Analýza rizik v heterogenním prostředí státní správy MěÚ Vsetín.

Risk analysis in a heterogeneous environment, government Vsetin Town Hall.

Bc. Zdeněk Janík

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Zdeněk JANÍK**
Osobní číslo:	**A08401**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Analýza rizik v heterogenním prostředí státní správy MěÚ Vsetín**

Zásady pro vypracování:

Projekt řeší praktickou úlohu praxe zaměřenou na přípravu řízení informační bezpečnosti v prostředí státní a veřejné správy na MěÚ ve Vsetíně.

1. **Teoretický souhrn problematiky a popis standardů systému managementu informační bezpečnosti.**
2. **Popis architektury informačního systému MěÚ Vsetín.**
3. **Provedení vstupní analýzy rizik a obchodních dopadů.**
4. **Analýza zpracování osobních údajů dle definice zákona č. 101/2000 Sb.**
5. **Popis zabezpečení lokalit, zálohování dat, bezpečnost uložení hodnotných dat a ochrana autentizačních informací.**
6. **Řízení aktiv a bezpečnost lidských zdrojů.**
7. **Předložení základních návrhů (doporučení) pro další postup v oblasti bezpečnosti informací, respektive budování systému managementu informační bezpečnosti (ISMS).**
8. **Návrh protiopatření procesních i technických (úprava stávajících interních předpisů – směrnic).**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **FRYŠAR, M. a kolektiv. Bezpečnost pro manažery, podnikatele a politiky. 1. vydání. Praha: Public History Praha, 2008. 176 s. ISBN 80-86445-22-4.**
2. **DOUCEK, P., NOVÁK, L., SVATÁ, V., Řízení bezpečnosti informací. 1. vydání. Praha: Professional publishings, 2008. 240s. ISBN 978-80-86946-88-7.**
3. **HÖNIGOVÁ, A., MATYÁŠ, V., Anglicko -- česká terminologie bezpečnosti informačních technologií. 1. vydání. Praha: Computer Press, 1996, ISBN 80-85896-44-3.**
4. **ŘEPA, V., Podnikové procesy -- Procesní řízení a modelování. 2. vydání. Praha: Grada, 2007. 281 s. ISBN 978-80-247-2252-8.**
5. **Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, navazující vyhlášky.**
6. **Zákon č. 365/2000 Sb. o informačních systémech veřejné správy, navazující vyhlášky.**
7. **ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - systémy managementu bezpečnosti informací - Požadavky.**

Vedoucí diplomové práce: **RNDr. Ing. Miloš Krčmář**
Ústav informatiky a umělé inteligence

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

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

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

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce obsahuje v teoretické části souhrn problematiky a popis standardů. Praktická část popisuje architekturu informačního systému MěÚ Vsetín. Zabývá se provedením vstupní analýzy rizik a obchodních dopadů, analýzou zpracování osobních údajů dle definice zákona č. 101/2000 Sb., kamerovým systémem Městské policie a zabezpečením lokalit, zálohováním dat, bezpečností uložení hodnotných dat a ochranou autentizačních informací. Pozornost je taktéž věnována řízení aktiv a bezpečnosti lidských zdrojů. Cílem práce je předložit základní návrhy (doporučení) pro další postup v oblasti bezpečnosti informací, respektive budování systému managementu informační bezpečnosti (ISMS).

Klíčová slova:

analýza rizik, hodnocení aktiv, řízení rizik, bezpečnostní politika, identifikace hrozeb, návrh opatření

ABSTRACT

This work contains a summary of the theoretical issues and a description of standards. The practical part describes the architecture of information system MěÚ Vsetín. It deals with the initial implementation of risk analysis and business impact analysis of processing of personal data as defined by Act No 101/2000 Coll. Camera system of the Town Police and security sites, data backup, security, storage and protection of valuable data authentication information. Attention is also paid to asset management and security of human resources. Aim of this work is to present the basic proposals (recommendations) for further action in the information security field, or building an information security management system (ISMS)

Keywords:

risk analysis, asset evaluation, risk management, security policy, identification of threats, the draft measures

Děkuji především rodině za podporu a pochopení. Dále pak kolegům z odboru informatiky MěÚ Vsetín za vstřícnost při studiu. Zároveň chci poděkovat všem zúčastněným pracovníkům MěÚ Vsetín za ochotu a čas strávený při konzultacích. V neposlední řadě RNDr. Ing. Miloši Krčmářovi za ochotu při spolupráci a vedení této práce.

Motto:

Bezpečnost je tak účinná, jak je silný její nejslabší článek.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně 8. 6. 2010

……
podpis diplomanta

OBSAH

ÚVOD

Úkolem této práce je provést analýzu rizik a obchodních dopadů, jako součásti systému řízení bezpečnosti IT, který se skládá z řady předcházejících i následných kroků, cyklicky opakovaných. V případě kdy je systém řízení bezpečnosti IT zaváděn u fungující organizace, nebo se jeho role výrazně mění, je analýza rizik nejvhodnějším vstupním bodem do procesu.

Před samotnou analýzou rizik je uveden popis architektury informačního systému MěÚ Vsetín a analyzováno zpracování osobních údajů dle definice zákona č. 101/2000 Sb. Práce se dále zabývá ochranou osob, organizace a jejích informačních systémů před riziky vyplývajícími z asociálního chování lidí, riziky fyzikálního vlivu přírody, technickými riziky a lidským selháním, nikoliv riziky, které jsou spíše riziky provozními či manažerskými (obchodními, politickými, sociálními, ekonomicko-finančními apod.). Zároveň se zabývá kamerovým systémem Městské policie a zabezpečením lokalit, zálohováním dat, bezpečností uložení hodnotných dat a ochranou autentizačních informací. Pozornost je taktéž věnována řízení aktiv a bezpečnosti lidských zdrojů.

Součástí procesu optimalizace činností jakékoliv organizace směřující k dosahování jejich cílů nejvhodnějším, nejúspornějším, nejúčinnějším a společensky nejpřijatelnějším způsobem, je i snižování rizik hrozících organizaci.

Teoretická část práce spočívá v souhrnu problematiky a popisu standardů.

Cílem práce je předložit základní návrhy (doporučení) pro další postup v oblasti bezpečnosti informací, respektive budování systému managementu informační bezpečnosti (ISMS)

Požadavkem zadavatele je dosažení následujících efektů:

- posouzení shody s požadavky standardu ČSN ISO/IEC 27001
- identifikace hrozeb
- návrh protiopatření procesních i technických (úprava stávajících interních předpisů - směrnic)

I. TEORETICKÁ ČÁST

1 CHARAKTERISTIKA ZKOUMANÉHO OBJEKTU

1.1 Objekt zkoumání

Název: Městský úřad Vsetín

Adresa: Svárov 1080, VSETÍN 755 24

IČO: 00304450

Telefon: 571 491 111

Fax.: 571 419 278

E-mail: posta@mestovsetin.cz

webové stránky: www.mestovsetin.cz

Město Vsetín je dle zákona veřejnoprávní korporací. Problematiku obecního zřízení upravuje zákon o obcích č. 128/2000 Sb., ve znění pozdějších předpisů. Orgány obce jsou zastupitelstvo, rada, starosta, městská policie a městský úřad. Městský úřad Vsetín (MěÚ) je současně úřadem s rozšířenou působností pro výkon státní správy pro 32 obcí ve správním obvodu.

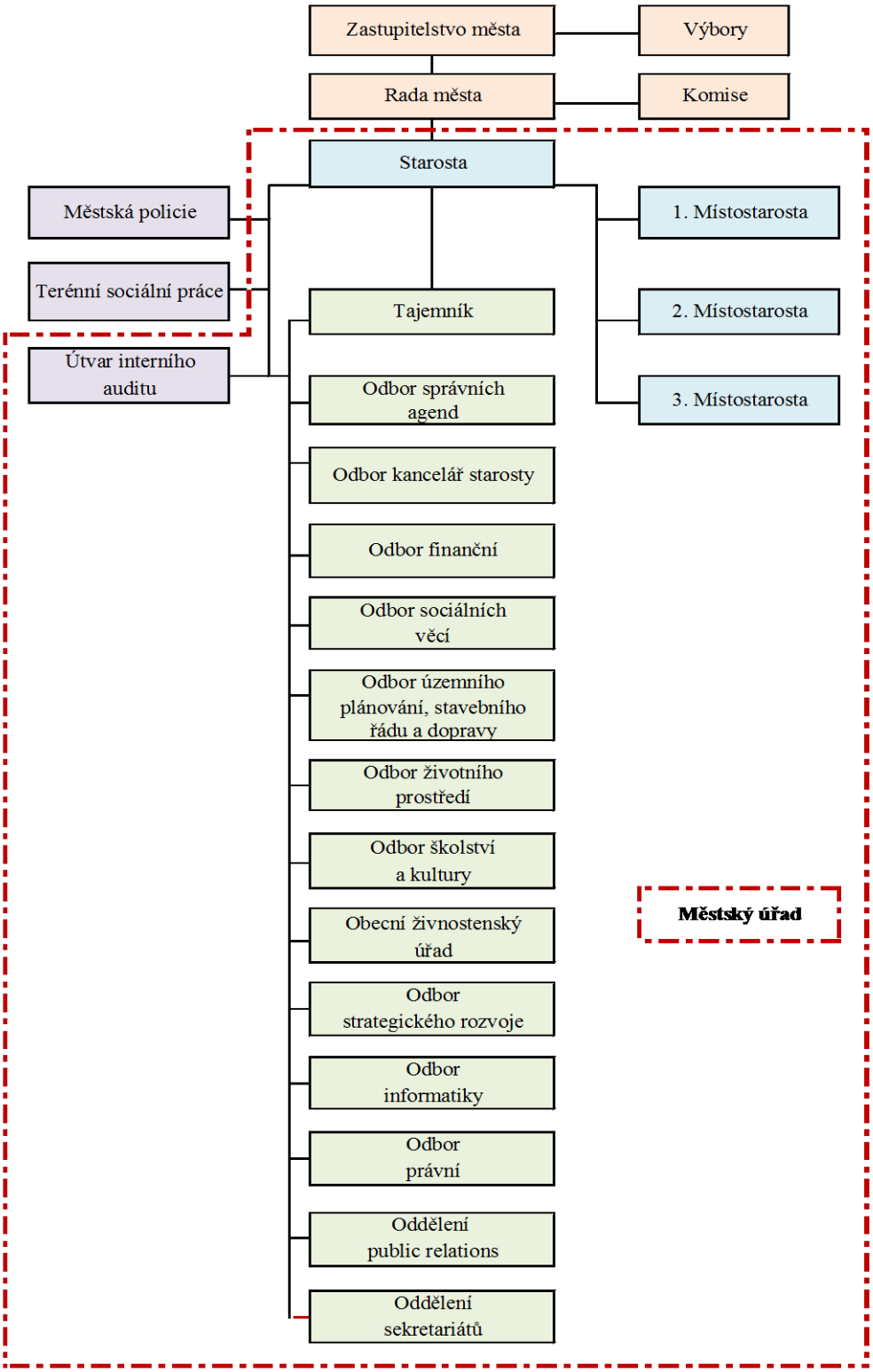
Městský úřad je výkonným orgánem zajišťujícím plnění požadavků na:

- plnění úkolů a činností schválených radou nebo zastupitelstvem města Vsetína (v oblasti jeho samostatné působnosti) a
- zabezpečování výkonu státní správy ve správním obvodu v rozsahu stanoveném zvláštními zákony (v oblasti přenesené působnosti) [7].

Městský úřad Vsetín tvoří dle zákona o obcích starosta, místostarostové, tajemník a ostatní zaměstnanci města Vsetín zařazení do Městského úřadu Vsetín. Pro výkon svých funkcí je městský úřad rozčleněn do 11 odborů a jednoho útvaru. Odbory jsou řízeny tajemníkem, útvar je řízen přímo starostou. Odbory jsou dále členěny na jednotlivá oddělení a úseky dle zajišťovaných činností.

Odbory jako takové jsou organizačními jednotkami Městského úřadu ve Vsetíně a byly zřízeny Radou města Vsetína pro jednotlivé úseky jeho činnosti. Odbory tak vykonávají činnost v samostatné i přenesené působnosti. Jednotlivé úkoly, které odbory vykonávají, jsou specifikovány v Organizačním řádu MěÚ Vsetín [11].

Uspořádání jednotlivých organizačních jednotek a jejich vzájemné vztahy jsou znázorněny v organizační struktuře MěÚ Vsetín.



Obr. 1. Organizační struktura MěÚ Vsetín [11]

2 INFORMAČNÍ BEZPEČNOST

Informační bezpečnost je jedním ze stěžejních pilířů při budování informačních systémů organizace libovolného typu, tedy i orgánu veřejné a státní správy - městského úřadu. Svým rozsahem však v oblasti strategického řízení a pracovních postupů výrazně přesahuje oblast informačních technologií, s kterými je někdy ne zcela přesně spojována. V moderní informační společnosti se informace stávají zásadním a vysoce hodnotným aktivem. Pro řadu subjektů vyplývají požadavky v oblasti ochrany informací z platné legislativy ČR a to především ze zákona č. 101/2000 Sb., o ochraně osobních údajů a jeho pozdějších novelizací.

Informační bezpečnost - je systém opatření z oblasti:

a) počítačové a komunikační bezpečnosti,
b) administrativní bezpečnosti a organizačních opatření,
c) personální bezpečnosti,
d) fyzické bezpečnosti informačního systému. [2]

Mezi **základní dokumenty režimové ochrany** patří: statut organizace (účel, cíl činnosti), organizační řád, pracovní řád, spisový a skartační řád, provozní řád pracoviště.

2.1 Bezpečnostní politika

Základním cílem bezpečnostní politiky je chránit aktiva organizace přiměřeným způsobem vzhledem k hodnotě aktiv. Zamezit ekonomickým ztrátám, zániku organizace, čili zamezit tomu, aby došlo k uplatnění (spuštění) rizika. Bezpečnostní politika je souhrnem standardů nebo pravidel pro konkrétní oblasti informační bezpečnosti, obsahuje hesla, mobilní komunikace, připojení třetích stran, řízení smluvních vztahů (povinné náležitosti smluv), řízení přístupových oprávnění, autentizace uživatelů, fyzická bezpečnost, šifrování dat, klasifikace informací apod. Bezpečnostní politiky v praxi definují požadavky, které jsou závazné pro danou oblast a musí být dodržovány. Jejich přínosem je vymezení mantinelů, které určují bezpečný prostor či chování. [10]

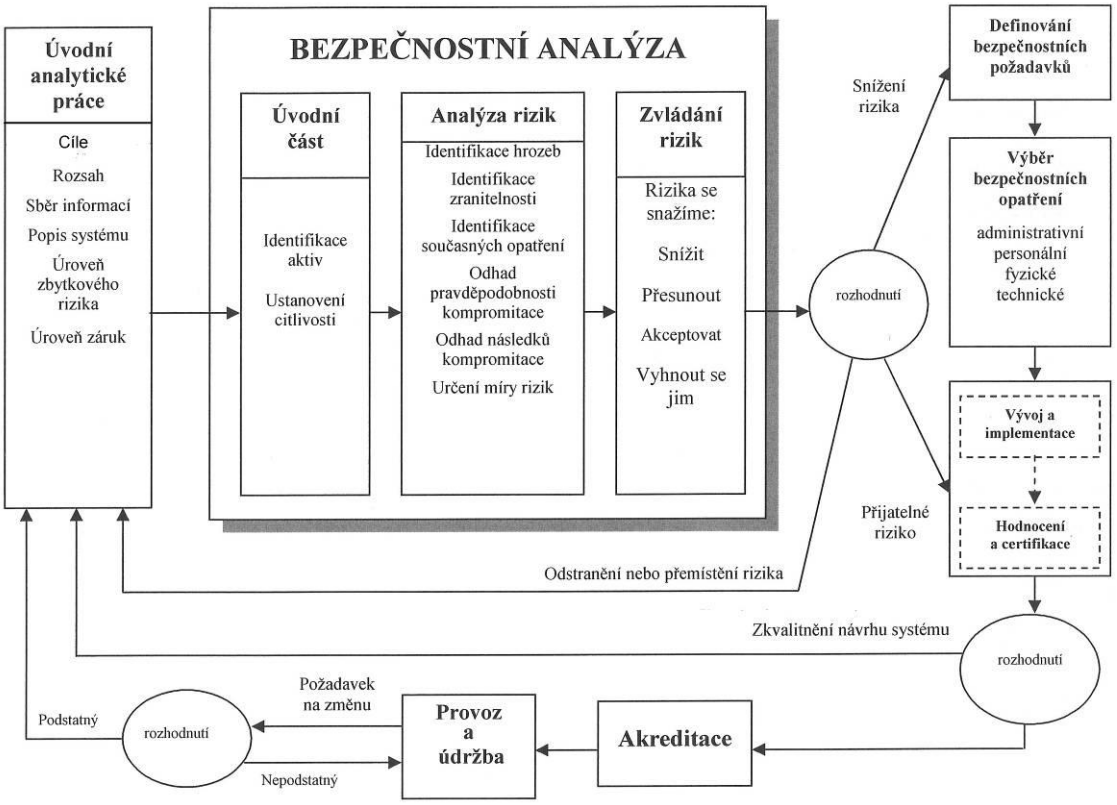
2.2 Bezpečnostní analýza IS

Bezpečnostní analýza IS je souhrnem metod pro zjišťování míry bezpečnosti IS, analýzou rizik a analýzou zvládání rizik. Jsou používány následující pojmy - aktivum (vše co má

hodnotu), hrozba (nebezpečnost, přístup, motivace), zranitelnost (interakce mezi hrozbou a aktivem), protiopatření (efektivita a náklady na pořízení, zavedení, provozování), hranice bezpečnostní analýzy (složky IS, budovy, zdroje pro IS). Více k pojmům je uvedeno v kapitole 2.5.

2.2.1 Obecný postup

Obecný postup řešení bezpečnosti IS začíná přípravnými pracemi, stanovují se hranice analýzy, identifikují aktiva - služby (informační, technické a komunikační), informační aktiva (databáze, datové soubory, dokumentace a manuály), plány při haváriích, SW aktiva, fyzická aktiva, stanovuje se hodnota aktiva (pořizovací, závislost IS na aktivu, cena informace atd.). Poté se provádí identifikace hrozeb, při které je důležitým prvkem zkušenost. Vytváří se seznam aktiv podle funkcí, analýza hrozeb a zranitelností, stanovení úrovně rizika, nejvýznamnější atributy, tj. co má největší negativní vliv na důvěrnost, integritu a dostupnost IS. Je nutné trvale se zabývat problémem jak na tyto negativní vlivy reagovat. Nabízí se zde celá řada reakcí, od jejich akceptování až po přijímání opatření na jejich eliminaci. Úroveň rizika může být zmenšena tím, že se v rámci procesu zvládání rizik implementuje taková architektura systému, která zahrnuje organizační, administrativní, personální, fyzické a technické bezpečnostní komponenty. Proces zvládání rizik tvoří plánování, organizování, řízení a kontrola zdrojů za účelem zajištění přijatelné zbytkové úrovně rizika a úměrných nákladů. Vybírání protiopatření. V oblasti bezpečnosti IS se setkáváme s určitými obtížemi, které vznikají jako důsledek dynamických změn rizikových faktorů a prudkého vývoje IT. Nejsou-li včas a adekvátně vzaty v úvahu všechny faktory rizika, může to vést k neefektivním a zbytečně drahým opatřením. Zvládání rizik musí být považováno za jeden z rozhodujících kroků řešení bezpečnosti.



Obr. 2. Bezpečnost a životní cyklus IS

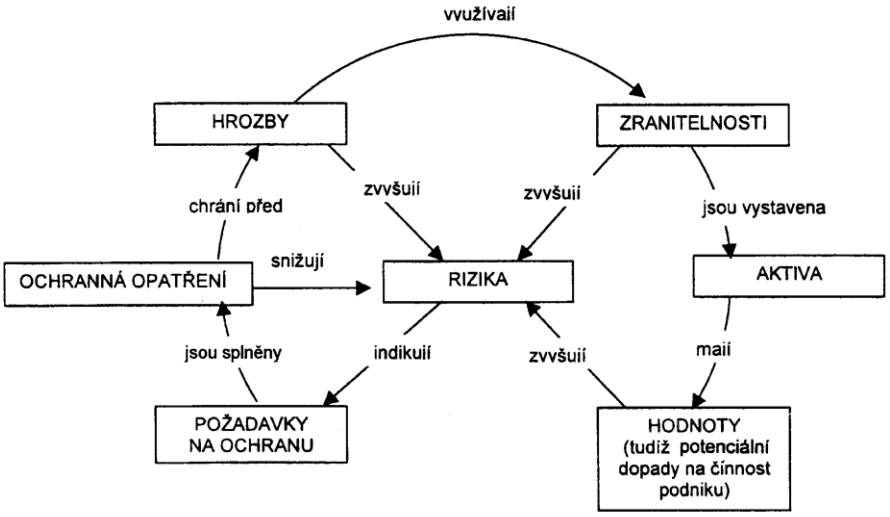
2.3 Rizika a hrozby působící na informační systém

Mechanismus uplatnění rizika probíhá tak, že hrozba využije zranitelnosti, překoná protiopatření a působí na aktivum, kde způsobí škodu (dopad).

Aktivum (svou hodnotou) motivuje člověka k aktivaci hrozby. Vůči působení hrozby se aktivum vyznačuje určitou zranitelností. Aktivum je zároveň chráněno protiopatřeními před hrozbami.

Protiopatření chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva. Protiopatření zároveň odrazují od aktivování hrozeb.

Hrozba působí jednak přímo na aktivum nebo na protiopatření, s cílem získat přístup k aktivu. Aby mohla hrozba působit, musí být aktivována. Pro svou aktivaci vyžaduje zdroje, tzn. vytvoření podmínek pro její působení.



Obr. 3. Mechanismus uplatnění rizika

Typické hrozby pro IS - neoprávněné čtení (z obrazovky, z klávesnice, z paměťových médií), zneužití zdrojů systému (zneužití služeb, vyřazení systému, viry, trojské koně, nedbalost), průniky (záměrné překonávání zabezpečení IS), nedostatek v návrhu, selhání komponenty (zařízení, nepředpokládané stavy IS, prostředí ovlivňování), modifikace prvků IS, odposlouchávání, modifikace přenášených zpráv, odepření komunikačních služeb

Možná rizika - katastrofy a živelné pohromy, chyby technického a programového vybavení - výpadek PC, poškození stopy disku, nečitelný disk, chyba v aplikačním programu poškozuje záznam, lidská nepozornost - chyba zavádění vstupních dat, zavedení a aktualizace nesprávných dat, fyzické poškození nosného média, úmyslné poškození (sabotáž, zlomyslnost uživatele, kriminalita, zpronevěra, korupce, špionáž), narušení soukromí (zvědavost, neúmyslné prozrazení soukromých informací).

Příznaky ohrožení systému - neexistující plán celkové ochrany, nedostatek vyváženosti celkových opatření (např. přehlížení osob pro manipulaci s daty), provozní nepořádek, nedostatečná dokumentace programů, nízká pracovní morálka, neadekvátní rozdělení odpovědností, nedostatek vnitřní kontroly bezpečnostních aspektů.

2.4 Etapy zabezpečení IS

Řešení bezpečnosti IS se prolíná všemi fázemi jeho životního cyklu, pro každou fázi musí být podrobně předepsány vstupní a výstupní dokumenty, např. pro úvodní studii jsou vstupními dokumenty právní předpisy, záměr vytvoření IS, bezpečnostní politika,

výstupními dokumenty jsou úvodní bezpečnostní studie, koncepce testování. Je nutné dodržet všechny níže rozepsané etapy.

1. Záměr vytvoření IS a vlastní úvodní studie (právní požadavky, bezpečnostní politika, charakteristika současného stavu, cílů, vztahu k okolí, všeobecná charakteristika IS, koncepce bezpečnosti a podmínky pro bezpečnost).
2. Rozpracování požadavků do konkrétních opatření, vytváří se bezpečnostní model včetně jeho architektury, návrhy rozhraní, ověření úplnosti návrhu, dotažení na úroveň SW, HW, organizace.
3. Implementace a zavádění - provozní dokumentace, realizace testů, získání akreditace, zaškolení obsluhy a uživatelů.
4. Běžný režim a provoz - průběžné školení, vedení záznamů, kontrola dodržování, analýza rizik, reakce na změny prostředí a změny požadavků.

Plán bezpečnostních opatření popisuje, jak daná organizace přistupuje k otázkám bezpečnosti, musí být dostatečně často revidován a musí být zkoumáno jeho dodržování. Vypracováním plánu bývá pověřena skupina odborníků pokud možno ze všech důležitých organizačních struktur firmy, velikost a struktura tohoto týmu závisí na velikosti firmy.

2.4.1 Součásti plánu bezpečnostních opatření

- Politika - vyhlášení bezpečnostních cílů (např. ochrana dat před katastrofami, před úniky mimo organizaci apod.), participace personálu, zodpovědnosti, závazky organizace na udržení bezpečnosti (počet vyčleněných pracovníků, minimální vyčleněné výdaje).
- Popis současného stavu.
- Doporučení ke splnění bezpečnostních cílů.
- Kompetence osob ke splnění bezpečnostních cílů (uživatelé PC ručí za svůj počítač, administrátor databázového systému zodpovídá za přístup k datům a jejich integritu, firma může pověřit zvláštního pracovníka zodpovědného za vytvoření obecných pravidel práce s daty a jejich uvolňování či rušení, pracovníci osobního oddělení zodpovídají za přijetí důvěryhodných a spolehlivých pracovníků atd.).
- Časový harmonogram.
- Trvalé sledování - záznamy, plán prověrek, inovací.
- Dodržování - seznámení všech pracovníků, dostatečná podpora vedení organizace.

2.4.2 Ochranné vrstvy IS

Kontroly bezpečnosti a přesnosti zabudované v systému, fyzická obrana, administrativní kontroly, legislativní a společenské prostředí.

Vybrané aspekty ochrany IS (prolínají se):

- personální - přihlédnutí při přijímání zaměstnanců, působení na bezpečnostní povědomí zaměstnanců, dohoda o zachování mlčenlivosti,
- organizační - kontrola, disciplinární opatření, hlášení bezpečnostních incidentů, správa oprávnění, práce s hesly, ochrana před viry a jinými nežádoucími programy včetně nelegálního SW, zálohování, postupy v případě havárií.

Odhad pravděpodobnosti vzniku nežádoucích situací:

- dlouhodobé sledování výskytu jevů (pojišťovny - počet požárů, počet obytných domů, výše škody, trestné činy, frekvence lidských chyb),
- sledování a charakteristika konkrétního systému (počet HW a SW chyb, objem dat apod.),
- odhad daného odborníka,
- Delfský přístup - pravděpodobnost výskytu jevu odhadována nezávislými odborníky, korekce mínění odborníků po srovnání jejich názorů, snaha po konsensu.

2.4.3 Základní aspekty ochrany dat, základní požadavky

Bezpečnost a správnost dat, oprávněnost přístupu k datům, právo na soukromí. Je nutné trvale plnit následující poznatky:

- udržovat dostatečnou míru bezpečnosti (absolutní bezpečnost nedosažitelná),
- náklady na zabezpečení by měly odpovídat stupni zranitelnosti systému a hodnotě dat,
- celkové riziko je součtem dílčích rizik - cílem je jeho minimalizace,
- při odhadu rizika se často pracuje s pojmy: pravděpodobnost výskytu chyby, kategorie velikosti ztrát, pravděpodobnost zabránění chybě, náklady na zabránění chybě,
- tři zásady - prevence (minimalizace pravděpodobnosti vzniku), minimalizace vzniklých škod, návrh rychlé a spolehlivé metody obnovy.

Tab. 1. Aspekty ochrany dat a možnosti zneužití

Hodnota	Utajení	Integrita	Dostupnost
Hardware		přetížení, zničení, narušení	krádež, ztracení, nedostupnost
Software	zcizení, kopírování, zneužití	viry, trojské koně, modifikace	vymazání, ukončení práva užívání
Personál	zneužití přístupových práv		výpověď, odchod na dovolenou
Data	odhalení, vnější narušitel, dedukce	poškození chybou SW, HW nebo uživatele	vymazání, záměna, zničení
Dokumentace		neautorizovaná úprava	ztráta, zcizení, poškození
Materiál			ztráta, zcizení, poškození

2.5 Definice základních pojmů

Aktivem je všechno, co má pro jednotlivce nebo organizaci hodnotu, která může být zmenšena působením hrozby. Aktiva se dělí především na hmotná (např. stroj, materiál, výrobek, finanční hotovost apod.) a na nehmotná (např. programy, data, morálka pracovníků, pověst organizace atd.). Existují ovšem i složitější systémy aktiv, které v sobě spojují jak hmotné, tak nehmotné prvky. Jejich nejtypičtějšími a nejčastějšími představiteli jsou: fyzické osoby (manažeři, ostatní zaměstnanci) a informační systémy, jež jsou rovněž kombinací hmotného a nehmotného majetku.

Audit je systematický, nezávislý a dokumentovaný proces získávání důkazů z auditu a jeho objektivního hodnocení s cílem stanovit rozsah splnění kritérií auditu.

Bezpečnostní perimetr tvoří cokoliv, co vytváří bariéru, například zdi nebo vstupní turniket na karty. Fyzické ochrany může být dosaženo prostřednictvím řady fyzických bariér kolem prostor a kolem prostředků zpracovávajících informace. Každá bariéra vytváří bezpečnostní perimetr a zajišťuje zvýšení ochrany. [3]

Bezpečnostní opatření je praxe, postup nebo mechanismus, který snižuje riziko.

Bezpečnostní politika jsou pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejích systémů IT.

Dostupnost je vlastnost, že je něco na požádání přístupné a použitelné autorizovanou entitou. Zjištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby. [8]

Důvěrnost je vlastnost, že informace není dostupná nebo přístupná neautorizovaným jednotlivcům, entitám, nebo procesům. [8]

Hodnota aktiva je základní charakteristikou aktiva, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti) aktiva, popř. kombinaci obou přístupů. Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení. [2] (Typickým příkladem je hodnota informace, která může být pro někoho nulová, pro někoho nesmírná.)

Hrozba je potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace. Hrozba je síla, událost nebo aktivita osoby, která má nežádoucí vliv na bezpečnost organizace nebo může způsobit škodu na jejích aktivech. [3] Hrozbou může být například požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy. Škoda, kterou způsobí hrozba při jednom působení na určité aktivum, se nazývá dopad hrozby. Dopad hrozby se může odvodit od absolutní hodnoty ztrát, do které jsou zahrnuty náklady na znovuobnovení činnosti aktiva nebo náklady na odstranění následků škod způsobených hrozbou. Základní charakteristikou hrozby je její úroveň.

Informace jsou výsledné, to je vybrané či jinak zpracované údaje (data), prezentované ve formě snadno čitelné, pochopitelné a využitelné subjektem, jemuž jsou určeny. Mohou být v elektronické formě nebo napsané (vytištěné) na papíře, vyřčené při jednání nebo zaznamenané na jiném médiu

Informační aktiva tvoří zejména databáze a datové soubory, systémová dokumentace, uživatelské manuály, školicí manuály, provozní nebo podpůrné postupy, postupy obnovy, dohody o zajištění záložního provozu a archivní informace.

Informační bezpečnost jsou všechny aspekty souvisící s definováním, dosažením a udržováním důvěrnosti, integrity, dostupnosti, individuální zodpovědnosti, autenticity a spolehlivosti. [3]

Informační systém (IS) je identifikovatelný funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracování, uchovávání a zpřístupňování informací. Informační systém integruje informační základnu (data), technické a programové vybavení, finanční prostředky, procedury a pracovníky. [3]

Integrita je vlastnost, že data nebyla změněna nebo zničena neautorizovaným způsobem, nebo že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautorizované manipulace se systémem.

Kryptografický prostředek tvoří zařízení, předměty, programy nebo kryptografické postupy, včetně kryptografických klíčů, které zajišťují ochranu informací.

Monitorování sledování a vyhodnocování provozních událostí.

Odpovědnost je schopnost, kterou je určena odpovědnost za události.

Ochranné opatření nebo také protiopatření je proces, procedura, technický či právní prostředek nebo cokoliv jiného, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby.[3] Protiopatření se navrhují s cílem předejít vzniku škody, nebo s cílem usnadnit překlenutí následků vzniklé škody. Protiopatření se zaměřují do oblastí snížení úrovně hrozby, snížení úrovně zranitelnosti, snížení následků působení hrozby, detekce nežádoucího vlivu s cílem včas indikovat působení hrozby a předejít možnosti jejího plného uplatnění, a do oblasti obnovení činnosti po působení hrozby. Z hlediska bezpečnostní analýzy je protiopatření charakterizováno efektivitou a náklady. Efektivita protiopatření vyjadřuje, nakolik protiopatření sníží účinek hrozby. Používá se ve fázi zvládání rizik jako jeden z hlavních parametrů při hodnocení vhodnosti použití daného protiopatření.

Riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní. Riziko vzniká vzájemným působením hrozby a aktiva. Hrozba, která nepůsobí na žádné aktivum, nemusí být při analýze rizik brána v úvahu. Aktivum, na které nepůsobí žádná hrozba, není předmětem analýzy rizik. Úroveň rizika je určena hodnotou aktiva, zranitelností aktiva a úrovní hrozby. Na růstu úrovně rizika se podílí úroveň hrozby,

zranitelnost a hodnota aktiva. Jedině protiopatření úroveň rizika snižuje. Zbytkové riziko je takové riziko, které je tak malé, že je pro systém přijatelné a není nutné podnikat další protiopatření k jeho snížení.

Role je úloha přidělená zaměstnanci v systému managementu bezpečnosti informací.

Zálohování je vytváření a uschovávání záložních kopií obchodních informací k zajištění kontinuity činnosti pro případ ztráty zdrojů [4].

Zničení informace je stav informací ve kterém jsou informace nepoužitelné, bez ohledu na příčiny.

Zranitelnost je nedostatek, slabina nebo stav analyzované entity (aktiva, systému, objektu), kterého může být využito hrozbou pro uplatnění jejího nežádoucího vlivu. Tato veličina vyjadřuje, jak chráněné je aktivum vůči působení dané hrozby. Obvykle se vyjadřuje bez rozměru (např. malá, střední a velká), nebo jako pravděpodobnost, že hrozba způsobí škodu.[3] Slabá místa mohou být využita k narušení zamýšleného chování IS. Zranitelnost se může projevit jak v oblasti důvěrnosti tak i integrity a dostupnosti. Využití zranitelnosti představuje hrozbu, se kterou souvisí odpovídající riziko.

2.6 ISMS - Systém managementu bezpečnosti informací - legislativa a standardy

Systém managementu bezpečnosti informací (dále též ISMS - Information Security Management System) je charakterizován jako soustava organizačních a technických opatření, která dostatečným způsobem eliminují rizika spojená se zachováním důvěrnosti, integrity a dostupnosti informací prostřednictvím pokrytí hrozeb doporučenými protiopatřeními dle norem ČSN ISO/IEC 27001:2006 a ČSN ISO/IEC 17799:2006. ISMS by měl odpovídat nejen platným ČSN/ISO standardům, ale i platné legislativě ČR, která se této oblasti týká.

Jde pouze o část celkového systému managementu organizace založené na přístupu (organizace) k rizikům činností, která jsou zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací. Systém managementu zahrnuje organizační strukturu, politiky, plánování činností, odpovědnosti, praktiky, postupy, procesy a zdroje. [8]

ISMS je efektivní způsob, jak lze efektivně řídit – zvládat bezpečnost informací, tedy implementovat takové procesy, postupy a opatření, aby bylo možno dosáhnout a udržet korektní úroveň bezpečnosti informačních aktiv za adekvátní cenu. ISMS eliminuje tyto slabiny a nabízí systematický, procesní a efektivní přístup k řízení bezpečnosti informací. Efektivitou v doslovném smyslu rozumíme i efektivitu investovaných financí a úsilí do bezpečnosti informací, protože lze postupovat na základě znalosti aktiv – hodnot, která chráníme a znalosti konkrétních rizik, která chceme eliminovat implementací protiopatření. ISMS je implementován dle metodik, které vycházejí z dále uvedených standardů. Zavedení ISMS přináší i zlepšení užitné hodnoty vlastního IS organizace, kdy přináší soustavné zvyšování kvality nejen v oblasti důvěrnosti informací, ale také zkvalitnění jejich integrity a dostupnosti. Toto je dáno cyklem PDCA, který se stále opakuje. [1]

2.6.1 Metodika - ČSN/ISO standardy

U procesů implementace ISMS vycházíme z metodik, které jsou vytvořeny, používají názvosloví a opírají se především o následující normy a standardy platné v ČR a EU:

- ČSN ISO/IEC 17799
- ČSN ISO/IEC 27001
- ČSN ISO/IEC TR 13335, ČSN ISO/IEC 27005
- ČSN ISO/IEC 15408
- ČSN EN ISO 19011

Na tyto normy se odvolává i platná legislativa ve svých prováděcích předpisech, například u Zákona o utajovaných skutečnostech.

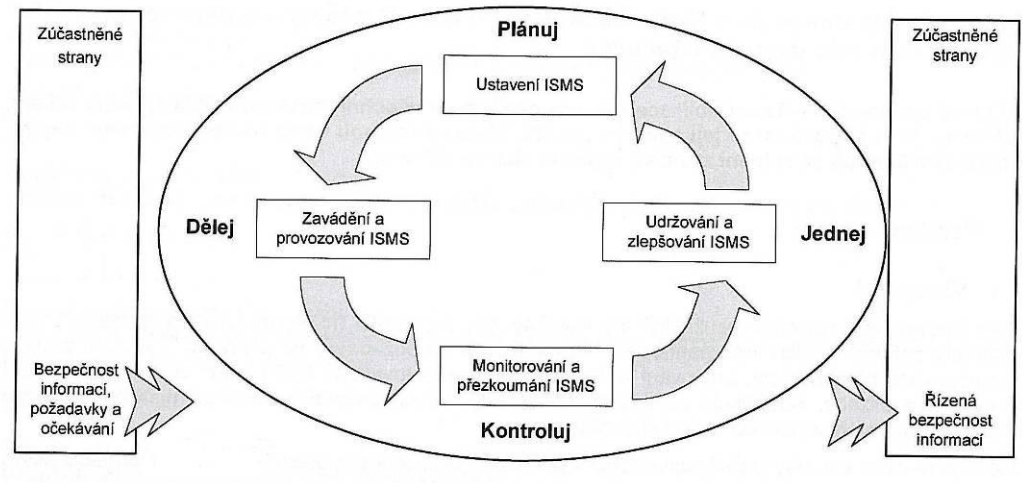
Podle požadavku konkrétního zadavatele může být metodika dále korigována či upřesněna tak, aby vyhovovala následujícím standardům či legislativě: **Control Objectives for Information and related Technology (COBIT), US Sarbanes-Oxley Act of 2002, IT Control Objectives for Sarbanes-Oxley.** [2]

2.6.2 Model PDAC

Pro zvolený subjekt byla jako základní metoda ISMS zvolen model PDAC. Koncept modelu PDAC poskytuje schematické vyjádření životního cyklu celého integrovaného systému řízení nebo jeho komponenty a zároveň zajišťuje i zpětnou vazbu. Tento přístup

umožňuje používat shodné metodiky a postupy pro řízení každé komponenty integrovaného systému řízení a ISMS jako celku.[4]

Zároveň je důležité sledovat a vyhodnocovat účinnost a účelnost.



Obr. 4. PDAC model aplikovaný na procesy ISMS [8]

Tab. 2. Vysvětlení modelu PDCA

Plánuj (ustavení ISMS) – PLAN	Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
Dělej (zavádění a provozování ISMS) – DO	Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
Kontroluj (monitorování a přezkoumání ISMS) - CHECK	Posouzení a kde je to možné i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
Jednej (udržování a zlepšování ISMS) - ACT	Přijeté opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS

3 VOLBA STRATEGIE ANALÝZY RIZIK

Možnosti dále uvedené popisují čtyři různé přístupy k analýze rizik. Základním rozdílem mezi těmito přístupy je hloubka analýzy rizik. Protože je obecně příliš nákladné provádět u všech zkoumaných systémů podrobnou analýzu rizik, a není rovněž efektivní věnovat vážným rizikům jen okrajovou pozornost, je nutné docílit mezi těmito možnostmi určitou rovnováhu.[2]

Ponecháme-li stranou možnost nedělat nic a při akceptování skutečnosti, že systém bude vystaven určitému počtu rizik neznámého rozsahu a síly, existují čtyři základní volby strategie pro analýzu rizik:

- použít stejný základní přístup u všech systémů, bez ohledu na rizika, kterým jsou systémy vystaveny, a akceptovat skutečnost, že úroveň bezpečnosti nemusí být vždy odpovídající,
- použít neformální přístup k provedení analýzy rizik a soustředit se na systémy, které jsou vnímány jako systémy vystavené nejvyšším rizikům,
- provést podrobnou analýzu rizik s použitím formálního přístupu pro všechny systémy,
- provést počáteční analýzu rizik „na hrubé úrovni“ a tím identifikovat systémy vystavené vysokým rizikům nebo kritické pro činnost organizace, a poté provést u těchto systémů podrobnou analýzu rizik, a aplikovat na všechny ostatní systémy základní bezpečnost.

Tyto různé možnosti pro řešení bezpečnostních rizik jsou v dalším popsány, a dále je uvedeno doporučení, kterému přístupu by měla být dána přednost. Jestliže se organizace rozhodne, že nebude, pokud jde o bezpečnost dělat nic nebo že odloží implementaci ochranných opatření, management by si měl být vědom možných důsledků tohoto rozhodnutí.

3.1 Základní přístup

Jako první možnost by organizace mohla aplikovat základní bezpečnost u všech systémů výběrem standardních ochranných opatření. V základních dokumentech a praktikách jsou navrženy různé druhy standardních ochranných opatření. Tento přístup má řadu výhod, mezi něž patří:

- pro analýzu a management rizik je u každé implementace ochranných opatření potřebné pouze minimální množství zdrojů, je tedy snížen čas a úsilí věnované výběru ochranných opatření,
- základní ochranná opatření mohou nabídnout cenově výhodná řešení, protože pro mnoho systémů mohou být bez velkého úsilí přijata totožná nebo podobná základní ochranná opatření v případě, že velké množství systémů organizace pracuje ve společném prostředí, a jsou-li bezpečnostní potřeby srovnatelné.

Nevýhody této volby jsou:

- jestliže je základní úroveň nastavena příliš vysoko, může být bezpečnost pro některé systémy příliš nákladná,
- je-li základní úroveň příliš nízká, pro některé systémy to může představovat nedostatek bezpečnosti, a výsledkem bude vysoký stupeň možného narušení bezpečnosti,
- při řízení změn, týkajících se bezpečností, mohou nastat potíže.

Mají-li všechny systémy organizace pouze nízkou úroveň bezpečnostních požadavků, může to být, pokud jde o náklady nejefektivnější strategie. V tomto případě musí být vybrána základní úroveň, odrážející stupeň ochrany požadovaný většinou systémů. Většina organizací bude vždy potřebovat splnit určité minimální standardy, aby ochránila citlivá data a byla ve shodě s legislativou a předpisy, např. legislativou na ochranu dat. Avšak tam, kde se systémy organizací liší v citlivosti, rozsahu a komplexnosti činnosti, nebylo by ani logické ani efektivní z hlediska nákladů aplikovat na všechny systémy obecný standard.

3.2 Neformální přístup

Tato možnost představuje neformální, pragmatickou analýzu rizik. Neformální přístup není založen na strukturovaných metodách, ale využívá znalosti a zkušenosti jednotlivců.

Výhodou této volby je, že nevyžaduje obvykle mnoho zdrojů nebo času. K provedení této neformální analýzy není nutné se naučit nové dodatečné dovednosti a tato analýza je provedena rychleji než podrobná analýza rizik.

Existuje však také několik nevýhod:

- bez určitého typu formálního přístupu nebo detailních seznamů kontrol vzrůstá pravděpodobnost opomenutí některých důležitých detailů,

- je obtížné obhájit implementaci ochranných opatření ve vztahu k rizikům odhadnutým tímto způsobem,
- v minulosti byly některé přístupy založeny na zranitelnostech, tj. byla implementována bezpečnostní ochranná opatření založená na identifikovaných zranitelnostech, aniž by se zvažovalo, zda existovaly některé hrozby, které by pravděpodobně využily tyto zranitelnosti, tj. zda vůbec existovala reálná potřeba ochranných opatření,
- může se vyskytnout určitý stupeň subjektivity; specifická předpojatost pracovníka provádějícího revizi může ovlivnit výsledky.

Pro mnoho organizací tato volba s ohledem na výše uvedené nevýhody nepředstavuje efektivní přístup k analýze rizik.

3.3 Podrobná formální analýza

Třetí možností je provést u všech systémů organizace podrobnou analýzu rizik. Podrobná analýza rizik zahrnuje hloubkovou identifikaci a ohodnocení aktiv, odhad hrozeb pro tato aktiva a odhad zranitelností. Výsledky těchto aktivit jsou potom použity k odhadu rizik a tedy k identifikaci zdůvodnitelných bezpečnostních ochranných opatření. Mezi výhody tohoto přístupu patří:

- je pravděpodobné, že budou pro potřeby každého systému identifikována vhodná ochranná opatření,
- výsledky podrobné analýzy mohou být využity v řízení změn týkajících se bezpečnosti.

Nevýhody této volby jsou:

- k získání výsledků vyžaduje značný objem času, úsilí a expertizu,
- existuje možnost, že bezpečnostní potřeby kritického systému budou řešeny příliš pozdě, protože všechny systémy by měly být posuzovány na stejné úrovni podrobností a k dokončení takové analýzy je potřeba značného objemu času a prostředků.

Není proto žádoucí používat podrobnou analýzu rizik u všech systémů.

3.4 Kombinovaný přístup

Čtvrtou možností je nejprve provést počáteční analýzu rizik na hrubé úrovni pro všechny systémy, která se soustřeďuje u každého případu na hodnotu systému pro činnost

organizace a na vážná rizika, jimž je systém vystaven. U systémů, které jsou identifikovány jako významné pro činnost organizace a/nebo vystavené vysokým rizikům, se přednostně provádí podrobná analýza rizik. Pro všechny zbývající systémy by měl být zvolen základní přístup. Tato volba umožňuje minimalizaci času a úsilí věnovaného na identifikaci ochranných opatření, přičemž stále ještě zajišťuje, že jsou vysoká rizika systémů chráněna příslušným způsobem. Mezi další výhody této volby patří:

- začlenění jednoduchého a rychlého přístupu pravděpodobně získá souhlas s přijetím programu analýzy rizik,
- bude možné rychle vytvořit strategický obraz organizačního bezpečnostního programu, který se stane pomocí při plánování,
- zdroje a peníze mohou být použity tam, kde to bude nejvýhodnější, a systémy, které budou pravděpodobně potřebovat nejvíce ochrany, budou řešeny jako první,
- aktivity sledování budou úspěšnější.

Jedinou potenciální nevýhodou je:

- protože počáteční analýzy rizik jsou provedeny na hrubé úrovni a potenciálně jsou méně přesné, nemusí být některé systémy identifikovány jako systémy vyžadující podrobnou analýzu rizik.

Tyto systémy by však měly být stále ještě pokryty základní bezpečností. Proto bychom se měli k těmto systémům vrátit v případech, kdy by bylo nutné zkontrolovat, zdali vyžadují více než jen základní přístup. Přijetí přístupu analýzy rizik na hrubé úrovni, kombinovaného se základním přístupem, a provedení podrobné analýzy rizik tam, kde je to vhodné, představuje pro většinu organizací nejefektivnější cestu.

Kombinovaný přístup k analýze rizik je rovněž doporučen pro provádění analýzy rizik u malých a středních organizací. Jeho pracnost je jen o málo vyšší než neformální přístup, přitom však poskytuje dokumentované a opakovatelné výsledky.

4 POSTUP PROVEDENÍ ANALÝZY RIZIK

4.1 Identifikace komponent a stanovení hranic analýzy rizik

Definovat pohled na ohodnocení vyžaduje nalézt a určit hranice systémů a organizační odpovědnost. Určit hranice systémů propojených sítěmi je vždy mnohem obtížnější. Mnoho organizací používá distribuovanou architekturu klient-server, kde servery a pracovní stanice spolu komunikují pomocí počítačové sítě. Tatáž síť je pak připojena k Internetu. Systém identifikujeme tak, že definujeme hranice okolo skupiny procesů, komunikací, datových úložišť a příslušejících zdrojů. Elementy uvnitř těchto hranic vytvářejí jednotlivý systém, vyžadující samostatná systémová bezpečnostní pravidla a nové vyhodnocení bezpečnosti, jakmile dojde k větší modifikaci systému. Každý element systému musí:

- být pod tímtéž přímým řízením,
- mít tutéž funkčnost nebo účel činnosti,
- mít v podstatě tytéž funkční charakteristiky a bezpečnostní potřeby,
- být umístěn v tomtéž obecném provozním prostředí.

Předtím, než se shromáždí vstup pro identifikaci a hodnocení aktiv, by měly být definovány hranice revize. Pečlivá definice hranic v tomto stádiu znamená, že se vyhneme zbytečné práci a zvýšíme kvalitu analýzy rizik. Popis hranic by měl jasně určit, které z dále uvedených prvků se při provádění revize analýzy rizik v uvažovaném systému zohlední. Typickými komponentami jsou například subsystém připojení k internetu, skupina pracovních stanic nebo souborový server.

4.2 Identifikace a ocenění aktiv

Aktivum je komponenta nebo část celkového systému, které organizace přímo přiřazuje hodnotu a pro kterou tudíž organizace požaduje ochranu. Při identifikaci aktiv by mělo být vzato v úvahu, že systém IT netvoří jen hardware a software.

Všechna aktiva uvnitř stanovených hranic analýzy musí být identifikována. Na druhé straně jakákoliv aktiva vyloučená z jakýchkoliv důvodů z okruhu analýzy je nutné přiřadit do jiné revize, aby se zajistilo, že nebudou opomenuta nebo přehlédnuta.

Poté, co byl splněn cíl identifikace aktiv vypracováním seznamu všech aktiv systému podléhajících analýze, se těmto aktivům přiřazují hodnoty, které reprezentují význam aktiv pro činnost organizace. To je možné vyjádřit ve smyslu bezpečnostních problémů, jako jsou potenciální nepříznivé dopady na činnost organizace plynoucí ze zpřístupnění, modifikace, nedostupnosti a/nebo zničení informací a dalších aktiv systému. Tak se identifikace a ohodnocení aktiv založené na potřebách činnosti organizace stává hlavním faktorem při determinaci rizik.

Vstupní údaje pro hodnocení aktiv by měly být zajištěny vlastníky a uživateli aktiv. Přiřazené hodnoty by se měly vztahovat k nákladům na pořízení a udržování aktiva na potenciální nepříznivé dopady na činnost organizace plynoucí ze ztráty důvěrnosti, integrity, dostupnosti, individuální odpovědnosti, autenticity a spolehlivosti. Každé z identifikovaných aktiv by mělo mít pro organizaci určitou hodnotu.

Hodnota aktiv je v tomto případě zjišťována v poměrné stupnici od 1 do 5. K jednotlivým stupňům jsou přiřazeny i orientační finanční hodnoty a porovnání s hodnotou majetku.

Tab. 3. Hodnota aktiv

Stupeň	Slovní popis	Finanční vyjádření	Porovnání s majetkem
1	Zanedbatelná	v řádu 1.000 Kč	spotřební materiál
2	Nízká	v řádu 10.000 Kč	drobný hmotný majetek
3	Střední	v řádu 100 000 Kč	hmotný majetek
4	Vysoká	v řádu 1 mil. Kč	investice
5	mimořádně vysoká	v řádu 10 mil. Kč a více	celý majetek organizace

4.3 Odhad úrovně hrozeb

Hrozba představuje možnost poškodit zkoumaný systém a jeho aktiva. V případě jejího výskytu by měla působit na systém v tom smyslu, že bude příčinou nežádoucích incidentů a tudíž nepříznivých dopadů.

Hrozby mohou být přírodního nebo lidského původu, a mohou být náhodné nebo úmyslné. Měly by být identifikovány zdroje jak náhodných tak úmyslných hrozeb a měla by být odhadnuta pravděpodobnost jejich výskytu. Podstatné je, aby nebyla přehlédnuta žádná

relevantní hrozba, protože by to mohlo mít za následek selhání nebo oslabení bezpečnosti systému.

Po identifikaci zdroje hrozby (kdo a co bylo příčinou hrozby) a cíle hrozby (tj. které prvky systému mohou být hrozbou ovlivněny), je nutné odhadnout pravděpodobnost hrozby. Přitom by se mělo přihlédnout k:

- četnosti hrozby (stanovit na základě zkušeností, statistiky, atd. jak často by se mohla hrozba vyskytnout.), zda-li může být aplikována statistika apod.,
- motivaci, vědomým a nutným možnostem, zdrojům, které jsou dostupné pro možné útočníky, a pocitu,
- atraktivnosti a zranitelnosti aktiv systému pro možné útočníky, jako zdroji záměrných hrozeb,
- geografickým faktorům jako je blízkost chemických továren nebo továren na zpracování nafty, možnosti extrémních povětrnostních podmínek a faktorům, které by mohly ovlivnit lidské chyby a chybné funkce zařízení, jako zdroji náhodných hrozeb.

Po dokončení odhadu existuje seznam identifikovaných hrozeb, aktiv nebo skupiny aktiv, které mohou tyto hrozby ovlivnit, a míra pravděpodobnosti výskytu hrozeb. Úroveň hrozeb je v tomto případě zjišťována v poměrné stupnici od 1 do 5. K jednotlivým stupňům jsou přiřazeny i orientační hodnoty četnosti výskytu a možných nepříznivých dopadů.

Tab. 4. Četnost výskytu hrozeb

Stupeň	Slovní popis	Četnost výskytu	Možný dopad
1	Zanedbatelná	jednou za více let	nevýznamný
2	Nízká	jednou ročně	znatelný
3	Střední	jednou měsíčně	krátkodobé vážné problémy
4	Vysoká	jednou za několik dnů	dlouhodobé vážné problémy
5	Mimořádně vysoká	několikrát denně	zánik organizace

4.4 Odhad míry zranitelností

Tento odhad identifikuje zranitelnosti, které mohou být využity hrozbami a odhaduje pravděpodobný stupeň slabých míst, tj. snadnosti jejich využití. Např. některá aktiva jsou

snadno manipulovatelná, snadno ukryta nebo přepravena - všechny tyto vlastnosti se mohou týkat zranitelností. Příklady zranitelností jsou:

- nechráněná spojení (například na Internet),
- neškolení uživatelé,
- chybný výběr a použití hesel,
- neexistence řádného řízení přístupu (logického a/nebo fyzického),
- neexistence zálohovacích kopií informací nebo softwaru,
- umístění v oblastech ohrožených záplavami.

Je důležité odhadnout, jak vážné jsou zranitelnosti, jinými slovy, jak snadno mohou být využity. Měla by být odhadnuta zranitelnost ve vztahu ke každé hrozbě, která by mohla tuto zranitelnost ve specifické situaci využít. Například zranitelnost na předstírání identity uživatele může být vysoká jako důsledek absence autentizace uživatele. Na druhé straně zranitelnost týkající se zneužití zdrojů může být nízká, protože dokonce i v případě chybějící autentizace uživatele jsou prostředky, pomocí kterých mohou být zdroje zneužity, limitovány.

Výsledkem je seznam zranitelností a odhad snadnosti jejich využití. Úroveň zranitelností je v tomto případě zjišťována v poměrné stupnici od 1 do 5.

Tab. 5. Úroveň zranitelnosti

Stupeň	**Slovní popis**	**Stupeň poškození aktiva**	**Účinnost protiopatření**
1	Zanedbatelná	zanedbatelné (1%)	dokonalá (100%)
2	Nízká	malé (5%)	velmi dobrá (80%)
3	Střední	střední (20%)	částečná (50%)
4	Vysoká	těžké (50%)	nízká (20%)
5	mimořádně vysoká	úplná destrukce (>80%)	zanedbatelná (<5%)

4.5 Hodnocení míry rizika

Tato kapitola je zaměřena na poslední etapu, což je vyhodnocení celkových rizik. Jak bylo již dříve uvedeno, aktiva, která mají hodnotu a určitý stupeň zranitelností, jsou v riziku

vždy, když existuje nějaká hrozba. Vyhodnocení rizik je kombinací potenciálních nepříznivých dopadů nežádoucích incidentů na činnost organizace a stupně odhadnutých hrozeb a zranitelností. Rizika představují míru vystavení se hrozbě, jehož subjektem může být systém a příslušná organizace. Rizika jsou funkcí:

- hodnot aktiv,
- hrozeb a s nimi spojených pravděpodobností výskytu, které mohou ohrozit aktiva,
- snadnosti využití zranitelností hrozbami, které vyvolají nežádoucí dopady,
- existujících a plánovaných ochranných opatření, která mohou snížit závažnost zranitelností, hrozeb a dopadů.

Cílem analýzy rizik je identifikovat a odhadnout rizika, kterým je systém a jeho aktiva vystaven, aby mohla být identifikována a vybrána vhodná a oprávněná bezpečnostní ochranná opatření. Při odhadování rizik je zvažováno několik aspektů včetně jejich dopadu a pravděpodobnosti.

Výsledkem tohoto kroku je seznam naměřených rizik pro každý z dopadů, který je důsledkem zpřístupněni, modifikace, nedostupnosti nebo zničení posuzovaného systému. Míry rizika pomáhají také identifikovat, která rizika by měla být při výběru ochranných opatření řešena jako první. Míra rizika při použití stupnic uvedených v předchozích kapitolách dosahuje hodnoty od 1 do 100 a je počítána podle vzorce:

Riziko = Hodnota aktiva * Úroveň hrozby * Míra zranitelnosti

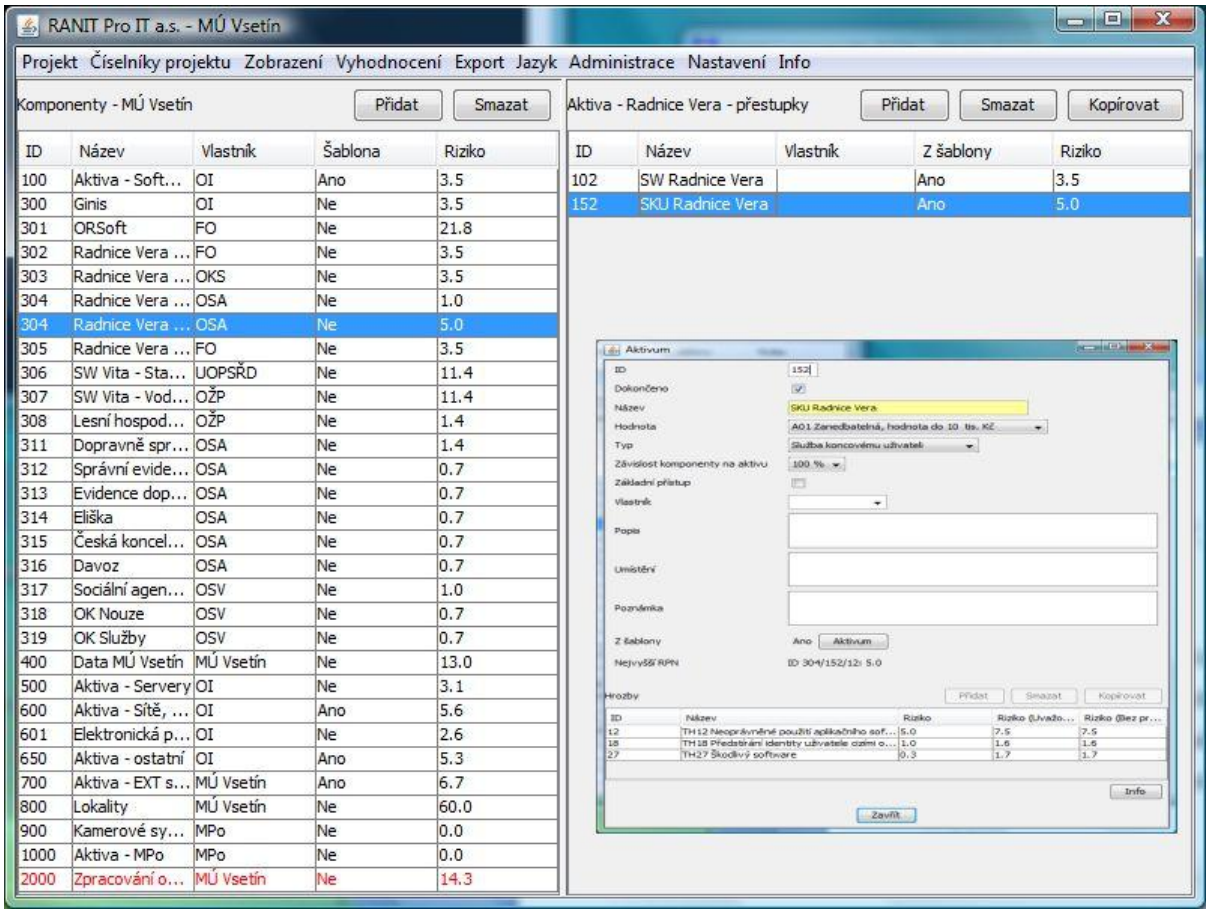
4.6 Software pro analýzu rizik - RANIT

RANIT je aplikace firmy ProIT a.s., vytvořená pro podporu provádění rizikových analýz. Slouží pro ukládání a vyhodnocování údajů získaných v průběhu řízených pohovorů s vlastníky aktiv nebo procesů. Program implementuje metodiku provádění rizikové analýzy podle ČSN ISO/IEC TR 13335 a ČSN ISO/IEC 27005 kombinovanou metodou. Pro potřeby malých organizací je poskytována zjednodušená verze programu. Použitá verze programu RANIT udržuje oddělené tabulky: komponent, aktiv, vlastníků, typů aktiv, hodnoty aktiv, hrozeb, úrovně hrozeb, míry zranitelnosti, ochranných opatření, barevného zvýraznění v závislosti na vypočtené míře rizika.

Položkám hodnoty aktiva, úrovně hrozby a míry zranitelnosti jsou pevně přiřazeny hodnoty použité pro výpočet míry rizika. Hodnoty jsou zvoleny tak, aby míra rizika dosahovala hodnot z intervalu 1 až 100.

Každému typu aktiva lze v průběhu implementace z tabulky hrozeb přiřadit hrozby, které jsou pro tento typ relevantní a budou nabízeny k výběru. Tento seznam je zároveň vodítkem při řízeném pohovoru s vlastníkem aktiva.

Každé hrozbě lze v průběhu implementace z tabulky protiopatření přiřadit ta ochranná opatření, která jsou pro tuto hrozbu relevantní a která budou nabízena k výběru. Tento seznam je zároveň vodítkem při řízeném pohovoru s vlastníkem aktiva.



Obr. 5. Uživatelské rozhraní SW RANIT

Program RANIT podporuje sběr údajů pro analýzu rizik následujícím postupem:

1. Založení komponenty, přiřazení vlastníka, volitelně vyplnění polí Popis, Umístění, Poznámka. Komponent může být v jednom projektu libovolný počet.

2. Založení aktiva jako součásti komponenty. Přiřazení typu aktiva, vlastníka a hodnoty aktiva. Volitelně vyplnění polí Popis, Umístění, Poznámka. Aktiv může být v jedné komponentě libovolný počet.
3. Založení hrozby vztahující se k aktivu. Hrozba je nabízena k výběru z tabulky hrozeb v závislosti na typu aktiva. Dále přiřazení úrovně hrozby výběrem z tabulky úrovní, přiřazení míry zranitelnosti výběrem z tabulky, přiřazení jednoho nebo více protiopatření výběrem z tabulky protiopatření. Hrozeb může být v jedné aktivitě libovolný počet.

Kdykoliv v průběhu vkládání dat lze vytvořit textový soubor ve formátu RTF, obsahující podrobný výpis a vyhodnocení všech získaných údajů, setříděný podle aktiv nebo podle vypočtené míry rizika.

Tabulky hrozeb a protiopatření obsahují kompletní provázané katalogy, celkem asi o 1200 položkách. Tabulky hodnoty aktiva, úrovně hrozby a míry zranitelnosti jsou naplněny standardními hodnotami pro výpočet relativní míry rizika v rozsahu 0 až 100.

Program RANIT je vytvořen v programovacím jazyce JAVA verze 5 a lze jej spustit na jakémkoli operačním systému na kterém běží J2SE Runtime Environment (JRE) společnosti Sun microsystems minimálně verze 5.0. Pro ukládání dat se používá databáze MS SQL. [13]

II. PRAKTICKÁ ČÁST

5 ARCHITEKTURA INFORMAČNÍHO SYSTÉMU MĚÚ VSETÍN

5.1 Vize informačního systému

Hlavní vizí IS MěÚ Vsetín je postupný přechod od stávajícího heterogenního systému k novému homogennímu programovému vybavení. V průběhu posledních let byla realizována homogenizace operačních systémů, která zjednodušila síťovou správu, jak v rovině operačních systémů serverů, tak pracovních stanic.

Homogenizace aplikací – probíhá postupný přechod od jednotlivých roztříštěných a vzájemně nekomunikujících aplikací k modulárním vzájemně komunikujícím celkům.

Homogenizace datové základny je již na vysoké úrovni – v podstatě všechny IS MěÚ využívají databázový systém MS SQL2005.

Velký důraz je kladen na rozvoj systémů pro podporu informování veřejnosti a podporu elektronických forem komunikace s veřejností.

5.2 Finanční zabezpečení

Pro plánování způsobu a rozsahu financování je vypracováván rámcový finanční plán na období čtyř až pěti let s roční aktualizační periodou. Tento rámcový finanční plán obsahuje plánování finančních prostředků na:

- provoz a údržbu používaných zařízení a informačních technologií,
- nákup informačních technologií v rámci pravidelného procesu obnovování techniky a programového vybavení, které je zastaralé, nefunkční nebo na hranici životnosti,
- pořizování nových informačních technologií v rámci plánovaných technologických změn,
- rozšiřování programového vybavení v rámci plánovaného rozšiřování podpory agend informačním systémem.

Financování rozvoje informačního systému je konkretizováno a prakticky realizováno každoročně sestavením rozpočtu města, který obsahuje konkrétní finanční rámec pro rozvoj informačního systému městského úřadu na následující kalendářní rok. Rozpočet schvaluje městské zastupitelstvo. Na základě následující tabulky je možné považovat investice

směřující do IS v průměrné výši cca 7 mil. Kč ročně jako dostatečné, ovšem pouze s malými finančními možnostmi pro inovace a rozšiřování.

Tab. 6. Výdaje na informační systém městského úřadu (v tis. Kč)

	Paragraf	Položka	2007	2008	2009	2010
Výpočetní technika	6171	5137	1 631	667	981	543
Investice	6171	6121,6122,6125	1 468	896	1 810	500
Všeobecný spotřební materiál	6171	5139	645	510	505	290
Servis	6171	5169	299	281	536	301
Služby a zpracování dat	6171	5168	1 900	1891	2146	2 767
Internet, www, Vismo	6171	5162	300	282	365	331
Údržba a opravy	6171	5171	430	350	400	460
Programové vybavení	6171	5172,611	840	795	1605	361
Celkové náklady (informatika)			7 513	5 671	8348	5 553
Objem rozpočtu MěÚ			665 000	700 000	515 000	813 000
% rozpočtu MěÚ			1,13	0,81	1,62	0,68

5.3 Materiální zabezpečení

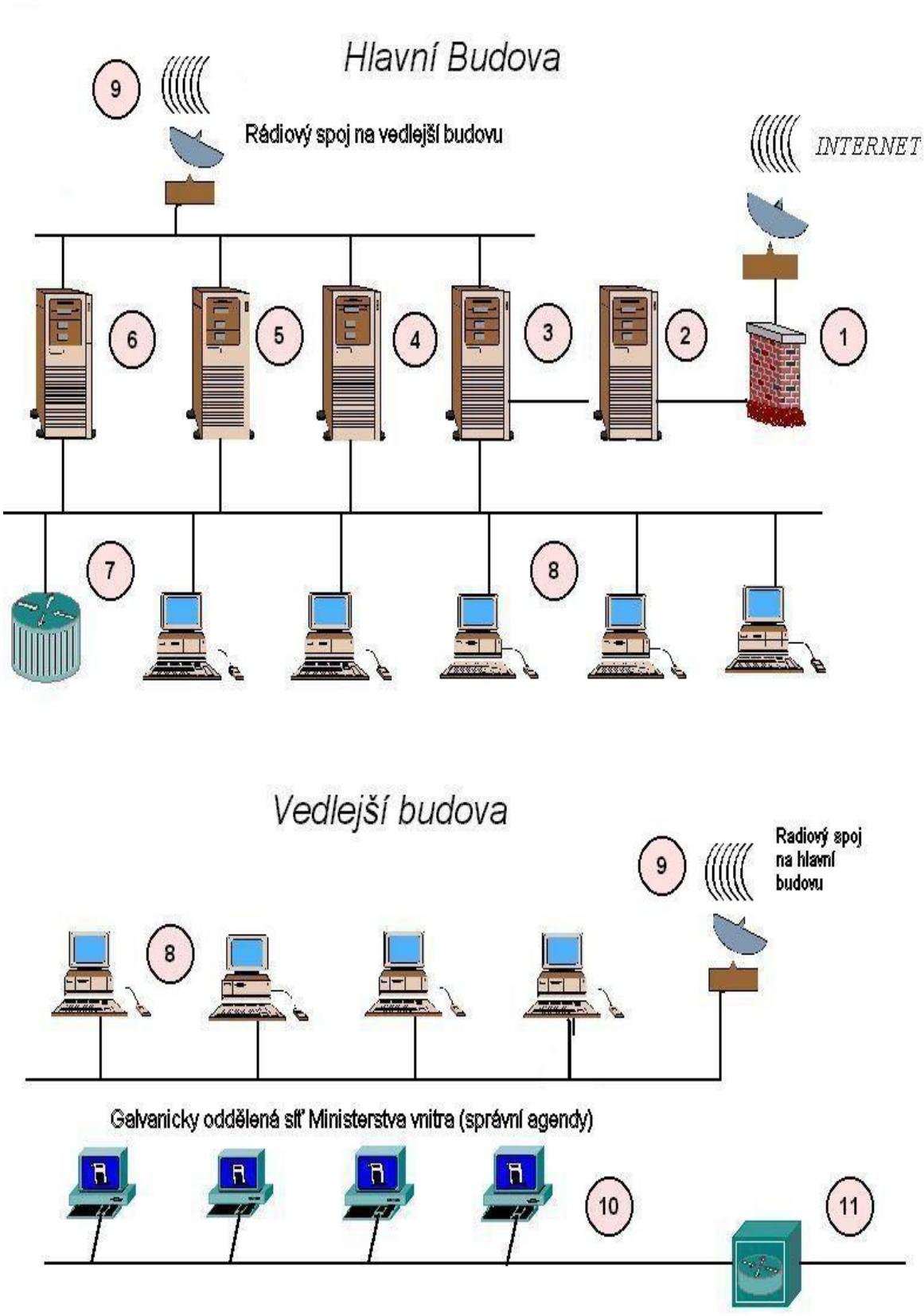
5.3.1 Hardware

Jak vyplývá z níže uvedené tabulky, hardwarové vybavení městského úřadu se periodicky obnovuje. Každoročně je pořízeno cca 25 nových uživatelských pracovišť. Systém zálohování firmy COMA komplexně vyřešil způsob zálohování dat serverů i uživatelů (každý uživatel má na fileserveru diskový prostor o kapacitě 2GB a může kdykoliv provést zálohu svých dat). Nový výkonný server – hlavní doménový řadič - zefektivnil správu síťového prostředí a nabídl uživatelům IS větší kapacitu sdílených zdrojů (Intranet).

Tab. 7. Určující hardwarové komponenty - servery

Pozice ve schématu	Funkční zařízení	Termín pořízení	Základní konfigurace
1	Firewall	2006	Cisco ASA 5510 Security plus
2	Proxy server	2009	HP řady DL 380 (rack provedení) 1x quadcore Intel Xeon E5440 2,8GHz, 8GB RAM, 2x HDD 146GB SAS RAID1, LAN 4 x 1Gbit/s MS Windows Server 2008 Standard KERIO Firewall, Kerio Connect
3	Doménový server Primární řadič domény	2009	HP řady DL 280G5 (rack provedení) 2x quadcore Intel Xeon E5440 2,8GHz, 16 GB RAM, 2x HDD 146GB SAS RAID1, LAN 4 x 1Gbit/s MS Windows Server 2008 Enterprise s Hyper-V (3virtuální stroje)
4	Doménový, poštovní a zálohovací server Sekundární řadič	2003	ATComputers, Mercury 87, 2x Intel Xeon 2GHz, 4GB RAM, pole RAID5 210GB MS Windows Server 2003 Standard MS Exchange2003
5	Databázový server	2006	ATComputers, Mercury MX5010HS, (rack provedení) 2x Intel Xeon 3,2GHz, 8GB RAM, pole RAID1 75GB, RAID5 250GB, RAID5 900GB, LAN 4 x 1Gbit/s MS Windows Server 2003 Etrprise 64bit MS SQL 2005
6	Server GIS	2001	ATComputers, Mercury 7200, IP III 850 MHz, 512 MB RAM, pole RAID 5 36,5GB
7	Router	2009	
8	Uživatelská pracoviště	2005 -	Pracovní stanice postavené na platformě procesoru Intel s různou výkonností odpovídající termínu pořízení
9	Rádiový spoj mezi budovami MěÚ	2009	Alcoma AL24F, 24GHz, 311Mbit/s.
10	LAN síť Ministerstva vnitra	2003-	Galvanicky oddělená terminálová síť Ministerstva vnitra ČR
11	Propoj MV ČR	2003-	Připojení na síť Ministerstva vnitra ČR

Čísla ve sloupci tabulky „pozice ve schématu“ odpovídají pozicím uvedeným na obrázku číslo 4 - Orientační schéma ICT technologií v budovách městského úřadu, na následující stránce.



Obr. 6. Orientační schéma ICT technologií v budovách městského úřadu.

5.3.2 Software

Některé IS jsou pro chod městského úřadu klíčové (používají je denně desítky uživatelů), jiné mají jen okrajový význam (zpracovávají se jednou za nějaké období zpravidla na lokálním pracovišti). Z klíčových agendových IS uvádím:

Spisová služba SSL Gordic

Radnice VERA s moduly: Registry obyvatel a ekonomických subjektů, Banka, Pokladna, Export do účetnictví, Tvorba rozpočtu, Příjmy – Daně a poplatky, Výdaje, Vymáhání pohledávek, Statistik, Splátky a půjčky.

Radnice ORTEX obsahuje moduly: Účetnictví, Mzdy a Personalistika, Majetek

Stavební úřad VITA

Geografický informační systém: Vektorové hranice parcel, Bloková mapa, Územně plánovací dokumentace, Letecké snímky, Digitální technická mapa, Digitální model terénu, Pasport místních komunikací, Pasport zeleně, Pasport rekreace a sportu

5.3.3 Vazby na ostatní systémy celostátní a mezinárodní

Vazba na Ministerstvo práce a sociálních věcí

Odbor sociálních věcí a zdravotnictví používá přímý přístup k databázím ministerstva přes dedikovaný pronajatý datový okruh.

Vazba na Ministerstvo průmyslu a obchodu ČR

Obecní živnostenský úřad pracuje v oddělené agendě Registr živnostenského podnikání (RŽP), provozované centrálně se zabezpečeným SSL přístupem pře internet do databáze ministerstva.

Vazba na IS Ministerstva vnitra ČR

Odbor správních agend používá v rámci svých kompetencí následující agendy. Evidenci řidičských průkazů a motorových vozidel, agendu občanských průkazů a cestovních dokladů. Tyto klientské aplikace jsou provozovány na stanicích připojených do LAN, která je galvanicky oddělena od vnitřní LAN MěÚ, s přímým připojením přes pronajatý okruh na servery Ministerstva vnitra ČR.

5.3.4 Rozhraní s veřejností

V současné době nabízí IS městského úřadu veřejnosti (mimo klasickou a elektronickou úřední desku) komunikační rozhraní na svých webových stránkách pomocí www aplikace Městského úřadu Vsetín (www.mestovsetin.cz), které slouží především k přenosu informací o městě a informací o činnosti městského úřadu směrem k veřejnosti. Přímé datové vstupy (elektronické formuláře) přes definované rozhraní jsou používány zatím spíše méně. V rámci projektu „ Zdravé město“ je na stránkách města v současné době umístěno několik dotazníků a formulářů žádostí, které mají občané možnost vyplnit a odeslat. Dále je v rámci projektu Metropolitní síť Vsetín umožněno on-line objednávání klientů na odboru správních agend.

5.3.5 Pracovníci

Odpovědnost za dosažení požadované úrovně využití informačních technologií je třeba vidět minimálně v těchto dvou rovinách:

- **obsahová (technologická)** – odpovědnost za dosažení požadované a touto strategií plánované technologické a obsahové stránky rozvoje informačního systému města – vedoucí odboru informatiky,
- **finanční** – odpovědnost za rozsah finančních prostředků, investovaných do rozvoje informačního systému má zastupitelstvo města (schvalování rozpočtu) případně rada města (schvalování rozpočtových změn).

Stav informačního systému města je pravidelně hodnocen a případná zodpovědnost je pak následně vyvozována souběžně s procesem aktualizace informační strategie, který bude z hodnocení dosažené úrovně informačního procesu vždy vycházet.

5.3.6 Architektura IS, ISVS

V rámci vstupní analýzy stavu informační bezpečnosti není dostatečný prostor na podrobnou diskusi návrhu architektury IS. Nicméně lze konstatovat, že IS MěÚ Vsetín je relativně heterogenní.

Problematika splnění požadavků zákona č. 365/2000 Sb. nebyla předmětem této analýzy. Je nutné konstatovat, že základní povinnosti vyplývající pro informační systémy veřejné

správy (dále jen ISVS) z uvedeného zákona a navazujících vyhlášek jsou splněny. Je vypracována informační koncepce a je k dispozici provozní dokumentace ISVS.

Navržená opatření:

V rámci dlouhodobého řízení informačních systémů veřejné správy zvážit možnosti centralizace IS MěÚ Vsetín.

5.4 Soulad IT/IS strategie s posláním Městského úřadu

Jak vyplývá z informační strategie a z poslání MěÚ, panuje zde soulad. Jednou z priorit MěÚ je péče o potřeby svých občanů. MěÚ se snaží, aby občanům byly dostupné veškeré možné informace. Toto například dokládají webové stránky města www.mestovsetin.cz. Dalším příkladem je projekt Metropolitní síť Vsetín, kde bylo mimo jiné zřízeno 11 PIAPů, internetových kiosků, kde je poskytován veřejně přístupný internet. Tyto informační panely jsou rozmístěny ve školách, ve vybraných úřadech a na veřejných místech ve Vsetíně.

6 ANALÝZA RIZIK

Model IS MěÚ Vsetín (dekompozice IS na komponenty a aktiva) lze využít jako základ pro formální analýzu rizik. Provedená přehledová analýza rizik s ohledem k rozsahu tohoto projektu nenahrazuje formální analýzu rizik v oblasti bezpečnosti informací. Požadavky na dostupnost a důvěrnost informací budou porovnány s aktuálním stavem řešení a případné nesrovnalosti budou popsány včetně návrhu nápravných opatření.

Výstupem výchozí analýzy je popis současného stavu bezpečnosti informací, odhalení nejvýznamnějších hrozeb vzhledem k hodnotě klíčových aktiv, hodnocení stávajících opatření, jejich funkčnost a návrh dalšího postupu k dosažení požadované úrovně bezpečnosti informací. Je potřeba projít stávající technicko-organizační opatření, která byla přijata k zajištění ochrany osobních údajů. To vše v kontextu na platnou legislativu ČR.

Cílem výchozí analýzy je vypracování základního dokumentu o stavu bezpečnosti informací dle platných norem ČSN ISO/IEC 17799 a zákona č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších novelizací, jednoduše řečeno, popsat „Co je“, „Co je potřeba s ohledem na bezpečnost informací a platnou legislativu mít“ a „Návrh řešení odstranění disproporcí“.

Základní dokument o stavu bezpečnosti informací musí obsahovat kapitoly:

- cíle a strategie bezpečnosti informací,
- popis současného stavu bezpečnosti informací,
- odhad nejvýznamnějších hrozeb vzhledem k hodnotě klíčových aktiv,
- hodnocení stávajících opatření, jejich funkčnost,
- návrh dalšího postupu k dosažení požadované úrovně bezpečnosti informací, případně certifikaci systému řízení bezpečnosti informací – ISMS.[9]

Výchozí analýza umožní následné efektivní řešení bezpečnosti informací například implementací systému řízení bezpečnosti informací (ISMS) a řešení legislativních požadavků podle zákona č. 101/2000 Sb., o ochraně osobních údajů.

Řešení problematiky navrženým postupem, tzn. provedení vstupní analýzy a následná implementace ISMS, šetří čas, náklady a dává jistotu, že výsledek řešení bude v souladu s požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů.

6.1 Úvodní diskuse k analýze rizik

Na MěÚ Vsetín byl započat proces řízení bezpečnosti informací. Procesy jsou navrženy teoreticky ve shodě s technickými standardy a doporučeními dobré praxe. Systém jako celek však není důsledně provozován. Podstatné procesy z hlediska efektivity sytému řízení bezpečnosti informací jsou realizovány v některých případech jen formálně nebo vůbec. Takovýto závěr potvrzuje přehledové posouzení míry zavedení systému řízení (managementu) bezpečnosti informací: V aktuálním stavu jsou splněny formální i obsahové požadavky standardu ČSN ISO/IEC 27001 středně (míra shody 53 %). Certifikace ISMS dle standardu ČSN ISO/IEC 27001 klade relativně striktní požadavky na organizaci, která usiluje o získání certifikátu shody s uvedeným standardem. Certifikace ISMS dle uvedeného standardu pro MěÚ Vsetín není aktuálně závazná ani nezbytná. Lze proto doporučit především revizi stávajícího systému řízení bezpečnosti informací s důrazem na, z hlediska charakteru činnosti MěÚ Vsetín, podstatné procesy jako například: posouzení rizik, řízení přístupů, nakládání s médii a redukci méně podstatných procesů.

Objektivním důvodem skutečnosti, že v aktuálním stavu nejsou všechny teoreticky zavedené procesy reálně provozovány, jsou zřejmě kapacitní důvody. Tentýž důvod bude i limitujícím faktorem pro výběr vhodných procesů systému řízení bezpečnosti informací.

6.2 Vstupní analýza stavu informační bezpečnosti

V rámci tohoto projektu nebyla prováděna analýza rizik obvyklým systematickým postupem, ale jen rámcová, neformální a namátková analýza vybraných aktiv. Dekompozice IS je provedena dle základních funkčních (aplikačních celků). Tato kapitola nenahrazuje formální analýzu rizik, nejedná se o úplný a systematický výčet hrozeb.

6.3 Analýza rizik - hranice revize

Předmětem analýzy rizik je informační systém společnosti MěÚ Vsetín. Pod pojmem IS rozumíme systém zpracování informací v celém životním cyklu informace (od vzniku/pořízení po archivaci/likvidaci). V rámci analýzy byl hodnocen IS společnosti MěÚ Vsetín ve všech specifikovaných lokalitách.

6.4 Analýza rizik – komponenty IS

V rámci této práce, není možné uvést seznam všech aktiv, pro názornost je uvedena pouze část vybraných komponent IS a dalších aktiv. Podrobné vyhodnocení analýzy rizik zpracované podle komponent IS je uvedeno v Příloze P I: Přehledová analýza rizik - komponenty - vyhodnocení podle dopadů.

Tab. 8. Seznam aktiv

Kód Aktiva	Název aktiva	Vlastník	Kód Aktiva	Název aktiva	Vlastník
001	Spisová služba Ginis	Odbor informatiky	**008**	SW Vita – stavební úřad	Odbor výstavby
002	IS Radnice Orsoft	Finanční odbor	**009**	SW Vita – vodoprávní úřad	Odbor životního prostředí
003	IS Radnice VERA-poplatky	Finanční odbor	**010**	Sociální agenda ISSA Geovap	Odbor sociálních věcí
004	IS Radnice VERA-pokladna	Finanční odbor	**011**	OK Nouze	Odbor sociálních věcí
005	IS Radnice VERA-registr obyvatel	Odbor správních agend	**012**	Elektronická pošta	Odbor informatiky
006	Kamerový systém	Městská policie	**013**	Lokality	MěÚ Vsetín
007	Česká kancelář pojistitelů	Odbor správních agend	**014**	Zpracování osobních údajů	MěÚ Vsetín

6.5 Přehledová analýza rizik

Přehledová analýza rizik vznikala postupně při konzultacích na jednotlivých pracovištích MěÚ. Výsledky z těchto konzultací jsou zpracovány pomocí SW Ranit. Vzhledem k velkému objemu dat je uvedeno pouze vyhodnocení aktiv podle rizika v Příloze P II: Přehledová analýza rizik – vyhodnocení rizik podle aktiv. V následující kapitole jsou uvedeny zápisy z konzultací.

6.6 Popis současného stavu bezpečnosti informací

Tato kapitola zahrnuje systematizovaný zápis z konzultací na jednotlivých odborech MěÚ. Účelem není náhrada úplného popisu IS, ani technické dokumentace ICT, ale zachycení informací, na jejichž základě byl připraven návrh dalšího postupu, případně elementárních

protiopatření. Oblasti, které nejsou popsány, nebyly v rámci úvodní analýzy posuzovány, respektive nebyly zpracovateli dostupné relevantní podklady.

6.6.1 Odbor informatiky

Součást MěÚ Vsetín, zajišťuje ve dvou lokalitách služby pro následující subjekty:

- MěÚ Vsetín,
- Městská policie Vsetín,
- Vsetínská správní a investiční, příspěvková organizace,
- Společnost pro komunitní práci Vsetín, obecně prospěšná společnost.

Zaměstnancům jsou dávány k dispozici USB flash paměti (HW), které jsou evidovány, nicméně nejsou prováděny jejich zálohy, a nejsou žádným způsobem chráněny (kryptograficky).

Infrastruktura:

LAN — síťová vrstva: Adresace dle RFC 1918: adresní rozsahy s maskou 255.255.255.0, používány 3 VLAN: 192.168.10.0, 192.168.20.0, 192.168.30.0

Routing na routeru 3COM (důvod v aplikačních řešeních - neschopnost dodavatelů být nezávislý na síťové vrstvě).

DHCP: dynamicky, umožňuje připojit neznámá zařízení

Microsoft doména: Active directory, primární doménový řadič, sekundární doménový řadič s vynucováním připojení do domény

DNS poskytuje PDC, pro interní doménu, interní DNS

Externí DNS poskytuje provozovatel metropolitní sítě

Elektronická pošta: externí od poskytovatele (POP3) na Kerio Mail server, odtud na MS Exchange v interní síti, výběr schránek na protokolu POP3

Zálohování: centrální — servery na autoloader, zálohování osobních dat uživatelů na server vsetin2 (tzv. uživatelské schránky), lokální zálohování je možné.

Antivir: Na serveru Winproxy Kerio Connect včetně antiviru McAfee (kontrola e-mailů) a ESET NOD32 pro kontrolu ostatní komunikace z internetu. Ve vnitřní síti je na stanicích i serverech používán ESET NOD32 (server a konzola na serveru vsetin2). Každý počítač musí mít instalován antivirový program ESET NOD32. Notebooky mají nainstalován ESET Smart Security. Externí počítače (např. volení zástupci) musí mít vlastní antivirový program (není upřesněno).

Kerio Mail server zahrnuje antispamové řešení. Dále zahrnuje logy obsahující celý e-mail a logy aplikací se zálohují společně s aplikacemi.

PC.Info — není popsáno jako zpracování osobních údajů, nicméně může být.

Problémy: heterogenita agend — je otázkou dlouhodobého řízení

6.6.2 Odbor životního prostředí včetně oddělení krizového řízení

MěÚ Vsetín je prověřen na „V“ stupeň II. ukládání v papírové podobě. Další osoby prověřeny bezpečnostním ředitelem na stupeň V. Existuje prostor pro ukládání písemností, kovový trezor certifikován NBÚ. Prostory jsou definovány a fungují jako režimové pracoviště.

Utajované informace v elektronické podobě nejsou zpracovávány v místě, ale v případě potřeby na Krajském úřadě Zlínského kraje.

Je zaveden systém havarijního a krizového plánování. Institut zvláštních skutečností není potřeba, všichni členové krizového štábu jsou prověřeni. Zpracovávání plánu krizové připravenosti obce s rozšířenou působností Vsetín. SW podpora krizového řízení není implementována, ale je používán ARGIS a IS pro podporu krizové řízení provozované Hasičským záchranným sborem Zlínského kraje. Přístup do IS Radnice Vera, registr obyvatel, Spisová služba Ginis, GIS - nedostupnost řádově ve dnech nečiní problém.

Základní informace jsou v počítači uloženy lokálně.

6.6.3 Městská policie Vsetín

Je implementována Směrnice pro obsluhu a provoz kamerového systému, do které je třeba doplnit povinnost evidovat záznamová média, aktuálně existuje jen povinnost tato média likvidovat (ředitel MP, nebo zástupce ředitele MP). Kamerový systém - posouzení rizik bylo provedeno neformálně. Je třeba dopracovat technicky přístupy - aktuálně nejsou přístupová oprávnění do kamerového systému, ani v módu prohlížení, ani přístupu do archivu (dvě různé aplikace). Na pracovišti je 5 PC, obsahujících lokální data, respektive data mimo centrální IS, která nejsou využívána mimo sídlo provozovatele. K ukládání dat nejsou využívána síťová úložiště. Ředitel MP: návrhy smluv na notebook, bez kryptografické ochrany. Personalistika: ekonomika, personalistika, ekonomika - na lokálním počítači, nejde o trvalá data.

Dále se používají aplikace Patros, Patrmv (pátrání po osobách a kradených vozidlech), jejich provozovatelem i správcem Ministerstvo vnitra ČR.

Elektronická pošta: existuje povědomí o nemožnosti posílat důvěrné, či jinak chráněné informace.

6.6.4 Odbor územního plánování, stavebního řádu a dopravy

Vysoké dopady nefunkčnosti hlavní agendové aplikace - Vita stavební úřad - generuje také dopady do Spisové Služby Ginis. Zaměstnanci mají podepsánu mlčenlivost, podobně jako většina směrnic je podepsána všemi podřízenými na odboru

6.6.5 Obecní živnostenský úřad

Lokální data nepříliš hodnotná, ztráta nevadí. Jako agendový systém je centrálně používána aplikace Ministerstva průmyslu a obchodu – Registr živnostenského podnikání.

Sdílené disky, využívány zřídka. Pracovníci odboru mají k dispozici 2 notebooky k vyhotovení zápisů v exteriéru, data údajně nejsou hodnotná, nejvýše je dočasně uložena kontrolní zpráva.

E-mail - nedostupnost - problém se sděleními ze strany Krajského úřadu, odpovědi klientům - spíše ztráta dobrého jména. Povědomí o možnosti ztráty důvěry v této souvislosti.

Školení zahrnující ochranu informací není realizováno systematicky. Povědomí o problematice pracovníci odboru mají i vzhledem k povinnosti mlčenlivosti ze zákona o živnostenském podnikání. Prostorové uspořádání kanceláří neumožňuje důsledně oddělit klienty při jednání.

6.6.6 Odbor kanceláře starosty

Pracovnice na pozici vedoucí odboru a zapisovatelka používají notebooky s důvěrnými daty, které nemají implementovánu kryptografickou ochranu. Je potřeba ošetřit.

Jsou prováděna školení - vstupní školení, odborná školení, školení na ochranu informací, systematická školení na ochranu informací nikoli.

6.6.7 Odbor právní

Jsou používány 2 notebooky, které mohou být vynášeny mimo lokalitu. Velmi pozitivně je hodnocena služba odboru informatiky, rychlá reakce, výborné odborné znalosti. Podpora IS podle subjektivního názoru dostatečná. Možnost školení v oblasti ochrany informací je zajištěna.

6.6.8 Odbor sociálních věcí

Potřeba specificky nakládat s daty odboru na sdílených discích, zejména oddělení sociálně právní ochrany dětí.

6.6.9 Odbor správních agend

Školení pracovníků — postupně školeni, plán školení. Školení zpracovatelů na oblast ochrany informací cca 1x za 3 roky.

6.6.10 Odbor finanční

Ekonomický software ORSOFT: rámcově vyhovuje bez výrazných problémů, podpora ze strany dodavatele je hodnocena dobře, subjektivně dostatečná. Osobní údaje jsou zpracovávány ve velké míře s nedostatečnou globální znalostí povinností a účelu zpracování.

Povědomí o problematice ochrany osobních údajů je, školení systematicky neprobíhá. Nelze vyloučit, že brigádníci, stážisté mohou být zpracovateli osobních údajů - málo pravděpodobné.

6.6.11 Útvar interního auditu

Personálně řídí tajemník, organizačně patří pod starostu. Útvar zodpovídá za plnění standardů podle ISO 9001, ISO 14001.

Data office aplikací jsou ukládána na síťové sdílené disky (disk K). Doporučuji v tomto případě ukládání na lokální disky - potřeba specifické ochrany dat útvaru.

Je používán notebook, který se vynáší mimo pracoviště a může obsahovat důvěrná data, není kryptograficky zabezpečen. Doporučení – nainstalovat zabezpečení.

Není vedena evidence zpracování osobních údajů.

6.6.12 Vsetínská správní a investiční příspěvková organizace

Tato příspěvková organizace sídlí v lokalitě Hlavní budova bez uzavřené nájemní smlouvy a plně využívá infrastruktury MěÚ. K informacím MěÚ mají přístup výhradně zaměstnanci příspěvkové organizace (ne externisté). Přístupy k informacím MěÚ jsou zřizovány na základě požadavku na zřízení přístupu podepsaném ředitelem organizace a tajemníkem MěÚ. Organizace nemá vlastního informatika - připojení, nastavení počítačů do sítě a správu provádějí informatici MěÚ. Počítače a uživatelé jsou členy domény MěÚ. Z hlediska dostupnosti IS nejsou evidovány žádné problémy. Organizace je vybavena standardními počítači a 3 kusy notebooku, které neobsahují chráněné informace.

Hlavní činnost organizace je kryta příspěvkem, doplňková činnost - nájem bytů.

Využívané části IS MěÚ Vsetín:

- GIS – prohlížení,
- připojení k internetu, MS Outlook - groupware systém (stejná doména jako MěÚ),
- sdílení složek na sdílených discích - směrnice, materiály RM a ZM,
- přístup k evidenci nemovitého majetku vlastněného městem.

Jménem města provádí správu majetku města, účetní evidence majetku, smlouvy uzavírá město.

Organizace zpracovává vlastní účetnictví a nahlížení do IS příspěvkové organizace ze strany města není, pokud je potřeba, jsou připraveny podklady.

Povinnost proškolit zaměstnance, povědomí o ochraně osobních údajů je shodná s MěÚ.

6.7 Analýza obchodních dopadů

Business Impact Analysis - analýza obchodních dopadů, dále jen BIA. Jedná se o odhad nejvýznamnějších hrozeb, vzhledem k hodnotě klíčových aktiv. Byla provedena neformálně a přehledově jako vhodná metoda pro získání základních informací o požadavcích na dostupnost, důvěrnost, integritu IS.

Pro hodnocení byla použita následující hodnotová stupnice:

0: ztráta/ bez dopadu

1: ztráta/dopad na úrovni spotřebního materiálu v hodnotě do 10 tis. Kč

2: ztráta/dopad v hodnotě 10-100 tis. Kč

3: ztráta/dopad v hodnotě 100 -300 tis. Kč

4: ztráta/dopad v hodnotě 300 tis-1 mil. Kč

5: ztráta/dopad v hodnotě 1-3 mil. Kč

6: ztráta/dopad v hodnotě 3-10 mil. Kč

7: ztráta/dopad v hodnotě 10-30 mil. Kč

8: ztráta/dopad v hodnotě 30-100 mil. Kč

9: ztráta/dopad v hodnotě nad 100 mil. Kč

10: ztráta/dopad zničující

Dopady na 5. stupni byly identifikovány u následujících hrozeb:

IS SW Vita - Stavební úřad / Ztráta dostupnosti v trvání 1 týden

Dopady na 6. stupni byly identifikovány u následujících hrozeb

IS Radnice Vera (poplatky, pokladna) / Úplná ztráta dat

IS Orsoft / Prozrazení cizím subjektům

IS Radnice Vera (poplatky, pokladna) / Prozrazení cizím subjektům

Další zpracování osobních údajů, prozrazení cizím subjektům nebo obchodní dopady na 7. stupni nebyly identifikovány. Uvedené dopady generují požadavky nejen na příslušné uvedené komponenty, ale přiměřeným způsobem i na obecné, podpůrné komponenty.

6.7.1 Analýza obchodních dopadů - závěry

Hrozby vedoucí k dopadům na 7. a vyšších stupních, z definice nepřijatelné nebyly identifikovány. V případě jejich identifikace je nezbytné aplikací příslušných protiopatření snížit pravděpodobnost jejich výskytu v maximální možné míře.

Hrozby vedoucí k dopadům na 6., 5. stupni (a nižších) je potřebné aplikací vhodných protiopatření snižovat na přijatelnou úroveň. Tato úroveň je v principu dána porovnáním dopadů s cenou protiopatření.

Z realizované analýzy dopadů vyplývá, že zásadními hrozbami IS Města Vsetína jsou hrozby vedoucí ke ztrátě dat a zejména ztrátě důvěrnosti dat. Hrozby vedoucí ke ztrátě dostupnosti, zejména v řádech hodin, resp. dnů nemají zásadní dopad.

7 ANALÝZA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ DLE DEFINICE ZÁKONA Č. 101/2000 SB.

7.1 Zpracování osobních údajů v rámci MěÚ Vsetín

MěÚ Vsetín je správcem i zpracovatelem osobních údajů dle definice zákona č. 101/2000 Sb.:

- § 4 písm. j) správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,
- § 4 písm. k) zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.

Podle ustanovení § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, se zpracováním osobních údajů rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

Správce osobních údajů je podle ustanovení § 5 zákona č. 101/2000 Sb. povinen zejména:

a) stanovit účel, k němuž mají být osobní údaje zpracovány,
b) stanovit prostředky a způsob zpracování osobních údajů,
c) zpracovat pouze přesné osobní údaje,
d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,
e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování
f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny.

Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, nebo pokud k tomu dal subjekt údajů předem souhlas. [5]

V aktuálním stavu jsou základní povinnosti správce splněny, především pro (rozsahem, významem) závažnější zpracování osobních údajů, nicméně jsou identifikována zpracování, kde základní povinnosti splněny nejsou.

Jsou identifikována i taková zpracování, která zřejmě nespadají pod výjimku ze zákonného požadavku na získání souhlasu subjektu údajů dle § 5 odst. 2 zákona č. 101/2000 Sb., který uvádí, získání souhlasu subjektu údajů se zpracováním osobních údajů není nutný především:

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,

b) jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů.

Zákonný požadavek na oznámení zpracování (§ 16 zákona č. 101/2000 Sb.) je závislý především na účelu zpracování osobních údajů (zákonem požadovaná evidence x jiný účel).
Zákonný požadavek na získání souhlasu subjektu je závislý opět na účelu zpracování osobních údajů, není nutný především v případech dle § 5 odst. 2 zákona č. 101/2000 Sb.

V každém případě je nutno splnit požadavky:

- § 5 zákona č. 101/2000 Sb. - Práva a povinnosti při zpracování osobních údajů, správce je povinen:

a) stanovit účel, k němuž mají být osobní údaje zpracovány,

b) stanovit prostředky a způsob zpracování osobních údajů,

další povinnosti viz. písmena c) - h) § 5 zákona č.101/2000 Sb. a § 13 zákona „Povinnosti osob při zabezpečení osobních údajů."

7.2 Kamerový systém Městské policie

Městská policie Vsetín provozuje kamerový systém. Tento kamerový systém je provozován se záznamem a jedná se tedy o systém, který zpracovává osobní údaje. Účel zpracování byl

stanoven v souladu s platnou legislativou ČR. Posouzení rizik bylo provedeno neformálně. Dokumentace technicko-organizačních bezpečnostních opatření k zajištění ochrany osobních údajů je zpracována (Směrnice pro obsluhu a provoz kamerového systému). Přístup k záznamům je řízen psanými i nepsanými pravidly. Je specifikována povinnost likvidovat záznamová média, evidence záznamových médií není formalizována. Doba uchování záznamů je jeden týden.

7.2.1 Diskuse ke kamerovému systému

1. Provozování takovéhoto kamerového systému je v obecné rovině přípustné pokud:
   a) Nezasahuje nadměrně do soukromí.
   b) Je specifikován relevantní účel sledování.
   c) Je stanovena lhůta pro uchování záznamů (ve stanovisku ÚOOÚ č.1/2006 je explicitně uvedeno: *„Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Uchovávaná data by měla být uchovávána v rámci časové smyčky např. 24 hodin, pokud jde o trvale střežený objekt, nebo případné i dobu delší, v zásadě však nepřesahující několik dnů, nejde-li o pořizování záznamů policejním orgánem podle Zvláštního zákona, a po uplynutí této doby vymazána.„* [14]
   d) Je řádně zajištěna ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním - viz § 13 zákona č. 101/2000 Sb.
   e) Subjekt údajů je o užití kamerového systému vhodným způsobem informován (např. nápisem umístěným v monitorované místnosti), viz § 11 odst. 5 zákona č. 101/2000 Sb., nejde-li o uplatnění zvláštních práv a povinností vyplývajících ze zvláštního zákona.
   f) Jsou garantována další práva subjektu údajů, zejména právo na přístup ke zpracovávaným datům a právo na námitku proti jejich zpracování, viz § 1 zákona č. 101/2000 Sb.
   g) Zpracování osobních údajů je třeba registrovat u Úřadu pro ochranu osobních údajů, nejde-li o uplatnění zvláštního práva či povinností

vyplývajících ze zvláštního zákona, viz § 18 odst. 1 písm. b) zákona č. 101/2000 Sb.

7.2.2 Kamerový systém - závěry

Městská policie Vsetín (Město Vsetín) jako provozovatel kamerového systému je správcem a zpracovatelem osobních údajů dle definice zákona č. 101/2000 Sb.

Je nutno splnit následující požadavky:

- § 5 zákona č. 101/2000 Sb. - Práva a povinnosti při zpracování osobních údajů, správce je povinen:
  - stanovit účel, k němuž mají být osobní údaje zpracovány,
  - stanovit prostředky a způsob zpracování osobních údajů,
- § 13 zákona č. 101/2000 Sb. „Povinnosti osob při zabezpečení osobních údajů".

Z uvedených požadavků jsou formálně splněny požadavky dle bodů a) a b) (viz. Směrnice pro obsluhu a provoz kamerového systému).

Požadavky § 13 zákona č. 101/2000 Sb. jsou splněny rámcově, v některých případech není možné jejich splnění prokázat. Doporučuji především:

- Provedení formální analýzy rizik (viz § 13 odst 3 zákona č. 101/2000 Sb.),
- Doplnění stávající dokumentace technicko-organizačních opatření k zajištění ochrany osobních údajů: Zejména ošetřit oblast evidence záznamových médií.

8 ZABEZPEČENÍ LOKALIT

Lokalitou je pro účely této analýzy rozuměno fyzické aktivum - prostory, jejichž účelem je umístění aktiv a jejíž hodnotu tvoří aktiva v ní umístěná. Fyzickou bezpečnost tvoří systém opatření, jejichž cílem je předcházet neautorizovanému přístupu, poškození, znehodnocení a zničení aktiv města v prostorách, ve kterých se nacházejí.

V rámci vstupní analýzy byly diskutovány lokality důležité z hlediska zpracování informací. Jedná se zejména o běžné kancelářské prostory a specifické lokality typu serverovna, spisovna, archív apod.

Posouzení úrovně zabezpečení je závislé zejména na charakteru aktiv umístěných v dané lokalitě:

- Běžné kancelářské prostory: prostory kde jsou ukládány operativně písemnosti charakteru zpracování osobních údajů.
- Režimová pracoviště.
- Pracoviště krizového řízení (Odbor životního prostředí): Prostory a trezor vhodný pro ukládání utajovaných informací do stupně „V". Certifikováno NBÚ.
- Serverovny: Technologické lokality pro provoz infrastruktury informačních systémů zpracovávajících hodnotné informace, mj. charakteru zpracování osobních údajů
- Spisovny: Lokality pro ukládání písemností charakteru zpracování osobních údajů.

V případě pracoviště krizového řízení vyplývá míra zabezpečení lokality přímo z charakteru informací, pro jejichž zpracování je prostor zabezpečen. Ve všech dalších případech by měla být opatření fyzické bezpečnosti navržena tak aby byla přiměřená charakteru zpracovávaných/uchovávaných informací. Tedy v principu by měla vycházet z posouzení rizik.

Stávající řešení fyzické bezpečnosti lokalit rámcově vychází z posouzení rizik, nicméně nejedná se o posouzení rizik systematické a formální. Takto je reálně zavedeno několik typů režimů lokalit bez explicitního důvodu v odlišných požadavcích na bezpečnost nebo odlišnostech prostředí.

8.1 Doporučení k zabezpečení lokalit

Návrh řešení zabezpečení lokalit by měl být v návaznosti na evidenci a stanovení hodnot aktiv v jednotlivých lokalitách v následujících oblastech:

- Kontroly vstupu osob
  - Způsob identifikace
  - Vstup zaměstnanců
  - Vstup dalších osob
- Režim práce v bezpečnostních zónách
  - Režim práce zaměstnanců
  - Režim provádění úklidových prací
- Bezpečnost aktiv
  - Objektová bezpečnost
  - Bezpečnost vstupních dveří
  - Umístění aktiv
  - Ochrana proti nebezpečí požáru
  - Ochrana proti dalším fyzickým nebezpečím
  - Dodávky energie

Z hlediska hodnoty aktiv a účelu jednotlivých lokalit navrhuji rozdělení do pěti kategorií:

1. Prostory pro veřejnost
2. Běžný kancelářský prostor
3. Režimové pracoviště - bezpečnostní zóna C (spisovna)
4. Režimové pracoviště - bezpečnostní zóna B (archiv, serverovna, ...)
5. Režimové pracoviště - bezpečnostní zóna A (prostory pro ukládání utajovaných informací klasifikovaných „V")

9 HROZBY, STÁVAJÍCÍ PROTIOPATŘENÍ, NÁVRH PROTIOPATŘENÍ

Uvádím hrozby, které byly identifikovány neformálně, v rámci obecných konzultací. Hrozby jsou uvedeny především jako zdůvodnění návrhů a doporučení pro další postup v oblasti řízení informační bezpečnosti. Uvedené hrozby jsou seřazeny dle stupně obecnosti od obecných po konkrétní. Podrobný seznam hrozeb a četnost jejich výskytu je uveden v příloze číslo 3 – Hrozby.

9.1 Procedurální bezpečnost

V aktuálním stavu je oblast bezpečnosti informací, ale i další oblasti (jakost, vztah k životnímu prostředí) procesně řízena.

9.1.1 Bezpečnost informací

Jak vyplývá ze struktury a obsahu dokumentů interní legislativy je posuzovaná oblast řízení bezpečnosti informací řešena dle relevantních technických standardů, zejména ČSN ISO/IEC 17799 (viz směrnice QS 42-03 Provozování IS, používání počítačových programů a ostatních prostředků ICT). Takovýto stav je z hlediska aktuálních, obecně přijímaných standardů uspokojivý. Diskuse potřeby zavedení procesního přístupu k řízení bezpečnosti je nad rámec tohoto projektu. Nicméně lze konstatovat:

- Z charakteru činnosti společnosti Město Vsetín vyplývají zvýšené požadavky na oblast bezpečnosti.
- Zavedení procesního přístupu k řízení oblasti informační bezpečnosti není výslovně požadováno žádným závazným právním předpisem. Nicméně povinnosti provozovatele IS se týkají mnoha oblastí (procedurální, administrativní, technické) a optimálním a efektivním řešením je akceptace obvyklých standardů pro tuto oblast.
- Zavedení procesního přístupu k řízení bezpečnosti pokrývá závažné hrozby v oblastech:
    - obecná odpovědnost provozovatele,
    - efektivita investic do bezpečnostních opaření, včetně opatření k zajištění dostupnosti.

Z posouzení stavu implementace procesů řízení bezpečnosti informací vyplývá, že ne všechny procesy jsou reálně zavedeny, resp. provozovány. Takovýto závěr vyplývá z posouzení reálného stavu zavedení systému na jednotlivých odborech. A dále ze skutečnosti, že některé oblasti systému řízení bezpečnosti informací jsou neaktuální, resp. nefunkční. Např. není zcela naplněn soulad s požadavky (odkazy na neplatnou legislativu v dokumentech), neprobíhá důsledně klasifikace a kontrola aktiv.

9.1.2 Bezpečnost informací - doporučení

S ohledem k vývoji v oblasti standardizace systémů managementu bezpečnosti informací doporučuji jako základ pro návrh/implementaci/provoz aktuální standardy z oblasti managementu bezpečnosti informací souhrnně označované jako Systém managementu informační bezpečnosti (ISMS). Podstatným přínosem je jednoznačně procesní přístup k managementu informační bezpečnosti, zahrnující i aspekt periodické aktualizace a zlepšování ISMS.

Pokračovat v managementu informační bezpečnosti dle uvedených standardů. Akceptovat nutnost procesního přístupu k managementu informační bezpečnosti.

Na základě těchto skutečností byla vypracována, následně v připomínkovém řízení projednána a posléze schválena směrnice QS 42-06 Bezpečnost informací, která je samostatnou přílohou této práce (příloha P IV: Směrnice - QS 42-06 Bezpečnost informací).

Stávající ISMS zpřehlednit a zjednodušit:

a) vypracovat, přijmout a prosazovat Politiku bezpečnosti informací,
b) dopracovat systém interní legislativy ve vztahu k informační bezpečnosti. Aktualizovat stávající směrnice tak aby byly stručné, přehledné a adresné, například ve struktuře:
    - Směrnice pro uživatele VT,
    - Směrnice pro řízení přístupů k IS,
    - Směrnice pro provoz ICT.

Zvyšovat povědomí o bezpečnosti, provádět školení zaměstnanců i managementu.

9.1.3 Ochrana osobních údajů

Hrozby spojené se ztrátou důvěrnosti jsou hodnoceny jako závažné hrozby. Jedním z důvodů je i skutečnost, že mnohá zpracovávaná data mají charakter osobních údajů dle definice zákona č. 101/2000 Sb.

Ke dnešnímu dni je již nově přijata samostatná směrnice pro ochranu osobních údajů. Ovšem povědomí o povinnostech vyplývajících ze zákona č. 101/2000 Sb., o ochraně osobních údajů není zcela uspokojivé.

Stávající outsourcingové smlouvy neřeší korektně oblast ochrany informací třetích stran. Nejsou systematicky přenášeny povinnosti zpracovatele osobních údajů na smluvní dodavatele (např. Vsetínskou správní a investiční p.o.).

Stávající řešení řízení přístupů k IS pro zpracování osobní údajů může ve výjimečných případech způsobit porušení požadavků § 13 odst. 4 zákona č. 101/2000 Sb., viz směrnice QS 42-03, čl. 5.7.2.1).

9.1.4 Ochrana osobních údajů - doporučení

Seznámit zaměstnance se Směrnicí pro ochranu osobních údajů a důsledně kontrolovat její dodržování. Provést formální analýzu rizik jako řešení požadavku § 13 odst. 3 zákona č.101/2000 Sb.

9.1.5 Kontinuita činností

Podstatné komponenty se nevyznačují striktními požadavky na dostupnost služby. Nicméně pro případ závažnějších událostí (např. požár serverovny) není k dispozici relevantní dokumentace, která by umožnila řešit poruchy/havárie procesně.

Je nutno požadavky a řešení systematizovat. Nejlépe vypracováním plánu řízení kontinuity činností na základě provedení formální Analýzy rizik.

9.1.6 Kontinuita činností - doporučení

Vytvořit relevantní technickou dokumentaci IS (infrastruktura i vlastní IS). Vypracovat a podle možností otestovat plán řízení kontinuity činností. Dořešit systematicky tzv. dobu opravy se smluvními partnery, jejichž služby směřují k zajištění (obnově) dostupnosti oprávněným uživatelům IS.

9.2 Technické hrozby

V rámci vstupní analýzy stavu informační bezpečnosti není dostatečný prostor na podrobné prověření všech aspektů návrhu, realizace a provozu ICT infrastruktury.
V rámci prováděné analýzy byly identifikovány některé nedostatky, nicméně doporučuji především ty části infrastruktury, které přímým způsobem podmiňují bezpečnost IS MěÚ Vsetín prověřit podrobněji (technické prověření, penetrační test apod.). Týká se především oblasti poskytování síťových služeb, perimetru připojení do Internetu.

9.2.1 Navržená opatření

V rámci procesních opatření vypracovat relevantní bezpečnostní politiku LAN/WAN a realizovat poskytování síťových služeb dle této politiky, vypracovat relevantní dokumentaci infrastruktury ICT.
Technická opatření: provést technické prověření technické infrastruktury (dokumentovaný stav v porovnání s reálným stavem, případně penetrační testování). Realizovat protiopatření dle doporučení závěrů analýzy rizik a technického prověření. DHCP: Omezit přidělování IP adres neznámým zařízením v lokální síti. Přidělovat IP adresy dynamicky na základě vynucené vazby mezi MAC a IP adresou. V návaznosti na úpravu dotčených IS zjednodušit směrování (routing) v interní síti.

Doporučuji provést technické prověření infrastruktury:

a. Perimetr sítě.
b. Přehledově LAN/WAN.
c. Přehledově síťové servery.
d. Namátkově pracovní stanice uživatelů.

Provést penetrační test:

- Externí nekooperativní - prověření perimetru sítě vůči útokům z Internetu.
- Interní kooperativní — odhalení slabin v zabezpečení komponent IS.

10 ZÁLOHOVÁNÍ DAT

Hrozby v oblasti ztráty dat jsou hodnoceny jako velmi závažné. Oblast zálohování dat je řešena relativně uspokojivě. Především v oblasti zálohování dat podstatných komponent IS. Jsou vytvářeny nezávislé zálohy, ale zálohovací politika neřeší všechny potřebné procesní aspekty (vývoz záloh, životní cyklus záložního média, evidence médií, likvidace médií).

Doporučení:

Aktualizovat, schválit a prosadit korektní zálohovací politiku, zahrnující mj. oblasti vytváření nezávislých záloh, vývoz záložních médií, životní cyklus záložního média, specifikaci zodpovědnosti apod.

10.1 Bezpečnost uložení hodnotných (důvěrných/citlivých) dat

Aktuální interní legislativa neřeší, resp. neřeší formálně závazně nakládání s hodnotnými daty, resp. tuto oblast ponechává na uvážení/odhadu vlastníka, či uživatele. Vlastní úsudek však i v dobré víře nemusí odpovídat elementárním požadavkům na bezpečnosti.

Není důsledně řešena problematika uložení důvěrných/citlivých dat na souborových serverech. Není řešena problematika uložení důvěrných/citlivých dat na přenosných počítačích.

Doporučení:

1. Dořešit oblast ukládání hodnotných (např. osobních, citlivých) dat na lokálních počítačích a souborových serverech, tak aby bylo dosaženo minimálně stejné míry zabezpečení těchto dat v elektronické podobě jako v podobě listinné.
2. Technickými a organizačními opatřeními zajistit a prosadit ukládání hodnotných, osobních dat v souborovém systému nebo databázi náležitě zabezpečených serverů, kde je možné přístup k nim podmíněný řádnou autentizací řídit a zaznamenávat a data chránit před ztrátou. Zajistit prokazatelnou informovanost uživatelů o nutnosti a důležitosti ochrany hodnotných, osobních dat. Provést kontroly pracovních stanic zda na nich nejsou uložena zbytková osobní, resp. citlivá data. Povinnost ukládat osobní, resp. citlivá data na zabezpečené úložiště popsat a zavést jako standard pro práci organizace.

3. Dořešit oblast použití přenosných počítačů ve smyslu vymezení oblasti použití a vynucení vhodných/dostatečných technických opatření (např. kryptografická ochrana dat uložených na přenosných počítačích).

10.2 Ochrana autentizačních informací

Tato oblast nebyla systematicky prověřena, nicméně s ohledem k nedostatečnému ošetření této oblasti v interní legislativě lze předpokládat neuspokojivý stav nakládání s autentizačními informacemi.

Doporučení:

Zavést a prosadit jednoznačná pravidla pro nakládání s citlivými autentizačními informacemi. Zvyšovat povědomí o bezpečnosti. Osobní certifikáty ukládat výhradně tak, aby bylo možno zabezpečit vlastníku certifikátu jednoznačnou kontrolu nad přístupem k privátnímu klíči certifikátu. Nejlépe uložením certifikátu na tokenu, čipové kartě apod.

11 POSOUZENÍ SHODY S POŽADAVKY STANDARDU ČSN ISO/IEC 27001

V této části jsou popsány cíle jednotlivých opatření dle standardu ČSN ISO/IEC 27001, zjištění a hodnocení funkčnosti stávajícího stavu těchto opatření v rámci MěÚ Vsetín a doporučení, která by měla být aplikována v dalších fázích procesu zavádění systému řízení bezpečnosti informací.

Tab. 9. Posouzení shody opatření s ČSN ISO/IEC 27001

Opatření (skupina opatření)	**Hodnocení (%)** *Dle dokumentace*	**Hodnocení (%)** *Zavedeno reálně*
A5 Bezpečnostní politika	100	75
A6 Organizace bezpečnosti informací	100	50
A7 Řízení aktiv	100	50
A8 Bezpečnost lidských zdrojů	100	50
A9 Fyzická bezpečnost a bezpečnost prostředí	100	75
A10 Řízení komunikací a řízení provozu	100	50
A11 Řízení přístupu	100	75
A12 Akvizice, vývoj a údržba informačních systémů	100	-
A13 Zvládání bezpečnostních incidentů	100	50
A14 Řízení kontinuity činností organizace	100	25
A15 Soulad s požadavky	100	30
Míra shody (%)	**100**	**53**

11.1 Bezpečnostní politika

Cíl: určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organizace, příslušnými zákony a směrnicemi.

Zjištění: Je vypracována směrnice „Ochrana informací" která má charakter bezpečnostní politiky v oblasti ochrany informací. Není prokazatelné, že je tato směrnice do důsledků prosazována a realizována.

Doporučení: Dokument bezpečnostní politiky je stěžejním dokumentem v rámci zavádění systému řízení bezpečnosti informací. Vytvořenou bezpečnostní politiku je potřeba udržovat a pravidelně aktualizovat na základě výsledku periodických bezpečnostních revizí. Dále je nutné bezpečnostní politiku velmi důsledně prosazovat (vypracovat poučení

pro uživatele, opakovaně školit a dalšími prostředky zvyšovat úroveň povědomí zaměstnanců o bezpečnosti informací, kontrolovat dodržování předpisů a využívat kárná opatření).

Hodnocení (0-100): 75

11.2 Organizace bezpečnosti informací

Cíl: řídit bezpečnost informací ve společnosti zřízením bezpečnostního fóra vedeného managementem společnosti, které by schvalovalo politiku bezpečnosti, definovalo odpovědnosti v oblasti bezpečnosti informací a koordinovalo implementaci bezpečnosti. Zároveň zachovávat bezpečnost zařízení pro zpracování informací a bezpečnost informačních aktiv, které jsou přístupné třetím stranám a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na jinou organizaci (outsourcing).

Zjištění: Město Vsetín má zřízeno bezpečnostní fórum (Fórum pro řízení bezpečnosti informací), není však jednoznačně definovaná osoba zodpovědná za bezpečnost informací v organizaci. Během prováděné analýzy bylo zjištěno, že některé uzavřené obchodní, respektive smluvní vztahy mezi společností Město Vsetín a jejími obchodními partnery nezohledňují dostatečné problematiku bezpečnosti informací nebo ji vůbec neřeší (například vztahy se Vsetínskou správní a investiční příspěvkovou organizací).

Doporučení: Doporučuji jednoznačně definovat odpovědnosti v oblasti bezpečnosti informací. Dále zhodnotit rizika, která vyplývají z přístupu třetích stran a zavést potřebná bezpečnostní opatření a požadavky, které budou zohledněny ve smlouvách s daným partnerem.

Hodnocení (0-100): 50

11.3 Řízení aktiv

Cíl: Nastavit a udržovat přiměřenou ochranu aktiv organizace. Udržovat přiměřenou ochranu aktiv společnosti prostřednictvím přesné evidence.

Zjištění: Evidence informačních aktiv je dle platných směrnic zavedena ne však důsledně (řešení dle směrnic: QS 42-07 Ochrana informací a QS 42-03 Provozování ICT)

Doporučení: Pro každé jednotlivé aktivum by měl být definovaný vlastník aktiva, který bude za dané aktivum zodpovědný. Aktiva by měla být ohodnocena dle důležitosti, kterou

pro organizaci má (aby mohla být přijata relevantní bezpečnostní opatření), Zároveň by u každého aktiva mělo být uvedeno jeho současné umístění - tento proces je součástí Analýzy rizik. Podobně je potřeba také identifikovat a roztřídit všechna informační aktiva (například smlouvy s klienty, dodavateli, nabídky, projektová dokumentace, účetní data apod.) dle stupně jejich potřebnosti, důležitosti a ochrany. Případně vytvořením směrnice pro klasifikaci informací zavést pravidla, jak informace třídit, značit, uchovávat a likvidovat.

Hodnocení (0-100): 50

11.4 Bezpečnost lidských zdrojů

Cíl: Snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace. Zajistit, aby si zaměstnanci (případně dodavatelé, třetí strany) byli vědomi bezpečnostních hrozeb a problému s nimi spjatých a byli připraveni se podílet na dodržování bezpečnostní politiky v průběhu své běžné práce.

Zjištění: Společnost má vypracovánu formální bezpečnostní politiku, role a odpovědnosti v oblasti bezpečnosti informací jsou formálně popsány. Zaměstnanci jsou částečně proškolováni nadřízenými pracovníky i v oblasti bezpečnosti informací, přesný rozsah a zaměření školení však není formálně upraveno. Jsou definována pravidla pro předávání informací o nově příchozích či odcházejících zaměstnancích mezi oddělením informatiky a personálním oddělením. Formálně jsou popsána pravidla pro uživatele ICT (například pravidla pro používání e-mailu, Internetu). Tato pravidla nejsou v některých ohledech dostatečná.

Doporučení: Revidovat bezpečnostní politiku (resp. příslušné směrnice) a redefinovat role a odpovědnosti v oblasti bezpečnosti informací. Zároveň doporučuji revidovat formálně popsaná pravidla, která uživatelé IT systému mají dodržovat (např. pravidla pro používání emailu, Internetu apod.). Noví zaměstnanci by měli absolvovat školení zaměřené na bezpečnost informací (prováděné kompetentní osobou - bezpečnostním manažerem) v předem připraveném a schváleném rozsahu. Doporučuji zavést formální proces disciplinárního řízení a definovat sankce, které pro zaměstnance vyplývají z porušení bezpečnostních ustanovení.

Hodnocení (0-100): 50

11.5 Fyzická bezpečnost a bezpečnost prostředí

Cíl: Zamezit neoprávněnému přístupu do vymezených oblastí a tím předcházet ztrátě, poškození nebo zcizení informací a prostředků pro zpracování informací.

Zjištění: Všechny stěžejní servery společnosti jsou umístěny v serverovnách. Centrální serverovna je režimové pracoviště s nedokonale zavedeným a formalizovaným režimem. EZS zavedeno, EPS nikoli. Proti náhlému výpadku elektrického proudu je k dispozici UPS zařízení. Serverovna je vybavena klimatizací. Přístupy do budov jsou volné. Spisovny jsou realizovány jako režimová pracoviště s nedokonale zavedeným a formalizovaným režimem. Archívy jsou dle informací zadavatele realizovány dle relevantní legislativy.

Prvky komunikační infrastruktury jsou uloženy v uzamčených rozvaděčích. Pro bezpečné zničení nebo opakované použití zařízení neexistují v rámci odboru IT formálně zavedené postupy.

Údržba zařízení neprobíhá důsledně na pravidelné bázi, spíše probíhá následně po výskytu poruchy.

Doporučení: Provést analýzu rizik s cílem získat správné informace o hodnotě uchovávaných aktiv a potenciální míře rizika a zavést odpovídající bezpečnostní opatření. Již nyní však vyplývají možná doporučení spočívající v definování zásad fyzické bezpečnosti.

Hodnocení (0-100): 75

11.6 Řízení komunikací a řízení provozu

Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracovávání informací, minimalizovat riziko selhání systému. Předcházet ztrátě, modifikaci nebo zneužití informací, prostřednictvím monitoringu detekovat neoprávněné aktivity.

Zjištění: Provozní postupy jsou zdokumentovány pouze z části, některé existují jen jako know-how správců ICT. Postupy změnového řízení nejsou zavedeny, nové systémy či nové verze již existujících systému nejsou formálně akceptovány. Plánování kapacit (volné místo na discích, výkon procesoru, zatížení sítě apod.) neprobíhá formálně, neexistuje žádná směrnice, která by tento proces upravovala. Město Vsetín využívá pravidelně aktualizovaný antivirový software. Operátorské deníky nejsou důsledně vedeny. Systém

umožňuje pořizování auditních záznamu, obsahující chybová hlášení a jiné bezpečnostně významné události, tyto záznamy však nejsou pravidelně procházeny a nejsou archivovány. Společnost provádí pravidelné zálohy, ale testování záloh (zda je možné ze záloh data obnovit) se provádí nepravidelně, spíše namátkově. Pro zachování bezpečnosti při likvidaci médii neexistují zavedené formální postupy (skartace, fyzické zničení). Neexistuje směrnice, která by tuto oblast systémově upravovala. Zároveň neexistuje žádná směrnice, která by definovala bezpečnostní požadavky při manipulaci s vyměnitelnými médii, požadavky na bezpečnost médií při přepravě či při výměně informací mezi organizacemi. Pravidelné vyhodnocování kvality služeb dodávaných třetími stranami neprobíhá. Třetím stranám přístupné systémy nejsou z hlediska řízení přístupů formálně a systematicky řešeny (např. přístupy Vsetínské správní a investiční, p.o.).

Doporučení: Zformalizovat všechny postupy a procedury týkající se řízení komunikací a řízení provozu. Zavést pravidelné činnosti týkající se procházení a vyhodnocování auditních záznamu (logu), plánování kapacit, vedení operátorských deníku, testování prováděných záloh, vyhodnocování kvality služeb poskytovaných třetími stranami.

Zálohovací média by měla být uložena s dostatečnou mírou bezpečnosti (dostupnosti, důvěrnosti). Dále doporučuji vytvořit (v souladu s celkovou bezpečnostní politikou organizace) směrnici definující bezpečnostní pravidla pro zacházení s médii (likvidace, přeprava médií) a pro výměnu informací mezi organizacemi.

Hodnocení (0-100): 50

11.7 Řízení přístupu

Cíl: Řídit přístup k informacím, předcházet neoprávněnému přístupu k operacím, systémům, počítačům, sítím, informačním systémům. Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití prostředků pro práci na dálku.

Zjištění: Řízení přístupů je zavedeno. Pravidelná revize přístupových oprávnění není prováděna. Není definována politika zachování bezpečnosti při práci na mobilních zařízeních. Někteří uživatele používají ke své práci notebooky, které obsahují hodnotná data. Tato data nejsou adekvátním způsobem zabezpečena (např. použitím šifrování dat). Obecné zásady prázdného stolu nejsou formálně zavedeny. Zásady prázdné obrazovky monitoru (automatické zamknutí obrazovky po 5-10 minutách nečinnosti) nejsou formálně

zavedeny. Existuje psaná politika hesel, požadované parametry, které by hesla měla splňovat, jsou uživatelům formálně sděleny. Řešení řízení přístupů k IS pro zpracování osobní údajů může ve výjimečných případech způsobit porušení požadavků § 13 odst. 4 zákona č. 101/2000 Sb., viz směrnice QS 42 - 03, čl. 5.7.2.1)

Doporučení: Zavést pravidla pro práci na mobilních zařízeních. Revidovat systém řízení přístupů.

Hodnocení (0-100): 75

11.8 Akvizice, vývoj a údržba informačních systémů

Cíl: Zajistit implementaci bezpečnosti do informačních systémů a ochránit tak důvěrnost, dostupnost a integritu informací.

Zjištění: Ve společnosti není prováděn vývoj aplikací - součástí posuzovaného informačního systému. Tato oblast nebyla v rámci této analýzy posuzována.

Doporučení: -

Hodnocení (0-100): -

11.9 Zvládání bezpečnostních incidentů

Cíl: Minimalizovat škody způsobené bezpečnostními incidenty a selháními, a sledovat je a učit se z nich.

Zjištění: Pro MěÚ Vsetín je vytvořen formální systém zvládání bezpečnostních incidentů (Kniha bezpečnostních incidentů, kniha bezpečnostních slabin).

Systém není reálně provozován, resp. není zaveden jako běžná součást provozu ICT. Vyhodnocování incidentů probíhá formálně. Systémové logy nejsou systematicky procházeny. V QMS jsou zavedena nápravná opatřená týkající se procesu řízení jakosti.

Doporučení: Revidovat a reálně provozovat systém zvládání bezpečnostních incidentů. Zároveň doporučuji pravidelně vyhodnocovat bezpečnostní incidenty a systémové logy a dostatečné dlouhou dobu je archivovat pro potřeby důkazního řízení.

Hodnocení (0-100): 50

11.10 Řízení kontinuity činností organizace

Cíl: Organizačně a technicky zajistit obnovu kritických procesu organizace v případě většího selhání nebo havárie, včetně rámcového zhodnocení dopadu při přerušení činnosti podniku. Jedná se zde především o otázky zálohování dat, reakce na zcizení prostředků VT, živelné katastrofy, výpadku elektrického napájení apod.

Zjištění: Není definována odpovědnost za kontinuitu činností, neexistuje ani rámcový havarijní plán. Testy záloh probíhají náhodně, není to pravidelný proces.

Doporučení: Na základě zpracované analýzy rizik vytipovat kritické procesy a pro tyto zpracovat plány obnovy (pro případy havárie, zcizení, živelné katastrofy, apod.), které by mely být pravidelně aktualizovány a testovány. Doporučuji provádět pravidelné testy obnovy dat ze záloh a tento proces řádně dokumentovat.

Hodnocení (0-100): 25

11.11 Soulad s požadavky

Cíl: Zajistit soulad všech postupu, oblastí a systému s definovanými bezpečnostními politikami a směrnicemi. Zároveň se vyvarovat porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavku. Tento soulad by měl být předmětem pravidelné revize (interního nebo externího auditu) a provádět by jej měly pouze osoby s odpovídající kvalifikací.

Zjištění: Společnost nemá vypracovánu bezpečnostní politiku, ovšem v rámci této práce je vypracována, schválena a uvedena do praxe směrnice QS 42-06 Bezpečnost informací, o které se dá konstatovat, že má charakter bezpečnostní politiky (viz. Příloha P IV: Směrnice QS 42-06 Bezpečnost informací). K pravidelnému auditu souladu s výše uvedenými požadavky (např. Zákonem číslo 101/2000Sb., o ochraně osobních údajů, Zákonem číslo 121/2000 Sb., o právu autorském apod.) nedochází.

Doporučení: Vyškolit zaměstnance na pozici interního auditora IS/IT, případně využít služeb externího auditora a provádět pravidelný audit IS/IT a kontroly shody s legislativními požadavky, bezpečnostní politikou a navazujícími směrnicemi a normami.

Hodnocení (0-100): 30

ZÁVĚR

Tato práce shrnuje analytické informace zjištěné při konzultacích a předkládá základní návrhy a doporučení pro další postup v oblasti bezpečnosti informací, respektive budování systému managementu informační bezpečnosti (ISMS). Na základě zjištěných informací byla zpracována analýza rizik. Jako procesní protiopatření, ke zjištěným nedostatkům byly vypracovány a následně schváleny základní části systémové bezpečnostní politiky informací, směrnice QS 42-06 Bezpečnost informací a QS 42-07 Ochrana osobních údajů. Dále byly identifikovány hrozby a definovány doporučení ke zlepšení.

V rámci posouzení shody s požadavky standardu ČSN ISO/IEC 27001, byly prověřeny činnosti organizace s konstatováním, že míra shody je na průměrné úrovni. Práce navrhuje opatření, jejichž implementací se zvýší úroveň shody.

Je nutné nadále pokračovat v započatém trendu a věnovat pozornost následujícím okruhům opatření. Pokračovat v procesu managementu bezpečnosti informací, dle obecně přijímaných standardů v přiměřeném rozsahu. Vypracovat základní dokument systémové bezpečnostní politiky informací, provést revizi směrnice QS 42-03 Provozování IS, používání počítačových programů a ostatních prostředků ICT. Provádět školení uživatelů, zaměřené na zvyšování povědomí o ochraně informací, včetně zahrnutí problematiky hrozeb v souvislosti se sociálním inženýrstvím.

V oblasti ochrany osobních údajů jsou základní povinnosti správce splněny, především pro (rozsahem, významem) závažnější zpracování osobních údajů, ovšem je potřeba více úsilí zaměřit na splnění požadavků zákona 101/2000 Sb. o ochraně osobních údajů a důsledně prosazovat zodpovědnost za provozování IS a dalších technologií.

Cílem práce bylo provedení vstupní analýzy rizik a obchodních dopadů, provedení analýzy zpracování osobních údajů a vytvoření směrnic řešících bezpečnost informací. Dále byly navrženy opatření ke zlepšení zabezpečení lokalit, zálohování dat, bezpečnosti uložených dat a ochrany autentizačních opatření.

Všech vytčených cílů bylo dosaženo.

CONCLUSION

This paper summarizes the analytical information gathered during consultation and offers basic suggestions and recommendations for further action in the field of information security, respectively, building management systems Information Security (ISMS). Based on the information has been prepared a risk analysis. As a procedural countermeasures, the identified deficiencies have been developed and subsequently approved the basic system of information security policies, directives 1942-1906 QS QS Information Security and Privacy 42-07. Further threats were identified and defined recommendations for improvement.

In conformity with the requirements of standard ISO / IEC 27001, have been examined by the organization, noting that the correspondence is at an average level. Labour proposes measures whose implementation will increase the level of compliance.

It is necessary to continue to continue that trend and pay attention to the following action lines. Continue the process of information security management, according to generally accepted standards within a reasonable range. Develop a basic document system security policy information, a revision of QS 42-03 IS Operation, computer programs and other means of ICT. Conduct user training, aimed at raising awareness on the protection of information, including the incorporation of the threats in the context of social engineering. In the field of protection of personal data are fundamental obligations of the controller are met, especially for (range, meaning) serious processing of personal data, but more effort is needed to focus on compliance with Act No. 101/2000 Coll. Privacy and consistently enforce accountability for the operation of the IS and other technologies.

The aim was to perform the risk analysis and business impact analysis of processing of personal data and the creation of guidelines dealing with information security. Further measures were designed to improve the security of sites, data backup, security and protection of stored data authentication measures. All such objectives have been achieved.

This paper summarizes the analytical information gathered during consultation and offers basic suggestions and recommendations for further action in the field of information security, respectively, building management systems Information Security (ISMS). Based on the information has been prepared a risk analysis. As a procedural countermeasures, the identified deficiencies have been developed and subsequently approved the basic system of information security policies, directives 1942-1906 QS QS Information Security and

Privacy 42-07. Further threats were identified and defined recommendations for improvement.

In conformity with the requirements of standard ISO / IEC 27001, have been examined by the organization, noting that the correspondence is at an average level. Labour proposes measures whose implementation will increase the level of compliance.

It is necessary to continue to continue that trend and pay attention to the following action lines. Continue the process of information security management, according to generally accepted standards within a reasonable range. Develop a basic document system security policy information, a revision of QS 42-03 IS Operation, computer programs and other means of ICT. Conduct user training, aimed at raising awareness on the protection of information, including the incorporation of the threats in the context of social engineering.

In the field of protection of personal data are fundamental obligations of the controller are met, especially for (range, meaning) serious processing of personal data, but more effort is needed to focus on compliance with Act No. 101/2000 Coll. Privacy and consistently enforce accountability for the operation of the IS and other technologies.

The aim was to perform the risk analysis and business impact analysis of processing of personal data and the creation of guidelines dealing with information security. Further measures were designed to improve the security of sites, data backup, security and protection of stored data authentication measures.

All such objectives have been achieved

SEZNAM POUŽITÉ LITERATURY

[1] FRYŠAR, M. a kolektiv. Bezpečnost pro manažery, podnikatele a politiky. 1. vydání. Praha: Public History Praha, 2008. 176 s. ISBN 80-86445-22-4.

[2] DOUCEK, P., NOVÁK, L., SVATÁ, V., Řízení bezpečnosti informací. 1. vydání. Praha: Professional publishings, 2008. 240s. ISBN 978-80-86946-88-7.

[3] HÖNIGOVÁ, A., MATYÁŠ, V., Anglicko–česká terminologie bezpečnosti informačních technologií. 1.vyd. Praha:Computer Press, 1996, ISBN 80-85896-44-3.

[4] ŘEPA, V., Podnikové procesy – Procesní řízení a modelování. 2. vydání. Praha: Grada, 2007. 281 s. ISBN 978-80-247-2252-8.

[5] Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, navazující vyhlášky.

[6] Zákon č. 365/2000 Sb. o informačních systémech veřejné správy, navazující vyhlášky.

[7] Zákon č. 128/2000 Sb., o obcích (obecním zřízení).

[8] ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - systémy managementu bezpečnosti informací - Požadavky.

[9] ČSN ISO/IEC 17799:2006 „Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací".

[10] Data security management 1/2009 – Bezpečnostní politiky v praxi

[11] Směrnice QS 55 – 01 Organizační řád MěÚ Vsetín (vnitřní směrnice MěÚ Vsetín).

[12] Směrnice QS 42 – 03 Provozování IS, používání počítačových programů a ostatních prostředků ICT (vnitřní směrnice MěÚ Vsetín).

[13] Firemní materiály společnosti Pro IT, a.s. (www.proit.cz, www.ranit.cz)

[14] Internetové stránky Úřadu pro ochranu osobních údajů (www.uoou.cz)

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIA	Business Impact Analysis (Analýza obchodních dopadů)
DHCP	Dynamic Host Configuration Protocol
GIS	Geografický informační systém
HW	Hardware
ICT	Informační a komunikační technologie
IP	Internet protokol
IS	Informační systém
ISMS	Systému managementu informační bezpečnosti
ISVS	Informační systém veřejné správy
IT	Informační technologie
LAN	Lokální počítačová síť
MAC	Media Access Control
MěÚ	Městský úřad
MP	Městská policie
NBÚ	Národní bezpečnostní úřad
ÚOOÚ	Úřad pro ochranu osobních údajů
PIAP	Personal Internet Access Point
PC	Osobní počítač
p.o.	Příspěvková organizace
POP3	Post Office Protocol version 3
RM	Rada města
RTF	Ritch text format
ZM	Zastupitelstvo města

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PŘEHLEDOVÁ ANALÝZA RIZIK - KOMPONENTY - VYHODNOCENÍ PODLE DOPADŮ

RANIT - MěÚ Vsetín

Poznámka:

Komponenta ID: 300
Název: Ginis
Hodnotit: Ano
Vlastník: OI
Popis: uživatelé: FO (osobní údaje)
MPV (3 přístupy)
OUPSŘD (26 přístupů) - dopady stejné jako SW Vita (zásadní dopady)
OŠaK - 7 přístupů
ÚIA - 2 přístupy (dopady nedostupnosti nejsou závažné),
VSI: 1 uživatel, přístup i k poště města, není kryto smlouvou
ObŽÚ - 10 přístupů, řízení přístupů, nedostupnost překlenutelná, provozní problémy, v případě ztráty dat by bylo nutno doplnit informace zřejmě 1 rok zpětně
OSV - 40 přístupů, kratší nedostupnost překlenutelná, nutnost dodfatečně doplnit
OKS - 15 přístupů
OP - nedostupnost: hodiny nejsou problém, dny nedostupnosti - komplikace, vícepráce
ztráta dat - komplikace, zásadní dopady ne
Umístění:
Poznámka: Hodnocení (OŽP): více než dva dny problém (čísla jednací)
OSV (týden nedostupnosti závažný problém)
OKS (nedostupnost může způsobit neodeslání pošty, přijeti pošty je možno v ručním režimu, delší nedostupnot - přechod na ruční režim, vícenáklady)
v případě ztráty dat by byla pravděpodobná obnova dat za aktuální rok

Dopad: Z07 Nedostupnost 2 d
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka: MPV
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2
Poznámka:
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka:
Finanční hodnota:

Dopad: Z15 Prozrazení cizím subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Dopad: Z15 Prozrazení cizím subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Komponenta ID: 301
Název: ORSoft
Hodnotit: Ano
Vlastník: FO
Popis: hodnocení FO
OKS: majetek prohlížení, personalistika (nedostupnost překlenutelná)
Umístění:
Poznámka:

Dopad: Z02 Nedostupnost 1 h
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A00 Bez dopadu - 0.0
Poznámka: hůlavní dopad ve mzdové agendě - organizačně zvládnutelné bez dopadů
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka: potřeba víceprací se zaúčtováním
problém s daňovým přiznáním
Finanční hodnota:

Dopad: Z10 Nedostupnost 4 T
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka: závažnější organizační a provozní problémy (FO)
Finanční hodnota:

Dopad: Z11 Ztráta dat od poslední zálohy
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka: záloha denní (subj. FO)
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Dopad: Z13 Prozrazení interním subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka: především problémy se ztrátou důvěrnosti mzdových informací
Finanční hodnota:

Dopad: Z15 Prozrazení cizím subjektům
Hodnota: A06 Velmi vysoká hodnota 3.000 - 10.000tis. Kč - 4.0
Poznámka: především mzdová agenda
Finanční hodnota:

Komponenta ID: 302
Název: Radnice Vera (poplatky, pokladna)
Hodnotit: Ano
Vlastník: FO
Popis:
Umístění:
Poznámka:

Dopad: Z02 Nedostupnost 1 h
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka:
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A02 Malá, hodnota 10 - 100 tis.Kč - 0.4
Poznámka:
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A06 Velmi vysoká hodnota 3.000 - 10.000tis. Kč - 4.0
Poznámka: ztráta informace o pohledávkách - ztráta pohledávek
Finanční hodnota:

Komponenta ID: 303
Název: Radnice Vera - volby
Hodnotit: Ano
Vlastník: OKS
Popis: Organizace voleb
Volební agenda
Umístění:
Poznámka:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka: tisk volebních seznamů dva dny před termínem voleb (protiopatření tisk v předstihu)

Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A02 Malá, hodnota 10 - 100 tis.Kč - 0.4
Poznámka: jen operativa (převzetí dat z registru obyvatel)
Finanční hodnota:

Komponenta ID: 304
Název: Radnice Vera - registr obyvatel
Hodnotit: Ano
Vlastník: OSA
Popis: uživatelé: MP: všichni strážníci (26) - nedostupnost řešitelný problém - organizační
UIK - 1 přístup, prohlížení, nedostupnost bez dopadů
OSV - 4 přístupy
OKS - k volbám, nedostupnost řešitelná
OP - nedostupnost řešitelná

Umístění:
Poznámka:

Komponenta ID: 304
Název: Radnice Vera - přestupky
Hodnotit: Ano
Vlastník: OSA
Popis: MPV: (všichni 27) (hodnocení dopadů MPV)
OSA: jen OÚ, citlivé údaje uvedeny jen v papírové podobě
(zdravotní stav, trestný čin)
Umístění:
Poznámka:

Dopad: Z02 Nedostupnost 1 h
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z03 Nedostupnost 3 h
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka:
Finanční hodnota:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka:
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A02 Malá, hodnota 10 - 100 tis.Kč - 0.4
Poznámka:
Finanční hodnota:

Dopad: Z10 Nedostupnost 4 T

Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2
Poznámka:
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Dopad: Z13 Prozrazení interním subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Komponenta ID: 305
Název: Radnice Vera - tvorba rozpočtu
Hodnotit: Ano
Vlastník: FO
Popis: Problém jen ztráta dat ve fázi tvorby rozpočtu
Umístění:
Poznámka:

Dopad: Z12 Úplná ztráta dat
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Komponenta ID: 306
Název: SW Vita - Stavební úřad
Hodnotit: Ano
Vlastník: UOPSŘD
Popis:
Umístění:
Poznámka:

Dopad: Z02 Nedostupnost 1 h
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z07 Nedostupnost 2 d
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T

Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2
Poznámka:
Finanční hodnota:

Dopad: Z15 Prozrazení cizím subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Komponenta ID: 307
Název: SW Vita - Vodoprávní úřad
Hodnotit: Ano
Vlastník: OŽP
Popis: Vodoprávní úřad
Umístění:
Poznámka: subjektivně: technické problémy, procesní problémy
podpora dodavatele nevyužívaná
zálohování subj. problémem IT

Dopad: Z02 Nedostupnost 1 h
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z07 Nedostupnost 2 d
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Dopad: Z10 Nedostupnost 4 T
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2
Poznámka:
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2

Poznámka:
Finanční hodnota:

Dopad: Z13 Prozrazení interním subjektům
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2
Poznámka:
Finanční hodnota:

Dopad: Z15 Prozrazení cizím subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Komponenta ID: 308
Název: Lesní hospodářská kniha
Hodnotit: Ano
Vlastník: OŽP
Popis: dodavatel spol. Foresta
nedostupnost není problém (lokální aplikace)
? zpracování OÚ
? povinnosti správce a zpracovatele
Umístění:
Poznámka:

Dopad: Z12 Úplná ztráta dat
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka: dopad nízký díky protiopatření - několikanásobná záloha
Finanční hodnota:

Dopad: Z13 Prozrazení interním subjektům
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2
Poznámka:
Finanční hodnota:

Dopad: Z14 Prozrazení smluvním subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Dopad: Z15 Prozrazení cizím subjektům
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč - 2.0
Poznámka:
Finanční hodnota:

Komponenta ID: 311
Název: Dopravně správní činnosti Yamaco
Hodnotit: Ano
Vlastník: OSA
Popis: evidence přestupků
Umístění:
Poznámka:

Dopad: Z02 Nedostupnost 1 h
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka:
problém jen s vyjádřením o pověsti
Finanční hodnota:

Dopad: Z12 Úplná ztráta dat
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka: znovupořízení dat
Finanční hodnota:

Komponenta ID: 312
Název: Správní evidence
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Komponenta ID: 313
Název: Evidence dopravně správních agend
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Komponenta ID: 314
Název: Eliška
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Komponenta ID: 315
Název: Česká koncelář pojistitelů
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A00 Bez dopadu - 0.0
Poznámka:
Finanční hodnota:

Dopad: Z10 Nedostupnost 4 T
Hodnota: A02 Malá, hodnota 10 - 100 tis.Kč - 0.4
Poznámka:
Finanční hodnota:

Komponenta ID: 316
Název: Davoz
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:

Dopad: Z10 Nedostupnost 4 T
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč - 1.2
Poznámka:
Finanční hodnota:

Komponenta ID: 317
Název: Sociální agenda ISSA Geovap
Hodnotit: Ano
Vlastník: OSV
Popis: OSV - 15 přístupů
hodnocení OSA

Umístění:
Poznámka:

Dopad: Z02 Nedostupnost 1 h
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč - 0.2
Poznámka:
Finanční hodnota:

Dopad: Z06 Nedostupnost 1 d
Hodnota: A02 Malá, hodnota 10 - 100 tis.Kč - 0.4
Poznámka:
Finanční hodnota:

Dopad: Z08 Nedostupnost 1 T
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč - 0.8
Poznámka:
Finanční hodnota:

Komponenta ID: 318
Název: OK Nouze
Hodnotit: Ano
Vlastník: OSV
Popis: správcem MPSV
zpracovatel Město Vsetín
16 přístupů
Umístění:
Poznámka:

Komponenta ID: 319
Název: OK Služby
Hodnotit: Ano
Vlastník: OSV
Popis: MPSV
8 přístupů
Umístění:
Poznámka:

Komponenta ID: 400
Název: Data MěÚ Vsetín
Hodnotit: Ano
Vlastník: MěÚ Vsetín
Popis:
Umístění:
Poznámka:

Komponenta ID: 500
Název: Aktiva - Servery
Hodnotit: Ano
Vlastník: OI
Popis:
Umístění:
Poznámka:

Komponenta ID: 601
Název: Elektronická pošta
Hodnotit: Ano
Vlastník: OI
Popis:
Umístění:

Poznámka: nedostupnost překlenutelná

Komponenta ID: 800
Název: Lokality
Hodnotit: Ano
Vlastník: MÚ Vsetín
Popis:
Umístění:
Poznámka:

Komponenta ID: 900
Název: Kamerové systémy
Hodnotit: Ano
Vlastník: MPo
Popis:
Umístění:
Poznámka:

Komponenta ID: 1000
Název: Aktiva - MPo
Hodnotit: Ano
Vlastník: MPo
Popis:
Umístění:
Poznámka:

Komponenta ID: 2000
Název: Zpracování osobních údajů MĚÚ Vsetín
Hodnotit: Ano
Vlastník: MĚÚ Vsetín
Popis:
Umístění:
Poznámka:

PŘÍLOHA P II: PŘEHLEDOVÁ ANALÝZA RIZIK - VYHODNOCENÍ RIZIK PODLE AKTIV

RANIT - MěÚ Vsetín

Poznámka:

Komponenta ID: 800
Název: Lokality
Hodnotit: Ano
Vlastník: MĚÚ Vsetín
Popis:
Umístění:
Poznámka:
Míra rizika: 60

Aktivum ID: 800/801
Název: MĚÚ - Hlavní budova
Hodnota: A09 Velmi vysoká hodnota nad 100 mil.Kč
Typ: Lokalita
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: MĚÚ Vsetín
Popis: Svárov 10/80 hlavní budova MĚÚ – cca 80 procent IS
vlastnictví: MĚÚ
Umístění:
Poznámka: Další právní subjekty (sdílejí protory), ICT nesdílejí
Zřejmě nadstandardní přístup do úprostor MĚÚ! (slabina fyz. bezp.)

Míra rizika: 60

Hrozba ID: 800/801/17
Hrozba: TH17 Požár
Úroveň hrozby: Z09 Nedostupnost 2 T
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 60

Komponenta ID: 301
Název: ORSoft
Hodnotit: Ano
Vlastník: FO
Popis: hodnocení FO
OKS: majetek prohlížení, personalistika (nedostupnost překlenutelná)
Umístění:
Poznámka:

Míra rizika: 21,8

Aktivum ID: 301/154
Název: SKU ORSoft
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služba koncovému uživateli
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis:
Umístění:
Poznámka:
Míra rizika: 21,8

Hrozba ID: 301/154/18
Hrozba: TH18 Předstírání identity uživatele cizími osobami
Úroveň hrozby: Z15 Prozrazení cizím subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.05.1 Bezpečnostní politika informací; A.06.2.2 Bezpečnostní požadavky pro přístup klientů; A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.10.1 Pořizování auditních záznamů; A.10.10.6 Synchronizace hodin
Účinnost protiopatření: C2 nízká 30%
Dopad: Z15 Prozrazení cizím subjektům - A06 Velmi vysoká hodnota 3.000 - 10.000tis. Kč
Poznámka:
Míra rizika: 21,8

Komponenta ID: 2000
Název: Zpracování osobních údajů MĚÚ Vsetín
Hodnotit: Ano
Vlastník: MĚÚ Vsetín
Popis:
Umístění:
Poznámka:
Míra rizika: 14,3

Aktivum ID: 2000/2019
Název: Zpracování osobních údajů MĚÚ Vsetín
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Typ: Datové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: MĚÚ Vsetín
Popis: osobní údaje pro výběrová řízení do doby ukončení výběrového řízení
Umístění: m.č. 716
Poznámka: v tištěné podobě do doby vrácení matariálů mevybraným uchazečům
v elektronické podobě - zápis z VŘ
předáno v el. i písemné podobě vedení + výběrová komise
Míra rizika: 14,3

Hrozba ID: 2000/2019/2

Hrozba: TH02 Chyba přenosu
Úroveň hrozby: Z15 Prozrazení cizím subjektům
Frekvence hrozby: F3 Střední (jednou měsíčně)
Úroveň zranitelnosti: R3 Střední
Protiopatření: A.10.8.1 Postupy a politiky při výměně informací
Účinnost protiopatření: C3 Částečná 50%
Poznámka:
Míra rizika: 14,3

Komponenta ID: 400

Název: Data MĚÚ Vsetín
Hodnotit: Ano
Vlastník: MĚÚ Vsetín
Popis:
Umístění:
Poznámka:
Míra rizika: 13

Aktivum ID: 400/405

Název: Data GIS - interní
Hodnota: A07 Velmi vysoká hodnota 10 mil.Kč - 30 mil. Kč
Typ: Datové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OI
Popis:
Umístění: vsetin 6,

Poznámka: riziko sníženo - obnova dat z e strany spol. T-mapy
Míra rizika: 13

Hrozba ID: 400/405/6

Hrozba: TH06 Chyby uživatele
Úroveň hrozby: Z07 Nedostupnost 2 d
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.10.10.1 Pořizování auditních záznamů; A.10.10.6 Synchronizace hodin; A.10.5.1 Zálohování informací; A.11.2.1 Registrace uživatele; A.11.3.1 Používání hesel
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 13

Komponenta ID: 306

Název: SW Vita - Stavební úřad
Hodnotit: Ano
Vlastník: UOPSŘD
Popis:
Umístění:
Poznámka:
Míra rizika: 11,4

Aktivum ID: 306/155
Název: SKU Vita - Stavební úřad
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služba koncovému uživateli
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis:
Umístění:
Poznámka:
Míra rizika: 11,4

Hrozba ID: 306/155/18
Hrozba: TH18 Předstírání identity uživatele cizími osobami
Úroveň hrozby: Z15 Prozrazení cizím subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.05.1 Bezpečnostní politika informací; A.06.2.2 Bezpečnostní požadavky pro přístup klientů; A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.10.1 Pořizování auditních záznamů; A.10.10.6 Synchronizace hodin
Účinnost protiopatření: C2 nízká 30%
Dopad: Z15 Prozrazení cizím subjektům - A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Poznámka:
Míra rizika: 11,4

Komponenta ID: 307
Název: SW Vita - Vodoprávní úřad
Hodnotit: Ano
Vlastník: OŽP
Popis: Vodoprávní úřad
Umístění:
Poznámka: subjektivně: technické problémy, procesní problémy
podpora dodavatele nevyužívaná
zálohování subj. problémem IT
Míra rizika: 11,4

Aktivum ID: 307/156
Název: SKU Vita - Vodoprávní úřad
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služba koncovému uživateli
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis:
Umístění:
Poznámka:
Míra rizika: 11,4

Hrozba ID: 307/156/18
Hrozba: TH18 Předstírání identity uživatele cizími osobami
Úroveň hrozby: Z15 Prozrazení cizím subjektům

Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.05.1 Bezpečnostní politika informací; A.06.2.2 Bezpečnostní požadavky pro přístup klientů; A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.10.1 Pořizování auditních záznamů; A.10.10.6 Synchronizace hodin
Účinnost protiopatření: C2 nízká 30%
Dopad: Z15 Prozrazení cizím subjektům - A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Poznámka:
Míra rizika: 11,4

Komponenta ID: 304

Název: Radnice Vera - přestupky
Hodnotit: Ano
Vlastník: OSA
Popis: MPV: (všichni 27) (hodnocení dopadů MPV)
OSA: jen OÚ, citlivé údaje uvedeny jen v papírové podobě
(zdravotní stav, trestný čin)
Umístění:
Poznámka:
Míra rizika: 5

Aktivum ID: 304/152

Název: SKU Radnice Vera
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služba koncovému uživateli
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis:
Umístění:
Poznámka:
Míra rizika: 5

Hrozba ID: 304/152/12

Hrozba: TH12 Neoprávněné použití aplikačního software
Úroveň hrozby: Z13 Prozrazení interním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R3 Střední
Protiopatření: A.08.2.1 Odpovědnosti vedoucích zaměstnanců; A.08.3.3 Odebrání přístupových práv; A.11.5.2 Identifikace a autentizace uživatelů
Účinnost protiopatření: C2 nízká 30%
Dopad: Z13 Prozrazení interním subjektům - A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Poznámka:
Míra rizika: 5

Komponenta ID: 300

Název: Ginis
Hodnotit: Ano
Vlastník: OI
Popis: uživatelé: FO (osobní údaje)
MPV (3 přístupy)

OUPSŘD (26 přístupů) - dopady stejné jako SW Vita (zásadní dopady)
OŠaK - 7 přístupů
ÚIA - 2 přístupy (dopady nedostupnosti nejsou závažné),
VSI: 1 uživatel, přístup i k poště města, není kryto smlouvou
ObŽÚ - 10 přístupů, řízení přístupů, nedostupnost překlenutelná, provozní problémy, v případě ztráty dat by bylo nutno doplnit informace zřejmě 1 rok zpětně
OSV - 40 přístupů, kratší nedostupnost překlenutelná, nutnost dodfatečně doplnit
OKS - 15 přístupů
OP - nedostupnost: hodiny nejsou problém, dny nedostupnosti - komplikace, vícepráce
ztráta dat - komplikace, zásadní dopady ne
Umístění:
Poznámka: Hodnocení (OŽP): více než dva dny problém (čísla jednací)
OSV (týden nedostupnosti závažný problém)
OKS (nedostupnost může způsobit neodeslání pošty, přijeti pošty je možno v ručním režimu, delší nedostupnot - přechod na ruční režim, vícenáklady)
v případě ztráty dat by byla pravděpodobná obnova dat za aktuální rok
Míra rizika: 3,5

Aktivum ID: 300/101
Název: SW Ginis
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Typ: Programové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis: spisová služba
Umístění: vsetin 3
Poznámka: hodnocení: podatelna
Míra rizika: 3,5

Hrozba ID: 300/101/23
Hrozba: TH23 Selhání aplikačního software
Úroveň hrozby: Z11 Ztráta dat od poslední zálohy
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.1.2 Řízení změn; A.10.1.4 Oddělení vývoje, testování a provozu; A.10.2 Řízení dodávek služeb třetích stran
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 3,5

Komponenta ID: 302
Název: Radnice Vera (poplatky, pokladna)
Hodnotit: Ano
Vlastník: FO
Popis:
Umístění:
Poznámka:
Míra rizika: 3,5

Aktivum ID: 302/102
Název: SW Radnice Vera
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Typ: Programové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis: registr obyvatel, evidence psů, hrací automaty, komunální odpad, MPolicie, organizace voleb, pokladna, přestupkové řízení, příjmy daně poplatky, splátky a půjčky, tvorba rozpočtu, volební agenda,

Umístění: vsetin 3
Poznámka: hodnocení: odbor finanční, paní Feilerová
Míra rizika: 3,5

Hrozba ID: 302/102/23
Hrozba: TH23 Selhání aplikačního software
Úroveň hrozby: Z11 Ztráta dat od poslední zálohy
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.1.2 Řízení změn; A.10.1.4 Oddělení vývoje, testování a provozu; A.10.2 Řízení dodávek služeb třetích stran
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 3,5

Komponenta ID: 303
Název: Radnice Vera - volby
Hodnotit: Ano
Vlastník: OKS
Popis: Organizace voleb
Volební agenda
Umístění:
Poznámka:
Míra rizika: 3,5

Aktivum ID: 303/102
Název: SW Radnice Vera
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Typ: Programové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis: registr obyvatel, evidence psů, hrací automaty, komunální odpad, MPolicie, organizace voleb, pokladna, přestupkové řízení, příjmy daně poplatky, splátky a půjčky, tvorba rozpočtu, volební agenda,

Umístění: vsetin 3

Poznámka: hodnocení: odbor finanční, paní Feilerová
Míra rizika: 3,5

Hrozba ID: 303/102/23
Hrozba: TH23 Selhání aplikačního software
Úroveň hrozby: Z11 Ztráta dat od poslední zálohy
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.1.2 Řízení změn; A.10.1.4 Oddělení vývoje, testování a provozu; A.10.2 Řízení dodávek služeb třetích stran
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 3,5

Komponenta ID: 305
Název: Radnice Vera - tvorba rozpočtu
Hodnotit: Ano
Vlastník: FO
Popis: Problém jen ztráta dat ve fázi tvorby rozpočtu
Umístění:
Poznámka:
Míra rizika: 3,5

Aktivum ID: 305/102
Název: SW Radnice Vera
Hodnota: A05 Vysoká, hodnota 1.000 - 3.000 tis.Kč
Typ: Programové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis: registr obyvatel, evidence psů, hrací automaty, komunální odpad, MPolicie, organizace voleb, pokladna, přestupkové řízení, příjmy daně poplatky, splátky a půjčky, tvorba rozpočtu, volební agenda,

Umístění: vsetin 3
Poznámka: hodnocení: odbor finanční, paní Feilerová
Míra rizika: 3,5

Hrozba ID: 305/102/23
Hrozba: TH23 Selhání aplikačního software
Úroveň hrozby: Z11 Ztráta dat od poslední zálohy
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.1.2 Řízení změn; A.10.1.4 Oddělení vývoje, testování a provozu; A.10.2 Řízení dodávek služeb třetích stran
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 3,5

Komponenta ID: 500
Název: Aktiva - Servery
Hodnotit: Ano
Vlastník: OI
Popis:
Umístění:
Poznámka:
Míra rizika: 3,1

Aktivum ID: 500/505
Název: Vsetin 7
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč
Typ: Fyzické aktivum - Hardware
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OI
Popis: virtuální server (vsetin 10)
Umístění: MĚÚ Serverovna
Poznámka: vsetin 7 - virtuální server, Firebird server, (YAMACO, evidence odpadového hosp inisoft,
NOEL SMS (objednávkový) systém
Míra rizika: 3,1

Hrozba ID: 500/505/3
Hrozba: TH03 Chyba údržby technického vybavení
Úroveň hrozby: Z07 Nedostupnost 2 d
Frekvence hrozby: F2 Nízká (jednou ročně)
Úroveň zranitelnosti: R2 Nízká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 3,1

Komponenta ID: 601
Název: Elektronická pošta
Hodnotit: Ano
Vlastník: OI
Popis:
Umístění:
Poznámka: nedostupnost překlenutelná
Míra rizika: 2,6

Aktivum ID: 601/459
Název: Data Mail (MS Exchange)
Hodnota: A04 Střední, hodnota 300 - 1.000 tis.Kč
Typ: Datové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OI
Popis:

Umístění:
Poznámka:
Míra rizika: 2,6

Hrozba ID: 601/459/6
Hrozba: TH06 Chyby uživatele
Úroveň hrozby: Z07 Nedostupnost 2 d
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.10.10.1 Pořizování auditních záznamů; A.10.10.6 Synchronizace hodin; A.10.5.1 Zálohování informací; A.11.2.1 Registrace uživatele; A.11.3.1 Používání hesel
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 2,6

Komponenta ID: 308
Název: Lesní hospodářská kniha
Hodnotit: Ano
Vlastník: OŽP
Popis: dodavatel spol. Foresta
nedostupnost není problém (lokální aplikace)
? zpracování OÚ
? povinnosti správce a zpracovatele
Umístění:
Poznámka:
Míra rizika: 1,4

Aktivum ID: 308/112
Název: Lesní hospodářská kniha
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč
Typ: Programové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis:
Umístění: data na vsetin 3, aplikace lokálně
Poznámka: hodnocení: odbor životního prostředí
Míra rizika: 1,4

Hrozba ID: 308/112/23
Hrozba: TH23 Selhání aplikačního software
Úroveň hrozby: Z11 Ztráta dat od poslední zálohy
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.1.2 Řízení změn; A.10.1.4 Oddělení vývoje, testování a provozu; A.10.2 Řízení dodávek služeb třetích stran
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 1,4

Komponenta ID: 311
Název: Dopravně správní činnosti Yamaco
Hodnotit: Ano
Vlastník: OSA
Popis: evidence přestupků
Umístění:
Poznámka:
Míra rizika: 1,4

Aktivum ID: 311/120
Název: Dopravně správní činnosti Yamaco
Hodnota: A03 Nízká, hodnota 100 - 300 tis.Kč
Typ: Programové aktivum
Závislost komponenty na aktivu: 100 %
Základní přístup: Ano
Popis přístupu:
Vlastník: OSA
Popis: producent: Yamaco

Umístění:
Poznámka:
Míra rizika: 1,4

Hrozba ID: 311/120/23
Hrozba: TH23 Selhání aplikačního software
Úroveň hrozby: Z11 Ztráta dat od poslední zálohy
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.1.2 Řízení změn; A.10.1.4 Oddělení vývoje, testování a provozu; A.10.2 Řízení dodávek služeb třetích stran
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 1,4

Komponenta ID: 304
Název: Radnice Vera - registr obyvatel
Hodnotit: Ano
Vlastník: OSA
Popis: uživatelé: MP: všichni strážníci (26) - nedostupnost řešitelný problém - organizační
UIK - 1 přístup, prohlížení, nedostupnost bez dopadů
OSV - 4 přístupy
OKS - k volbám, nedostupnost řešitelná
OP - nedostupnost řešitelná

Umístění:
Poznámka:
Míra rizika: 1

Aktivum ID: 304/153

Název: SKU Radnice Vera Java (matrika)
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služba koncovému uživateli
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis:
Umístění:
Poznámka:
Míra rizika: 1

Hrozba ID: 304/153/18
Hrozba: TH18 Předstírání identity uživatele cizími osobami
Úroveň hrozby: Z15 Prozrazení cizím subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká
Protiopatření: A.05.1 Bezpečnostní politika informací; A.06.2.2 Bezpečnostní požadavky pro přístup klientů; A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.10.1 Pořizování auditních záznamů; A.10.10.6 Synchronizace hodin
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 1

Komponenta ID: 317
Název: Sociální agenda ISSA Geovap
Hodnotit: Ano
Vlastník: OSV
Popis: OSV - 15 přístupů
hodnocení OSA

Umístění:
Poznámka:
Míra rizika: 1

Aktivum ID: 317/157
Název: SKU Vita - ISSA Geovap
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služba koncovému uživateli
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník:
Popis:
Umístění:
Poznámka:
Míra rizika: 1

Hrozba ID: 317/157/18
Hrozba: TH18 Předstírání identity uživatele cizími osobami
Úroveň hrozby: Z15 Prozrazení cizím subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R2 Nízká

Protiopatření: A.05.1 Bezpečnostní politika informací; A.06.2.2 Bezpečnostní požadavky pro přístup klientů; A.06.2.3 Bezpečnostní požadavky v dohodách se třetí stranou; A.10.10.1 Pořizování auditních záznamů; A.10.10.6 Synchronizace hodin
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 1

Komponenta ID: 312

Název: Správní evidence
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:
Míra rizika: 0,7

Aktivum ID: 312/705

Název: Správní evidence
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služby dodavatelů
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OSA
Popis: Pasy, OP, registr obyvatel
Provozovatel Ministerstvo vnitra
Umístění:
Poznámka: 15 PC (společně s dopravními agendami)
Míra rizika: 0,7

Hrozba ID: 312/705/20

Hrozba: TH20 Předstírání identity uživatele smluvními partnery
Úroveň hrozby: Z14 Prozrazení smluvním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 0,7

Komponenta ID: 313

Název: Evidence dopravně správních agend
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:
Míra rizika: 0,7

Aktivum ID: 313/708

Název: Evidence dopravně správních agend
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč

Typ: Služby dodavatelů
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OSA
Popis: Správce ministerstvo vnitra
registr vozidel
Umístění:
Poznámka: 15 PC (společně s dopravními agendami)
Míra rizika: 0,7

Hrozba ID: 313/708/20
Hrozba: TH20 Předstírání identity uživatele smluvními partnery
Úroveň hrozby: Z14 Prozrazení smluvním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 0,7

Komponenta ID: 314
Název: Eliška
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:
Míra rizika: 0,7

Aktivum ID: 314/706
Název: Eliška
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služby dodavatelů
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OSA
Popis: Správce ministerstvo dopravy
Umístění:
Poznámka:
Míra rizika: 0,7

Hrozba ID: 314/706/20
Hrozba: TH20 Předstírání identity uživatele smluvními partnery
Úroveň hrozby: Z14 Prozrazení smluvním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 0,7

Komponenta ID: 315
Název: Česká koncelář pojistitelů
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:
Míra rizika: 0,7

Aktivum ID: 315/704
Název: Česká koncelář pojistitelů
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služby dodavatelů
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OSA
Popis: Provozovatel, správce ČKP
Umístění:
Poznámka:
Míra rizika: 0,7

Hrozba ID: 315/704/20
Hrozba: TH20 Předstírání identity uživatele smluvními partnery
Úroveň hrozby: Z14 Prozrazení smluvním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 0,7

Komponenta ID: 316
Název: Davoz
Hodnotit: Ano
Vlastník: OSA
Popis:
Umístění:
Poznámka:
Míra rizika: 0,7

Aktivum ID: 316/703
Název: Davoz
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služby dodavatelů
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OSA
Popis: ověření původu, navedení dovezených vozidel
provozovatel, správce Ministerstvo dopravy
Umístění:
Poznámka:

Míra rizika: 0,7

Hrozba ID: 316/703/20
Hrozba: TH20 Předstírání identity uživatele smluvními partnery
Úroveň hrozby: Z14 Prozrazení smluvním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 0,7

Komponenta ID: 318
Název: OK Nouze
Hodnotit: Ano
Vlastník: OSV
Popis: správcem MPSV
zpracovatel Město Vsetín
16 přístupů
Umístění:
Poznámka:
Míra rizika: 0,7

Aktivum ID: 318/706
Název: OK Nouze
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služby dodavatelů
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OSV
Popis: MPSV
Umístění:
Poznámka:
Míra rizika: 0,7

Hrozba ID: 318/706/20
Hrozba: TH20 Předstírání identity uživatele smluvními partnery
Úroveň hrozby: Z14 Prozrazení smluvním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 0,7

Komponenta ID: 319
Název: OK Služby
Hodnotit: Ano
Vlastník: OSV
Popis: MPSV
8 přístupů

Umístění:
Poznámka:
Míra rizika: 0,7

Aktivum ID: 319/706
Název: OK Služby
Hodnota: A01 Zanedbatelná, hodnota do 10 tis. Kč
Typ: Služby dodavatelů
Závislost komponenty na aktivu: 100 %
Základní přístup: Ne
Vlastník: OSV
Popis: MPSV
Umístění:
Poznámka:
Míra rizika: 0,7

Hrozba ID: 319/706/20
Hrozba: TH20 Předstírání identity uživatele smluvními partnery
Úroveň hrozby: Z14 Prozrazení smluvním subjektům
Frekvence hrozby: F1Občasná (jednou za více let)
Úroveň zranitelnosti: R4 Vysoká
Protiopatření:
Účinnost protiopatření: C2 nízká 30%
Poznámka:
Míra rizika: 0,7

Komponenta ID: 900
Název: Kamerové systémy
Hodnotit: Ano
Vlastník: MPo
Popis:
Umístění:
Poznámka:

Komponenta ID: 1000
Název: Aktiva - MPo
Hodnotit: Ano
Vlastník: MPo
Popis:
Umístění:
Poznámka:

PŘÍLOHA P III: HROZBY

Referenční období 1 - 2 roky

Hrozba	Popis hrozby	Výskyt hrozby
TH01 Chyba provozu	Hrozba pokrývá situaci, kdy osoby odpovědně za zajišťování provozu serverového systému, mohli udělat chybu při plnění svých pracovních úkolů.	Nenastalo
TH03 Chyba údržby technického vybavení	Hrozba chyby údržby technického vybavení pokrývá situaci, kdy by osoby odpovědné za údržbu technického vybavení, mohly udělat chybu při plnění svých pracovních úkolů.	Nenastalo
TH04 Chyba údržby/ úpravy programového vybavení	Hrozba chyby údržby programového vybavení zahrnuje možnost, že by lidé nebo organizace, které jsou odpovědné za údržbu programového vybavení, mohli udělat chybu při své práci.	Max. jednotky za rok
TH05 Chybné směrování zpráv	Hrozba chybného směrování pokrývá situaci, kdy informace přenášené po síti mohou být doručeny na nesprávnou adresu.	Nenastalo
TH06 Chyby uživatele	Hrozba chyby uživatele pokrývá situaci, kdy uživatelé by mohli dělat chyby při používání aplikace.	Jednotky/rok
TH07 Infiltrace komunikací	Infiltrace komunikace pokrývá následující druhy incidentů: - Neoprávněné proniknutí do systému například díky využití chyby přetečení zásobníku - Vydávání se za jiný server - Vydávání se za existujícího uživatele e-commerce aplikace - Vydávání se za nového uživatele e-commerce aplikace - Znepřístupnění služeb (úmyslné) - Spamming (rozesílání nevyžádaných emailů) - Flaming (zahlcení diskusních fór nesmyslnými či urážlivými zprávami	Nenastalo
TH08 Krádež provedená cizími osobami	Hrozba krádeže cizí osobou hrozí zejména dokumentaci a fyzickým aktivům. Krádež je zpravidla možné charakterizovat za provedenou cizími osobami v případě kdy došlo k vloupání. Zranitelnost vůči krádeži vyplývá z jednoduchosti, se jakou je možné aktivum odnést, a na času, který je nutný pro	Nenastalo
	zajištění náhradního zařízení.	
TH09 Krádež provedená identifikovatelnými osobami	Hrozba krádeže identifikovatelnými osobami hrozí zejména dokumentaci a fyzickým aktivům. Identifikovatelnou osobou je kdokoliv, kdo má legitimní důvod pro práci v budově jako uklízečky, pracovníci dodavatelských firem apod. Úroveň hrozby je odvozena hlavně z počtu předchozích případů, z typu krádeží tj. zda byly drobné či nikoli, ze skutečnosti, zda byly krádeže prováděny zaměstnanci, smluvními partnery nebo návštěvníky a z morálky personálu. Zranitelnost je přímo závislá na rozsahu narušení fungování organizace a času, který je nutný pro nahrazení zařízení.	Nenastalo
TH10 Nedostatek zaměstnanců	Hrozba nedostatku personálu pokrývá situaci v níž nepřítomnosti klíčových osob z jakýchkoli důvodů. Úroveň hrozby pokrývá jednoduchost s jakou mohou být nahrazeni. Zranitelnost vůči nedostatku personálu závisí na rozsahu v jakém by nedostatek personálu	Nenastalo

	mohl ovlivnit fungování organizace.	
TH11 Negativní vlivy prostředí	Prašné, vhké, suché, teplé studené....prostředí	Nenastalo
TH12 Neoprávněné použití aplikačního software	Neoprávněné použití aplikace pokrývá možnost, že některý uživatel použije účet, k němuž má oprávněný přístup k provádění neoprávněných činností. Příkladem může být například pracovník mzdového oddělení, který použije aplikaci pro mzdové účetnictví pro zvýšení vlastního platu.	Nenastalo
TH13 Popření	Tato hrozba pokrývá: - Případ, kdy osoba popře, že poslala určitou zprávu (popření původu) - Případ, kdy osoba popře, že přijala určitou zprávu (popření přijetí)	Nenastalo
TH14 Poškození paměťového média	Nečitelnost zálohovacích médií	Nenastalo
TH15 Poškození vedení	Poškození komunikačních vedení	Nenastalo
TH16 Poškození vodou	Hrozba poškození vodou pokrývá incident při němž by mohla fyzických aktiv systému (včetně dokumentace a magnetických médií) poškozena vodou. Míra zranitelnosti budovy a místnosti vůči poškození vodou závisí na rozsahu v jakém může voda zatopit místnost, na rozsahu v jakém může poškodit zařízení a na tom do jaké míry naruší funkčnost organizace.	Nenastalo
TH17 Požár	Hrozba požáru pokrývá incident poškození libovolných fyzických aktiv systému (včetně dokumentace a magnetických médií) požárem. Míra zranitelnosti budovy a místnosti vůči požáru závisí na rozsahu na který se požár po vypuknutí může rozšířit a na míře, se jakou naruší fungování organizace.	Nenastalo
TH18 Předstírání identity uživatele cizími osobami	Hrozba falšování uživatelské identity cizími osobami zahrnuje pokusy cizích osob získat neautorizovaný přístup k informacím tak, že se vydávají za oprávněného uživatele.	Nenastalo
TH19 Předstírání identity uživatele identifikovatelnými osobami	Hrozba falšování uživatelské identity identifikovatelnými osobami zahrnuje pokusy neautorizovaných uživatelů získat přístup k informacím, ke kterým nemají oprávnění přistupovat. Tito uživatelé se mohou pokusit získat přístup k těmto informacím tak, že se vydávají za jiného uživatele.	Nenastalo
TH20 Předstírání identity uživatele smluvními partnery	Hrozba falšování uživatelské identity smluvními poskytovateli služeb zahrnuje pokusy osob, které pracují pro smluvní poskytovatele služeb, získat neautorizovaný přístup k informacím tak, že se vydávají za jinou osobu.	Nenastalo
TH21 Přesměrování zpráv	Tato hrozba pokrývá - Aktivní odposlech -Vložení falešné zprávy - Úmyslné doručení zprávy v chybné následnosti - Úmyslné zpoždění doručení zprávy - Úmyslná změna směrování Pokud útočník dokáže přimět cílový systém útoku, aby komunikoval přes jeho vlastní počítač, může útočník zachytit zprávu, pozměnit ji a poslat dále.	Nenastalo
TH22 Přírodní katastrofa	Hrozba přírodní katastrofy pokrývá poškození lokality nebo jejího prostředí incidentem způsobeném přírodní	Nenastalo

	poměry (záplava) nebo lidmi (dopravní nehoda). Míra zranitelnosti prostředí nebo lokality závisí na rozsahu, s jakým katastrofa ovlivní chod organizace.	
TH23 Selhání aplikačního software	Hrozba selhání aplikačního programového vybavení pokrývá situaci, kdy by logika aplikačních programů mohla obsahovat chyby.	Jednotky/rok
TH24 Selhání dodávky energie	Hrozba výpadku napájení pokrývá situaci výpadku elektrické sítě.	Jednotky/více let
TH25 Selhání klimatizace	Hrozba výpadku klimatizace pokrývá situaci nutnosti přerušení práce z důvodu změny teploty mimo přijatelné meze, způsobené selháním klimatizačního zařízení.	Nenastalo
TH26 Selhání systémového software	Hrozba selhání systémového nebo síťového programového vybavení pokrývá situaci, kdy by systémové nebo síťové programové vybavení mohlo selhat a způsobit tak nedostupnost systému nebo oslabit další bezpečnostní mechanismy.	Nenastalo
TH27 Škodlivý software	Destruktivní a škodlivé programy mohou být: - viry - trojské koně - červi Emailové viry a škodlivé přenositelné programy jako např. Active X prvky jsou pokryty v hrozbě Začlenění škodlivých programů Tato hrozba pokrývá: - emailové viry - škodlivé přenositelné programy (škodlivé Active X applety) Emailové viry jsou v současnosti mnohem běžnější než viry přenášené disketami. Pokud se dostanou na síť, mohou rychle nakazit mnoho počítačů a mohou závažně narušit funkčnost systémů. Technologie Java a Active X zapříčinily vznik nových bezpečnostních problémů. Uživatelé nyní spouštějí programy pocházející zvnějšku organizace, někdy z neznámých zdrojů. Tyto programy často nejsou v organizaci testovány. Je možné, že škodlivé programy vytvořené použitím těchto technologií by mohly způsobit škodu na systémech	Jednotky/rok
TH28 Technické selhání hardware počítačů	Hrozba technické závady počítače pokrývá vznik faktorů, které zvyšují pravděpodobnost závady počítače nebo serveru Míra zranitelnosti vůči hrozbě závady počítače závisí na snadnosti obnovit funkčnost počítače po vzniku této hrozby.	Jednotky/ rok
TH29 Technické selhání komunikačních služeb	Tato hrozba pokrývá: - Nedostupnost poskytovatele služeb (ISP) - Selhání datového spojení - Nedoručení zprávy - Doručení v chybné následnosti (neúmyslné) - Pozdní doručení (neúmyslné) - Odepření služby (neúmyslné) Na Internetu neposkytuje smlouvu o úrovni služby. Není možné garantovat, jak dlouho bude trvat, než se zpráva nebo paket dostane k příjemci, ani to, že se tam nakonec vůbec dostane	Jednotky/ rok
TH30 Technické selhání periferního zařízení	Tato hrozba pokrývá okolnosti, které zvyšují pravděpodobnost vzniku technické závady tiskového zařízení. Míra zranitelnosti vůči závadě tiskového zařízení závisí na jednoduchosti obnovení funkčnosti při poruše.	Jednotky/rok
TH31 Technické selhání síťových	Tato hrozba pokrývá okolnosti, které zvyšují pravděpodobnost vzniku technické závady síťového	Jednotky/rok

komponent	distribučního prvku, síťové brány,zařízení pro řízení sítě . Míra zranitelnosti vůči závadě síťového distribučního prvku závisí na jednoduchosti obnovení jeho funkčnosti při poruše.	
TH32 Technické selhání paměťových zařízení	Tato hrozba pokrývá okolnosti, které zvyšují pravděpodobnost vzniku technické závady paměťového zařízení. Míra zranitelnosti vůči závadě paměťového zařízení závisí na jednoduchosti obnovení funkčnosti při poruše.	Jednotky/rok
TH33 Terorismus, extremismus	Hrozba terorismu pokrývá činnost organizovaných skupin hodlajících dosáhnout politických nebo ekonomických cílů násilím	Nenastalo
TH34 Úmyslná škoda způsobená cizími osobami	Hrozba úmyslného poškození identifikovatelnými osobami zahrnuje činy vandalismu a další případy, kdy dojde k fyzickému poškození informačního systému nebo podpůrných zařízení, které provedli osoby bez povoleného vstupu do budovy.	Nenastalo
TH35 Úmyslná škoda způsobená identifikovatelnými osobami	Hrozba úmyslného poškození identifikovatelnými osobami zahrnuje činy vandalismu a další případy, kdy dojde k fyzickému poškození informačního systému nebo podpůrných zařízení, které provedli osoby s povoleným vstupem do budovy.	Nenastalo
TH36 Zachycení komunikace	Tato hrozba pokrývá: - Pasivní odposlech - Monitorování objemu nebo původu a cíle komunikace Jednoduchost zachycení komunikace je ovlivněna dvěma faktory: -přenosovým médiem -druhem použitého protokolu Zachycení některých druhů komunikace na Internetu je relativně snadné. Útočník může instruovat cílový systém svého útoku aby komunikoval prostřednictvím specifických počítačů (k nimž má přístup útočník)	Nenastalo
TH37 Zneužití systémových zdrojů	Zneužití systémových prostředků pokrývá zneužití prostředků systému, který patří organizaci pro nepracovní činnosti. Tato hrozba může například pokrývat: - používání textového editoru pro osobní korespondenci - používání vývojářských prostředků k vytváření programů pro externí organizace -používání přístupu k Internetu pro prohlížení stránek a stahování souborů, které nejsou spojeny s pracovní náplní	Neidentifikováno

PŘÍLOHA P IV: SMĚRNICE QS 42-06 BEZPEČNOST INFORMACÍ

Město Vsetín, Městský úřad Vsetín, Svárov 1080, 755 01 Vsetín , IČ0: 00304450		
Město Vsetín **Městský úřad Vsetín**	**SMĚRNICE číslo** **QS 42-06**	Výtisk č.: neřízená kopie Vydání: 1 Účinnost od: 1. 4. 2010 Přepis: Janík Počet stran: 20 Počet příloh: 2

BEZPEČNOST INFORMACÍ

Obsah:

Rozdělovník: 1x útvar interního auditu v listinné
zaměstnanci města Vsetín v elektronické podobě

	Zpracoval	Ověřil	Ověřil	Schválil	Schválil
Odbor	Informatiky	Právní	Útvar int. auditu	pro Městský úřad	pro Městskou policii
Funkce	Vedoucí odboru	Vedoucí odboru	Vedoucí utvaru	Tajemník	Starostka
Jméno	Bc. Zdeněk Janík	Mgr. Robert Rafaj	Ing. Radmila Matochová	Ing. Karel Měřínský	Květoslava Othová
Datum					
Podpis					

Záznam o seznámení

Potvrzuji seznámení s organizační směrnicí města Vsetín č. QS 42-06, název: **Bezpečnost informací**

FUNKCE	JMÉNO A PŘÍJMENÍ	DATUM, PODPIS

1 Účel a cíl směrnice

1.1. Účelem této organizační směrnice je určit zásady ochrany informací, stanovit jednotný a jednoznačný systém odpovědnosti, vedení a řízení efektivních bezpečnostních praktik a zajistit ochranu důvěrnosti, integrity a dostupnosti informací při komunikaci uvnitř Městského úřadu Vsetín, Městské policie Vsetín a organizačních složek města Vsetína i mezi organizacemi a občany. Předmětem ochrany jsou jakékoliv nosiče údajů a informací, jako jsou např. písemné materiály a dokumenty, magnetická média – diskety i pevné disky, optická datová (paměťová) média, paměti počítačů a osobních záznamníků apod. Chráněny jsou i všechny formy přenosů údajů a informací, tedy přenosy poštovní, kurýrní, osobní, telefonické, telegrafické, faxové, datové apod.

1.2. Město Vsetín podle této směrnice buduje, zavádí, udržuje a soustavně zlepšuje dokumentovaný systém řízení bezpečnosti informací organizace (ISMS), a to v kontextu všech činností a rizik. Použitý proces je, založen na modelu PDCA.

1.3. Cílem této směrnice je zajistit soulad ochrany informací s platnými právními předpisy České republiky, příslušnými licenčními ujednáními a respektování zákonných práv občanů, organizací a pracovníků úřadu na ochranu informací.

1.4. Směrnice je zpracována v souladu s doporučeními normy pro řízení informační bezpečnosti ČSN ISO/IEC 17799:2006 „Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací" a normy pro zavádění a provoz ISMS ČSN ISO/IEC 27001:2006 „Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky".

1.5. Nedílnou součástí je zabezpečení kontroly dodržování zásad ochrany informací.

2 Oblast a rozsah platnosti

2.1. Směrnice je určena pro vnitřní potřebu MěÚ Vsetín, je závazná pro všechny uživatele IS a ICT MěÚ Vsetín. Uživateli IS a ICT MěÚ Vsetín jsou zejména zaměstnanci města Vsetín začleněni do Městského úřadu Vsetín a Městské policie Vsetín

2.2. Tato směrnice se přiměřeně vztahuje i na fyzické osoby, které jsou v obdobném nebo jiném smluvním vztahu k MěÚ (dohody o pracích konaných mimo pracovní poměr, mandátní smlouvy apod.).

2.3. Směrnice nabývá účinnosti dne 1. 4. 2010.

3 Vymezení pojmů, zkratky

3.1 Vymezení pojmů:

MěÚ

Pro účely této směrnice se pod pojmem MěÚ rozumí Městský úřad Vsetín, Městská policie Vsetín a organizační složky města Vsetína

Informační systém MěÚ
Informačním systémem se rozumí funkční celek, zabezpečující cílevědomé a systematické pořizování, zpracovávání a uchovávání informací v datových souborech, v pamětech počítačů nebo na paměťových nosičích výpočetní techniky a jejich zpřístupňování. Informační systém zahrnuje informační základnu, technické prostředky (hardware), programové prostředky (software), technologii, procedury a pracovníky.

Bezpečnost informací
Je chápána jako celek složený z jednotlivých opatření organizační bezpečnosti, zajištění ochrany aktiv, personální a fyzické bezpečnosti a bezpečnosti informačních technologií pro zajištění dostupnosti, integrity a důvěrnosti informací.
Základem prosazení informační bezpečnosti MěÚ je realizace a prosazení systému managementu bezpečnosti informací ve všech oblastech bezpečnosti.
Systém managementu bezpečnosti informací (*ISMS*) je zaveden v souladu s normou ČSN ISO/IEC 27001:2006 a je zaveden pravidelně udržovaný systém správy záznamů ISMS.
Informační bezpečnost je ve všech součástech MěÚ prosazována v souladu s deklarovaným cílem a strategií a odpovídají za ni na všech úrovních vedoucí zaměstnanci.
Se zavedeným systémem řízení jsou seznámeni **všichni** zaměstnanci města Vsetína
K údržbě a zlepšování ISMS jsou prováděny pravidelné audity informační bezpečnosti a jsou přijímána nápravná a preventivní opatření.

Aktivum
Cokoli co má pro organizaci hodnotu.

Autenticita
Vlastnost zajišťující, že identita subjektu nebo zdroje je taková, za kterou je prohlašována.

Důvěrnost
Informace je přístupná jen těm, kteří jsou oprávněni mít přístup k této informaci.

Integrita
Přesnost a kompletnost informace a metod jejího zpracování.

Dostupnost
Informace a s nimi spjatá aktiva jsou uživatelům přístupná v dob ě, kdy je požadují.

Dopad
Výsledek nežádoucího incidentu.

Bezpečnost IT
Všechny aspekty související s definováním, dosažením a udržováním důvěrnosti, integrity, dostupnosti, individuální autenticity a spolehlivosti.

Spolehlivost
Vlastnost zajišťující konzistentní zamýšlené chování a jeho výsledky.

Zbytkové riziko
Riziko které zůstává po implementaci ochranných opatření.

Riziko
Potenciální možnost, že daná hrozba využije zranitelnosti aktiv nebo skupiny aktiv a způsobí tak ztrátu nebo zničení aktiv.

Analýza rizik

Proces identifikování bezpečnostních rizik, stanovující jejich závažnost a identifikující oblasti, která vyžadují ochranná opatření.

Management rizik
Celkový proces identifikování, kontrolování a eliminování nebo minimalizování nepředvídatelných událostí.

Bezpečnostní opatření
Praxe, postup, nebo mechanizmus, který snižuje riziko.

Integrita systému
Vlastnost, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautorizované manipulace se systémem.

Hrozba
Potenciální příčina nežádoucího incidentu, který může mít následek poškození systému nebo organizace.

Zranitelnost
Zahrnuje slabé místo aktiva nebo skupiny aktiv, které může být využito hrozbou.

3.2 Zkratky

ISMS	Systém řízení bezpečnosti informací (information security management systém)
IT	Informační technologie
ICT	Informační a komunikační technologie
IS	Informační systém
HW	Hardware - technické prostředky výpočetní techniky
OI	Odbor informatiky
PDCA	Plánuj, Dělej, Kontroluj, Jednej (Plan, Do, Check, Act)
SW	Software - počítačový program, programové vybavení
MP	Městská policie

4 Odpovědnosti a pravomoci

Specifikace odpovědností a pravomocí je uvedena v matici odpovědnosti - příloha číslo 1 směrnice QS 42-03.
Odpovědnost za stav a řízení informační bezpečnosti má správce bezpečnosti informací. Za každodenní řešení problematiky informační bezpečnosti a šetření bezpečnostních incidentů je odpovědný manažer informační bezpečnosti.
Odpovědnost za zavedení a dodržování bezpečnostních opatření a spolupráci při šetření bezpečnostních incidentů nesou vedoucí zaměstnanci.
Odpovědnost za dodržování bezpečnostních opatření a ohlášení bezpečnostních incidentů nesou zaměstnanci.

5 Kritéria hodnocení rizik

Metodika hodnocení rizik v MěÚ je podrobněji uvedena v základním dokumentu Metodika hodnocení rizik informační bezpečnosti (bude dopracován).
Bezpečnostní opatření jsou vybrána na základě prováděného hodnocení rizik a požadavků zákonných a jiných norem.
Hodnocení rizik má za cíl určit možné hrozby, zranitelnosti a rizika hodnoceného systému, odhadnout ztráty, které mohou vzniknout působením hrozeb na informační aktiva zařazená do ISMS MěÚ.
Hodnocení rizik je prováděno na základě následujících kritérií:

a) stanovení hodnot informačních aktiv MěÚ z hlediska požadavků na jejich dostupnost, důvěrnost a integritu,

b) určení požadavků relevantní legislativy a požadavků vyplývajících z uzavřených smluvních vztahů,

c) určení možných dopadů identifikovaných hrozeb, reálných pravděpodobností jejich uskutečnění a určení úrovně rizik pro informační aktiva,

d) určení akceptovatelné úrovně rizika pro informační aktiva MěÚ;

e) snížení či likvidace rizik prostřednictvím pokrytí hrozeb doporučenými protiopatřeními dle ČSN ISO/IEC 17799:2006 „Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací".

Informační aktiva MěÚ byla seskupena do pěti základních skupin:

a) Centrální informační systémy a data jimi zpracovávaná;

b) Podpůrné informační systémy a data jimi zpracovávaná;

c) Personální informační systémy a data jimi zpracovávaná;

d) Infrastruktura ICT;

e) Spisy (informace v listinné formě).

Analýza rizik je aktualizována v periodě dvou let nebo v případě změn v informačních systémech a změn v požadavcích na informační bezpečnost.

6 Zásady celkové bezpečnostní politiky

6.1. Prohlášení vedení MěÚ

Vedení města Vsetína podporuje stanovené cíle a strategii bezpečnosti a ochrany informací MěÚ, MP Vsetín a organizačních složek. Vyjádřením této podpory je schválení směrnice Bezpečnost informací.
Město Vsetín vyjadřuje touto směrnicí svoji strategii trvalého zajišťování bezpečnosti a ochrany informací, jež jsou součástí řídících procesů v rámci organizační struktury města Vsetína.

6.2. Systém managementu bezpečnosti informací MěÚ

Působnost systému managementu bezpečnosti informací (ISMS) zahrnuje celý Městský úřad, Městkou polici Vsetín a organizační složky města s důrazem na jeho vykonávané činnosti a s tím související provoz informačních a komunikačních technologií.
ISMS je zavedeno na základě vymezení jeho působnosti, závěrů analýzy rizik, plánu řízení rizik a výběru vhodných opatření k zavedení informační bezpečnosti v rámci MěÚ.

6.3. Řídící dokumenty informační bezpečnosti MěÚ

Jsou jasně stanovena pravidla, kompetence a odpovědnosti v oblasti bezpečnosti IT a každý uživatel je s nimi seznámen. Jedná se o soubor interních směrnic, a metodických pokynů, obsahujících příslušná ustanovení se vztahem k IS spolu s odkazy na platné legislativní nařízení. Všechny tyto dokumenty, jsou uvedeny **v příloze B** této směrnice.

7 Organizace bezpečnosti

7.1 Bezpečnostní role

7.1.1 Správce bezpečnosti informací

Je odpovědný za rozpracování pokynů a úkolů bezpečnostních politik do podoby prováděcích předpisů a dále za stanovení správné konfigurace systémů z hlediska bezpečnosti.
Dále je odpovědný za monitorování provozu systémů, činnosti uživatelů a správců systémů a aplikací.
Je důležité, aby tato osoba měla aktuální informace a znalosti o nejnovějších bezpečnostních problémech, rizicích a řešeních.
K jeho úkolům patří:

a) dohled, vykonávaný společně s Manažerem informační bezpečnosti, nad dodržováním informační bezpečnosti,
b) nahlášení všech narušení bezpečnostní politiky a schválených bezpečnostních procedur vlastníkovi informací a Manažerovi informační bezpečnosti,
c) sestavení bezpečnostních příruček a směrnic pro jednotlivé systémy, aplikace a procesy,
d) monitorování aktivit uživatelů a správců v systémech a aplikacích,
e) vyhodnocování záznamů aktivit monitorování a poskytování souhrnných výsledků Manažerovi informační bezpečnosti,
f) přijetí operativních opatření při zjištění skutečného nebo hrozícího bezpečnostního incidentu,
g) vedení dokumentace o zjištěných bezpečnostních incidentech a jejich řešení,
h) posouzení připravovaných změn v systémech, aplikacích a procesech z pohledu bezpečnosti informací,
i) evidence a správa identifikačních předmětů (čipové karty, tokeny apod.) používaných při práci s ICT.

7.1.2 Manažer informační bezpečnosti

Je odpovědný za organizační a metodické řízení informační bezpečnosti z pohledu celého MěÚ. Definuje pravidla pro bezpečnost informací společně s vlastníky procesů a informací a Správcem bezpečnosti IT. Působí jako poradce vedení ve věcech bezpečnosti. Může rovněž provádět rizikové analýzy. Prosazuje uplatňování bezpečnostních požadavků při vývoji aplikací a změnách konfigurace. Organizuje provádění auditů informační bezpečnosti. Přijímá podněty ke zlepšení informační bezpečnosti a hlášení o bezpečnostních nedostatcích či incidentech.

Jeho důležitým úkolem je rovněž koordinace spolupráce s partnerskými organizacemi.

Úkoly Manažera informační bezpečnosti jsou zejména:

a) příprava a revize bezpečnostních směrnic s platností pro celou organizaci,
b) metodické a organizační řízení programu informační bezpečnosti v celé organizaci,
c) určení působnosti pro, správce bezpečnosti a správce systémů a aplikací,
d) sestavení Plánu informační bezpečnosti a jeho předložení vedení MěÚ,
e) dohled nad plněním úkolů stanovených v Plánu informační bezpečnost,
f) přijímaní podnětů ke zlepšení informační bezpečnosti a hlášení o bezpečnostních nedostatcích či incidentech
g) koordinace prozkoumávání bezpečnostních incidentů,
h) Organizace interních a externích auditů informační bezpečnosti.

7.1.3 Auditor informační bezpečnosti

Auditor je nezávislá osoba, uvnitř nebo vně MěÚ, která kontroluje stav informační bezpečnosti, velmi podobně jako účetní auditor kontroluje správnost účetních záznamů. Je důležité, aby auditor byl nezávislý, nezúčastněný na správě bezpečnosti.

7.2 Infrastruktura informační bezpečnosti

Cílem organizace bezpečnosti je stanovit rámec pro řízení, prosazování a kontrolu informační bezpečnosti v rámci MěÚ.

Bezpečnostní role vymezují odpovědnosti a pravomoci v rámci systému informační bezpečnosti MěÚ. Bezpečnostní role jsou přiřazeny k vybraným funkcím:

a) **řídící role** jsou přiřazeny vedoucím zaměstnancům MěÚ, Městské policie Vsetín a organizačních složek, kteří odpovídají za řízení informační bezpečnosti na svém odboru a za správu informačních aktiv,

b) **výkonné bezpečnostní role** jsou přiřazeny orgánům a osobám odpovědným za řízení informační bezpečnosti MěÚ; jedná se o bezpečnostní management,

c) **role řízení kontinuity činností jsou** přiřazeny orgánům a osobám odpovědným za správu řízení kontinuity činností MěÚ,

d) **role ve změnovém řízení** jsou přiřazeny osobám odpovědným za správu požadavků na IT MěÚ,

e) **uživatelské role** jsou přiřazeny zaměstnanci, který v rozsahu přidělených pravomocí využívá informace MěÚ.

Obsazení rolí uvedených pod písmeny a), b) a c) je zajištěno následující organizační strukturou:

- Manažer informační bezpečnosti – tajemník MěÚ,
- Správce informační bezpečnosti – vedoucí odboru informatiky,
- Auditor informační bezpečnosti.

Konkrétní obsazení těchto rolí je uvedeno v *příloze A* této směrnice.

I ostatní zaměstnanci města Vsetína jsou pak v určité roli z hlediska bezpečnosti IT. Těmito rolemi jsou: vlastník procesů a dat, dodavatel systémů a služeb, projektant systémů a aplikací, správce systému, správce aplikace a uživatel.
Veškeré nově zaváděné technologie zpracovávající informace a soukromé prostředky zpracovávající pracovní informace podléhají schvalovacímu procesu a musí obsahovat řešení informační bezpečnosti. Za schválení odpovídají příslušní vedoucí zaměstnanci MěÚ.
Opatření organizace bezpečnosti zahrnují řízení informační bezpečnosti v rámci MěÚ s důrazem na přidělení odpovědností a koordinaci informační bezpečnosti, definování schvalovacího procesu prostředků IT, zajištění ochrany informací ve smlouvách s externími stranami a zajištění spolupráce s externími stranami v oblasti informační bezpečnosti;

7.3 Určení zodpovědnosti

Zodpovědnost za ochranu jednotlivých aktiv a provádění procesů je jasně definována. Celkovou zodpovědnost za vývoj, implementaci a podporu bezpečnostních opatření má Manažer informační bezpečnosti, za jejich realizaci v systémech ICT pak Správce bezpečnosti informací. Zodpovědnost za jednotlivá aktiva však zůstává jejich vlastníkům nebo příslušným vedoucím. Proto jsou také oni odpovědni za každodenní dodržování bezpečnostních opatření, a to i v případě, že prováděním bezpečnostních opatření pověřili jinou osobu nebo organizaci.

7.4 Bezpečnost přístupu třetích stran

7.4.1 Typy přístupu

Zvláště důležité je správně posoudit typ přístupu třetí strany. Rizika plynoucí z přístupu přes síťové propojení jsou zásadně odlišná od rizik plynoucích z fyzického přístupu. Typy přístupu mohou tedy být rozděleny na:

- Fyzický přístup, tj. do budov, kanceláří, technologických prostor,
- logický přístup, tj. k databázím, informačním systémům.

7.4.2 Bezpečnostní aspekty smluv s třetími stranami

Všechny přístupy třetích stran k neveřejným informacím MěÚ jsou smluvně ošetřeny nebo je jiným způsobem zajištěna ochrana těchto informací. Vyplývající rizika musí být ještě před umožněním takového přístupu identifikována a náležitě ošetřena.
Příkladem takového přístupu může být dodávka nového informačního systému (popis procesů, specifikace, data pro testování atd.) stejně jako přístup úklidové nebo bezpečnostní služby do prostor budovy MěÚ.
Smlouvy musí obsahovat z hlediska bezpečnost:

- Obecná pravidla bezpečnosti,

- ochranu aktiv,
- opatření umožňující ukončení nebo změnu smluvního vztahu bez bezpečnostního rizika,
- pravidla pro utajení, nešíření informací, neporušení integrity a dostupnosti aktiv,
- specifikaci každé zpřístupněné služby a její úrovně,
- v případě potřeby podmínky vzájemného přechodu, příp. odchodu personálu třetí strany,
- konkrétní smluvní závazky,
- odpovědnosti smluvené a vyplývající z právních norem,
- ochranu duševního vlastnictví a autorského práva,
- podmínky, metody a oblasti přístupu,
- právo monitorovat a povolovat aktivity uživatele,
- právo auditovat smluvní povinnosti,
- pravidla pro řešení havarijních situací,
- odpovědnost za práci a vlastní produkty,
- systém hlášení a komunikace v oblasti bezpečnosti,
- pravidla procesu řízení změn,
- pravidla školení.

8 Řízení a klasifikace aktiv

8.1 Odpovědnost za aktiva

Cílem identifikace a ohodnocení aktiv MěÚ je zabezpečit jejich přiměřenou ochranu.
Důležitá informační aktiva MěÚ jsou evidována v rámci ISMS, je stanovena odpovědnost za jejich správu a je určen jejich vlastník. Za evidenci aktiva odpovídá jejich vlastník.
Vlastníkem aktiva je zaměstnanec MěÚ, který nese za aktivum odpovědnost. Pro všechna důležitá aktiva musí vlastníci určovat přiměřená bezpečnostních opatření.
Uživatelem aktiva je zaměstnanec, jenž aktivum používá ke své práci. Uživatel aktiva je povinen dodržovat bezpečnostní opatření pro zacházení s aktivem stanovená vlastníkem.

8.2 Klasifikace informací

Cílem klasifikace informací je zajištění přiměřenosti ochrany informačních aktiv MěÚ. Informace jsou klasifikovány na základě jejich potřebnosti a důležitosti pro zabezpečení činností MěÚ. Klasifikace probíhá v rámci analýzy rizik.
Každá informace, se kterou je nakládáno v rámci MěÚ má přiřazen klasifikační stupeň. Za obecné stanovení klasifikačního stupně k informačním aktivům odpovídá vlastník aktiva. Za přidělení konkrétního stupně klasifikace k informaci (v elektronické i listinné formě) odpovídá původce (autor, zhotovitel) informace.
Stupeň klasifikace MěÚ charakterizuje důležitost ochrany informace MěÚ a upřesňuje způsob, jak s ní lze nakládat. Soubor klasifikačních stupňů tvoří klasifikační schéma.

Pro účely klasifikace informací MěÚ je stanoveno následující klasifikační schéma:

- **Neveřejná** data. Jsou to data, která souvisí se strategií MěÚ. Data, která MěÚ spravuje, aktualizuje a rozvíjí ve svém informačním systému ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění změn a doplňků, a dalších zákonů (viz. výše). Tato data jsou dále členěna.
- **Veřejná data**. Data, která mohou být veřejně přístupná, aniž by byl porušen zákon č 101/2000 Sb., o ochraně osobních údajů, v platném znění, či jiný právní předpis.

Za účelem ochrany informací MěÚ jsou stanovena pravidla pro zacházení s informacemi MěÚ. Tato pravidla upřesňují zacházení s informacemi v souladu s jejich klasifikací v dokumentech, počítačových systémech, sítích, mobilních počítačích, hlasové komunikaci obecně, v multimédiích, v poštovním styku a při použití faxů.

9 Personální bezpečnost Prohlášení

Personální bezpečnost je součástí širší personální politiky a jejím cílem je pokrytí hrozeb představovaných zaměstnanci, dodavateli, zákazníky, nezkušenými uživateli, hackery, profesionály a špióny. Cílem je rovněž ochrana vlastních zaměstnanců. Podrobné pokyny týkající se pracovně právních vztahů jsou uvedeny v Pracovním řádu a ve směrnici QS 62-01 Personální záležitosti a zajištění kvalifikace.
Dosahování, udržování a zvyšování bezpečnostního povědomí bude prováděno v souladu a podle postupů, definovaných po stránce odborné (bezpečnost informací a informačních systémů) Manažerem informační bezpečnosti, po stránce vzdělávacího procesu Personálním pracovníkem MěÚ. Ve zvláštních případech bude tato problematika zmiňována i v rámci programů, definovaných přímo vedoucími zaměstnanci MěÚ.

10 Fyzická bezpečnost a bezpečnost prostředí

10.1 Základní cíle

Cílem fyzické bezpečnosti je chránit aktiva MěÚ a prostředí, ve kterém se nacházejí, před možnými riziky narušení a také chránit bezpečnost a zdraví zaměstnanců města. Zahrnuje především následující úkoly:

- předcházet neautorizovanému přístupu, poškození a zásahům do prostor, technologií a informací MěÚ,
- předcházet ztrátě, poškození a/nebo prozrazení aktiv MěÚ a dále též předcházet přerušení činností MěÚ,
- předcházet prozrazení nebo zcizení informací a prostředků pro zpracovávání informací v MěÚ,
- chránit bezpečnost a zdraví zaměstnanců MěÚ v souladu se zákoníkem práce a předpisy vztahujícími se k problematice BOZP a požární ochrany.

Bezpečnostní zóny jsou chráněny přiměřenými kontrolami vstupu tak, aby bylo zajištěno, že osoba, která vstupuje do těchto prostor MěÚ, má ke vstupu oprávnění.

10.2 Klasifikace oblastí

Cílem klasifikace oblastí je rozdělení prostor MěÚ do lokalit, ve kterých platí různá bezpečnostní pravidla. Vedoucí odborů jsou zodpovědní za to, že veškeré prostory v MěÚ jsou zařazeny do odpovídající lokality.
Prostory MěÚ jsou rozděleny na:

- **Lokality neveřejné.** Serverovny a datová centra, prostory s výpočetní a spojovací technikou, bezpečnostními zařízeními nebo se záložními systémy, archivy, spisovny, jiné prostory, které nejsou určeny pro veřejnost.
- **Lokality pro veřejnost – přístupné s omezením .** – kanceláře, zasedací místnosti
- **Lokality pro veřejnost** Jsou to místnosti s přepážkami na kontaktních místech, podatelny, chodby a schodiště atd.

10.3 Kontrola vstupu osob

Vstup do **objektů MěÚ mimo míst určených pro veřejnost mají** povolen pouze zaměstnanci MěÚ. Přístup jiných osob do budovy je upraven příkazem tajemníka.

10.4 Bezpečnost zařízení

Zařízení MěÚ je libovolný technický, technologický nebo softwarový prostředek, který se používá pro zpracování, manipulaci či ukládání informací MěÚ. Zařízení MěÚ (včetně zařízení, která se používají mimo objekty MěÚ) jsou fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů.
Zařízení zpracovávající informace MěÚ jsou umísťována tak, aby se minimalizovalo riziko působení vnějších vlivů a neautorizovaného přístupu.
Zařízení zpracovávající informace MěÚ jsou fyzicky chráněna v závislosti na stupni klasifikace informací jimi zpracovávaných. Zařízení MěÚ jsou též chráněna před výpadkem elektrického proudu nebo jinými anomáliemi napájení.
Pro správnou a bezpečnou funkci všech používaných zařízení a zajištění stálé dostupnosti a integrity činnosti MěÚ, je pravidelně a v souladu s pokyny výrobce prováděna údržba zařízení.
Napájecí, telekomunikační kabely a jiné kabely pro technická zařízení jsou přiměřeně chráněny proti odposlechu nebo poškození.
Oprava nebo likvidace zařízení, případně nosiče informací na nichž byly zpracovávány chráněné informace MěÚ je prováděna takovým způsobem, aby zaměstnancem, nebo zaměstnancem třetí strany nebylo možné získat z tohoto zařízení informace, které na něm byly zpracovávány, a s nimiž tito zaměstnanci nejsou oprávněni se seznamovat.
Specifické nosiče, zejména určené pro archivaci jsou uloženy minimálně ve dvou od sebe vzdálených lokalitách v zabezpečeném prostoru.
Zařízení a aktiva MěÚ nesmějí být přemisťována bez schválení odpovědnou osobou a bez evidence.
Jsou organizovány namátkové kontroly za účelem zjištění nedovoleného pohybu majetku a aktiv, tyto kontroly provádí vedoucí zaměstnanci.

11 Řízení komunikací a provozu

11.1 Provozní postupy a odpovědnosti

Řízení provozu tvoří soubor opatření spojených s řízením provozu informačních technologií MěÚ (dále též IT MěÚ). Provoz IT MěÚ se řídí postupy, požadavky a pravidly, která jsou řádně popsána v rámci směrnice QS 42-03 provozování IT. Za prosazení bezpečnostních požadavků v oblasti řízení provozu IT MěÚ odpovídá vedoucí odboru informatiky.
V rámci IT MěÚ je zajištěno odpovídající oddělení vývojového, testovacího a provozního prostředí s cílem předcházet provozním problémům způsobovaným vývojovými a testovacími aktivitami. Jako součást oddělení těchto aktivit je definován proces uvedení změny do provozního prostředí.

11.2 Nově zaváděné technologie

Veškeré nově zaváděné technologie zpracovávající informace a soukromé prostředky zpracovávající pracovní informace podléhají schvalovacímu procesu a musí obsahovat řešení informační bezpečnosti. Pracovníci používající tyto prostředky mají povinnost oznámit tyto skutečnosti příslušnému vedoucímu zaměstnanci. Za schválení odpovídají příslušní vedoucí zaměstnanci MěÚ.

11.3 Ochrana proti škodlivým a automaticky spouštěným programům

V rámci MěÚ je užíváno pouze schválené legální programové vybavení z důvěryhodných zdrojů. Užívání programového vybavení je kontrolováno.
Je zajištěno trvalé monitorování provozu důležitých částí IS MěÚ z hlediska aktivit potenciálních škodlivých programů. Možnost zavedení škodlivých programů do IS je minimalizována stanovením a prosazením vhodných postupů pro jejich odhalování a prevenci. Pro případ napadení škodlivým programem jsou stanoveny postupy a pravidla, se kterými jsou seznámeni všichni uživatelé IS MěÚ.

11.4 Správa provozního programového vybavení a zálohování

Informace nezbytné pro MěÚ a pro provoz IS jsou, pro případ bezpečnostního incidentu, zajištěny uceleným systémem zálohování a obnovy ze záloh. Tento systém je navržen v souladu s potřebami řízení kontinuity činností MěÚ. *Bližší povinnosti stanoví vnitřní směrnice QS 42-03 provozování IS, používání výpočetní techniky a ICT*

11.5 Postupy pro manipulaci s informacemi

Bezpečnost při zacházení s médii v oblastech správy vyměnitelných počítačových médií, likvidace nosičů dat, postupů pro manipulaci s informacemi a bezpečnost systémové dokumentace je řešena dle ustanovení směrnice pro oblast řízení a klasifikace aktiv a pro oblast fyzické bezpečnosti a bezpečnosti prostředí.

11.6 Výměna informací a programů

Výměna informací s externími subjekty je **přesně specifikována** včetně upřesnění bezpečnostních požadavků, schválena a ošetřena **na úrovni smluvního vztahu**.
Jsou stanoveny zásady, pravidla a postupy užívání elektronické pošty a jsou s nimi seznámeni všichni uživatelé IS tak, aby nedošlo k ohrožení provozu IS a zájmů MěÚ.

12 Řízení přístupu

12.1 Požadavky na řízení přístupu

Řízení přístupu je soustava opatření zaměřená na ochranu a kontrolu přístupu uživatelů k informacím a službám informačních systémů MěÚ. V rámci MěÚ je vytvořen, prověřován, udržován a prosazován systém řízení přístupu uživatelů IS MěÚ (dále též řízení přístupu),

který se opírá o stanovené postupy a činnosti a o organizační strukturu danou stanovením rolí, pravomocí a odpovědností.
Přidělování rolí a konkrétních přístupových práv jednotlivým uživatelům je prováděno na základě žádostí nadřízených vedoucích zaměstnanců (formulář QF 62-01-11).
Za stanovení politiky řízení přístupu a její prosazování v rámci jednotlivých IS MěÚ odpovídá manažer informační bezpečnosti. Za řízení přístupu v rámci jednotlivých IS odpovídají zaměstnanci pověření výkonem role správce aplikace.

12.2 Řízení přístupu k aplikacím
Řízení přístupu k aplikacím je řešeno v souladu s obecným řízením přístupu k IS s důrazem na prosazení mechanizmů omezujících přístup k informacím a funkcím aplikací v souladu s požadavky na řízení přístupu.

12.2.1 Časové omezení práce s aplikacemi
Jsou zavedeny procedury a mechanismy zajišťující, aby neaktivní pracovní stanice pracující s informačními systémy obsahujícími neveřejné informace byly odpojeny v případě nečinnosti po uplynutí předem stanovené doby od tohoto informačního systému. Např. aktivací spořiče obrazovky se zamknutím stanice, případně automatickým odhlášením uživatele.

12.3 Monitorování přístupu k systému a jeho použití
V rámci IS MěÚ jsou pro jednotlivé části stanoveny a prosazovány způsoby a postupy monitorování včetně rozsahu a ochrany pořizování auditních záznamů a jejich zálohování a archivace.
Auditní záznamy a záznamy zjištěných bezpečnostních událostí jsou pravidelně kontrolovány a vyhodnocovány.
Správnost časových údajů v auditních záznamech je zajištěna synchronizací času IS MěÚ.

12.4 Mobilní výpočetní prostředky a práce na dálku
Použití mobilních zařízení pro práci s IS MěÚ na dálku a vzdálený přístup k vnitřním IS MěÚ podléhají posouzení a schválení tajemníkem a vedoucím odboru informatiky a jsou řádně dokumentovány s ohledem na možná rizika

12.5 Bližší povinnosti zaměstnanců při řízení přístupu upravuje směrnice QS 42-03, *provozování IS, používání výpočetní techniky a ICT*

13 Pořízení, vývoj a údržba informačních systémů

Cílem opatření vývoje a údržby IS MěÚ je prosadit informační bezpečnost do celého životního cyklu užívaných IS od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu. Implementace součástí IS MěÚ a návrh jejich změn je v MěÚ spojen se stanovením vhodných bezpečnostních požadavků.

13.1 Bezpečnostní požadavky systémů
Provádění správy provozního prostředí zahrnuje provozování prověřeného a otestovaného programového vybavení, aktualizaci programového vybavení, vedení a vyhodnocování auditních záznamů, archivaci předešlých verzí programového vybavení a užívání nástrojů a postupů doporučených výrobcem (dodavatelem) programového vybavení.

13.2 Bezpečnost procesů vývoje a podpory

V rámci MěÚ podléhají veškeré změny informačních systémů, prostředí a aplikací postupům změnového řízení. V rámci změnového řízení je definován způsob provádění změn, vymezeny role, stanoven způsob dokumentace změn a popsány základní změnové činnosti.
Změna IS MěÚ je řízená úprava prostředí IS MěÚ oproti standardní dokumentované podobě, která mění chování IS jako celku nebo jeho částí.
Veškeré změny a provozní události jsou dokumentovány a zaznamenávány. Dokumentaci vývoje a údržby tvoří dokumentace změn, smluvní dokumentace a dokumentace kontrol.

14 Řízení kontinuity činností a správa bezpečnostních incidentů

14.1 Aspekty řízení kontinuity činností

Cílem je zabránit přerušení činností MěÚ a chránit MěÚ před následky závažných chyb, katastrof a nepředvídatelných událostí nebo tyto následky minimalizovat. Důraz je položen na ochranu kritických procesů MěÚ souvisejících s hlavními informačními systémy MěÚ.
V rámci MěÚ je vytvořen, prověřován, udržován a prosazován proces řízení kontinuity činností MěÚ (dále jen řízení kontinuity), který se opírá o definované postupy, činnosti a organizační strukturu.

14.2 Správa bezpečnostních incidentů

Cílem správy bezpečnostních incidentů je zajistit, aby incidenty a bezpečnostní slabiny byly komunikovány způsobem, který umožní včasnou nápravu s využitím formalizovaného a obecně známého postupu.
Bezpečnostní incident tvoří jedna nebo série nežádoucích nebo neočekávaných událostí informační bezpečnosti, které mají podstatnou šanci na kompromitaci podnikatelských operací a ohrožují informační bezpečnost.
Pro zajištění zpětné vazby při řešení bezpečnostních incidentů je prováděno jejich vyhodnocení. Vyhodnocení bezpečnostních incidentů je vzato v úvahu při revizi směrnice a plánů řízení kontinuity činností.

14.3 Kontinuita činností a analýza dopadů

Za celkové řízení a koordinaci řízení kontinuity v rámci MěÚ odpovídá tajemník MěÚ, vedoucí odborů za oblast v jejich gesci. Tajemník MěÚ svolává v případě potřeby Krizový štáb.
Zásady a opatření řízení kontinuity v oblasti IT naplňuje a prosazuje správce informační bezpečnosti.
Proces řízení kontinuity IT je rozpracován, popsán a dokumentován v rámci dokumentace řízení kontinuity, která zahrnuje havarijní plán (plán řízení kontinuity činností a seznam kontaktů) a plán obnovy (postup obnovy jednotlivých aktiv).

14.4 Testování, udržování a přezkoumávání plánů kontinuity

Systém řízení kontinuity je pravidelně revidován a aktualizován tak, aby byl zajištěn jeho soulad s potřebami MěÚ a byly odstraněny zjištěné nedostatky. Za údržbu systému řízení kontinuity odpovídá manažer informační bezpečnosti. Revize řízení kontinuity je provedena v případě potřeby, minimálně však 1x ročně.

15 Shoda s požadavky

15.1 Shoda s právními normami

Cílem je vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.
Pro zabezpečení informací MěÚ jsou jednoznačně definovány a zdokumentovány všechny relevantní zákonné a smluvní požadavky. MěÚ se řídí především zákony a nařízeními v oblastech obchodně právní, pracovně právní, občansko právní, trestní a správní.
Zvláštní pozornost věnují vedoucí zaměstnanci MěÚ dodržování ustanovení zákonů o ochraně duševního vlastnictví (především zákon č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským – autorský zákon), a ustanovením zákona č. 101/2000 Sb. o ochraně osobních údajů v platném znění.
Zajištění souladu s legislativou na ochranu osobních údajů dle zákona č.101/2000 Sb. v rámci MěÚ zajišťuje Právní odbor MěÚ. Právní odbor a manažer informační bezpečnosti poskytuje doporučení vedoucím zaměstnancům, uživatelům, třetím stranám a spolupracujícím organizacím k ochraně osobních údajů.
Prostředky pro zpracování informací MěÚ jsou provozovány pouze pro plnění služebních úkolů v rámci MěÚ. Jakékoliv použití těchto prostředků mimo pracovní rozsah, bez schválení vedoucím zaměstnancem, je považováno za zneužití těchto prostředků.
Použití služebního počítače pro neoprávněné účely je považováno za porušení pracovní kázně. Všichni uživatelé jsou obeznámeni s přesným rozsahem jejich přístupu. Popis činnosti, postupů a přístupů je uveden ve směrnici QS 42-03.

15.2 Posouzení bezpečnostní politiky a technické shody

Cílem posouzení bezpečnostní politiky a technické shody je zajistit shodu systémů se směrnicí a přijatými normami. Povinností všech vedoucích zaměstnanců MěÚ, je vést své podřízené k dodržování bezpečnostních zásad a opatření ISMS.
K zajištění plného souladu bezpečnostních zásad informační bezpečnosti a technických komponent systémů MěÚ se všemi technickými normami, s doporučením výrobců, případně s jinými technickými požadavky, je prováděna pravidelná kontrola shody.

15.3 Hlediska auditu systému

Cílem zabezpečení auditu informační bezpečnosti a auditu provozovaných informačních systémů je zajistit ochranu provozních systémů, IS a auditních nástrojů v průběhu i po skončení auditu.
Auditní požadavky a činnosti zahrnující kontrolu informační bezpečnosti a IS MěÚ jsou plánovány a schváleny, tak aby se minimalizovalo riziko narušení činností MěÚ.
Záznamy o provedených auditech jsou ukládány odděleně od ostatní dokumentace a jsou klasifikovány v závislosti na klasifikaci auditovaných informací MěÚ.

16 Závěrečná ustanovení

16.1 Kontrola dodržování ustanovení směrnice

Vedoucí zaměstnanci zajistí kontrolu plnění povinností vyplývajících z ustanovení směrnice v mezích své působnosti (majetek, aktiva).
Vedoucí zaměstnanci zajistí, aby byli se směrnicí seznámeni všichni zaměstnanci MěÚ.
Porušení zásad, postupů a pravidel informační bezpečnosti MěÚ zaměstnancem je považováno za porušením pracovní kázně a může být důvodem k rozvázání pracovního poměru.

16.2 Revize směrnice

Revize tohoto dokumentu je provedena v případě potřeby, minimálně však jednou ročně.

Za zpracování, prosazení, údržbu a revize dokumentu odpovídá manažer informační bezpečnosti MěÚ.

16.3 Audit směrnice

K prověření shody ustanovení tohoto dokumentu s reálným stavem v rámci MěÚ se provede audit.
Provádění interních i externích auditů se řídí vnitřními předpisy MěÚ.

Příloha 1: Role a odpovědnosti

Nositeli povinností a zodpovědností, vyplývajících z této směrnice jsou osoby, jimž tato povinnost vyplývá z funkčního zařazení v organizační struktuře MěÚ, nebo jimž to stanovují jiné bezpečnostní dokumenty nebo koncepty uvedené v této směrnici.
Pro účely tohoto materiálu je uživatelem míněn každý, kdo pracuje s informačními aktivy MěÚ v MěÚ to bez ohledu na funkční (pracovní) zařazení. Uživateli jsou tedy např. zaměstnanci MěÚ, externí konzultanti, externí pracovníci, pracovníci externích společností, které jsou ve smluvním vztahu k MěÚ. Všichni tito uživatelé, ať již dat, informací či prostředků informačního systému, jsou vázáni interními předpisy, směrnicemi, standardy a normami a jsou povinni respektovat všechna ustanovení směrnice a z ní vycházejících opatření a směrnic.

Role a odpovědnosti v oblasti bezpečnosti

obecné role

a) osoba odpovědná za využívání ICT v úřadu (gestor) – starosta města,

b) provozovatel - ve smyslu zákona č. 128/2000 Sb. – město Vsetín,

c) systémový správce (OS Windows, Linux),

d) správce aplikací

e) správce účtů,

f) uživatel – viz výše.

Body c - e zastávají pověření zaměstnanci odboru informatiky

bezpečnostní role

a) manažer informační bezpečnosti, tj. tajemník

b) správce informační bezpečnosti, tj. vedoucí odboru IT

c) auditor informační bezpečnosti, tj. pracovník útvaru interního auditu

Příloha 2: Řídící dokumenty informační bezpečnosti

Dokumenty určené pro všechny zaměstnance

- **Bezpečnost informací** MěÚ (tento dokument) definuje hlavní bezpečnostní cíle, stanovuje základní zásady informační bezpečnosti a určuje pravomoci a odpovědnosti pro její řízení.
- **Směrnice pro uživatele výpočetní techniky** popisuje základy správného používání počítačového vybavení v MěÚ pro uživatele.
- **Směrnice pro nakládání s osobními údaji** upravuje postup při zpracování a ochraně osobních údajů zpracovávaných v podmínkách MěÚ.

Dokumenty určené pro bezpečnostní management:

- **Metodika hodnocení rizik informační bezpečnosti** obsahuje metodiku hodnocení rizik a popisuje jeden cyklus managementu rizik v oblasti bezpečnosti informací.
- **Analýza bezpečnostních rizik IT/IS – doporučená opatření** výběr opatření ke zvládání rizik, identifikuje a hodnotí rizika.