanovuje rizika příslušná každému zranitelnému místu a hrozbě. Účelem takového dokumentu je snížení rizik na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde je jejich minimalizace neefektivní (4).

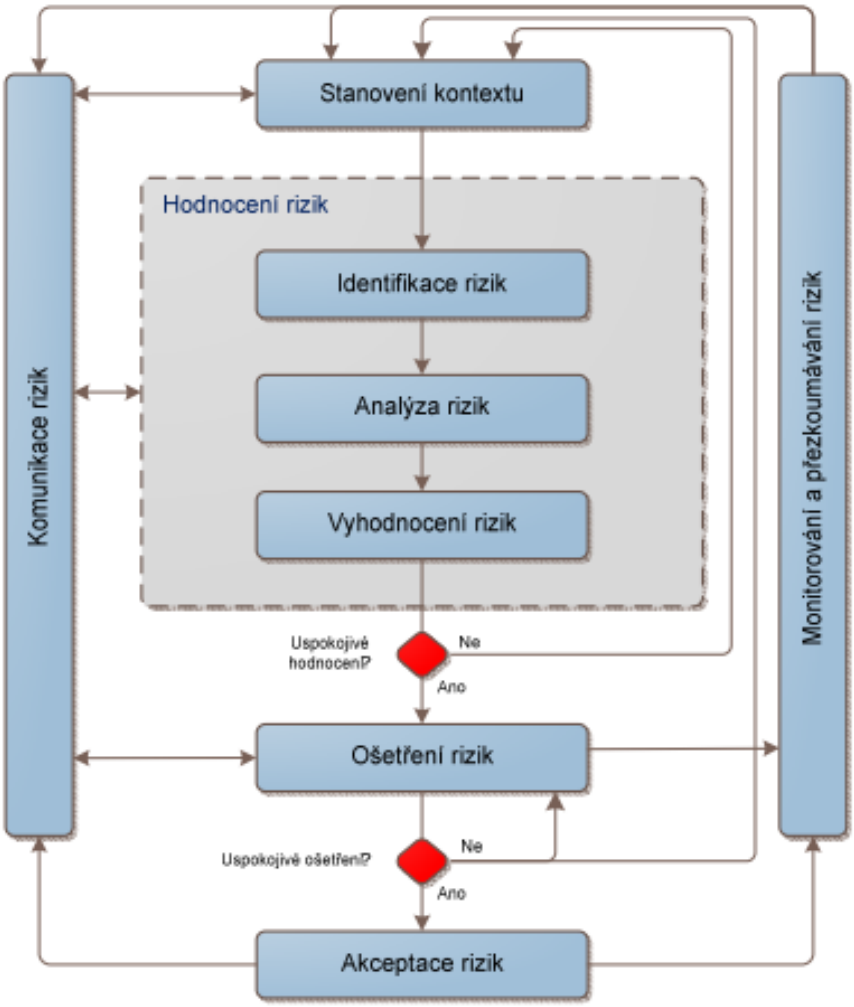
Prvním krokem, který je pro řízení rizik důležitý, je **identifikace aktiv** a určení jejich významu pro organizaci. Pro každé identifikované aktivum (hmotný i nehmotný majetek) je potřeba vyjádřit míru jeho důvěrnosti, integrity a dostupnosti. Nedílnou součástí je konkrétní popis aktiva a jejich ohodnocení ve formě tabulky. Doporučuje se seskupit aktiva, která k sobě logicky patří a identifikovat vlastníka daného aktiva (4, 7).

Hodnocení aktiv může být přistupováno kvantitativní metodou, kdy může být hodnota aktiva vyjádřena penězi, nebo kvalitativní hodnotou, která vyjadřuje dopad na organizaci v případě ztráty nebo poškození aktiva. Pro hodnocení lze využít i řadu nástrojů a programů (4).

Dalším krokem řízení rizik je **identifikací hrozeb**, které mohou potenciálně způsobit nežádoucí incident, který může mít za následek poškození systému nebo organizace a jejich aktiv. Hrozby můžeme rozdělit do několika kategorií, buď mají původ přírodní (zemětřesení, blesk, požár, povodně, apod.) nebo způsobené lidským faktorem (odposlech, chyba uživatele, apod.). Dále je dělíme na náhodné (vymazání souboru, apod.) a úmyslné (zcizení, úmyslné poškození, apod.), nebo také na vnitřní a vnější.

Z pohledu bezpečnosti je žádoucí, aby jak náhodné tak úmyslné hrozby byly identifikovány a měla by být odhalena jejich úroveň a pravděpodobnost. Je nutné každou hrozbu ohodnotit z pohledu pravděpodobnosti (4).

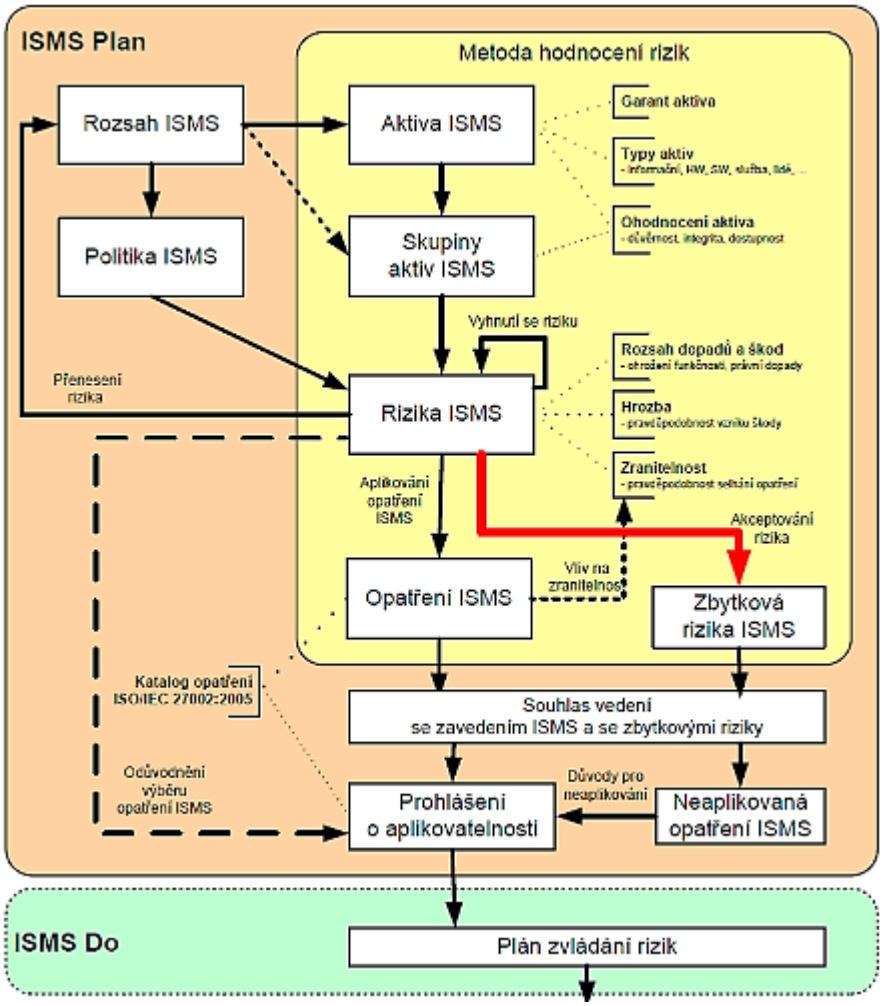
Zvládání rizik je závěrečný krok řízení rizik, který řeší návrh vhodných forem ochrany. Na zákaldě identifikovaných bezpečnostních potřeb a definování priorit je nutné zvolit vhodná bezpečnostní opatření, která mají za cíl efektivně eliminovat rizika.



Obrázek 6: Celý proces řízení rizik (Zdroj: 6)

Souhlas vedení se zavedením ISMS a se zbytkovými riziky jsou dva formální kroky. První z nich je souhlas vedení organizace s návrhem bezpečnostních opatření, která jsou nutná pro snížení bezpečnostních rizik. Současně s tím, by se vedení mělo vyjádřit, zda jsou existující zbytková rizika pro chod organizace přijatelná či nikoli (7).

Prohlášení o aplikovatelnosti je povinným dokumentem pro organizace, které usilují o shodu svého ISMS a normou ISO/IEC 27001. Jedná se o dokumentované prohlášení, které popisuje cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná na ISMS dané organizace (7, 8).



Obrázek 7: Přehled činností při ustanovení ISMS (Zdroj: 7)

2.3.2 Zavádění a provoz ISMS

Tato etapa životního cyklu ISMS se soustředí na prosazení všech bezpečnostních opatření tak, jak byla navržena v předchozí etapě při ustanovení ISMS. Důležité je především připravit dílčí plán, kde jsou upřesněny termíny, odpovědné osoby apod. Všechna bezpečností opatření by měla být zdokumentována v tzv. Příručce bezpečnosti informací a mělo by dojít k vysvětlení bezpečnostních principů všem uživatelům a

manažerům. Během této etapy zavádění ISMS je nezbytné provést následující činnosti (7):

- formulovat dokument „Plán zvládání rizik“ a započít s jeho zaváděním,
- zavést plánovaná bezpečnostní opatření a zformulovat příručku bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření definovaných oblastí bezpečnosti informací,
- definovat program budování bezpečnostního podvědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky a zejména z oblasti řízení bezpečnosti,
- upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele,
- zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty a
- řídit zdroje, dokumenty a záznamy ISMS.

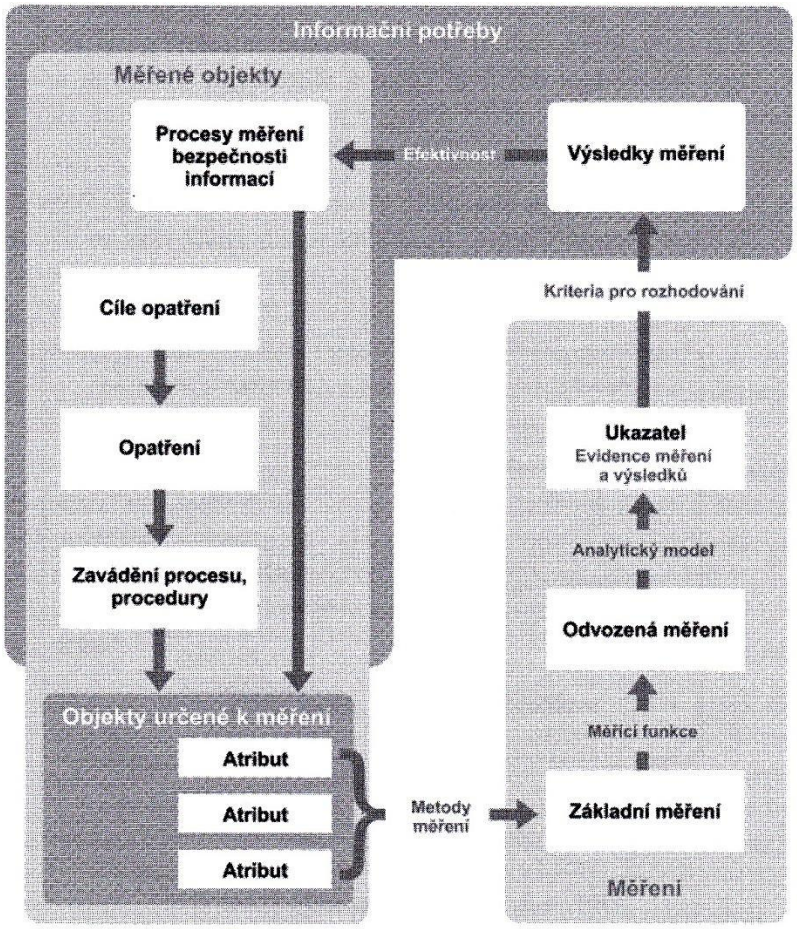
Plán zvládání rizik je důležitým dokumentem, který popisuje všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik, stanové cíle a priority těchto činností, omezující faktory a potřebné zdroje (finanční, personální, znalostní apod.). Dále jednoznačně definuje osobní odpovědnost za provádění jednotlivých naplánovaných činností. Při sestavování tohoto plánu se vychází především ze dvou zdrojů informací – výsledky řízení rizik a informace získané při pravidelném přehodnocování ISMS. Na základě rozdílu mezi bezpečnostními potřebami a skutečným stavem bezpečnostních opatření je možné dobře definovat potřebné činnosti pro zlepšení stavu ISMS (7).

Příručka bezpečnosti informací je pojem, který souhrnně označuje dokumenty, jako jsou bezpečnostní politiky, bezpečnostní směrnice apod., které dlouhodobě určují bezpečnostní principy, pravidla, zásady a odpovědnosti, které pomáhají při prosazování vybraných bezpečnostních opatření. Je důležité definovat kdo, co, kdy, kde a jak má učinit (7).

Jedním z nejdůležitějších prvků při prosazování ISMS je **prohlubování bezpečnostního podvědomí**, za kterým se skrývá promítnutí všech definovaných pravidel a postupů do skutečného chování všech odpovědných pracovníků a uživatelů.

Abychom předcházeli bezpečnostním incidentům je potřeba všem pracovníkům vysvětlovat bezpečnostní principy a pravidla, seznamovat je s bezpečnostními riziky a projednávat s nimi bezpečnostní incidenty, jejich příčiny a skutečné i potenciální následky. Jedině tímto systematickým a nekončícím procesem bude možné zajistit větší odolnost nejslabšího článku pomyslného řetězu ISMS – lidského faktoru (7).

Dalším důležitým tématem, které je spojeno s prosazováním efektivního řízení bezpečnosti, je **měření účinnosti** aplikovaných bezpečnostních opatření. Je potřeba definovat a pravidelně sledovat objektivní údaje o skutečném fungování systému řízení bezpečnosti, na základě kterých můžeme provádět důležitá rozhodnutí a opatření. Způsob, jakým je informační bezpečnost měřena, vidíme na obrázku 8 (7).



Obrázek 8: Model měření bezpečnosti informací (Zdroj: 12)

Řízení dokumentace je poslední krokem zavedení ISMS. Pro umožnění kontroly správnosti fungování ISMS je podstatné vytvořit definovaná pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace řízení bezpečnosti (včetně odebírání,

zneplatnění a skartace neplatných verzí dokumentů. Zároveň je podstatné vytvářet systematické záznamy o jednotlivých provedených činnostech ISMS, kde jsou uvedeny: osoby, činnost, termín a místo realizace, výsledky atd.) (7).

2.3.3 Monitorování a přezkoumání ISMS

Hlavním úkolem třetí etapy zavádění ISMS je zajištění účinné zpětné vazby. Mělo by dojít k prověření všech aplikovaných bezpečnostních opatření a jejich důsledku na ISMS. V této části zavádění ISMS je nutné provést následující činnosti (7):

- monitorovat a ověřit účinnost prosazení bezpečnostních opatření,
- provést interní audity ISMS, jejich náplň pokryje celý rozsah ISMS a
- připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace (včetně revize zbytkových a akceptovatelných rizik).

Provádění kontrol ISMS je základní zpětnou vazbou, kterou provádí všechny osoby na manažerských postech, které mají za fungování ISMS nějakou odpovědnost. Tyto osoby by se měli starat o svěřené úkoly, o to zda dochází k naplnění bezpečnostních požadavků a o hodnocení adekvátnosti bezpečnostních opatření. Součástí kontrol je i schopnost včasné detekce chyb, úspěšných i neúspěšných pokusů o narušení bezpečnosti nebo schopnost sledování bezpečnostních událostí a včasná detekce bezpečnostních incidentů (7).

Interní audity ISMS je dalším kritickým krokem zpětné vazby, které na rozdíl od kontrol zajišťují potřebný nezávislý pohled na fungování ISMS. Jedná se o systematický, nezávislý a dokumentovaný proces pro získání hodnocení o splnění předem stanovených kritérií (7, 9).

Přezkoumání ISMS vedením organizace je činnost, která je prováděna k určení vhodnosti, přiměřenosti a efektivnosti předmětu zkoumání k dosažení stanovených cílů. Za vstupy pro přezkoumání patří všechny informace o fungování ISMS za dané období, především pak výsledky auditů, zpětná vazba odpovědných osob a třetích stran, analýza rizik, výsledky měření účinnosti. Výstup přezkoumání může být ve formě zprávy o slabých a silných stránkách (SWOT analýza) (7, 9).

2.3.4 Údržba a zlepšování ISMS

Poslední etapou celého cyklu prosazování ISMS je jeho udržování a zlepšování. V tomto kroku by mělo docházet ke sběru podnětů ke zlepšení ISMS a k nápravě všech nedostatků – neshod, které se v ISMS objevují (7).

Soustavné zlepšování je využití zpětné vazby, tedy zkušenosti a nápady uživatelů ISMS. Pro rozvoj ISMS je důležitá motivace pracovníků sdílet a navrhovat, co je vhodné a žádoucí na chodu ISMS zlepšit. U všech podnětů je nutné zvážit jejich dopady a rizika (7).

Odstranění nedostatků ISMS má dvě formy (7):

- opatření k nápravě a
- preventivní opatření.

Opatření k nápravě je reaktivní formou řešení nedostatků, které se již projevily. A je tedy reakcí na neshodu (7).

Naproti tomu preventivní opatření je proaktivní formou řešení nedostatků ISMS. V tomto případě se nedostatek ještě neprojevil, ale odklad jeho řešení by mohl vést k negativní události (7).

2.4 Normy řady 27000

Řada norem pro **systém řízení bezpečnosti informací** ISO/IEC 27000 ideově vychází z konceptu PDCA a jejím základem jsou normy, jež jsou uvedeny na obrázku 10. Rodina norem má pomoci organizacím všech typů a velikostí zavést a provozovat ISMS. Níže jsou uvedeny základní normy popisující systém řízení bezpečnosti informací (4,7):

ISO/IEC 27000:2018 - Přehled a slovník definuje pojmy a terminologický slovník pro všechny ostatní normy z této série. Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací.

ISO/IEC 27001:2013 - Požadavky je hlavní norma pro ISMS, dříve známá jako BS7799-2, podle které jsou systémy certifikovány. V hlavní části normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování,

přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému řízení informační bezpečnosti.

ISO/IEC 27002:2013 - Soubor postupů je sbírka nejlepších bezpečnostních praktik a může být využita jako kontrolní seznam všeho správného, co je nutno pro bezpečnost informací v organizaci udělat. Obsahuje podrobný výklad vhodných bezpečnostních opatření. Celkem obsahuje 113 bezpečnostních opatření rozdělených do 14 oblastí.

Obrázek 9: Skupiny opatření podle ISO/IEC 27002:2013 Zdroj: (12)

ISO/IEC 27003:2017 – Směrnice pro implementaci systému řízení bezpečnosti informací poskytuje doporučení pro ustanovení a implementaci ISMS v souladu s ISO/IEC 27001. Norma vysvětluje proces návrhu a implementace ISMS pomocí popisu zahájení, definování a plánování projektu ISMS.

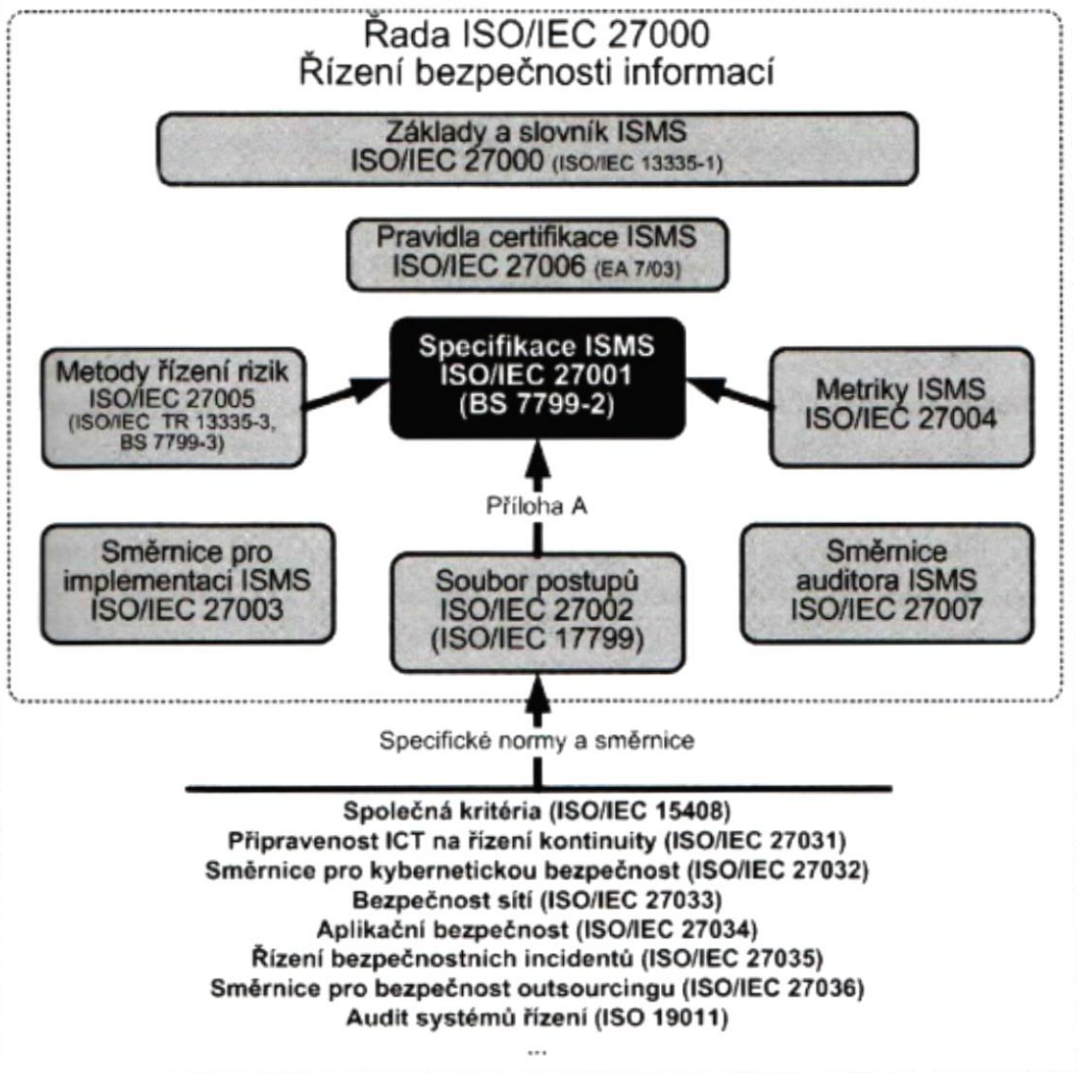
ISO/IEC 27004:2016 – Měření je pro organizace pomůckou k měření a prezentaci efektivity jejich systémů řízení bezpečnosti informací. Program měření bezpečnosti informací zahrnuje procesy rozvoje metrik a měření, provádění měření, analýzu dat a hlášení výsledků měření a dále proces vyhodnocení a zlepšování programu měření.

ISO/IEC 27005:2011 – Řízení rizik bezpečnosti informací obsahuje doporučení a techniky pro řízení rizik bezpečnosti informací s ohledem na požadavky dle ISO/IEC 27001. Kromě doporučení spojených s řízením rizik tato norma obsahuje i rozsáhlé katalogy hrozeb a zranitelností.

ISO/IEC 27006:2015 – Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací. Tato norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací a doplňuje tak požadavky obsažené v ISO/IEC 27001.

ISO/IEC 27007:2017 – Guidelines for Information security management systems auditing obsahuje doporučení k provádění auditů ISMS podle ISO/IEC 27001.

ISO/IEC 27008:2011 - Guidance for auditors on ISMS controls se soustředí na způsoby auditu a kontroly bezpečnostních opatření.



*Obrázek 10: Koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací (*Zdroj*: 7)*

2.5 Kyberkriminalita

Rozvoj informačních technologií s sebou přináší i nová podvodná jednání. Kyberkriminalita je trestná činnost, která je páchaná v oblasti informačních a komunikačních technologií. Nejčastější hrozby v této oblasti jsou uvedeny v tabulce níže.

Hrozba	Popis
Porušení autorizace	Osoba, která je autorizována k použití zdroje pro jistý účel jej použije k jinému, neautorizovanému účelu.
Obejití řízení	Útočník využije bezpečnostních mezer v systému nebo jeho slabin.
Potlačení služby	Omezení legitimního přístupu k informacím nebo jiným zdrojům v síti.
Nezákonný odposlech	Informace je získávána monitorováním přenosového kanálu.
Emisní nebo VF odposlech	Informace je extrahována z vysokofrekvenčního vyzařování nebo emisí či jiných elektromagnetických jevů, ke kterým dochází při provozu elektronického zařízení.
Nelegitimní použití	Zdroj je používán neautorizovanou osobou nebo neautorizovaným způsobem.
Indiskrece	Autorizovaná osoba prozradí důvěrnou informaci neautorizované osobě z neopatrnosti nebo za úplatu.
Únik informace	Získání důvěrné informace neautorizovanou osobou nebo systémem.
Narušení integrity	Konzistence dat je narušena jejich neautorizovaným vytvořením, úpravou nebo vymazáním.
Změna dat při přenosu	Přenášená data jsou během přenosu informačním kanálem změněna, odstraněna nebo zcela vyměněna.
Maškaráda	Jedna entita (osoba nebo systém) se představuje jako jiná entita.
Vytěžení odpadových médií	Informace je získávána z magnetických nebo papírových médií, vyhozených do odpadu.
Fyzický průnik	Útočník získá kontrolu na systémem proniknutím k jeho ovládacím prvkům.
Replay	Zachycená kopie legitimní transakce je využita pro opětovný přenos s nelegitimním úmyslem.
Popření skutečnosti	Strana zúčastněná ve vzájemné komunikaci později popře, že k takové komunikaci došlo.
Vyčerpání zdrojů	Jistý zdroj, např. port, je úmyslně natolik zatížen, že je znemožněno používání služby, která je na něj vázána, řádnými uživateli.
Podvržení služby	Podvržený systém nebo systémová komponenta, které se vůči uživatelovi chovají jako běžná součást systému, slouží k získání citlivých informací od důvěřivého uživatele.
Krádež	Kritický prvek bezpečnostního systému (např. přístupová karta) nebo veškerá citlivá informace jsou zcizeny.
Analýza provozu	Informace je neautorizovanou entitou získána pomocí sledování provozu a výběrem podstatných jeho částí.
Zadní vrátka	Do systému je zabudována vlastnost nebo vložena součást, která při jisté konstelaci vstupních dat umožní obejít bezpečnostní mechanismy.
Trojský kůň	Software obsahuje zdánlivě nevinnou nebo neviditelnou část kódu, který – pakliže je spuštěn – ohrozí bezpečnost uživatele.

Obrázek 11: Typické hrozby (Zdroj: 14)

Může se zdát, že výčet není úplný, zahrnuje totiž všechny známé způsoby útoků, nikoliv jejich metody. Např. viry nebo červi současně patří do kategorie „obejití řízení“ a „maškarády“ a jsou jen realizací této kombinace formy útoku (14).

Mezi nejznámější projevy kyberkriminality patří (15):

- Botnet – lze jednoduše definovat jako síť softwarově propojených botů (program v infikovaném počítači plnící příkazy útočníka), který provádí činnost na základě příkazů správce (útočníka). Taková síť disponující vysokým výpočetním výkonem je využívaná zejména k nelegální činnosti.
- Malware – je označení pro jakýkoliv škodlivý software, který je využíván za účelem narušení standardní činnosti počítačového systému, zisku informací, či k získání přístupu k počítačovému systému. Pod souborným pojmem malware se skrývá celá řada škodlivého softwaru, jedná se o následující pojmy: adware, spyware, viry, červi, trojské koně, backdoor, rootkity, keylogger nebo ransomware.
- Ransomware - jedná se o tzv. vyděračský software, který brání či omezuje uživatele v používání počítačového systému do doby, než dostane útočník zaplaceno. Ransomware se do počítače dostane nejčastěji pomocí malware.
- Spam – jedná se o hromadně šířené nevyžádané sdělení, nejčastěji reklamního charakteru. V širším slova smyslu se jedná o veškeré nevyžádané sdělení zahrnující i škodlivý kód.
- Phishing – tímto pojmem se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj. Typickou metodou jsou podvodné webové stránky vypadající stejně jako originální stránky vyžadující vyplnění přihlašovacích údajů.
- Podvodné webové stránky
- Hacking – označuje souhrn metod pro narušení bezpečnosti nebo stability počítačového systému. Podle motivace můžeme rozdělit hackery na „white hats“, jejichž motivace je odhalení bezpečnostních děr a je tedy nedestruktivního charakteru. Opak jsou „black hats“, jejichž motivace je způsobit uživateli škodu.

- Cracking – cracking znamená tzv. prolamování nebo obcházení ochranných prvků počítačového systému, programů nebo aplikací, s cílem jejich následného neoprávněného užití. Za crackery bývají označování právě hackeři z kategorie „black hats“.
- Internetové pirátství – jedná se o pojem zastřešující kriminalitu, jež porušuje práva duševního vlastnictví (autorského práva a průmyslového práva)
- Sniffing – je metoda nelegálního odposlechu dat procházejících počítačovou sítí při komunikaci mezi poskytovanou službou a počítačovým systémem. Technicky se tak děje pomocí odchytávání a čtení TCP paketů.
- DoS, DDoS útoky – pojem DoS je zkratkou pro anglické spojení „denial of service“, což v překladu znamená „odepření služby“. Cílem takového útoku je vyřazení z činnosti nebo snížení výkonu počítačového systému, pomocí zahlcení systému falešnými požadavky.
- Sociální inženýrství – nelze za každých okolností považovat za kybernetický útok, ale je to předpoklad aby byla řada kybernetických útoků úspěšná. Jde o způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Obrana proti sociotechnickým útokům není jednoduchá, jelikož působí na nejslabší článek systému – člověka. Následující tabulka shrnuje jednotlivé oblasti sociotechnického útoku spolu s nepoužívanějšími taktikami a způsoby obrany (14).

Oblast útoku	Sociotechnické taktiky	Obrana
Telefon (help desk)	Předstírání identity, přesvědčování	Zaměstnanci nesmí vydávat svá hesla a důvěrné informace
Vchod do budovy	Vniknutí v převleku	Průkazy, ostraha, trénink zaměstnanců
Kancelář	Nahlížení přes rameno	Hesla psát pouze s jistotou, že se nikdo nedívá
Kancelář	Procházení budovy a hledání odemknutých kanceláří	Každý host by měl být eskortován
Serverové místnosti	Pokus o logování, odstranění vybavení, nahrání trojského koně, který získává data	Serverové místnosti musí být pořád zamčené, měl by být veden inventář vybavení
Telefonní ústředna	Kradení linek a přesměrování	Kontrola meziměstských a mezikontinentálních hovorů
Odpadkové koše	Prohledávání odpadků	Odpadkové kontejnery v zabezpečené a monitorované oblasti, skartovat všechny důležité dokumenty, bezpečné mazaní magnetických medií
Intranet-Internet	Software na odchytávání hesel	Sledování programového vybavení počítačů
Kancelář	Zcizení dokumentů	Hierarchie důvěrnosti dokumentů a adekvátní zacházení s nimi

Obrázek 12: Oblasti sociotechnických útoků, taktika a obrana (Zdroj: 14)

2.6 ISMS ve státní správě

Státní správa je z pohledu ISMS a jeho zavádění nejpotřebnější oblast z pohledu množství a členitosti zpracovávaných údajů. K této oblasti by mělo být přistupováno specificky a to z několika důvodu, za prvé velká část dokumentů existuje v papírové podobě, za druhé je komplikované hodnocení dopadů při analýze rizik a konečně je také komplikovaná mezirezortní komunikace. A především jsou ve veřejné správě omezené prostředky na zabezpečení ochrany a efektivní obranu informačních aktiv, je tedy nutné využít tyto zdroje efektivně a zabezpečit především kritické systémy (4).

2.7 Informační systémy veřejné správy

Informační systémy veřejné správy (ISVS) jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Ministerstvo vnitra zajišťuje rozvoj, výstavbu a metodické řízení ISVS. Prostřednictvím atestace dlouhodobého řízení ISVS, atestace způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní a kontrolní

činnosti realizuje zpětnou vazbu na metodiky a vyhlášky k zákonu č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů a jejich dodržování v praxi. Projektovým přístupem omezuje vznik duplicit při provozování ISVS. Zabezpečuje reálné požadavky na čerpání financí z veřejných rozpočtů v oblasti ICT. Připravuje technologické podmínky pro efektivnější výkon veřejné moci (11).

Zákon o informačních systémech veřejné správy stanoví práva a povinnosti správců informačních systémů veřejné správy (ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. V návaznosti na to upravuje působnost Ministerstva vnitra jako ústředního správního úřadu pro tvorbu a rozvoj informačních systémů veřejné správy. Zákon vytváří podmínky, aby kvalitní informační systémy byly dobrým nástrojem pro výkon veřejné správy (11).

Právní předpisy však blíže nespecifikují, jak konkrétně mají orgány veřejné správy k řízení kvality ISVS přistupovat, existuje pouze obecné doporučení využít mezinárodně uznávané normy a metody (10, 11).

V případě obcí jsou ISVS například:

- evidence uložených pokut (správních sankcí) podle § 58 a 59 zákona č. 128/2000 Sb., o obcích,
- evidence plátců místních poplatků podle zákona č. 565/1990 Sb., o místních poplatcích,

• evidence obyvatel.

A ISVS naopak nejsou:

- provozní informační systémy,
- operační systémy, webové prohlížeče, e-mailový klienti, textový a tabulkový editory, ty nejsou samy o sobě ISVS.

2.8 Ganttův diagram

Ganttův diagram je horizontální pruhový graf vyvinutý jako nástroj pro kontrolu výroby v roce 1917 americkým inženýrem Henry L. Ganttem. Ganttův diagram, který se často

používá při řízení projektů, poskytuje grafické znázornění harmonogramu, který pomáhá plánovat, koordinovat a sledovat konkrétní úkoly v projektu (16).

Graf je tvořen horizontální osou, která představuje celkový časový rozsah projektu, rozdělený do stejně dlouhých časových jednotek (dnů, týdnů apod.) a vertikální osou, kterou tvoří jednotlivé úkoly projektu. Horizontální pruhy různých délek reprezentují časové rozpětí jednotlivých úkolů (16).

Gantův diagram nám dává jasnou představu o stavu projektu. V základní podobě Ganttův diagram neobsahuje vztahy mezi činnostmi, ale moderní softwarové nástroje pro plánování projektů do něj tyto závislosti, čáry nebo šipky vedoucí od konce činnosti A k začátku činnosti B, obvykle zakomponovávají (16).

3 ANALÝZA SOUČASNÉHO STAVU

Tato kapitola se zabývá analýzou současného stavu informační bezpečnosti a sestává z několika částí. V následující části bude představena organizace a její struktura, dále bude zanalyzovaný stav informačních a komunikačních technologií a analýza zabezpečení objektu, konečně budou vyhodnoceny rizika pomocí maticové metody.

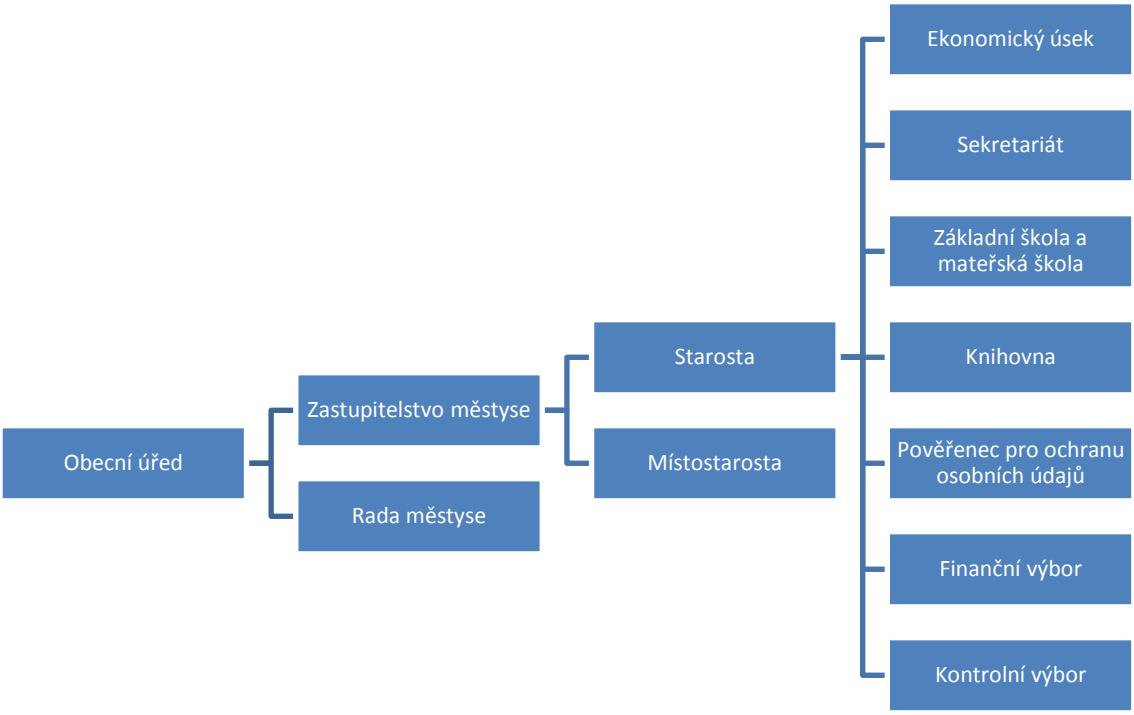
3.1 Představení organizace

Z důvodu bezpečnosti informací organizace nebude v této práci uváděn její název nebo jakákoli informace, která by vedla k její identifikaci.

Jako podklad zpracování této práce jsem zvolil obecní úřad nejmenované obce. Obec je veřejnoprávní korporací a má vlastní majetek. Podle platných právních úprav obcí se jedná o obec městského charakteru – městys. Městys je základním územním samosprávným společenstvím občanů, tvoří územní celek, který je vymezen hranicí území obce.

3.1.1 Organizační struktura obce

Obec spadá do veřejné správy, čili je organizační struktura daná. Obecní úřad zaměstnává celkem 10 zaměstnanců na plný úvazek včetně uvolněného starosty, dále úřad zaměstnává několik osob na částečný úvazek včetně místostarosty a členů zastupitelstva. Obec je samostatně spravována zastupitelstvem obce a dalšími orgány obce jsou rada obce, starosta, obecní úřad a zvláštní orgány obce. Zastupitelstvo je složeno z 15-ti členů, kteří rozhodují o věcech patřících do samostatné působnosti městyse. Starosta se stará o reprezentaci obce a vedení úřadu, o zastoupení v jeho nepřítomnosti se stará místostarosta. Rada městyse je výkonným orgánem obce v oblasti samostatné působnosti. Při výkonu samostatné působnosti odpovídá rada městyse zastupitelstvu městyse.



Obrázek 13: Organizační schéma obce

3.2 Analýza ICT

O správu ICT se stará externí firma. V objektu se nachází dva stolní počítače (počítače sekretářky a ekonomky, počítače jsou fyzicky nezabezpečené). Dále jsou v síti dva přenosné počítače, které využívá starosta a místostarosta. V kanceláři starosty se nachází server s operačním systémem MS Windows Server 2008, který obsluhuje provoz informačního systému HELIOS Fenix. Chod serveru v případě výpadku proudu zajišťuje UPS. Zálohování uživatelských stanic probíhá každý den na datové úložiště NAS, které je stejně jako router umístěno v kanceláři starosty. Pro síťovou infrastrukturu jsou použité nestíněné kabely kategorie 5 vedené u stropu v plastových lištách.

3.2.1 Hardware

- Kabeláž UTP kategorie 5
- Počítače: CPU Intel Pentium 4x2,6 GHz; RAM 2GB; HDD 500GB
- Notebooky: CPU Intel Pentium, 4x2,56 GHz; RAM 2GB; HDD 250GB
- Server: CPU: Intel Xeon; 3MB cache, processor 2.40GHz, 95W, RAM: 4GB (2x2), počet slotů: 4; HDD: 2x500G

- NAS: 2x 2.5/3.5" SATA II/III HDD nebo SSD, CPU Realtek RTD1296 Quad-core 1.4 GHz, 2GB DDR4, RAID 0, 1 nebo JBOD
- UPS
- Multifunkční síťová tiskárna
- Router

3.2.2 Software

Na všech počítačích je nainstalovaný operační systém MS Windows 10. Zaměstnanci, kteří mají přidělený počítač, mají na počítači vytvořený účet s heslem do systému. Na všech počítačích se nachází běžné kancelářské aplikace MS Office 2013, antivirový program ESET Smart Security Premium, pro veřejnou správu slouží primárně aplikace informačního systému HELIOS Fenix. Informační systém, který je dostupný na všech stanicích, obsahuje moduly Účetnictví, Pokladna, Výkaznictví, Kniha došlých faktur, Pohledávky a místní poplatky, Majetek, Banka, Registr obyvatel, Územně identifikační registr a Registr nemovitostí.

3.3 Analýza zabezpečení objektu

Budova, kde sídlí obecní úřad, je situována na náměstí v centru obce. Tuto budovu sdílí s více subjekty. Pobočka České pošty a obecního úřadu se nachází v přízemí dvoupatrové budovy s tím, že je obecní úřad oddělen od ostatních částí objektu a má svůj vlastní vchod.

Vstup na obecní úřad je v čele budovy. Za vstupními dveřmi se nachází první kancelář, kde sídlí sekretářka, zároveň se zde nachází podatelna a Czech POINT. Dalšími dveřmi se dostaneme do kanceláře ekonomky. Dále se zde nachází dvě kanceláře, jedna z nich pro starostu a druhá pro místostarostu. Všechny dveře jsou opatřeny zámkem. V budově je instalován bezdrátový zabezpečovací systém s detektorem pohybu a požáru. V objektu se nenachází žádný bezpečnostní kamerový systém. Všechny okna i vstupní dveře jsou zabezpečený mřížemi a zámkem.

3.4 Analýza rizik

V této části práce budou analyzovány a ohodnoceny rizika organizace. Abychom mohli zkoumat míru rizik, musíme mít k dispozici informace o aktivech, kterých se tato rizika týkají. Proto musí být nejprve provedena identifikace a ohodnocení aktiv. Dále je

potřeba identifikovat hrozby a určit pravděpodobnost jejich výskytu. Následně vyhodnotíme zranitelnost jednotlivých aktiv a konečně vypočítáme míru rizika.

3.4.1 Identifikace a hodnocení aktiv

K hodnocení aktiv je třeba stanovit škálu (stupnici) hodnotících kritérií od nejméně důležitých až po nejdůležitější aktiva. Tuto stupnici můžeme vidět v první tabulce, kde hodnota 1 znamená nízkou hodnotu aktiva a naopak hodnota 5 značí vysokou hodnotu aktiva pro organizaci a zároveň potenciálně velký dopad na chod organizace. Jednotlivé váhy a jejich slovní hodnocení můžeme vidět v tabulce číslo 1.

Tabulka 1: Stupnice hodnocení aktiv (Zdroj: 4)

Hodnocení aktiva	Míra dopadu
1	Žádný dopad na organizaci
2	Zanedbatelný dopad na organizaci
3	Potíže či finanční ztráta
4	Vážné potíže či podstatné finanční ztráty
5	Existenční potíže

Za pomoci odpovědného zaměstnance úřadu byla provedena identifikace a ohodnocení aktiv. Identifikované aktiva městyse jsou uvedeny v následující tabulce včetně jejich rozdělení do specifických kategorií. U každého aktiva je stanovena hodnota z pohledu důvěrnosti, integrity a dostupnosti. Z těchto hodnot byla vypočítána váha aktiva pomocí zprůměrování těchto hodnot.

Tabulka 2: Identifikace a ohodnocení aktiv

Kategorie	Aktivum	Dostupnost	Důvěrnost	Integrita	Váha
Data	Osobní údaje	3	5	4	4
	Účetní data	3	5	4	4
	Dokumenty a smlouvy	3	5	4	4
	Zálohy dat	4	5	5	5
Hardware	Pracovní stanice	2	3	3	3
	Multifunkční tiskárny	1	1	1	1
	ICT Infrastruktura	4	3	4	4
	Server	3	4	2	3
	Přenosná média	2	3	3	3

	UPS	3	1	1	2
	Datové úložiště NAS	4	5	4	4
Software	Operační systém	3	2	2	2
	Informační systém	3	4	4	4
	Programové vybavení	2	3	3	3

3.4.2 Identifikace zranitelností a hrozeb

Aby bylo možné sestavit matici zranitelnosti, je důležité identifikovat nejdříve samotné hrozby a pravděpodobnost jejich výskytu. K hodnocení pravděpodobnosti bude opět použita škála 1 až 5. Hodnota 1 značí nejméně pravděpodobnou hrozbu, naopak hodnota 5 značí hrozbu nejpravděpodobnější. Při identifikaci hrozeb jsem používal normu ISO/IEC 27005, kde jsou uvedeny všechny typické hrozby.

Tabulka 3: Stupnice hodnocení hrozeb

Hodnocení hrozby	Pravděpodobnost
1	Velmi nízká
2	Nízká
3	Střední
4	Vysoká
5	Velmi vysoká

Tabulka 4: Identifikace a ohodnocení hrozeb

Kategorie	Hrozba	Pravděpodobnost
Fyzické a přírodní	Požár	1
	Povodeň	1
	Úder blesku	1
Technické	Selhání síťové infrastruktury	2
	Selhání softwaru	3
	Ztráta nebo poškození dat	3
	Selhání koncové stanice	3
Výpadek služeb	Výpadek elektřiny	4
	Výpadek internetového připojení	3
Lidský faktor	Kyberkriminalita	4
	Pochybení zaměstnanců (neúmyslné)	3
	Porušení mlčenlivosti	2
	Záměrné škodlivá činnost	2
	Fyzické narušení objektu	2
	Krádež nebo poškození aktiva	3
	Kompromitace hesel	2

3.4.3 Matice zranitelnosti

Po dokončení identifikace a ohodnocení aktiv a hrozeb, můžeme tyto veličiny postavit proti sobě do jedné tabulky a posoudit zranitelnost jednotlivých aktiv. I zde je zranitelnost vyjádřena škálou 1 až 5, kde vyšší hodnota vyjadřuje vyšší zranitelnost. Hrozba však vždy nemusí působit na každé aktivum plnou mírou, respektive nemusí na aktivum působit vůbec, proto se v tabulce nacházejí a prázdná pole. Sestavenou matici zranitelnosti můžeme vidět v následující tabulce.

Tabulka 5: Matice zranitelnosti

	Pravděpodobnost	Osobní údaje	Účetní data	Dokumenty a smlouvy	Zálohy dat	Pracovní stanice	Multifunkční tiskárny	ICT Infrastruktura	Server	Přenosná média	UPS	Datová úložiště NAS	Operační systém	Informační systém	Programové vybavení
Hodnota aktiva		4	4	4	5	3	1	4	3	3	2	4	2	4	3
Požár	1	5	5	5	5	5	5	5	5	5	5	5	2	2	
Povodeň	1	5	5	5	5	5	5	5	5	5	5	5	2	2	
Úder blesku	1	4	3	3	5	5	5	5	5	2	5	5	2	1	
Selhání síťové infrastruktury	2				2			2	2			2		2	
Selhání softwaru	3	3	3	3	3	1	1	2	1			3	1	1	5
Ztráta nebo poškození dat	3	5	4	4	5										2
Selhání koncové stanice	3	2	3	3		5						2	1	1	1
Výpadek elektřiny	4	2	1	2		4	1	2	2				2	2	2
Výpadek internetového připojení	3	2				2									
Kyberkriminalita	4	5	4	4	4	4			3	3	3	5	2	5	3
Pochybení zaměstnanců (neúmyslné)	3	4	4	4	3	1	2	2	2	2	2	3	2	3	2
Porušení mlčenlivosti	2	5	4	5	2										
Záměrné škodlivá činnost	2	4	4	4	4	2	2	2	2	2	2	2	2	3	2
Fyzické narušení objektu	2	4	2	3	2	3	3	3	3	3	3	3	1	1	1
Krádež nebo poškození aktiva	3	5	5	5	5	5	5	5	5	5	5	5	2	4	4
Kompromitace hesel	2	5	4	4	5	2						5	3	4	3

3.4.4 Matice rizik

Matice rizik se sestavuje pomocí výpočtů míry rizika a to pomocí vzorce $R = T * A * V$, kde „R“ vyjadřuje výslednou míru rizika, „T“ je pravděpodobnost vzniku hrozby, „A“ značí hodnotu aktiva a „V“ vyjadřuje zranitelnost aktiva. Před sestavením matice rizik je ještě nutné stanovit hranice rizik. Tyto hranice jsou popsané v tabulce 6.

Tabulka 6: Hodnotící stupnice pro matici rizik

Míra rizika	Popis
0-10	Bezvýznamné riziko
11-20	Akceptovatelné riziko
21-30	Mírné riziko
31-60	Nežádoucí riziko
61 a více	Nepřijatelné riziko

Tabulka 7: Matice rizik

Hodnota aktiva		Osobní údaje	Účetní data	Dokumenty a smlouvy	Zálohy dat	Pracovní stanice	Multifunkční tiskárny	ICT Infrastruktura	Server	Přenosná média	UPS	Datová úložiště NAS	Operační systém	Informační systém	Programové vybavení	Součet		
	Pravděpodobnost	4	4	4	5	3	1	4	3	3	2	4	2	4	3			
Požár	1	20	20	20	23	13	5	18	15	13	8	22	5	7	0	190	564	
Povodeň	1	20	20	20	23	13	5	18	15	13	8	22	5	7	0	190	472	
Úder blesku	1	16	12	12	23	13	5	18	15	5	8	22	5	4	0	159	504	
Selhání síťové infrastruktury	2	0	0	0	19	0	0	15	12	0	0	17	0	15	0	77	509	
Selhání softwaru	3	36	36	36	42	8	3	22	9	0	0	39	7	11	40	289	275	
Ztráta nebo poškození dat	3	60	48	48	70	0	0	0	0	0	0	0	0	0	16	242	53	
Selhání koncové stanice	3	24	36	36	0	40	0	0	0	0	0	26	7	11	8	188	235	
Výpadek elektřiny	4	32	16	32	0	43	4	29	24	0	0	0	19	29	21	249	219	
Výpadek internetového připojení	3	24	0	0	0	16	0	0	0	0	0	0	0	0	0	40	147	
Kyberkriminalita	4	80	64	64	75	43	0	0	36	32	20	87	19	73	32	624	97	
Pochybení zaměstnanců (neúmyslné)	3	48	48	48	42	8	6	22	18	16	10	39	14	33	16	368	425	
Porušení mlčenlivosti	2	40	32	40	19	0	0	0	0	0	0	0	0	0	0	131	121	
Záměrné škodlivá činnost	2	32	32	32	37	11	4	15	12	11	7	17	9	22	11	251	293	
Fyzické narušení objektu	2	32	16	24	19	16	6	22	18	16	10	26	5	7	5	222	197	
Krádež nebo poškození aktiva	3	60	60	60	70	40	15	55	45	40	25	65	14	44	32	625		
Kompromitace hesel	2	40	32	32	47	11	0	0	0	0	0	43	14	29	16	264		
Součet		564	472	504	509	275	53	235	219	147	97	425	121	293	197			

3.4.5 Vyhodnocení analýzy rizik

Z výsledné matice rizik vyplývá, že mezi nejvíce riziková aktiva úřadu patří osobní údaje, zálohy dat, účetní data, dokumenty, smlouvy a datové úložiště NAS. Jedná se tedy především o data, informace nebo jejich nosiče. Zároveň se většinou jedná o citlivé a diskrétní informace. V případě ztráty nebo úniku těchto dat hrozí finanční a právní spory. Proto by se měl úřad soustředit na jejich zabezpečení a přiměřeně investovat do jejich ochrany. Mezi největší hrozby patří kyberkriminalita, krádež nebo poškození aktiva a neúmyslné pochybení zaměstnanců.

4 VLASTNÍ NÁVRH ŘEŠENÍ

Na základě provedených analýz je sestaven konkrétní návrh řešení pro zlepšení stavu bezpečnosti informací podle ISMS. Opatření budou navržená na základě analytické části práce a v souladu s normou ČSN ISO/IEC 27001:2013.

Úřad nemá motivaci zavádět ISMS z toho pohledu, že to tento sektor přímo nevyžaduje a žádný z dodavatelů či jiných institucí tento systém po úřadu nepožaduje. Zároveň obec zatím nemá vyhrazené zdroje, jak finanční tak personální, pro tento projekt. Avšak obec si uvědomuje důležitost bezpečnosti informací a chce být preventivně chráněna a seznámena s hrozbami, které na úřad a její aktiva působí.

Na základě provedené analýzy jsem se rozhodl vypracovat projekt implementující soubory opatření, které ošetřují největší rizika, která na organizaci působí, rizika z kategorie nepřijatelné. Primárně se tedy především rizika následující – kyberkriminalita, neúmyslné pochybení zaměstnanců a krádež nebo poškození aktiva. Také se zaměřím na aktiva, která vyžadují vysokou úroveň zabezpečení.

V této práci se tedy zaměřím na popis implementace následujících souborů opatření:

- A.7 Bezpečnost lidských zdrojů,
- A.11 Fyzická bezpečnost a bezpečnost prostředí a
- A.12 Bezpečnost provozu,

tyto soubory opatření by měly ošetřit rizika bezpečnosti informací s ohledem na výsledky analýzy rizik.

Není nutné zavádět všechna opatření z toho důvodu, že organizace o certifikaci ISMS zatím neusiluje. V následující tabulce je shrnuto, která opatření budou aplikována, která již aplikována jsou a která je třeba revidovat.

Tabulka 8: Soubor opatření

Označení	Opatření	Stav
A.7	**Bezpečnost lidských zdrojů**	
A.7.1	**Před vznikem pracovního vztahu**	
A.7.1.1	Prověřování	Aplikováno
A.7.1.2	Podmínky pracovního vztahu	Aplikováno
A.7.2	**Během pracovního vztahu**	
A.7.2.1	Odpovědnosti vedení organizace	Aplikovat

A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	Aplikovat
A.7.2.3	Disciplinární řízení	Aplikovat
A.7.3	**Ukončení a změna pracovního vztahu**	
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	Aplikováno
A.11	**Fyzická bezpečnost a bezpečnost prostředí**	
A.11.1	**Bezpečné oblasti**	
A.11.1.1	Fyzický bezpečnostní perimetr	Revidovat
A.11.1.2	Fyzické kontroly vstupu	Revidovat
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	Aplikováno
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	Aplikováno
A.11.1.5	Práce v bezpečných oblastech	Neaplikovat
A.11.1.6	Oblasti pro nakládku a vykládku	Neaplikovat
A.11.2	**Zařízení**	
A.11.2.1	Umístění zařízení a jeho ochrana	Revidovat
A.11.2.2	Podpůrné služby	Revidovat
A.11.2.3	Bezpečnost kabelových rozvodů	Aplikováno
A.11.2.4	Údržba zařízení	Aplikovat
A.11.2.5	Přemístění aktiv	Aplikovat
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	Aplikovat
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	Aplikovat
A.11.2.8	Uživatelská zařízení bez obsluhy	Aplikovat
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	Aplikovat
A.12	**Bezpečnost provozu**	
A.12.1	**Provozní postupy a odpovědnosti**	
A.12.1.1	Dokumentované provozní postupy	Revidovat
A.12.1.2	Řízení změn	Aplikovat
A.12.1.3	Řízení kapacit	Aplikovat
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	Neaplikovat
A.12.2	**Ochrana proti malwaru**	
A.12.2.1	Opatření proti malwaru	Revidovat
A.12.3	**Zálohování**	
A.12.3.1	Zálohování informací	Revidovat
A.12.4	**Zaznamenávání formou logů a monitorování**	
A.12.4.1	Zaznamenávání událostí formou logů	Neaplikovat
A.12.4.2	Ochrana logů	Neaplikovat
A.12.4.3	Logy o činnosti administrátorů a operátorů	Neaplikovat
A.12.4.4	Synchronizace hodin	Neaplikovat
A.12.5	**Správa provozního softwaru**	
A.12.5.1	Instalace softwaru na provozní systémy	Aplikovat
A.12.6	**Řízení technických zranitelností**	
A.12.6.1	Řízení technických zranitelností	Aplikovat
A.12.6.2	Omezení instalace softwaru	Aplikovat
A.12.7	**Hlediska auditu informačních systémů**	
A.12.7.1	Opatření k auditu informačních systémů	Neaplikovat

4.1 A.7 Bezpečnost lidských zdrojů

A.7.1 Před vznikem pracovního poměru

Cíl: *„Zajistit, aby zaměstnanci a smluvní strany chápali své povinnosti, a zajistit, aby byli vhodní pro úlohy, pro které jsou uvažováni“* (12, s.15).

A.7.1.1 Prověřování

Opatření: „*Prověření minulosti všech uchazečů o zaměstnání by mělo být prováděno v souladu s příslušnými zákony, nařízeními a v souladu s etikou a mělo by být úměrné požadavkům souvisejícím s činností organizacím klasifikací informací, ke kterým má být umožněn přístup, a vnímaným rizikům“* (12, s.15).

Toto opatření je již aplikováno, uchazeč o zaměstnání je řádně prověřen. Organizace se ověřuje uchazeče pomocí minimálně jednoho posudku, životopisu, potvrzení proklamovaného vzdělání a odborné kvalifikace, dokladu totožnosti i pomoci výpisu z rejstříku trestů.

A.7.1.2 Podmínky pracovního poměru

Opatření: *„Smlouvy se zaměstnanci a smluvními stranami by měly uvádět odpovědnosti zaměstnanců/smluvních stran a organizace za bezpečnost informací“* (12, s.16).

Smluvní povinnosti zaměstnanců musí odrážet politiky organizace pro informační bezpečnost. Je důležité, aby bylo splněno a vyjasněno, že před získáním přístupu k citlivým informacím musí být podepsána smlouva o ochraně informací a o zachování mlčenlivosti. Měla by být stanovena odpovědnost za klasifikaci informací a správu aktiv organizace spojených s informacemi a také povinnost zaměstnance ve vztahu k nakládání s informacemi získaných od jiných subjektů. A také upřesnit opatření, která budou následovat v případě nedodržení bezpečnostních požadavků. Tyto podmínky jsou již zahrnuty v pracovní smlouvě, opatření je tedy implementováno.

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“* (12, s.17).

A.7.2.1 Odpovědnosti vedení organizace

Opatření: „*Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustanovenými politikami organizace"* (12, s.17).

Starosta by měl být zodpovědný za seznámení podřízených osob s pravidly, povinnostmi a rolemi ve vztahu k bezpečnosti informací. Po každém zaměstnanci by mělo být vyžadováno dodržovat bezpečnostní pokyny, se kterými je řádně seznámen. Vedení organizace je zodpovědné za kontinuální vzdělávání a motivování zaměstnanců v oblasti bezpečnosti informací. Vedení má také povinnost zřídit anonymní kanál pro ohlašování porušení politik nebo postupů v oblasti bezpečnosti informací.

Popis	Časový rozsah	Náklady
Vytvoření odpovědností a rolí bezpečnosti informací	6 hodin	6x1000 Kč
Vytvoření motivačního plánu	5 hodin	5x300 Kč

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Opatření: Všichni zaměstnanci úřadu, kteří mají relevantní vztah k bezpečnosti informací, musí dostávat odpovídající vzdělání a školení pro zvyšování podvědomí bezpečnosti informací a musí být pravidelně informováni o změnách v politikách a postupech bezpečnosti informací. Vzdělání a školení je nutné provádět pravidelně a je nutno určit personál, který toto školení vyžaduje (12).

Toto opatření by mělo vést ke snížení rizika neúmyslné pochybení zaměstnanců a kyberkriminality. Je doporučeno provést vstupní proškolení pro nové zaměstnance a zaměstnance, kteří ještě nebyli v této problematice proškoleni a následně v pravidelných cyklech provádět školení, které znalosti doplňuje a aktualizuje. Na úřadě není zaměstnaná osoba, která by mohla provádět školení v této oblasti, je tedy nutné využít externí školící společnost. Náklady dvoudenního vstupního proškolení v této problematice jsou 8000,- Kč za jednoho zaměstnance. Náklady na pravidelné přeškolení, které probíhá jednou za dva roky, jsou vyčísleny na 4000,- Kč za jednoho zaměstnance. Absolvováním těchto školení by mělo dojít k snížení rizika neúmyslného pochybení zaměstnanců a snížení rizika kyberkriminality, přičemž by měli být zaměstnanci více imunní proti nástrahám virtuálního prostředí a zaměstnanci by měli být schopni rozpoznat bezpečnostní hrozby a incidenty a umět na ně reagovat. Součástí

tohoto bodu je také vytvoření související dokumentace, která bude udržovat záznamy o vzdělání a školení, plán a pravidla jako například koho a co školit.

Popis	Časový rozsah	Náklady
Vytvoření politik pro školení	4 hodiny	4x 1000 Kč
Vstupní školení	2 dny	4x 8000 Kč
Pravidelná školení	1 den/2 roky	4x 2000 Kč

A.7.2.3 Disciplinární řízení

Opatření: „*Měly by existovat formální disciplinární proces, oznámený všem, pro podniknutí kroků vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací*“ (12, s.18).

Disciplinární proces není možné zahájit bez ověření, že došlo k narušení informační bezpečnosti. V případě že došlo k narušení, je třeba vést správný a spravedlivý disciplinární proces s podezřelým zaměstnancem. V tomto procesu by se měly stanovit odstupňované reakce, které berou v potaz okolnosti jako například povahu a závažnost narušení nebo vliv na organizaci. Dále je nutno vzít v úvahu jestli se jedná o první nebo opakovaný přestupek a jestli byl zaměstnanec řádně proškolen. Uvedené náklady jsou náklady za vypracování disciplinárního řízení a souvisejících smluv advokátní kanceláří.

Popis	Časový rozsah	Náklady
Vytvoření postupů disciplinárního řízení		5000 Kč

A.7.3 Ukončení a změna pracovního poměru

Cíl: „*Chránit zájmy organizace jako součást procesu změny nebo ukončení pracovního poměru*“ (12, s.19).

A.7.3.1 Odpovědnosti při ukončení a změně pracovního poměru

Opatření: „*Odpovědnosti a povinnosti v oblasti informační bezpečnosti, které zůstávají v platnost i po ukončení zaměstnání, by měly být definovány, sděleny zaměstnanci nebo smluvní straně a měly by být prosazovány*“ (12, s.19).

Zaměstnanci musí po ukončení pracovního vztahu respektovat bezpečnostní požadavky a odpovědnosti plynoucí z pracovní smlouvy a smlouvy o mlčenlivosti. Tyto požadavky jsou již zahrnuty v pracovní smlouvě.

4.2 A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Bezpečné oblasti

Cíl: „*Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace*“ (12, s.33).

A.11.1.1 Fyzický bezpečnostní perimetr

Opatření: „*Měly by být definovány bezpečnostní perimetry a ty by měly být použity k ochraně oblastní, které obsahují buď citlivé, nebo kritické informace a vybavení pro zpracování informací*“ (12, s.33).

Bezpečnostní perimetry by měly být definovány a jejich síla a umístění by měly být odvozené od bezpečnostních požadavků aktiv, od technických a ekonomických možností organizace a od výsledků analýzy rizik. Perimetr by neměl být nikde přerušen – neměla by být nikde místa, kudy lze proniknout. Měla by být zřízena recepce s obsluhou nebo jiný nástroj pro řízení fyzického přístupu do budovy.

Přiměřený fyzický bezpečnostní perimetr je již na objekt aplikován, avšak není nikde definován a popsán. Bezpečnostní perimetr je tvořen zdmi budovy, bezpečnostními dveřmi, mřížováním na oknech a dveřích a alarmem. Je nutné vytvořit popis perimetru, jeho umístění a na jakých aktivech a rizicích je závislý. Dále je nutné vytvořit plán kontroly fyzického bezpečnostního perimetru. Návrh směrnice fyzického bezpečnostního perimetru se nachází v příloze I.

Popis	Časový rozsah	Náklady
Definování fyzického perimetru a plánu jeho kontroly	4 hodiny	4x1000 Kč
Kontrola fyzického perimetru	4 hodiny/rok	4x300 Kč

A.11.1.2 Fyzické kontroly vstupu

Opatření: „*Zabezpečené oblasti by měly být na vstupu chráněny vhodnými opatřeními, aby se zajistilo, že přístup mají povolen pouze oprávněné osoby*“ (12, s.33).

V úředních hodinách je volný přístup na obecní úřad do první místnosti, kde se nachází podatelna a sekretářka, není tedy možnost, aby se potenciální útočník dostal do budovy bez povšimnutí. Do ostatních prostor budovy nemá veřejnost volný přístup. Měla by být zvážena opatření evidence totožnosti, data a času příchodu a odchodu návštěvníků, kteří vstupují do oblastí, kam nemá veřejnost přístup a kde jsou uchovávaný důvěrné

informace. Návrh směrnice pro fyzické kontroly vstupu a záznam fyzického vstupu se najdeme v příloze II.

Popis	Časový rozsah	Náklady
Vytvoření knihy záznamů přístupů	1 hodin	1x300 Kč

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Opatření: „*Měla by být navržena a uplatněna opatření pro fyzickou bezpečnost kanceláře, místností a vybavení“* (12, s.34).

Toto opatření je již zavedeno, všechny kanceláře jsou opatřeny zámkem, okna jsou zabezpečena mřížemi, na úřadě je instalován bezpečnostním systémem detektoru pohybu, který je aktivní v době nepřítomnosti zaměstnanců. První místnost funguje jako recepce s obsluhou, kam je volný přístup pro veřejnost, do dalších částí objektu mohou pouze oprávněné osoby.

A.11.1.4 Ochrana před vnějšími a přírodními hrozbami

Opatření: „*Měla by být navržena a uplatněna fyzická ochrana před přírodními katastrofami, zlomyslnými útoky nebo nehodami“* (12, s.35).

Toto opatření je již aplikováno v přiměřeném rozsahu. V budově je instalován požární detektor, před úderem blesku budovu chrání hromosvod a přepěťová ochrana. Vzhledem ke geografické poloze objektu není objekt ohrožen povodněmi ani zemětřesením.

A.11.2 Zařízení

Cíl: „*Zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace“* (12, s.36).

A.11.2.1 Umístění zařízení a jeho ochrana

Opatření: „*Zařízení by mělo být umístěno a chráněno tak, aby byla snížena rizika z hrozeb a nebezpečí ze strany životního prostředí a z možností neoprávněného přístupu“* (12, s.36).

Zařízení umístěná v první místnosti jsou umístěna v prostorech, kam má veřejnost přímý přístup. Výpočetní technika by měla být umístěna v zamykatelných skříňkách a klíče od zámků by měly být uschovány na bezpečném místě, s tím že jejich výpůjčka

bude evidována. Vybavení pro ukládání dat by mělo být zabezpečeno, aby se zabránilo neoprávněnému přístupu. Před bleskem je budova chráněna hromosvodem a přepěťovou ochranou. Dále by měla být stanovena pravidla pro stravování, pití a kouření v blízkosti vybavení pro zpracování a uložení informací. Aktivní prvky a server jsou umístěny v citlivé zóně, v kanceláři starosty, od které mají klíče pouze odpovědně osoby. Je to nejvhodnější místnost v budově, avšak zařízení by měly být bezpečně umístěny ve skříni se zámkem. Návrh pravidel pro umístění zařízení a jeho ochranu jsou uvedeny v příloze III.

Popis	Časový rozsah	Náklady
Úložné skříně pro počítačové stanice		2x1000 Kč
Serverová skříň		9000 Kč
Instalace skříní	4 hodiny	4x600 Kč
Vytvoření pravidel pro umístění zařízení a jeho ochrany	3 hodiny	3x1000 Kč

A.11.2.2 Podpůrné služby

Opatření: Zařízení by mělo být chráněno před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb (elektřiny, telekomunikace, zásobování vodou, kanalizace, větrání a klimatizace) (12).

Pro předcházení výpadku napájení klíčových zařízení (server, NAS) je k dispozici UPS zařízení. UPS zařízení zajišťuje napájení při výpadku primárního zdroje elektřiny, tak aby bylo se předešlo ztrátám dat. U zařízení není pravidelně kontrolovaná jeho funkčnost a připravenost. Je tedy nutné zavést politiky pro pravidelnou kontrolu tohoto zařízení a samozřejmě správné zapojení tohoto zařízení. Navrhuji také zakoupit další UPS zařízení pro osobní počítače.

Popis	Časový rozsah	Náklady
UPS pro počítače		2000 Kč
Instalace UPS	2 hodiny	2x600 Kč
Kontrola záložních zdrojů	2 hodiny/půlroku	4x600 Kč

A.11.2.3 Bezpečnost kabelových rozvodů

Opatření: *Silová a telekomunikační kabeláž určená pro přenos dat nebo podpůrných informačních služeb by měla být chráněna před odposloucháváním, rušením nebo poškozením* (12, s.37).

Nyní jsou kabely pro komunikace vedeny na stěnách pod stropem v plastových lištách a jsou odděleny od vedení napájecích kabelů, tak aby se zabránilo rušení. Aktivní prvky musí být umístěny na bezpečném místě, toto řeší opatření A.11.2.1.

A.11.2.4 Údržba zařízení

Opatření: „*Zařízení by mělo být správně udržováno pro zajištění jeho stálé dostupnosti a integrity*“ (12, s.37).

Zařízení musí být udržována v souladu s doporučenými servisními intervaly a specifikací dodavatele. Opravy a servis by měla být prováděny pouze autorizovanými pracovníky. Všechny podezřelé stavy a chyby by měly být zaznamenány stejně tak jako informace o nápravné a preventivní údržbě. Měly by být dodrženy všechny požadavky na údržbu vyplývající z pojistných smluv (12).

Je tedy nutné vytvořit dokumentaci, která obsahuje přehledný seznam zařízení s doporučenými servisními intervaly a specifikací dodavatele, se záznamy o opravách, servisu zařízení a chybách zařízení. V případě údržby zařízení externím technikem nebo odesláním zařízení mimo objekt musí být zajištěno, že nedojde k úniku citlivých informací a jestliže ano musí být zajištěno uložení informací na bezpečné médium.

Popis	Časový rozsah	Náklady
Vytvoření dokumentace o servisu zařízení	6 hodin	6x300 Kč
Servis zařízení		5000 Kč /rok

A.11.2.5 Přemístění aktiv

Opatření: „*Zařízení, informace nebo software by neměly být přemístěny mimo organizaci bez předchozího povolení*“ (12, s.37).

Povolení o přemístění aktiva uděluje vlastník aktiva respektive jeho nadřízený. Při udělení povolení musí být přihlédnuto k tomu, o jaké aktivum se jedná a o jak citlivé aktivum se jedná, za jakým účelem má být přemístěno, kdo ho chce přemístit a na jaký časový interval má být aktivum přemístěno. Při navrácení aktiva by měl být ověřen soulad. Je nutné, aby byla zaznamenána identita osoby, která přemístila aktivum, časový interval přemístění a aby byla zaznamenáno jeho navrácení.

Popis	Časový rozsah	Náklady
Vytvoření politik pro přemístění aktiv	3 hodiny	3x1000Kč

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Opatření: „*Bezpečnost by se měla týkat aktiv mimo prostory organizace, s přihlédnutím k různým rizikům činnosti mimo prostory organizace*“ (12, s.38).

Použití zařízení pro zpracování informací mimo prostory organizace musí být schváleno vedoucím zaměstnance. Při použití zařízení mimo organizaci musí být splněno:

Zařízení nebo média, která jsou přemístěná mimo organizaci, nesmí být ponechána bez dozoru. Při použití zařízení mimo organizaci musí být dodržovány pokyny výrobce. Musí být zvoleny přiměřená opatření pro konkrétní lokalitu pracoviště na základě posouzených rizik. Rizika poškození, krádeže apod. se mohou lišit podle lokality, je tedy nutné vybrat vhodné opatření (např. uzamykatelné skříňky, politiky prázdného stolu, zabezpečené komunikace atd.)

Popis	Časový rozsah	Náklady
Vytvoření politiky bezpečnosti zařízení a aktiv mimo prostory organizace	3 hodiny	3x1000 Kč

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Opatření: „*Všechny části zařízení obsahující paměťová média by měly být prověřeny s cílem zajistit, aby byla před likvidací nebo opakovaném použití odstraněna nebo bezpečně přepsána všechna citlivá data a licencovaný software*“ (12, s.38).

Zařízení, které je určeno k likvidaci nebo opakovanému použití, musí být zkontrolováno, jestli neobsahuje paměťová média. Tyto paměťová média musí být fyzicky zničená, vymazána nebo přepsána pomocí technik, které neumožňují obnovení původních dat. K této činnosti je vhodné využít certifikovanou firmu.

Popis	Časový rozsah	Náklady
Vytvoření pravidel pro bezpečnou likvidaci	2 hodiny	2x1000 Kč

A.11.2.8 Uživatelská zařízení bez obsluhy

Opatření: „*Uživatelé by měli zajistit přiměřenou ochranu neobsluhovaného zařízení*“ (12, s.38).

Měly by být vytvořené politiky, které uživatele informují o bezpečnostních požadavcích a postupech pro ochranu neobsluhovaného zařízení a o odpovědnosti za realizaci této ochrany.

Uživatelé musí dodržovat následující pravidla, uživatelé:

- by měli ukončit aktivní relace po dokončení činnosti, pokud nemohou být zabezpečeny vhodným blokovacím mechanismem, například heslem.
- by se měli odhlásit z aplikací nebo síťové služby, pokud je dále nepotřebují.
- by měli nepoužívané zařízení zabezpečit před neoprávněným použitím pomocí zámku nebo hesla.

S těmito pravidly musí být uživatelé řádně seznámeni, viz opatření 7.2.1.

Popis	Časový rozsah	Náklady
Vytvoření pravidel pro zařízení bez obsluhy	3 hodina	3x1000 Kč

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: „*Pro vybavení pro zpracování informací by měla být přijata zásada prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií, a zásada prázdné obrazovky“* (12, s.39).

Citlivé nebo kritické informace, ať už v papírové podobě nebo na elektronickém paměťovém médiu, by měly být uzamčeny, pokud nejsou využívány, zejména v nepřítomnosti zaměstnance. Počítače bez obsluhy by měly být zamčené a zabezpečené heslem nebo jiným autentizačním prvkem. Média obsahující citlivé nebo klasifikované informace by měla být ihned odebrána z tiskáren.

Tyty zásady snižují riziko neoprávněného přístupu, ztráty a poškození informací během běžné pracovní doby i mimo ni. Se zásadami by měly být zaměstnanci seznámeni a měli by je dodržovat. V příloze IV a V najdeme návrh politiky prázdného stolu respektive návrh informačního plakátu pro podporu dodržování zásad čistého stolu.

Popis	Časový rozsah	Náklady
Vytvoření zásad prázdného stolu	3 hodiny	3x1000 Kč

4.3 A.12 Bezpečnost provozu

A.12.1 Provozní postupy a odpovědnosti

Cíl: „*Zajistit správné a bezpečné provozování vybavení pro zpracování informací“* (12, s.39).

A.12.1.1 Dokumentace provozních postupů

Opatření: *„Provozní postupy by měly být dokumentovány a být k dispozici všem uživatelům, kteří je potřebují“* (12, s.39).

Pro provozní činnosti spojené s vybavením pro zpracování informací a s komunikačním vybavením by měly být připraveny dokumentované postupy, jako jsou postupy pro zapnutí a vypnutí počítače, zálohování, údržba zařízení, zacházení s médii, správa počítačové místnosti a zacházení s poštou a bezpečnost práce. Náklady na vytvoření postupů pro zálohování, údržbu zařízení, správu počítačové místnosti jsou uvedeny v kapitolách (podle pořadí) A.12.3.1 Zálohování informací, A.11.2.4 Údržba zařízení a A.11.2.1 Umístění zařízení a jeho ochrana.

Popis	Časový rozsah	Náklady
Vytvoření dokumentovaných postupů	16 hodin	16x1000 Kč

A.12.1.2 Řízení změn

Opatření: „*Změny v organizaci, podnikových procesech, vybavení pro zpracování informací a systémech, které mají vliv na bezpečnost informací, by měly být řízeny a kontrolovány“* (12, s. 40).

Měla by se určit změny a způsob jejich zaznamenání, posoudit jejich dopad, postup jejich schvalování a ověření splnění jejich požadavků na bezpečnost informací. Se změnou a jejíma podrobnostmi musí být seznámeni všechny zainteresované osoby.

Popis	Časový rozsah	Náklady
Vytvoření politik řízení změn	3 hodiny	3x1000 Kč

A.12.1.3 Řízení kapacit

Opatření: „*K zajištění požadovaného výkonu systému z pohledu budoucích požadavků na kapacity by mělo být používání zdrojů monitorováno, optimalizováno a naplánováno“* (12, s.41).

Z toho důvodu je nutné, aby IT správce pravidelně sledoval, optimalizoval a plánoval výkon systémů. V tomto případě se jedná zejména o kapacitu úložných zařízení a výkon výpočetních zařízení.

Popis	Časový rozsah	Náklady
Kontrola kapacit	4 hodiny/rok	4x600 Kč

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

V dané organizaci se nenachází oddělení vývoje, testování ani provozu, z toho důvodů nebude opatření aplikováno.

A.12.2 Ochrana proti malwaru

Cíl: „*Zajistit, že informace a vybavení pro zpracování informací jsou před malwarem chráněny*“ (12, s.42).

A.12.2.1 Opatření proti malwaru

Opatření: „*Měla by být implementována opatření pro detekci, prevenci a zotavení na ochranu před malwarem, v kombinaci s vhodným zvyšováním povědomí uživatelů*“ (12, s.42).

Na počítačích je již instalován antivirový software NOD32, který detekuje používání podezřelých webových stránek. Software poskytuje komplexní ochranu všech zařízení. Licence tohoto produktu zahrnuje následující technologie: firewall, antiphising, antivirus a antispyware, ochrana proti botnetu, antispam a šifrování dat. Důraz by měl být kladen na vzdělávání uživatelů, jelikož lidský faktor se uvádí jako největší zranitelnost systému.

V rámci opatření by měly být implementovány tyto kroky:

- stěžejním opatřením je antivirový software, který musí být nainstalovaný a zapnutý na všech počítačových stanicích a serverech. Je nutno aby měl systém definované automatické a pravidelné aktualizace,
- na všech uživatelských stanicích musí být spuštěn firewall,
- uživatelé nesmí bez souhlasu správce vypínat antivirovou ochranu a firewall nebo manipulovat s nastavením antivirového softwaru. Uživatelé nesmí přerušovat probíhající testy na přítomnost virů,

- nefunkčnost antivirového systému nebo zjištění viru či jiného abnormálního stavu je nutné ihned oznámit správci IT, který situaci prošetří a zajistí nápravu, v příloze VI nalezneme návrh formuláře pro hlášení jakéhokoliv bezpečnostního incident,
- uživatelé musí absolvovat pravidelné školení týkající se hrozeb v oblasti informační bezpečnosti (viz A.7.2.2) a měly by být pravidelně informováni o aktuálních hrozbách a seznámeni s antivirovým desaterem podle knihy Problematika ISMS v manažerské informatice., viz následující odstavec,
- je zakázáno instalování softwaru a doplňků z neověřených a neschválených zdrojů,
- na web je přístup povolen pouze z výchozího prohlížeče internetu, který pomocí antivirového softwaru filtruje podezřelé a škodlivé webové stránky, na tyto stránky je zakázaný přístup,
- soubory získané z externí sítě, emailu nebo média musí být nejprve skenovány antivirových softwarem.

Uživatelé by měli být seznámeni se základními pravidly v této oblasti uvedenými v seznamu níže. Antivirové desatero podle (7, s.112):

1) Používejte antivirové programy – *Antivirový program je základní stavební kámen celé informační bezpečnosti a chrání všechny vstupní body do informačního systému. V současném globálním světě se nerozlišují zdroje elektronicích dat na „bezpečné“ a „nebezpečné“, ale jen na „potenciálně nebezpečné“. Škodlivé kódy se do počítače mohou dostat pomocí elektronické pošty (v současné době asi nejčastější zdroj nákazy), navštívených webových stránek, prostřednictvím lokální sítě nebo i díky originálnímu CD (prodej zavirovaného software).*

2) Pozor na elektronickou poštu – *Největší nebezpečí v současné době představují škodlivé kódy využívající elektronickou poštu ke svému šíření. Ochrana je postavena na minimalizaci hrozby. K doporučením patří nepoužívat náhled (preview) e-mailové zprávy (některé kódy jsou schopné se aktivovat bez otevření přílohy pouhým otevřením zprávy). Dále je vhodné nepoužívat posílání zpráv v HTML formátu (do něj může být*

třeba při odpovídání vložen ze zavirovaného počítače nebezpečný kód). Prostý test je jediný bezpečný. Pozor na jakékoliv přílohy u elektronické pošty!

3) Pozor na nelegální programy – *Kopírování nelegálních programů mimo autorskoprávní hledisko znamená nebezpečí z hlediska bezpečnostního. Nebezpečí je ve výrobci, který si hlídá legálnost programů na počítačích a v případě neregulérně pořízených programů neumožňují některé z bezpečnostního hlediska kritické funkce (např. záplatování). Příkladem je operační systém Windows XP, který je sice možné v nelegální verzi používat, ale není možné z něj průběžně odstraňovat nebezpečné chyby pomocí služby Windows Update.*

4) Rozmyslete si, jaké webové stránky navštěvujete – *Mnoho webových stránek obsahuje škodlivé kódy, které jsou schopné se přímo instalovat do počítače a zde způsobit řadu problémů. Vyhýbat se „pochybným" stránkám, kde hrozí riziko takovéto nebo podobné infekce (erotika, nelegálně šířené hry, programy a hudba, sériová čísla, cracky, warez, hackeři apod.) je naprostá nutnost.*

5) Používejte personální firewall – *Pokud jste připojeni k internetu, je nezbytně nutné používat personální firewall, což je počítačový program, který kontroluje veškerý datový provoz směřující do počítače i z něj, přičemž blokuje provoz nevyžádaný nebo nežádoucí (útoky hackerů či virů). Mnoho škodlivých kódů současné doby se přitom šíří prostřednictvím internetu (tedy nikoliv pomocí e-mailů nebo zavirovaných souborů). Tyto kódy zpravidla využívají bezpečnostních děr a nedostatků k tomu, aby přímo z internetu napadaly nedostatečně zabezpečené počítače. Problémem je, že antivirové programy si s podobnými kódy zpravidla neporadí. Potíž není technického rázu, ale v principu (síťový červ doputuje do počítače po síti, přičemž „žije" pouze v paměti stroje a pokud si nevytváří na disku konkrétní soubor, antivirové programy jej ignorují). I kdyby jej totiž z paměti odstranili, ve zlomku sekundy je škodlivý kód v paměti počítače znovu. Celý systém by pak skončil v nekonečné smyčce nahrávání a odstraňování červa. Právě před podobnými útoky chrání personální firewall.*

6) Elektronicky podepisujte a šifrujte – *Stoprocentní bezpečnost prostě neexistuje – ani ve světě reálném, ani ve světě kybernetickém. Proto se připravte na možné útoky, a aby jejich případné následky byly co nejmenší. K výborné prevenci patří používání elektronického podpisu, protože umožňuje varovat před jakýmikoliv změnami*

v dokumentech či souborech (a mají-li tyto být napadeny virem, pak jsou samozřejmě modifikovány). Elektronický podpis použitý při komunikaci pak může velmi dobře posloužit k ověření identity odesílatele zprávy (tedy že zprávu skutečně odeslal ten a ten člověk, a nikoliv pouze virus, který se za něj vydává). Technologie šifrování dat zase zajišťuje, že i kdyby se k nim útočník dostal, získá pouze nesmyslnou změť znaků, ale nikoliv použitelné informace. Šifrování navíc chrání nejen před viry, které kradou z počítače dokumenty, ale i proti jakýmkoliv jiným nepovolaným osobám.

7) Získejte informace – *Stokrát prověřená pravda říká, že se lépe bojuje s nepřítelem, kterého známe, než s neznámou hrozbou. Informovanost o problematice antivirových prostředků v odborném tisku poskytne odpovědi na mnohé otázky, stejně jako rady, jak řešit konkrétní situace. Přitom je třeba informace důsledně filtrovat – pokud přijde e-mailem od přítele či kolegy varování před neobludnějším virem všech dob, které vás vyzývá k rozeslání na co nejvíce adres, jde pravděpodobně o hoax (nesmyslná poplašná zpráva, která se šíří světem s cílem obtěžovat uživatele počítačů.)*

8) Důsledně a opakovaně záplatujte – *Většina výrobců software zcela bez uzardění připouští, že jejich programy mohou obsahovat chyby. Připouštění možnosti existence chyb přenáší odpovědnost na uživatele, Takto vznikly právě patche – záplaty. Jedná se o menší programy, které mají za cíl po aplikaci na příslušném počítači upravit zdrojové kódy mateřského programu a jeho konfiguraci tak, aby se odstranily zjištěné problémy. Ty mohou být několikerého rázu – kolize příslušného programu s jiným, špatná funkce v některých případech, nechtěná vlastnost, kterou mohou využít hackeři nebo viry apod.*

9) Zálohujte svá data – *Zálohovat, zálohovat a zase zálohovat! Když nenávratně zmizí z počítače veškerá data, jak dlouho bude trvat jejich obnova ze záloh a jiných zdrojů? Přitom může jít o útok počítačového viru, krádeže počítače či o nešťastnou událost (tekutina v elektronice počítače).*

10) V případě potřeby se obraťte na odborníky – *Následky útoků většiny počítačových virů lze odborně odstranit. K tomu je třeba určitých znalostí a nástrojů. Statistiky jsou v tomto směru neúprosně smutné – plných 95 procent škod přičítaných počítačovým virům nepřipadá na vrub právě jim, ale neodborným pokusům se s nimi vypořádat! Při zašifrování disku virem nelze nejprve odstranit virus, ale použít ho k dešifrování disku, až pak ho lze odstranit (jinak jsou data nenávratně znehodnocena).*

Popis	Časový rozsah	Náklady
Nastavení antivirového softwaru	4 hodiny	4x600 Kč
Vytvoření politik opatření proti malwaru	4 hodiny	4x1000 Kč

A.12.3 Zálohování

Cíl: „*Ochrana před ztrátou dat“ (12, s.43).*

A.12.3.1 Zálohování informací

Opatření: „*Pravidelně by měly být pořizovány a testovány záložní kopie informací, softwaru a bitových kopií systému v souladu se schválenou politikou zálohování“* (12, s.43).

V případě, že nenadále havárie nebo jiné nečekané události způsobující ztrátu dat jsou uživatelská data a systémová data zálohovány. Zálohování probíhá v reálném čase přírůstkovou metodou do centrálního úložiště NAS. Zálohy jsou šifrovaná pomocí šifry AES. Tyto zálohy jsou umístěné ve stejném objektu jako samotná zálohovaná zařízení, je tedy nutné, aby byly pravidelně vytvářeny kopie těchto záloh a aby byly umisťovány do odlišného objektu, tak aby v případě poškození budovy (například požárem) nebyly kopie poškozeny. Jednou z nabízených možností je i zálohování do cloudu, ale jako bezpečnější varianta se jeví zrcadlení dat na další disk, který bude uložen v jiném objektu obce. Dále musí být vytvořeny přesné postupy obnovy, které definují všechny kroky, které je nutné provést pro obnovení dat ze zálohy. Neméně důležitým krokem je pravidelná kontrola stavu záloh a precizní označení všech záloh (co záložní médium obsahuje, datum vytvoření atd.) Navrhuji tedy pořídit externí disk s podporou šifrování, na který se budou jednou za týden zrcadlit kompletní obrazy vytvořené zálohy přírůstkovou metodou.

Popis	Časový rozsah	Náklady
Pořízení externího disku		4000 Kč
Nastavení zálohování	4 hodiny	4x600Kč
Kontrola záloh	1 hodina/měsíc	12x300Kč
Vytvoření politik pro zálohování a postupů pro obnovení ze zálohy	6 hodin	6x1000 Kč

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: „*Zaznamenávat události a vytvářet záznamy“* (12, s.44).

Z důvodu vysoké ceny technologií pro sběr a správu záznamů aktivit uživatelů a nerelevantnímu přínosu bezpečnosti informací, nebude toto opatření aplikováno.

A.12.5 Správa provozního softwaru

Cíl: „*Zajistit integritu provozního software“* (12, s.46).

A.12.5.1 Instalace softwaru na provozní systémy

Opatření: „*Musí být implementovány postupy řízené instalace softwaru na provozních systémech“* (12, s.47).

Opatření tohoto bodu jsou již navržená v odstavci A.12.6.2.

A.12.6 Řízení technických zranitelností

Cíl: „*Zabránit zneužívání technických chyb“* (12, s.47).

A.12.6.1 Řízení technických zranitelností

Opatření: „*Informace o technických zranitelnostech používaných informačních systémů by měly být získávány včas a organizace by měla přijmout vhodná opatření k řešení souvisejícího rizika“* (12, s.47).

Pro účinné řízení technických zranitelností je nezbytný aktuální a kompletní seznam aktiv. Konkrétní informace potřebné pro správu technických zranitelností zahrnují dodavatele softwaru, čísla verzí, aktuální stav nasazení a osobu v organizaci odpovědné za software. V reakci na identifikaci potenciálních technických zranitelností by měla být přijata vhodná a včasná opatření. Pro navázání efektivního procesu řízení technických zranitelností je třeba dodržovat následující pokyny:

- organizace by měla definovat a stanovit role a odpovědnosti spojené s řízením technické zranitelnosti, včetně sledování zranitelnosti, hodnocení rizika zranitelností, oprav, sledování aktiv.
- jakmile byla identifikována potenciální technická zranitelnost, organizace by měla určit související rizika a vhodná opatření, která mají být přijata, takovým opatřením může být záplata zranitelných míst systému nebo použití jiných kontrol. Pokud není k dispozici bezpečnostní záplata, je třeba zvážit jiné kontroly, jako jsou:

1) vypnutí služeb nebo schopností souvisejících se zranitelností,
2) přizpůsobení nebo přidání řízení přístupu, např. firewally apod.,
3) zvýšené monitorování pro detekci útok nebo
4) zvyšování povědomí o této zranitelnosti.

Technické zranitelnosti budou řízeny správcem IT, který v rámci údržby zařízení bude kontrolovat, jestli jsou systémy aktuální a záplatované a zajistí jejich eventuální nápravu.

Popis	Časový rozsah	Náklady
Vytvoření politik řízení technických zranitelností	3 hodiny	3x1000Kč
Vytvoření seznamu softwaru	4 hodiny	4x600Kč
Pravidelná půlroční kontrola		5000Kč

A.12.6.2 Omezení instalace softwaru

Opatření: *„Měla by být zavedena a implementována pravidla pro instalaci softwaru uživateli“* (12, s.49).

Nekontrolovaná instalace softwaru na zařízeních může vést k zavedení zranitelnosti zařízení a následně k úniku informací, ztrátě integrity nebo jiných incidentů týkajících se bezpečnosti informací nebo porušení práv duševního vlastnictví. Pomocí přidělených práv by měla být instalace jakéhokoliv softwaru zakázaná. Eventuální instalace může být provedena pouze administrátorem a za předpokladu, že je software z ověřeného zdroje a že nedojde k ohrožení systému.

Popis	Časový rozsah	Náklady
Vytvoření pravidel pro instalaci softwaru	2 hodiny	2x1000Kč
Nastavení uživatelských práv	4 hodiny	4x600Kč

4.4 Shrnutí opatření

Pro přehlednost jsem vytvořil tabulky, kde se střetávají největší hrozby s navrženými opatřeními, které na dané hrozby přímo působí.

Tabulka 9: Opatření proti pochybení zaměstnanců

Hrozba	Opatření
Pochybení zaměstnanců	Prověřování
	Podmínky pracovního vztahu
	Odpovědnosti vedení organizace
	Povědomí, vzdělávání a školení o bezpečnosti informací
	Disciplinární řízení
	Odpovědnosti při ukončení nebo změně pracovního vztahu
	Uživatelská zařízení bez obsluhy
	Zásada prázdného stolu a prázdné obrazovky monitoru
	Dokumentované provozní postupy
	Zálohování informací
	Omezení instalace software

Tabulka 10: Opatření proti krádeži nebo poškození aktiv

Hrozba	Opatření
Krádež nebo poškození aktiva	Fyzický bezpečnostní perimetr
	Fyzické kontroly vstupu
	Zabezpečení kanceláří, místností a vybavení
	Ochrana před vnějšími hrozbami a hrozbami prostředí
	Umístění zařízení a jeho ochrana
	Údržba zařízení
	Bezpečnost zařízení a aktiv mimo prostory organizace
	Přemístění aktiv
	Bezpečná likvidace nebo opakované použití zařízení
	Uživatelská zařízení bez obsluhy
	Zásada prázdného stolu a prázdné obrazovky

Tabulka 11: Opatření proti kyberkriminalitě

Hrozba	Opatření
Kyberkriminalita	Povědomí, vzdělávání a školení bezpečnosti informací
	Údržba zařízení
	Zařízení bez obsluhy
	Zásada prázdného stolu a prázdné obrazovky monitoru
	Opatření proti malwaru
	Zálohování informací
	Omezení instalace softwaru

4.5 Metriky

Metriky jsou nástroj, který slouží jako ukazatel nebo hodnotící kritérium používané k objektivnímu hodnocení úrovně efektivnosti. Volba vhodných metrik je jedním z klíčových faktorů správného fungování řízení bezpečnosti. Vybral jsem jeden ukazatel pro každou ze zaváděných oblastí opatření. Celkem tedy tři metriky vycházející z normy ISO/IEC 27004:2009.

Ochrana proti škodlivým programům

Název měření	**Ochrana proti škodlivým programům**
Cíl opatření	A.12.2 Ochrana proti malwaru
Objekt měření a atributy	
Objekt měření	1. Hlášení incidentů 2. Logy antivirových programů
Atribut	Incident způsobený škodlivým programem
Popis základní metriky	
Základní metrika	1. Počet bezpečnostních incidentů způsobených škodlivými programy 2. Celkový počet zablokovaných útoků způsobených škodlivými programy
Metoda měření	1. Počet bezpečnostních incidentů způsobených škodlivými programy 2. Spočítání počtu záznamů o zablokovaných útocích
Typ metody měření	1. Objektivní 2. Objektivní
Měřítko	1. Celá čísla od nuly do nekonečna 2. Celá čísla od nuly do nekonečna

Typ měřítka	1. Ordinální 2. Ordinální
Jednotka měření	1. Bezpečnostní incident 2. Záznam
Popis odvozené metriky	
Odvozená metrika	Síla ochrany antivirových programů
Funkce měření	Počet bezpečnostních incidentů způsobených škodlivými programy / Počet detekovaných a zablokovaných útoků způsobených škodlivými programy
Popis indikátoru	
Indikátor	Trend detekovaných útoků, které nebyly zablokovány, za více period hlášení
Analytický model	Porovnává se současný poměr s předcházejícím
Popis rozhodovacích kritérií	
Rozhodovací kritéria	Křivka trendu by měla zůstat pod stanoveným počtem. Výsledný trend by měl být klesající nebo alespoň stabilní.
Výsledky měření	
Interpretace indikátorů	Vzrůstající trend značí zhoršující se shodu, klesající trend ukazuje na zlepšující se shodu. Jestliže je trend vzrůstající, je potřeba prozkoumat příčinu tohoto jevu a zavést další opatření.
Forma hlášení	Spojnice trendu, která popisuje poměr detekce a prevence škodlivých programů, překrytá spojnicemi trendů předešlých period hlášení.
Frekvence/perioda	
Frekvence sběru dat	Měsíčně
Frekvence analýzy dat	Půlročně
Frekvence hlášení	Půlročně

Vyškolený personál ISMS

Název měření	**Vyškolený personál ISMS**
Cíl opatření	A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací
Objekt měření a atributy	

Objekt měření	Databáze zaměstnanců
Atribut	Záznam školení
Popis základní metriky	
Základní metrika	1) Počet zaměstnanců, kteří se zúčastnili školení ISMS v souladu s ročním plánem školení ISMS. 2) Počet zaměstnanců, kteří se měli zúčastnit školení ISMS
Metoda měření	Spočítají se záznamy s řádky týkající se školení se stavem „Zúčastnil(a) se“
Typ metody měření	Objektivní
Měřítko	Číselné
Typ měřítka	Poměrové
Jednotka měření	Zaměstnanec
Popis odvozené metriky	
Odvození metrika	Procento vyškoleného personálu na ISMS
Funkce měření	(Počet zaměstnanců, kteří se zúčastnili školení ISMS/počet zaměstnanců, kteří se měli zúčastnit školení ISMS) x 100
Popis indikátoru	
Indikátor	Sloupcový diagram za použití barevného rozlišení prahů definovaných analytickým modelem.
Analytický model	0-50% červená, 51-80% žlutá, 81-100% zelená
Popis rozhodovacích kritérií	
Rozhodovací kritéria	Červená – je nutné provést zásah a analyzovat příčinu neshody a špatného výkonu Žlutá – indikátor by měl být sledován pro možný nepříznivý trend Zelená – požadovaný stav, není vyžadováno žádné opatření
Výsledky měření	
Formy hlášení	Sloupcový diagram se sloupci barevně rozlišenými na základě rozhodovacích kritérií. Součástí by měl být slovní popis metriky a interpretace výsledků.
Frekvence/perioda	
Frekvence sběru dat	Ročně

Frekvence analýzy dat	Ročně
Frekvence hlášení	Ročně

Finanční ztráta způsobená krádeží nebo poškozením aktiva

Název měření	**Finanční ztráta způsobená krádeží nebo poškozením aktiva**
Cíl opatření	A.11 Fyzická bezpečnost a bezpečnost prostředí
Objekt měření a atributy	
Objekt měření	Krádež nebo poškození aktiva
Atribut	Finanční hodnota aktiv
Popis základní metriky	
Základní metrika	Celková finanční ztráta způsobená poškozením nebo krádeží aktiva
Metoda měření	Součet hodnot finančních ztrát způsobenými krádeží nebo poškozením aktiva
Typ metody měření	Objektivní
Měřítko	Číselné
Typ měřítka	Nominální hodnota
Jednotka měření	Peněžní jednotky
Popis indikátoru	
Indikátor	Grafické zobrazení jednotlivých částek a celkové sumy.
Analytický model	Celková suma by měla být ideálně nulová. Jakékoliv jiné stavy musí být analyzované a případně musí být zavedena další opatření.
Popis rozhodovacích kritérií	
Rozhodovací kritéria	Ideální a přijatelný stav je hodnota 0. Jakákoliv nenulová hodnota musí být analyzována.
Výsledky měření	
Formy hlášení	Grafické zobrazení jednotlivých částek a celkové sumy újmy. Včetně popisu jednotlivých incidentům a příčin.
Frekvence/perioda	

Frekvence sběru dat	Ročně
Frekvence analýzy dat	Ročně
Frekvence hlášení	Ročně

4.6 Ekonomické zhodnocení

Tabulka 12: Ekonomické zhodnocení

Opatření	Lidské zdroje (v Kč)		Finanční zdroje (v Kč)	
	Jednorázové	Opakované (ročně)	Jednorázové	Opakované (ročně)
Bezpečnost lidských zdrojů				
Před vznikem pracovního vztahu				
Prověřování				
Podmínky pracovního vztahu				
Během pracovního vztahu				
Odpovědnosti vedení organizace	6x1000 5x300			
Povědomí, vzdělávání a školení bezpečnosti informací	4x1000		32000	8000
Disciplinární řízení			5000	
Ukončení a změna pracovního vztahu				
Odpovědnosti při ukončení nebo změně pracovního vztahu				
Fyzická bezpečnost a bezpečnost prostředí				
Bezpečné oblasti				
Fyzický bezpečnostní perimetr	4x1000	4x300		
Fyzické kontroly vstupu	1x300			

Zabezpečení kanceláří, místností a vybavení				
Ochrana před vnějšími hrozbami a hrozbami prostředí				
Práce v bezpečných oblastech				
Oblasti pro nakládku a vykládku				
Zařízení				
Umístění zařízení a jeho ochrana	3x1000 4x600		11000	
Podpůrné služby	2x600	4x600	2000	
Bezpečnost kabelových rozvodů				
Údržba zařízení	6x300	5000		
Přemístění aktiv	3x1000			
Bezpečnost zařízení a aktiv mimo prostory organizace	3x1000			
Bezpečná likvidace nebo opakované použití zařízení	2x1000			
Uživatelská zařízení bez obsluhy	3x1000			
Zásada prázdného stolu a prázdné obrazovky monitoru	3x1000			
Bezpečnost provozu				
Provozní postupy a odpovědnosti				
Dokumentované provozní postupy	16x1000			
Řízení změn	3x1000			
Řízení kapacit		4x600		
Princip oddělení prostředí vývoje, testování a provozu				
Ochrana proti malwaru				
Opatření proti malwaru	4x1000 4x600			
Zálohování				
Zálohování informací	4x600 6x1000	12x300	4000	

Zaznamenávání formou logů a monitorování				
Zaznamenávání událostí formou logů				
Ochrana logů				
Logy o činnosti administrátorů a operátorů				
Synchronizace hodin				
Správa provozního softwaru				
Instalace softwaru na provozní systémy				
Řízení technických zranitelností	3x1000 4x600			5000
Řízení technických zranitelností				
Omezení instalace softwaru	2x1000 4x600			
Hlediska auditu informačních systémů				
Opatření k auditu informačních systémů				
Celkem	**81800**	**14600**	**54000**	**13000**

Celkem tvoří jednorázové zaváděcí náklady podle odhadu 135800 Kč a pravidelné roční náklady na opatření jsou 27600 Kč. Hodinové mzdy se liší podle toho, jaká činnost je třeba vykonat a tedy podle typu specializace osoby, nejnižší hodinovou mzdou 300 Kč/hodinu jsou ohodnoceny úkoly, které můžou vykonat zaměstnanci úřadu, mzda 600 Kč/hodinu je mzdou servisního IT technika a mzda 1000 Kč/hodinu náleží externímu specialistovi informační bezpečnosti. Hodnoty mezd i časových údajů jsou pouze orientační a mohou se lišit od reálného projektu.

Roční rozpočet schvalovaný obecním zastupitelstvem se pohybuje okolo 30000000 Kč. Zaváděcí náklady by tedy poměrově tvořili necelé půl procento ročního rozpočtu obce.

4.7 Časový harmonogram

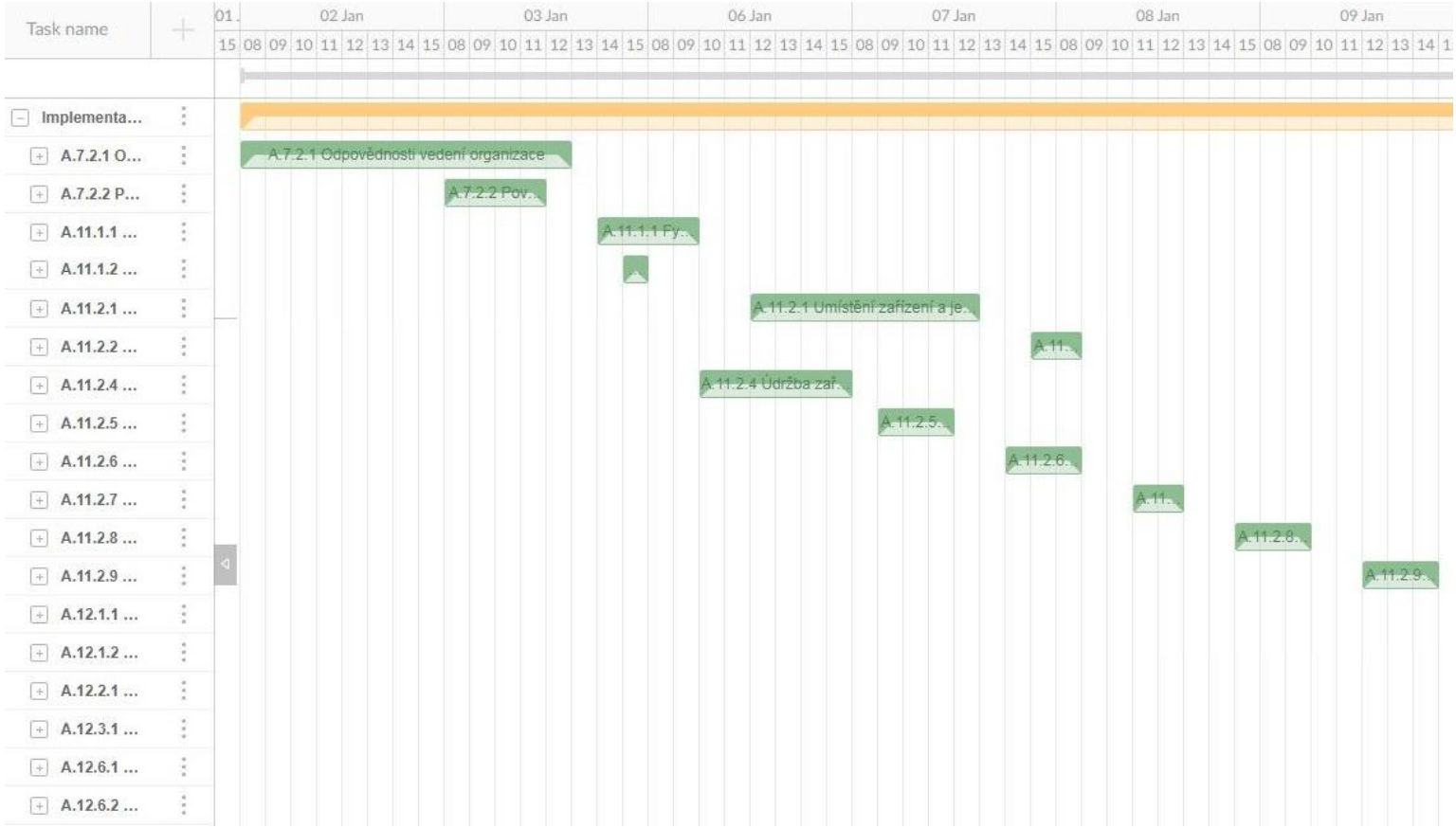
Všechny výše popsané opatření by měly být součástí první etapy, která implementuje opatření působící na největší hrozby. Začátek projektu implementace jsem stanovil na začátek příštího roku, jelikož na příští rok, už by mohly být teoreticky uvolněny prostředky pro tento projekt. Pro zpracování časového plánu jsem využil Ganttův diagram, kam jsem zadal časové hodnoty a návaznost činností a vypočítal odhadovanou

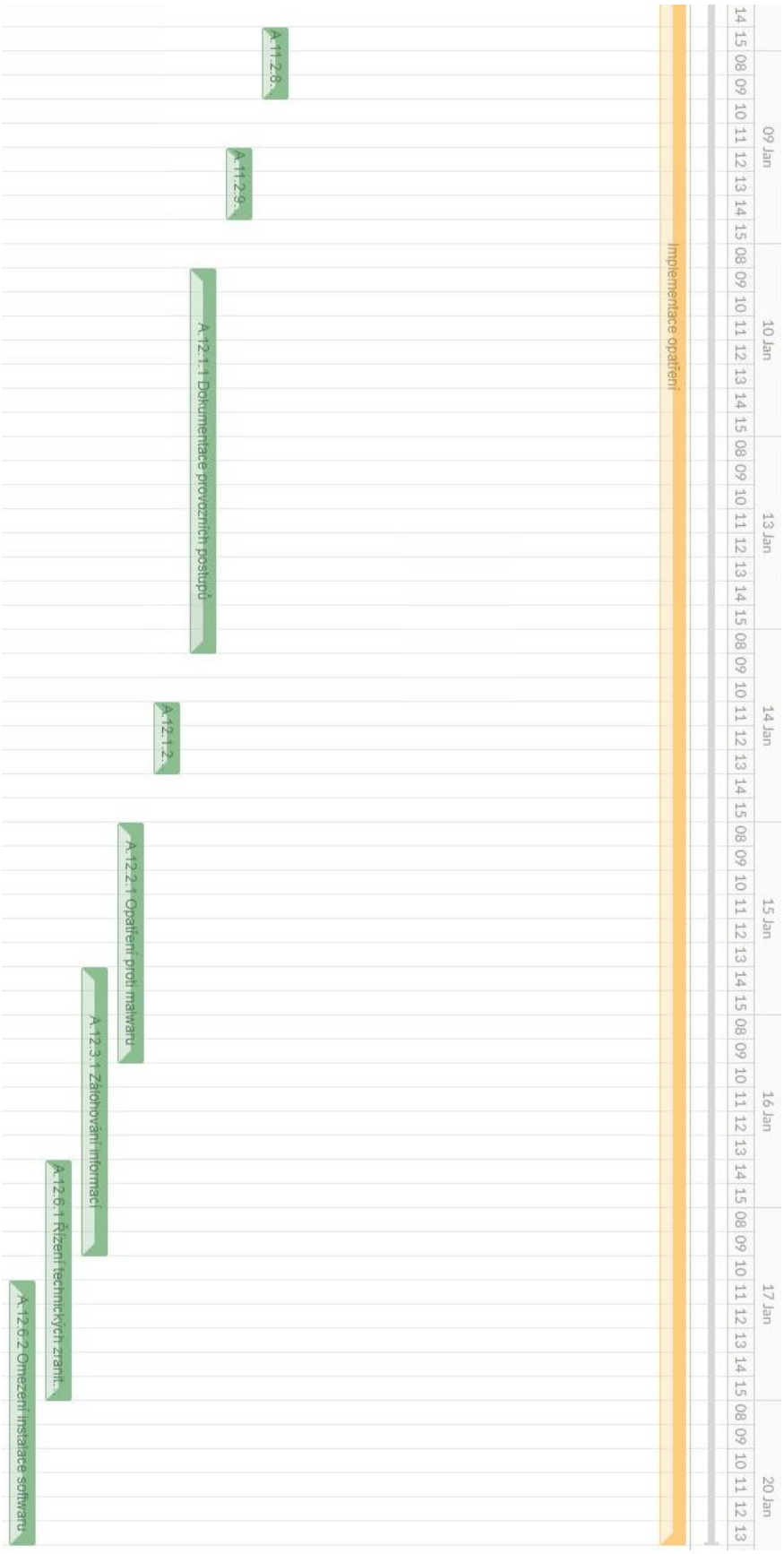
celkovou délku implementace opatření první etapy. Pořadí činností jsem volil podle toho, jak na sebe logicky navazují respektive podle jejich priority, čím vyšší priorita, tím dřív začne jejich realizace. Tabulka 13 obsahuje seznam všech činností s přiřazenou zodpovědnou osobou za aktivitu, začátkem činnosti a jejím trváním.

Tabulka 13: Časový harmonogram

Popis	Přiřazeno	Začátek	Trvání (v hod.)
Celkový odhad		02/01/20 08:00	102
Implementace opatření		02/01/20 08:00	102
A.7.2.1 Odpovědnosti vedení organizace		02/01/20 08:00	13
Vytvoření odpovědností a rolí bezpečnosti informací	Specialista IB	02/01/20 08:00	6
Vytvoření motivačního plánu	Starosta	03/01/20 08:00	5
A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací		03/01/20 08:00	4
Vytvoření dokumentace	Specialista IB	03/01/20 08:00	4
A.11.1.1 Fyzický bezpečnostní perimetr		03/01/20 14:00	4
Definování fyzického perimetru a plánu jeho kontroly	Specialista IB	03/01/20 14:00	4
A.11.1.2 Fyzické kontroly vstupu		03/01/20 15:00	1
Vytvoření knihy záznamů přístupů	Starosta	03/01/20 15:00	1
A.11.2.1 Umístění zařízení a jeho ochrana		06/01/20 12:00	9
Instalace úložných skříní	IT technik	07/01/20 09:00	4
Vytvoření pravidel pro umístění zařízení a jeho ochrany	Specialista IB	06/01/20 12:00	3
A.11.2.2 Podpůrné služby		07/01/20 15:00	2
Instalace UPS	IT technik	07/01/20 15:00	2
A.11.2.4 Údržba zařízení		06/01/20 10:00	6
Vytvoření dokumentace o servisu zařízení	Starosta	06/01/20 10:00	6
A.11.2.5 Přemístění aktiv		07/01/20 09:00	3
Vytvoření politik pro přemístění aktiv	Specialista IB	07/01/20 09:00	3
A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace		07/01/20 14:00	3
Vytvoření politiky bezpečnosti zařízení a aktiv mimo prostory organizace	Specialista IB	07/01/20 14:00	3
A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení		08/01/20 11:00	2
Vytvoření pravidel pro bezpečnou likvidaci	Specialista IB	08/01/20 11:00	2
A.11.2.8 Uživatelská zařízení bez obsluhy		08/01/20 15:00	3
Vytvoření pravidel pro zařízení bez obsluhy	Specialista IB	08/01/20 15:00	3
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky		09/01/20 12:00	3

monitoru			
Vytvoření zásad prázdného stolu	Specialista IB	09/01/20 12:00	3
A.12.1.1 Dokumentace provozních postupů		10/01/20 09:00	16
Vytvoření dokumentovaných postupů	Specialista IB	10/01/20 09:00	16
A.12.1.2 Řízení změn		14/01/20 11:00	3
Vytvoření politik řízení změn	Specialista IB	14/01/20 11:00	3
A.12.2.1 Opatření proti malwaru		15/01/20 08:00	10
Nastavení antivirového softwaru	IT technik	15/01/20 14:00	4
Vytvoření politik opatření proti malwaru	Specialista IB	15/01/20 08:00	4
A.12.3.1 Zálohování informací		15/01/20 14:00	12
Nastavení zálohování	IT technik	16/01/20 14:00	4
Vytvoření politik pro zálohování a postupů pro obnovení ze zálohy	Specialista IB	15/01/20 14:00	6
A.12.6.1 Řízení technických zranitelností		16/01/20 14:00	10
Vytvoření politik řízení technických zranitelností	Specialista IB	16/01/20 14:00	3
Vytvoření seznamu softwaru	IT technik	17/01/20 12:00	4
A.12.6.2 Omezení instalace softwaru		17/01/20 11:00	11
Vytvoření pravidel pro instalaci softwaru	Specialista IB	17/01/20 11:00	2
Nastavení uživatelských práv	IT technik	20/01/20 10:00	4


Task name
01
02 Jan
03 Jan
06 Jan
07 Jan
08 Jan
09 Jan
Implementa...
A.7.2.1 O...
A.7.2.2 P...
A.11.1.1 ...
A.11.1.2 ...
A.11.2.1 ...
A.11.2.2 ...
A.11.2.4 ...
A.11.2.5 ...
A.11.2.6 ...
A.11.2.7 ...
A.11.2.8 ...
A.11.2.9 ...
A.12.1.1 ...
A.12.1.2 ...
A.12.2.1 ...
A.12.3.1 ...
A.12.6.1 ...
A.12.6.2 ...
A.7.2.1 Odpovědnosti vedení organizace
A.7.2.2 Pov...
A.11.1.1 Fy...
A.11.2.1 Umístění zařízení a je...
A.11...
A.11.2.4 Údržba zař...
A.11.2.5...
A.11.2.6...
A.11...
A.11.2.8...
A.11.2.9...



Obrázek 14: Ganttův diagram implementace

Odhadovaná délka implementace opatření je 102 hodin rozdělených do 19 dní. Do kalkulace jsou zahrnuta omezeni jako pracovní doba, pracovní dny nebo časová mezera mezi navazujícími činnostmi.

4.8 Rizika projektu

V této kapitole bych rád uvedl rizika, která mohou způsobit neuskutečnění projektu respektive neúspěšné dokončení projektu. Je třeba upozornit na tyto rizika, vyhodnotit tyto rizika a přijmout vhodná opatření. Mezi tyto rizika patří:

- nedostatek času pro úspěšné provedení projektu nebo jeho jednotlivých fází,
- nekvalitní vypracování dodávaných a zpracovávaných částí díla,
- právní rizika,
- personální rizika (nezastupitelnost, nekvalifikovanost nebo špatné proškolení zainteresovaných osob),
- finanční rizika (neuvolnění finančních zdrojů, případný výpadek finančních prostředků apod.),
- nedostatečná komunikace a předávání informací mezi členy projektového týmu navzájem,
- nadměrná procesní administrativní náročnost řízení projektu,
- špatná koordinace a komunikace mezi samosprávou a úřadem.

4.9 Přínos práce

Jako hlavní přínos této práce vidím zvýšení informační bezpečnosti ve vybrané obci pomocí provedení analýzy rizik a návrhu implementace opatření a pomocí rozšíření povědomí o bezpečnosti informací. V případě, že bude obec uvažovat o certifikování systému řízení bezpečnosti informací podle standardu ISO 27000, bude už mít představu, jaké povinnosti a náklady to s sebou přináší. Tato práce může sloužit jako úvod do problematiky systému řízení informační bezpečnosti a metodika pro snižování celkového rizika ve veřejné správě.

Dalším přínosem je povědomí o řízení a hodnocení rizik a aktiv obce, které je v této práci popsáno. Jako další přínos bych uvedl seznámení vedení obce, zaměstnanců a

veřejnosti s největšími hrozbami působící na aktiva a se standardy bezpečnosti informací ISO 27000, které se stávají v dnešní době stále aktuálnější. Přínosem je tedy především samotné pochopení důležitosti a rozšíření povědomí o důležitosti informačního bezpečnosti.

ZÁVĚR

Hlavní i dílčí cíle této práce byly splněny, když jsem na základě teoretických znalostí uvedených v první části práce zanalyzoval prostředí obecního úřadu, vyhodnotil rizika spojené s informační bezpečností a následně navrhnul vhodná a přiměřená opatření pro snížení celkového rizika obecního úřadu z pohledu informační bezpečnosti. Pro dosažení toho cíle jsem využil normy systému řízení informační bezpečnosti ISO/IEC 27000. Pomocí vhodných opatření jsem se snažil snížit největší analyzovaná rizika. Pro kontrolu efektivnosti systému jsem navrhnul metriky, pomocí kterých můžeme dostat zpětnou vazbu fungování systému. Poté jsem implementaci těchto opatření zhodnotil z pohledu lidských a finančních zdrojů a následně i z časového hlediska.

Při implementaci opatření je velice důležitá součinnost specialisty informační bezpečnosti se zadavatelem, tedy obecním úřadem. Pro úspěch projektu je nezbytná dobrá komunikace a spolupráce těchto dvou subjektů a také komunikace mezi samosprávou a obecním úřadem. Realizace projektu závisí na vyčlenění dostatečných zdrojů na tento projekt. V případě přidělení dostatku zdrojů na tento projekt, je třeba před zahájením projektu proškolit všechny uživatele pomocí metodiky SAE.

Je důležité si uvědomit, že řízení bezpečnosti informací je nikdy nekončící proces a tedy, že zavedením opatření v organizaci práce nekončí, naopak začíná.

POUŽITÁ LITERATURA

(1) KOCH, Miloš a Jan DOVRTĚL. *Management informačních systémů.* Brno: Akademické nakladatelství CERM, 2006. ISBN 80-214-3262-4.

(2) POŽÁR, Josef. *Manažerská informatika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

(3) VODÁČEK, Leo a Antonín ROSICKÝ. *Informační managment: Poslání, pojetí a aplikace.* Praha: Managment Press, 1997. ISBN 80-85943-35-2.

(4) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(5) BÉBR, Richard a Petr DOUCEK. *Informační systémy pro podporu manažerské práce.* Praha: Professional Publishing, 2005. ISBN 80-864-1979-7.

(6) *ČSN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnostní informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, 2014.

(7) DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-807-4310-508.

(8) *ČSN ISO/IEC 27001:2005 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnostní informací – Požadavky*. Praha: Úřad pro technickou normalizaci, 2014.

(9) *ČSN ISO/IEC 9001:2009 Systém managementu kvality - Požadavky*. Praha: Úřad pro technickou normalizaci, 2009.

(10) Zákon č. 365/2000 Sb., o informačních systémech veřejné správy. *Ministerstvo vnitra České republiky* [online]. Praha, 2016 [cit. 2019-04-16]. Dostupné z: https://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx

(11) Metodický pokyn Řízení kvality informačních systémů veřejné správy. *Ministerstvo vnitra České republiky* [online]. Praha [cit. 2019-04-16]. Dostupné z: https://www.mvcr.cz/clanek/rizeni-kvality-informacnich-systemu-verejne-spravy.aspx

(12) *ČSN ISO/IEC 27002:2013 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnostní informací – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, 2014.

(13) *ČSN ISO/IEC 27004:2009 Informační technologie – Bezpečnostní techniky – Řízení bezpečnostní informací – Měření.* Praha: Úřad pro technickou normalizaci, 2011.

(14) JIROVSKÝ, Václav. *Kybernetická kriminalita*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

(15) KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, z. s. p. o, 2016 [cit. 2019-05-07]. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

(16) *ČSN ISO/IEC 27005:2011 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(17) ROUSE, Margaret. What is Gantt chart?. *Software Quality information, news and tips* [online]. 2007 [cit. 2019-05-10]. Dostupné z: https://searchsoftwarequality.techtarget.com/definition/Gantt-chart

(18) Clean Desk Poster. In: *Privacy information, tips and expert interview - PrivacySense.net* [online]. [cit. 2019-05-10]. Dostupné z: http://www.privacysense.net/clean-desk-poster/

SEZNAM OBRÁZKŮ

Obrázek 1: Bezpečnost informací (Zdroj:4) 13
Obrázek 2: Vzájemné vztahy bezpečností v organizaci (Zdroj: 4) 14
Obrázek 3: Přiměřená bezpečnost za akceptovatelné náklady (Zdroj: 4) 15
Obrázek 4:Model PDCA v ISMS (životní cyklus ISMS) (Zdroj: 4) 17
Obrázek 5: Uspořádání terminologie řízení rizik (Zdroj: 7) 19
Obrázek 6: Celý proces řízení rizik (Zdroj: 6) 20
Obrázek 7: Přehled činností při ustanovení ISMS (Zdroj: 7) 21
Obrázek 8: Model měření bezpečnosti informací (Zdroj: 12) 23
Obrázek 9: Skupiny opatření podle ISO/IEC 27002:2013 Zdroj: (12) 26
Obrázek 10: Koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací 27
Obrázek 11: Typické hrozby (Zdroj: 14) 29
Obrázek 12: Oblasti sociotechnických útoků, taktika a obrana (Zdroj: 14) 32
Obrázek 13: Organizační schéma obce 36
Obrázek 14: Ganttův diagram implementace 74

SEZNAM TABULEK

Tabulka 1: Stupnice hodnocení aktiv (Zdroj: 4) 38
Tabulka 2: Identifikace a ohodnocení aktiv 38
Tabulka 3: Stupnice hodnocení hrozeb 39
Tabulka 4: Identifikace a ohodnocení hrozeb 39
Tabulka 5: Matice zranitelnosti 40
Tabulka 6: Hodnotící stupnice pro matici rizik 41
Tabulka 7: Matice rizik 42
Tabulka 8: Soubor opatření 44
Tabulka 9: Opatření proti pochybení zaměstnanců 63
Tabulka 10: Opatření proti krádeži nebo poškození aktiv 63
Tabulka 11: Opatření proti kyberkriminalitě 64
Tabulka 12: Ekonomické zhodnocení 68
Tabulka 13: Časový harmonogram 71

SEZNAM PŘÍLOH

PŘÍLOHA I: Směrnice pro fyzický bezpečnostní perimetr

PŘÍLOHA II: Fyzické kontroly vstupu

PŘÍLOHA III: Bezpečnost zařízení

PŘÍLOHA IV: Zásada čistého stolu

PŘÍLOHA V: Zásada čistého stolu - plakát

PŘÍLOHA VI: Hlášení bezpečnostního incidentu

PŘÍLOHA I

Směrnice pro fyzický bezpečnostní perimetr

Cílem fyzické bezpečnosti je předcházet neautorizovanému přístupu, poškození a zásahům do informací a prostor úřadu <NÁZEV ÚŘADU>. Za tím účelem:

- je stanoven fyzický bezpečnostní perimetr, který zahrnuje budovu úřadu na adrese <ADRESA ÚŘADU>
- je stanovena perimetrová bezpečnostní ochrana, která je tvořena konstrukcí budovy tedy zdmi a existuje pouze jeden vchod do budovy, který slouží pro veřejnost i zaměstnance a který je v době nepřítomnosti zaměstnanců sledován bezpečnostním systémem s detektorem pohybu. Vstupní dveře jsou zabezpečeny zámkem a jsou bezpečnostního charakteru. Všechna okna jsou zabezpečena mřížemi. Průchod perimetrem je v době přítomnosti zaměstnanců kontrolován sekretářkou.
- je stanovena vnitřní ochrana, kterou zabezpečuje bezdrátový zabezpečovací systém s detektorem pohybu. Dále je zde umístěn protipožární systém, s poplachovým zařízením.
- je budova rozdělena na veřejnou část, která sestává ze vstupní místnosti, další místnosti jsou neveřejné prostory, kam je přístup umožněn pouze zaměstnancům, případně třetím stranám na základě smluvního vztahu nebo se souhlasem odpovědné osoby.
- je stanovena citlivá zóna, kterou tvoří kancelář starosty, kde se nachází router, server a úložné zařízení. Do této zóny je vstup povolen pouze vlastníkům aktiv, které se zde nacházejí nebo s doprovodem odpovědné osoby.

<PLÁN BUDOVY SE ZNÁZORNĚNÝM PERIMETREM A ZÓNAMI>

PŘÍLOHA II

Fyzické kontroly vstupu

Pro kontrolu fyzického přístupu do budovy <ADRESA> je využíváno vstupního místa, kontrolované zaměstnanci úřadu. Do vstupní místnosti úřadu je umožněn vstup veřejnosti v úředních hodinách, dále do budovy je vstup umožněn pouze zaměstnancům, případně třetím stranám na základě smluvního vztahu nebo se souhlasem odpovědné osoby. Je nutné evidovat totožnost, datum a čas příchodu a odchodu návštěvníků, kteří vstupují do citlivé oblasti, kam nemá veřejnost přístup a kde jsou uchovávaný důvěrné informace a citlivá aktiva.

Jméno	**Příjmení**	**Datum**	**Čas příchodu**	**Čas odchodu**	**Účel vstupu**

PŘÍLOHA III

Bezpečnost zařízení

Informační aktiva musí být umístěny tak, aby byla snížena působící rizika a minimalizovány příležitosti pro neautorizovaný přístup, poškození nebo krádež aktiva. Za tímto účelem:

- jsou aktivní prvky sítě, servery a datová úložiště umístěny v citlivé zóně, v uzamykatelných skříních.
- je zakázáno pít, jíst a kouřit v okolí výše zmíněných zařízení.
- jsou ostatní počítačové stanice umístěny v zamykatelných skříňkách.
- musí být aktivní prvky, servery a datové úložiště připojeny k obvodu s ochranou proti přepětí. Pro tyto zařízení a počítačové stanice musí být zajištěn systém nepřetržitého napájení elektrickým proudem, záložním zdrojem UPS, který vydrží zařízení napájet minimálně 15 minut po výpadku dodávky energie.
- musí být všechna zařízení provozována v souladu s doporučením výrobce, to se týká intervalu servisních prohlídek a oprav. Servis musí být prováděn pouze oprávněnými osobami.

PŘÍLOHA IV

Zásada čistého stolu

Přehled

Pro zvýšení bezpečnosti důvěrnosti informací, přijala organizace <NÁZEV ORGANIZACE> zásady čistého stolu. Toto pravidlo by mělo zajistit, že všechny citlivé a důvěrné informace, ať v papírové nebo digitální podobě, zařízení pro ukládání dat nebo jiný hardware jsou zamknuty nebo odloženy na bezpečné místo, když není pracovní místo využíváno. Tato politika by měla snížit riziko neautorizovaného přístupu a ztráty nebo poškození informací během nepřítomnosti zaměstnance. Zásada čistého stolu je důležitým opatřením standartu ISO 27000

Rozsah

Tato politika platí pro všechny zaměstnance.

Pravidla

Kdykoliv je pracovní místo bez přítomnosti zaměstnance po delší dobu jsou vyžadovány následující kroky:

1. Všechny citlivé a důvěrné dokumenty a přenosná úložiště a zařízení musí být uklizeny z pracovního stolu a musí být zamknuty v zásuvce nebo kartotéce.
2. Všechny citlivé dokumenty, které mají být vyhozeny, musí být nejprve skartovány.
3. Počítačové stanice musí být uzamknuty v době nepřítomnosti zaměstnance a úplně vypnuty na konci pracovní doby.
4. Klíče pro přístup do zásuvek a kartoték nesmí zůstat na pracovním stole.
5. Všechny dokumenty, které zůstaly v tiskárně na konci pracovní doby, by měly být zlikvidovány.

Dodržování

Dodržování těchto pravidel bude kontrolováno starostou nebo jiným nadřízeným.

Neshoda

Všechny výše zmíněné pravidla jsou vyžadovány po všech zaměstnancích. Každý zaměstnanec, u něhož bylo zjištěno, že tuto zásadu porušili, může být předmětem disciplinárního řízení až do ukončení pracovního poměru.

V ……. dne …… ……..

podpis

PŘÍLOHA V

Přepracováno z anglického originálu (18)

PŘÍLOHA VI

Hlášení bezpečnostního incidentu

ID hlášení o incidentu (přidělí pracovník IS):

E-mail:

Telefon:

Místo výskytu incidentu Úřad: Adresa:	**Incident nahlásil** Jméno: Telefon: E-mail:
Datum výskytu:	**Čas výskytu:**

Typ bezpečnostního incidentu (viz příloha Seznam možných typů hrozeb, případně i jiný typ)

Způsob vzniku incidentu: úmyslný ☐ náhodný ☐ přírodního charakteru ☐

Popis incidentu (míra poškození, nebo narušení informačního systému, jaká data byla poškozena, případně odcizena, jak dlouho byl IS nedostupný, kdo incident způsobil, atd.)