BEZPEČNOST PŘEPÁŽKOVÝCH PRACOVIŠŤ KATASTRÁLNÍHO ÚŘADU PRO ZLÍNSKÝ KRAJ

Safety of the counter workplaces of
Cadastral Office for Zlin region

Bc. Štěpán Forman

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Štěpán FORMAN**
Osobní číslo:	**A08430**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost přepážkových pracovišť Katastrálního úřadu pro Zlínský kraj**

Zásady pro vypracování:

1. **Proveďte analýzu současného stavu zabezpečení.**
2. **Konkretizujte bezpečnostní bezpečnostní rizika.**
3. **Zpracujte návrh způsobů řešení bezpečnostních rizik.**
4. **Práci doplňte obrazovou a grafickou dokumentací.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUDVÍK, M., Teorie bezpečnosti počítačových sítí. Praha: Computer media, 2008. 98 s. ISBN 978-80-86-686-35-6**
2. **JAŠEK, R., Informacní a datová bezpecnost. 1. vyd. Academia centrum UTB, 2006. 140 s. ISBN 8073184567**
3. **SODOMKA, Petr. Informační systémy v podnikové praxi. 1. vyd. Brno, Computer Press a. s., 2006.**
4. **RAK , Roman, MATYÁŠ, Václav, ŘÍHA, Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha : Grada Publishing, a.s., 2008, 664 s. ISBN 978-80-247-2365-5.**
5. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno : Computer Press, 2004. s. 190. ISBN 80-251-0106-1.**
6. **Soubor postupů pro management bezpečnosti informací, ČSN ISO/IEC 27002:2005**
7. **Informační technologie – systémy managementu bezpečnosti informací, ČSN ISO/EIC 27001:2006**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá bezpečností přepážkových pracovišť Katastrálního úřadu pro Zlínský kraj, které jsou využívány zaměstnanci všech organizačních útvarů Katastrálního úřadu pro Zlínský kraj. Diplomová práce popisuje a analyzuje současný stav přepážkových pracovišť a navrhuje možnosti řešení zjištěných nedostatků. V praktické části, navrhuji opatření, které je vhodné realizovat pro další bezpečný a bezproblémový provoz přepážkových pracovišť Katastrálního úřadu pro Zlínský kraj.

Klíčová slova: informační bezpečnost, zabezpečovací technika, kamerový systém, bezpečnostní systémy, havarijní plánování

ABSTRACT

This thesis focuses on the safety of counter workplaces at Cadastral Office for Zlin region, which are used by employees of all departments of the cadastral office. Describes and analyzes current state of the counter workplaces and suggests possible solutions to identified deficiencies. In the practical part I suggest measures that should be implemented for the safe and smooth operation of counter workplaces.

Keywords: information security, security equipment, camera´s system, security systems, emergency planning

Tímto bych chtěl poděkovat vedoucímu diplomové práce JUDr. Vladislavu Štefkovi za odborné rady, připomínky a vstřícnost, kterou mi poskytoval při zpracování diplomové práce. Také chci poděkovat své rodině za podporu a trpělivost, kterou se mnou po celou dobu studia měla.

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.

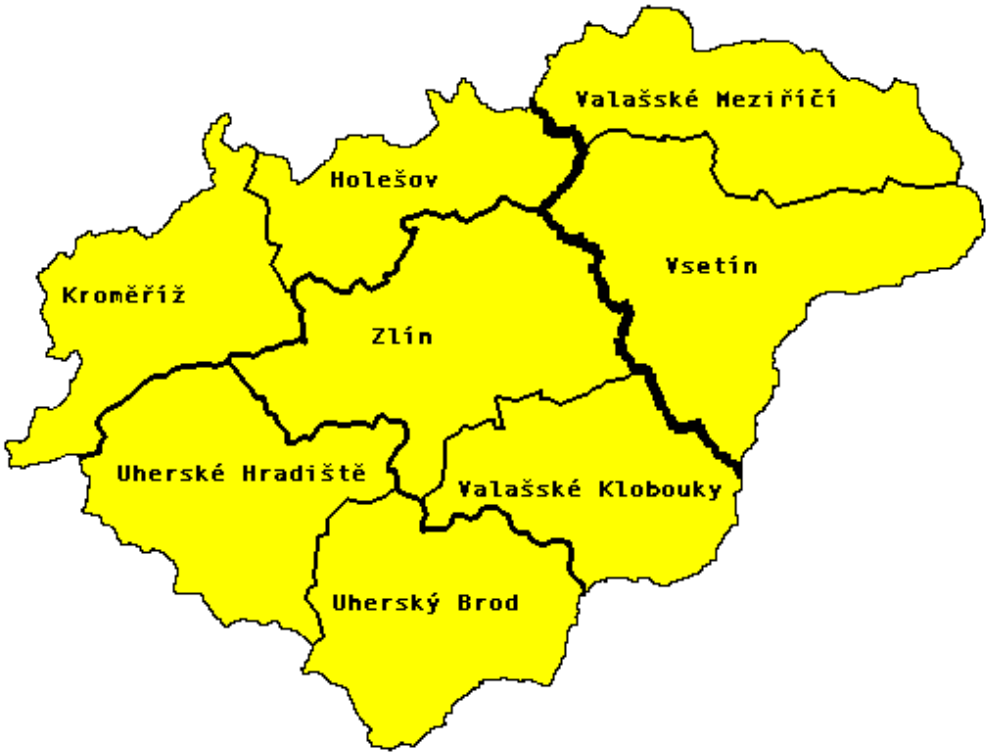
Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

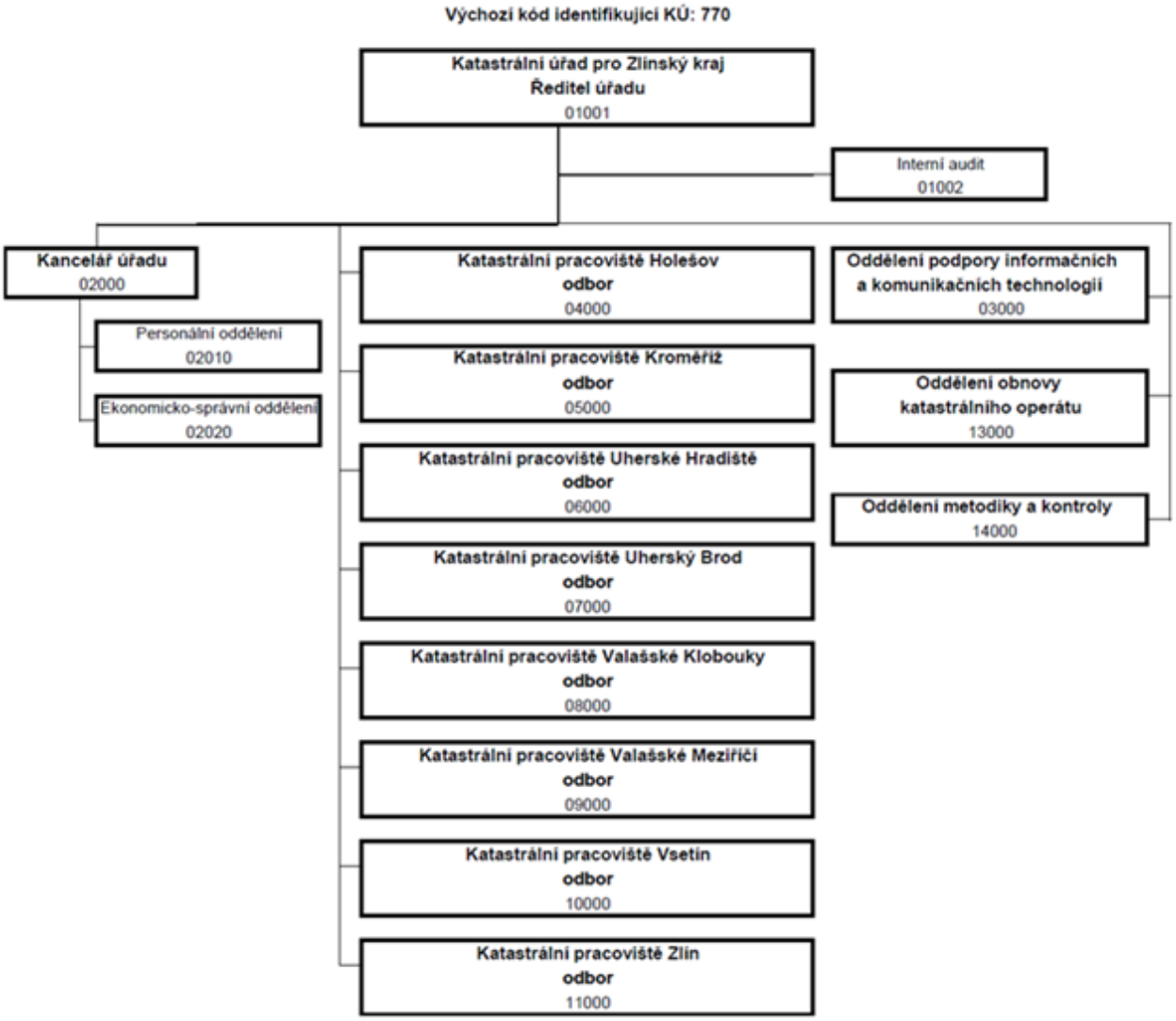
Katastrální úřad pro Zlínský kraj (dále jen "KÚ") byl zřízen 1. ledna 2004 ustanovením § 2 odst. 2 zákona č. 359/1992 Sb., o zeměměřických a katastrálních orgánech, ve znění zákona č. 175/2003 Sb. Vykonává působnost pro územní obvod Zlínského kraje (příloha č. 1). Ve smyslu § 3 zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, ve znění pozdějších předpisů, je organizační složkou státu a také jeho účetní jednotkou. Orgánem vykonávajícím funkci zřizovatele je dle § 64 zákona č. 218/2000 Sb., zákona o rozpočtových pravidlech, Český úřad zeměměřický a katastrální (dále jen "ČÚZK").



Obrázek 1: Územní působnost Katastrálního úřadu pro Zlínský kraj
[vlastní tvorba]

Katastrální úřad je správním úřadem pro katastr nemovitostí včetně zápisů věcných práv k nemovitostem. Věcná působnost katastrálního úřadu je vymezena § 5 zákona č. 359/1992 Sb., o zeměměřických a katastrálních orgánech, ve znění zákona č. 175/2003 Sb.

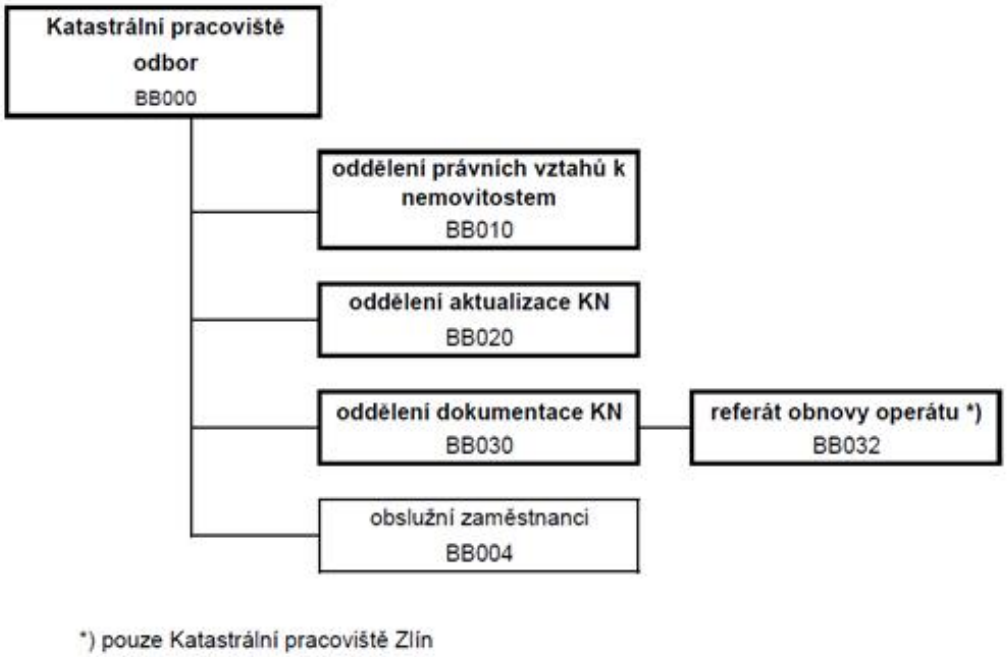
Organizační členění je následující:



Obrázek 2: Organizační schéma KÚ [15]

Katastrální pracoviště jsou vnitřními organizačními jednotkami KÚ a vykonávají státní správu katastru nemovitosti, správu podrobného pole polohového a plní další úkoly na úseku katastru nemovitosti.

Jejich organizační členění je následující:



Obrázek 3: Organizační schéma katastrálních pracovišť [15]

Útvary katastrálních pracovišť zajišťují následující činnosti:

Organizační útvar na úseku právních vztahů k nemovitostem zajišťuje tyto činnosti:

- vyznačuje v protokolu vkladů a záznamů doručení listin v pořadí jak byly doručeny, zakládá řízení, vyznačuje plomby a další údaje o průběhu řízení (operace) související s dále uvedenými činnostmi,
- rozhoduje o návrzích na povolení vkladu, o zamítnutí vkladu, nebo výmazu práv k nemovitostem do katastru nemovitostí,
- kontroluje správnost výše úhrady správního poplatku za návrh na zahájení řízení o povolení vkladu do katastru nemovitostí, provádí činnosti související s vybíráním nedoplatku nebo vrácením přeplatku správního poplatku,
- zjišťuje způsobilost listin nebo ohlášení určených k záznamu nebo k vyznačení poznámek o právech k nemovitostem a jiných údajů katastru,
- zasílá oznámení o provedené opravě chyby v katastrálním operátu nebo o tom, že oprava na návrh nebyla provedena, protože se nejedná o chybu, pokud se týká práva k nemovitostem, popřípadě rozhoduje v dané věci ve správním řízení,

- kontroluje věcnou správnost aktualizace a provádí zplatňování budoucího stavu zápisu práv v Informačním systému katastru nemovitostí (ISKN),
- jedná se státními orgány, obcemi, vlastníky a jinými oprávněnými při zápisu vlastnických a jiných věcných práv k nemovitostem,
- vede seznam úředně ověřených podpisových vzorů statutárních orgánů právnických osob,
- zabezpečuje činnosti podatelny vč. Elektronické podatelny a výpravny navazující na informační systém datových schránek (EPVDS) stanovené spisovým a jednacím řádem KÚ,
- potvrzuje uznání pravosti podpisu oprávněných osob na smlouvách předkládaných ke vkladu nebo na listinách předkládaných k záznamu do katastru,
- po vkladu vyznačuje doložku o povolení a provedení vkladu na smlouvách,

Organizační útvar na úseku aktualizace katastrálních operátů zajišťuje zejména tyto činnosti:

- vede na podkladě příslušných listin protokoly o revizi katastrálního operátu, o porušení pořádku a záznam pro další řízení, vyznačuje průběh vlastního řízení (operací) v protokolech vkladů a záznamů, popřípadě ostatní rozhodnutí a o potvrzení geometrických plánů, dále v protokolech o průběhu obnovy katastrálního operátu nebo o průběhu pozemkových úprav,
- zpracovává návrh aktualizace údajů Souboru popisných informací (SPI) na podkladě příslušných listin po předchozím předání vkladu nebo záznamu k aktualizaci, vyznačuje v Souboru grafických informací (SGI) obnovu katastrálního operátu,
- potvrzuje geometrické plány a upřesněné přídělové plány, ověřuje kopie prvopisu geometrického plánu,
- vkládá údaje potvrzovaného geometrického plánu do digitální katastrální mapy nebo katastrální mapy digitalizované, zpracovává návrh aktualizace uvedených map a vyznačuje změny v grafické katastrální mapě podle příslušné listiny,
- vydává oznámení o opravě chyby údajů katastru nemovitostí, které jsou výsledkem zeměměřických činností, vedení nebo obnovy katastrálních operátů, popřípadě rozhoduje v dané věci ve správním řízení,
- provádí revizi katastru nemovitostí,

- vede řízení o změně hranic katastrálních území, vyjadřuje se k průběhu navrhované změny hranice obce nebo městského obvodu, popřípadě městské části statutárního města z hlediska správy katastru nemovitostí, a vyznačení pravomocných rozhodnutí o změně hranice katastrálního území oznamuje Českému statistickému úřadu a Zeměměřickému úřadu,
- připravuje návrhy na změnu názvu katastrálního území a návrhy na nové pomístní názvy pozemkových tratí,
- zpracovává návrhy rozhodnutí o označení hranic pozemků na náklad vlastníka nebo návrh rozhodnutí o označení hranic obce na náklad obce,
- kontroluje správnost výše správního poplatku za přijetí žádosti o potvrzení geometrického plánu, rozhoduje o vrácení správního poplatku,

Organizační útvar na úseku dokumentace katastru nemovitostí zajišťuje zejména tyto činnosti:

- dokumentuje, případně skartuje jednotlivé části operátů katastru nemovitostí, bývalé evidence nemovitostí, jednotné evidence půdy a pozemkového katastru, včetně pozemkových, popř. železničních knih a zemských desek,
- vyznačuje žádosti o poskytnutí údajů z katastru nemovitostí,
- poskytuje údaje z katastru nemovitostí ve formě veřejných listin nebo ve formě, která nemá povahu veřejných listin, ověřené opisy nebo kopie ze sbírky listin a z dokumentace výsledků šetření a měření pro vedení a obnovu katastrálního operátu,
- poskytuje údaje o bodech základního a podrobného polohového, výškového a tíhového bodového pole z územní působnosti katastrálního pracoviště,
- ověřuje náležitosti žádostí a poskytuje počítačové soubory s údaji katastru nemovitostí na technických nosičích dat,
- vede průběh vyřizování žádostí o poskytování podkladů pro měření osobám oprávněným vykonávat zeměměřické činnosti,
- vede seznam prostor, ve kterých jsou podrobné body povinně určovány v souřadnicovém systému jednotné trigonometrické sítě katastrální (S-JTSK), a prostor, ve kterých vlivem lidské nebo přírodní činnosti dochází v terénu k posunům znemožňujícím dodržení stanovené přesnosti katastrální mapy a předkládá změny v těchto seznamech k oznámení ve Zpravodaji ČÚZK a způsobem umožňujícím dálkový přístup,

- zajišťuje obnovu katastrálního operátu přepracováním SGI v případě grafické katastrální mapy, námitkové řízení a přípravu vyhlášení platnosti obnoveného operátu i v případě, že je obnova prováděna oddělením obnovy katastrálního operátu, a to pokud tato činnost není na základě rozhodnutí ředitele KÚ svěřena útvaru na úseku vedení katastrálních operátů, zpracovává projekt obnovy katastrálního operátu přepracováním v katastrálním území vyhotovovaných KP, přebírá výsledky zeměměřických činností pro potřeby obnovy katastrálního operátu provedených na základě smluv,
- spolupracuje s oddělením obnovy katastrálního operátu, pozemkovým úřadem při obnově katastrálního operátu nebo provozovatelem geodetického informačního systému,
- spolupracuje s oddělením metodiky a kontroly a kanceláří úřadu při přípravě smluv o provádění zeměměřických činností pro potřeby obnovy katastrálního operátu,
- při obnově katastrálního operátu novým mapováním zajišťuje ve spolupráci s oddělením obnovy katastrálního operátu zjišťování průběhu hranic,
- zajišťuje námitkové řízení při obnově katastrálního operátu novým mapováním nebo přepracováním, zpracovává návrhy rozhodnutí o podaných námitkách proti obsahu obnoveného operátu, popřípadě rozhoduje v dané věci ve správním řízení,
- kontroluje správnost výše úhrady správního poplatku za vydání opisu, výpisu, kopie z katastru nemovitostí a rozhoduje o vrácení správního poplatku,

Jednotlivá katastrální pracoviště se při výkonu těchto činností spoléhají na informace uložené v informačních systémech i mimo ně. Ztráta spolehlivosti, dostupnosti a integrity informací uložených v těchto informačních systémech může nejen citelně poškodit dobré jméno KÚ, ale zapříčinit i velmi vysoké ekonomické škody. V extrémním případě může vážně narušit plnění základního poslání resortu zeměměřictví a katastru. Proto je velmi důležité zajistit bezpečnost informačních systémů a chránit informace v jakékoliv podobě a formě. Tato práce má za cíl definovat ochranu a bezpečnost cenných informací v rámci katastrálních pracovišť.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA INFORMAČNÍHO SYSTÉMU

Bezpečnostní politika informačních systémů (IS) je nedílnou součástí všeobecné bezpečnostní politiky organizace a lze si pod ní představit ucelený souhrn bezpečnostních zásad, norem, praktik, předpisů definujících způsoby zabezpečení, souhrn bezpečného využívání informačních zdrojů v rámci organizace nezávisle na použitých informačních technologiích.

Jejím úkolem je především konkrétně definovat:

- Co chceme chránit
- Proč to chceme chránit
- Jakým způsobem to chceme chránit
- Jakým způsobem ověříme, že je ochrana dostatečná a funkční
- Co budeme dělat, pokud ochrana selže

Bezpečnostní politiku IS je nutné pravidelně aktualizovat, ať již s ohledem na neustále se měnící podmínky v oblasti IT, ale také je třeba brát v potaz například i na průběžně se měnící plány a cíle organizace pro kterou je tato politika vytvářena.

Při tvorbě bezpečnostní politiky organizace je jedním z nejdůležitějších kroků provedení analýzy a následného hodnocení rizik, která mohou organizaci hrozit. Správně provedená analýza dokáže nejlépe odhalit slabá místa v systému a tím pádem je možné přijmout efektivnější opatření, organizace je pak mnohem lépe připravena na případný bezpečnostní incident a ve většině případů je možné minimalizovat ztráty, které by daný incident mohl způsobit.

2 ANALÝZA RIZIK

Analýza rizik je jednou z nejdůležitějších součástí systémového řešení bezpečnosti informačního systému, která předchází vytvoření bezpečnostní politiky informačního systému. Existuje mnoho způsobů, jak lze analýzu rizik vytvořit a ustanovení co vše by měla obsahovat. Různé způsoby realizace analýzy rizik podrobně popisuje mezinárodní norma ISO/IEC TR 13335, která také definuje tyto čtyři základní typy provádění analýzy rizik.

2.1 Typy realizace analýzy rizik

2.1.1 Základní přístup

Organizace nemusí mít analýzu rizik vypracovánu vůbec nebo jsou rizika brána v potaz pouze jako skutečnosti, které se mohou stát, ale nejsou proti nim vytvořena příslušná opatření. Jedná se o řešení, které využívají hlavně malé firmy s omezeným finančním rozpočtem.

2.1.2 Neformální přístup

Jedná se o metodu, při které jsou rizika posuzována dle subjektivních znalostí a zkušeností člověka, který dobře zná informační systém dané organizace - často se tedy jedná o administrátora počítačové sítě společnosti. Tento způsob analýzy může být dostačující, ale nedokáže dokonale nahradit podrobnou a odbornou analýzu rizik prováděnou specialistou.

2.1.3 Podrobná analýza rizik

Jedná se o nejpodrobnější časově i finančně nejnáročnější metodou analýzy rizik – je však zaručeno téměř přesné hodnocení rizik a kvalitní návrh řešení. Klasický postup podrobné analýzy spočívá v identifikaci zaměření a aktivit organizace, dále pak stanovení hodnocení rizik a návrhu odpovídajících opatření.

V praxi se také často využívá kombinace obou těchto metod – pomocí neformálního přístupu jsou IS rozděleny na skupiny podle důležitosti a pro kritické a středně kritické IS je pak provedena podrobná analýza.

2.2 Základní pojmy analýzy rizik

2.2.1 Aktivum

Pod pojmem aktivum se v oblasti analýzy rizik rozumí každá věc (ať už hmotná nebo nehmotná), která má pro danou organizaci nějakou hodnotu. Posuzování hodnoty aktiva je založeno na velikosti škody způsobené jeho zničením či ztrátou. Obvykle se při stanovení této hodnoty vychází z jeho nákladových charakteristik (pořizovací ceny, reprodukční pořizovací ceny), mohou to být ale i charakteristiky výnosové (pokud aktivum přináší dobře identifikovatelné zisky či jiné významné přínosy pro subjekt). Mezi výnosové charakteristiky patří i vlastnosti aktiva, sloužící k dosahování zisků nepřímo – například postavení na trhu, ochranná známka, ale i kvalifikace a know-how zaměstnanců.

2.2.2 Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva, který může hrozba využít pro uplatnění svého nežádoucího vlivu. Zranitelnost vyjadřuje jak citlivé je aktivum na působení dané hrozby. Zranitelnost vzniká všude tam, kde dochází k interakci mezi hrozbou a aktivem.

Úroveň zranitelnosti se hodnotí podle následujících faktorů:

- Citlivost – náchylnost aktiva k poškození hrozbou
- Kritičnost – důležitost aktiva

2.2.3 Protiopatření

Lze definovat jako cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Cílem protiopatření je předejít vzniku škody nebo usnadnit překlenutí následků vzniklé škody.

Při výběru vhodného protiopatření se bere ohled na jeho účinnost, zároveň však je nutné, aby jeho pořízení, zavedení a provozování neznamenalo pro společnost příliš vysoké náklady.

2.2.4 Riziko

Riziko vzniká vzájemným působením hrozby a aktiva. Hrozba, která nepůsobí žádné riziko, nemusí být v analýze rizik brána v potaz. Aktivum, na které nepůsobí žádné hrozby, není předmětem analýzy rizik.

2.3 Postup analýzy rizik

2.3.1 Stanovení hranice analýzy

Prvním krokem celé analýzy rizik je vyloučení aktiv, na která nepůsobí žádná hrozba, popř. je tato hrozba nebo hodnota aktiva natolik malá, že nemá cenu aktivum zahrnovat do analýzy.

2.3.2 Identifikace aktiv

V praxi není problém s poměrně malým úsilím identifikovat velké množství aktiv, které je vhodné seskupovat do celků podle podobných vlastností tak, aby se vytvořily skupiny aktiv, která následně vystupují jako jedno aktivum. Tímto přístupem lze značně zjednodušit celou analýzu a po určení vhodného protiopatření pro takovouto skupinu aktiv je možné toto protiopatření aplikovat na každé jednotlivé aktivum.

2.3.3 Identifikace hrozeb

Hrozba je jakýkoliv jev, událost, aktivita nebo osoba, který má nežádoucí vliv na bezpečnost nebo může způsobit škodu. Při identifikaci hrozeb lze vycházet ze seznamu hrozeb sestavených podle literatury, vlastních zkušeností a průzkumů dříve provedených analýz. Hrozby se mohou odvozovat také od subjektu, jeho statusu (podnikatelský subjekt, orgán veřejné správy, nezisková organizace, atd.), postavení na trhu, hospodářských výsledků, záměrů podnikatele. Pro získání vlastního seznamu hrozeb subjektu je vhodné použít některou z metod jako brainstorming, metoda Delphi, apod

Hrozbou může být například:

- přírodní živel (požár, záplava, vichřice, blesk, …)
- nehoda (ztráta, technická závada, havárie, …),
- zanedbání (pozapomenutí, nesprávný postup, …),
- neetické chování (špionáž, konflikt zájmů, korupce, …),
- kriminalita (krádež, sabotáž, terorismus, …).

2.3.4 Analýza hrozeb a zranitelností

Pří této analýze se posuzuje každá hrozba vůči každému aktivu. U aktiv, na která může hrozba působit, se stanoví úroveň hrozby a úroveň zranitelnosti aktiva. Při analýze hrozeb se berou v úvahu již realizovaná protiopatření.

2.3.5 Pravděpodobnost jevu

Pro analýzu rizik je zároveň nutné udělat alespoň odhad pravděpodobnosti výskytu jevu. Tento údaj pak doplňujeme k jednotlivým možným kombinacím aktiv a hrozeb, čímž vzniká ucelená informace, na jejímž základě se provádí výběr adekvátních protiopatření.

Při analýze rizik se často pracuje s veličinami, které nelze v mnoha případech přesně změřit ani určit – jejich hodnota mnohdy spočívá pouze na kvalifikovaném odhadu specialisty vyjadřujícího se jen na základě svých zkušeností.

2.4 Metody analýzy rizik

2.4.1 Kvantitativní metoda

Vyznačuje se tím, že rizika jsou vyjádřena v určitém rozsahu – například jsou obodována 1 až 10. Úroveň je určována obvykle kvalifikovaným odhadem, což je jednodušší a rychlejší než kvalitativní metoda a nepřináší to tak vysoké finanční náklady na provedení analýzy.

Pravděpodobně nejznámější a v oblasti IT často používanou je metodika CRAMM , která byla původně vyvinuta pro potřeby vlády Velké Británie, ale v současnosti je široce využívána jako uznávaný prostředek pro analýz rizik.

2.4.2 Kvalitativní metoda

Je založena na přesném matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Tato metoda poskytuje přesnější výstupy, její provedení však vyžaduje několikanásobně více času, úsilí a finančních prostředků.

Výsledkem zpracované analýzy je přehled použitých opatření, jejich cena a časová náročnost jejich provedení. Na základě těchto informací je pak možné aktualizovat bezpečnostní politiky organizace, popř. havarijní plány pro kritické IS. [8]

3 INFORMAČNÍ BEZPEČNOST

Informační bezpečností se rozumí soubor technických a organizačních opatření přijatých a provedených za účelem ochrany informací ve všech podobách. Informační bezpečnosti se dosahuje použitím vhodné kombinace organizačních postupů, pravidel, směrnic, organizačních struktur, technického a softwarového zabezpečení.

Za minimum v oblasti softwarového zabezpečení se považují následující metody:

- antivirová ochrana
- ochrana pomocí firewallu
- zálohování dat
- fyzická ochrana dat

V současné době se k tomuto minimu velmi často přidávají také:

- šifrování dat
- ochrana proti spamu

3.1 Antivirová ochrana

Antivirová ochrana je zřejmě nejvyužívanější metodou pří ochraně dat, především proto, že většina počítačů je v dnešní době připojena k síti Internet. Jedná se tak spíše než o ochranu samotných dat o ochranu operačního systému počítače, který by mohl být v případě napadení virem hrozbou pro data, která jsou uložena nejen v něm, ale i na síťových discích. Antivirový systém však nezabrání například tomu, že zlomyslný uživatel, nebo neoprávněná osoba data zkopíruje, poškodí nebo odstraní.

Moderní antivirový systém používá při vyhledávání potencionálních hrozeb kombinaci těchto tří metod:

- porovnáváním signatur škodlivého kódu
- heuristická analýza
- kontrolní součty a rezidentní ochrana

3.1.1 Porovnávání signatur škodlivého kódu

Tato metoda vychází z předpokladu, že každý virus obsahuje jistý unikátní řetězec – signaturu, která ho dokáže jednoznačně identifikovat. Pokud se tento řetězec vyskytuje například ve spustitelném souboru, je tento napaden virem. [1]

Již ze samotné definice této metody vyplývají její výhody i nevýhody. Největší nevýhodou této metody detekce škodlivého kódu je, že dokáže odhalit pouze známé viry a jiné škůdce, není však schopna detekovat ani jakkoliv modifikované (polymorfismus, komprimace spustitelného škodlivého kódu) varianty již známého škodlivého kódu. Její velkou výhodou oproti například heuristické analýze je bezesporu rychlost a nízká náročnost na systémové prostředky hostitelského systému.

3.1.2 Heuristická analýza

Základem heuristické analýzy je vyhledávání podezřelých projevů programů, které bývají využívány počítačovými viry [1]. Díky tomuto testování lze odhalit i zcela neznámé nebo pozměněné viry, které by nebylo možné detekovat pomocí porovnáním signatur. Heuristická analýza patří svou náročností k největším a zároveň nejpomalejším metodám detekce škodlivého kódu, zejména na pomalejších počítačích může výrazně ovlivnit výkon celého operačního sytému a tím i spouštěných aplikací.

3.1.3 Kontrolní součty, rezidentní ochrana

Pomocí kontrolních součtů lze do značné míry zrychlit a zefektivnit celý proces nalezení viru nebo škodlivého kódu. Idea celé této metody spočívá v tom, že je proveden výpočet kontrolních součtů všech napadnutelných souborů (např. exe, com, sys soubory) a tyto kontrolní součty jsou uloženy do databáze antiviru. V případě napadení sledovaného souboru virem nebo pozměněním jeho obsahu se změní kontrolní součet a antivirový systém může provést další opatření – typicky další kontroly pomocí signatur nebo heuristickou analýzu. Naopak, pokud se kontrolní součet souboru nezmění, není nutné takovýto soubor podrobovat dalšímu zkoumání – lze ho považovat za autentický a již prověřený.

Rezidentní ochrana pak automaticky kontroluje všechny nové, pozměněné, ale i spouštěné soubory a zabraňuje průniku, popř. dalšímu šíření viru.

Moderní antivirové systémy v praxi používají kombinaci všech metod, přičemž jejich přesnost a efektivita závisí zejména na aktuálnosti databáze signatur a vzorců škodlivého chování. Ve firemním prostředí je proto vhodné využít možností centrálního nastavení antiviru (s omezením jakékoliv možnosti změny konfigurace antiviru ze strany běžného uživatele), s nastavením automatických aktualizací, čímž je možné dosáhnout vysoké míry

spolehlivosti takového systému bez nutnosti fyzicky kontrolovat stav jednotlivých počítačových stanic.

3.2 Firewall

Firewall je zařízení, které pomocí jisté množiny pravidel definuje, jaký síťový provoz bude povolovat a zamítat. Jedná se tedy o oddělení a ochranu vnitřního informačního systému od vnějšího potenciálně nebezpečného prostředí. V základní konfiguraci firewall zabraňuje neoprávněnému vzdálenému uživateli v přístupu k datům, pomocí pokročilejších firewallů (ať už softwarových nebo hardwarových) je pak navíc možné kontrolovat a řídit síťový provoz oběma směry, čímž je také možné zabránit například neautorizovanému přenosu dat směrem do internetu (viry, trojské koně, spyware) nebo toho aby byl náš systém zneužit k nekalým účelům (rozesílání spamu, napadení dalších vlastních, ale i cizích systémů).

Firewally je možné rozdělit na tyto tři typy:

3.2.1 Statické paketové filtry

Statické paketové filtry kontrolují v každém paketu, který jimi prochází informace obsažené v hlavičce diagramu protokolu IP, která obsahuje zejména IP adresu odesílatele a příjemce, zdrojový a cílový port identifikující program nebo službu, které tento paket náleží. Na základě jejich vyhodnocení filtrují síťový provoz v případě, že informace uvedené v paketu neodpovídají přednastaveným pravidlům.

Oblíbeným cílem útočníků je například protokol ICMP a to jak v útocích s odepřením služeb (DoS, Denial of Service), tak ve slídění neboli obhlídce (reconnaissance) a proto jej většina statických paketových filtrů běžně blokuje. Statické paketové filtry dokážou síťový provoz kontrolovat rychleji než stavové a proxy firewally, což může být výhodné, pokud v síti probíhá útok nebo je firewall silně zatížen. [6]

3.2.2 Stavové firewally

Stavové firewally kromě běžného statického filtrování paketů navíc ve zvláštní stavové tabulce sledují aktivní spojení a dokáží zablokovat jakýkoliv síťový provoz, který neodpovídá záznamům nacházejícím se v této tabulce navázaných spojení. Jedná se výkonově náročnější řešení, které však díky tomuto vylepšení dokáže na rozdíl od statických filtrů zachytit většinu pokusů o obhlídku a také běžné typy útoků. [6]

3.2.3 Proxy firewally

Proxy firewall jsou nejvyspělejším a zároveň nejméně běžným typem firewall. Tyto firewally jsou také stavové, protože blokují nezavedená a nepovolená spojení. Proxy firewally, ale poskytují vyšší úroveň zabezpečení, protože vnitřní a vnější hostitelské systémy spolu nekomunikují přímo, ale jedině přes proxy firewall v roli prostředníka. [6]

Uživatel připojený za proxy firewallem se tedy k externímu webovému serveru připojuje následujícím způsobem:

1. Interní klient odešle do proxy firewallu požadavek na určité adresy URL
2. Proxy si vyžádá danou adresu URL od externího serveru
3. Externí server odpoví proxy firewallu
4. Proxy server odešle odpověď internímu klientu

Mezi hlavní výhody proxy firewallů v porovnání s jinými typy firewallů lze zařadit:

- vnitřní IP adresy jsou skryty za adresou proxy
- poskytují nejpřesnější auditní záznamy ze všech typů firewallů (umožňují protokolování a zasílání záznamů do syslog serverů)
- nejsou zranitelné vůči falšování IP adres (přes proxy neprochází pakety přímo do vnitřní sítě)
- umožňují zavedení autentizace uživatelů (proxy nemůže použít neoprávnění osoba ve vnitřní síti)

Proxy firewally se v sítích považují za nejbezpečnější typy firewallů. V případě jejich nasazení je však třeba pamatovat, že proxy server představuje úzké hrdlo zpomalující celou síť [6]

V praxi je ve většině případů nutné zvážit, jak moc restriktivní podmínky zvolíme, v každém případě firewall musí být natolik transparentní, aby neobtěžoval, v horším případě nebránil v práci uživateli, zároveň však musí být schopen zabránit co nejvíce útokům a odradit případné útočníky – proto se nejčastěji volí kombinace (rychlého) hraničního směrovače - statického paketového filtru a stavového firewallu umístěného za směrovačem.

3.3 Zálohování dat

Jedním ze základních prostředků, který zajišťuje provozovatelům a správcům informačních systémů jistý stupeň bezpečnosti a tedy i jistý stupeň ochrany proti dlouhodobému výpadku nebo porušení či úplnému zničení dat, je důsledné zálohování provozovaných informačních systémů.

Správci odpovědní za provoz informačních systémů musí zajistit odpovídající systém zálohování a obnovy tak, aby bylo možné obnovit plný provoz poškozeného informačního systému. Zálohována musí být data uložená v informačních systémech, data o nastavení systémů, v případě potřeby programy, operační a podpůrné systémy tak, aby mohl být provoz informačního systému obnoven v požadovaném rozsahu, čase a stáří dat.

Správci informačních systémů jsou povinni důsledně dodržovat pravidla a postupy zálohování dat informačních systémů dle předem vypracovaných zálohovacích plánů, které musí být uloženy na bezpečném místě, kde jsou v případě potřeby k dispozici odpovědným zaměstnancům. Jsou-li data archivována v zašifrované podobě, je nutno přiložit průvodní dokument popisující způsob zašifrování a místo uložení dešifrovacích klíčů či hesel.

Dle potřeby musí být aplikovány kombinace různých metod zálohování (inkrementální, plná záloha, denní, týdenní záloha atd.) tak, aby byla zajištěna co možná nejkompletnější záložní kopie dat. Dále musí být uplatňovány principy bezpečné manipulace s archivními médii a je nutné ukládat vybrané zálohy strategických IS mimo budovy s provozovaným systémem.

Dalším důležitým prvkem zajišťujícím spolehlivost obnovovacích postupů musí být jejich pravidelně prověřování a testování, aby se potvrdilo, že jsou účinné a že mohou být provedeny ve vymezeném čase.

3.4 Fyzická ochrana dat

V zájmu zajištění fyzické bezpečnosti informačních systémů je nutné, aby přístup do místností, v nichž jsou umístěny servery nebo jiná klíčová zařízení, měly pouze oprávněné osoby (obvykle administrátoři) a ostatní osoby jako jsou například servisní technici, úklidová služba, atd. pouze za přítomnosti této oprávněné osoby.

V případě neoprávněného vstupu nebo havárie, která fyzicky ohrožuje technické zařízení serverovny, je ke vstupu oprávněn pracovník ochranné služby, která je zodpovědná za bezpečnost v budově a za zpřístupnění místností v případě krajní nouze. Vstup návštěv (neoprávněných osob) do těchto prostor musí být omezen jen na předem schválené a odůvodněné případy.

Musí být veden seznam osob, které tyto prostory navštívily, a také techniků třetích stran, auditorů bezpečnosti a inspektorů. Po celou dobu těchto návštěv musí být zajištěn dozor těchto návštěv, aby bylo minimalizováno riziko ohrožení provozu a bezpečnosti IS.

Základní požadavky na zabezpečení serverových místností:

- vstupní dveře, v případě potřeby okna musí být odolná vůči vniknutí pomocí mechanického násilí s využitím jednoduchých nástrojů (rozbití, vypáčení, vyražení),
- vstupní dveře nesmí být z vnější strany opatřeny klikou umožňující jejich otevření bez klíče nebo přístupového kódu a musí být zajištěno, aby nezůstávaly otevřeny z nedbalosti,
- místnost musí být chráněna před výpadkem elektrického proudu
- místnost musí být chráněna před požárem
- místnost musí být chráněna před vysokou teplotou – klimatizace či dostatečná ventilace
- veškeré servery musí být chráněny před náhodnou manipulací – zablokování klávesnice, automatické uzamčení po určené době nečinnosti

3.5 Aktualizace operačního systému a aplikací

Výrobci pravidelně zveřejňují záplaty operačních systémů a aplikací a informují o slabinách, jež byly objeveny v průběhu existence systému. Instalace těchto záplat (patchů) je rozhodující pro zvýšení odolnosti hostitelského počítače vůči známým slabinám. Mít

nainstalované nejnovější záplaty může být časově náročné, ale je nezbytné, aby administrátoři systému znali a odstranili slabá místa dříve, než jich útočníci zneužijí [6]

Aktualizace většiny běžných operačních systémů (Windows, Linux, MAC OS) je možné nakonfigurovat na automatické stažení a instalaci nejnovějších záplat, vždy je však nutné zvážit možný dopad instalace těchto nových záplat na používané aplikace, proto se zejména ve velkých společnostech využívá možnosti řízené distribuce aktualizací s využitím interního aktualizačního serveru (např. WSUS server) nebo aplikací třetích stran. Lze tak dosáhnou toho, že na klientské stanice jsou instalovány pouze aktualizace, které jsou předem otestovány a schváleny příslušnými pracovníky dané organizace.

3.6 Ochrana proti nevyžádané poště (spamu)

Podle posledních průzkumů až 90% veškeré odeslané elektronické pošty tvoří nevyžádaná pošta, z níž nemalé procento navíc představují viry a trojské koně. Je proto zřejmé, že není na místě tento problém přehlížet a každá organizace by měla provést alespoň nějaká protiopatření k minimalizaci možných škod.

Základní funkcí antispamového filtru je roztřídění zpráv na nevyžádanou poštu a zprávy, které mají být uživateli doručeny. Všechny zprávy jsou analyzovány na základě předem určených pravidel a označovány jako podezřelé, popřípadě mohou být rovnou odstraňovány.

Metod, které jsou pro analýzu zpráv používány je mnoho, mezi základní a nejčastěji používané patří tyto dvě:

- seznamy známých spamovacích domén – tzv. DNS Blacklists
- analýza obsahu zpráv

3.6.1 DNS Blacklists (DNSBL)

Jedná se o specielně vytvořené, veřejně dostupné seznamy domén, které jsou známy tím, že jsou z nich hromadně rozesílány nevyžádané zprávy. Jeden z prvních takovýchto seznamů byl vytvořen již v roce 1997 jako reakce na velký nárůst počtu nevyžádané pošty a primárně sloužil k informování poskytovatelů internetových služeb (ISP) o tom, že jsou jimi spravované domény zneužívány k rozesílání spamu.

V dnešní době jsou tyto seznamy přímo využívány k filtrování nevyžádané pošty na straně příjemce.

3.6.2 Analýza obsahu zpráv

Tato metoda na rozdíl od DNSBL analyzuje přímo obsah přijatých zpráv, ve kterých hledá určitá slova a ohodnocuje je procentuelní pravděpodobností „spamovosti“. Pokud pak celkové hodnocení zprávy překročí nastavenou hranici (většinou 100%), je možné zprávu označit jako nevyžádanou a provést další kroky zabraňující jejímu šíření.

3.7 Komplexní zabezpečení počítačových stanic

Komplexní ochrana počítačových stanic představuje kombinaci všech výše uvedených prostředků ochrany počítačových stanic a sítě do jednoho softwarového balíku. Tento přístup ve většině případů dokáže zjednodušit správu všech komponent, což je z pohledu administrátora jasnou výhodou oproti využití jednotlivých systémů, ať už od jednoho nebo více výrobců. Nevýhodou tohoto přístupu může být nefunkčnost celého systému v případě programové chyby nebo napadení specializovaným škodlivým kódem určeným k vyřazení funkčnosti tohoto konkrétního systému.

Je důležité si uvědomit, že toto minimum tvoří ucelený systém, který lze kompromitovat nedodržením, případně neaktuálností kteréhokoliv z jeho podsystémů, proto je jeho důležitou součástí neustálá kontrola funkčnosti a aktuálnosti jednotlivých jeho složek, ale například i operačního systému celého počítače.

3.8 Autentizace uživatelů (hesla, platnost hesel, tokeny)

Metody pro autentizaci (přihlášení) uživatelů do operačních systémů je několik a nejčastěji se dělí podle toho, jakým způsobem ověřujeme uživatelovu identitu:

- ZNALOST - uživatel se prokáže znalostí, kterou „by měl“ vědět pouze on - typicky například heslo, vstupní PIN nebo například šifrovací klíč uložený na disku
- VLASTNICTVÍ – k ověření uživatele se zde používá nějaký předmět, tzv. token.
- BIOMETRIKA – měří se biometrické vlastnosti uživatele – otisky prstů, geometrie ruky, oční sítnice, atd.

3.8.1 Autentizační metoda „Znalost“

Nejstarším a v současné době pravděpodobně nejrozšířenějším způsobem získání autentizační informace je její zadání z klávesnice (důkaz znalosti něčeho – something to know). [1]

Tato metoda však také patří mezi nejméně bezpečné. Je totiž nutné zajistit, aby heslo bylo dostatečně bezpečné a zároveň pro uživatele snadno zapamatovatelné aby nedošlo k tomu, že si jej například napíše na papír, který si nalepí na monitor.

Vždy je nutné najít kompromis mezi složitostí hesla a jeho bezpečností, za nejzákladnější požadavky lze považovat tato kritéria:

- délka hesla by měla být nejméně 6 znaků
- heslo by mělo obsahovat alespoň jedno malé, jedno velké písmeno a číslici
- heslo by nemělo být snadno odhadnutelné a nemělo by se jednat o slovníkové slovo
- měla by být omezena maximální doba platnosti hesla, např. vynucením jeho změny po určité době

V rámci ústupků uživatelům se velmi často „zapomíná“ na poslední zmíněný bod, a tak není výjimkou, že například i u takových důležitých systémů jako je např. internetové bankovnictví není systémem vynuceno měnit heslo po uplynutí určitého časového období a uživatel používá jedno jediné nezměněné heslo i po dobu několika let.

Dalším dobrým pravidlem je nastavení minimálního stáří hesla, které určuje, že po nastavení nového hesla jej uživatel nesmí po jistý počet dní změnit. Tím lze zabránit v praxi docela často vídanému chování některých uživatelů, kteří si několikrát po sobě změní heslo, aby si ve výsledku mohli nastavit zpět své původní heslo.

3.8.2 Autentizační metoda „Vlastnictví“

V poslední době stále častěji používaná metoda, která od uživatele nevyžaduje, aby si pamatoval složitá hesla, ale aby vlastnil (something to have) přidělený „token“. Tím může být například USB token, čipová karta nebo bezkontaktní čip. Její hlavní nevýhodou je možnost snadného zneužití při krádeži a také jednoduchost duplikace tokenu, proto se tato metoda používá spíše pro zabezpečení objektů a docházkové systémy, pro autentizaci do důležitějších systémů je požadováno doplnění o další prvek zabezpečení – tzv. více faktorová autentizace.

Zajímavá je možnost propojení bezpečnostního předmětu s dalšími systémy podniku. Uživatel tak může mít jednu kartu pro odemykání kanceláře, docházkový systém, výdej obědů i přihlašování do počítačové sítě. [1]

3.8.3 Autentizační metoda „Biometrika“

Této metodě zcela jistě patří budoucnost. Identifikace uživatelů podle jejich biometrických údajů patří mezi nejpřesnější metody, v současné době se však jedná o finančně velmi nákladnou metodu – tedy za předpokladu, že požadujeme vysokou spolehlivost a bezpečnost použitého řešení.

3.8.4 Více faktorová autentizace

V praxi bývá využita kombinace dvou, popř. všech tří z výše uvedených metod, aby bylo dosaženo vyšší bezpečnosti.

Základní metody autentizace se pak rozšiřují na celkem 7 možností:

	A	B	C	D	E	F	G
Znalost	x			x		x	x
Token		x		x	x		x
Biometrika			x		x	x	x

Tabulka 1: Typy více faktorové autentizace [1]

Možnosti A-C, jsme probírali v minulých odstavcích – jedná se o jedno faktorové autentizace.

Možnost D je typicky realizována čipovou kartou, USB tokenem nebo autentizačním kalkulátorem (something to have) s nutností zadat PIN pro přístup k jeho obsahu (something to know). Již jen touto kombinací lze podstatně zvýšit bezpečnost celé autentizace a zabránit tak například zneužití ukradeného tokenu.

Nutností však je, aby se tento token po několikanásobném špatném zadání tohoto hesla zablokoval.

Možností „zablokování“ je hned několik:

- Automatické smazání všech informací uložených uvnitř.
- Po zablokování lze token pouze ručně smazat pomocí utilit.
- Pro odblokování se musí zadat další kód, většinou označovaný jako PUK.
- po zadání kódu PUK má uživatel s heslem/pinem dalších 10 pokusů.
- po zadání PUK může ten, kdo zná PUK kód nastavit nové heslo/PIN.

Nejlepším řešením z hlediska bezpečnosti je pravděpodobně první z možností, je však nutné pamatovat na možnost úmyslného zablokování tokenu například zlomyslným kolegou, který záměrně zadá chybně heslo, aby byly certifikáty a digitální ID v něm

uložené zničeny. Proto je důležité i tzv. „připoutání k tělu“, které spočívá v tom, že se token použije například i pro vstup do budovy/kanceláře, čímž se značně snižuje pravděpodobnost, že uživatel token při odchodu z pracoviště zapomene na stole a někdo jej zneužije.

Možnosti E – G se v praxi využívají výrazně méně. Vyplatí se pouze tam, kde je nutné dosáhnout velmi vysokého stupně zabezpečení a je tak možné akceptovat vysokou finanční náročnost celého řešení.

3.9 Šifrování dat

V obecné rovině existují dva způsoby jak chránit data. Je možné je zaheslovat nebo zašifrovat. Mezi těmito dvěma přístupy existuje zásadní rozdíl v tom, že heslování pouze omezuje přístup k datům, zatímco šifrování pracuje přímo s daty, jejichž obsah se šifrou mění a není tedy tak snadné dostat se k jejich původnímu obsahu.

K šifrování se využívá mnoho metod, které lze podle způsobu využití šifrovacích klíčů rozdělit na tyto dvě skupiny:

3.9.1 Symetrické šifrování

Symetrické šifrování je založeno na jednom šifrovacím klíči, kterým lze zprávu jak zašifrovat, tak i dešifrovat.

Z bezpečnostního hlediska je nevýhodou jednoznačně to, že se používá pouze jeden klíč, který je příjemci šifrované zprávy nutné doručit bezpečným způsobem. Nedoporučuje se odesílat klíč stejným kanálem jako samotnou zprávu a to ani s delším časovým odstupem, protože v případě odposlechu klíče i zprávy není problém takto zašifrovaná data rozluštit.

Nejčastěji používané algoritmy symetrického šifrování:

Algoritmus DES (Data Encryption Standard)

Tento algoritmus byl vyvinut již v polovině 70. let minulého století ve společnosti IBM. Jeho podstatou je šifrování textu (dat) rozděleného po 64 bitových blocích. Šifrovací klíč je také 64 bitový, ale pouze 56 bitů je použito pro kódování a každý osmý bit je paritní. V současné je již 56 bitový klíč algoritmu DES nedostačující a dnešními technickými prostředky – výpočetním výkonem hrubou silou prolomitelný, proto byl zaveden algoritmus 3DES, který na každý datový blok aplikuje 3 klíče DES a vzniká tak 168 bitová šifra.

Díky tomuto trojnásobnému šifrování je ale tento algoritmus velmi pomalý a prakticky použitelný pouze pro menší objemy dat.

Algoritmus AES (Advanced Encryption Standard)

AES byl vytvořen na zakázku vlády Spojených států Amerických, která potřebovala šifrovací algoritmus pro ukládání svých dokumentů. Stejně jako u DES jde o blokový šifrovací algoritmus, výchozí velikost bloku je zde ale 128bitů. Pokud jsou šifrovaná data delší, jsou rozdělena právě na tyto 128bitové bloky a po jednom zpracována. Pokud jsou data kratší, je nutné je doplnit na odpovídající délku.

Délka klíče může být 128bitů, 192bitů nebo 256 bitů.

Algoritmus CAST

CAST je 128 bitový algoritmus, který vyvinuli Stafford Taveres a Carlisle Adams. Jeho velkou výhodou je rychlost a to, že je volně dostupný k použití. Právě proto je velmi často využíván vývojáři Open Source aplikací, např. ve známém PGP k šifrování elektronické pošty.

Algoritmus IDEA (International Data Encryption Algorithm)

Poslední ze symetrických šifer, kterou zde uvedu je IDEA. Bloková šifra zveřejněná až v roce 1992 o délce bloku 64 bitů s klíčem dvojnásobné velikosti, tedy 128 bitů. Je to poměrně dobře navržená silná šifra schopná rychle (zhruba 2x rychleji než DES) zpracovávat velká množství dat, bohužel se jedná o patentovanou technologii, která není dostupná pro širokou veřejnost. To je také důvod, proč se i přes své výhody příliš nerozšířila.

3.9.2 Asymetrické šifrování

Tato metoda byla vyvinuta Whitfieldem Diffiem a Martinem Hellmanem v roce 1975. Na rozdíl od symetrického šifrování využívá dvou klíčů:

- veřejný klíč – tento klíč slouží jen k zašifrování dat a je tedy možné jej například zveřejnit na webovém serveru nebo poslat odesílateli nezabezpečeným způsobem
- soukromý klíč – klíč je použitelný jen k rozšifrování dat, která byla zašifrována odpovídajícím veřejným klíčem. Tento klíč je nutné uchovat v tajnosti.

Algoritmus RSA

Jednou z prvních a i přes to dnes jednou z nejpoužívanější šifrou tohoto typu je algoritmus RSA, pojmenovaný po svých tvůrcích, kterými byli Ron Rivest, Adi Shamir a Len Adleman. Byla vyvinuta v roce 1977 a využívá možností modulární aritmetiky, resp. složitosti až nemožnosti zpětného rozkladu dostatečně velkého čísla na součin dvou prvočísel, z jejichž kombinace bylo vytvořeno.

Obrázek 4: Princip asymetrického šifrování pomocí soukromého a veřejného klíče [vlastní tvorba]

Zdálo by se, že symetrické šifrovací algoritmy v porovnání s konkurencí v podobě asymetrických šifer nemají budoucnost, ale skutečností je, že většina dnešních produktů stále ještě využívá symetrických šifer. Jejich výhodou je totiž až 100x vyšší rychlost šifrováni a dešifrování v porovnání s asymetrickými algoritmy, což je například v případě šifrování velkých objemů dat na discích prioritou. V tomto konkrétním případě navíc není nutné jakkoliv předávat šifrovací klíč – ten kdo data šifruje, je zároveň i dešifruje.

Algoritmů je samozřejmě velké množství, některé z nich jsou již považovány za technologicky zastaralé anebo existuje metoda jak jejich šifru prolomit, další šifry teprve vznikají nebo jsou na vzestupu.

4 FYZICKÁ BEZPEČNOST

4.1 Mechanické zábranné systémy

Mechanické zábranné systémy (MZS) jsou považovány za základní prvek ochrany objektů a osob v průmyslu komerční bezpečnosti. Pod MZS řadíme veškeré mechanické prvky, které ztěžují násilné vniknutí nepovolaných osob do chráněné zóny nebo objektu především přes oplocení nebo cestou dveřních a okenních otvorů. [2]

Základní úlohou MZS tedy je vytvořit překážku, na jejíž překonání musí pachatel vynaložit určité úsilí. Doba potřebná k překonání MZS by měla být co nejdelší a měla by ideálně zabránit násilnému proniknutí do chráněné zóny v době kratší než je doba potřebná k zalarmování a přivolání ostrahy. [2]

Základní úlohou MZS je tedy zabránit:

- násilnému proniknutí osoby do chráněné zóny
- znehodnocení techniky a zařízení uvnitř chráněné zóny
- krádeži předmětů a dalších hodnot z prostoru chráněné zóny
- umístění nebezpečného předmětu ve chráněném prostoru

Podle normy ČSN EN 50131 lze mechanické zábranné systémy rozdělit do těchto tří ochranných zón:

Obvodová ochrana

Zajišťuje bezpečnost okolo daného objektu. Obvodem objektu se většinou rozumí jeho hranice realizované obyčejně přírodními nebo umělými překážkami (vodní toky, ploty, zdi, apod.). Prostředky obvodové ochrany mají za úkol upozornit osobu, že vstupuje do vymezeného prostoru, případně slouží k zabránění vstupu do tohoto prostoru.

Do této skupiny lze zařadit:

- zdi a ploty
- průchozí prvky u zdí a plotů (brány, otvory, atd.)
- vrcholová ochrana (ostnatý drát, hroty, apod.)
- visací zámky, petlice, turnikety, atd.

Plášťová ochrana

Základním prvkem plášťové ochrany, která slouží proti vniknutí narušitele do střeženého prostoru je stavební konstrukce objektu.

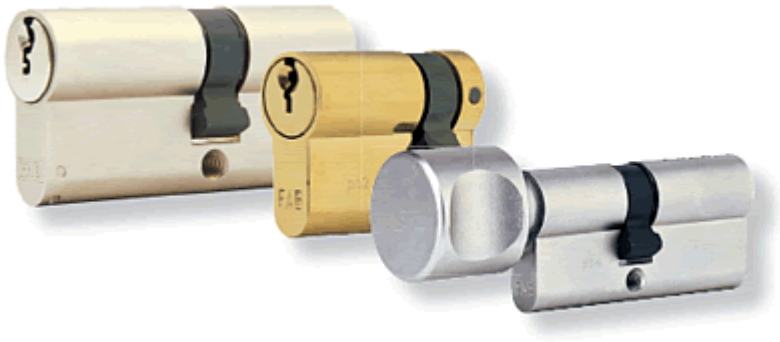
Do této skupiny lze zařadit:

- okna a dveře
- mříže
- ostatní otvory, kterými lze do střeženého objektu vstoupit.

Individuální ochrana

Všechny bezpečnostní prvky, jejichž úkolem je ochrana a zabezpečení uložených cenných předmětů, peněz, dokumentů a jiných aktiv před odcizením.

Především to mohou být: zámky, trezory, přepážky, ohnivzdorné skříně a další zařízení přímo chránící majetek a věci, které mají pro společnost nebo jednotlivce nějakou cenu.



Obrázek 5: Předmětová ochrana – bezpečnostní zámky [21]

Pyramida bezpečnosti

Pyramida bezpečnosti je jednotící prvek, který usnadňuje a zpřehledňuje identifikaci výrobků s ověřenou úrovní jakosti. Požadavky na výrobky zařazené do pyramidy bezpečnosti jsou přitom sjednoceny s požadavky pro certifikaci NBÚ. Nabízí jednoduchou orientaci při výběru mechanických zábran. Značení výrobků podle pyramidy bezpečnosti je v souladu s požadavky na zabezpečení majetku.

Výrobky jsou zařazeny do čtyř skupin na základě certifikace podle normy ČSN P ENV 1627. Jednotlivé stupně bezpečnosti jsou na obalech výrobků odlišeny barvou a číslem. Základním předpokladem zařazení výrobků do systému pyramidy bezpečnosti je jeho

přezkoušení zkušební laboratoří a u certifikačního orgánu pak následná certifikace odolnosti výrobku proti násilnému vniknutí. [21]

Obrázek 6: Pyramida bezpečnosti [21]

4.2 Poplachové zabezpečovací a tísňové systémy

Poplachový zabezpečovací a tísňový systém je v normě ČSN EN 50131 definován jako systém na detekci a indikaci přítomnosti, vstupu anebo pokusu narušitele o vstup do chráněného prostoru. Pro dosažení maximální účinnosti by měl být poplachový zabezpečovací a tísňový systém kombinován s vhodnými prostředky a postupy fyzické bezpečnosti. [22]

Touto normou jsou zároveň definovány čtyři stupně zabezpečení:

Stupeň 1: Nízké riziko

> Předpokládá se, že lupič nebo vetřelec mají malou znalost zabezpečovacích a tísňových systémů a mají k dispozici omezený sortiment snadno dostupných nástrojů.

Stupeň 2: Nízké až střední riziko

> Předpokládá se, že lupič nebo vetřelec mají omezenou znalost zabezpečovacích a tísňových systémů a používání běžného nářadí a přenosných přístrojů.

Stupeň 3: Střední až vysoké riziko

> Předpokládá se, že lupič nebo vetřelec jsou obeznámeni se zabezpečovacími a tísňovými systémy a mají rozsáhlý sortiment nástrojů a přenosných přístrojů.

Stupeň 4: Vysoké riziko

> Používá se, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponent zabezpečovacích a tísňových systémů.

Je žádoucí, aby všechna použitá zařízení a jejich součásti odpovídaly co nejvyššímu stupni na základě požadavků stanovených při analýze a následném návrhu celého bezpečnostního systému.

V praxi se nejčastěji používají tyto tři základní typy aktivních technických prostředků ochrany majetku:

- elektronické zabezpečovací systémy
- kamerové systémy
- systémy kontroly a řízení vstupu

4.2.1 Elektronický zabezpečovací systém

Základem celého systému je tzv. ústředna EZS, která musí být umístěna v prostoru s co nejvyšším možným stupněm zabezpečení, aby byla co nejvíce eliminována možnost ovlivnění její činnosti zvenčí. Ústředna EZS zejména:

- ovládá signalizační, přenosová, zapisovací a jiná zařízení
- přijímá a vyhodnocuje signály přijímané od detektorů
- napájí jednotlivé komponenty EZS elektrickou energií
- za použití elektromagnetických nebo kódových zámků umožňuje změnu stavu celého systému EZS
- umožňuje diagnostiku systému EZS [2]

4.2.1.1 Režimy EZS

Běžná ústředna EZS dokáže pracovat v těchto režimech:

Vypnuto (DISARM)

Ústředna je neaktivní - po objektu je možné se pohybovat a narušení detektoru je ústřednou ignorováno.

Vypnutí systému probíhá ve většině případů tak, že pokud oprávněná osoba vstoupí do střeženého prostoru, je aktivován čas, do kterého musí být systém převeden do klidového režimu, jinak je vyhlášen poplach.

Zapnuto (ARM)

Ústředna je ve stavu hlídání, v objektu se nikdo nepohybuje a na narušení detektoru ústředna reaguje dle programu poplachem. Nezbytnou podmínkou pro přechod systému do tohoto stavu je to, aby byly všechny zóny v klidu. Díky této vlastnost většiny dnešních ústředen se vylučuje např. opomenutí uzavření dveří případně přítomnost další osoby v objektu – osoba obsluhující klávesnici je na stav upozorněna a není ji umožněno převést systém do stavu ARM.

Zapnuta plášťová ochrana (STAY)

V tomto režimu jsou detektory rozděleny na dvě skupiny. První skupina je zařazena do hlídání a tvoří plášťovou ochranu, druhá je z režimu hlídání vyřazena a její signály o narušení jsou ignorovány. Tento stav umožňuje pohyb osob v hlídaném prostoru s detekcí proti narušení z vnější strany.

Režim podsystémů (AREA)

Některé zabezpečovací ústředny je možné dělit na podsystémy. Hlídaný objekt je rozdělen na samostatné části, které lze zapínat a vypínat samostatně.

4.2.1.2 Typy zón EZS

Každý nainstalovaný detektor může být v ústředně zařazen do jedné nebo více zón. Programově se volí vlastnosti zón a druh reakce systému na narušení detektoru. Uvedené typy zón jsou opět používané u většiny EZS. V následujícím výčtu jsou uvedeny nejčastěji používané typy zón a způsob rekce na jejich narušení.

Okamžitá zóna

Vypnuto - Narušení detektoru je ignorováno

Zapnuto - Narušení detektoru způsobí okamžitě poplach

Zpožděná zóna

Vypnuto - Narušení detektoru je ignorováno

Zapnuto - Narušení detektoru spustí čas pro příchod. Během tohoto času musí být zadán platný kód a systém musí být vypnut. Pokud není systém vypnut do stanoveného času pro příchod, je aktivován poplach.

24 hodinová zóna

Vypnuto - Narušení detektoru způsobí okamžitě poplach

Zapnuto - Narušení detektoru způsobí okamžitě poplach

Plášťová zóna (STAY)

Vypnuto - Narušení detektoru je ignorováno

Zapnuto - Narušení detektoru způsobí poplach

STAY - Narušení detektoru je ignorováno - pokud je ústředna zapnutá v režimu STAY (plášťová ochrana) pak narušení zóny definované jako STAY je ignorováno. Ostatní zóny reagují dle nastavení.

4.2.1.3 Detektory EZS

Mezi běžné používané detektory využívané v systémech EZS patří:

Infračervené detektory pohybu (Pasivní infračervené detektory)

V současnosti nejčastěji používané detektory jsou založeny na pasivním infračerveném snímání pozadí a v případě, že dojde k pohybu jakéhokoliv „teplého objektu“ v dosahu detektoru je vyhlášeno narušení. Detektor se skládá z IR senzoru a z čočky, která dělí hlídaný prostor do zón. V případě, že pohybující osoba vstoupí do jedné z těchto zón je zaznamenán nárůst IR signálu, v opačném případě – pokud osoba zónu opustí, je senzorem zaznamenán pokles. Při pohybu osoby po prostoru tedy dochází ke střídání nárůstu a poklesu IR signálu, který je vyhodnocován elektronikou čidla a v případě, že charakteristika odpovídá pohybu osoby, je vyhlášen poplach.

I přes značnou odolnost současných detektorů proti falešným poplachům je při instalaci třeba dodržovat určité zásady. Jednou z nejdůležitějších je potřeba zamezit tomu aby čidlo detektoru „vidělo“ na zdroje sálajícího tepla (horkovzdušné topení, kamna, krb, infra

zářiče). Problémem může být i Slunce, které je poměrně silným IR zdrojem a může způsobovat falešné poplachy.

Mikrovlnné detektory pohybu

V tomto případě se jedná se o aktivní detektor - obsahuje vysílač a přijímač mikrovlnného signálu nejčastěji s frekvencí kolem 10GHz. K detekci pohybu je využíván princip Dopplerova jevu, kdy se vyhodnocuje odražená vlna od objektu. Pokud se tedy v oblasti dosahu detektoru pohybuje osoba, mění se takto odražená vlna a detektor vyhlásí narušení. Tato vlastnost umožňuje použít detektor v prostorách, kde IR detektor použít nelze. Problémem této technologie je malá odolnost k rušení jinými detektory stejného typu, zářivkovými světelnými zdroji a také snadné pronikání mikrovlnného signálu sklem a tenkými stěnami (sádrokarton, dřevo). Tato vlastnost může být důvodem častějších falešných poplachů, například narušením způsobeným osobou pohybujícím se mimo hlídanou místnost.

Magnetické kontakty

Slouží k detekci otevření oken a dveří – jsou založeny na jednoduchém principu rozpojení dvou elektricky vodivých kontaktů, čímž dojde k přerušení obvodu a je možné s poměrně velkou přesností a spolehlivostí detekovat narušení stráženého prostoru.

Akustické detektory rozbití skla

Pracují na principu akustického sledování prostoru. Vyhodnocují slyšitelnou část zvuku, která vzniká tříštěním skla a tlakovou vlnu, která vzniká v okamžiku rozbíjení skla. Obsahují mikrofon, pomocí kterého jsou tyto dvě složky monitorována a vyhodnocovány.

Otřesové detektory

Používají se nejčastěji pro hlídání zdí, trezorů, dveří a všech ploch, které lze překonat destrukčním způsobem. Snímacím prvkem je většinou piezoelektrický prvek, na kterém při jeho chvění vzniká napětí. Takto vzniklé napětí je vyhodnocováno a dle jeho průběhu a intenzity je vyhlášeno narušení. Detektor schopen zaznamenat rázy (kladivo, sbíječka) i opakované chvění způsobené například řezáním nebo plamenem.

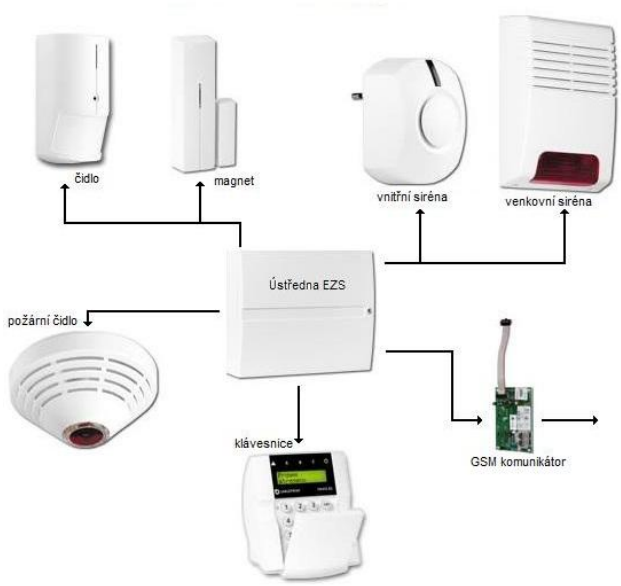
Infrazávory

Obsahují dvě části. V jedné je aktivní vysílač infračerveného záření, který je detekován přijímačem umístěným ve druhé samostatné časti. V okamžiku, kdy je IR paprsek přerušen, je vyhlášeno narušení. Infrazávory lze použít na detekci průchodu osob plochou, případně i jako obvodová ochrana území nebo objektu.

Podle normy ČSN EN 50131 musí každý systém EZS v souladu se svou konfigurací splňovat alespoň tyto funkční požadavky:

- detekce vniknutí – čidla musí být konstruovány tak, aby byla maximalizována detekce skutečného vniknutí a minimalizováno riziko planých poplachů
- detekce sabotáže – komponenty EZS, musí obsahovat prostředky zamezující v přístupu k jejich vnitřním součástkám, celý systém pak musí být schopen odhalit a pokusit se odeslat zprávu o možné sabotáži.
- rozpoznání poruchy – systém musí být schopen odhalit a nahlásit poruchu každé své jednotlivé součásti – např. na základě nefunkčnosti periodické komunikace s touto vadnou komponentou

Samotná složitost implementace těchto požadavků je určena především požadovaným stupněm zabezpečení celého EZS.

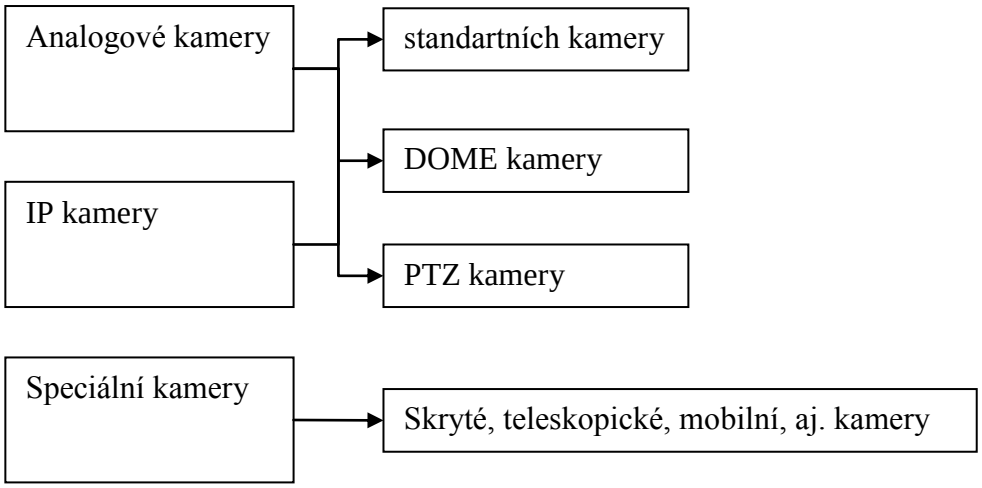


Obrázek 7: Příklad jednoduchého zapojení prvků EZS [23]

4.2.2 Kamerové systémy

Kamerový bezpečnostní systém je využitelný nejen jako monitorovací zařízení schopné v případě bezpečnostního incidentu poskytnout vyšetřovatelům důkazní materiál, ale nové technologie těchto systémů již v dnešní době umožňují i samotnou detekci pachatele v případě narušení chráněného prostoru. [27].

Základní dělení kamer:



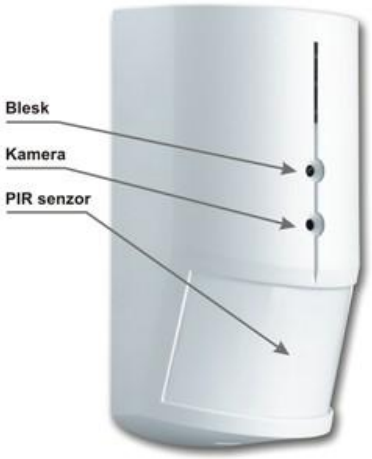
Obrázek 8: Základní dělení kamer
[vlastní tvorba]

Základní rozdíl mezi analogovými a IP kamerami (drátovými i bezdrátovými) je ve způsobu přenosu dat. Zatímco u analogových kamer dochází ke konverzi obrazu na elektrické veličiny (napětí a proud), které jsou zobrazovány, popř. ukládány na záznamová zařízení, u IP kamer dochází k přenosu informací pomocí IP protokolu a mohou být tedy přímo dostupné na internetu. Implementace zapojení analogové kamery je jednodušší, IP kamery již však v dnešní době poskytují vyšší komfort užívání i vyšší rozlišení, proto jsou i přes vyšší nároky na infrastrukturu nasazovány mnohem častěji.

Obrázek 9: Příklad kompaktního kamerového systému [18]

Kvůli nedostatkům běžných statických (ale i otočných kamer), pak vznikly:

- DOME kamery – velmi odolné vůči úmyslnému poškození nebo vandalům, nejčastěji montované do průhledného kopulovitého krytu umístěného na zdi nebo stropě,
- PTZ kamery (Pan Tilt Zoom) - jsou vybaveny možností otáčení a naklánění kamery ve všech směrech až v úhlu 360 stupňů, díky čemuž je možné minimalizovat tzv. hluchá místa běžná u klasických kamer,
- Speciální kamery - méně běžné a určené pro předem přesně vymezené použití. Do této skupiny jsou zařazovány například skryté kamery maskované jako PIR detektor, teleskopické a mobilní kamery.



Obrázek 10: Bezdrátový PIR detektor s kamerou [25]

Tyto systémy však i přes jejich dynamický vývoj nedokáží zaručit 100% garanci detekce pachatele a proto je nutné je implementovat v kombinaci s EZS.

4.2.3 Systémy kontroly a řízení vstupu

Systémy kontroly a řízení vstupu dokážou regulovat přístup osob, resp. vozidel do chráněných prostor nebo ke chráněným zařízením, případně informacím, na základě přidělených přístupových práv. Tato zařízení umožňují sledovat pohyb osob v definovaných prostorových zónách, k čemuž využívají koncové akční prvky, např. elektrické zámky, turnikety, brány, propusti a další. Jako nositel přístupového oprávnění jsou využívána různá média, např. magnetické a čipové karty, čipové přívěšky různých tvarů a nejnověji se využívá biometrických informací, jako jsou např. otisky prstů, zobrazení oční duhovky nebo sítnice nebo obraz obličeje. [22]

4.3 Elektronická požární signalizace

Elektronická požární signalizace je soubor technických zařízení sloužících k detekci požáru a vyvolání poplachu. Nejčastěji bývá integrální součástí EZS, na nějž jsou zapojeny hlásiče požáru. Na ústředně EZS je pak možné nastavit jak má celý systém na signály z těchto detektorů reagovat - nejčastěji tedy dojde k automatickému odeslání hlášení dohledovému centru nebo přímo nejbližšímu útvaru Hasičského záchranného sboru.

Požární hlásiče lze podle principu činnosti rozdělit takto:

- manuální
- automatické

Manuální požární hlásiče slouží k vyhlášení poplachu osobou, která požár nebo jiný nebezpečný stav zjistí. Tlačítkové požární hlásiče jsou vždy červené barvy a musejí být uzpůsobeny tak, aby nemohlo dojít k jejich samovolné nebo náhodné aktivaci.

Automatické požární hlásiče jsou zařízení, která reagují na průvodní jevy požáru automaticky a odesílají tuto informaci bez zásahu zvenčí. Nejlepším umístěním detektoru je střed stropu místnosti, jejíž prostor je třeba střežit. Pokud nelze detektor umístit do středu místnosti, je dobré jej umístit co nejblíže středu, v krajním případě alespoň 20cm od rohu místnosti [26]

V současné době se nejvíce využívají detektory založené na těchto dvou principech:

Opticko-kouřové detektory

Uvnitř detektoru je vyhodnocovací komůrka, která je prosvětlována IR diodou a je vyhodnocována světelná ztráta. Pokud se do detektoru dostane kouř, vzroste ztráta infračerveného signálu nad vymezenou mez a detektor vyhlásí poplach. Nevýhodou tohoto typu detektorů je možnost zvýšeného rizika falešných poplachů v prašném prostředí. Výhodou je reakce již na kouř, kdy je možné zachytit požár již ve fázi doutnání a zabránit tak větším škodám než je nezbytně nutné.

Tepelné detektory

Pracují na principu vyhodnocování nejvyšší teploty v místnosti a modernější modely mohou také vyhodnocovat rychlost nárůstu teploty. Pokud je překročena maximální nastavená teplota nebo je detekován vyšší nárůst teploty než je povoleno, je vyvolán poplach. Tepelné detektory nejsou tak náchylné na prach a nečistotu, k jejich aktivaci je však třeba plamen, který způsobí nárůst teploty. Reagují tedy na požár s určitým zpožděním.

Kombinované (opticko-kouřové) detektory

Využívají předností obou metod – kdy k vyhlášení poplach stačí překročení parametrů jen jedné ze sledovaných veličin.

Ionizační detektory

Tento typ detektoru využívá malého radioaktivního zářiče, který s využitím ionizujícího záření detekuje kouř vycházející z ohniska požáru. S ohledem na závažnost ohrožení lidského zdraví a životního prostředí nejsou tyto detektory příliš vhodné pro prostory s trvalým pobytem osob (byty, kanceláře, apod.).

Ostatní a speciální typy detektorů

Existuje samozřejmě velké množství různých dalších typů detektorů, mezi které patří například tlakové a odporové hlásiče EPS, které pracují na principu detekce změny tlaku, popř. odporu při změně tepelných vlastností ve střeženém prostoru, případně i speciální typy jakou jsou například lineární optické detektory, které pracují na podobném principu jako infra závory v případě EZS – obsahují dva prvky, z nichž jeden signál vysílá a druhý přijímá a detekuje se přerušení procházejícího signálu, v tomto případě však ne narušitelem, ale kouřem.

5 HAVARIJNÍ PLÁNOVÁNÍ

Havarijní plány by měly být vypracovány pro všechny provozované informační systémy, popř. alespoň pro ty, které jsou označeny jako kritické a jejichž zničení, poškození nebo i krátkodobý výpadek může pro organizaci znamenat vážné ohrožení.

Tyto dokumenty, musí obsahovat především podrobné informace o:

- zvolené strategii obnovy
- akceptovatelné době výpadku (ADV)
- kritickém období informačního systému (ekonomické závěrky, apod.)
- základních vlastnostech stávajících provozních komponent
- základních vlastnostech náhradních komponent
- umístění a odpovědnosti za náhradní technologie
- alternativním umístění části nebo celého systému
- zálohování a instalačních médiích
- servisních a dodavatelských organizacích
- personálním obsazení havarijního týmu

Při výběru nejvhodnějších strategií obnovy se nejčastěji vychází ze stanovených akceptovatelných dob výpadku (ADV), které v praxi vymezují dobu, během níž by měla být havárie informačního systému odstraněna. Samozřejmě, že je nutné zohledňovat také případné další dopady havárie, jako jsou například ztráta know-how, možné poškození dobrého jména podniku nebo v případě státní správy i možné finanční postihy za nedodržení zákonných ustanovení, která jsou pro organizaci závazná.

Takto stanovenou ADV lze navíc zkrátit organizačními opatřeními, jako jsou například:

- unifikace technického vybavení – v případě, že organizace vlastní více komponent, např. serverů je výhodné, aby byly totožné nebo alespoň snadno zaměnitelné. V případě poškození kritického IS je pak možné jeho provoz obnovit v relativně krátkém čase.
- dohody s dodavateli – smluvním zajištěním podmínek včasného dodání důležitého vybavení nebo služeb dodavatelem kritického systému lze dosáhnout výrazného zkrácení ADV

- pohotovostní zásoby – vybrané důležité systémové zdroje je vhodné držet jako skladové zásoby, které lze v případě havárie ihned nasadit do provozu místo poškozené komponenty.

Podle možností organizace je pak navrženo jedno z těchto řešení obnovy dat:

Studená záloha (cold site) – tato záloha představuje předem vytipované vhodné prostory, částečně vybavené základní infrastrukturou (zdroje elektrické energie, telekomunikační přípojky, přípojky do sítí LAN, WAN apod.). Tyto prostory je možné dle havarijního plánu konkrétního systému během několika dnů vybavit potřebnou technikou a spustit v těchto prostorách alespoň částečný provoz daného informačního systému.

Teplá záloha (warm site) - tato záloha představuje dostupné vhodné prostory s potřebnou síťovou vybaveností, ve kterých je umístěna část nebo všechny potřebné plně provozuschopné systémové zdroje IS nebo aplikace. Podle potřeb daného systému je předinstalováno potřebné programové vybavení, aktuální konfigurace a data jsou doplněna ze záloh. Předpokládaná doba poskytování služeb tohoto záložního zařízení může dosáhnout několik měsíců.

Horká záloha (hot site) – tato záloha představuje dostupné, plně provozuschopné záložní výpočetní centrum, disponující všemi záložními systémovými zdroji vybraných strategických informačních systémů. Tyto zdroje budou využity v případě havárie, kdy vzhledem k jejímu rozsahu není možné v rámci tolerované doby výpadku zajistit obnovení provozu v původní lokalitě. Toto záložní centrum je vybaveno veškerou potřebnou technikou, programovými prostředky a komunikačními službami včetně aktuálních konfigurací a parametrizace a základní datové základny (data jsou průběžně do záložního centra instalována offline např. 1x měsíčně ze záloh) tak, aby bylo možné po implementaci posledních dostupných záloh dat v horizontu několika hodin obnovit provoz kritických informačních systémů. Předpokládaná doba poskytování služeb tohoto záložního centra může dosáhnout několik měsíců.

Zrcadlová záloha (mirror site) - jedná se o plně redundantní zařízení s plným, v reálném čase prováděným, zrcadlením informací. Tato záloha je zcela identická s primárním systémem a poskytuje nejvyšší stupeň přístupnosti systému, protože zpracovávaná a ukládaná data jsou současně ukládána do primárního i zrcadlového systému.

II. PRAKTICKÁ ČÁST

6 POPIS A ANALÝZA SOUČASNÉHO STAVU

6.1 Základní údaje o svěřeném majetku

Katastrální úřad využívá k plnění svých úkolů majetek státu, k němuž má v souladu s § 9 zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupováním v právních vztazích příslušnost hospodařit.

Majetek musí být využíván účelně, efektivně a hospodárně včetně potřebného zajišťování oprav a údržby tak, aby nedošlo ke snížení jeho rozsahu a hodnoty. Jediným omezujícím faktorem při správě majetku jsou disponibilní finanční prostředky na opravy a údržbu budov.

KÚ pro Zlínský kraj využívá pro svou činnost 3 budovy ve vlastnictví státu - budova Katastrálního pracoviště Holešov, budova Katastrálního pracoviště Kroměříž, budova Pozemkové knihy v Uherském Hradišti. V budově Katastrálního úřadu pro Zlínský kraj a Katastrálního pracoviště Zlín má KÚ příslušnost hospodařit s 65/100 vlastnického podílu státu, v budově Katastrálního pracoviště Vsetín má příslušnost hospodařit s 57/100 vlastnického podílu státu a v budově Katastrálního pracoviště Uherský Brod má příslušnost hospodařit s 31/100 vlastnického podílu státu. Prostory katastrálních pracovišť ve Valašském Meziříčí, Uherském Hradišti a Valašských Kloboukách jsou v nájmu.

Jedna z nemovitostí ve vlastnictví státu, k níž má příslušnost hospodařit KÚ, je zatížena věcným břemenem vstupu a vjezdu na pozemek pro Geodezii Brno, a.s. dle smlouvy o věcném břemeni ze dne 22. 6. 2000.

Obrázek 11: Sídla katastrálních pracovišť KÚ pro Zlínský kraj
[vlastní snímek]

Údržba a správa majetku jsou zajišťovány kombinovaným způsobem, tzn. jak vlastními zaměstnanci, tak i externími společnostmi. Ostatní služby, jako je např. ostraha a hlídací služby, stravovací služby, revize zařízení, konzultační a poradenské služby jsou zajišťovány výhradně dodavatelsky.

6.2 Informační bezpečnost

6.2.1 Rozdělení počítačových stanic

6.2.1.1 Rozdělení podle použité platformy

Pracovní stanice a notebooky v počítačové síti ČÚZK, jejíž součástí je i počítačová síť Katastrálního úřadu pro Zlínský kraj, jsou provozovány na následujících platformách:

Typ stanice	Operační systém	
Pracovní stanice	Microsoft Windows XP	32bit
	Microsoft Windows 7	32 / 64bit
Notebooky	Microsoft Windows XP	32bit
	Microsoft Windows Vista	32bit
	Microsoft Windows 7	32 / 64bit

Tabulka 2: Operační systémy provozované na pracovištích KÚ pro Zlínský kraj

Standardním operačním systémem pro běžné uživatele je v současné době Microsoft Windows XP Proffesional ve 32bitové edici, stanice a notebooky s novějšími verzemi tohoto operačního systému jsou určeny pouze pro pracovníky oddělení podpory ICT a zaměstnance s přidělenými služebními notebooky, jejichž součástí je přeinstalovaná některá z novějších verzí tohoto operačního systému.

Žádné starší operační systémy (Windows 95, 98, ME) ani jiné varianty uvedených OS (zejména Windows XP Home Edition) není dovoleno na počítačích provozovat – zejména z důvodu, že v nich není implementována podpora funkcí domény.

V případě potřeby výjimky z tohoto pravidla je nutné získat schválení od ředitele odboru informatiky ČÚZK na podkladě písemné a řádně zdůvodněné žádosti.

6.2.1.2 Rozdělení podle způsobu využití

Administrátorské pracovní stanice:

- využívají se k administraci komponent počítačové sítě
- uživatelé musejí být členy oddělení podpory ICT nebo informatiky katastrálních pracovišť, v případě nutnosti zařazení zaměstnance jiného útvaru je nutný písemný souhlas vedoucího oddělení podpory ICT, popř. jemu nadřízeného vedoucího zaměstnance

- na těchto stanicích jsou uživatelé zařazeni do skupiny Security4 a současně do lokálních skupin Power Users, popř. Administrators

Standardní pracovní stanice:

- využívají se k běžné práci zaměstnanců zejména s Informačním systémem katastru nemovitostí (ISKN)
- výjimečně se využívají jako servery pro některé aplikace, popř. intranetové servery
- využívají se pro testování aplikací, operačních systémů, apod.
- omezení pro uživatele jsou pak definována bezpečnostními politikami odpovídajícími bezpečnostní skupinou přiřazenou konkrétnímu uživateli.

Pracovní stanice pro odbornou veřejnost:

- jedná se o počítače přístupné pro odbornou veřejnost v k tomu vyhrazených veřejně nepřístupných prostorách
- jsou automaticky zařazeny do nejnižší možné bezpečnostní skupiny
- jedinou přístupnou aplikací je zde ISKN – popř. další schválené aplikace umístěné přímo na ploše (do ostatních složek, na disky a k aplikacím které zde nejsou umístěny, nemá uživatel přístup)
- uživatel nemá možnost jakkoliv měnit konfiguraci počítačové stanice
- na tyto stanice jsou aplikovány filtry pomocí politik zabezpečení protokolu IP, které zabraňují přístupu na všechny adresy, které nejsou explicitně povoleny
- jsou zde zakázána jakákoliv úložná zařízení (CD / DVD / USB porty) – zakázáním v BIOSu nebo mechanickým zabezpečením
- na PC je možné pracovat jen pod dohledem zaměstnance úřadu
- jediným možným výstupem je předem nastavená síťová tiskárna – ke které však nemá odborná veřejnost přímý přístup – tiskové výstupy podléhají kontrole zaměstnancem úřadu.

Pracovní stanice pro nahlížení do katastru nemovitostí, tzv. kiosky:

- počítače dostupné v nehlídaných prostorách určené laické veřejnosti
- jsou automaticky zařazeny do bezpečnostní skupiny Security0
- jedinou přístupnou aplikací je zde webová aplikace „Nahlížení do katastru nemovitostí“, která je také dostupná na adrese http://nahlizenidokn.cuzk.cz/

- na těchto stanicích je zabráněno přístupu do jakýchkoliv jiných systémů a jsou zde aplikována pravidla zabraňující uživateli provést jakoukoliv akci, která mu není povolena
- samotné stanice jsou umístěny v uzavřených uzamykatelných boxech zabraňujících uživateli v přímém přístupu k pracovní stanici a jakékoliv fyzické manipulaci s nimi

Zaměstnanecké notebooky:

- využívají se k práci v počítačové síti katastrálního úřadu nebo off-line, bez připojení do jakékoliv počítačové sítě.
- připojení k Internetu (či k jiné síti) jinak než prostřednictvím vnitřní počítačové sítě ČÚZK není dovoleno, pokud je notebook připojen do počítačové sítě ČÚZK. Není-li připojen do počítačové sítě ČÚZK, je dovoleno pouze v případě, že na notebooku je spuštěn firewall, aktualizovaný a aktivní antivir
- připojení notebooku, který splňuje výše uvedené podmínky do vnitřní sítě ČÚZK z jiné sítě nebo Internetu je možné výhradně přes šifrované VPN spojení, přičemž notebook musí být vybaven schváleným VPN klientem a schválenými prostředky pro ověřování VPN přístupů.

Administrátorské notebooky:

- základní pravidla administrátorských notebooků jsou stejná jako u zaměstnaneckých
- administrátoři mají navíc k notebooku přístup na úrovni lokálního administrátora
- administrátoři patřící do skupiny VPN uživatelů mají základní VPN funkcionalitu rozšířenou o přístup prostřednictvím služby Terminal Services (protokol RDP) na stanice a zařízení v adresním rozsahu příslušného kraje.

6.2.1.3 Rozdělení podle uživatelských rolí

V rámci počítačové sítě ČÚZK jsou definovány bezpečnostní skupiny specifikující rozsah přístupových práv uživatelů ke komponentám počítačové sítě.

O zařazení účtu zaměstnance do bezpečnostní skupiny rozhoduje vedoucí zaměstnanec příslušného základního organizačního útvaru, rozhodnutí o přiřazení do určené skupiny musí být uloženo v tištěné formě.

Uživatelé jsou rozděleni do skupin označovaných Security0 až Security4, přičemž každá z těchto skupin definuje odpovídající bezpečnostní politiku s těmito právy:

Security0:

- určena pro externí pracovníky (zejména odborná a laická veřejnost). Skupina s největšími restrikcemi. Uživatel nemá možnost zasahovat do konfigurace počítače, jsou nepřístupná veškerá výměnná média (disketa, CD-ROM, USB porty). Dále nemá možnost přístupu na žádný lokální ani síťový disk. Je zobrazena pouze ikona Windows Internet Exploreru a programové vybavení, které je explicitně definováno ve společné složce na disku U:\Start_Host.

Security:

- základní skupina pro zaměstnance katastrálních pracovišť, kteří mají jednotné programové vybavení (definováno ve složkách U:\Start\Programy a U:\Plocha). Uživatel nemá právo zasahovat do konfigurace počítače. Veškerá nastavení může provádět pouze administrátor (nastavení tiskárny, klávesnice, apod.). Administrátor má možnost doplnění individuální nabídky do Start a Plocha v uživatelově adresáři U:\Uzivatel\username. Uživateli není povoleno procházet síť, nemá přístup na výměnná média a má přístup pouze na vybrané lokální a síťové disky (C, R, U, V).

Security1_c:

- skupina pro pracovníky, kteří poskytují údaje na disketách, ale je nežádoucí jejich přístup na lokální disk C. Restrikce jsou stejné jako u skupiny Security, přístupné jsou pouze disky A, R, U.

Security1:

- skupina pro pracovníky resortu, kteří poskytují údaje na disketách. Restrikce jsou shodné se skupinou Security. Na rozdíl od této skupiny mají přístup k lokálnímu disku C a síťovému Mají přístupné disky A, C, R, U, V.

Security1&K:

- skupina s restriktivními opatřeními, která jsou shodná se skupinou Security. Liší se pouze v přístupných discích. Mají přístupné disky A, C, K, R, U, V.

Security1&ST:

- skupina s restriktivními opatřeními, která jsou shodná se skupinou Security. Liší se pouze v přístupných discích. Mají přístupné disky A, C, R, S, T, U, V.

Security2:

- skupina s rozšířenými právy, uživatel ale přesto nemůže zasahovat do konfigurace počítače, nemá možnost procházet síť (skrytá ikona Okolní počítače). Umožněn přístup na všechny mapované disky (disky lokální a všechny síťové, které jsou definovány v logon skriptu).

Security3:

- skupina určená pro vedoucí pracovníky. Uživatel v této skupině má možnost v omezené míře zasahovat do konfigurace počítače (např. nastavení pozadí plochy). Společná nabídka start a plocha je převzata z U:\Start\Programy a U:\Plocha. Menu a plocha uživatele je umístěna na lokálním disku (C:\Windows\Profiles\%username%), kam má uživatel možnost sám si doplňovat potřebné zástupce.

Security3_spol

- stejné jako skupina Security3. Rozdíl je v tom, že menu a plocha uživatele je na disku U:\Uzivatel\username a nikoliv na lokálním disku.

Security4:

- skupina pro pracovníky z oblasti IT. Uživatel má plnou kontrolu nad počítačem, může měnit konfiguraci počítače, procházet síť, vytvářet a rušit libovolná síťová připojení. Vlastní plocha a nabídka start jsou umístěny na lokálním disku.

Security4-iecert:

- skupina určená pro pracovníky s certifikátem (podatelny apod.) umožňující kontrolovat a měnit nastavení u certifikátů. Na tyto uživatele se aplikuje politika, která jim povolí záložku Možnosti\Obsah v Internet Exploreru.

KUAdmins:

- skupina pro lokální administrátory. Uživatel má plnou kontrolu nad počítačem včetně změn konfigurace. Nemá žádná omezení týkající se procházení sítě a vytváření nebo rušení síťových připojení. U této skupiny jsou pouze nastaveny bezpečností omezení pro práci s Internet Explorerem. Vlastní plocha a nabídka start jsou umístěny na lokálním disku.

KUAdmins-spol:

- nastavení je shodné jako u skupiny KUAdmins. Rozdíl je v tom, že menu a plocha uživatele je na disku U:\Uzivatel\username a nikoliv na lokálním disku. Využívá společnou plochu a nabídku start z disku U.

6.2.2 Uživatelská hesla

Každý uživatel může změnit pouze heslo svého osobního účtu, případně heslo jemu přiděleného privilegovaného účtu. V případě zapomenutí hesla je možné požádat o změnu hesla informatika nebo jemu nadřízeného administrátora počítačové sítě, který však může změnit uživateli heslo pouze na základě žádosti uživatele při osobním kontaktu, ve výjimečných případech může být odblokování provedeno i na základě telefonické žádosti, pokud si je administrátor jist totožností uživatele. [17]

Uživatelské heslo je vždy kromě hesla inicializačního nastaveno samotným uživatelem a musí splňovat tato kritéria:

- délka hesla musí být minimálně 6 znaků
- heslo musí obsahovat vždy minimálně jeden znak ze 3 volitelných znakových sad ze 4 možných znakových sad: malá písmena (a-z), velká písmena (A-Z), číslice (0-9) nebo nealfanumerické znaky (např. +, -, _, @, %). Heslo nesmí být jednoduše uhodnutelné (jména blízkých osob, data narození, tel. čísla, SPZ apod.) a nesmí být běžné slovníkové slovo (české ani anglické)
- uživatel je informován minimálně 14 dnů před expirací jeho hesla zprávou o této skutečnosti při každém přihlášení. Heslo se musí měnit minimálně jednou za 90 dní
- minimální doba platnosti hesla je stanovena na 1 den,
- nové heslo nesmí být stejné jako poslední 2 hesla a nesmí z něj být ani lehce odvoditelné (např. pejsek1a, pejsek2b, Pejsek1A),

- neúspěšné přihlášení – pokud uživatel 4x po sobě zadá nesprávné heslo, účet je automaticky zablokován na 15 minut [17]

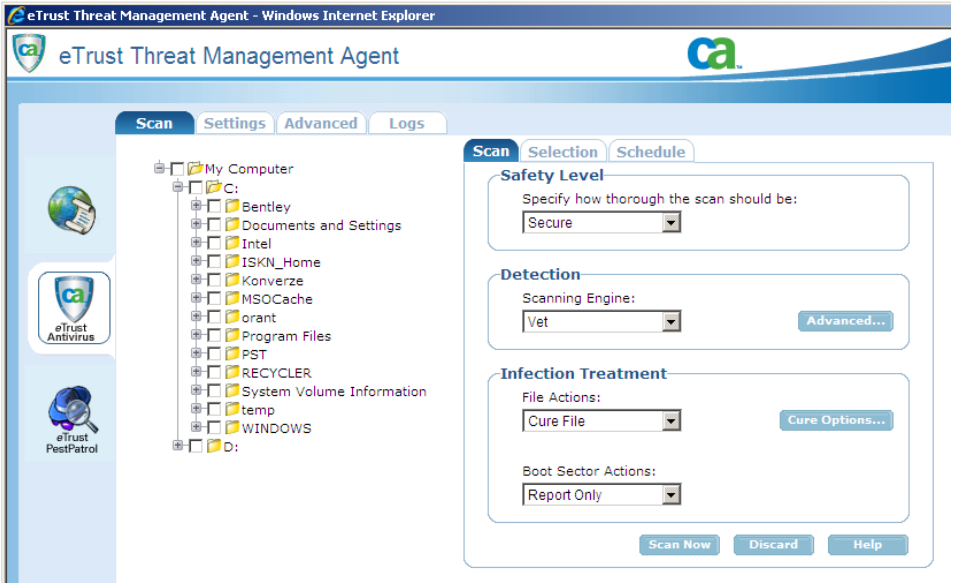
Půjčování a sdělování hesel a dalších autentizačních prvků jiným osobám (vč. zaměstnanců úřadu) je zakázáno. Uživatel nese plnou odpovědnost za všechny činnosti, které byly vykonány pod jeho uživatelským účtem. Pokud má uživatel podezření, že jeho heslo bylo prozrazeno, musí si ihned heslo změnit a tuto skutečnost nahlásit přímému nadřízenému jako bezpečnostní incident. [17]

Je přísně zakázáno provádět nebo i pokoušet se o neautorizovaný přístup k počítačům i jiným zařízením sítě. Opakované neautorizované přístupy, získání jiných než přidělených přístupových práv mohou být posouzeny jako zvlášť hrubé porušení pracovní kázně. Pokud uživatel získá takový přístup jakýmkoliv způsobem (např. v důsledku softwarové nebo hardwarové chyby), je povinen tuto skutečnost neprodleně oznámit administrátorovi počítačové sítě KÚ nebo auditorovi bezpečnosti. [17]

6.2.3 Antivirový systém

6.2.3.1 Klientské počítačové stanice

V celém resortu Českého úřadu zeměměřického a katastrálního úřadu je jednotně na všech pracovních stanicích nainstalován centrálně spravovaný antivirový systém od společnosti Computer Associates - CA eTrust ITM ve verzi R8. Běžní uživatelé nemají možnost jakkoliv zasahovat do jeho konfigurace, administrátoři oddělení podpory ICT katastrálního úřadu a informatici katastrálních pracovišť pak mají možnost jejich omezené konfigurace, mohou provést ruční spuštění aktualizace virové databáze a spustit jednorázový test souborů uložených na lokálních discích.



Obrázek 12: CA eTrust ITM R8 – ruční spuštění antivirového skeneru [vlastní snímek]

Automatické aktualizace jsou prováděny minimálně dvakrát denně s využitím aktualizačního serveru umístěného přímo v resortní počítačové síti.

Díky této striktně dané konfiguraci jsou schopni administrátoři odboru informatiky ČÚZK monitorovat stav antivirového systému, monitorovat případné lokální incidenty a předejít napadení počítačové sítě.

6.2.3.2 Přenosné počítačové stanice

Na služebních noteboocích vybraných vedoucích zaměstnanců katastrálního úřadu je povoleno využívat antivirové systémy od jiných společností na základě předchozího schválení auditorem bezpečnosti katastrálního úřadu a za předpokladu vlastnictví příslušného počtu licencí.

Jejich aktualizace se provádí přímo ze sítě Internet a nejsou spravovány centrálně. V případě že se vyskytne podezření na nefunkčnost antiviru nebo na napadení notebooku virem nebo jiným škodlivým kódem je zaměstnanec povinen tuto skutečnost ohlásit místně příslušnému informatikovi, popř. zaměstnanci oddělení podpory ICT a po dobu do vyřešení problému zařízení nepřipojovat do resortní počítačové sítě.

6.2.4 Aktualizace operačního systému

Všechny pracovní stanice a notebooky musí být zapojeny do domény ČÚZK a pomocí doménových politik jsou u nich aktualizace operačního systému nakonfigurovány podle tohoto klíče:

6.2.4.1 Pracovní stanice bez ISKN, včetně notebooků

Mají povinně nastavenou automatickou instalaci aktualizací vydaných společností Microsoft s využitím interního Windows Server Update Services (WSUS) serveru. Tato serverová aplikace pravidelně a zcela automaticky stahuje aktualizace zveřejněné na webu Microsoft update a umožňuje administrátorům volit, které aktualizace chtějí instalovat a zároveň je s její pomocí instalovat na klientské stanice, bez ohledu na tom jestli jsou připojeny k síti Internet.

6.2.4.2 Pracovní stanice s nainstalovaným ISKN

U těchto stanic je nutné, aby byly aktualizace záplat řádně otestovány jak na referenčním tak i na vybraném pilotním pracovišti. Proto se jejich instalace provádí ve dvouměsíčním intervalu pomocí jiných IS, konkrétně s využitím systému pro komplexní správu počítačových stanic – CA Unicenter Desktop and Server Management.

V případě že jde o aktualizaci typu Servicepack je také nutné mimo kroků uvedených v předchozím odstavci zajistit schválení dodavatelem ISKN.

6.2.5 Firewall

Na všech pracovních stanicích i noteboocích je aktivován integrovaný firewall operačního systému Windows, poskytující základní ochranu před možnými útoky z LAN / WAN, celé počítačová síť je pak chráněna hardwarovými firewally a vynucením používání proxy serveru pro přístup k síti Internet. Běžným uživatelům je pomocí doménových politik znemožněno jakkoliv manipulovat s nastavením tohoto firewallu, u uživatelů s právy administrátora je umožněno stav firewallu měnit.

6.2.6 CA Unicenter Desktop and Server Management

CA Unicenter DSM představuje komplexní systém na správu, inventarizaci a automatizaci instalací software (včetně OS) pro velké podnikové počítačové sítě. Poskytuje administrátorům velký komfort a obecně zjednodušuje správu všech komponent počítačové sítě nezávisle na platformě, na které tyto komponenty běží.

Základem celého systému je jeden centrální Enterprise Manager (Server), který získává informace z podřízených Domain Managerů, které přímo komunikují s těmito třemi moduly instalovanými na jednotlivé počítačové stanice v počítačové síti:

6.2.6.1 Software Delivery

Služba Software Delivery se využívá k distribuci software v geograficky rozptýlených lokalitách, přispívá k automatizaci administrace software a zjednodušuje upgrade stanic na nový operační systém

Umožňuje automatickou distribuci a instalaci software na základě výsledků získaných z inventarizace PC pomocí modulu Asset Management nebo individuálně na základě požadavku provedeného administrátorem v DSM Exploreru.

V prostředí počítačové sítě KÚ pro Zlínský kraj se možností tohoto modulu prozatím využívá zcela výjimečně, většina instalací se stále provádí manuálně s využitím instalační šablony definované odborem informatiky ČÚZK.

6.2.6.2 Remote Control

Služba Remote Control poskytuje centrálně spravovaný systém vzdáleného přihlašování na počítačové stanice. Dovoluje provést operace s libovolnou stanicí nebo skupinou stanic, např. je vypnout, restartovat nebo převzít ovládání stanice v několika režimech.

6.2.6.3 Asset Management

Pravděpodobně nejdůležitější a nejvyužívanější komponenta celého systému. Řeší detailní inventarizaci HW a SW v rámci celé podnikové sítě. Nástroj umožňuje provádět inventarizaci stanic a serverů napříč všemi běžně užívanými platformami.

Takto získané údaje, slouží katastrálnímu úřadu pro kontrolu dodržování počtů nainstalovaných licencí jednotlivých aplikací, i jako podklad pro pravidelnou inventarizaci HW a to i na úrovni jednotlivých komponent počítačových stanic.

6.2.6.4 DSM Explorer

Srdcem celého systému je DSM Explorer, administrátorská konzole, ve které je možné získat podrobné informace o HW, SW a konfiguraci každé stanice zapojené do tohoto systému, vytvářet různé dotazy a z nich následně reporty do několika běžně užívaných formátů.

Je zde také možné vytvářet a spravovat jak statické tak i dynamické skupiny počítačových stanic a na ně aplikovat různá pravidla. Například není problém pomocí informací z Asset Manageru vytvořit dynamickou skupinu počítačových stanic, které mají neaktuální verzi jakéhokoliv nainstalovaného SW a na tyto stanice zcela automatizovaně instalovat novou verzi software pomocí Software Delivery.

6.2.7 Zálohování dat

V celém resortu Českého úřadu zeměměřického a katastrálního (a tedy i na Katastrálním úřadě pro Zlínský kraj) se k zálohování dat používají zálohovací mechaniky HP Ultrium LTO2 fyzicky umístěné na databázových serverech (B servery), serverech systémového managementu (S servery) a aplikačních serverech (A servery).

Obrázek 13: Zálohovací mechanika HP Ultrium LTO2 [20]

Přesný název produktu	HP StorageWorks Ultrium 448 Tape Drive
Technologie zápisu	LTO-2 Ultrium 448
Úložná kapacita	200GB nekomprimovaně, 400 GB s kompresí
Střední doba bezporuchového provozu	250 000 hodin
Rychlost přenosu dat	173 GB za hodinu
Velikost vyrovnávací paměti	64 MB
Rozhraní hostitelského počítače	SAS (3 Gb/sec)
Podpora šifrování	Ne
Provedení	5.25-inch half-height
Rozměry produktu (Š × H × V)	14.48 x 20.57 x 4.06 cm
Hmotnost produktu	1.45 kg

Pomocí těchto mechanik jsou na všech osmi katastrálních pracovištích Katastrálního úřadu pro Zlínský kraj zálohována:

- data kritických a středně kritických informačních systémů
  - archivní logy Oracle databáze Informačního systému katastru nemovitostí
  - data ekonomického a personálního systému
  - data systému Microgeos Nautil (tam kde je nainstalován)
- uživatelská data uložená na síťových discích
- kompletní obsah lokálního Exchange serveru (e-maily)
- obsah Intranetu katastrálního úřadu
- ostatní data určená k zálohování.

Z výše uvedeného je zřejmé, že data uložená na jednotlivých (uživatelských) klientských stanicích nejsou zálohována, s čímž jsou zaměstnanci seznámeni a je jim doporučeno ukládat všechna důležitá data na předem vyhrazený a do zálohy zařazený síťový disk.

Zálohování se provádí podle tohoto klíče:

1. Management server – zálohuje se na tři sady pásek po 5 kusech. Pásky se každý den cyklicky střídají a každá páska je znovu použita vždy jednadvacátý den po jejím předchozím použití
2. Aplikační server – stejný princip zálohy jako na management serverech - tři sady pásek po 5 kusech. Pásky se každý den cyklicky střídají a každá páska je znovu použita vždy jednadvacátý den po jejím předchozím použití

3. Databázový server – zálohuje se na jednu sadu pásek čítající 3 pásky. Pásky se vyměňují jednou za týden. Páska je přepsána vždy třetí týden po jejím předchozím použití.

Obrázek 14: Bezpečnostní schránka pro přenos pásek
[vlastní snímek]

Pásky musejí být označeny podle této předem dané konvence:

Management a aplikační servery (S a A servery)

Pásky jsou označeny kódem ve tvaru: **XXXX_DD_SS**, kde:

- XXX je numerický kód pracoviště podle číselníku ČÚZK
- DD označuje pořadí pásky v rámci týdne (PO, UT, ST, CT, PA)
- S je označení sady pásek

Databázové servery (B servery)

Pásky jsou označeny kódem ve tvaru **XXX_LOGY_S**

kde:

- XXX je numerický kód pracoviště podle číselníku ČÚZK
- S je označení sady pásek

V názvech pásek nesmí být používána diakritika a minimálně jedna sada pásek je vždy umístěna na bezpečném úložišti mimo budovu úřadu. V případě Katastrálního pracoviště Zlín se například jedná o trezor lokální pobočky Komerční banky.

6.2.8 Omezení přístupu do sítě Internet

Jak již bylo zmíněno v jedné z předchozích kapitol pro přístup k síti Internet se využívá centrálně spravovaného proxy serveru, který je zároveň jediným způsobem jak se může uživatel dostat ke stránkám a službám dostupným na webu.

Uživatelé jsou rozděleni do tří skupin:

- Uživatelé s přístupem pouze k volně dostupným stránkám
- Uživatelé s neomezeným přístupem k síti Internet
- Administrátoři

6.2.8.1 Uživatelé s přístupem pouze k volně dostupným stránkám

Tito uživatelé mají povolen přístup jen k předem schváleným a prověřeným webovým stránkám. Mezi tyto volně dostupné stránky jsou zařazeny zejména projekty přímo nebo nepřímo řízené ČÚZK, webové stránky jednotlivých ministerstev, Vlády a Parlamentu České republiky. Jejich kompletní seznam je k dispozici v příloze č. 2

6.2.8.2 Uživatelé s neomezeným přístupem k síti Internet

Jedná se zejména o vedoucí pracovníky katastrálního úřadu, řadové zaměstnance oddělení podpory ICT a vybrané pracovníky, kteří k některým svým činnostem potřebují přístup k Internetu. Jejich přístup je však striktně omezen jen na HTTP protokol – jiné služby nemohou využívat.

6.2.8.3 Administrátoři

Vybraní administrátoři mají na základě schválení vedoucím oddělení podpory ICT povolen přístup do sítě Internet pomocí aplikace Microsoft Firewall Client for ISA Server, která jim umožňuje v neomezené míře používat všechny na Internetu dostupné protokoly, jako jsou např. FTP, RDP, IMAP, aj.

Všichni uživatelé bez výjimky musí dodržovat tento kodex:

- zaměstnanci nesmí nepřistupovat k internetovým stránkám se závadným obsahem (nezákonným nebo nevhodným pro pracovní prostředí, např. pornografie, hazardní hry nebo drogy). Aktivity uživatele nesmí být v rozporu s příslušnými zákony a normami, včetně etických norem a interních předpisů úřadu.
- nesmí se jakkoliv snažit o získání neoprávněných přístupů ke zdrojům na Internetu, nesmí provádět činnosti vedoucí k poškozování práv jiných subjektů, neoprávněně prohlížet, poškozovat jejich data.
- nesmí provádět aktivity vedoucí k narušení soukromí jiných osob, porušování autorských práv (zasahování do technických opatření využívaných vlastníky autorských práv k ochraně nebo identifikaci jejich děl) nebo se tato opatření pokoušet obejít (stahování nelegálních kopií programů, hudby, videa, aj.).

Český úřad zeměměřický a katastrální si jako nadřízený orgán katastrálních úřadů vyhrazuje právo:

- zablokovat přístup k internetovým stránkám považovaným za nevhodné. Úmyslné pokusy o přístup k těmto zdrojům jsou porušením pracovní kázně.
- sledovat přenos dat, vyhodnocovat ho a zavést denní limity na přenos dat pro uživatele a informovat ředitele katastrálních úřadů o uživatelích, kteří tyto limity překročili. [17]

6.3 Fyzická bezpečnost

Jako ústředna EZS je na Katastrálním pracovišti ve Zlíně použita Galaxy 500, která má samostatnou desku zdroje a desku s elektronikou. Mezi hlavní výhody této ústředny patří její modulárnost – obsahuje čtyři komunikační sběrnice, ke kterým je možné připojit klávesnice, koncentrátory, komunikační moduly a jiné komponenty. Jako napájení je použito stejnosměrné napětí o hodnotě 12V.

Celkem je na ústřednu napojeno 44 pasivních infračervených detektorů, 2 akustické detektory rozbití skla, 18 magnetických detektorů, 6 stropních PIR detektorů a 2 mikrovlnné detektory.

Ovládání systému je zprostředkováno pomocí dvou klávesnicových ovládacích panelů umístěných v dosahu obou vchodů do budovy - v zóně společných prostor, což umožňuje bezpečné odkódování celé EZS, kterýmkoliv oprávněným uživatelem.

Komunikaci s dohledovou službou zajišťuje radiový modul, jištěný navíc druhým komunikačním kanálem řešeným připojením na linku pevného telefonního rozvodu.

Celá budova je rozdělena na čtyři zóny:

- Katastrální úřad pro Zlínský kraj
- Český statistický úřad
- Geodezie Brno
- společné prostory

Každou z prvních tří uvedených zón dokáže aktivovat / deaktivovat jen oprávněná osoba, společné prostory se kódují / dekódují automaticky v závislosti na stavu zbývajících zón.

Obrázek 15: Ústředna EZS na Katastrálním pracovišti ve Zlíně
[vlastní snímek]

Katastrální úřad pro Zlínský kraj má uzavřenu smlouvu (vzorová smlouva - příloha č. 3) se společností System Plus Zlín, s.r.o., která pro úřad zajišťuje:

- provoz pultu centrální ochrany s vlastním výjezdem a s garancí dojezdu. EZS je na PCO připojena pomocí vlastní rádiové sítě NAM Global (ve frekvenčním pásmu 459 MHz) a záložním připojením přes GSM síť
- provoz Pultu Požární ochrany s výjezdem Hasičského Záchranného Sboru
- pravidelný servis a revize EZS

Tato firma zahájila svou činnost již v roce 1990, přičemž od počátku její existence je kladen důraz na maximální profesionalitu, spolehlivost a kvalitu provedených prací a instalované techniky v zabezpečeném objektu.

Veškeré informace a poznatky, které jsou firmě poskytnuty o majiteli, výši chráněných hodnot, či bezpečnostních opatřeních považují pracovníci firmy za přísně důvěrné. [24]

Fyzickou bezpečnost objektu zvyšují mechanické zábranné systémy, jako jsou například bezpečnostní zámky umístěné ve dveřích protipožárního typu, mříže na oknech přízemního podlaží a také dveřní a mřížové přepážky umístěné na chodbách jednotlivých pater budovy, ve které Katastrální úřad pro Zlínský kraj sídlí.

6.4 Havarijní plánování

Havarijní plány pro jednotlivé informační systémy provozované na pracovištích Katastrálního úřadu pro Zlínský kraj patří mezi stěžejní dokumenty v oblasti bezpečnosti informačních systémů.

V současné době se týkají těchto systémů:

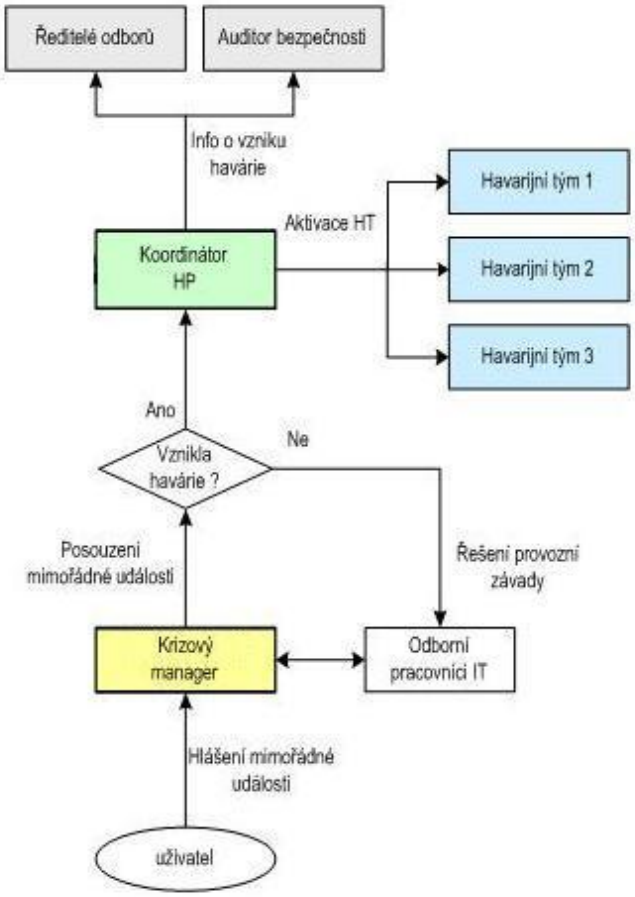
Název IS	Stručný popis IS	stupeň	ADV
Brightstor Arcserve	zálohovací systém	kritický	1 den
ISKN	Informační systém katastru nemovitostí	kritický	2 dny
LAN	LAN – lokální počítačová síť	kritický	2 dny
Exchange server	elektronická pošta	kritický	2 dny
EIS	Ekonomický informační systém	střední	2 – 10 dní
DC2	Datacentrum 2 - personální a mzdový systém	střední	2 – 10 dní
Microgeos Nautil	obnova katastrálního operátu	střední	5 dní
CA DSM	systémový management	střední	5 dní
PC	klientské stanice	střední	neurčeno
ostatní HW	Směrovače, routery, firewally	střední	neurčeno

Tabulka 3: IS provozované na Katastrálním úřadě pro Zlínský kraj

Havarijní plány mají povahu interních dokumentů určených pouze pověřeným zaměstnancům a jsou zpracovány pro každé z osmi katastrálních pracovišť Katastrálního úřadu pro Zlínský kraj. První verze těchto dokumentů (s průměrným počtem stran 230) byla vypracována již v roce 2004 a od té doby jsou průběžně aktualizovány a doplňovány s každou změnou v infrastruktuře informačních systémů.

Ve většině případů byla pro případ nutnosti obnovy dat zvolena metoda studené zálohy (cold site) – výměna poškozeného serveru za čistý záložní stroj, instalace, konfigurace operačního systému a následná obnova dat ze zálohovacích pásek.

Pro potřeby řízení a koordinace činností v případě vzniku havárie byla navržena organizační struktura havarijního managementu.



Obrázek 16: Krajská úroveň havarijního plánování [16]

Tato struktura je dvouúrovňová – krajská a centrální. V případě, že havárie přesáhne působnost kraje, předávají se exekutivní pravomoci pro řešení havarijního stavu na centrální úroveň.

Na obou úrovních řízení havarijních plánů se vyskytují tyto role:

- krajský (centrální) krizový manager
- krajský (centrální) koordinátor havarijního plánování
- krajský (centrální) havarijní tým
- ostatní zaměstnanci

6.4.1 Krizový manager

Krizový manager ať už na krajské nebo centrální úrovni je v oblasti havarijního plánování povinen:

- přebírat hlášení o předpokládaných haváriích a mimořádných událostech z těchto zdrojů:
  - ředitelé útvarů, odborů, oddělení
  - informatiků a administrátorů komponent IS
  - koncových uživatelů informačních systémů
- distribuovat požadavky na posouzení těchto situací a stavů na pověřené zaměstnance za účelem jejich zhodnocení
- koordinovat postupy při posuzování rozsahu a dopadu mimořádné události a kvalifikovaném odhadu maximální doby výpadku informačního systému

6.4.2 Koordinátor havarijního plánování

Tato osoba má za úkol zejména:

- přebírat hlášení o vzniku havárií od krajského krizového managera a ve spolupráci s dalšími odpovědnými osobami rozhodovat o postupu řešení havárie
- informovat o vzniku havárie na krajské úrovni centrálního koordinátora havarijního plánování
- v případě, že havárie přesáhla působnost kraje, informovat o situaci centrálního koordinátora, další pravomoci pro řízení a řešení havárie jsou pak předány centrálnímu koordinátorovi,
- informovat o vzniku havarijních stavů vedoucí zaměstnance na krajské úrovni
- rozhodovat o aktivaci havarijních plánů na krajské úrovni a mobilizaci havarijních týmů na podnět krajského krizového managera
- koordinovat součinnost havarijních týmů na krajské úrovni při řešení havárií a poskytovat jim potřebnou manažerskou podporu
- podávat návrhy k aktualizaci a doplnění částí havarijních plánů na krajské úrovni

6.4.3 Havarijní tým

Skupina pověřených odborně způsobilým zaměstnanců, která zajišťuje řádné provedení všech kroků nutných k rychlé obnově poškozeného systému dle příslušného havarijního plánu. Havarijní tým je řízen vedoucím havarijního týmu, který odpovídá krizovému managerovi za řádné provedení celého havarijního plánu a koordinuje činnost celého týmu.

6.4.4 Ostatní zaměstnanci

Každý zaměstnanec katastrálního úřadu je v oblasti zajištění kontinuity provozních činností a havarijního plánování povinen:

- okamžitě hlásit jakoukoliv mimořádnou událost, která by mohla vést nebo vede ke vzniku havárie svému nadřízenému, který tuto událost hlásí odpovědnému administrátorovi oddělení podpory ICT, správci databáze KÚ nebo informatikovi katastrálního pracoviště
- cílem všech jeho dalších činností, pokud je to v jeho možnostech, je minimalizovat dopad havárie případně odvrátit bezprostřední ohrožení:
    - postupovat podle požárních a poplachových směrnic, dle možností dále:
        - odnést důležitá datová média a písemné materiály
        - odnést výpočetní techniku
        - zajistit dozor u vystěhovaných věcí
    - při ohrožení vodou:
        - zajistit provizorní ochranu výpočetní techniky, datových médií a písemné dokumentace plastovou fólií,
        - uzavřít příslušný přívod vody
        - zajistit vystěhování techniky, médií a dokumentů do prostor, které nejsou ohroženy ani zasaženy
    - hlásit výpadky klimatizace, poškození hlásičů požáru, vlhkosti, atd.

7 NÁVRHY ŘEŠENÍ ZJIŠTĚNÝCH NEDOSTATKŮ

7.1 Autentizace pomocí USB tokenů

Pro zvýšení bezpečnosti přepážkových pracovišť by bylo vhodné místo přihlašování pomocí hesel využít možností autentizace pomocí USB tokenů.

Zvolené tokeny iKey řady 4000 jsou typickým příkladem řešení zabezpečení pomocí dvou faktorové autentizace. Na rozdíl od běžně využívaného jednoduchého zabezpečení heslem, které nemusí být příliš bezpečné – i přes nastavení minimální složitosti hesla a jeho pravidelné obměny zde záleží hlavně na individuálním přístupu konkrétního uživatele – který může úmyslně, popř. i nevědomky (nejčastěji z důvodu snadné zapamatovatelnosti) volit heslo, které je snadno odhadnutelné nebo v krátké době prolomitelné.

Použitím certifikátů uložených v tokenu a přístupového hesla pro přístup k nim tento problém do jisté míry odbourává. Uživatel si musí pamatovat (something to know) pouze 4 místný PIN kód a mít u sebe token (something to have).

O zbývající se postará certifikát uložený v tokenu. Ke generování párových klíčů se využívá privátní klíč uložený přímo v tomto zařízení a díky certifikaci FIPS 140-2 Level 3 je zajištěno, že tento klíč a další uložená data nemohou být přečtena bez fyzického poškození tokenu. V případě pěti nesprávných pokusů o zadání PIN kódu jsou data v něm uložená zničena a je nutná intervence správce, který má možnost provést inicializaci tokenu a obnovu certifikátů z bezpečného úložiště.

Obrázek 17: USB token iKey 4000
[vlastní snímek]

Pro pracovníky přepážkových pracovišť Katastrálního úřadu pro Zlínský kraj by pak hlavním přínosem bylo zejména:

Snížení rizika odečtení hesla – díky tomu, že se pro autentizaci využívá dvou faktorové řešení, není ani případné odečtení PIN kódu k tokenu na rozdíl od přihlašovacího hesla uživatele velkým rizikem. K přihlášení je nutný i fyzický přístup k tokenu.

Automatické uzamčení PC při vzdálení se zaměstnance – volitelně, avšak v případě přepážkových pracovišť spíše vynuceně lze s využitím tzv. „připoutání k tělu“ automaticky uzamykat pracovní stanici v případě opuštění pracovního místa, např. za účelem donesení tiskového výstupu zákazníkovi.

Sjednocení a zjednodušení autentizace do různých IS – s použitím tokenů lze snadněji dosáhnout sjednocení přihlašovaní do ostatních informačních systémů, které nejsou přímo provozovány resortem a nemohou tedy využívat jednotného doménového přihlášení – např. Czechpoint, Informační systém datových schránek, apod.

7.2 Šifrování dat na klientských počítačových stanicích

Mezi největší slabiny současné bezpečnostní politiky považuji zabezpečení klientských počítačových stanic (vč. přepážkových pracovišť) a administrátorských notebooků, které nejsou nijak chráněny před zneužitím dat – například v případě krádeže – přestože mohou obsahovat citlivá data.

Obrázek 18: Detail umístění pracovní stanice na přepážkovém pracovišti

[vlastní snímek]

Řešením by bylo využití možností operačních systémů Windows 7 Ultimate, které obsahují možnost šifrování obsahu celého pevného disku utilitou BitLocker Drive Encryption.

Mezi výhody využití BitLockeru na těchto stanicích patří:

- úplná integrace do operačního systému
- šifrování všech uživatelských dat včetně operačního systému
- možnost využití čipových karet / tokenů pro autentizaci

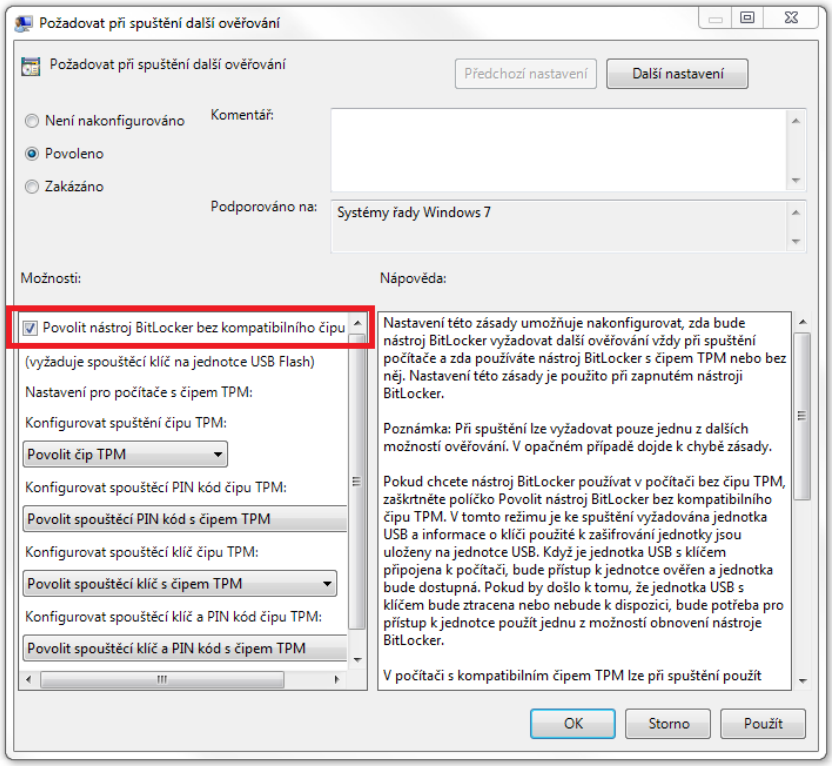
Katastrální úřad pro Zlínský kraj má v majetku tyto typy klientských stanic a NTB:

označení	operační systém	TPM	rok výroby
HP 7600 DC	Windows XP Prof. /Win 7 Prof.	ano	2006
HP 7800 DC	Windows XP Prof. /Win 7 Prof.	ano	2008
ASUS V1S	Windows Vista Bussines	ano	2009
ASUS UL30VT	Windows 7 Prof.	ne	2010

Tabulka 4: Typy používaných počítačových stanic

U stanic, které nemají integrován čip TPM je nutné před spuštěním BitLockeru provést následující úpravu konfigurace politik operačního systému:

1. Spusťte Group Policy Editor – gpedit.msc
2. Konfigurace počítače -> šablony pro správu -> součásti systému Windows -> šifrování jednotky pomocí služby BitLocker -> jednotky operačního systému
3. V pravém panelu zvolte „Požadovat při spuštění další ověřování“
4. Změňte konfiguraci na „Povoleno“
5. Zkontrolujte zaškrtnutí checkboxu „Povolit nástroj BitLocker bez kompatibilního čipu TPM“



Obrázek 19: Deaktivace vynuceného použití TPM čipu
[vlastní snímek]

Nastavení je samozřejmě možné analogicky provést i na vybrané skupině počítačů umístěných v doméně Active Directory systému Windows prostřednictvím doménových politik.

Vzhledem k tomu, že se moje práce věnuje bezpečnosti přepážkových pracovišť, ponechám praktické řešení šifrování dat na noteboocích stranou a zaměřím se na nastavení konfigurace počítačových stanic používaných na přepážkách – HP 7600 DC.

7.2.1 Šifrování pomocí BitLockeru

Počítačové stanice v majetku Katastrálního úřadu pro Zlínský kraj jsou v současné době (březen 2011) vybaveny operačním systémem Windows XP Proffesional, předpokládá se však, že během července tohoto roku bude proveden upgrade všech stanic na nový operační systém Windows 7. Toho by šlo využít a pro stanice přepážkových pracovišť pořídit verzi Ultimate a využít BitLocker k šifrování dat jak na systémového, tak i datového oddílu.

Nástroj BitLocker umožňuje využití vestavěného TPM čipu k uložení šifrovacího klíče, přičemž u systémového oddílu jsou k dispozici tyto možnosti:

- dešifrování pomocí spouštěcího klíče na přenosném médiu
- automatické dešifrování šifrovacím klíčem z TPM
- dešifrování dat šifrovacím klíčem z TPM v kombinaci s PIN kódem

Uložení startovacího klíče na přenosné USB médium není příliš vhodné – přestože tento přístup nenutí uživatele, aby si pamatovali složitá hesla, ale přenáší autentizaci na vlastnictví předmětu, nepředstavuje z pohledu bezpečnosti velký přínos - neumožňuje použití dodatečného PIN kódu a v případě zavedení USB tokenů pro přihlašování uživatelů do operačního systému by to pro uživatele znamenalo nosit sebou další zařízení.

Kompromisem by mohlo být využití BitLockeru v režimu automatického dešifrování pomocí klíče uloženého v TPM, čímž se dosáhne dostatečné ochrany pro případ krádeže pevného disku nebo změny konfigurace systému. Pomocí TPM je při startu ověřován kontrolní součet BIOSu, Boot manageru a MBR, není možné tedy nabootovat ani z Live CD a pokusit se o offline přístup k datům uloženým na chráněném disku. Tento přístup ovšem neřeší možnost odcizení celé počítačové stanice a následného zneužití uložených dat – proto jej také nepovažuji za přínosné řešení.

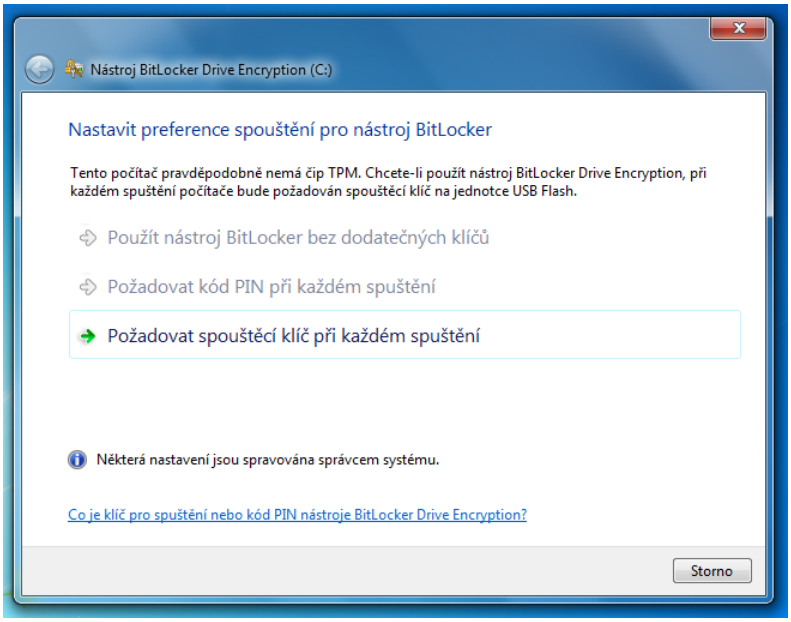
Ideálním řešením z pohledu bezpečností je zcela jistě dvou faktorová autentizace šifrovacím klíčem uloženým v TPM s využitím PIN kódu, z praktického hlediska je však nutné zajistit, aby obsluhy přepážkových stanic, které nejsou každý den shodné, vlastnily každá svůj vlastní PIN kód nebo alespoň pro každou stanici jeden sdílený.

7.2.2 Šifrování systémového oddílu

Před samotným zašifrováním dat je nutné v BIOSu povolit, případně prověřit, zda je povolen TPM čip, starající se o bezpečné uložení šifrovacího klíče. O všechny následující kroky se postará přímo průvodce šifrováním nástroje BitLocker.

Prvním krokem je inicializace TPM čipu, během níž se provede převzetí vlastnictví TPM čipu a nastavení přístupového hesla, které je nutné pro některé další operace s čipem.

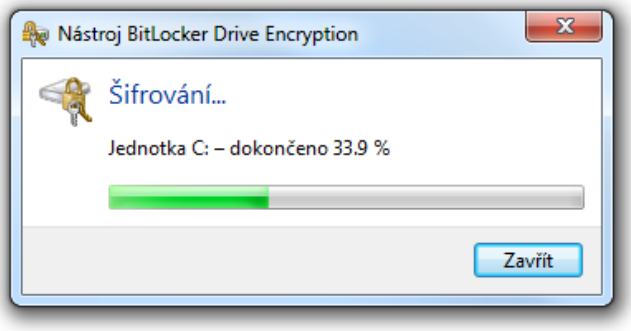
Po dokončení tohoto nastavení a restartu PC se již přistupuje přímo k nastavení způsobu uložení šifrovacího klíče, ve které v našem případě vybíráme „Požadovat kód PIN při každém spuštění“ – tedy uložení dešifrovacího klíče přímo do TPM čipu s nutnosti dalšího ověření PIN kódem.



Obrázek 20: BitLocker: Výběr metody autentizace uživatele [vlastní snímek]

Jelikož se jedná o šifrování celého obsahu pevného disku pomocí 128bit AES (volitelně 256bit) algoritmu je také nutné, uložit nebo vytisknout i takzvaný Obnovovací klíč – 48 místné číselné heslo, které je poslední záchranou v případě, že by selhalo ověření pomocí TPM čipu nebo bylo přihlášení zablokováno po několikanásobném zadání špatného PIN kódu.

Během šifrování lze s PC bez omezení pracovat, jakákoliv zátěž procesoru však znamená znatelné zpomalení celého procesu.



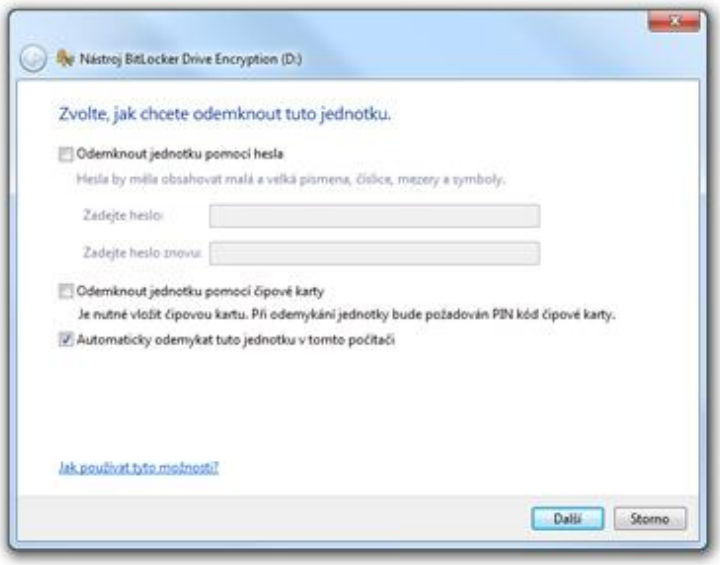
Obrázek 21: BitLocker: Průběh šifrování Systémového oddílu [vlastní snímek]

Šifrovanou jednotku pak lze snadno rozpoznat podle ikonky zámku. Data jsou ve výchozím nastavení šifrována algoritmem AES 128 Diffuser, který má minimální dopad na výkon operačního systému.

7.2.3 Šifrování datového oddílu

Také datový oddíl, může obsahovat citlivá data, je také možné šifrovat. BitLocker pro datový oddíl nabízí několik možností:

- dešifrování dat po zadání hesla
- dešifrování dat po vložení čipové karty (USB tokenu)
- automatické dešifrování klíčem uloženým na systémovém svazku



Obrázek 22: Automatické odemykání datového oddílu [vlastní snímek]

Z praktického hlediska se jeví jako nejvhodnější využití automatického dešifrování klíčem uloženém na systémovém oddílu, i přes to, že to není z bezpečnostního hlediska tak dobré řešení jako nabízená možnost dešifrování certifikátem uloženým na čipové kartě (USB tokenu). Hlavním důvodem pro tuto variantu je výše zmiňované časté střídání obsluh podatelny a také to, že systémový oddíl, na kterém bude dešifrovací klíč uložen je již BitLockerem zašifrován (není tedy snadné tento šifrovací klíč zneužít).

Podle tvrzení společnosti Microsoft je zpomalení způsobené šifrováním všech dat na disku symetrickým algoritmem AES 128 zanedbatelné, podle praktických měření dochází ke zhruba 20% snížení výkonu disku, což je v případě běžného kancelářského PC u zaměstnanců přepážkových pracovišť bez problému akceptovatelné.

7.3 Kamerový systém

Jedním z dalších návrhů na vylepšení bezpečnosti přepážkových pracovišť katastrálního úřadu může být umístění kamery snímající oblast pro klienty umístěnou u těchto pracovišť. Záznamem obrazu a volitelně i zvuku by bylo dosaženo nejen vyšší bezpečnosti našich zaměstnanců, ale zároveň by to dovolilo získaná data prezentovat na našich internetových stránkách, kde by se potencionální klienti např. mohli podívat na aktuální vytíženost pracovišť a přizpůsobit tomu svůj příchod.

Pro praktickou realizaci jsem vybral IP kameru Cisco VC220, která je vhodná pro použití ve vnitřních prostorách a zároveň by svou cenou a snadností implementace do současné počítačové sítě neznamenala pro katastrální úřad velkou finanční zátěž.

Obrázek 23: IP kamera Cisco VC220 [29]

Základní parametry IP kamery Cisco VC220:

- typ kamery: Dome
- napájení: externí, PoE
- video: 640x480 (VGA), 320x240 (QVGA), 160x120 (QQVGA)
- zoom: optický 3,6x, digitální 4x
- audio: ano
- možnost připojení na EZS (integrovaný PIR, detekce pohybu)
- vestavěný IR filtr (noční provoz)

Jak je zřejmé z obrázku č. 23 jedná se o kameru, jejíž předností je odolnost proti fyzickému poškození, relativně malá velikost a podpora funkcí PTZ. Díky ovládacímu software je možno plně využít těchto možností a kamerou otáčet v úhlech 23 – 90° s kombinovaným optickým a digitálním zoomem až 14,4x s volitelnou frekvencí snímkování od 1 až do 30 snímků za vteřinu při maximálním rozlišení 640x480 pixelů. Pro napájení kamery je dodáván klasický síťový adaptér, kameru je však možné napájet i pomocí ethernetového kabelu, podporuje totiž technologii PoE (Power over Ethernet).

Pro provoz ve zhoršených světelných podmínkách je vybavena IR LED diodami, které jsou využity i vestavěným PIR detektorem, který je možné pomocí GPIO konektorů připojit ke stávající EZS.

Obrázek 24: IP kamera Cisco VC220 – vstupy a výstupy [29]

Záznam je možné ukládat do standardního formátu MPEG-4 a MJPEG formátu, které umožňují jak snadné vyhledávání v archivovaných záznamech tak i možnost poskytovat obraz v reálném čase např. na webových stránkách. Mezi speciality – v našem případě však spíše nepoužitelné pak patří například možnost nechat si zasílat informační zprávy na e-mail nebo Jabber klienta v případě, že je kamerou detekován pohyb v době, kdy je nastavena do režimu střežení.

Správa všech nastavení této kamery se provádí výhradně přes přehledné webové rozhraní s možností využití šifrování pomocí https protokolu, který zaručuje vysokou bezpečnost.

S ohledem na platná ustanovení zákona č. 101/2000 Sb. (Zákon o ochraně osobních údajů) a usnesením Úřadu pro ochranu osobních údajů týkajících se kamerových systémů by také bylo potřeba zajistit tyto formální náležitosti:

- získat řádný souhlas zaměstnanců pracujících na přepážkových pracovištích
- zajistit informování veřejnosti o monitorování prostoru kamerovým systémem
- předem jasně stanovit účel pořizování záznamů
- jasně stanovit pravidla a lhůtu pro uchovávání záznamů
- zajistit registraci u ÚOOÚ

S ohledem na výše uvedené se zdá být vhodným kompromisem ukládání záznamů pouze v době kdy je EZS v režimu střežení (ochrana majetku proti krádeži), zajistit informovanost veřejnosti vylepením informačních samolepek na vchodové dveře a v době provozu přepážkových pracovišť pouze online přenášet aktuální dění bez ukládání záznamu. Lhůtu pro uchovávání údajů by pak vzhledem ke zvolenému účelu bylo možné stanovit např. jen na 24 hodin.

7.4 Tísňový hlásič

Obsluhy přepážkových pracovišť manipulují s hotovostí od klientů, proto by bylo vhodné zvýšit jejich bezpečnost instalací dodatečných tísňových hlásičů propojených s ústřednou EZS.

Pro tento účel se používají tyto speciální tísňové hlásiče:

- tlačítkové tísňové hlásiče
- tísňové lišty
- detektory poslední bankovky

Tlačítkové hlásiče se nejčastěji používají ve dvou provedeních, podle toho jak jsou aktivovány – ruční a nožní (pedálové) tlačítkové hlásiče.

Tísňové lišty jsou aktivovány nadzvednutím pohyblivé části nohou, čímž se brání vzniku falešných poplachů, jak tomu může být u tísňových pedálů.

Ideálním produktem splňujícím všechny stanovené podmínky se zdá být tísňové tlačítko HB304 s pamětí od společnosti GE Security. Toto tlačítko je určeno pro použití hlavně v kancelářských prostorech, skladech, na přepážkových pracovištích, atd. Díky nízkému profilu je možno tlačítko umístit kdekoliv, aniž by zmenšilo volný pracovní prostor. Nenápadný vzhled zbytečně neupoutává pozornost případného útočníka. Tvar pohyblivé části je navržen tak, aby nemohlo dojít k náhodné aktivaci tísňového tlačítka a spustit poplach je možné jen prsty. Červená LED dioda indikuje aktivaci tlačítka, takže je možno zpětně určit, kterým tlačítkem byl poplach vyvolán. [28]

Obrázek 25: Tísňový hlásič GeSecurity HB304 [28]

Detektory poslední bankovky jsou speciální tísňové hlásiče, které je možné nainstalovat do pokladny, resp. přihrádek na bankovky a poplach je u nich vyvolán při odebrání všech bankovek z této přihrádky.

Obrázek 26: Detektor poslední bankovky S3555 [19]

7.5 Změna přístupu k havarijnímu plánování

Dokumenty havarijního plánování, manuály a plány postupů obnovy informačních systémů budou funkční pouze tehdy, pokud budou aktuální. S tím souvisí i ověření praktické proveditelnosti celých havarijních plánů, popř. jejich dílčích částí.

Navrhuji proto provádět pravidelná cvičení odpovědných zaměstnanců – alespoň jednou za půl roku a to tímto způsobem:

1. ověření kompletního havarijního plánu náhodně vybraného informačního systému jedním z pracovišť Katastrálního úřadu pro Zlínský kraj

2. ověření použitelnosti (čitelnosti) náhodně zvoleného archivačního média všemi katastrálními pracovišti

O takto provedeném testování bude za každé katastrální pracoviště Katastrálního úřadu pro Zlínský kraj proveden zápis, který bude vyhodnocen administrátory oddělení podpory ICT a na jeho základě předloženy řediteli katastrálního úřadu návrhy na úpravu – zefektivnění stávajících havarijních plánů.

ZÁVĚR

Ve své diplomové práci se zabývám analýzou současného stavu přepážkových pracovišť v podmínkách Katastrálního úřadu pro Zlínský kraj. Při výkonu státní správy v oblasti katastru nemovitostí se katastrální pracoviště spoléhají na informace uložené v informačních systémech i mimo ně. Ztráta spolehlivosti, dostupnosti a integrity informací uložených v těchto systémech by proto měla velmi negativní, ne-li fatální dopad na chod celého úřadu a je důležité zajistit bezpečnost a ochranu těchto informací v jakékoliv formě.

Během analýzy bylo zjištěno, že Katastrální úřad pro Zlínský kraj má vypracovánu poměrně dobrou bezpečnostní politiku na úrovni jednotlivých informačních systémů (včetně podrobných havarijních plánů), ale samotné počítačové stanice přepážkových pracovišť nejsou nijak zvlášť chráněny.

V praktické části proto navrhuji opatření, která při minimálních finančních a organizačních nárocích řeší zjištěné nedostatky a rozšiřují stávající možnosti ochrany zaměstnanců, majetku a informací, které jsou v tomto prostoru soustředěny.

ZÁVĚR V ANGLIČTINĚ

In my diploma thesis I analyze the current state of counter workplaces in conditions of the Cadastral Office for Zlin region. The state administration execution relies on information stored in information systems and also beyond these systems. Loss of reliability, availability and integrity of information stored in these systems should therefore very negative, if not a fatal impact on the running of the office and it is important to ensure the safety and protection of this information in any form.

During the analysis it was found that the Cadastral Office for Zlin region has adopted a fairly good security policy at the level of individual information systems (including detailed emergency plans), but the counter workplaces computers itself are not specifically protected.

In practical part I suggest measures which solve identified gaps and expand the existing possibilities for protecting employees, assets and information that are concentrated in this area, with the minimum financial and organizational demands.

SEZNAM POUŽITÉ LITERATURY

[1] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press a.s., 2004. s. 190. ISBN 80-251-0106-1

[2] IVANKA, J., Systemizace bezpečnostního průmyslu I. 3. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. 123 s. ISBN 978-80-7318-850-4

[3] JAŠEK, R., Informační a datová bezpečnost. 1. vyd. Zlín: Academia centrum UTB, 2006. 140 s. ISBN 8073184567

[4] KINDL, J., Projektování bezpečnostních systémů I. 2. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 134 s. ISBN 978-80-7318-554-1

[5] LUDVÍK, M., Teorie bezpečnosti počítačových sítí. Praha: Computer media, 2008. 98 s. ISBN 978-80-86-686-35-6

[6] NORTHCUTT, S., Bezpečnost počítačových sítí. 1. vyd. Praha: Computer Press a.s., 2005, 592 s. ISBN 80-251-0697-7

[7] RAK, R., MATYÁŠ, V., ŘÍHA Z., Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada Publishing, a.s., 2008, 664 s. ISBN 978-80-247-2365-5.

[8] SMEJKAL, V., RAIS, K., Řízení rizik ve firmách a jiných organizacích. 2.vyd. Praha: Grada Publishing, a.s., 2006. 296 s. ISBN 80-247-1667-4.

[9] SODOMKA, P., Informační systémy v podnikové praxi. 1. vyd. Brno, Computer Press a. s., 2006. 351 s. ISBN 80-251-1200-4.

Interní dokumenty ČÚZK:

[10] Bezpečnostní politika ochrany informací, 2006

[11] Bezpečnostní směrnice pro provoz, údržbu a rozvoj IT, 2004

[12] Havarijní plány katastrálního úřadu pro Zlínský kraj, 2011

[13] Instalační šablona ISKN, 2009

[14] Konfigurační standard pro pracovní stanice, notebooky a uživatele, 2006

[15] Organizační řád KÚ pro Zlínský kraj, 2010

[16] Politika havarijního plánování v resortu ČÚZK, 2006

[17] Pravidla práce s výpočetní technikou pro uživatele, 2004

Elektronické zdroje:

[18] CCTV cameras guide, Fingerprint Security Ltd.

[19] Detektor poslední bankovky S3555, ADI Global a.s.

[20] HP StorageWorks Ultrium 448 TapeDrive Datasheet, HP Česká republika

[21] Jak si správně vybrat cylindrickou vložku [online], Assa Abloy s.r.o. [cit. 23. března 2011]. Dostupné z WWW: http://www.fab.cz/katalog/jak-si-spravne-vybrat

[22] Norma ČSN EN 50 131

[23] Produktová nabídka, Turkon s.r.o.

[24] Profil společnosti [online], Systém Plus Zlín s.r.o. [cit. 13. dubna 2011]. Dostupné z WWW: http://www.systemplus.cz/profil.htm

[25] Přehled bezdrátových detektorů pohybu, Jablotron s.r.o.

[26] Přiručka k EZS Paradox, Systemplus s.r.o.

[27] Technické zabezpečenie ochrany poštových prevádzok [online], Trilobit [cit. 28. března 2011]. Dostupné z WWW: http://trilobit.fai.utb.cz/technicke-zabezpecenie-ochrany-postovych-prevadzok

[28] Tísňové tlačítko HB304, GE Security

[29] VC220 Camera datasheet, Cisco Systems Inc.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADV	Akceptovatelná doba výpadku
AES	Advanced Encryption Standard
BIOS	Basic input/output system
CA	Computer Associaties
CSÚIS	Centrální systém účetních informací státu
ČSN	České státní normy
ČÚZK	Český úřad zeměměřický a katastrální
DC2	Datacentrum 2 - personální systém
DDNS	Dynamic Domain Name System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSBL	DNS based Blackhole List
DoS	Odepření služeb (Denial of Services)
DSM	Desktop and server Management
DVD	Digital Versatile Disc
EIS	Ekonomický informační systém
EKU	Extended key usage
EPS	Elektronická požární signalizace
EPVDS	Elektronická podatelna a výpravna navazující na informační systém datových schránek
EZS	Elektronický zabezpečovací systém
FTP	File Transfer Protocol
GE	General Electric company
GPIO	General Purpose Input / Output

HP	Hewlett-Packard Company
HTTP	Hypertext Transfer Protocol
HW	Hardware
HZS	Hasičský záchranný sbor
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICT	Information and communications technology
IDEA	International Data Encryption Algorithm
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IR	Infra Red
IS	Informační systém
ISA	Internet Security and Acceleration Server
ISKN	Informační systém katastru nemovitostí
ISP	Internet Services Provider - Poskytovatel internetových služeb
IT	Informační technologie
KP	Katastrální pracoviště
KÚ	Katastrální úřad
LAN	Local Area Network
LED	Light Emitting Diode
MBR	Master Boot Record
MPEG	Moving Picture Experts Group
MZS	Mechanický zábranný systém
NTP	Network Time Protocol
OS	Operační systém
PC	Osobní počítač

PCO	Pult Centrální Ochrany
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PIR	Passive infrared sensor
PoE	Power over Ethernet
PUK	PIN Unlock Key
RDP	Remote Desktop Protocol
RSA	Rivest, Shamir, Adleman cypher
RTP	Real-time Transport Protocol
SDK	Software developement kit
SGI	Soubor grafických informací
S-JTSK	Souřadnicový systém jednotné trigonometrické sítě katastrální
SMTP	Simple Mail Transfer Protocol
SPI	Soubor popisných informací
SW	Software
TPM	Trusted platform module
ÚOOÚ	Úřad pro ochranu osobních údajů
UPnP	Universal Plug & Play
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
VGA	Video Graphics Array
VPN	Virtual Private Network
WAN	Wide Area Network
WIFI	Wireless Fidelity
WSUS	Windows Server Update Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ÚZEMNÍ PŮSOBNOST KATASTRÁLNÍHO ÚŘADU PRO ZLÍNSKÝ KRAJ

Názvy, sídla a obvody územní působnosti katastrálních pracovišť Katastrálního úřadu pro zlínský kraj

Katastrální pracoviště Holešov se sídlem v Holešově, které vykonává působnost pro územní obvody obcí:

Blazice, Bořenovice, Brusné, Bystřice pod Hostýnem, Holešov, Horní Lapač, Chomýž, Chvalčov, Jankovice, Komárno, Kostelec u Holešova, Kurovice, Lechotice, Loukov, Ludslavice, Martinice, Míškovice, Mrlínek, Němčice, Osíčko, Pacetluky, Podhradní Lhota, Prusinovice, Přílepy, Rajnochovice, Roštění, Rusava, Rymice, Slavkov pod Hostýnem, Třebětice, Vítonice, Zahnašovice, Žeranovice.

Katastrální pracoviště Kroměříž, se sídlem v Kroměříži, které vykonává působnost pro územní obvody obcí:

Bařice-Velké Těšany, Bezměrov, Břest, Cetechovice, Dřínov, Honětice, Hoštice, Hulín, Chropyně, Chvalnov-Lísky, Jarohněvice, Karolín, Koryčany, Kostelany, Kroměříž, Kunkovice, Kvasice, Kyselovice, Litenčice, Lubná, Lutopecny, Morkovice-Slížany, Nítkovice, Nová Dědina, Pačlavice, Počenice-Tetětice, Prasklice, Pravčice, Rataje, Roštín, Skaštice, Soběsuky, Střílky, Střížovice, Sulimov, Šelešovice, Troubky-Zdislavice, Uhřice, Věžky, Vrbka, Zářičí, Zástřizly, Zborovice, Zdounky, Zlobice, Žalkovice.

Katastrální pracoviště Uherské Hradiště, se sídlem v Uherském Hradišti, které vykonává působnost pro územní obvody obcí:

Babice, Bílovice, Boršice, Boršice u Blatnice, Břestek, Březolupy, Buchlovice, Částkov, Hluk, Hostějov, Huštěnovice, Jalubí, Jankovice, Kněžpole, Kostelany nad Moravou, Košíky, Kudlovice, Kunovice, Medlovice, Mistřice, Modrá, Nedachlebice, Nedakonice, Ořechov, Ostrožská Lhota, Ostrožská Nová Ves, Osvětimany, Podolí, Polešovice, Popovice, Salaš, Staré Hutě, Staré Město, Stříbrnice, Stupava, Sušice, Svárov, Topolná, Traplice, Tučapy, Tupesy, Uherské Hradiště, Uherský Ostroh, Újezdec, Vážany, Velehrad, Zlámanec, Zlechov.

Katastrální pracoviště Uherský Brod, se sídlem v Uherském Brodě, které vykonává působnost pro územní obvody obcí:

Bánov, Bojkovice, Březová, Bystřice pod Lopeníkem, Dolní Němčí, Drslavice, Horní Němčí, Hostětín, Hradčovice, Komňa, Korytná, Lopeník, Nezdenice, Nivnice, Pašovice, Pitín, Prakšice, Rudice, Slavkov, Starý Hrozenkov, Strání, Suchá Loz, Šumice, Uherský Brod, Vápenice, Veletiny, Vlčnov, Vyškovec, Záhorovice, Žitková.

Katastrální pracoviště Valašské Klobouky, se sídlem ve Valašských Kloboukách, které vykonává působnost pro územní obvody obcí:

Biskupice, Bohuslavice nad Vláří, Brumov-Bylnice, Dolní Lhota, Drnovice, Haluzice, Horní Lhota, Jestřabí, Křekov, Lipová, Loučka, Ludkovice, Luhačovice, Návojná, Nedašov, Nedašova Lhota, Petrůvka, Podhradí, Poteč, Pozlovice, Rokytnice, Rudimov, Sehradice, Slavičín, Slopné, Šanov, Štítná nad Vláří-Popov, Študlov, Tichov, Újezd, Valašské Klobouky, Valašské Příkazy, Vlachova Lhota, Vlachovice, Vysoké Pole.

Katastrální pracoviště Valašské Meziříčí, se sídlem ve Valašském Meziříčí, které vykonává působnost pro územní obvody obcí:

Branky, Dolní Bečva, Horní Bečva, Hutisko-Solanec, Choryně, Jarcová, Kelč, Kladeruby, Kunovice, Lešná, Loučka, Mikulůvka, Oznice, Podolí, Police, Prostřední Bečva, Rožnov pod Radhoštěm, Střítež nad Bečvou, Valašská Bystřice, Valašské Meziříčí, Velká Lhota, Vidče, Vigantice, Zašová, Zubří.

Katastrální pracoviště Vsetín, se sídlem ve Vsetíně, které vykonává působnost pro územní obvody obcí:

Bystřička, Francova Lhota, Halenkov, Horní Lideč, Hošťálková, Hovězí, Huslenky, Jablůnka, Janová, Karolinka, Kateřinice, Lačnov, Leskovec, Lhota u Vsetína, Lidečko, Liptál, Lužná, Malá Bystřice, Nový Hrozenkov, Pozděchov, Prlov, Pržno, Ratiboř, Růžďka, Seninka, Střelná, Ústí, Valašská Polanka, Valašská Senice, Velké Karlovice, Vsetín, Zděchov.

Katastrální pracoviště Zlín, se sídlem ve Zlíně, které vykonává působnost pro územní obvody obcí:

Bělov, Bohuslavice u Zlína, Bratřejov, Březnice, Březová, Březůvky, Dešná, Dobrkovice, Doubravy, Držková, Fryšták, Halenkovice, Hostišová, Hrobice, Hřivínův Újezd, Hvozdná, Jasenná, Kaňovice, Karlovice, Kašava, Kelníky, Komárov, Lhota, Lhotsko, Lípa, Lukov, Lukoveček, Lutonina, Machová, Mysločovice, Napajedla, Neubuz, Oldřichovice, Ostrata, Otrokovice, Podkopná Lhota, Pohořelice, Provodov, Racková, Sazovice, Slušovice, Spytihněv, Šarovy, Tečovice, Tlumačov, Trnava, Ublo, Velký Ořechov, Veselá, Vizovice, Vlčková, Všemina, Zádveřice-Raková, Zlín, Želechovice nad Dřevnicí, Žlutava.

PŘÍLOHA PII: SEZNAM VOLNĚ DOSTUPNÝCH WEBOVÝCH STRÁNEK

Resortní webové stránky:	
http://www.cuzk.cz	Český úřad zeměměřický a katastrální
http://nahlizenidokn.cuzk.cz	Nahlížení do katastru nemovitostí
http://dataz.cuzk.cz	Databáze bodových polí
http://czepos.cuzk.cz	Česká síť permanentních stanic pro určování polohy
http://katastralnimapy.cuzk.cz	Katastrální mapy
http://archivnimapy.cuzk.cz	Archivní mapy
http://www.vugtk.cz	Výzk. ústav geodetický, topografický a kartografický
Vláda, Parlament, Ministerstva:	
http://www.vlada.cz	Vláda České republiky
http://www.psp.cz	Parlament České republiky
http://www.senat.cz	Senát Parlamentu České republiky
http://www.mdcr.cz	Ministerstvo dopravy
http://www.mfcr.cz	Ministerstvo financí
http://www.mkcr.cz	Ministerstvo kultury
http://www.army.cz	Ministerstvo obrany
http://www.mpsv.cz	Ministerstvo práce a sociálních věcí
http://www.mmr.cz	Ministerstvo pro místní rozvoj
http://www.mpo.cz	Ministerstvo průmyslu a obchodu
http://www.justice.cz	Ministerstvo spravedlnosti
http://www.msmt.cz	Ministerstvo školství, mládeže a tělovýchovy
http://www.mvcr.cz	Ministerstvo vnitra
http://www.mzv.cz	Ministerstvo zahraničních věcí
http://www.mzcr.cz	Ministerstvo zdravotnictví

http://www.mze.cz	Ministerstvo zemědělství
http://www.mzp.cz	Ministerstvo životního prostředí
Weby provozované ministerstvy:	
http://inspire.gov.cz	Národní geoportál INSPIRE
http://wwwinfo.mfcr.cz	Administrativní registr ekonomických subjektů
http://cedr.mfcr.cz	Centrální evidence dotací z rozpočtu
http://app.mfcr.cz/FKVS	Informační systém finanční kontroly ve veřejné správě
https://isp.mfcr.cz	Informační systém o platu a služebním příjmu
https://portal.statnipokladna.cz	Státní pokladna
http://forms.mpsv.cz/uir/	Územně identifikační registr adres
http://www.justice.cz/	Obchodní rejstřík Evidence úpadců Evidence znalců a tlumočníků Přehled státních zástupců Přehled soudců
https://isir.justice.cz	Insolvenční rejstřík
http://aplikace.mvcr.cz/adresa/	Adresy v České republice
http://aplikace.mvcr.cz/sbirka-zakonu/	Sbírka zákonů a mezinárodních smluv
http://www.isvs.cz	Informační systémy veřejné správy
https://portal.gov.cz	Portál veřejné správy České republiky
http://www.mojedatovaschranka	Informační systém datových schránek
http://www.czechpoint.cz	Czechpoint
Akreditované certifikační autority:	
http://www.ica.cz	První certifikační autorita
http://www.postsignum.cz	PostSignum
http://www.edientity.cz	eIdentity
Ostatní webové stránky:	
http://slovnik-cizich-slov.abz.cz	ABZ.cz: slovník cizích slov

http://www.nature.cz	Agentura ochrany přírody a krajiny
http://www.cas.cz	Akademie věd České republiky
http://www.ujc.cas.cz	Akademie věd ČR - Ústav pro jazyk český
http://www.wkonline.cz	ASPI Online
http://www.bozpinfo.cz	BOZP info
http://www.ccs.cz	CCS - nákup PHM
http://www.centralniadresa.cz	Centrální adresa
http://www.cak.cz	Česká advokátní komora
http://www.cnb.cz	Česká národní banka
http://abok.cnb.cz/	Česká národní banka - systém ABO-K
http://www.ceskaposta.cz	Česká pošta, s.p.
http://www.cssz.cz	Česká správa sociálního zabezpečení
http://www.cmkos.cz	Českomoravská konfederace odborových svazů
http://www.chmi.cz	Český hydrometeorologický ústav
http://www.vykazy.cz	Český statistický úřad - výkazy
http://www.datacentrum.cz	DataCentrum (helpdesk)
http://elev.institutpraha.cz	e-learning Institutu pro Státní správu
http://gem.b2bcentrum.cz	Elektronické tržiště pro veřejnou správu
http://www.epusa.cz	Elektronický portál územních samospráv
http://www.ekcr.cz	Exekutorská komora ČR
http://maps.google.cz	Google Mapy
http://www.isvz.cz	Informační systém o veřejných zakázkách
http://www.imsbrno.cz	Institut mezioborových studií (IMS) Brno
http://iss-edu.edoceo.cz	Institut státní správy
http://www.iso.org	International Organization for Standardization
http://idos.cz	Jízdní řády

http://www.mapy.cz	Mapy.cz
http://www.muni.cz	Masarykova univerzita Brno
http://monumnet.npu.cz	MonumNet - Seznam památek
http://www.jasu.org	MÚZO Praha
http://www.nsoud.cz	Nejvyšší soud ČR
http://www.nssoud.cz	Nejvyšší správní soud ČR
http://www.deutschepost.de	Německá pošta
http://www.nkcr.cz	Notářská komora ČR
http://www.poczta-polska.pl	Polská pošta
http://www.obce.cz	Portál Města a obce online
http://www.pfcr.cz	Pozemkový fond České republiky
http://www.pravidla.cz	Pravidla českého pravopisu
http://www.sbirka.cz	Sbírka předpisů České republiky
http://www.epravo.cz	Sbírka zákonů, judikatura, právo
http://www.posta.sk	Slovenská pošta
https://www.katasterportal.sk	Slovensky Katastrálny portál
http://slovnik.seznam.cz	Slovnik
http://www.sodexo.cz	Sodexo - elektronické objednávání stravenek
http://www.soka-cr.cz	Státní okresní archiv v Chrudimi
https://servicedesk.stc.cz	Státní tiskárna cenin - Service Desk
http://unmz.cz	Stránky publikovaného obsahu ÚNMZ
http://www.edenred.cz	stravenky TICKET RESTAURANT
http://www.vsb.cz	Technická univerzita Ostrava - Vysoká škola báňská
http://www.upol.cz	Univerzita Palackého v Olomouci
http://www.compet.cz	Úřad pro ochranu hospodářské soutěže
http://www.vutbr.cz	Vysoké učení technické v Brně

http://www.zpmvcr.cz	Zdravotní pojišťovna ministerstva vnitra ČR
http://www.rzp.cz	Živnostenský rejstřík
http://eur-lex.europa.eu	Přístup k právu Evropské unie
http://ftp.aspi.cz	ASPI - právní předpisy
http://www.beck-online.cz	Beck Online - právní předpisy
http://www.iss-edu.cz	Portál e-learningových kurzů MV ČR

PŘÍLOHA P III: SYSTEM PLUS – VZOROVÁ SMLOUVA O NAPOJENÍ NA PULT CENTRÁLNÍ OCHRANY

Smlouva o dílo č. 0000

o připojení elektrické zabezpečovací signalizace na pult centrální ochrany a monitorování objektu

Zhotovitel: System plus Zlín, s.r.o.
sídlo firmy: Kelníky 28, 763 07 Velký Ořechov
provozovna: Pod Babou 4260, 760 01 Zlín
zastoupený: Zdeňkem Džoganikem – jednatelem
IČO: 25558021
DIČ: CZ25558021
společnost je zapsaná u: KOS v Brně, oddíl C, vložka 1459

Objednatel: ……
sídlo firmy: ……
zastoupený: ……
IČO: ……
DIČ: ……
společnost je zapsaná u: ……
e-mail pro fakturaci: ……

Pro objekt:
název objektu: ……
adresa objektu: ……
tel. spojení do objektu: ……
e-mail: ……

Dodavatel EZS /tel. kontakt System plus Zlín, s.r.o. / 577 211 157
Servis a pravidelné revize zajištěné dodavatelem EZS: ano ne

1. Předmět smlouvy:
1.1 Předmětem této smlouvy je závazek zhotovitele poskytovat ochranu objektu objednatele napojením elektrické zabezpečovací signalizace (dále jen EZS) na pult centralizované ochrany (dále jen PCO) zhotovitele.

1.2 Zhotovitel poskytuje ochranu objektu objednatele na základě poplachového signálu z EZS objednatele přeneseného do systému PCO zhotovitele:
a) Okamžitým výjezdem zásahové jednotky do objektu objednatele s cílem odvrátit nebezpečí a zabránit škodám, a to v nejkratším čase od obdržení poplachového signálu, pokud nenastanou nepředvídatelné okolnosti.
b) Kontrolou objektu a provedením nezbytných opatření k zajištění bezpečnosti objektu při jeho narušení, zejména vnějším střežením objektu do příjezdu policejních orgánů a obnovení činnosti EZS, pokud objednatel nevydá jiný pokyn.
c) Okamžitým oznámením zjištěného stavu příslušným orgánům, jestliže nelze vlastním přičiněním nebo úsilím zabránit škodě, nebo je podezření, že narušením objektu byl spáchán trestný čin nebo přestupek.

d) Vyrozuměním objednatele nebo jím pověřené osoby.

1.3 Předmětem této smlouvy není, a za neplnění této smlouvy se nepovažuje, jestliže pracovníci zásahové jednotky přes vynaložené úsilí nedopadnou narušitele objektu.

2. Další ujednání:

Objednatel splní následující podmínky pro připojení na PCO:

2.1 Objekt bude vybaven zařízením EZS s ústřednou schopnou komunikace:
a) pomocí metalické telefonní linky nebo
b) pomocí dodaného zařízení zhotovitele (vysílač NAM, komunikátor GPRS-SMS, ethernet komunikátor)

2.2 EZS bude v objektu objednatele instalována oprávněnou fyzickou či právnickou osobou. Systém EZS musí splňovat ČSN 33 4590, resp. ČSN EN 50 131 a komponenty EZS budou mít platný atest pro minimálně stupeň zabezpečení 2 - nízké až střední riziko dle ČSN EN 50131-1.

2.3 Obsluha EZS v objektu bude prováděna osobami, které byly prokazatelně seznámeny s činností a obsluhou.

2.4 Objekt bude (dle charakteru) vybaven potřebnými mechanickými zábranami proti vloupání.

2.5 Objednatel bude neprodleně informovat o nových skutečnostech, které mají vliv pro připojení na PCO, zavazuje se aktualizovat kontaktní osoby pro vyrozumění v případě narušení objektu.

2.6 Objednavatel tímto prohlašuje, že je oprávněn nakládat se střeženým předmětem ostrahy (objektem) z titulu vlastnictví či nájemní smlouvy, a že tento předmět ostrahy je samostatně pojištěn smlouvou proti škodám na majetku v souvislosti s krádeží vloupáním.

3. Cena a platební podmínky

3.1 Cena:
Za připojení na PCO: -----,- Kč + DPH
Za technické zabezpečení přenosu: -----,- Kč + DPH / měsíc
Za použití tísňového tlačítka (napadení osob) -----,- Kč + DPH / měsíc
Za pravidelné zasílání výpisu historie EZS e-mailem -----,- Kč + DPH
Za střežení objektu dle bodu 4.8. a nad rámec uvedený v bodě 4.3 této smlouvy. -----,- Kč + DPH / 1hod.

3.2 Paušální čili opakované platby za technické zabezpečení přenosu budou prováděny na základě vystavené faktury se splatností 10 dní na účet banky HVB ve Zlíně, č.ú. XXXXXXX/XX00, variabilní symbol je číslo faktury. Faktury budou vystavovány čtvrtletně dopředu tj. za I. čtvrtletí 1. 1., za II. čtvrtletí 1. 4., III. čtvrtletí 1. 7., IV. čtvrtletí 1. 10. Tento den bude považován za datum uskutečnění zdanitelného plnění.
Vystavení faktury bude provedeno během prvních 15 dní příslušného měsíce, který připadá jako první měsíc čtvrtletí.

3.3 Cena je uvedena bez DPH, daň bude vypočtena při fakturaci dle zákona o DPH.
Objednatel se zavazuje uhradit cenu za provedené služby do 10 kalendářních dnů ode dne doručení faktury.

4. Zhotovitel se zavazuje:
4.1 Zajistit bezprostředně po přijetí poplachového signálu fyzické prověření příčin vyslání signálu a zabránění vzniku následných majetkových a jiných škod. Zásah bude proveden profesionálními pracovníky s cílem co nejrychlejšího dosažení objektu objednatele tak, aby bylo v co největší míře zabráněno vzniku následných majetkových a jiných škod.

4.2 Na místě zásahu jsou pracovníci zhotovitele povinni se přesvědčit o příčině signálu. V případě skutečného napadení postupovat neprodleně tak, aby bylo zabráněno vzniku následných majetkových a jiných škod, uvědomit Policii ČR nebo městskou policii a zástupce objednatele, popř. zajistit pachatele, který škodu způsobil. Při těchto činnostech se řídí pracovníci obecně závaznými předpisy, především pak ustanovením §13 a §14 trestního zákona, aj. zákonných ustanovení, dotýkajících se ochrany majetku a zdraví osob.

4.3 Pokud nebude nutný okamžitý zásah, zhotovitel se zavazuje, že bude vstup a zásahy do vnitřních prostor objektu objednatele provádět pouze v přítomnosti osob, jež jsou uvedeny jako oprávnění zástupci objednatele (kontaktní osoby). Pokud se do 30 min odpovědná osoba nedostaví, povinnost ve smyslu tohoto bodu pomíjí.

4.4 Poskytovat odbornou pomoc a informace ke zvýšení účinnosti ochrany objektů.

4.5 K přísné mlčenlivosti o všech skutečnostech, se kterými se seznámí v souvislosti s plněním ustanovení této smlouvy i po skončení smluvního vztahu.

4.6 Spolupracovat při připojení na PCO a testování spolehlivosti EZS prováděném instalační firmou.

4.7 V případě vzniku škody zaviněné zhotovitelem, bude tato řešena v návaznosti na jeho pojistnou smlouvu a odpovědnosti za způsobené škody.

4.8 V případě potřeby zajistit fyzické střežení objektu, pokud by to situace vyžadovala.

5. Společná ujednání:
5.1 V případě, že nebude provedena platba za plnění dle předmětu této smlouvy ve stanoveném termínu a dohodnuté výši, má zhotovitel právo objednatele z PCO bez prodlení odpojit. O odpojení bude zhotovitel objednatele informovat.

5.2 Zhotovitel není odpovědný za neplnění činností obsažené v bodě 1. Předmět smlouvy v případě, kdy objednatel nemá poskytnuty funkční služby: přenos tel. linkou, přenosy GPRS -SMS, přenos internetem.

5.3 Smlouva se uzavírá na dobu neurčitou. Každá ze smluvních stran ji může vypovědět bez uvedení důvodů doporučeným dopisem s tříměsíční výpovědní lhůtou. Výpovědní lhůta začíná běžet od prvního dne měsíce následujícího po doručení výpovědi. Doplňky nebo změny této smlouvy je třeba společně projednat a realizovat písemnou formou jako doplněk smlouvy.

5.4 Obě smluvní strany souhlasí s tím, že mohou být druhou stranou prezentovány ve firemní dokumentaci, kde budou uvedeny jen všeobecné informace a vzájemně se tímto obě smluvní strany nebudou poškozovat.

5.5 Smlouva je vyhotovena ve dvou výtiscích uložených u objednatele 1ks a u zhotovitele 1ks.

5.6 Smlouva nabývá platnosti dnem podpisu oprávněných zástupců obou smluvních stran.

5.7 Při přerušení telefonní linky, zrušení služby GPRS-SMS u mobilního operátora, zrušení služby u provozovatele internetu, nedobití kreditu SIM karty nelze zařízení EZS považovat za funkční a monitorovat na PCO.

5.8 Výše úhrady za nedůvodný opakovaný výjezd se stanovuje na **xxx,- Kč + DPH** (při nedbalém zabezpečení objektu, včasným neodvoláním poplachu nebo nedůvodného vyslání signálu z tlačítka „Tíseň“).

Ve Zlíně dne ……..