Mesto Malacky, Radlinského 2751/1, 901 01 Malacky

Metodika manažmentu rizík pre oblasť informačnej bezpečnosti mesta Malacky

Verzia:	0.1
Počet strán / príloh:	33/2
Dátum účinnosti:	01.08.2011
Vypracoval:	ATEMSEC, a.s.

Obsah

Skratky

IS	Informačný systém
MsÚ	Mestský úrad
SMIB	Systém riadenia informačnej bezpečnosti

1 Úvod

Ministerstvo financií Slovenskej republiky v súlade so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy, Výnosom z 9. júna 2010 č. 312/2010 o štandardoch pre informačné systémy verejnej správy a metodickým pokynom k tomuto výnosu vyžaduje zavádzanie a dodržiavanie štandardov týkajúcich sa bezpečnosti informačných systémov verejnej správy (§28 až §42 z Výnosu 312/2010). V súvislosti so spomínanými legislatívnymi úpravami bol vypracovaný tento dokument, ktorý popisuje proces manažmentu rizík pre oblasť informačnej bezpečnosti (ďalej len „manažment rizík“) a definuje prístup mesta Malacky k tomuto procesu.

V rámci tohto dokumentu je popísaný systém manažmentu rizík založený na identifikácii, analýze a hodnotení rizík spojených s informačnou činnosťou prostredníctvom informačných systémov mesta Malacky a ohrození aktív. Základom pre implementáciu systému manažmentu rizík je preto analyzovanie informačných systémov mesta Malacky, určenie vzájomných závislostí a prepojení procesov zabezpečujúcich výkon správy, informačných systémov, prostredníctvom ktorých sa procesy vykonávajú a aktív, ktoré sú nevyhnutné pre existenciu a funkčnosť príslušných informačných systémov a tiež identifikácia a ohodnotenie zraniteľných miest a hrozieb, ktoré majú potenciál poškodiť alebo zničiť aktíva.

Mestom Malacky sa pre účely tohto dokumentu rozumie výkonný orgán mesta – Mestský úrad (a jeho organizačné zložky) a poriadkový orgán mesta – Mestská polícia.

1.1 Cieľ

Cieľom tohto dokumentu je definovať metodiku manažmentu rizík pre oblasť informačnej bezpečnosti, prostredníctvom ktorej bude implementovaný jednotný postup riadenia a monitorovania rizík v súvislosti s informačnými systémami v rámci mesta Malacky.

1.2 Základné pojmy

Informácia je správa, údaj, hodnota, fakt, oznámenie o určitej udalosti, jave, činnosti alebo iné dáta, ktoré sa ďalej spracúvajú. Je tak označovaný aj druh poznania alebo správy, ktorý možno použiť v prospech prijatia rozhodnutia alebo zlepšenia určitej činnosti.

Informačný systém je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických a programových prostriedkov, ktoré sú súčasťou informačného systému.

Informačná činnosť je získavanie, poskytovanie a sprístupňovanie údajov, zhromažďovanie, spracúvanie, prenos, ukladanie, archivácia a likvidácia údajov; informačnú činnosť vykonáva mesto Malacky ako správca, resp. prevádzkovateľ informačného systému prostredníctvom procesov pokrývajúcich výkon jednotlivých úsekov správy.

Aktívum je programové vybavenie, technické zariadenie, poskytované služby, kvalifikované osoby, dobré meno a informácie, dokumentácia, zmluvy a iné skutočnosti, ktoré považuje mesto Malacky za citlivé.

Hrozba je okolnosť alebo udalosť (úmyselná alebo náhodná), ktorá má potenciál poškodiť alebo zničiť informačný systém alebo akýkoľvek jeho prvok.

Zraniteľnosť je vlastnosť aktíva, cez ktorú sa hrozba môže prejaviť.

Bezpečnostný incident je úmyselné využitie zraniteľného miesta k spôsobeniu škôd/strát na aktívach informačného systému, alebo neúmyselné vykonanie akcie, ktorej výsledkom je škoda na aktívach.

Riziko je možnosť, že zraniteľnosť v systéme ovplyvní overenie alebo dostupnosť, pravosť, integritu alebo dôvernosť spracúvaných alebo prenesených údajov, ako aj vážnosť dopadu úmyselného alebo neúmyselného využitia takejto zraniteľnosti. Riziko tak predstavuje funkciu aktív (A), hrozieb (T) a zraniteľných miest (V).

Akceptovateľné riziko je taká hodnota rizika, ktorú je mesto Malacky schopné, resp. ochotné znášať.

Dôvernosť je vlastnosť, že informácia nie je dostupná alebo prístupná neautorizovaným jednotlivcom, entitám, alebo procesom.

Integrita je vlastnosť, že informácie neboli zmenené alebo zničené neautorizovaným spôsobom.

Dostupnosť je zaistenie, že autorizovaní užívatelia majú v prípade požiadavky prístup k informáciám a aktívam.

Analýza rizík je proces ktorý zahrňuje identifikáciu a ohodnotenie aktív, identifikáciu a ohodnotenie hrozieb a zraniteľných miest informačného systému.

Proces manažmentu rizika je systematická aplikácia politiky, postupov a praktík mesta Malacky na úlohy, ktoré určujú súvislosti, identifikujú, analyzujú a hodnotia riziko, zaoberajú sa rizikom, monitorujú a oznamujú ho.

2 Manažment rizík

Manažment rizík je kľúčovým nástrojom pre systematické riadenie bezpečnosti informačných systémov. Dôkladná znalosť skutočných rizík v súvislosti s informačnými systémami rozhoduje o výbere a presadzovaní vhodných bezpečnostných opatrení, ktoré sú schopné znížiť možnosť výskytu, resp. rozsah negatívnych dopadov. Manažment rizík je preto základom pre každý systém riadenia informačnej bezpečnosti.

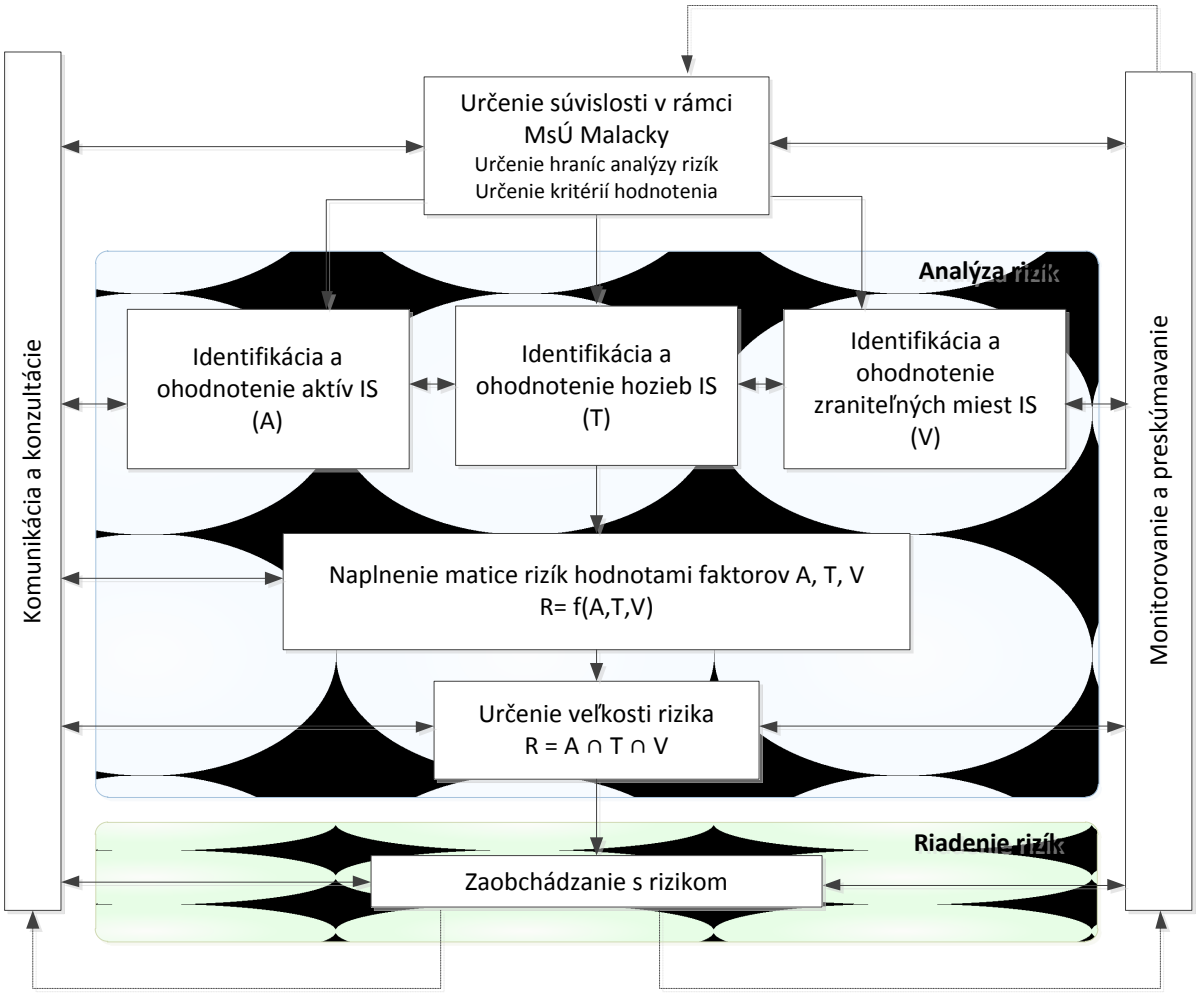
Mesto Malacky si uvedomuje významnosť procesu manažmentu rizík a pod týmto termínom chápe systematickú koordináciu činností zameraných na znižovanie rizík na akceptovateľnú úroveň. Manažment rizík sa preto prenáša do cieľov a úloh mesta Malacky, pričom priraďuje zodpovednosť konkrétnym zamestnancom, ktorí sú definovaní v rámci bezpečnostnej politiky informačných systémov. Mesto Malacky si stanovuje manažment rizík ako integrálnu súčasť riadiacej praxe a ako taký musí byť implementovaný na každom stupni v rámci organizácie.

V užšom význame mesto Malacky chápe manažment rizík ako proces na základe, ktorého sa dosahuje a udržuje primeraná úroveň dôvernosti, dostupnosti, integrity, autentickosti a spoľahlivosti údajov, ktoré sú zhromažďované, spracovávané, prenášané, sprístupňované a archivované v rámci informačných systémov mesta Malacky. Na základe uvedeného chápania manažmentu rizík, mesto Malacky stanovilo nasledovné základné funkcie manažmentu rizík:

- identifikovanie a analyzovanie informačných systémov, informačných procesov a súvisiacich aktív,
- identifikovanie a analyzovanie hrozieb pôsobiacich na informačné systémy a jeho prvky,
- identifikovanie a analyzovanie zraniteľných miest v rámci informačných systémov, informačných procesov a súvisiacich aktív,
- analýza a ohodnotenie rizík súvisiacich s informačnými systémami, informačnými procesmi a ich aktívami,
- špecifikovanie vhodných protiopatrení na základe vykonanej analýzy rizík,
- monitorovanie zavádzania a fungovania protiopatrení, ktoré sú nevyhnutné na efektívnu ochranu informačných systémov a ich aktív,

- monitorovanie vyhodnotených rizík, ktoré boli označené ako akceptovateľné alebo zostatkové v rámci analýzy rizík,
- včasne reagovanie na odhalené bezpečnostné incidenty.

Základné funkcie manažmentu rizík informačných systémov mesta Malacky sa napĺňajú prostredníctvom systematickej aplikácie jednotlivých procesov, ktoré sú znázornené na obrázku Obrázok 1.



Obrázok 1 Proces manažmentu rizík

Proces manažmentu rizík sa skladá z dvoch kľúčových častí, a to z analýzy rizík informačných systémov a riadenia rizík. Analýza rizík vytvára predpoklady na vyhodnotenie rizík, ktoré mesto Malacky nie je ochotné akceptovať z pohľadu jeho činnosti a bezpečnostných požiadaviek a proces riadenia rizík, vytvára predpoklady na minimalizáciu neakceptovateľných rizík prostredníctvom prijímania rôznych preventívnych opatrení. Ďalšie procesy manažmentu rizík ako proces stanovenie súvislosti, proces komunikácie a konzultácií

či proces monitorovania a preskúmavania vytvárajú nevyhnutný predpoklad naplnenia cieľa procesu analýzy rizík, ale aj procesu zaobchádzania s rizikami.

Proces komunikácie a konzultácií tvorí základný zdroj informácií nevyhnutných pri všetkých procesoch manažmentu rizík.

Proces monitorovania a preskúmavania je zdrojom preverovania a hodnotenia prijatých preventívnych opatrení z pohľadu ich efektívnosti a účinnosti, ale taktiež je zdrojom preverovania a hodnotenia akceptovateľných rizík mesta Malacky, pretože tieto riziká sa za určitých podmienok môžu stať rizikami neakceptovateľnými.

Proces manažmentu rizík mesta Malacky je kontinuálnym procesom, ktorý je zabezpečovaný implementáciou bezpečnostnej politiky, príslušných smerníc a nariadení v rámci všetkých dotknutých orgánov mesta.

2.1 Určenie súvislostí

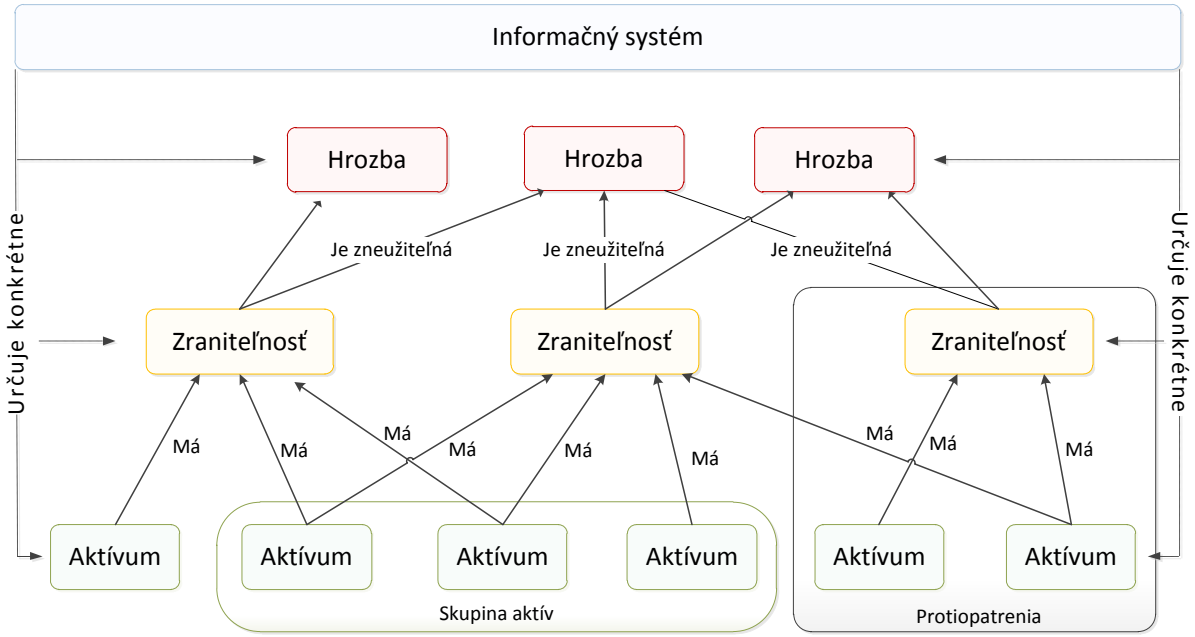
Určenie súvislostí manažmentu rizík (Obrázok 1) vzhľadom na pôsobnosť mesta Malacky vychádza zo základných požiadaviek, ktoré sú zhrnuté do dvoch základných okruhoch, a to:

- povinnosť mesta vykonávať činnosť v súlade s legislatívou SR,
- potreba ochrany záujmov mesta.

Tieto základné okruhy určovania súvislostí odzrkadľujú východiská, ktoré sú základom primárnych funkcií manažmentu rizík. To znamená, že zohľadňujú aktuálne legislatívne požiadavky, z ktorých mestu Malacky vyplývajú povinnosti ich napĺňania a zapracovania do vnútorných činností. Okrem analyzovania právneho prostredia je potrebné analyzovať i vnútorné prostredie mesta vzhľadom na nevyhnutné informácie a informačné systémy zabezpečujúce základné ciele a chod mesta.

Základné okruhy určovania súvislostí vytvárajú rámec pre ekonomicky efektívny a technicky účinný manažment rizík v komplexnom prostredí informačných systémov mesta Malacky, a to skĺbením dvoch relatívne samostatných oblastí zodpovedností. Prvá je povinnosť každého orgánu verejnej správy chrániť zverené informačné zdroje. Na druhej strane stále vzrastá potreba zdieľania informačných zdrojov, a teda i zaistenia primeranej ochrany dát informačných systémov.

Kľúčovým predpokladom pre definovanie vhodného rámca je tak pochopenie vzťahov medzi faktormi determinujúcimi existenciu a veľkosť rizika, a to aktívami, zraniteľnými miestami a hrozbami. Tento vzťah je znázornený na obrázku Obrázok 2.



Obrázok 2 Vzťah hrozieb, zraniteľnosti, aktív a protiopatrení

Základný mechanizmus vzťahu faktorov rizika v rámci analýzy rizík prebieha nasledovne:

- Hrozba využíva zraniteľné miesto, prekonáva protiopatrenia a pôsobí na aktívum, kde spôsobí škodu (negatívny dopad).
- Aktívum a jeho hodnota motivuje útočníka k aktivácií hrozby. Voči pôsobeniu hrozby sa aktívum vyznačuje určitou zraniteľnosťou. Aktívum je zároveň chránené protiopatreniami pred hrozbami.
- Protiopatrenia chránia aktíva a prostredníctvom modifikácie zraniteľností zmierňujú alebo celkom zabraňujú pôsobeniu hrozieb na aktíva.
- Hrozby pôsobia priamo na zraniteľné miesta aktív alebo na implementované protiopatrenia, s cieľom získať prístup k aktívam. Aby mohla hrozba pôsobiť, musí byť aktivovaná. Pre svoju aktiváciu vyžaduje zdroje, t. j. vytvorenie podmienok pre ich pôsobenie.

Proces určenia súvislosti, vytvára vstupný rámec analýzy rizík prostredníctvom dvoch podprocesov:

- určenie hraníc analýzy rizík,
- kritéria hodnotenie rizika informačných systémov.

2.1.1 Určenie hraníc analýzy rizík

Určenie hraníc analýzy rizika je významným predpokladom úspešného splnenia cieľa analýzy rizika, ktorým je ohodnotenie a určenie akceptovateľných a neakceptovateľných rizík v súvislosti s informačnými systémami a tým aj **ochrana aktív** súvisiacich s danými informačnými systémami pred poškodením v dôsledku bezpečnostných incidentov.

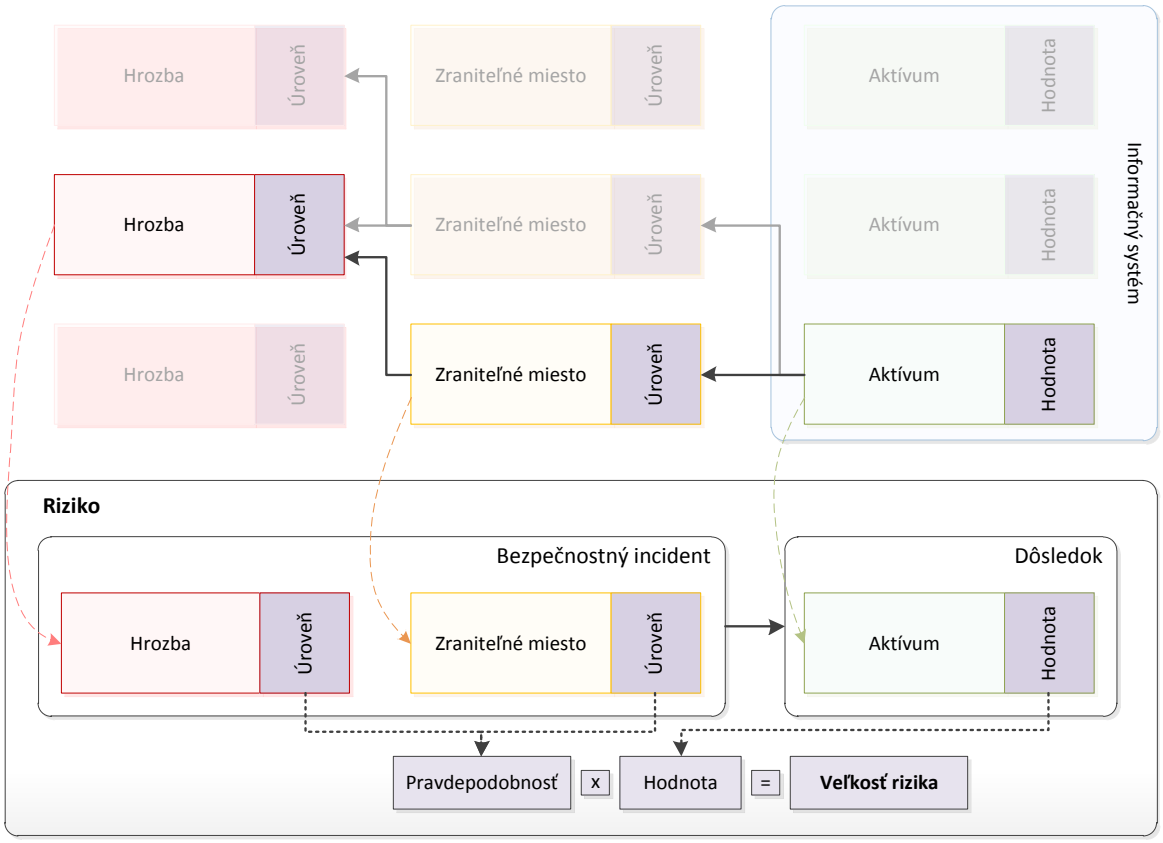
Hranica analýzy rizík je pomyselná čiara oddeľujúca aktíva, ktoré budú zahrnuté do analýzy rizík, od tých ostatných. Vo všeobecnosti sa bude analýza rizík vykonávať pre kritické aktíva, ktoré sú definované kritickosťou informačného systému, resp. súvisiacich procesov. V niektorých špecifických prípadoch môže byť hranica analýzy rizík, teda výber množiny aktív zvolený na základe iných kritérií, napríklad sa analýza rizík môže vykonávať nad aktívami konkrétneho orgánu mesta (napr. MsÚ).

Krok určenia hraníc analýzy neobsahuje samotnú identifikáciu množiny aktív (tá je súčasťou analýzy rizík v kroku „Identifikácia a ohodnotenie aktív IS“) ale jeho výsledkom je definovanie kritérií, na základe ktorých bude táto množina identifikovaná. Primárnym kritériom určenia rámca analýzy rizík je teda **kritickosť aktív**.

2.1.2 Kritéria hodnotenie rizika

V rámci procesu riadenia rizík informačných systémov je nevyhnutné stanoviť všeobecne platné a jasné kritéria prijateľnosti a neprijateľností rizík, tak aby sa predchádzalo nedorozumeniam, z ktorých môžu vzniknúť rôzne krízové situácie.

Tento prístup vychádza zo základnej definície rizika, ktorá vo všeobecnosti vníma riziko ako možnosť, že budúca udalosť bude mať nepriaznivé dopady. Možnosť vzniku udalosti je kvantifikovaná pravdepodobnosťou a nepriaznivé dopady hodnotou ohrozených záujmov. V prípade rizík v súvislosti s informačnou bezpečnosťou mesta Malacky bude riziko definované unikátnou kombináciou aktíva a zraniteľného miesta (ktoré aktívum má) a hrozby (ktorá môže zraniteľné mesto využiť). Hrozba spolu so zraniteľným miestom determinujú možnosť vzniku bezpečnostného incidentu, ktorého pravdepodobnosť je vyjadrená kombináciou úrovne hrozby a zraniteľného miesta. Hodnota aktíva určuje chránený záujem, na ktorý má bezpečnostný incident negatívny dopad. Veľkosť rizika je potom kvantifikovaná kombináciou pravdepodobnosti bezpečnostného incidentu a hodnoty aktíva (viď. Obrázok 3).



Obrázok 3 Určenie veľkosti rizika pre oblasť informačnej bezpečnosti

Pri stanovení kritérií prijateľnosti či neprijateľnosti rizík pre oblasť informačnej bezpečnosti mesto Malacky vychádza z kvalitatívnej metódy podľa STN ISO/IEC TR 13335, ktorú využíva na hodnotenie rizík informačných systémov, a ktorá umožňuje hodnotiť riziká na základe hodnoty aktíva, úrovne hrozby a úrovne zraniteľného miesta.

Mesto Malacky stanovilo kategórie pre hodnotenie prijateľnosti, resp. neprijateľnosti rizík informačných systémov nasledovne:

1. Kategórie pre určenie pravdepodobnosti bezpečnostného incidentu (Tabuľka 1)
2. Kategórie pre určenie hodnoty aktíva (Tabuľka 2)
3. Kategórie pre vyhodnotenie prijateľnosti rizika (Tabuľka 3)

Tabuľka 1 Kategórie pravdepodobnosti bezpečnostného incidentu

Bezpečnostný incident									
Úroveň hrozby	Malá			Stredná			Veľká		
Úroveň zraniteľnosti	M	S	V	M	S	V	M	S	V
Pravdepodobnosť	1	2	3	2	3	4	3	4	5

Tabuľka 2 Kategórie veľkosti dopadov

Dôsledok bezpečnostného incidentu			
Hodnota aktíva	Malá	Stredná	Veľká
Veľkosť	1	2	3

Tabuľka 3 Kritéria prijateľnosti a neprijateľnosti rizík

Akceptovateľnosť rizika				
		Veľkosť dôsledkov		
		1	2	3
Pravdepodobnosť	5	A/N	N	N
	4	A/N	N	N
	3	A	A/N	N
	2	A	A	A/N
	1	A	A	A

V tabuľke Tabuľka 3 je stanovený prístup k ohodnoteniu rizika, na základe kombinácie veľkosti dôsledkov (hodnoty aktíva) a pravdepodobnosti vzniku bezpečnostného incidentu (kombinácia úrovne hrozby a zraniteľného miesta). Vstupné hodnoty oboch dimenzií sú výstupom hodnotenia z tabuliek Tabuľka 1 a Tabuľka 2. Takto zvolený prístup umožňuje kategorizovať mieru rizika do troch skupín, a to akceptovateľná miera rizika (A), akceptovateľná miera rizika za určitých podmienok (A/N) a neakceptovateľná miera rizika (N).

Akceptovateľná miera rizík je charakterizovaná tým, že riziká informačných systémov, ktorých miera spadá do tejto skupiny, sú pre mesto Malacky prijateľné, a teda nie je potrebná implementácia ochranných opatrení. Je však dôležité si uvedomiť, že tieto riziká je potrebné monitorovať vzhľadom na často meniace sa podmienky prostredia.

Za určitých podmienok akceptovateľná miera rizika je charakterizovaná, tým že v určitom čase sú tieto riziká akceptovateľné, ale v niektorých prípadoch sa stávajú neakceptovateľnými, preto pri rizikách, ktoré patria do tejto skupiny, je nevyhnutný monitoring v užšom časovom intervale. Akceptácia vyplýva z daných podmienok v čase.

Neakceptovateľná miera rizika je charakterizovaná neprijateľnosťou týchto rizík pre mesto Malacky a potrebou prijatia preventívnych opatrení na ich zníženie.

2.2 Analýza rizika

Analýza rizík informačných systémov predstavuje základný proces manažmentu rizík pre oblasť informačnej bezpečnosti mesta Malacky. Tento proces je založený na identifikácii aktív podľa kritérií zvolených v rámci určenia hranice analýzy rizík (viď. 2.1.1), ohodnotení týchto aktív, a tiež identifikácii a ohodnotení hrozieb a zraniteľných miest, a určení pravdepodobnosti ich uskutočnenia a dopadov na analyzované aktíva.

Výsledkom analýzy rizík je kvantifikácia veľkosti rizika na základe kombinácií faktorov rizika (A, V, T). Tento proces stanovenia veľkosti rizika priamo súvisí so stanovenými kritériami hodnotenia rizík (viď. 2.1.2), a to tak, že získané miery rizík sa porovnávajú so stanovenými kritériami a klasifikujú sa do vytvorených troch úrovní (akceptovateľná miera rizika, akceptovateľná miera rizika za určitých podmienok a neakceptovateľná miera rizika).

Prístup mesta Malacky k procesu analýzy rizík vychádza zo štandardov ako ISO/IEC 177799/2000 a STN ISO/IEC TR 13335, ktoré poskytujú odporúčania pre riadenie bezpečnosti informačných systémov. Na základe implementovania tohto prístupu je mesto Malacky schopné zaistiť ochranu informačných systémov a všetkých jeho prvkov a zároveň spĺňať predpoklady právnych predpisov platných na území SR v oblasti informačnej bezpečnosti.

Proces analýzy rizík zahŕňa nasledovné oblasti:

- identifikácia a ohodnotenie aktív,
- identifikácia a ohodnotenie hrozieb,
- identifikácia a ohodnotenie zraniteľností.

2.2.1 Identifikácia a ohodnotenie aktív

Cieľom identifikácie aktív je vytvorenie zoznamov všetkých aktív, ktoré ležia vo vnútri stanovenej hranice analýzy rizík (viď. 2.1.1). Vo všeobecnosti sa pod termínom aktívum chápe všetko čo prináša ekonomický úžitok organizácií. V rámci analýzy rizík mesta Malacky sa pod termínom aktívum budú chápať tieto kategórie:

- informácie,
- programové vybavenie,
- technické zariadenia,
- ľudské zdroje.

Proces identifikácie aktív začína vytvorením zoznamu všetkých aktív v rámci mesta Malacky. Aktíva sú usporiadané do štruktúrovaného zoznamu vo forme tabuľky (Tabuľka 4), ktorý následne slúži pre identifikáciu aktív v rámci stanovenej hranice analýzy rizík podľa zvolených kritérií. Štruktúra zoznamu nie je fixná a je možné ju prispôsobovať podľa aktuálnych potrieb.

Tabuľka 4 Zoznam aktív

Zoznam aktív mesta Malacky

Kategória aktív	Skupina	Podskupina	Popis
Informácie	Dáta	Kmeňové údaje	
		Transakčné údaje	
	Metadáta	Heslá	
Programové vybavenie	Aplikačný SW	Agendové aplikácie	
		Podporné aplikácie	
	Operačný SW	Operačný systém	
Technické zariadenia	Výpočtová technika	Počítače	
		Servery	
		Periférne zariadenia	
	Záznamové médiá	Tlačové výstupy	
		Zálohovacie média	
	Komunikačné zariadenia	Sieťové zariadenia	
		Kabeláž	
Ľudské zdroje	Užívatelia	Pracovníci	
		Manažment	
	Tretie strany	Dodávatelia	
		Odberatelia	

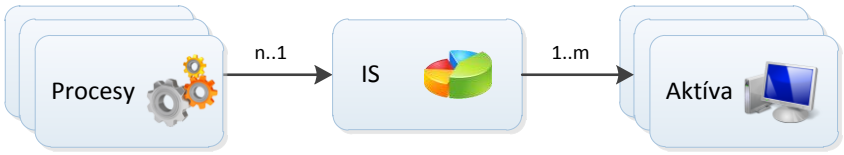
Proces identifikácie aktív sa vykonáva formou štruktúrovaných rozhovorov, fyzickou obhliadkou miest, ako aj štúdiom relevantných dokumentov, smerníc, nariadení v rámci mesta Malacky. Identifikácia aktív mesta Malacky je vykonávaná bezpečnostným manažérom stanoveným v bezpečnostnej politike mesta v súčinnosti s vlastníkmi aktív a používateľmi aktív.

Vytvorenie zoznamu všetkých aktív je predpokladom ďalšieho kroku procesu identifikácie aktív, ktorým je výber množiny aktív v rámci stanovenej hranice analýzy rizík. Implicitným

kritériom pre tento výber je kritickosť aktíva. Preto je dôležité definovať štandardný postup pre určenie kritických aktív.

Identifikácia kritických aktív

Kľúčovou vlastnosťou aktíva spadajúceho do manažmentu rizík pre oblasť informačnej bezpečnosti je, že je základnou súčasťou informačného systému. Teda informačný systém používa jednotlivé aktíva na realizáciu informačnej činnosti, ktorá je jeho primárnou úlohou. Samotná informačná činnosť je definovaná a organizovaná prostredníctvom procesov mesta Malacky. Týmto sa vytvára vzťah medzi procesmi, informačným systémom a aktívami (viď. Obrázok 4)



Obrázok 4 Vzťah medzi procesmi, informačným systémom a aktívami

Centrálnym prvkom tohto vzťahu je informačný systém, ktorý predstavuje funkčný celok spájajúci procesy, ktoré zastrešujú informačnú činnosť a aktíva, prostredníctvom ktorých sa táto činnosť vykonáva. Pri identifikácii kritických aktív preto mesto Malacky primárne vychádza z určenia kritickosti informačných systémov, pričom vychádza z predpokladu, že ak je informačný systém kritický tak aj jednotlivé jeho procesy sú kritické a analogicky aj **všetky aktíva, ktoré sú nevyhnutné pre zabezpečenie informačnej činnosti prostredníctvom kritického informačného systému sú kritické**.

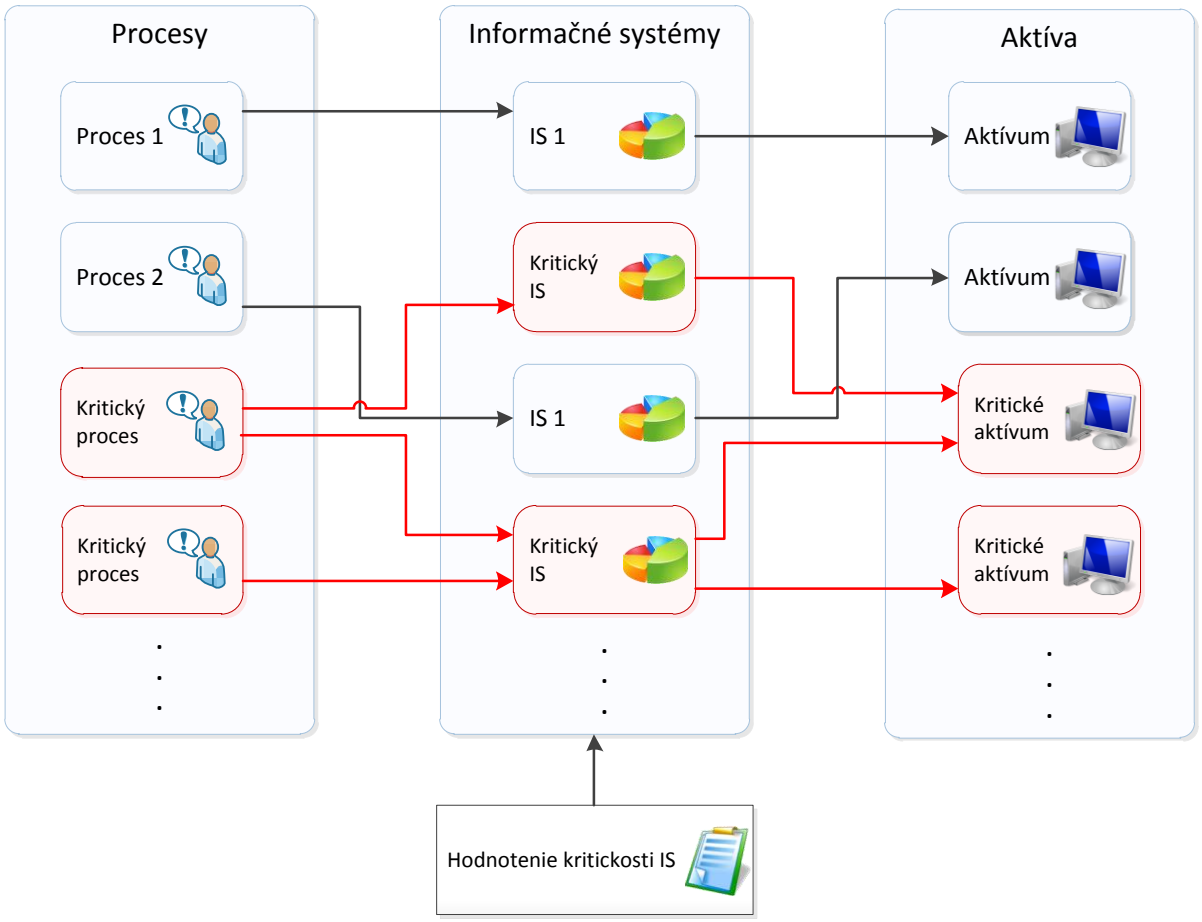
Prvým krokom identifikácie kritických aktív je určenie kritických informačných systémov. Mesto Malacky stanovuje kritickosť informačných systémov na základe dotazníkovej metódy. Dotazník pre určenie kritickosti informačného systému implementuje požiadavky dôvernosti, integrity a dostupnosti údajov spracovávaných a poskytovaných prostredníctvom informačného systému. Dotazník je uvedený v prílohe *Príloha č.1 Dotazník k určeniu kritických informačných systémov*.

Na základe vyhodnotenia všetkých informačných systémov mesta Malacky prostredníctvom dotazníka pre určenie kritickosti informačného systému sa stanoví bodové a percentuálne hodnotenie informačného systému. Mesto Malacky považuje informačné systémy s percentuálnym ohodnotením do 60% za nekritické z pohľadu stanovených kritérií a pokladá informačné systémy s percentuálnym ohodnotením **nad 60% za kritické informačné systémy**.

Ďalším krokom identifikácie kritických aktív je výber množiny aktív zo zoznamu aktív mesta Malacky (Tabuľka 4), ktoré sú nevyhnutné pre zabezpečenie informačnej činnosti prostredníctvom kritického informačného systému a ako také sú považované za kritické. Okrem tohto primárneho kritéria je možné použiť aj sekundárne kritéria a do zoznamu kritických aktív zahrnúť aj ďalšie aktíva, ktoré sa nevzťahujú ku kritickým informačným systémom, ale mesto Malacky ich považuje za kritické (napríklad vysoká obstarávacia cena aktíva a pod.)

Na základe určenia kritických informačných systémov je možné identifikovať aj kritické procesy, ktorých znalosť primárne slúži pre ďalšie kroky analýzy rizík (identifikácia a ohodnotenie hrozieb a zraniteľných miest) a pre riadenie rizík (viď. 2.3) pri navrhovaní a zavádzaní účinných protiopatrení.

Výsledkom celého procesu identifikácie kritických aktív (Obrázok 5) je zoznam kritických aktív, ktoré sú predmetom ďalšej analýzy. Tento zoznam vytvára vstup pre následný proces ohodnotenia kritických aktív. V rámci zoznamu kritických aktív je možné kvôli zvýšeniu prehľadnosti aktíva zoskupovať do celkov podľa relevantnosti vzhľadom na ich funkciu a hodnotu v rámci informačných systémov.



Obrázok 5 Proces identifikácie kritických aktív

Ohodnotenie kritických aktív

Ohodnotenie kritických aktív mesta Malacky je proces kvantifikácie ich významnosti vzhľadom na ich nevyhnutnosť v rámci informačnej činnosti prostredníctvom informačných systémov, resp. z pohľadu ich hodnoty a záujmu ochrany. Mesto Malacky vytvorilo tri úrovne ohodnotenia aktív, a to:

- malá (M),
- stredná (S),
- veľká (V).

Malá - poškodením, zničením alebo stratou aktíva môže dôjsť k narušeniu jedného alebo viacerých procesov vykonávaných prostredníctvom informačného systému mesta; vzniknutý následok však nemá vplyv na výkon správy v kompetenčnom rozsahu mesta Malacky.

Stredná - poškodením, zničením alebo stratou aktíva dôjde k narušeniu jedného alebo viacerých procesov vykonávaných prostredníctvom informačného systému mesta; vzniknutý následok bude mať čiastočný vplyv na výkon správy v kompetenčnom rozsahu mesta Malacky.

Veľká - poškodením, zničením alebo stratou aktíva môže dôjsť k úplnému prerušeniu jedného alebo viacerých procesov vykonávaných prostredníctvom informačného systému mesta; vzniknutý následok bude mať podstatný vplyv na kontinuálny výkon správy v kompetenčnom rozsahu mesta Malacky.

Príklad možného ohodnotenia kritických aktív, ktorý vychádza zo zoznamu kritických aktív vytvoreného v kroku *Identifikácia kritických aktív* je v tabuľke Tabuľka 5. Na základe určenia kritickosti jednotlivých aktív mesta Malacky prijíma adekvátne opatrenia na zníženie ich zraniteľných miest a zníženie možných hrozieb, ktoré by mohli ovplyvniť tieto aktíva.

Tabuľka 5 Príklad ohodnotenia kritických aktív

Ohodnotenie kritických aktív mesta Malacky

Kritické aktíva	Hodnota	Popis
Server 1	Veľká (V)	Využívaný v rámci šiestich kritických procesov
Dátová knižnica	Veľká (V)	Neexistencia papierovej formy údajov
PC zostava	Malá (M)	Existencia externých záloh
Prístupové heslá	Stredná (S)	Iná osoba, ktorá pozná prístupové heslo
Router 2	Malá (M)	Alternatívne zariadenie pre zabezpečenie prístupu do internetu

2.2.2 Identifikácia a ohodnotenie hrozieb

V tejto etape analýzy rizík sa identifikujú a ohodnotia hrozby, ktoré predstavujú okolnosti, resp. udalosti, ktoré majú potenciál poškodiť aktíva informačných systémov, alebo v horšom prípade zničiť informačný systém ako taký. Hrozby tak predstavujú vecnú podstatu bezpečnostných incidentov, ktorá je nutnou, avšak nie postačujúcou podmienkou, aby bezpečnostný incident nastal (na to, aby bezpečnostný incident nastal je potrebné využitie zraniteľného miesta – viď. Obrázok 2).

Identifikácia hrozieb

Pri identifikácií hrozieb mesta Malacky vychádza zo zoznamov, ktoré sú súčasťou príloh technických noriem STN ISO/IEC TR 13335-3 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT. Do týchto

zoznamov boli pridané aj ďalšie hrozby, ktoré vyplývajú z Kódexu praxe manažérstva informačnej bezpečnosti (STN ISO/IEC 27002).

Relevantnosť hrozby sa stanovuje na základe zhodnotenia potenciálu hrozby poškodiť minimálne jedno kritické aktívum identifikované v predchádzajúcom kroku (viď. 2.2.1).

Mesto Malacky vytvorilo štyri základné skupiny zoznamov, a to:

- hrozby pôsobiace na automatizované prostriedky spracovania,
    - neautorizovaný logický prístup k údajom v informačných systémoch,
    - neautorizovaný fyzický prístup k údajom v informačných systémoch,
    - technická porucha,
    - infiltrácia škodlivého kódu,
    - výpadok dodávky elektrickej energie,
    - neautorizovaný prístup do siete mesta;
- hrozby v oblasti fyzickej a objektovej bezpečnosti,
- hrozby v oblasti organizačnej a personálnej bezpečnosti,
- hrozby tretích strán.

Všetky uvedené zoznamy sú súčasťou prílohy *Príloha č.2 Zoznam hrozieb informačných systémov*.

Ohodnotenie hrozieb

Mesto Malacky si uvedomuje, že hrozba má potenciál spôsobiť negatívny dôsledok informačnému systému alebo jeho prvkom. Preto každú hrozbu hodnotí voči každému kritickému aktívu alebo skupine aktív, ktoré sú uvedené v zozname kritických aktív (viď. 2.2.1, resp. Tabuľka 5). Ohodnotenie úrovne hrozby je založené na zhodnotení možnosti, že nastane udalosť, ktorá hrozbu predstavuje. Pri hodnotení hrozby sa neprihliada na schopnosť hrozby poškodiť aktíva informačného systému, ale odhaduje sa striktne iba pravdepodobnosť, resp. možnosť výskytu udalosti, pričom sa abstrahuje od ďalších okolností, ktoré má tento výskyt potenciál spôsobiť.

Mesto Malacky stanovilo štyri kategórie ohodnotenia úrovne hrozby, a to:

- neexistujúca,
- malá (M),
- stredná (S),
- veľká (V).

Neexistujúca hrozba predstavuje udalosť s nulovou možnosťou uskutočnenia.

Malá hrozba (M) predstavuje udalosť, ktorá má teoretickú možnosť uskutočnenia, pričom za posledný rok sa udalosť nevyskytla.

Stredná hrozba (S) predstavuje udalosť, ktorá má teoretickú možnosť uskutočnenia, pričom za posledný rok sa udalosť vyskytla maximálne 2 krát.

Veľká hrozba (V) predstavuje udalosť, ku ktorej dochádza pomerne často a za posledný rok sa udalosť vyskytla viac ako 2 krát.

V rámci hodnotenia hrozieb je možné, použiť aj ďalšie kvalitatívne kritéria na určenie hodnoty hrozby (napr. expertný odhad v závislosti od znalosti úrovne implementovaných ochranných opatrení apod.). Dôležité je, aby ohodnotenie hrozieb vyjadrovalo mieru presvedčenia hodnotiteľa o možnosti výskytu hrozby (udalosti) bez ohľadu na možné dopady hrozieb na aktíva mesta Malacky.

Pre zvýšenie prehľadnosti je možné hrozby zoskupovať do celkov podľa relevantnosti vzhľadom na ich funkčné charakteristiky a potenciál spôsobiť škodu špecifickým skupinám aktív. Pri ohodnotení úrovne skupiny hrozieb platí, že úroveň skupiny je stanovená na najvyššiu úroveň z úrovni jednotlivých hrozieb zahrnutých do skupiny. Príklad ohodnotenia hrozieb je uvedený v tabuľke (Tabuľka 6).

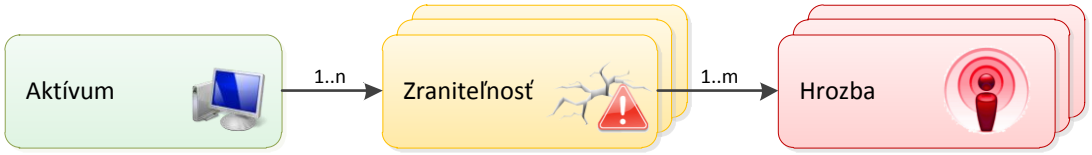
Tabuľka 6 Príklad ohodnotenia hrozieb

Ohodnotenie hrozieb

Skupina hrozieb / Hrozba	Úroveň
Výpadok dodávky elektrickej energie	Veľká (V)
• Výpadky dodávky elektrickej energie v dôsledku kolísania napätia v elektrickej sieti	Veľká (V)
• Poškodenie vonkajšieho elektrického vedenia	Malá (M)
Infiltrácia škodlivého kódu	Stredná (S)
• Implementácia škodlivého programového kódu (vírus, trojský kôň, ..) do IS	Stredná (S)
• Phishing - podvodné emaily alebo webové stránky	Malá (M)

2.2.3 Identifikácia a ohodnotenie zraniteľných miest

Zraniteľné miesta predstavujú vlastnosti prostredia (fyzického, personálneho a elektronického), v rámci ktorého sa realizuje informačná činnosť prostredníctvom informačných systémov a ktoré vytvárajú podmienky pre pôsobenie hrozieb na aktíva. Kvalitatívne sú tieto vlastnosti ovplyvňované najmä aplikovanými ochrannými opatreniami. Zraniteľné miesta tak vytvárajú logické prepojenie medzi hrozbami a aktívami (viď. Obrázok 6), ktorého dôsledkom je poškodenie, alebo zničenie informačného systému.



Obrázok 6 Vzťah medzi aktívami, zraniteľnými miestami a hrozbami

Cieľom procesu identifikácie a ohodnotenia zraniteľných miest je nájsť zraniteľné miesta v prostredí mesta Malacky, definovať prepojenia medzi hrozbami a aktívami a ohodnotiť významnosť identifikovaných zraniteľných miest.

Identifikácia zraniteľných miest

Pri identifikácii zraniteľných miest sa postupuje formou štruktúrovaných rozhovorov, obhliadkou fyzického prostredia, ako aj štúdiom relevantných dokumentov, smerníc a nariadení v rámci mesta Malacky. Jednotlivé zraniteľné miesta sú identifikované vzhľadom na identifikované kritické aktíva (viď. 2.2.1) a vzhľadom na identifikované hrozby (viď. 2.2.2), čím sa popisuje prepojenie hrozieb a aktív prostredníctvom zraniteľných miest.

Zraniteľné miesta informačných systémov mesta sa určujú na základe stanovených základných skupín prostredí, a to:

- fyzické prostredie,
- personál, manažérske a administratívne procedúry a opatrenia,
- hardvér, softvér alebo komunikačné zariadenia a prostriedky.

Zraniteľné miesta sú charakterizované faktormi ako citlivosť, kritickosť či dostupnosť. Ako príklad zraniteľného miesta vzhľadom na fyzické prostredie môžeme uviesť nevytvorenie smernice režimových opatrení. Nevytvorenie tejto smernice vytvára trhlinu v zabezpečení napríklad objektu pred nepovoleným vstupom.

Ohodnotenie zraniteľných miest

Mesto Malacky vytvorilo tri kategórie ohodnotenia úrovne zraniteľného miesta, a to:

- malá (M),
- stredná (S),
- veľká (V).

Malá zraniteľnosť (M) – je zložité využiť zraniteľnosť, sú implementované dobré bezpečnostné opatrenia.

Stredná zraniteľnosť (S) - zraniteľnosť by mohla byť využitá, sú implementované určité bezpečnostné opatrenia.

Veľká zraniteľnosť (V) - je jednoduché využiť zraniteľnosť, sú implementované slabé alebo žiadne ochranné opatrenia.

Výsledkom procesu hodnotenia zraniteľných miest je ich zoznam vzhľadom ku konkrétnemu aktívu (viď. Tabuľka 7).

Tabuľka 7 Príklad zoznamu zraniteľných miest ku konkrétnemu aktívu

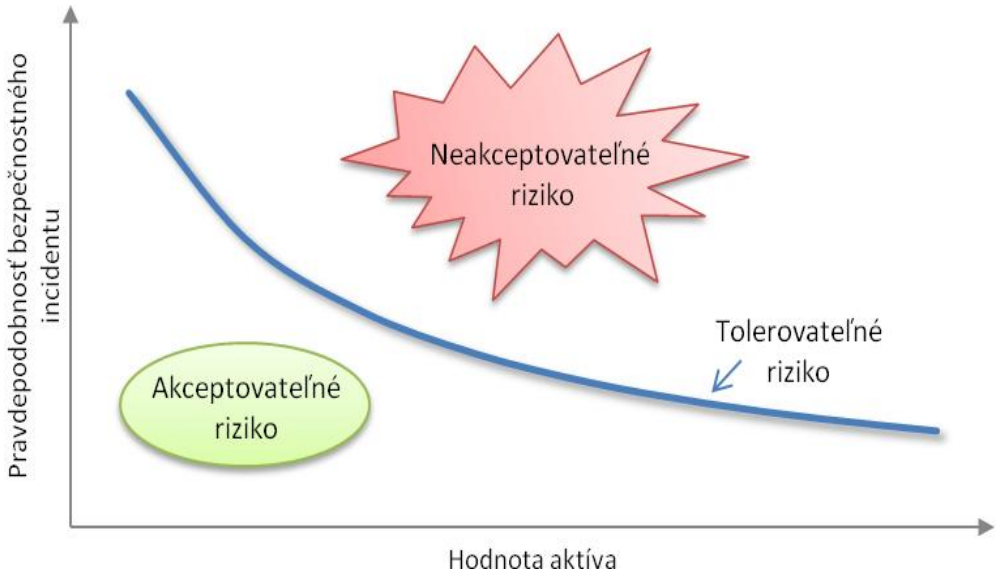
Ohodnotenie zraniteľných miest

Aktívum	Zraniteľné miesto	Úroveň
Server 1	Okno v miestnosti (1.NP) nechránené mrežami	Veľká (V)
	Vchod do miestnosti chránený bezpečnostnými dverami	Malá (M)
	Nedostatočná antivírová ochrana	Stredná (M)

2.2.4 Určenie veľkosti rizika a hodnotenie rizika

Veľkosť rizika je elementárna vlastnosť rizika, ktorá vyjadruje presvedčenie hodnotiteľa o možnosti výskytu rizikovej udalosti a závažnosti dôsledkov. Veľkosť rizika v rámci popísaného prístupu k analýze rizík mesta Malacky sa stanovuje na základe kombinácie ohodnotených úrovní aktív, zraniteľných miest týchto aktív a hrozieb. Kombinácia ohodnotenej úrovne hrozby (viď. 2.2.2) spolu s úrovňou zraniteľného miesta (viď. 2.2.3) kvantifikujú možnosť vzniku bezpečnostného incidentu, ktorého negatívny dopad na aktívum je určený hodnotou aktíva. Veľkosť rizika je potom vyjadrená kombináciou pravdepodobnosti bezpečnostného incidentu a hodnoty aktíva (viď. Obrázok 3).

Cieľom určenia veľkosti rizika je definovať toleranciu rizika. Tolerancia rizika vyjadruje či je dané riziko akceptovateľné alebo neakceptovateľné z pohľadu požadovaného stavu informačnej bezpečnosti (viď. Obrázok 7). Tolerancia rizika sa určuje na základe stanovených kritérií akceptovateľnosti rizika (viď. 2.1.2)



Obrázok 7 Určenie tolerancie rizika

Pri určení veľkosti rizika sa teda vychádza z ohodnotení jednotlivých faktorov rizika. Určenie veľkosti rizika je možné ilustrovať na príklade nasledovného rizika (Tabuľka 8):

Tabuľka 8 Príklad ohodnotenia rizika

Ohodnotenie faktorov rizika

Faktor	Popis	Úroveň/Hodnota
Aktívum	Server 1	Veľká (V)
Zraniteľnosť	Nezabezpečený vchod do miestnosti v rámci pracoviska	Veľká (V)
Hrozba	Neodborná alebo neprimeraná manipulácia	Malá (M)

Príklad ukazuje ohodnotenie faktorov rizika, na základe definovaných úrovní. Veľkosť rizika sa získa po dosadení do tabuliek definujúcich kategórie pre určenie tolerancie rizika (Tabuľka 1, Tabuľka 2). Príklad dosadenia ohodnotení z príkladu rizika uvedeného v tabuľke Tabuľka 8 je uvedený v nasledujúcich tabuľkách (Tabuľka 9, Tabuľka 10)

Tabuľka 9 Príklad určenia pravdepodobnosti bezpečnostného incidentu

Bezpečnostný incident									
Úroveň hrozby	**Malá**			Stredná			Veľká		
Úroveň zraniteľnosti	M	S	**V**	M	S	V	M	S	V
Pravdepodobnosť	1	2	**3**	2	3	4	3	4	5

Tabuľka 10 Príklad určenia veľkosti dopadov

Dôsledok bezpečnostného incidentu			
Hodnota aktíva	Malá	Stredná	**Veľká**
Veľkosť	1	2	**3**

Na základe kombinácie úrovne zraniteľného miesta a hrozby sa kvantitatívne vyjadrí pravdepodobnosť vzniku bezpečnostného incidentu (Tabuľka 9). Veľkosť dopadu bezpečnostného incidentu sa kvantitatívne vyjadrí na základe hodnoty aktíva (Tabuľka 10).

Veľkosť rizika sa stanoví prostredníctvom kombinácie určenej pravdepodobnosti bezpečnostného incidentu a veľkosti jeho dopadu. Aby bolo možné povedať, či veľkosť rizika zodpovedá kategórii akceptovateľných alebo neakceptovateľných rizík, je nevyhnutné porovnať určenú veľkosť rizika s vopred stanovenými kritériami v kapitole 2.1.2. Určenie tolerancie rizika sa uskutočňuje v procese hodnotenia rizika.

Hodnotenie rizika

Hodnotenie rizika je proces, na základe ktorého sa porovnáva veľkosť rizika získaná v procese analýzy rizika s vopred určenými kritériami rizika (viď. Tabuľka 3). Výstupom z procesu hodnotenia rizika je prioritizovaný zoznam rizík, ktoré je nevyhnutné riadiť. Proces riadenia rizík, v rámci ktorého sa zaobchádza s rizikom a prijímajú sa rôzne opatrenia na znižovanie jeho veľkosti na akceptovateľnú úroveň je popísaný v kapitole 2.3.

Príklad hodnotenia rizika uvedeného v tabuľke Tabuľka 8 a určenie jeho akceptovateľnosti je uvedený v tabuľke Tabuľka 11. V tomto prípade má riziko poškodenia servera (aktívum) v dôsledku neodbornej manipulácie (hrozba), ktorú umožnil nezabezpečený vchod do miestnosti (zraniteľné miesto) neakceptovateľnú úroveň a preto je potrebné prijať ďalšie protiopatrenia na znižovanie jeho veľkosti.

Tabuľka 11 Príklad hodnotenia rizika

Akceptovateľnosť rizika

		Veľkosť dôsledkov		
		1	2	**3**
Pravdepodobnosť	5	A/N	N	N
	4	A/N	N	N
	3	A	A/N	**N**
	2	A	A	A/N
	1	A	A	A

2.3 Riadenie rizík

Riadenie rizík je proces, v rámci ktorého sa identifikujú a navrhujú možnosti, ktorými je za aktuálnych podmienok možné reagovať na neakceptovateľné riziko za účelom zníženia jeho veľkosti.

2.3.1 Ochranné opatrenia

Snahou mesta Malacky je znížiť mieru všetkých rizík minimálne na akceptovateľnú hodnotu, ktorú je schopné, resp. ochotné znášať. Spôsob ako znížiť neakceptovateľnú mieru rizika, je implementovať adekvátne ochranné opatrenia, po prijatí ktorých sa riziko zníži na úroveň zostatkového rizika. Toto zostatkové riziko sa od pôvodného rizika líši práve o riziko redukované ochrannými opatreniami.

Návrh ochranných opatrení vychádza primárne z realizovanej analýzy rizík a identifikácie zraniteľných miest. Znalosť zraniteľných miest a ich kvalitatívnych vlastností umožňuje návrh preventívnych opatrení, ktoré zabraňujú tomu, aby bezpečnostný incident nastal. V prípade, že nie je technicky alebo ekonomicky možné zaviesť preventívne opatrenie, je možné navrhnúť ochranné opatrenia založené na transfere dopadov bezpečnostných incidentov na tretiu stranu (napr. poistenie, zmluvná pokuta, ..).

Mesto Malacky zaviedlo v rámci ochrany informačných systémov systém riadenia informačnej bezpečnosti, ktorého cieľom je ochrana informačných systémov prostredníctvom:

- stanovenia bezpečnostnej politiky a súvisiacich zodpovednosti,
- prehľadu aktív, ich ocenenia a klasifikácie,
- identifikácie hrozieb v oblasti bezpečnosti informácií,
- eliminácie alebo zníženia rizík v tejto oblasti,
- zvýšenia povedomia i zodpovednosti zamestnancov pri práci s informáciami,
- vypracovania riadiacej dokumentácie,
- identifikácie a vynútenia dodržiavania legislatívnych a zmluvných požiadaviek.

2.3.2 Systém riadenia informačnej bezpečnosti mesta Malacky

Mesto Malacky si uvedomuje významnosť bezpečnosti informačných systémov, a preto bol v rámci riadenia implementovaný systém riadenia informačnej bezpečnosti. Základným cieľom SMIB je ochrana aktív pred hrozbami (viď. predchádzajúce časti) a zabezpečenie kontinuity činnosti mesta Malacky. Vytvorený systém riadenia rizík informačných systémov nie je statický systém. Implementácia systému riadenia je kontinuálny proces a nie jednorazový projekt.

Pri zavádzaní SMIB preto mesto Malacky vychádza z Demingovho PDCA cyklu (Plan - Do – Check – Act):

P - Plánovanie (Plan) bezpečnostnej politiky, cieľov, procesov a procedúr relevantných pre riadenie rizika a zlepšovanie informačnej bezpečnosti, s cieľom priniesť výsledky v súlade s celkovou politikou a cieľmi mesta Malacky.

D - Zavedenie a prevádzka (Do) bezpečnostnej politiky, opatrení, procesov a postupov.

C - Monitorovanie a preskúmanie (Check) vhodnosti procesov voči politike informačnej bezpečnosti, cieľom a praktickým skúsenostiam.

A - Udržiavanie a zlepšovanie (Act) vykonávaním nápravných a preventívnych činnosti, založených na výsledkoch z interných auditov SMIB, preskúmaniach riadiacimi pracovníkmi alebo na základe iných relevantných informácií.

3 Použitá literatúra

1. Zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov.
2. Zákon č. 241/2001 Z.z. Zákon NR SR č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.
3. BS 7799, smernica pre riadenie bezpečnosti IT (britský štandard).
4. ISO/IEC TR 13335-1 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 1: Koncepcie a modely bezpečnosti IT.
5. ISO/IEC TR 13335-2 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 2: Riadenia a plánovanie bezpečnosti IT.
6. ISO/IEC TR 13335-3 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT.
7. ISO/IEC TR 13335-4 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 4: Výber bezpečnostných opatrení.
8. STN ISO/IEC 27002 Informačné technológie. Kódex praxe manažérstva informačnej bezpečnosti.
9. ISO/IEC 15408-1 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT. Časť 1: Úvod a všeobecný model.
10. ISO/IEC 15408-2 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT. Časť 2: Bezpečnostné funkčné požiadavky.
11. ISO/IEC 15408-3 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT. Časť 3: Požiadavky na zaručiteľnosť bezpečnosti.
12. STN ISO 31000 Manažérstvo rizika.

Príloha č.1 Dotazník k určeniu kritických informačných systémov

Hodnotenie kritickosti IS

ID	Kritérium	Odpoveď	Počet bodov	Pridelené body
1	Sú údaje v rámci tohto IS prístupné na základe zákona o slobodnom prístupe k informáciám?	áno	0	
		nie	3	
		čiastočne	2	
2	Sú v rámci tohto IS spracovávané OU?	áno	3	
		nie	0	
3	Sú v rámci tohto IS spracovávané osobitné kategórie OU?	áno	4	
		nie	0	
4	Sú údaje v rámci tohto IS spracovávané len elektronicky?	áno	6	
		nie	0	
5	Má IS vstupné rozhranie na externé informačné systémy?	áno	3	
		nie	0	
6	Má IS výstupné rozhranie na externé informačné systémy?	áno	3	
		nie	0	
7	Koľko používateľov pracuje s IS?	<10 %	0	
		10 % - 20 %	4	
		>20 %	8	
8	Koľko softvérových aplikácií je využívaných v rámci IS?	<10 %	0	
		10 % -20 %	4	
		>20 %	8	
Súčet získaných bodov			38	
Percentuálne vyjadrenie				

Príloha č.2 Zoznam hrozieb informačných systémov

Tabuľka 12 Neautorizovaný logický prístup k údajom v informačných systémoch

P. č.	Hrozba
1	Uhádnutie hesla a následný nepovolený vstup do informačného systému resp. domény dôsledkom zapisovania hesla na rôzne média
2	Uhádnutie hesla a následný nepovolený vstup do informačného systému resp. domény dôsledkom nesprávnej dĺžky a štruktúry hesla
3	Uhádnutie hesla a následný nepovolený vstup do informačného systému resp. domény dôsledkom nekonečného zadávania hesla (viacnásobné skúšanie a následné nájdenie hesla - možnosť využitia špeciálneho softvéru slovníkový útok alebo hrubá sila)
4	Uhádnutie hesla a následný nepovolený vstup do informačného systému resp. domény dôsledkom odčítania hesla z klávesnice
5	Uhádnutie hesla a následný nepovolený vstup do informačného systému dôsledkom skrytého programu, ktorý napodobňuje zobrazovanie prihlasovacej obrazovky
6	Zablokovanie prístupu do informačného systému resp. domény (alebo jeho časti) po neúspešných prihláseniach oprávnenej osoby.
7	Zablokovanie prístupu do informačného systému resp. domény (alebo jeho časti) v dôsledku zabudnutia prístupového hesla oprávnenou osobou alebo v dôsledku úmyselného zmenenia prístupového hesla.
8	Nepovolený vstup do informačného systému resp. domény dôsledkom nedostatočnej kombinácie zabezpečovacích prvkov (lokálne aplikácie)
9	Nepovolený vstup do informačného systému resp. domény dôsledkom straty zabezpečovacích prvkov (token, prístupová karta).
10	Nepovolený vstup do informačného systému využitím „štandardných“ (inštalačných) prístupových hesiel, ktoré používajú dodávatelia systémov pre ich inštaláciu alebo údržbu.
11	Nepovolený vstup do IS zneužitím dôvery užívateľa počítačovej siete zriadením príťažlivého uzla a poskytovaním atraktívnych služieb alebo údajov (ak bude užívateľ uzla vyzvaný, aby si zvolil prístupové heslo, dá sa predpokladať že toto bude podobné alebo zhodné s jeho heslom používaným na iných systémoch).
12	Nepovolený vstup do informačného systému resp. domény dôsledkom úmyselného (vydieranie, vlastný prospech) alebo neúmyselného (prerieknutie, požiadanie kolegu o láskavosť) vyzradenie hesla.
13	Nepovolený vstup do informačného systému resp. domény osobou, ktorá v minulosti mala oprávnený prístup do informačného systému (bývalí zamestnanci, preradení zamestnanci na iné oddelenie, bývalí administrátori)
14	Nepovolený prístup k dátam dôsledkom nesprávneho ukladania dát resp. nesprávneho nastavenia ich zdieľania s ostatnými užívateľmi v sieti
15	Možnosť neautorizovaného otvorenia kancelárskeho elektronického dokumentu (Word, Excel, Acrobat) obsahujúceho osobné údaje

P. č.	Hrozba
16	Nesprávne smerovania/presmerovanie dát v sieti

Tabuľka 13 Neautorizovaný fyzický prístup k údajom v informačnom systéme

P. č.	Hrozby
1	Nepovolený vstup do informačného systému pripojením sa na externé komunikačné porty (USB, FireWire, RS-232,..)
2	Nepovolený prístup k zapisovacím zariadeniam informačného systému (CD/DVD-R, FDD,..)
3	Možnosť nezistiteľného neautorizovaného prístupu do hardvéru informačného systému
4	Možnosť korektného čítania dát z pevného disku informačného systému v inom, neautorizovanom systéme
5	Nepovolený vstup do informačného systému spustením vlastného operačného systému z prenosného média (štart z diskety, USB pamäte,..)
6	Nepovolený Vstup do základnej konfigurácie informačného systému (BIOS)
7	Nepovolený vstup do informačného systému dôsledkom nedostatočnej kombinácie zabezpečovacích prvkov
8	Možnosť odčítavať údaje z obrazovky informačného systému
9	Nepovolený prístup k dátam dôsledkom preskúmavania zapožičaných, darovaných alebo vyradených prenosných pamäťových médií a pevných diskov pracovných staníc

Tabuľka 14 Technická porucha

P. č.	Hrozby
1	Technické zlyhanie (fyzická strata prenosnej schránky s diskom, zničenie prenosného disku mechanickým úderom, poškodenie povrchu disku, poškodenie kontaktového poľa prenosnej schránky, poškodenie zavádzacej stopy) záznamového alebo zálohovacieho média (magnetické pásky, diskety, digitálne záznamové prenosné médiá, HDD) spôsobené úmyselným alebo neúmyselným konaním.
2	Technické zlyhanie ostatných fyzických aktív IS (napájací zdroj, matičná doska, operačná pamäť, monitor, disketová alebo CD mechanika atď.) spôsobené úmyselným alebo neúmyselným konaním
3	Technické zlyhanie sieťových komponentov
4	Chyba prenosu
5	Zhoršenie kvality záznamového média
6	Poškodenie záznamového média
7	Chyba údržby

P. č.	Hrozby
8	Nesprávne smerovania/presmerovanie dát
9	Single Points of Failure dôsledkom logickej chyby úmyselne spôsobenej neautorizovaným vzdialeným prístupom
10	Single Points of Failure dôsledkom logickej chyby spôsobenej zlyhaním systému
11	Single Points of Failure dôsledkom logickej chyby úmyselne spôsobenej neautorizovaným fyzickým prístupom

Tabuľka 15 Infiltrácia škodlivého kódu

P. č.	Hrozby
1	Nelicencovaný softvér a následná neexistujúca podpora zo strany výrobcu, pri vzniknutých problémoch
2	Generovania neznámych funkcii softvéru (časté zlyhania operačného a aplikačného programu) dôsledkom inštalácie nelicencovaného softvéru
3	Problémová a nedostatočná aktualizácia softvéru (operačný systém, aplikačné programy) a oprava chýb (i bezpečnostných) dôsledkom nelicencovaného softvéru
4	Zlyhanie prístupu k dátam v čase potreby, dôsledkom používania nelicencovaného softvéru
5	Phishing - podvodné emaily alebo webové stránky, ktoré sa snažia vylákať osobné údaje z užívateľov, ako sú napríklad čísla kreditných kariet, PIN čísla atď.
6	Implementácia škodlivého programového kódu (vírus, trojský kôň - password – stealing trojan, deštruktívne trojany, backdoor, dropper downloader, proxy trojan, červ, spam, hoax, makrovírusy, spyware, adware, dialer) do IS v dôsledku nechráneného pripojenia do siete Internet
7	Implementácia škodlivého programového kódu (vírusu) do IS v dôsledku používania neautorizovaných prenosných zálohovacích médií

Tabuľka 16 Výpadok dodávky elektrickej energie

P. č.	Hrozby
1	Časté výpadky dodávky elektrickej energie v dôsledku kolísania napätia v elektrickej sieti
2	Poškodenie vonkajšieho elektrického vedenia
3	Výpadok elektrickej energie a zlyhanie napájaného informačného systému.

Tabuľka 17 Neautorizovaný prístup do siete mesta Malacky

P. č.	Hrozby
1	Nepovolený vstup do informačného systému dôsledkom nezabezpečených portov s následným prienikom do vnútornej siete

2	Nepovolený vstup do informačného systému dôsledkom nezabezpečených portov s následným sledovaním firemnej aktivity
3	Implementácia škodlivého programového kódu (vírusu) do IS v dôsledku nechráneného pripojenia do siete Internet
4	Nepovolený vstup do informačného systému dôsledkom pripojenia do siete iným ako firemným počítačom (tento počítač má neobmedzené možnosti spúšťania programov, zneužívanie na hľadanie bezpečnostných dier v systéme)
5	Utajené napojenie na sieť a sledovanie komunikácie dôsledkom nešifrovaného prenosu dát v sieti (odpočúvanie a modifikácia dát pri prenose v sieti)
6	Blokovanie firemnej komunikácie dôsledkom zahltenia e-mailových schránok firmy veľkým množstvom nevyžiadanej pošty (SPAM).
7	Zamietnutie služby – (DOS Denial of Service resp. *DDoS Distributed Denial of Service*)

Tabuľka 18 Hrozby v oblasti fyzickej a objektovej bezpečnosti

P. č.	Hrozby
1	Vyhotovenie neautorizovanej kópie dokumentov s osobnými údajmi (kopírovacie zariadenie, fotografia)
2	Neautorizovaný prístup k dokumentom v papierovej forme dôsledkom prehľadávania odpadkových košov, hľadanie odhodených výstupov z informačného systému
3	Odcudzenie, poškodenie a pozmenenie dokumentov s osobnými údajmi
4	Vizuálna špionáž – sledovanie napr. s pomocou vhodnej optiky (napr. z vedľajšej budovy) oprávnených užívateľov pri zadávaní prístupových hesiel, alebo sledovanie zobrazovaných výstupov z informačného systému
5	Neoprávnená úmyselná alebo neúmyselná manipulácia s prenosnými zálohovacími médiami
6	Nedovolená manipulácia s otvoreným ohňom
7	Nedodržanie BOZP a bezpečnostných požiarnych predpisov
8	Nezabezpečenie objektu proti elektrickému výboju spôsobeného bleskom
9	Chyba údržby
10	Možnosť prenesenia požiaru z vedľajších objektov
11	Skrat na elektrickom vedení
12	Pretrhnutie vodnej nádrže a následné zaplavenie priestorov spoločnosti, v ktorých sa nachádzajú osobné údaje
13	Vyliatie sa vodných tokov do priestorov spoločnosti, následkom prudkých alebo dlho trvajúcich dažďov
14	Presakovanie vody do zariadení a následné krátke spojenie (skrat) dôsledkom chybného utesnenie

Tabuľka 19 Hrozby v oblasti organizačnej a personálnej bezpečnosti

P. č.	Hrozby
1	Neodborná alebo neprimeraná manipulácia
2	Chyba obsluhy
3	Neautorizovaný prístup k osobným údajom
4	Neautorizovaný prístup tretej strany k osobným údajom
5	Neoprávnené odpočúvanie
6	Úmyselné alebo neúmyselné porušovanie zásad ochrany osobných údajov
7	Vydierateľnosť osôb ktoré majú autorizovaný prístup k osobným údajom
8	Rutinná práca (napr. zabudnutý dokument v skenery alebo v tlačiarni)
9	Nepovolený vstup do informačného systému zneužitím totožnosti - sociálne inžinierstvo (napr. predstavovanie sa ako IT technik a vyžadovanie si hesla od užívateľa po telefónne alebo emailom)
10	Dočasná indispozícia alebo skrytá psychická porucha oprávnenej osoby
11	Úmyselné alebo neúmyselné zaevidovanie nesprávneho údaja do IS (úmyselné vnášanie nesprávnych alebo neautentických vstupných údajov do informačného systému resp. do komunikačných kanálov napr. v účtovníctve využívanie tzv. mŕtvych duší)
12	Inferencia, teda odvodenie chránenej informácie z prístupných údajov (je možné odvodiť citlivé údaje, ktoré nesmú byť verejne dostupné, vhodnou kombináciou verejne prístupných agregovaných údajov)
13	Poruchy v činnosti informačného systému vyplývajúce z omylov či neprítomnosti kľúčovej osoby, z dôvodu ochorenia, dovolenky, služobnej cesty, prípadne rozviazania pracovného pomeru alebo náhleho úmrtia
14	Zneužitie výsostného postavenia (napr. administrátorské práva)

Tabuľka 20 Hrozby tretích strán

P. č.	Hrozby
1	Nedodržanie zmluvných podmienok
2	Únik informácií
3	Porušenie obchodného tajomstva
4	Prerušenie vývoja daného softvéru a následnej podpory jeho aktualizácie
5	Nekompatibilita poskytnutého softvéru so softvérmi v rámci mesta Malacky